Davide Bacco

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

Quantum communications between Space and Earth

D. Bacco, A. Dall'Arche, D. Marangon, F. Gerlin, M. Barbieri, M. Canale,
N. Laurenti, C. Barbieri, G. Vallone, P. Villoresi

Quantum key distribution permits to communicate in a perfectly secure way, unfortunately nowadays quantum commercial cryptography is limited by physical aspects.
It has been demonstrated that it is possible to increase this bound using a free-space quantum channel, and in particular a space channel to exchange single photons between Earth and Space.
Our aim is to realize a complete QKD scheme between Earth and Space in order to be able to establish a secure communication and also to demonstrate that a global quantum network is now possible. In particular our work is focused on the physical layer of the system, working on integration with existing telescopes and studying the atmosphere turbulence and the protocol security. We examine signal propagation through a turbulent atmosphere for uplink and downlink solutions, discussing the contribution of beam spreading and beam wandering.
A model for the background noise during night and day-time is considered too, and we discuss the expected error-rate due to the imperfect compensation of polarization in the channel.
An important parameter of a QKD system is the expected secret key bits (ratio between final secret bits to the number of bits sent); we evaluate the generation rate for different configurations (uplink, downlink) and for some protocols.
In traditional security proofs, the secret key rate is upper- bounded by assuming key streams of infinite length.
In a practical scenario, like quantum satellite communications, the temporal interval of the key exchange and the achievable bit-rate at the receiver may be constrained by availability of satellites and also by huge channel losses. Hence, it is necessary to consider the impact of finite key length effects on the security of a given QKD protocol.
We propose results that prove the experimental feasibility of distilling unconditionally secure keys of finite length in different noise conditions and according to two distinct security notions. These depend on the chosen attack: general quantum attack or intercept-and-resend attack.
These models entail two different notions of secrecy, which we call general and pragmatic, respectively. Pragmatic secrecy ensures higher secret key rates as compared with general one.
On the other hand, in the presence of harsh channel conditions (both in terms of QBER and losses), the use of pragmatic secrecy opens the way to the distillation of a secret key, whereas this is not possible under the general secrecy constraint. The price to be paid for this advantage is the vulnerability to general quantum attacks.
Nonetheless, as long as a quantum memory is not available to the eavesdropper, we do believe that this represents a valid and viable solution to obtain a secret key for an experimentally realistic number of exchanged photons.
Furthermore, it should be pointed out that pragmatic secrecy offers forward security: if a key is produced today with pragmatic secrecy, it will be secure for any future task, even if a quantum memory will be present.