Multi-user quantum key distribution with entangled photons from a semiconductor chip

C. Autebert[1], J. Trapateau[2], A. Orieux[2], A. Lemaître[3], C. Gomez-Carbonnel[3], E. Diamanti[2], I. Zaquine[2], S. Ducci[1]

[1] Laboratoire MPQ, Université Paris Diderot, Sorbonne Paris Cité, CNRS-UMR 7162, 75013 Paris, France
[2] LTCI, CNRS, Télécom ParisTech, Université Paris-Saclay, 75013 Paris, France
[3] LPN, UPR20 CNRS, Marcoussis, France
e-mail: eleni.diamanti@telecom-paristech.fr

Abstract

We experimentally demonstrate a multi-user quantum key distribution scheme based on polarization entangled photons emitted from an AlGaAs chip and standard telecom wavelength division multiplexers.

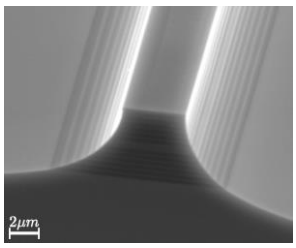
Introduction

The implementation of quantum cryptographic protocols, and in particular quantum key distribution (QKD), is typically based on the use of single photons (or attenuated coherent light) or entangled photon pairs [1]. The latter allows for enhanced performance, for instance, with respect to the attainable communication range [2], and also crucially opens the way to device-independent schemes [3]. In the context of the emerging quantum communication networks, the practical implementation of such protocols will require efficient and easily integrated entangled photon sources. Additionally, the use of such resources needs to be optimized via multiplexing techniques as in current fiber telecommunication networks. Here we address these requirements and demonstrate a multi-user quantum key distribution scheme using a semiconductor source of entangled photons operating at room temperature and standard telecom wavelength division multiplexers.

Experimental setup and results

Our experimental setup is based on an AlGaAs waveguide (Fig. 1a) and is schematically shown in Fig. 1b. The device is pumped by a Ti:saphir laser at 778 nm and generates photon pairs within a large bandwidth (about 120 nm) around 1556 nm via type-II spontaneous parametric down conversion (SPDC) [4]. The weak birefringence of the TE and TM guided modes at telecom wavelengths allows direct generation of the polarization entangled Bell state: $\left|\Psi^{+}\right\rangle = \left(\left|HV\right\rangle + \left|VH\right\rangle\right)/\sqrt{2}$, where $H(V)$ stands for horizontal (vertical) polarization. Due to the energy conservation in the nonlinear process, the signal and idler photons of the generated pairs exhibit frequency anti-correlation in the entire bandwidth. Thus, standard telecom dense wavelength division multiplexers (DWDM) can be used to separate them. An entangled state can then be shared between two users who receive the photons from symmetric channels with respect to the degeneracy wavelength $2\lambda_p$ [5]. In our experiment, we use an 8-channel commercial DWDM with a channel width and channel separation of 0.8 nm (100 GHz). We are able to show polarization entanglement for four channel pairs corresponding to four different pairs of users.

In order to implement the BBM92 QKD protocol [6] with our setup, the photons of the generated entangled pairs are projected in the natural or diagonal polarization basis using a half-wave plate and a fiber polarizing beam splitter (PBS) and detected with InGaAs free-running single photon detectors (Fig. 1b). By calculating the visibility of their coincidence measurements in the two bases, the two selected users (Alice and Bob) can then estimate the quantum bit error rate (QBER) of their communication and derive the secret key generation rate using standard security proof techniques [2].

a) 

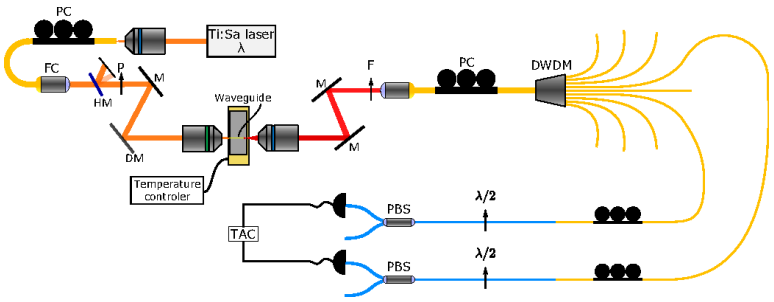
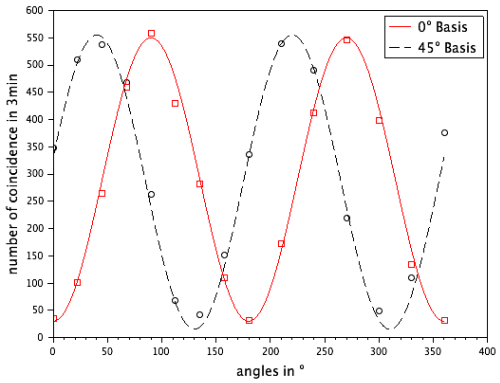
b) 

Fig. 1: a) Scanning electron microscope image of the AlGaAs chip. b) Sketch of the multi-user quantum key distribution experimental setup.

In Fig. 2a, we show the obtained visibility curves for the ITU (International Telecommunication Union) channel pair 23-27 in the natural and the diagonal polarization bases. The mean visibility is equal to 86.7% and the QBER is equal to 6.6% leading to a secret key generation rate of 3.2 bit/s at zero distance (Fig. 2b). We have also performed QKD over a long distance using 25-km fiber spools between the DWDM and PBS components on both channels, hence adding up to a 50-km distance between the two users. The corresponding results are shown in Fig. 2b together with the theoretical prediction of the secret key generation rate as a function of the distance between Alice and Bob for our experimental parameters. The results for the other channel pairs are similar to the ones shown here with some variations mainly due to the slightly different losses of the DWDM channels.

a) 

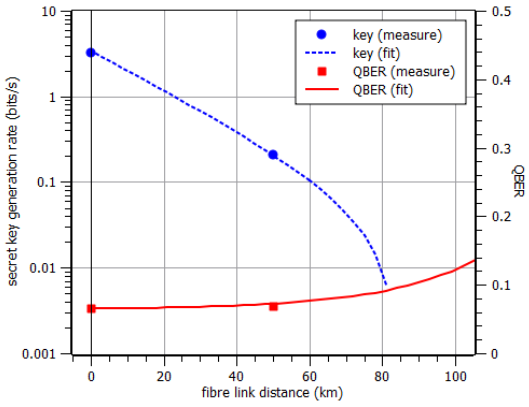
b) 

Fig. 2: a) Visibility curve in the natural and diagonal polarization bases for ITU channel pair 23-27. b) Evolution of the secret key generation rate and the QBER as a function of the distance between Alice and Bob for ITU channel pair 23-27.

Conclusion

We have demonstrated quantum key distribution between multiple users using entangled photon pairs generated by an AlGaAs chip over a total distance of 50 km. Standard telecom DWDM with 40 channels can readily allow to extend the use of a single source to 40 users. The setup robustness and flexibility as well as the electrical injection compatibility of our source [7] make our implementation particularly appealing for practical secure quantum communications within network infrastructures.

References

[1] V. Scarani et al, “The security of practical quantum key distribution”, Rev. Mod. Phys. 81, 1301 (2009).
[2] X. F. Ma, C.-H. F. Fung, and H.-K. Lo, “Quantum key distribution with entangled photon sources,” Phys. Rev. A 76, 012307 (2007).
[3] S. Pironio et al, “Device-independent quantum key distribution secure against collective attacks,” New J. Phys. 11, 045021 (2009).
[4] C. Autebert, N. Bruno, A. Martin, A. Lemaitre, C. Gomez Carbonell, I. Favero, G. Leo, H. Zbinden, and S. Ducci, “Integrated AlGaAs source of highly indistinguishable and energy-time entangled photons,” Optica 3, 143 (2016).
[5] J. Trapateau, J. Ghalbouni, A. Orieux, E. Diamanti, and I. Zaquine, “Multi-user distribution of polarization entangled photon pairs,” J. Appl. Phys. 118, 143106 (2015).
[6] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” Phys. Rev. Lett. 68, 557 (1992).
[7] F. Boitier et al, “Electrically injected photon-pair source at room temperature”, Phys. Rev. Lett 112, 183901 (2014).