Security of quantum key distribution with intensity correlations

Víctor Zapatero[1], Álvaro Navarrete[1], Kiyoshi Tamaki[2], & Marcos Curty[1]

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

UniversidadeVigo

UNIVERSITY OF TOYAMA

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, in so revealing a necessary condition for the significance of the former.

1. Characterizing the intensity correlations

NOTATION

$\vec{a}_k = a_1 a_2 \dots a_k$ (record of intensity settings selected up to round k)
α_k (actually emitted intensity in round k)

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

PHYSICAL ASSUMPTIONS ON THE CORRELATIONS

Assumption 1. The photon-number statistics of the source conditioned on the value of the actual intensity, α_k, are poissonian:

$$p(n_k|\alpha_k) = \frac{e^{-\alpha_k}\alpha_k{}^{n_k}}{n_k!}.$$

Assumption 2. For all possible records of settings, $\vec{a}_k$,

$$\left|1 - \frac{\alpha_k}{a_k}\right| \leq \delta_{\max}.$$

That is to say, $\alpha_k \in [a_k^-, a_k^+]$ with $a_k^\pm = a_k(1 \pm \delta_{\max})$, where $\delta_{\max}$ is the maximum relative deviation of the actual intensity with respect to its setting. From assumptions 1 and 2, it follows that

$$p_{n_k|\vec{a}_k} = \int_{a_k^-}^{a_k^+} g_{\vec{a}_k}(\alpha_k)\frac{e^{-\alpha_k}\alpha_k{}^{n_k}}{n_k!}\,d\alpha_k\,.$$

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

2. Main analytical result

CENTRAL IDEA

The main idea is to **pose a restriction on the maximum bias that Eve can induce between the n-photon yields and errors associated to different intensity settings**, in so enabling the application of the decoy-state method. Fundamentally, **the restriction follows from the indistinguishability of non-orthogonal quantum states**, captivated by what we call **"the Cauchy-Schwarz constraint"**.

QUANTITATIVE BOUNDS

In what follows, we refer to the standard polarization encoding BB84 protocol. Precisely, for any given round k, photon number n, intensity setting c and bit value r, we define the yield and the error probability as $Y_{n,c}^{(k)} = p^{(k)}(\text{click}|n,c,\text{Z},\text{Z})$ and $H_{n,c,r}^{(k)} = p^{(k)}(\text{click}|n,c,\text{X},\text{X},r)$, respectively. Also, note that we are conditioning here to coincident basis choices by Alice and Bob (Z or X). Then, for any two distinct intensity settings a and b, one can show that their yields and error probabilities satisfy

$$G_-\left(Y_{n,a}^{(k)}, \tau_{ab,n}^{\xi}\right) \leq Y_{n,b}^{(k)} \leq G_+\left(Y_{n,a}^{(k)}, \tau_{ab,n}^{\xi}\right)$$

and

$$G_-\left(H_{n,a,r}^{(k)}, \tau_{ab,n}^{\xi}\right) \leq H_{n,b}^{(k)} \leq G_+\left(H_{n,a,r}^{(k)}, \tau_{ab,n}^{\xi}\right)$$

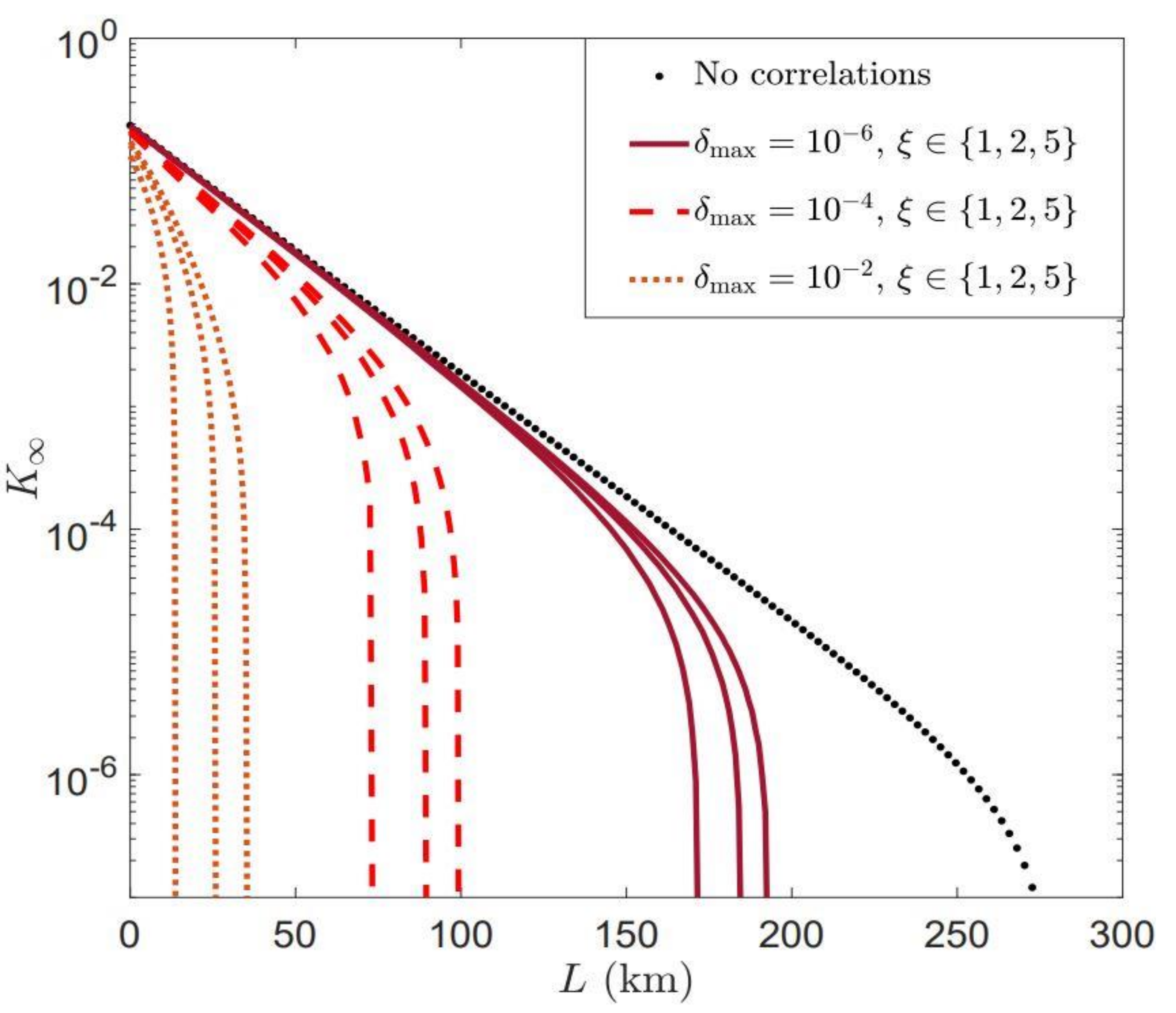
for all k and n, where G_- and G_+ are known functions that follow from the Cauchy-Schwarz constraint, ξ is the correlation range and

$$\tau_{ab,n}^{\xi} = \begin{cases} e^{a^- + b^- - (a^+ + b^+)}\left[1 - \sum_c p_c\left(e^{-c^-} - e^{-c^+}\right)\right]^{2\xi} & \text{if } n = 0 \\ e^{a^+ + b^+ - (a^- + b^-)}\left(\frac{a^- b^-}{a^+ b^+}\right)^n\left[1 - \sum_c p_c\left(e^{-c^-} - e^{-c^+}\right)\right]^{2\xi} & \text{if } n \geq 1. \end{cases}$$

Here, p_c is the probability of using intensity setting c in any given protocol round.

3. Numerical results

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



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

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

for certain Bernoulli sequences $\{X_i\}_{i=1}^N$ 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.**