Free-Space Quantum key Distribution Link at Gigahertz Clock Rates

V. Fernandez (1), D. Arroyo (1), M. J. Garcia (1), AB. Orue (2)
1: Institute of Applied Physics, Spanish National Research Centre (CSIC), Serrano 144, 28006 Madrid, (Spain)
e-mail: veronica.fernandez@iec.csic.es
2: Area of Scientific Culture (CSIC), Serrano 117, Madrid, (Spain)
b.orue@orgc.csic.es

Abstract

A high-clock-rate free-space quantum key distribution system (QKD) for urban-span applications is presented. The aim is to securely transmit cryptographic keys at high transmission rates between two locations in Madrid separated by a distance of 3 km: the Spanish National Research Centre (CSIC) and the telecommunications operator Telefonica.

Introduction

Free-space links in short-range distance applications generally offer simpler and cheaper installation, more flexibility and higher transmission rates than optical fibre. For this reason, it may constitute an alternative candidate for QKD over fibre-optic point-to-point links or passive optical networks. Moreover, free-space links at near-infrared wavelengths offer less absorption and distortion of the optical signal than optical fibre. These factors may constitute a good incentive to companies or banks that wish to exchange cryptographic keys in urban-area applications with absolute secrecy. Since QKD needs to be implemented in conjunction with the *one time pad*, speed is a major factor to be considered. Therefore if this approach wants to be competitive secure key transmissions need to be performed at considerably higher clock rates than those currently employed (MHz). Therefore a high-clock-rate (GHz) QKD system for short-range urban-span applications is proposed here.

Motivation

Research on free-space QKD systems has been especially focused on increasing the transmission distance of the free-space links in locations situated far from urban areas. This is mainly aimed to develop satellite-based secure communications. However, much less attention has been paid in short-distance QKD systems for urban areas. Although these offer some advantages previously mentioned they are not exempt from some drawbacks. One of them is the presence of turbulence in this type of location. Some contributors to this phenomenon are originated by industrial equipment (ducts, pipes), machines (internal combustion engine) or simply by vehicles. Turbulences cause beam wandering, which strongly affects laser beam alignment and need to be reduced by carefully designing Bob's optics. In addition the higher presence of pollutants causes a further absorption of the optical signal (see Fig. 1).

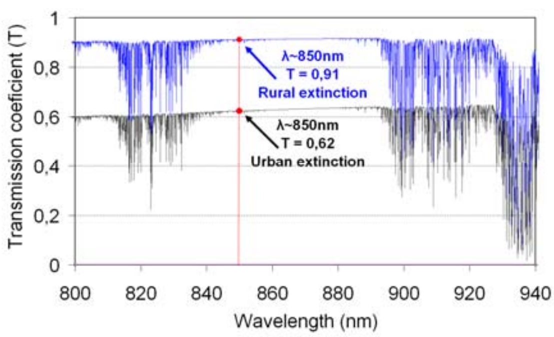

Figure 1. Comparison of the transmission coefficient T as a function of wavelength for a horizontal path of 1km for two types of aerosol: one commonly found in urban areas and another characteristic from rural locations. Results were calculated using an atmospheric transmission simulation code (Modtran4.0)

Nevertheless, short-range free-space systems offer considerable advantages over long-distance ones. A satellite can be considered as a third party of a QKD protocol that needs to be established as a secure relay station, which is by no means a trivial task. Additionally, long-distance free-space QKD systems are technologically more challenging, and due to the higher distances involved the transmission bit rates are considerably lower. Therefore many companies situated in urban areas might find a short-distance free-space QKD system an alternative option since it can offer higher bit rate, lower cost and less complexity than long-distance free-space systems.

Proposed QKD system

The proposed short-distance QKD system is shown in Figs. 2 and 3. The main aim is to securely transmit quantum keys between two locations in Madrid situated at 3 km of distance at high clock frequencies (up to 3.3 GHz). These two locations will be the Institute of Applied Physics, of the Spanish National Research Centre (CSIC) and the telecommunications operator Telefonica. To achieve high transmission rates Alice will use a fast GHz pre-programmed pulse pattern generator in conjunction with λ ~ 850 nm vertical-cavity surface emitting lasers (VCSELS) controlled by high-speed drivers. Two high extinction-ratio polarisers will provide the two nonorthogonal states necessary to implement the B92 protocol. A spatial filter will 'clean up' the beam from imperfections and higher order spatial modes. A beam expander will be used to generate a collimated and sufficiently large beam to decrease divergence effects throughout propagation. At Bob, a cassegrain telescope will be used to efficiently focus the beam, and two Silicon single-photon avalanche diodes (SPADs) will detect the photons from Alice. In addition, a high speed Time Interval Analyser (TIA) will analyse and process the optical signal and establish the degree of security in the transmission. Especial care must be paid to one of the most critical parts of the system, which is the filtering of the solar background radiation from the sun. For this purpose, a combination of spatial, spectral and software filtering will be used. The timing synchronisation between Alice and Bob's stations will be performed by multiplexing a different wavelength than that used for the quantum states encrypting the key. This will permit faster synchronisation compared to systems using software phase locked loop driven (PLL) by either the photo-detection events received at Bob [1] or by the Global Positioning System (GPS) [2]. We believe this type of synchronisation in conjunction with a GHz-clocked source will result in secure key transmission rates considerably higher than those currently achieved. Current systems for this application are typically clocked at only a few MHz, translating in secure key transmission rates in the order of a few hundred of bits^{-1} or less.

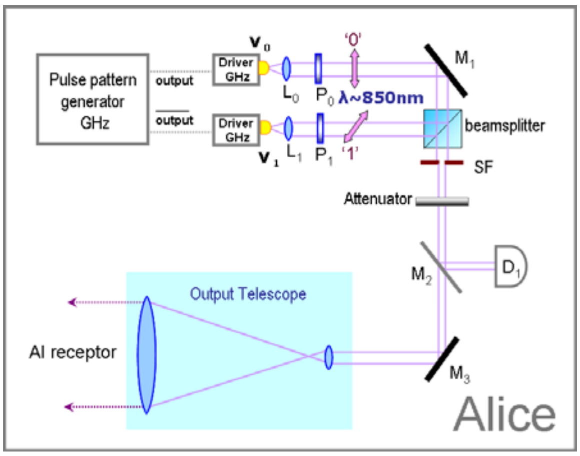

Figure 2. Alice's module. V_0 and V_1 are two VCSELs; L_0 and L_1 are two optical lenses; P_0 and P_1 are two high extinction-ratio polarisers; M_1, M_2 and M_3 are three high-reflectivity mirrors; and SF is a spatial filter.

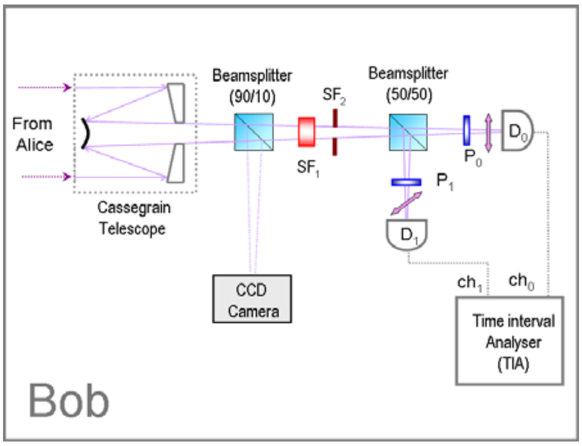

Figure 3. Bob's module. SF_1 and SF_2 are a set of spectral filters and a spatial filter, respectively; P_0 and P_1 are two high extinction-ratio polarisers; M_1 is a high-reflectivity mirror; and D_0 and D_1 are single-photon detectors.

Conclusions

A high-speed free-space QKD system for urban-span secure communication links has been proposed. A combination of high-clock frequency generator and high-data transmission laser diodes at Alice in conjunction with an optical synchronisation at a different wavelength will permit faster key generation than those currently achieved.

Acknowledgement

We would like to thank the Ministerio of Educación y Ciencia, project TSI2007_62657 and CDTI, Ministerio de Industria, Turismo y Comercio (Spain), in collaboration with Telefónica I+D, Project SEGUR@ with reference CENIT-2007 2004.

References

1. J. G. Rarity et al, Journal of Modern Optics, volume 48 (2001) page 1887
2. T. Schmitt-Manderbach et al. Physical Review Letters, volume 98 (2007) article 010504.