Secure long-distance Quantum Key Distribution

Hugo Zbinden
GAP - Quantum Technologies, University of Geneva

For the last twenty years, Quantum Key Distribution has developed from simple proof of principle experiments to commercial systems. However, it is still very rarely used in practice for many different reasons ranging from the high cost of the devices and dedicated fibre infrastructure, limited key generation rates and transmission distance, blind trust in classical cryptosystems to unawareness of security threads in communication.

In this talk, we present our recent work in pushing the transmission distance to its limits, while limiting the complexity and cost of the technology such that it can be used in a commercial product [1].

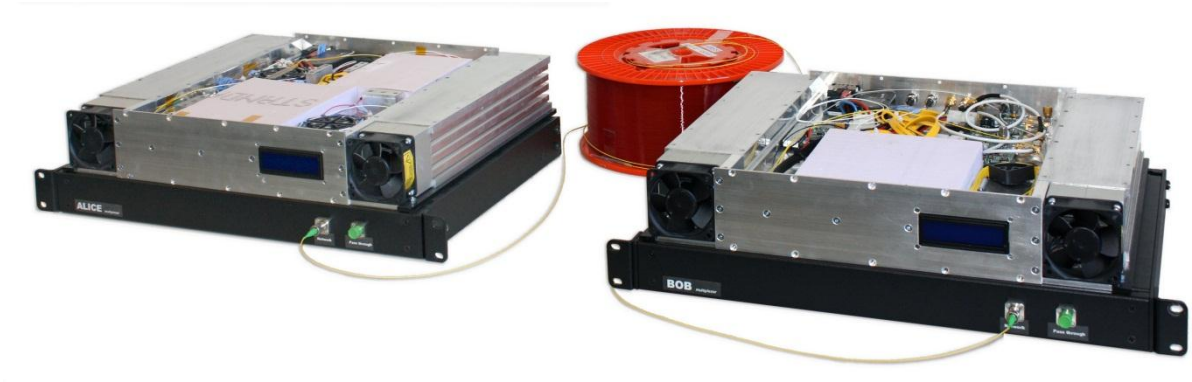

Fig. 1: Picture of the open QKD prototypes (external detectors not shown).

There are a few key ingredients for such a system:

- *Compact, low-noise single photon detectors*: The progress in increasing transmission distance has been closely linked to the progress of single photon detectors at telecom wavelengths. In particular in the past, record-distance experiments were achieved with superconducting detectors requiring heavy cryogenic cooling. In our experiments, we rely on free-running InGaAs/InP avalanche photon diodes cooled with very efficient and compact Stirling coolers [2].
- *Finite-key security analysis:* The employed QKD protocol (in our case the coherent-one-way protocol) needs to be resistant to photon-number-splitting attacks which become very efficient at high transmission loss. Moreover, the security analysis must take into account finite-key effects in an efficient way [3]. Indeed, at low detection rates the block sizes for classical post processing can no longer be arbitrarily long, if integration times need to stay practical. Then, we are able to state a security parameters ε_{QKD}, which indicates the chance that an eavesdropper with unlimited power can obtain 1 bit of information. In our experiment we choose a ε_{QKD} of $4 \cdot 10^{-9}$.

- *Low-loss fibre:* Finally, most evidently fibre loss should be low. Collaboration with Corning Inc. allows us to take profit of the most recent ultra-low-loss fibres featuring attenuation as low as 0.16 dB/km [4].

We will show how the experimental parameters are adjusted as a function of the fibre length for optimum performance (in particular the detector temperature as illustrated in Fig. 2). As a result, with a detector temperature of -120^{o} C, we manage to exchange secret keys over more than 300km (52 dB loss).

Finally, we will discuss ways to further increase transmission distance and rate. We also present solutions to create random numbers at GHz rates [5].

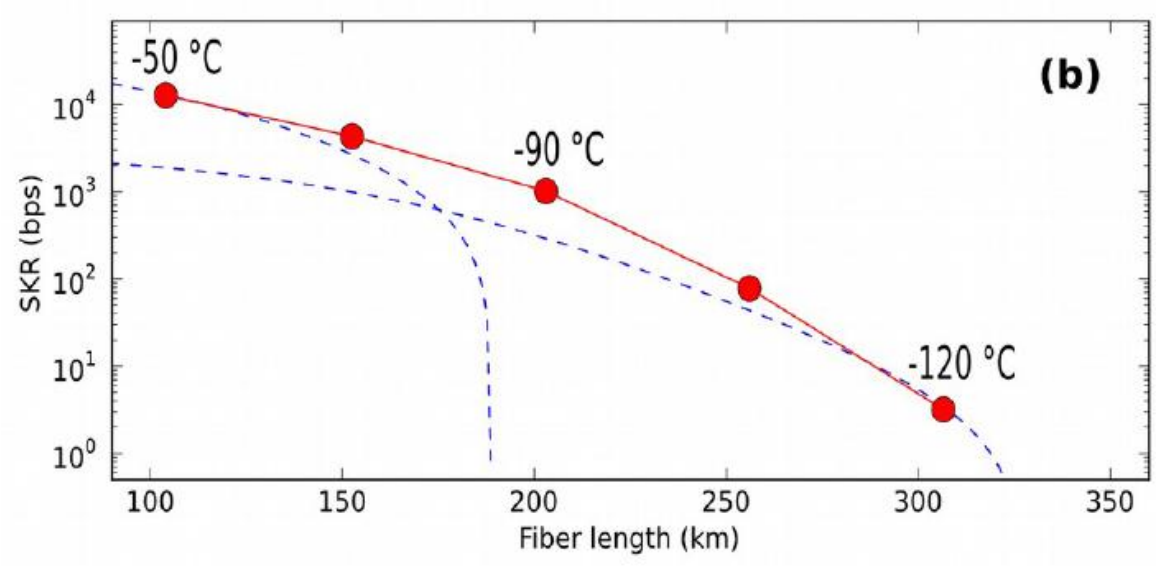

Fig. 2: Secret key rate (SKR) vs. fibre length. Red points: Experimental results obtained with the indicated detector temperatures. Dotted line: Calculated SKR for -50^{o}C and -120^{o}C, respectively.

References:

1) B. Korzh et. al., *Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre,* Nature Photonics **9**, 163-168 (2015).

2) B. Korzh, N. Walenta, T. Lunghi, N. Gisin, H. Zbinden. *Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency*, Appl. Phys. Lett. 104, 081108 (2014).

3) C. Lim, M. Curty, N. Walenta, F. Xu,H. Zbinden. *Concise security bounds for practical decoy-state quantum key distribution* , Phys. Rev. A **89**, 022307 (2014).

4) Corning SMF-28® ULL fibre

5) A. Martin, B. Sanguinetti, C. Lim, R. Houlmann, H. Zbinden, Quantum Random Number Generation for 1.25-GHz Quantum Key Distribution Systems, J. of Lightwave Techn. **33** (13), 2855 (2015)