Security of quantum key distribution with intensity correlations

Victor Zapatero¹, Álvaro Navarrete¹, Kiyoshi Tamaki², & Marcos Curty¹

¹Telecommunications, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
²Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan

Universidad de Vigo

arXiv:2105.11165

Summary

Decoy-state quantum key distribution (QKD) is a popular method to approximately achieve the performance of ideal single-photon sources by means of simpler and practical laser sources. In high-speed decoy-state QKD systems, however, intensity correlations between succeeding pulses leak information about the users’ intensity settings, thus invalidating a key assumption of this approach. Here, we solve this pressing problem by developing a general technique to incorporate arbitrary intensity correlations to the security analysis of decoy-state QKD. This technique only requires to experimentally quantify two main parameters: the correlation range and the maximum relative deviation between the selected and the actually emitted intensities. As a side contribution, we provide a non-standard derivation of the asymptotic secret key rate formula from the non-asymptotic one, so revealing a necessary condition for the significance of the former.

1. Characterizing the intensity correlations

NOTATION

\[ \bar{a}_k = a_1, a_2, \ldots, a_k \] (record of intensity settings selected up to round k)

\[ a_k \] (actually emitted intensity in round k)

In full generality, \( a_k \) is a continuous random variable whose probability distribution, \( g_{\bar{a}_k}(a_k) \), is fixed by the record of settings \( \bar{a}_k \).

PHYSICAL ASSUMPTIONS ON THE CORRELATIONS

Assumption 1. The photon-number statistics of the source conditioned on the value of the actual intensity, \( a_k \), is Poissonian:

\[ p(n|a_k) = e^{-a_k}a_k^n n!
\]

Assumption 2. For all possible records of settings, \( \bar{a}_k \),

\[ 1 - \frac{\bar{a}_k}{a_k} \leq \delta_{\text{max}} \]

That is to say, \( a_k \in \bar{a}_k \) with \( a_k = a_k(1 \pm \delta_{\text{max}}) \), where \( \delta_{\text{max}} \) is the maximum relative deviation of the actual intensity with respect to its setting. From assumptions 1 and 2, it follows that

\[ p_{n_k|a_k} = \sum_{a_k} g_{\bar{a}_k}(a_k) e^{-a_k}a_k^n n!
\]

Assumption 3. The intensity correlations have a finite range, say \( \xi \), such that \( g_{\bar{a}_k}(a_k) \) is independent of those settings \( a_j \) with \( k - j > \xi \).

3. Numerical results

The rate-distance performance of the decoy-state BB84 is shown in terms of the maximum relative deviation, \( \delta_{\text{max}} \), and the correlation range, \( \xi \). A typical channel model is used, with detection efficiency \( \eta_{\text{det}} = 65\% \), attenuation coefficient \( a_{\text{att}} = 0.2 \text{dB/km} \), and dark count rate \( p_d = 7.2 \cdot 10^{-8} \).

4. On the existence of an asymptotic formula

The so-called post-selection technique is invoked to establish the asymptotic equivalence between the secret key rate against collective attacks and the corresponding one against coherent attacks, whenever a certain permutation-invariance property holds. Nevertheless, pulse correlations of any kind generally invalidate this property, and therefore the equivalence disappears.

Alternatively, in this work we provide a simple and non-standard derivation of the asymptotic limit, in so revealing a necessary and sufficient condition for the asymptotic formula to apply. The condition can be written as

\[ \lim_{n \to \infty} \frac{\sum_{i=1}^{n} \text{Cov}[X_i, X_j]}{N^2} = 0 \]

for certain Bernoulli sequences \( X_i^n \) directly related to the observables, \( N \) being the number of transmitted signals. If the above convergence condition does not hold, no asymptotic limit exists for the secret key rate.