Nicola Laurenti

Department of Information Engineering, University of Padova
Via Gradenigo 6/b - 35131 Padova, Italy
nil@dei.unipd.it

Experimental QKD with finite-key security analysis for noisy channels

N. Laurenti, D. Bacco, M. Canale, G. Vallone, P. Villoresi

In QKD implementations, each session is typically chosen long enough so that the secret key rate approaches its asymptotic limit. However, this choice may be constrained by the physical scenario, as in the perspective use with satellites, where the passage of one terminal over the other is restricted to a few minutes.
In this work, we experimentally evaluate, in a realistic setup and with different channel conditions, the robustness of a recent finite-key theoretical tight-bound ensuring secrecy against the most general quantum attacks. We compare the experimental results obtained by using this bound with the ones achieved with a new finite-key bound tailored for ensuring secrecy against individual attacks.
We then show, for different values of the QBER, the minimum number of raw bits to be exchanged in order to obtain a given secret key length. This provides a valuable tool for practical QKD, as it allows to know in advance, depending on the channel noise, how many bits have to be exchanged for obtaining the desired secret key length.
The relevance of the proposed analysis is mainly directed to practical QKD and, in particular, to scenarios where the number of exchanged qubits is limited by physical constraints, as in the notable case of satellite QKD, where channel losses and visibility play a major role in limiting the efficiency and the availability of the quantum link.
The results indicate that viable conditions for effective symmetric, and even one-time-pad, cryptography are achievable.