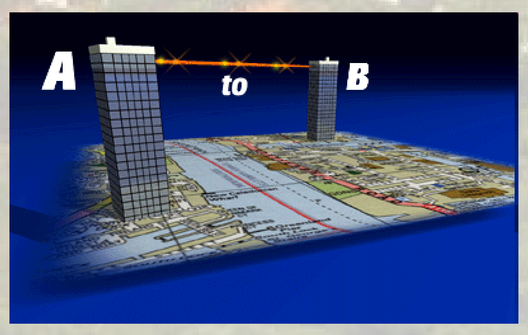
High-speed free-space quantum key distribution with automatic tracking for short-distance urban links

Alberto Carrasco-Casado [1], María-José García-Martínez [2],Natalia Denisenko [2], Verónica Fernández [2]
1. Carlos III University, Avda. Universidad 200, Madrid 28911, Spain
2. Spanish National Research Council (CSIC), Calle Serrano 144, Madrid 28006, Spain

Veronica.Fernandez@iec.csic.es

QUANTUM KEY DISTRIBUTION IN FREE SPACE

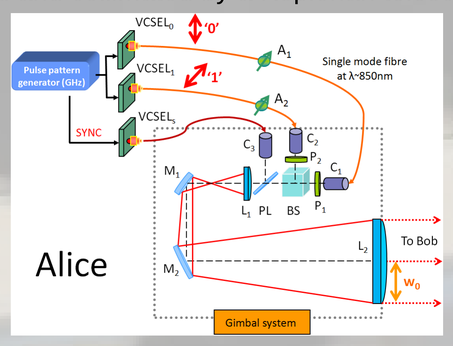


- **Free-space optics (FSO)** in general, has a considerable advantage over **optical fiber**, namely their **flexibility of installation** and **portability**. Unlike optical fiber, that becomes a sunk cost when the customer leaves, FSO can be moved to different locations as required.
- **QKD applied to short free-space links** in urban areas is an interesting alternative to current **public-key cryptography**, which is threatened by a **quantum computer attack**. In this context, QKD is aimed principally to financial, government and military institutions located within the same city. However, for QKD to be a realistic alternative it needs to be implemented at **high speed** and implement a suitable **automatic tracking** that corrects for fast beam deviations caused by atmospheric turbulence.

QKD SYSTEM

Alice

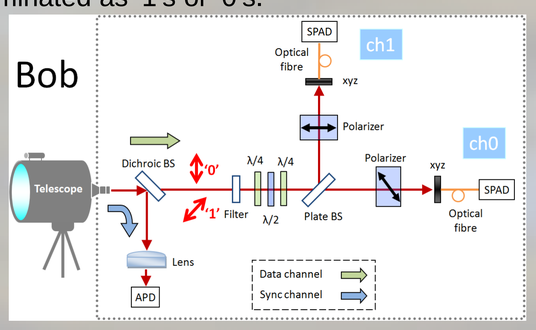
Single photons strongly attenuated from two vertical-cavity emitting lasers (VCSELs) at λ ~ 850nm will become bits of the initial quantum key. Each output is linearly polarised – vertically and diagonally – to encrypt '0's ands '1's, respectively, and both beams are then expanded and collimated by a Keplerian telescope.



A_1 and A_2 are fibre-coupled attenuators; P_1 and P_2 are high-extinction ratio polarizers; C_1, C_2 and C_3 are optical collimators, BS is a 50/50 beamsplitter, PL is a pellicle beamsplitter; L_1 and L_2 are achromatic doublet lenses and M_1 and M_2 are high-reflectivity mirrors.

Bob.

The three beams from Alice are focused by a Schmidt-Cassegrain telescope at the receiver and spectrally discriminated by a dichroic mirror. Then, by a specific orientation of the analyzers both states are discriminated as '1's or '0's.



APD is avalanche photodiode; SPAD is single photon avalanche detector and xyz are traslation stages.

A further analysis of the detection events allows Alice and Bob to establish the level of security and the distillation of the secret key.

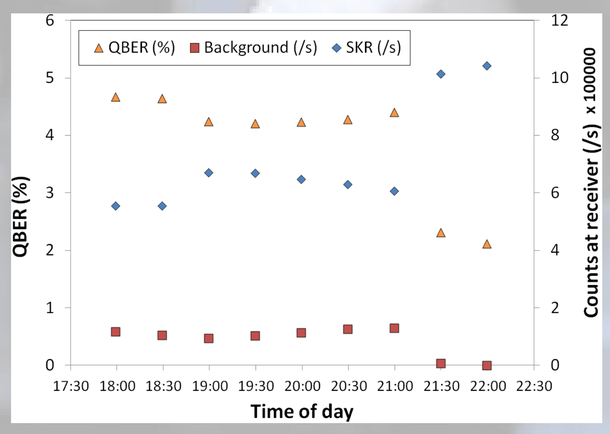
TIMING SYNCHRONISATION

A separate optical signal at a different wavelength is used to transmit the clock signal from Alice to Bob. This ensures that no timing fluctuation occurs between both clocks. This is done by a third laser ($VCSEL_S$) emitting at λ ~1550 nm and high temporal precision.

INFLUENCE OF ENVIROMENTAL CONDITIONS

Solar background

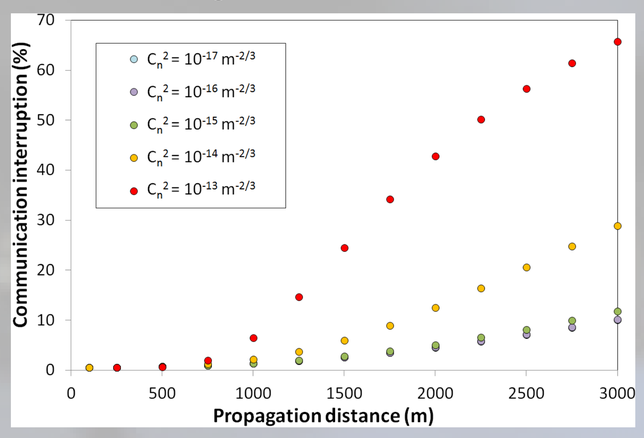
Many external factors influence the error – or quantum bit error rate (QBER) – of a QKD system, with the background and turbulence being the most critical ones. The effect of background for a 300m link can be seen in the next figure where the secret key rate (SKR), QBER and background rate were measured at 1.5 GHz clock frequency between 17:30 and 22:00 hours.



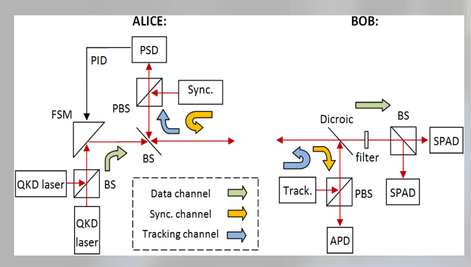
The background radiation is reduced by using a combination of spectral, spatial and software filtering.

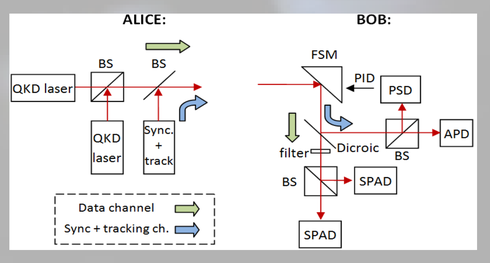
Turbulence

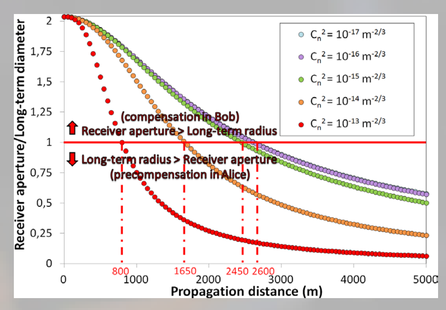
Turbulence usually affects a free-space optical link through two effects: beam spreading and beam wandering. The first causes an enlargement of the beam size and the second, random deflections of its position. Both effects can be modeled by a *long term beam radius* at the receiver. Depending on the intensity of the turbulence and the distance this radius can be larger than larger than the receiver's aperture, and loss of the reception of the signal can thus take place. The next graph shows the percentage of 'no reception' for our QKD system simulated as a function of the distance for several turbulent regimes:



HIGH SPEED TRACKING SYSTEM

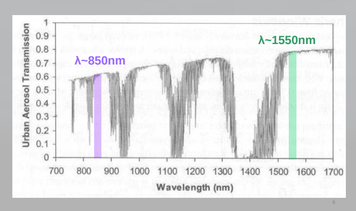






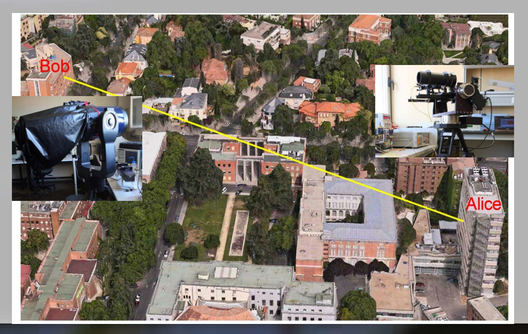
Atmosphere as the quantum channel

- Good transmission 1st and 2nd telecomms windows
- No birefringent
- No dispersive
- Weather dependent
- Sensitive to turbulence



THE 300m QKD LINK

Emitter and receiver were characterised at a distance of 300 m between the Information Security Institute (CSIC) and the Institute of Agricultural Sciencies (CSIC) at Serrano Campus, shwoing the QKD link was capable of achieving a sifted bit rate 4 times larger than those of simialr systems reported to date and a secret key rate one order of magnitude higher



ACKNOWLEDGEMENTS
We would like to thank the Ministerio de Economía y Competitividad, project TEC2012-35673