Davide Marangon

Department of Information Engineering, University of Padova
Via Gradenigo, 6B - 35137 Padova, Italy
davmar@dei.unipd.it

Random bits, true and unbiased, from athmospheric turbulence.

D. Marangon, G. Vallone, P. Villoresi

In recent years an even growing effort has been done by both theoretical and experimental scientists, in order to refine and strengthen the unconditional security of the quantum key distribution protocols.
The area of research has been mainly centered on the modeling of the quantum channel, on possible attacks by Eve and on the ways of tamper them.
A persistent problem of the QKD protocols is however the part regarding the generation of the raw key. Even before the sifting procedure and even before the transmission of the "encoded" photons, it is strictly required the raw key being drawn from a set of uniformly and independently distributed keys. The set of the possible initial keys is generated by random number generators (RNG). The whole security introduced by Quantum Mechanics would then be completely useless if algorithmic and deterministic generators were used (the so called pseudo-RNG).
Getting the access to true randomness, it is then one of the last fundamental steps for the upcoming everyday application of Quantum Cryptography and Quantum Communications.
True randomness can be achieved by exploiting the intrinsic probabilistic nature of quantum processes or the uncomputability of the highly chaotic ones. Recently we then developed a method to extract random bits by taking advantage of the optical turbulence which affects a laser beam propagating through the atmosphere. Both classical and quantum communications often use strong "probe" laser beams for aiming and synchronization purposes. However the turbulent dynamic of the terrestrial atmosphere induces unpredictable variations of the air refractive index which randomly distort the wavefront of the optical coherent radiation.
We present then the results obtained by exploiting the optical noise on a "probe" laser beam sent through the islands of La Palma and Tenerife (the 144 km long free space optical link used in recent experiments of QKD and quantum teleportation) which let us generate strong and true random bits.