EPJ Web of Conferences **238**, 11004 (2020) https://doi.org/10.1051/epjconf/202023811004
EOSAM 2020

Autocompensating high-dimensional quantum cryptography by phase conjugation in 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 a system based on phase conjugation in optical fibers for autocompensating high-dimensional quantum cryptohraphy. Phase changes and coupling effects are auto-compensated by a single loop between Alice and Bob. Bob uses a source of coherent states and next Alice attenuate them up to a single photon level and thus 1-qudit states are generated for implementing a particular QKD protocol, for instance the BB84 one, together with decoy states to detect eavesdropping attacks.

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. On the other hand, 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 modes in few-mode optical fibers and spatial codirectional modes in multicore optical fibers. One of the advantages of using optical modes is that high-dimensional QKD (HD-QKD) can be implemented, which improves the security. However, one of the most important drawbacks is that all modes need to keep stable over large distances along optical fibers. Mode instability is due to the modal coupling undergone by the modes in their propagation in optical fibers with small imperfections or slow temporal perturbations. To overcome this drawback some polarization autocompensating techniques have been proposed in cryptography with 1-qubit quantum states [1] or even with 1-qudits acquiring random relative phases [2]. In this work we propose a general autocompensating quantum cryptography technique based on phase conjugation for both few-mode optical fibers (FMF) and multicore optical fibers (MCF) where modal coupling is not negligible. Input multimode coherent states are launched and later attenuated in their path back up to a single photon level (weak coherent states), that is, 1-qudit states are produced. Moreover, decoy states have also to be generated for security purposes. Optical devices for QKD with collinear modes of FMFs can be realized by using both fiber and micro-optical components, and with codirectional modes of MCFs by using also integrated optical components.

2 Phase conjugation of coherent states

Let us consider a four-wave mixing (FWM) nonlinear interaction system of length L as shown in figure 1. Operator $\hat{a}_3 \equiv \hat{a}_3(0)$ is associated to the optical mode transmitted along the FWM system, and $\hat{a}_4 \equiv \hat{a}_4(L)$ is associated to the “reflected” optical mode. Likewise, there are two pump waves with very large amplitudes A_1 and A_2 and initial phases equal to zero. The nonlinear interaction strength is given by the coupling coefficient $\kappa = \chi_{eff}|\mathrm{A}_1||\mathrm{A}_2|\,\mathrm{L}$, where χ_{eff} is an effective nonlinear susceptibility. It is wellknown that the following operator transformations are fulfilled

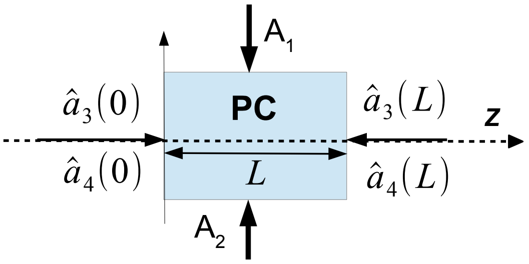

Figure 1. Four-wave mixing with two pump waves.

$$\begin{aligned} \hat{a}_3(L) \equiv \hat{a}_{o3} &= s\,\hat{a}_3 + it\,\hat{a}_4^{\dagger} \\ \hat{a}_4(0) \equiv \hat{a}_{o4} &= s\,\hat{a}_4 + it\,\hat{a}_3^{\dagger} \end{aligned} \tag{1}$$

where $s = \sec(\kappa L), t = \tan(\kappa L)$. Next, let us consider a coherent state $|\alpha_3 0_4\rangle$ excited in one optical fiber mode and incident on the FWM system. The output state is given by $|L\rangle = |\alpha_3 0_4\rangle = e^{\alpha\hat{a}^{\dagger}_{o3} - \alpha^{\star}\hat{a}_{o3}}\,|00\rangle \rightarrow |L_c\rangle = |s\alpha\rangle\,|-it\alpha^{\star}\rangle$, where equation (1) has been used, that is, the FWM is a phase conjugator (PC). Note that the reflected coherent state has been conjugated. We are interested on multimode coherent states, that is, $|L\rangle = |\alpha_1 ... \alpha_N\rangle$ excited in N optical modes, therefore the output state will be

$$|L_c\rangle = (|s\alpha_1\rangle\,| - it\alpha_1^{\star}\rangle)...(|s\alpha_N\rangle\,| - it\alpha_N^{\star}\rangle) \tag{2}$$

[*] e-mail: suso.linares.beiras@usc.es
[**] e-mail: daniel.balado.souto@usc.es

3 Phase conjugation for HD-QKD

Let us consider a FMF or MCF optical fiber supporting d modes with operators $\hat{a}_i$, $i = 1, ..., d$ in order to implement HD-QKD with 1-qudit states. For sake of simplicity we assume that polarization-maintaining optical fibers are used [3]. In that case, FMFs have negligible modal coupling, however unpredictable relative phases still happen [2]. In general, each optical mode will undergo coupling to other modes and therefore the state reaching Bob system from the Alice system will be a unpredictable 1-qudit state which prevents us to implement any protocol for QKD. Next, we show how to overcome this drawback with phase conjugation. We start from the spatial Heisenberg equation describing the modal coupling,

$$-i\hbar\frac{\partial\hat{a}_i}{\partial z} = \hbar\left(\beta_i\sum_{ij}\delta_{ij}\hat{a}_j + \sum_{ij}\kappa_{ij}\hat{a}_j\right) \equiv \sum_{ij}C_{ij}\hat{a}_j \qquad (3)$$

β_i are propagation constants and κ_{ij} are modal coupling coefficients. C_{ij} is a symmetric matrix, therefore the matrix solution $S_{ij} = \exp\{iC_{ij}z\}$ of differential equation (3) is a complex symmetric matrix, that is, $S_{ij} = S_{ji}$. On the other hand, modal coupling is an unitary transformation, therefore $S_{ij}^{-1} = S_{ij}^{\star}$. Next, let us consider q different modal couplings along z direction from a point B to point A with total matriz $M = S_1 \cdots S_q$. Therefore, if we have a PC at A we obtain $M' = S_q^{\star} \cdots S_1^{\star}$, and after the light has traveled the path back and forth, the total coupling matrix is $M'M = \mathbb{I}$, that is, the unpredictable modal coupling has been removed. Therefore if we start from a state $|L\rangle$ undergoing modal coupling, the state after the PC and travelling the path back is $|L_c\rangle$ given by equation (2). This is the key result to be used in a QKD system.

4 BB84 autocompensating system

By using the PC shown in section 2 together with the theoretical results of section 3 we design an autocompensating optical system for HD-QKD BB84 quantum cryptography in optical fibers as shown in figure 2. The first device of the system is a states generator (SG) located in Bob system, which emits a multimode coherent state $|L\rangle = |\alpha_1...\alpha_N\rangle$ excited in N optical modes of a FMF or MCF fiber, with $\alpha_1 = ... = \alpha_N$, in order to generate states belonging to unbiased basis. Next, one (for FMFs) or several (for MCFs) optical circulators c launches the state towards Alice. A Demultipexer-Multuplexer (D-M) device is needed to produce delays τ between modes if a FMF is used; if we use a MCF then the D-M device is not required. Next, quantum state reaches the PC, where a previous phase shifter (PS) is found in off-position. We must stress that each single mode coherent state (a core in a MCF) becomes a multimode coherent state due to modal coupling. Now, the reflected state in the PC device goes through the PS which introduces phases θ_i on the coherent states. We obtain 1-qudit states in Alice system starting from the multimode coherent states and attenuated up to single photon level,

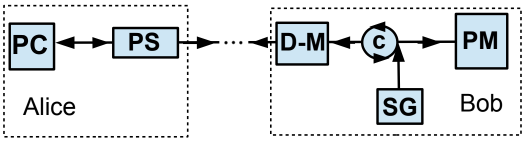

Figure 2. Basic setup of autocompensating high-dimensional cryptography by phase conjugation.

$$|L_c\rangle = \sum_i \frac{1}{\sqrt{N}}\{e^{i\theta_1}|1_1\rangle + ... + e^{i\theta_N}|1_N\rangle\} \qquad (4)$$

These states must belong to two N-dimensional biased basis. Likewise, Alice has to produce decoy states for security purposes. When the 1-qudit again reaches the Bob system finds the D-M device, which cancels the delays τ between states $|1_j\rangle$. Finally, the circulator drives the state up to the device that implements projective measurements (PM) [2]. We show in figure 3 an integrated quantum projector (IQP) for the case of MCFs. It is formed by four directional couplers 3dB ($\mathrm{D}_{\pi/4}$) and an inversor ($\mathrm{D}_{\pi/2}$) together with ($3\pi/2$)-phase shifters. At the input of IQP there are four phase-shifters ϵ_i, i=1, ..., 4 which allow to choose the measurement basis. As an example, let us consider ϵ_i=0 at the input 1-quart state $|L_i\rangle = 2^{-1}(|1_{o1}\rangle - i|1_{o2}\rangle - i|1_{o3}\rangle - |1_{o4}\rangle)$. It can easily calculated that the output state is $|L_o\rangle = |1_1\rangle$, that is, it is projected on the mode 1 and so on with other unbiased orthogonal states as for example $|L_i\rangle = 2^{-1}(|1_{o1}\rangle - i|1_{o2}\rangle + i|1_{o3}\rangle + |1_{o4}\rangle)$, which is projected on $|1_2\rangle$.

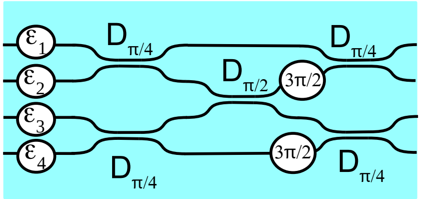

Figure 3. Sketch of an integrated quantum projector.

5 Conclusions

We have presented an autocompensating technique based on phase conjugation for quantum cryptography in FMF and MCF optical fibers. A single loop allows to autocompensate the undesidered modal coupling, and thus a HD-QKD BB84 protocol can be implemented.

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

References

[1] D.S.Bethune,W.P.Risk, New J.Phys., **4**,42(2002)

[2] D.Balado, J.Liñares, X.Prieto-Blanco, D.Barral, JOSA B **36**, 2793-2802 (2019)

[3] L.Wang, S.LaRochelle, Opt.Lett.**40** 5846-5849 (2015)