Quantum cryptography with position and momentum of the photon

P. H. Souto Ribeiro(1), M.P. Almeida(2), D.S. Lemelle(3), and S. P. Walborn(4)
1: Instituto de Física - Universidade Federal do Rio de Janeiro –
CP 68528 – Rio de Janeiro – RJ - 21 941 – 972 – Brazil (phsr@if.ufrj.br)
2: Department of Physics - University of Queensland (marcelo@physics.uq.edu.au)
3: Instituto de Física - Universidade Federal do Rio de Janeiro (lem@if.ufrj.br)
4: Instituto de Física - Universidade Federal do Rio de Janeiro (swalborn@if.ufrj.br)

Abstract

We review a series of experiments demonstrating the use of the transverse position and momentum of the photon to encode qbits in quantum key distribution protocols. We show that it is possible to implement BB84 and BBM protocols through the discretization of the position and momentum spaces. We also present proof of principle demonstrations for protocols using higher order alphabets with single photons and position-momentum and with two-photons and position-momentum plus polarization.

Introduction

Quantum cryptography, or quantum key distribution(QKD) is probably the most developed practical application in the new field of quantum information [1]. While it is still unknown if quantum computers are reliable and if they can offer some advantage over classical ones, there are commercial systems working with quantum cryptography. Even though its development was relatively fast, several challenges still prevent quantum cryptography to disseminate to all secret communication applications in private and military business. Low bit rate transmission and small distance ranges, are among the main limitations of the present systems.

Even though polarization has usually been the most used degree of freedom of the photon, other schemes have been proposed and implemented using energy-time, for instance [2]. In this work, we present a series of experiments[3,4,5,6] demonstrating the use of the transverse position and momentum of the photon in different QKD protocols. The interest in the use of this degree of freedom is related to: i) the simplicity in the preparation and detection for both single photon and two-photon entangled states; ii) the possibility of implementing alphabets with more than two levels(qdits with d>2); iii) the possibility of combining it with other degrees of freedom like the polarization, for instance.

Experiments

In a first experiment[3], shown in Figure 1, we show that it is possible to replace the photon polarization by its transverse position and momentum, in a BB84 protocol. Position and momentum states can be prepared with lenses. If Alice prepares a position state and Bob measures in the right basis, we see two distinguishable spots, as in the upper Figure2a and b. If Bob measures in the wrong basis, we see the extended beams in Figure2c and d, where the spots representing the bits 1 and 0, cannot be distinguished from each other anymore.

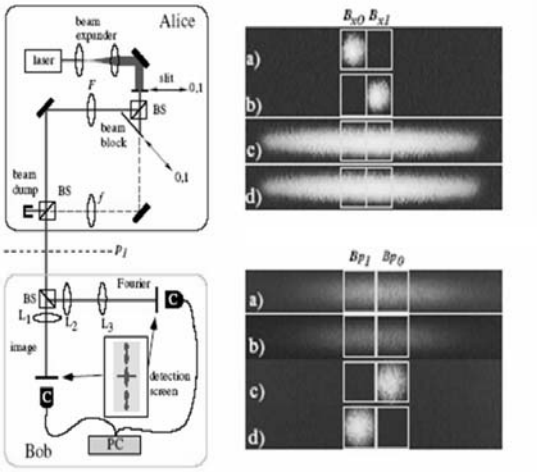

Figure 1: Experimental set-up: single photon.

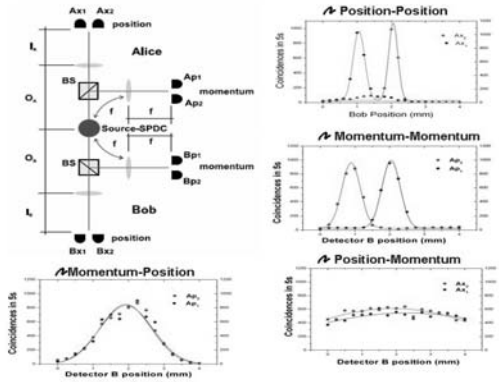

Figure 2: Experimental set-up : entangled photons

In a second experiment[4], we show that the BBM[7] protocol can also replace polarization with position-

momentum of the photons. The BBM protocol is equivalent to the BB84 protocol, but runs with entangled pairs of photons instead of single photons. In Figure 2, the experimental set-up and results are shown. The principle is the same as in the previous experiment. When Alice and Bob measure in coincident basis, two positions or two momenta are distinguishable, otherwise they cannot be distinguished.

In a third experiment[5], we show that it is possible to run two parallel BBM protocols with pairs of photons. One using polarization entanglement and other using position-momentum entanglement. It is also seen that a qdit protocol can also be implemented, with d=4, being two levels in the polarization and 2 levels in the position-momentum.

In a fourth experiment[6], we show that the use of position-momentum of the photon, allows the encoding of higher order alphabets. See Figure 4. Instead of qbits, qdits with d=37 are transmitted from Alice to Bob. This allows the enhancement of the amount of shared information per photon and also improves the sensitivity to eavesdropping. The principle is the same as the qbit protocol. The difference is that instead of using two positions and two momenta in the preparation and detection planes, 37 cells are used.

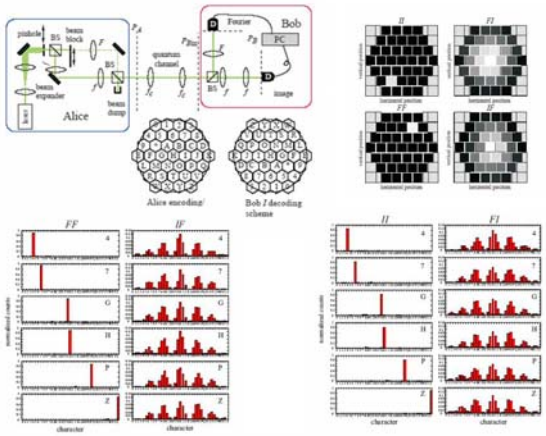

Figure 4: Experimental set-up: single photon with d=37.

Conclusions

In conclusion, we have presented four experiments, using the transverse position and momentum of the photon for encoding bits and dits of information in QKD protocols. In the first one, a single-photon BB84 protocol is implemented with position-momentum instead of polarization. In the second one, a BBM protocol is implemented with position-momentum instead of polarization. In a third one, two BBM protocols are implemented in the same pair of photons, one with polarization and other with position-momentum. In the fourth one, a 37 levels byte is encoded in a single photon, and a BB84-like protocol is implemented. Those experiments show that position-momentum of the photons are interesting for academic and pedagogical purposes and might be useful in practical QKD, once the transmission issue is properly addressed..

Acknowledgements

CNPq, CAPES, FAPERJ, Institutos do Milênio de Informação Quântica, PRONEX and FUJB have funded this work.

References

[1] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden; Rev. Mod. Phys. **74**, 145 (2002)

[2] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin; Phys. Rev.Lett. **84**, 4737 (2000)

[3] D. S. Lemelle, M. P. Almeida, P. H. Souto Ribeiro and S. P. Walborn; Am. J.of Phys. **74**, 542 (2006)

[4] M. P. Almeida, S. P. Walborn, and P. H. Souto Ribeiro; Phys. Rev. A, **72** 022313 (2005).

[5] M. P. Almeida, S. P. Walborn and P. H. Souto Ribeiro; Phys. Rev. A-Rapid Communication **73**, 040301(R) (2006)

[6] S. P. Walborn, D. S. Lemelle, M. P. Almeida and P. H. Souto Ribeiro, Phys. Rev. Lett. **96**, 090501 (2006)

[7] C. H. Bennett, G. Brassard, and N. D. Mermin; Phys. Rev. Lett. **68**, 557 (1992)