Quantum cryptography with position and momentum of the photon
M.P. Almeida, D.S. Lemelle, S. P. Walborn and P. H. Souto Ribeiro
Instituto de Física - Universidade Federal do Rio de Janeiro
CP 68528 – Rio de Janeiro – RJ - 21 941 – 972
Brazil
phsr@if.ufrj.br

Abstract
We review a series of experiments demonstrating the use of the transverse position and momentum of the photon to encode qu-bits in quantum key distribution protocols. It is shown that a perfect analogy with the protocols based on the photon polarization is achieved under discretization of the position and momentum spaces. It is also shown that protocols using higher order alphabets can be implemented with single photons and position-momentum and with two-photons and position-momentum plus polarization.

Introduction
Quantum cryptography 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.

The term quantum cryptography is not actually proper. In fact, classical cryptography is already able to provide perfect security in secret communication between two parties, traditionally called Alice and Bob. The problem is that perfect security is only achieved with the so called one time pad protocol. In this protocol, it is assumed that Alice and Bob share a secret key in the beginning of the protocol. In order to obtain full security, the key is required to have the same size of the message. Therefore, Alice and Bob are left with the problem of sharing large secret random keys, before the communication starts. What is usually called quantum cryptography, is actually a quantum key distribution (QKD) protocol, which continuously provide Alice and Bob with secret random strings that can be used as keys in the one time pad protocol.

The idea of taking advantage of the quantum properties of the light for implementing a QKD protocol, was introduced by Bennet and Brassard in a famous work [2]. The protocol, also called BB84, is based on the preparation of polarization states in a single photon (it is important to be a n=1 Fock state) by Alice and the detection by Bob, using two maximally overlapping polarization basis. As the preparation of n=1 Fock states are usually very hard, there is also a version of this QKD protocol based on the use of two polarization entangled photons [3].

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 [4]. In this work, we present a series of experiments [5,6,7,8] 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 facts like the simplicity of the preparation and detection, the simplicity in the preparation of two-photon entangled states, the possibility of implementing alphabets with more than two levels (qu-dits with d>2) and the possibility of combining it with other degrees of freedom like the polarization, for example.

Experimental Setup
The BB84 QKD protocol can be described using Figure 1. In the beginning, Alice and Bob choose two polarization working basis, for instance, horizontal/vertical (HV) and +45/-45 degrees (+/-). Alice chooses randomly between one of the two basis and prepares one photon state and send it to Bob (Figure 1a,b). In receiving the photon, Bob also chooses randomly between measuring it in one of the two basis. At the end of the transmission, Alice and Bob compare, through ordinary communication channels, their lists of measurement basis (but not the polarization states prepared and measured), keeping the ones in which the preparation and measurement basis coincide and discarding the rest. At the end of this protocol, they share a common string of secret bits. What happens if somebody (usually called Eve) tries to eavesdrop the shared information? In
Figure 1c, it is shown that Eve will need to choose between one of the measurement basis. Therefore, she will have 50% chance of succeeding and 50% chance of failing. When she fails, she disturbs the state prepared by Alice and it will produce bit errors in the raw key. By analyzing the final bit string, it is possible for Alice and Bob, to know if somebody has tried to spy their communication.

![Figure 1: BB84 protocol scheme. a) Alice prepares photons in the H-V basis and Bob measures in the right basis. b) Alice prepares photons in the H-V basis and Bob measures in the wrong basis. c) Eve tries to steal information.](image)

In a first experiment[5], shown in Figure 2, 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 Figure 2a and b. If Bob measures in the wrong basis, we see the extended beams in Figure 2c and d, where the spots representing the bits 1 and 0, cannot be distinguished from each other anymore.

![Figure 2: Experimental set-up and results for demonstrating the equivalence between BB84 protocol with polarization and position-momentum of the photon.](image)

In a second experiment[6], we show that the BBM 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 3, the experimental set-up and results are shown. The principle is the same as in the previous experiment. When Alice and Bob measure in the same basis, two positions or two momenta are distinguishable, otherwise they cannot be distinguished.

In a third experiment[7], 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. See Figure 4. It is also seen that a qu-dit protocol can also be implemented, with d=4, being two levels in the polarization and 2 levels in the position-momentum. The upper bar diagrams in Figure 4, correspond to position-momentum measurements and the lower bar diagrams correspond to simultaneous polarization measurements.
Figure 3: Experimental set-up and results for demonstrating the equivalence for the BBM protocol with polarization entangled and position-momentum entangled photons.

Figure 4: Experimental set-up for demonstrating the simultaneous BBM protocol with simultaneous polarization and position-momentum entanglement.

Figure 5: Experimental set-up for demonstrating the use of higher order alphabets in a BB84 protocol using the position and momentum of the photon. The beam was divided in 37 different cells.

In a fourth experiment[8], we show that the use of position-momentum of the photon, allows the encoding of higher order alphabets. Instead of qu-bits, qu-dits 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 security of the protocol. The
principle is the same as the qu-bit protocol. The difference is that instead of using two positions and two momenta in the preparation and detection planes, 37 cells are used.

Conclusions

In conclusion, we have presented four different Quantum Key Distribution protocols, using the transverse position and momentum of the photon for encoding bits of information. In the first one, a one-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 promising for communication applications.

Acknowledgements

The authors thank C. H. Monken, S. Pádua, A. Z. Khoury and D. Jonathan, for helpful and fruitful discussions. CNPq, CAPES, FAPERJ, Institutos do Milênio de Informação Quântica, PRONEX and FUJB have funded this work.

References