Autocompensating Measurement-Device-Independent quantum cryptography in few-mode optical fibers

Jesús Liñares-Beiras[1,*], *Xesús* Prieto-Blanco[1], *Daniel* Balado[1] and *Gabriel M.* Carral[1,**]

[1]Quantum Materials and Photonics Research Group, Department of Applied Physics, Faculty of Physics / Faculty of Optics and Optometry, University of Santiago de Compostela, Campus Vida s/n, E-15782, Santiago de Compostela, Galicia, Spain.

Abstract. We present an autocompensating quantum cryptography technique for Measurement-Device-Independent quantum cryptography devices with different kind of optical fiber modes. We center our study on collinear spatial modes in few-mode optical fibers by using both fiber and micro-optical components. We also indicate how the obtained results can be easily extended to polarization modes in monomode optical fibers and spatial codirectional modes in multicore optical fibers.

1 Introduction

Quantum cryptography is based on the properties of quantum mechanics to obtain secure quantum key distribution (QKD) by using different protocols. The seminal protocol has been the so-called BB84 one in which four states define a set of two mutually unbiased basis. The security in line is guaranteed by the laws of physics, but side channel attacks are still posible. However, the Measurement-Device-Independent (MDI) quantum cryptography [1] has solved the detector side channel attacks. As to the different emisor channel attacks they can be solved *ad hoc*. On the other, different optical fiber systems have been proposed to implement QKD cryptography. Such systems can use different kind of modes, for instance, polarization modes in monomode optical fibers, spatial collinear modes in few-mode optical fibers (FMF) and spatial codirectional modes in multicore optical fibers. However, a common problem is that at least four linear combinations of two modes have to be used and therefore these modes need to keep stable over large distances of optical fibers. Mode instability is due to the modal coupling undergone by the modes in their propagation along real optical fibers with small imperfections or (slow) temporal perturbations. To overcome this drawback polarization autocompensating techniques have been proposed in cryptography with single-photon quantum states [2]. In this work we propose an autocompensating quantum cryptography technique for two-photon quantum states, and in particular Autocompensating MDI-QKD (A-MDI-QKD). We study in detail two collinear modes of a few-mode optical fiber by using both fiber and micro-optical components. The results can be easily extended to both polarization and codirectional modes. The photonic devices are analogous to those ones used in 1-qudit cryptography [3].

*e-mail: suso.linares.beiras@usc.es
**e-mail: gabrielmaria.carral@rai.usc.es

2 Basis and Bell states for A-MDI-QKD

A FMF can support several collinear modes. Let us consider the horizontal and vertical Hermite-Gaussian (HG) modes, which are denoted as X and Y modes. Likewise, we assume a biphoton quantum source, or alternatively, two sources of weak coherent pulses together with decoy states for security purposes. Moreover, let us consider that the initial state is excited in HG modes rotated $\pi/4$,

$$|L_i\rangle = |L_{hi}\rangle\,|L_{vi}\rangle = \rangle \frac{1}{2}(|1_{hX}\rangle + |1_{hY}\rangle)\,(|1_{vX}\rangle + |1_{vY}\rangle) \quad (1)$$

where subindices h, v stand for modes in Alice and Bob paths. The basic setup of the quantum cryptographic system is shown in figure 1. The transmission between Alice (A) and Charlie (C) and Bob (B) and C is made by means of FMFs. The state (1) is produced by the initial states generator (ISG) (a SPDC source or two lasers). Moreover, the systems A-(A) and B-(A) contain autocompensating optical devices and a quantum states generator device by

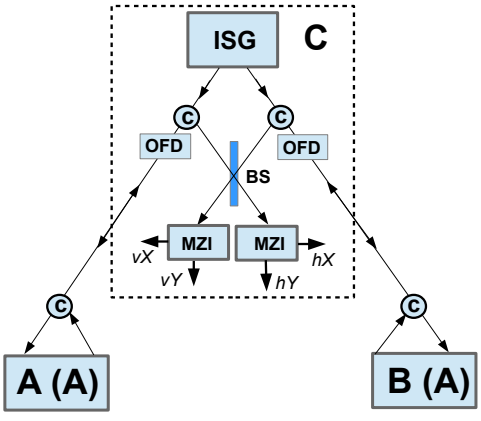

Figure 1. Basic setup of the cryptographic A-MDI-QKD system.

phase shifting. Finally, in the C system there is a detection system with a Beam-Splitter (BS), two Mach-Zehnder Interferometers (MZI) and four detectors $\{hX, hY, vX, vY\}$. A and B have to use the following modal basis

$$\begin{aligned}\mathcal{B}_1 &= \{\tfrac{1}{\sqrt{2}}(|1_{aX}\rangle \pm |1_{aY}\rangle)\} = \{|1_{a\binom{P}{N}}\rangle\}\\ \mathcal{B}_2 &= \{\tfrac{1}{\sqrt{2}}(|1_{aX}\rangle \pm i|1_{aY}\rangle)\} = \{|1_{a\binom{L}{D}}\rangle\},\quad a = h, v\end{aligned} \tag{2}$$

Note that the standard MDI protocol has states $|1_{aX}\rangle, |1_{aY}\rangle$, which are not suitable for MDI autocompensating purposes. When A and B receive the single photon state they have to choose a relative phase $\theta = \{0, \pi, \pi/2, -\pi/2\}$ in order to send a single photon state to C in base $\mathcal{B}_1$ or $\mathcal{B}_2$. When single photon states reach the C system then a BS entangles the single photon states and Bell states are produced, that is, the unitary transformation $\hat{U}_x = \exp\{i(\pi/4)\sigma_x\}$ has to be implemented, where σ_x is the first Pauli matrix. HOM states are also obtained, as for example: $|2_{hX}\rangle, |2_{vX}\rangle, ...$, however they are not used in the MDI protocol because provide ambiguous information. They can be used to calibrate the system, that is, to check that photons reach the C system at the same time. By post-selecting the events where they use the same basis, it is easy to check that the Bell states are obtained for all biphoton states: $|1_{h\alpha}1_{v\alpha'}\rangle$, with $\alpha, \alpha' = P, N$ or $\alpha, \alpha' = L, D$, that is,

$$\begin{aligned}|\Psi^-\rangle &= \tfrac{1}{\sqrt{2}}(|1_{hX}1_{vY} - |1_{vX}1_{hY})\\ |\Phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|1_{hX}1_{hY} + |1_{vX}1_{vY})\end{aligned} \tag{3}$$

$|\Psi^-\rangle$ is obtained if $\alpha \neq \alpha'$ and $|\Phi^+\rangle$ if $\alpha = \alpha'$. The probability of detecting these states is 1/2 in each event in the same basis. The results can be extended to polarization modes H, V and two codirectional modes 1,2 (two-core optical fiber) by the formal changes: $(X, Y) \equiv \{(H, V), (1, 2)\}$,

3 Photonic system for A-MDI-QKD

Autocompensating is obtained after one loop implemented by optical circulators (c). We present the main devices to achieve autocompensating MDI-QKD. One of them is an optical fiber delay (OFD) device placed just after the circulators in the C system. This device can be realized by a MZI with a Dove prism (DP) and an external optical path (optical fiber), as shown in figure 2. It produces a delay τ between states $|1_X\rangle$ and $|1_Y\rangle$, in order to introduce phases θ in A and B systems and obtain the different biphoton states. Next, autocompensating devices (A) are placed in A and B after the circulators. A sketch of these devices is shown figure 3. It can easily be checked that by the unitary transformation $\hat{U}_y = \exp\{i(\pi/2)\sigma_y\}$ any random unitary transformation between modes X and Y from C to A (and B) due to modal coupling by imperfections or slow temporal perturbations is compensated along the path back between A (B) and C. Transformation $\hat{U}_y$ can be implemented at A and B systems by a local loop with two cylindrical lens converters (CLC) which shift $\pm\pi/2$ the HG modes and a DP rotated $\pi/4$ as shown in figure 3. Note that when the state reaches again the ODF device the modes X and Y become synchronous again. Therefore the states reach the BS at the same time in the C system.

4 Detection photonic device

The detection system after the BS is formed by two MZIs and four detectors: hX, hY, vX, vY as shown in figure 1. The MZIs are identical to the one used inside the OFD device shown in figure 2, that is, it works like a BS depending on the spatial mode. Thus, X modes are detected in the horizontal direction and the Y modes in the vertical direction. The Bell states are identified by different coincidences results according to equation (3). The steps of the BB84 protocol can be followed to obtain QKD.

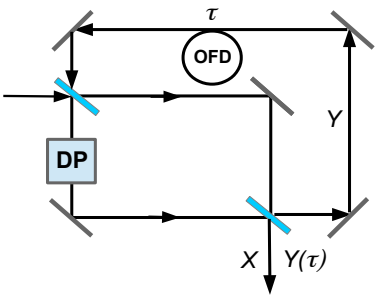

Figure 2. Basic setup of a OFD device.

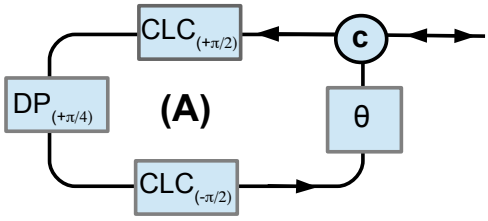

Figure 3. Basic setup of the autocompensating system.

5 Conclusions

We have proposed autocompensating MDI-QKD by using two spatial modes (Hermite-Gaussian ones) of FMF fibers and suitable biphoton quantum states. An unitary transformation (a $\pi/2$-rotation) is required, which is implemented by a local loop containing a DP between two cylindrical lens converters. The results can be extended to both polarization and codirectional modes.

Acknowledgement. Authors wish acknowledge the financial support of this work by Xunta de Galicia, Consellería de Educación, Universidades e FP, Grant GRC Nº ED431C2018/11 and a predoctoral grant (D. Balado, 2017), co-financied with the European Social Fund.

References

[1] H. Lo, M. Curty, B. Qi, Phys. Rev. Lett., **108**, 130503 (2012)
[2] D. S. Bethune, W. P. Risk, New J. Phys., **4**, 42 (2002)
[3] D. Balado, J. Liñares, X. Prieto-Blanco, J. Mod. Opt. **66**, 947-957 (2019)