

Secure Quantum Key Distribution with Thermal States

M. Lucamarini (1), K. Tamaki (2), G. Di Giuseppe (3)

1: University of Camerino, Department of Physics, Via Madonna delle Carceri, 9 - 62032 Camerino (MC), Italy.
marco.lucamarini@unicam.it

2: NTT Basic Research Laboratories, Kanagawa, Japan. (tamaki@will.brl.ntt.co.jp)

3: University of Camerino, Camerino (MC), Italy. (gianni.digiuseppe@unicam.it)

Abstract

The majority of experimental and theoretical QKD developed so far concerns pure coherent states from a laser source. On the other side there are many instances of practical use in which mixed incoherent states play a major role, like in current wireless telecommunications in the microwave regime. In this work we study how the more or less chaotic nature of light can affect the security of QKD, in the case of decoy-state BB84 and strong-pulse B92. It turns out that the secure QKD gain pertaining to mixed thermal states is comparable with that obtained with pure coherent states.

Introduction

Perhaps it is not universally known that the first QKD experiment was not performed with a *coherent* light source, like a laser, but rather with a LED, emitting *incoherent* light in pulses of about 500 ns each [1]. Once the global phase of each pulse is averaged out the only difference relevant to QKD between coherent and incoherent light is the associated photon-number statistics, which is Poissonian (Eq.1a) for a coherent source like a laser, and Thermal, (Eq.1b) for an incoherent source like a LED or an antenna. In other

$$P_n^P(\mu) = e^{-\mu} \frac{\mu^n}{n!} \quad (1a) \quad P_n^T(\mu) = \frac{\mu^n}{(1+\mu)^{1+n}} \quad (1b)$$

terms the pureness of the quantum states used for QKD is not essential to work out a security proof. Even so it is fundamental for establishing the practical performances of a QKD setup. For example the operational range of a laser-based BB84 is strongly limited by the Poissonian statistics obeyed by the source, which allows Eve to perform a quite powerful photon-number-splitting attack (PNS). In PNS Eve exploits the multiphoton pulses accidentally created by Alice to eavesdrop on the channel. The percentage of multiphoton pulses clearly depends on the photon-number statistics of the source. By consequence when incoherent light is taken into account new subtle threats might play a role. For instance the photons might group into bunches, according to the so called *bunching effect* of the chaotic light [2], so that the percentage of zero and multiphoton pulses can increase if the source is incoherent, and the PNS become more powerful.

In the present work we discuss the unconditional security of QKD performed with chaotic light, i.e. following the thermal statistics of Eq.(1b). We consider a pair of long-range QKD protocols, the BB84 with decoy states [DS-BB84, 3] and the B92 with a strong reference pulse [SP-B92, 4], and provide the secure gain pertaining to them as a function of the distance between the users.

BB84 and DS-BB84

Let's consider BB84 first, performed ideally with the experimental apparatus of Ref. [5], which includes a coherent source of light. The secure gain for this situation is drawn as a black line in the top diagram of Figure 1. The gain is optimized for every distance by varying μ . As mentioned earlier the security argument

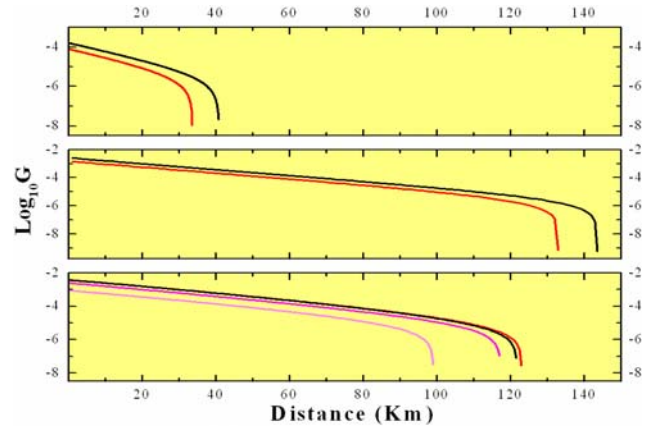


Figure 1: Secure Gain vs Distance for three different protocols. The experimental parameters for the communication channel and the detectors are from [5]. For each distance the Gain was optimized varying the pulse photon-number μ . **Top diagram:** BB84 performed with coherent light (black line) and incoherent light (red line). **Middle diagram:** Infinite-Decoy-State BB84 with coherent (black line) and incoherent light (red line), **Bottom diagram:** Strong-Pulse B92 with coherent light (black line) and incoherent light with coherence ratios $r_c = 10^3$ (light magenta line on the left), $r_c = 10^4$ (magenta line) and $r_c = 10^6$ (red line on the right). The average photon number is 10^{10} photons per pulse.

does not depend on the particular photon-number statistics, but the practical performances do. When the thermal distribution of Eq.(1b) is used to calculate the percentage of multiphotons from an incoherent source one obtains the rate drawn as a red line in the top diagram of Figure 1. It is apparent that both the gain and the maximum achievable distance with

incoherent light are lower than with coherent one, in accordance with the intuitive picture sketched in the Introduction.

The same behavior but on larger distances is met when we consider DS-BB84 [3]. In the middle diagram of Figure 1 is plotted the secure gain pertaining to this protocol, in the case of an infinite number of decoy states. The black line concerns the coherent light source, while the red line the incoherent one. Also in this case the gain and the maximum achievable distance for chaotic light are both lower than for coherent light. Analogous results should hold for more practical DS-BB84, in which only a finite number of decoy states is used. In fact the unconditional security of this kind of protocol depends on the crucial inequality written in Eq.(2), which

$$\frac{P_n(\mu)}{P_n(\mu')} > \frac{P_m(\mu)}{P_m(\mu')} \quad (2)$$

remains true both for coherent ($P_n = P_n^P$) and incoherent light ($P_n = P_n^T$), when $\mu < \mu'$, $n < m$.

SP-B92

A different approach must be used when dealing with SP-B92 [4]. In this case the menace is represented by the unambiguous-state-discrimination attack (USD). In USD Eve stops all the pulses uninformative to her while delivering all the others. The stopped pulses are concealed in the natural losses of the communication channel. The power of USD is inversely proportional to the trace distance D between the two B92 quantum states. If the states are pure and coherent then D can be shown to be less than $\sqrt{\pi\mu}$, while if they are mixed and thermal D is less than $\sqrt{4\mu}$. So, quite nicely, one expects the secure gain of an incoherent SP-B92 to be higher than that of a coherent SP-B92. However things are not so simple. SP-B92 is the only protocol in which the variance of the photon-number plays a role. It is known that the variance related to a coherent state is exactly μ , the mean photon number. On the contrary the variance of a thermal state depends, in general, on the coherence time of Alice's source T_c and on the detection time of Bob's detector T_m [2]. In particular it amounts to

$$Var(n) = \eta\mu + (\eta\mu)^2 \left[\frac{1}{2r_c^2} (e^{-2r_c} + 2r_c - 1) \right] \quad (3)$$

r_c is the ratio between T_m and T_c . Note that a non

infinite coherence time implies that the source is not monochromatic, which is natural in a pulsed regime.

In the bottom diagram of Figure 1 we plotted the variance-accounted gain pertaining to SP-B92 with coherent (black line) and incoherent light (red colored lines). The value of the ratio r_c ranges from 10^3 (left-side line in light-magenta) to 10^4 (middle-side line in magenta) to 10^6 (right-side line in red). The left-side line corresponds to a thermal-state gain which is well below the coherent-state one. On the contrary the right-side line represents a thermal-state gain which overcomes the coherent-state one. Although expected, this result is not entirely lacking in surprise, as it is natural to associate the best performances of a QKD setup to the one involving the purest states.

Conclusions

In this work we studied how the practical rendering of a QKD setup is modified by the photon number statistics of its source. We did not report lengthy details about security proofs, even because in many cases they are a trivial extension of existing proofs. We reported the secure gain of two long-range QKD protocols run with a thermal source. We showed that a coherent source is not necessarily better than an incoherent one for a secure QKD. This seems to be particularly true for B92-like protocols, even if in this case the requirements on the source-coherence might be quite demanding. It is worthwhile to mention that our work suggests the possibility of a future QKD performed in the microwave regime with the same off-the-rack antennas currently employed in wireless telecommunications, even if in this regime the detectors dark counts can represent a serious hindrance.

We acknowledge useful discussions with P. Tombesi and D. Vitali.

References

1. C. H. Bennett *et al.*, J. Cryptol. **5**, 3 (1992).
2. R. Loudon, *The quantum theory of light* (Clarendon Press, Oxford, 1979).
3. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); X.-B. Wang, *ibid.* **94**, 230503 (2005); H.-K. Lo *et al.*, *ibid.* **94**, 230504 (2005).
4. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992); K. Tamaki *et al.*, quant-ph/0607082.
5. C. Gobby *et al.*, Appl. Phys. Lett. **84**, 3762 (2004).