Journal of Physics B: Atomic, Molecular and Optical Physics

PAPER • OPEN ACCESS

Quantum secrecy in thermal states

To cite this article: Elizabeth Newton *et al* 2019 *J. Phys. B: At. Mol. Opt. Phys.* **52** 125501

View the article online for updates and enhancements.

OPEN ACCESS
IOP Publishing
Journal of Physics B: Atomic, Molecular and Optical Physics
J. Phys. B: At. Mol. Opt. Phys. 52 (2019) 125501 (9pp)
https://doi.org/10.1088/1361-6455/ab1e91

Quantum secrecy in thermal states

Elizabeth Newton[1], **Anne Ghesquière**[1], **Freya L Wilson**[1], **Benjamin T H Varcoe**[1] 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: a.ghesquiere@leeds.ac.uk

Received 24 August 2018, revised 20 December 2018
Accepted for publication 1 May 2019
Published 28 May 2019

Abstract

We propose to perform quantum key distribution using quantum correlations occurring within thermal states produced by low power sources such as LEDs. These correlations are exploited through the Hanbury Brown and Twiss effect. We build an optical central broadcast protocol using a superluminescent diode which allows switching between laser and thermal regimes, enabling us to provide comparable experimental key rates in both regimes. We provide a theoretical analysis and show that quantum secrecy is possible, even in high noise situations.

Keywords: quantum secrecy, thermal states, discord, Hanbury Brown and Twiss, quantum correlations

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

Prelude

In 2016, China launched what Gibney dubbed the *first quantum satellite* [1], the intent of which is to perform quantum key distribution between the satellite and ground stations, see for instance [2]. This is just one of the current practical schemes designed to perform quantum secure key distribution and communication between parties; other examples include the DARPA network [3], the SECOQC project [4], or the Durban-QuantumCity project [5, 6], which use fibre-optic technologies to build quantum networks. These technologies rely on optical communication setups that were proven to be sufficient for performing quantum key distribution (QKD) [7]. Optical setups commonly work over great distances and achieve high bit rate; for instance, the Cambridge Quantum Network achieves a secure key rate of about 2.5 Mb s^{-1} [8, 9]. Such heavy duty infrastructure is, however, impractical for a plethora of short distance applications which nonetheless require high levels of encryption. Examples include key distribution and renewal between a mobile device and a medical implant, between an electronic car key and its lock or even between a mobile device and a password blackbox. These low power applications may need shorter key, lower bandwidth and as a result, an infrastructure built on high power lasers, single photons or entangled photons sources, may well be unsuitable. Reducing light source requirements to LEDs producing thermal states would allow us to explore the realm of low power applications and to appeal to a different set of customers.

The consideration of thermal states as a resource for QKD is not merely a technological preference, quite far from it. Thermal radiation is bunched, meaning that its quanta are likely to be detected in correlated pairs. These correlations produce quantum discord, as demonstrated by Ragy and Adesso using the Rényi entropy [10]. Furthermore, Pirandola [11] establishes theoretically that non-zero quantum discord is necessary for QKD, and that positive discord in a central broadcast-type protocol allows a quantum secure key to be extracted even with high levels of noise. Indeed, quantum discord has been established as a measure of quantum correlations [12]. Correlations can be qualified using the second-order correlation coefficient, generally known as $g^{(2)}(\tau)$, defined as

$$g^{(2)}(\tau) = \frac{\langle Y(t)Y(t+\tau)\rangle}{\langle Y(t)\rangle\langle Y(t+\tau)\rangle},$$

where $Y(t)$ is the radiation intensity. Radiation can then be characterised using $g^{(2)}$ as: anti-bunched (purely non classical) when $g^{(2)}(0) < 1$, coherent when $g^{(2)}(0) = 1$, and bunched

0953-4075/19/125501+09$33.00

when $g^{(2)}(0) > 1$ [13]. We use this classification in order to experimentally verify that we are operating in the thermal regime, as can be seen later in figures 3 and 4.

To exploit the correlations within bunched pairs requires the photon pairs to be separated and shared between two parties (e.g. Alice and Bob); this is done using the Hanbury Brown and Twiss (HBT) interferometer [14, 15], designed in the 50's to remedy the shortcomings of amplitude interferometers, such as the Michelson interferometer [16, 17], used in astronomy to determine the radius of stellar objects. The HBT's table-top set-up is simple: a source shines onto a beamsplitter, creating two arms, each shining onto a separate detector. The theory behind the observed interference effect has been studied by a number of authors, amongst the first Purcell [18] and Mandel [19, 20], whose papers provide a nicely intuitive pre quantum optical description (see [21]) of the statistics.

Mandel's analysis relies on the fact that what we count are not the photons themselves, but the photoelectrons ejected by the detector. Fluctuations in that number have two origins: very fast fluctuations in the intensity of the incoming signal, and the stochasticity of the reaction of the photo-sensitive material to its interaction with the radiation field (namely the ejection of a photoelectron). However, the detector is also fundamentally limited by its reaction time (or bandwidth) and therefore, very fast fluctuations may occur undetected. Yet, if these fluctuations are invisible, the correlations between them are not; in the original experiment and in current radio astronomy, the data used for calculations is often data which has been fed through a correlator (either hardware or software).

The production of photoelectrons is completely characterised by its average number $\overline{n_T}$ and several experiments have been performed to estimate it, such as [22–24]. These photon-counting experiments highlight that the bandwidth of the detector relates to the coherence time τ_c of the source, and that when the observation time $T \ll \tau_c$, $\overline{n_T}$ follows a single-mode Bose–Einstein distribution. This is in fact how thermal states are usually modelled in quantum optics, especially since this distribution naturally arises through the modelling of blackbody radiation. Thermal sources have short coherence times, so to resolve thermal behaviour, we require broadband detectors to satisfy $T \ll \tau_c$. Resolving thermal behaviour in a HBT set-up means that the individual detection events of the divided photons must take place within the coherence time.

A natural objection to the use of thermal states for quantum cryptography is the lifetime of the correlations, perhaps in light of the fragility of entanglement. However, current common implementations include very large telescope arrays such as VLA, ATCA or soon the SKA; another famous usage is the observation of the cosmic microwave background. Furthermore, the original HBT experiment was performed in the optical regime. In either regime, the correlations literally survive astronomical distances in free space. The use of thermal states therefore, naturally emerges as a potential partner to optical QKD techniques, especially with the rise of technologies such as WiFi and Bluetooth, which offer ever-increasing possibilities, such as through wall or medium range free space communications. Furthermore, we will show in the following, that in either the optical or the microwave regime, the protocol described below is quantum secure.

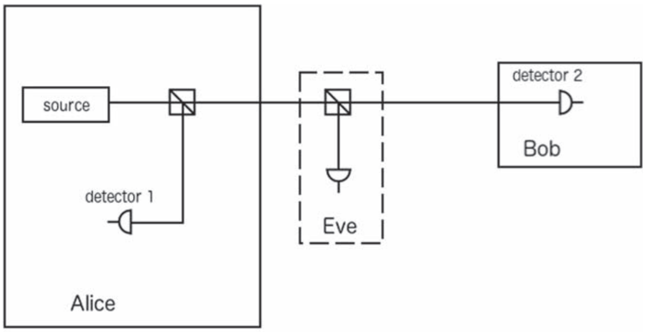

Figure 1. Schematic of the protocol. Even though Alice controls the source, this is a central broadcast because the signal is split between Alice and Bob. Alice does not prepare their state.

Next we describe the protocol we propose. We continue with a discussion of the eavesdropper (Eve), which will naturally lead us to analysing the security of the protocol and its theoretical modelling. As such, we show experimental results, as well as further theoretical discussions, including on the issue of detector noise.

Protocol

We propose a central broadcast protocol, reminiscent of Maurer and Wolf's scenario 1 in [25], shown on figure 1. It is described as follows:

- Alice creates a beam from a trusted thermal source.
- They then use a trusted beamsplitter with transmittance η_1 to divert and detect part of the transmission and send the rest on to Bob (Eve).
- The bunched nature of a thermal source means that fluctuations present at Alice's detector are correlated with those at Bob's detector.
- These fluctuations can be sliced into bits any number of ways, but with no loss of generality, we assume here that a fluctuation above the signal mean is a 1 and one below the mean is a 0.
- In order to detect an eavesdropper, Alice sends small random chunks of data to Bob who performs a $g^{(2)}$ calculation to verify thermality.
- 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 on figure 2. In order to simulate high levels of noise, we consider an attenuator channel between η_2 and Bob, equivalent to adding a beamsplitter of transmittance η_4 between η_2 and Bob, with a input state of variance N at the second input arm.

Let us emphasise that this is not a prepare-and-send scheme, but instead relies on central broadcasting. This means that although we assume that Alice controls the source, they

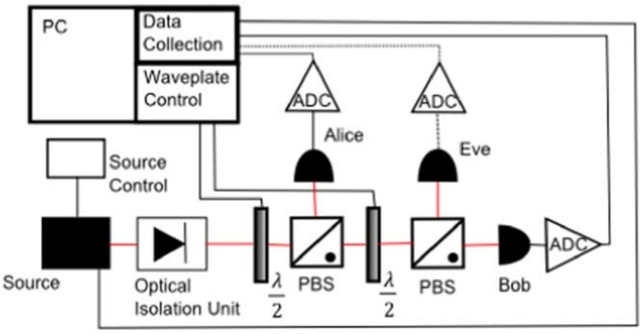

Figure 2. Diagram of the experimental set-up. Thermal or coherent light is produced at the source. The combination of half wave plate $\left(\frac{\lambda}{2}\right)$ and polarising beam splitter (PBS) acts as a controllable beam splitter, allowing a controlled amount of light through. This first combination acts as η_1, directing part of the beam to Alice, and the second combination acts as η_2, directing a further part of the beam to Eve.

do not in fact, prepare their states. Most current QKD schemes use a point-to-point scheme; as a result, in these schemes thermal states are a hindrance. We shall show here that this is not the case in a Central Broadcast Scheme.

Even if Eve interferes with the signal on its way to Bob via the most powerful attack available, we assume that she has no control over any part of Alice's apparatus, including the source, the beamsplitter (η_1) or the detector. Similarly, she has no control over Bob's detector.

The security of this protocol arises from the quantum correlations within the thermal fluctuations, those responsible for the Hanbury Brown and Twiss effect. Upon arrival at η_1 from the source, a bunched pair will either travel whole to Alice, travel whole onwards to face η_2 or split between Alice and η_2. Any pair travelling onwards to η_2 (and then η_4) will suffer the same fate, but the pairs we can exploit are those splitting between Alice and either Bob or Eve. Using the quantum correlations within the pairs is what allows us to cascade the beamsplitters this way, however, at the cost of photons pairs, and so of correlations. For instance, when η_1 is at 50%, half the light goes to Alice, the rest is to be shared between Eve and Bob. If η_2 is also at 50%, only a quarter of the original source signal is available to Bob (provided full transmission at η_4).

To model our protocol, we must know how to model Eve and for that, we must understand what actions she can take. Alice controls everything, from the source to their detector, including η_1. This means that the only place for Eve to 'insert' herself is on Bob's branch of the distribution, much like on most current prepare-and-send QKD schemes.

By current standards, the most powerful attack at Eve's disposal is a collective Gaussian attack. This is typically modelled by Eve mixing one mode out of an EPR sate with Bob's signal and recording the outcome for measurement upon Alice and Bob's classical communication [26]. As such, it is the attack modelled in this paper.

However, it is doubtful that Eve can, in fact, obtain any relevant information in a central broadcast scheme (CBS). The reason for that lies in the physics of the correlations themselves.

One conceivable attack would be for Eve to measure the signal going to Bob and reproduce it. We rely on bunched pairs, correlated via second-order temporal coherence. Should Eve be able to measure and reproduce Bob's photons fast enough, what prevents her from escaping detection?

The operative words in that sentence are 'fast enough'. Eve cannot beat Heisenberg's uncertainty principle, which limits her ability to detect and recreate withing a specific time, which is the signal coherence time τ_c. In the case of our experiment, $\tau_c \approx 5$ ps. Correlations in bunched pairs exist only for detection during that time. Simply applying Heisenberg's uncertainty principle, setting $\Delta t = \tau_c/2$, yields $\Delta E \geqslant 8.2 \times 10^{-28}$ eV for a photon of energy $E = 1.59$ eV. This is the maximum uncertainty which Eve is allowed for detecting and recreating the photon, to have a chance at fooling Alice and Bob by making Bob's detector click within the allotted time. This uncertainty does not of course, account for shot noise, and Eve can only allow for detection and/or preparation noise within the ΔE margin. Vacuum energy here is $E_0 = \frac{1}{2}\hbar c/\lambda \approx 0.13$ eV; this means that a single inescapable unit of shot noise is enough to push Eve past her limit.

This is a very crude argument, but it demonstrates that a simple intercept-and-resend scenario is useless. Actually, as we have explained before, Eve gains very little in using even an entangling cloner, because of the probabilistic ways that the photon pairs will split at η_1 then at η_2.

Modelling

Thermal states are Gaussian states; these states can be easily defined and manipulated through their first and second moments [27, 28]. 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 $\gamma_{\text{in}} = 2(\bar{n} + 1)\boldsymbol{I}$, where $\bar{n}$ is the average photon number and $\boldsymbol{I}$ the identity matrix, and null displacement. We consider in the present work, a displaced thermal state, with covariance matrix as before, but with non-null displacement (it can also be construed as a noisy coherent state).

We use the Bose–Einstein distribution

$$\bar{n} = \frac{1}{e^{\hbar\omega/k_B T} - 1}, \tag{1}$$

acknowledging all the caveats highlighted in the introduction, and considerdetectors measuring radiation at 30 GHz and $T = 300$ K, so that $\bar{n} = 1309$.

A beamsplitter is modelled as

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

where $\mu_i = \sqrt{1 - \eta_i}$ represents the loss. The input state at the first beamsplitter contains the thermal source and a vacuum state; it has covariance matrix and operator vector

$$\gamma_{\text{in}} = \begin{pmatrix} V_s^x & 0 \\ 0 & V_s^p \end{pmatrix} \bigoplus \boldsymbol{I}.$$

Since we give Eve an entangling cloner, she inputs one mode of her state at η_2 so the input state is of the form

$$\gamma_{\text{in}}^{\eta_2} = \gamma_{\text{out}}^{\eta_1} \bigoplus \begin{pmatrix} V_e^x & 0 \\ 0 & V_e^p \end{pmatrix}.$$

The output covariance matrix is

$$\Gamma_{\text{out}} = \begin{pmatrix} \Gamma_a & \Gamma_{ea} & \Gamma_{ab} & \Gamma_{an} \\ \Gamma_{ea} & \Gamma_e & \Gamma_{eb} & \Gamma_{en} \\ \Gamma_{ab} & \Gamma_{eb} & \Gamma_b & \Gamma_{bn} \\ \Gamma_{an} & \Gamma_{en} & \Gamma_{bn} & \Gamma_n \end{pmatrix}$$

where the sub-matrices of interest are

$$\begin{aligned}
\Gamma_a &= \begin{pmatrix} \mu_1^2 V_s^x + \eta_1 & 0 \\ 0 & \mu_1^2 V_s^p + \eta_1 \end{pmatrix}, \\
\Gamma_e &= \begin{pmatrix} \mu_2^2(\eta_1 V_s^x + \mu_1^2) + \eta_2 V_e^x & 0 \\ 0 & \mu_2^2(\eta_1 V_s^p + \mu_1^2) + \eta_2 V_e^p \end{pmatrix}, \\
\Gamma_{ea} &= \begin{pmatrix} \mu_1 \sqrt{\eta_1} \mu_2 (V_s^x - 1) & 0 \\ 0 & \mu_1 \sqrt{\eta_1} \mu_2 (V_s^p - 1) \end{pmatrix}, \\
\Gamma_{eb} &= \begin{pmatrix} -\mu_2 \sqrt{\eta_2} \sqrt{\eta_4} (\eta_1 V_s^x + \mu_1^2 - V_e^x) & 0 \\ 0 & -\mu_2 \sqrt{\eta_2} \sqrt{\eta_4} (\eta_1 V_s^p + \mu_1^2 - V_e^p) \end{pmatrix}, \\
\Gamma_b &= \begin{pmatrix} \eta_4(\eta_2(\eta_1 V_s^x + \mu_1^2) + \mu_2^2 V_e^x) + \mu_4^2 N & 0 \\ 0 & \eta_4(\eta_2(\eta_1 V_s^p + \mu_1^2) + \mu_2^2 V_e^p) + \mu_4^2 N \end{pmatrix},
\end{aligned} \tag{2}$$

In fact, Eve's full input state can be written as

$$\gamma_{\text{eve}} = \begin{pmatrix} \nu \boldsymbol{I} & \sqrt{\nu^2 - 1}\boldsymbol{Z} \\ \sqrt{\nu^2 - 1}\boldsymbol{Z} & \nu \boldsymbol{I} \end{pmatrix},$$

with $\boldsymbol{Z}$ the Pauli-Z matrix. However, only one mode of the EPR mixes with the legal signal at η_2. Since the rest of their state is unavailable to us, and of little practical value, we can trace it out for the sake of clarity. We can make further assumptions on Eve's state; she can be merely there and tap the channel, in which case, her inputs is one shot noise unit $V_e = 1\text{SNU}$. If she inputs a state, the minimum variance she can get away with is $V_e = 2\text{SNU}$, where 1SNU comes from her coherent state and the complementary 1SNU through shot noise.

We make the channel between η_2 and Bob a thermal noise channel by inputting a state of variance

$$N = \frac{\eta_4 \chi}{1 - \eta_4}, \qquad \text{with} \qquad \chi = \frac{1 - \eta_4}{\eta_4} + \epsilon,$$

and ϵ the channel excess noise [28]. The input state at η_4 is

$$\gamma_{\text{int}}^{\eta_4} = \gamma_{\text{out}}^{\eta_2} \bigoplus \begin{pmatrix} N & 0 \\ 0 & N \end{pmatrix},$$

where $\gamma_{\text{out}}^{\eta_2}$ is the state at the output of η_2 and N as defined previously.

The remaining block sub-matrices are given in the Appendix.

The secrecy will be witnessed using the secret key rate $K(A: B\|E)$, defined here in terms of its lower bound as $K(A: B\|E) = I(A: B) - \chi(B: E)$, where $\chi(B: E)$ is the Holevo bound, between Bob and Eve, which maximises their mutual information $I(B: E)$.

We define the mutual information as

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

where $S(\Gamma)$ is the Von Neumann entropy. The Von Neumann entropy $S(\rho) = -\text{Tr}(\rho \log \rho)$, for a Gaussian state, is simply determined in terms of the symplectic eigenvalues x_i of its covariance matrix Γ [28], as $S(\Gamma) = \sum_{i=1}^{k} g(x_i)$, where

$$g(x) = \left(\frac{x+1}{2}\right)\log\left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right)\log\left(\frac{x-1}{2}\right).$$

The correlation in the pairs shared between Alice and Bob is described with the quantum discord, $D(B|A)$, 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. We define the discord $D(B|A)$ as,

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

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

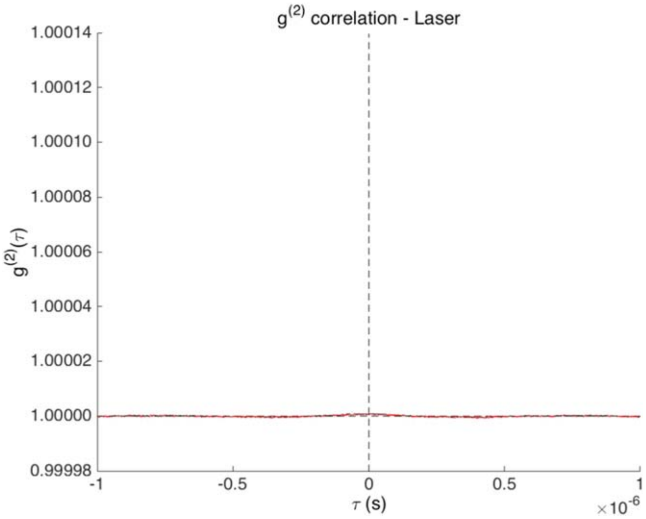

Figure 3. Experimental results : second order correlation coefficient for coherent states.

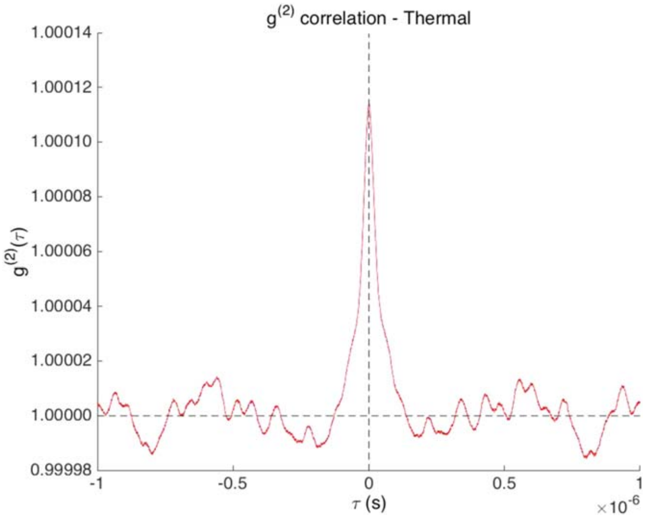

Figure 4. Experimental results : second order correlation coefficient for thermal states.

is the covariance matrix of B conditionned by a homodyne measurement on A [29], with $X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $()^{-1}$ the pseudo-inverse.

We write the Holevo bound $\chi(B: E)$ as

$$\chi(B\colon E) = S(\Gamma_e) - S(\Gamma_{e|x_b}),$$

where we estimate $\Gamma_{e|x_b}$ as above, using the submatrices we have derived through our modelling.

Results

The protocol was realised experimentally. The thermal source consists of a tuneable laser consisting of a superluminescent diode and an external cavity. When run above the operating current, the laser emitted non-thermal coherent light; when run below this operating current, it acted as a diode, producing thermal light. This effectively acts as a switch allowing the addition or removal of thermality in the source without altering any other part. We apply no modulation to the signal beyond that of the source. The source bandwidth was measured to be $\Delta\lambda = 0.4$ nm spread around a centre wavelength of $\lambda_0 = 780.09$ nm and the coherence time is as mentioned above, $\tau_c = 4.8$ ps. The detectors are ThorLabs Det36A photodiodes, coupled to a LeCroy Waverunner 44xi oscilloscope; the combined integration time is 14 ns and the oscilloscope samples at 5 GSps.

To determine the $g^{(2)}(0)$ coefficient, the source is run above and blow its operating current, so that we can make sure of its use as a thermal source. The data is normalised to zero; then the two data streams are shifted relative to each other by a time step defined by the sample rate $\Delta t = 0.2$ ns. Figures 3 and 4 show the second order correlations for each regime and show that

$$g^{(2)}(0)|_{\text{thermal}} > g^{(2)}(0)|_{\text{coherent}},$$

which we expected. In particular, figure 4 shows that in the thermal regime, $g^{(2)}(0) > 1$, which means that we are dealing with bunched radiation, fluctuations and as a result, correlations. Using the experimental parameters mentioned above, we can calculate a theoretical value of $g^{(2)}$ (0) = 1.0001 [30, 31], which agrees with the experimental values. This value of second order correlation is much less than 2; this is the result of experimental constraints, such as the relatively long integration time with respect to the source linewidth. However, by contrast, figure 3 shows virtually no deviation of $g^{(2)}(0)$ from 1. Since what we are interested in is the presence of correlations, not necessarily how much correlations there are (though obviously, the more the better), we can qualitatively establish the thermality of our source when it operates under its operating current. We now shine it through two variable beamsplitters, the first dividing a portion to Alice, and the second splitting the remaining light between Eve and Bob.

The data streams are sliced into bit strings. The information quantities are calculated using the Shannon entropies $H(x) = -\sum p(x)\log(p(x))$, where the $p(x)$'s are the measured frequencies. We plot the secret key rate $K'(A : B\|E) = I(A : B) - I(B : E)$ in figure 5.

The use of thermal light clearly provides a higher key rate than coherent light. The most optimal regime is for Alice and Bob to both receive equal portions of light, so the key rate peaks when $\eta_1 = 0.5$. We note easily that $K'(A : B\|E)$ (which is a lower bound) is negative when $\eta_1 \rightarrow 1$, so when no signal goes to Alice and as a result, they share no information with Bob. Recall that Alice is in control of η_1, and we assume that Eve cannot adversely affect this beamsplitter. When $\eta_1 = 0.5$, $K'(A : B\|E)$ decreases as η_2 decreases (so when Eve gets more of the signal) but nonetheless, it remains positive, meaning that key exchange is always possible, albeit with reduced rate in the high loss regimes. Furthermore, unlike conventional continuous variable schemes, a central broadcast scheme has the advantage that it does not exhibit a sharp drop off, so a secret key can always be produced. We should remark that since this specific implementation of the

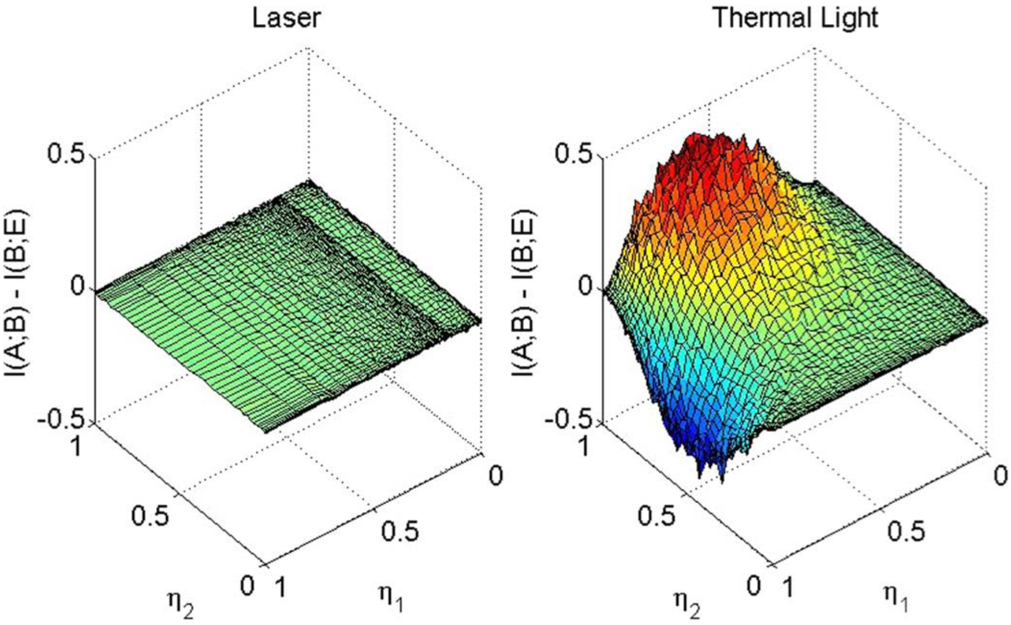

Figure 5. Experimental results : secret key rate for coherent states (left) versus thermal states (right). η_1 is controlled by Alice; when $\eta_1 = 1$, she has no signal and therefore, the key rate becomes negative. Similarly, as $\eta_1 \to 0$, she gains the advantage over Bob and Eve. As expected, the most advantageous value is when $\eta_1 = 0.5$.

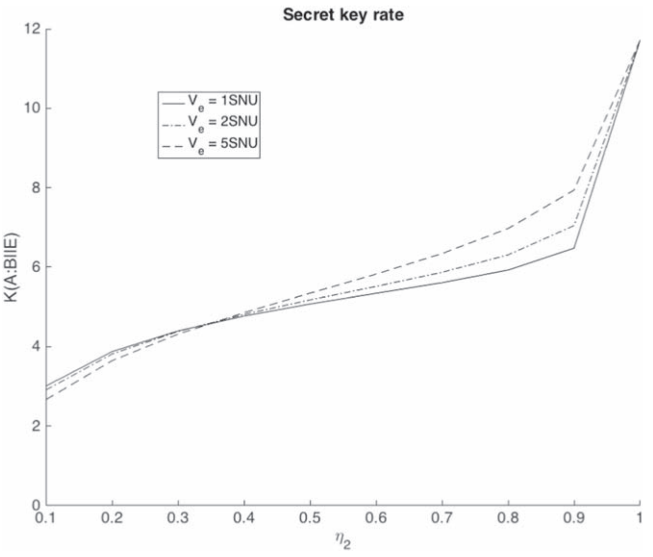

Figure 6. Secret key rate $K(A\colon B||E)$, plotted against η_2, for $\eta_4 = -7$ dB and $\epsilon = 10^{-2}$. The full line shows the secret key rate when the complementary input at η_2 is a vacuum state. The dashed-dotted line shows the secret key rate when Eve inputs a coherent state; the dashed line, when $V_e = 5$SNU. Visibly, any input on the part of Eve improves the key rate. As η_2 approaches full transmission, the secret key rate increases rapidly. The x-axis is cropped for readability.

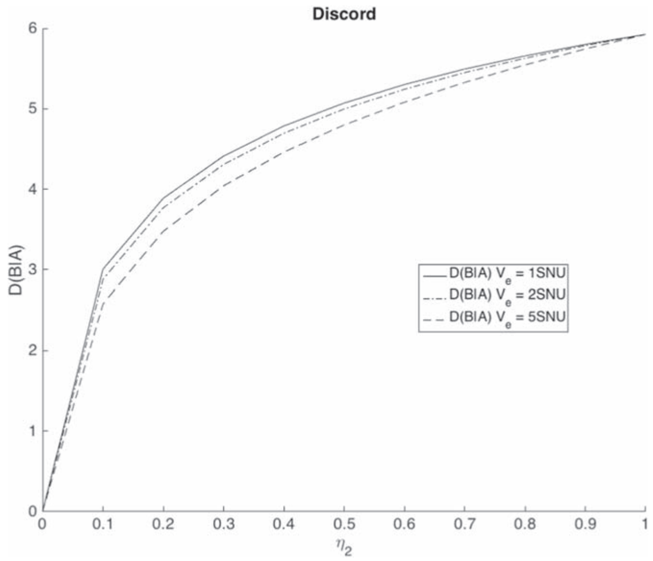

Figure 7. Discord $D(B|A)$, plotted against η_2, for $\eta_4 = -7$ dB and $\epsilon = 10^{-2}$. The full line shows the discord when the complementary input at η_2 is a vacuum state. The dashed-dotted line shows the discord when Eve inputs a coherent state; the dashed line, when $V_e = 5$SNU. As η_2 increases, so does the portion of the signal which goes to Bob and therefore, so does the discord. A non-vacuum complementary input at η_2 reduces the discord as it interferes with the correlated signal which Bob shares with Alice.

scheme uses broadband detectors, it is not sensitive to the loss of phase information. That being said, the theoretical analysis considers homodyne detection and would detect attacks which affect phase.

As seen on figure 6, the secret key rate is always positive, and so we conclude that there is always secrecy. It does, however, stagnate until η_2 approaches unity, i.e. until Eve lets most of the signal through. Key exchange is slow until Eve lets signal out; as a result, Eve is easily detectable. Let us recall also, that $K(A:B||E)$ is a lower bound; we can therefore expect better key rates. The secret key rate improves if Eve inputs a coherent state $V_e = 2$SNU, albeit marginally. This improvement is more pronounced if Eve inputs a thermal state $V_e = 5$SNU.

A crossover is obvious on the figure; at $\eta_2 = 30\%$ (so actually fairly low), Alice and Bob lose out if Eve inputs

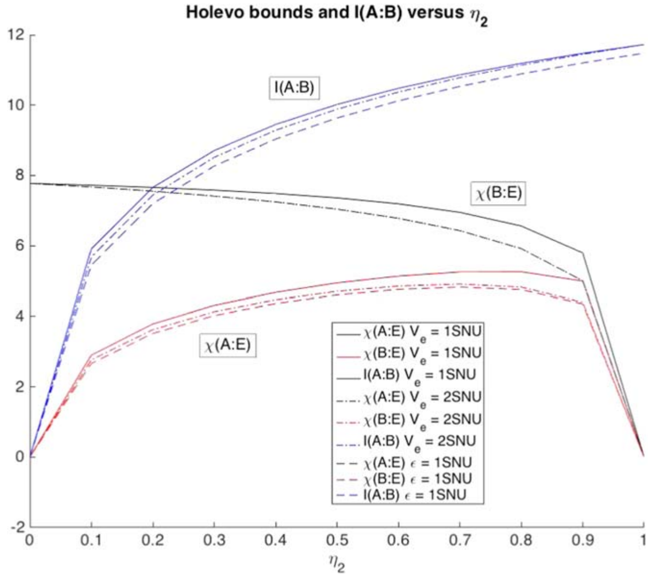

Figure 8. Holevo bounds and mutual information, plotted against η_2, for $\eta_4 = -7$ dB and $\epsilon = 10^{-2}$. The full line indicate that the complementary input at η_2 is a vacuum state; the dashed-dotted line, that $V_e = 2$SNU. Eve gains no more information by inputting a non-vacuum state; in fact, she fares worse. By contrast, the mutual information is only marginally reduced. The dashed line illustrates a channel excess noise $\epsilon = 1$SNU; as we expect, $I(A:B)$ and $\chi(B:E)$ suffer from a higher excess noise, but not $\chi(A:E)$ as neither Alice nor Eve are concerned with the thermal noise channel.

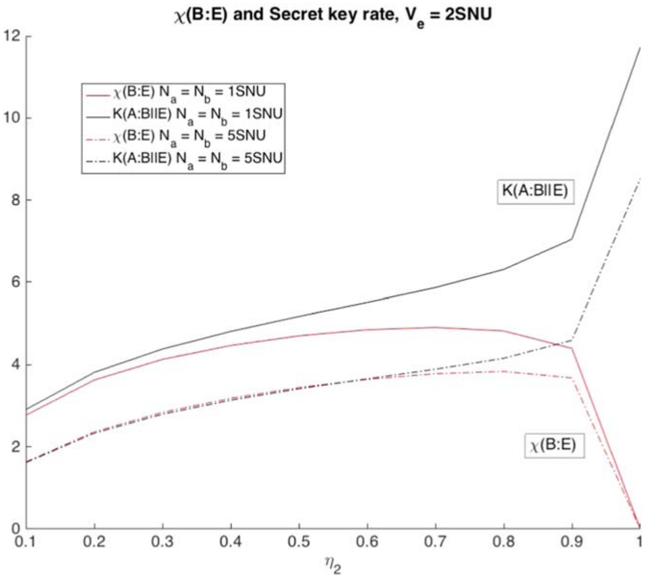

Figure 9. Effects of the detector noise on $\chi(B:E)$ and $K(A\colon B||E)$, $\eta_4 = -7dB$ and $\epsilon = 10^{-2}$. The full lines indicates that the detector noise at Alice and Bob's detectors, respectively N_a and N_b, are 1SNU. The dashed lines show such noise at 5SNU. The secret key rate suffers from detector noise, but so does $\chi(B:E)$. The x-axis is cropped for readability.

anything. As η_2 increases, Bob gets more and more of the signal; as a result, Alice and Bob's mutual information increases, and as can be seen on figure 8, $I(A:B)$ increases faster than $\chi(B:E)$.

Figure 7 demonstrates the effect of the presence of Eve on the discord. Of highest importance to us is that the discord is always positive. This means that the correlations between Alice and Bob are always quantum, and as a result, so is our security. As the transmittance η_2 increases, Eve gets less and less signal, so naturally, the discord increases. When Eve's input is higher than 1SNU (so when she inputs a coherent state), the discord gets worse, but not significantly.

Figure 8 shows how Eve's input influences the amount of information she could gain, by the input of a state such as defined previously. Contrary to what one might expect, coming from a point-to-point prepare-and-send mindset, Eve does not gain much by inputting a coherent state. The Holevo bounds $\chi(A:E)$ and $\chi(B:E)$ are worse for $V_e = 2$SNU than they are for $V_e = 1$SNU (vacuum). This scheme relies on bunched radiation; Eve's effect is to destroys these pairs. As a result, she becomes (separately) correlated with Alice and with Bob, which is what the Holevo bounds show. Her inputting a coherent state will not provide her with any more information, since it will not increase her correlation with either Alice nor Bob.

On figure 8, we also explore briefly the influence of channel excess noise ϵ (dashed lines). We note that $\chi(A:E)$ is not affected by ϵ; since the thermal noise channel is that which separates Eve and Bob, Alice is not affected. This is not the case for $I(A:B)$ and $\chi(B:E)$ which are both reduced by the channel excess noise. However, that reduction is insufficient to cause the key rate great damage. It is reduced but not significantly enough to impede key distribution.

Concluding remarks

The outcome of this analysis is that our scheme can always be considered quantum secure, since both the secret key rate and the discord are positive. Furthermore, we have shown that Eve's input is merely a disturbance, not only to the legal parties but most importantly to herself. This is simply a result of the physics; the thermal radiation is correlated and since Eve can only place herself after it has been split at η_1 (and therefore she has no access to Alice's information), she can gain little information. Eve's attack might be construed as a jamming attack; she is detected prior to reconciliation, can construct no key, but she can prevent Alice and Bob from building key.

Although we have included thermal channel noise, we have so far neglected the issue of preparation noise and of detector noise. We note that any preparation noise from the source is thermal, and so a part of the thermal state input at η_1, therefore affects both Alice and Bob (and Eve).

Detector noise, on the other hand, affects Alice and Bob individually and independently. Adding detector noise to Alice's and Bob's signal yields $V_a = V_a^{\text{pure}} + N_a$ and $V_b = V_b^{\text{pure}} + N_b$. We assume that Eve has no detector noise. Figures 6–8 were plotted for detector noise at the mandatory unit of shot noise, $N_a = N_b = 1$SNU. Detector noise will prevent Alice and Bob from detecting their correlations, but will not increase the correlations between Alice (Bob) and Eve. Therefore, it reduces the secret key rate, but also the Holevo bounds $\chi(A\colon E)$ and $\chi(B\colon E)$, as illustrated on figure 9. Although the key rate remains positive, detector noise is the greatest threat to it.

Figure 6 through 9 are plotted using theoretical values, and show a best case scenario. In contrats, figure 5 is obtained directly with experimental data and illustrate the limitations associated with the bandwidth. This explains the apparent discrepancies of scale.

There remains to be had perhaps, a discussion about distance. This issue is a subtle one. Bunched pairs (and quantum correlations) survive astronomical distances; in fact, they only vanish upon measurement. However, the correlations themselves will disappear if the photons are detected outside the coherence time. This means that the distance between η_1 and either Alice or Bob itself is not important; however, the path from η_1 to Alice and from η_1 to Bob should be of more or less equal length, i.e. within the coherence time of the source. This of course, places restrictions on Eve's attack, such as we have already described.

A central broadcast scheme is attractive because the source need not be controlled to the extent of a point-to-point scheme, and two parties can negotiate a key based on their correlated local noise. This leads to a number of potential applications for key exchange in a microwave system, such as long distance satellite communications and for example, between mobile phones in a mobile network, mass synchronisation of secure keys within an office space connected to a WiFi node, or even key synchronisation between a mobile phone and an implanted medical device.

NOTE IN REVIEW : since sending this work to publication, the authors have become aware of a subsequent publication [32].

Data that support the findings of this study are available from the Research Data Leeds Repository with the identifier https://doi.org/10.5518/206 [33].

Acknowledgments

The authors are grateful to network collaborators J Rarity, S Pirandola, C Ottaviani, T Spiller, N Luktenhaus and W Munro for very fruitful discussions. This work was supported by funding through the EPSRC Quantum Communications Hub EP/M013472/1 and additional funding for FW from Airbus Defense & Space.

Appendix. Full results

On the output of η_2, the submatrices are as follows

$$
\begin{aligned}
\gamma_a &= \begin{pmatrix} \mu_1^2 V_s^x + \eta_1 & 0 \\ 0 & \mu_1^2 V_s^p + \eta_1 \end{pmatrix}, \\
\gamma_b &= \begin{pmatrix} \eta_2(\eta_1 V_s^x + \mu_1^2) + \mu_2^2 V_e^x & 0 \\ 0 & \eta_2(\eta_1 V_s^p + \mu_1^2) + \mu_2^2 V_e^p \end{pmatrix}, \\
\gamma_e &= \begin{pmatrix} \mu_2^2(\eta_1 V_s^x + \mu_1^2) + \eta_2 V_e^x & 0 \\ 0 & \mu_2^2(\eta_1 V_s^p + \mu_1^2) + \eta_2 V_e^p \end{pmatrix}, \\
\gamma_{ea} &= \begin{pmatrix} \mu_1 \sqrt{\eta_1} \mu_2 (V_s^x - 1) & 0 \\ 0 & \mu_1 \sqrt{\eta_1} \mu_2 (V_s^p - 1) \end{pmatrix}, \\
\gamma_{eb} &= \begin{pmatrix} -\mu_2 \sqrt{\eta_2} (\eta_1 V_s^x + \mu_1^2 - V_e^x) & 0 \\ 0 & -\mu_2 \sqrt{\eta_2} (\eta_1 V_s^p + \mu_1^2 - V_e^p) \end{pmatrix}, \\
\gamma_{ab} &= \begin{pmatrix} -\mu_1 \sqrt{\eta_1} \sqrt{\eta_2} (V_s^x - 1) & 0 \\ 0 & -\mu_1 \sqrt{\eta_1} \sqrt{\eta_2} (V_s^p - 1) \end{pmatrix}.
\end{aligned}
\quad ,
$$

On the output of η_4, the submatrices are as follows

$$
\begin{aligned}
&\Gamma_a = \begin{pmatrix} \langle X_a^2 \rangle & 0 \\ 0 & \langle P_a^2 \rangle \end{pmatrix}, \quad \Gamma_e = \begin{pmatrix} \langle X_e^2 \rangle & 0 \\ 0 & \langle P_e^2 \rangle \end{pmatrix}, \\
&\Gamma_{ea} = \begin{pmatrix} \langle X_a X_e \rangle & 0 \\ 0 & \langle P_a P_e \rangle \end{pmatrix}, \quad \Gamma_{eb} = \sqrt{\eta_4} \gamma_{eb}, \\
&\Gamma_{ev} = -\mu_4 \gamma_{eb}, \quad \Gamma_{ab} = \sqrt{\eta_4} \gamma_{ab}, \quad \Gamma_{an} = -\mu_4 \gamma_{ab} \\
&\Gamma_b = \begin{pmatrix} \eta_4 \langle X_b^2 \rangle + \mu_4^2 N & 0 \\ 0 & \eta_4 \langle P_b^2 \rangle + \mu_4^2 N \end{pmatrix}, \\
&\Gamma_n = \begin{pmatrix} \mu_4^2 \langle X_b^2 \rangle + \eta_4 N & 0 \\ 0 & \mu_4^2 \langle P_b^2 \rangle + \eta_4 N \end{pmatrix} \\
&\Gamma_{bn} = \begin{pmatrix} \mu_4 \sqrt{\eta_4} (N - \langle X_b^2 \rangle) & 0 \\ 0 & \mu_4 \sqrt{\eta_4} (N - \langle P_b^2 \rangle) \end{pmatrix}
\end{aligned}
$$

ORCID iDs

Anne Ghesquière https://orcid.org/0000-0003-1595-7473
Benjamin T H Varcoe https://orcid.org/0000-0001-7056-7238

References

[1] Gibney E 2016 One giant step for quantum internet *Nature* **535** 478–9

[2] Liao S-K *et al* 2017 *Nature* **549** 43–7

[3] Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J and Yeh H 2005 arxiv:quant-ph/0503058v2

[4] Peev M *et al* 2009 *New J. Phys.* **11** 075001

[5] Petruccione F and Mirza A 2010 *Quest* **6** 52–5 https://hdl.handle.net/10520/EJC89774

[6] Mirza A and Petruccione F 2010 *J. Opt. Soc. Am.* B **27** A185–8

[7] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95

[8] Wonfor A *et al* 2017 High performance field trials of qkd over a metropolitan network Poster presentation QCrypt 2017

[9] Shields A 2017 Practical demonstration QCrypt 2017

[10] Ragy S and Adesso G 2013 *Phys. Scr.* **2013** 014052

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

[12] Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 *Rev. Mod. Phys.* **84** 1655

[13] Fox M 2006 *Quantum Optics An Introduction* (Oxford: Oxford University Press)

[14] Brown R H and Twiss R Q 1956 *Nature* **177** 27–9

[15] Brown R H and Twiss R Q 1956 *Nature* **178** 1046–8

[16] Michelson A A 1881 *Am. J. Sci.* **22** 120–9

[17] Michelson A A and Morley E W 1887 *Am. J. Sci.* **XXXIV** 333–45 https://history.aip.org/exhibits/gap/PDF/michelson.pdf

[18] Purcell E M 1956 *Nature* **178** 1449–50

[19] Mandel L 1958 *Proc. Phys. Soc.* **72** 1037

[20] Mandel L 1959 *Proc. Phys. Soc.* **74** 233

[21] Glauber R J 1963 *Phys. Rev.* **131** 2766–88

[22] Tan P K, Yeo G H, Poh H S, Chan A H and Kurtsiefer C 2014 *Astrophys. J. Lett.* **789** L10

[23] Martínez Ricci M L, Mazzaferri J, Bragas A V and Martínez E O 2007 *Am. J. Phys.* **75** 707–12

[24] Koczyk P, Wiewiór P and Radzewicz C 1995 *Am. J. Phys.* **64** 240–5

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

[26] Grosshans F, Acín A and Cerf N J 2007 Continuous-variable quantum key distribution *Quantum Information Continuous Variables Light* (London: Imperial College) pp 63–83

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

[28] García-Patrón Sanchez R 2007 *PhD Thesis* Thesis Universite Libre de Bruxelles

[29] 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

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

[31] Mandel L and Wolf E 1995 *Optical Coherence and Quantum Optics* (Cambridge: Cambridge University Press)

[32] 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

[33] Newton E 2019 Data for Thermal State QKD, https://doi.org/10. 5518/206 University of Leeds, 2019