Autocompensating high-dimensional quantum cryptography by using integrated photonic devices in multicore optical fiber spatial multiplexing systems

***Daniel Balado*[1], *Xesús Prieto-Blanco*[1], *David Barral*[2], *Jesús Liñares*[1]**

[1]*Area of Optics, 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*

[2] *Centre de Nanosciences et de Nanotechnologies C2N, CNRS, University of Paris-Saclay, Route de Nozay, 91460 Marcoussis, Paris, France*

In the last years, space division multiplexing has been proposed to further increase the data bandwidth in optical communications, therefore a high interest has arisen about new optical fibers such as few-mode fibers and multicore fibers (MCF) [1]. Consequently, the implementation of quantum cryptography in these new optical fibers can be regarded as a strategic task, particularly if we take into account that high-dimensional cryptography [2] can be implemented. The main drawbacks are related to modal cross-talking and random delays and relative phases acquired by spatial modes under propagation. The first drawback can be notably minimized by using optical fibers with a low cross-talking. For instance, MCFs with well-separated cores can be used, and accordingly it is enough to focus on the second drawback where relative phases and delays have to be autocompensated. Autocompensating techniques have been suggested for polarization modes some years ago [3] and therefore restricted to a bidimensional Hilbert space. However, if spatial modes are considered in order to get high-dimensional quantum key distribution (QKD) then new autocompensating and projective measurement devices are needed.

In this work we propose a high-dimensional QKD based on autocompesating with spatial modes of a MCF by using integrated photonic devices together with optical fiber components. We also present integrated optical devices for quantum projective measurements. We use the BB84 protocol which requires working with mutually unbiased bases (MUBs) $\{|L_{\mu(j)}\rangle\}$, $\mu = 1,...,D$, $j = 1,...,N$, that is, $|\langle\, L_{\mu(j)}|L_{\mu'(j')}\rangle|^2 = 1/D = \mathscr{P}$, $j \neq j'$ $(j, j' = 1,...,N)$ $\forall\, \mu, \mu' = 1,...,D$. Without lost of generality we consider a Hilbert space of dimension $D = 4$ (ququart states) and four bases ($N = 4$) although higher dimensions could be considered. In particular, we choose the following set of MUBs: $B_1 = \{(1/2)(1,1,1,1); (1/2)(1,1,-1,-1); (1/2)(1,-1,-1,1); (1/2)(1,-1,1,-1)\}$, $B_2 = \{(1/2)(1,-1,-i,-i); (1/2)(1,-1,i,i); (1/2)(1,1,i,-i); (1/2)(1,1,-i,i)\}$, $B_3 = \{(1/2)(1,-i,-i,-1); (1/2)(1,-i,i,1); (1/2)(1,i,i,-1); (1/2)(1,i,-i,1)\}$, $B_4 = \{(1/2)(1,-i,-1,-i); (1/2)(1,-i,1,i); (1/2)(1,i,-1,i); (1,i,1,-i)\}$. Note that for these MUBs $\mathscr{P} = 1/4$ and moreover only the relative phases 0, π, $\pm\pi/2$ are used to generate the sixteen single photon states.

The physical implementation is made by an encryption system formed by Alice and Bob subsystems. The first one consists of an integrated device to achieve a modal inversion for autocompensating, together with integrated electro-optic phase shifters to produce the sixteen quantum states of the four MUBs. The primary quantum state generation, for instance the ququart $|L\rangle = (1/2)(|1_1\rangle + i|1_2\rangle + |1_3\rangle + i|1_4\rangle)$, and the detection of any of the sixteen final quantum states (projective measurements) is made in the Bob subsystem. It is composed by a primary quantum state generator (integrated device with directional couplers and integrated phase shifters) and a multiround trip controller implemented by an integrated electro-optical device, which also does inversions required for autocompensating. Finally, there is a detection device where quantum states are measured once a double-round trip is realized. This detection device consists of four integrated optical devices (four chips) where projective measurements are made. Random measurements are made by using directional couplers to obtain sixteen outputs, that is, the single photon state has the same probability of being measured in some of the four bases.

References

[1] N. Bai, E. Ip,Y. Huang, E. Mateo, F. Yaman, M. Li, S. Bickham, S. Ten, J. Liñares, C. Montero, V. Moreno, X. Prieto, V. Tse, K.. Chung, A.P.T. Lau, H. Tam, C. Lu, Y. Luo, G. Peng, G. Li, T. Wang, "Mode-division multiplexed transmission with inline few-mode fiber amplifier", Optics Express, **20** 2668-2680 (2012).

[2] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M.J. Padgett, T. Konrad, F. Petruccione, N. Ltkenhaus, A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases", Phys. Rev. A **88**, 032305 (2013).

[3] D.S. Bethune, W.P. Risk, "Autocompensating Quantum Cryptography", New Journal of Physics **4**, 42 (2002).