Simultaneous observation of correlations in position-momentum and polarization variables

M. P. Almeida, S. P. Walborn,* and P. H. Souto Ribeiro
Instituto de Física, Universidade Federal do Rio de Janeiro, Caixa Postal 68528, Rio de Janeiro, RJ 21941-972, Brazil
(Received 21 September 2005; published 18 April 2006)

We demonstrate experimentally that it is possible to prepare and detect photon pairs created by spontaneous parametric downconversion which exhibit simultaneous position-momentum and polarization correlations. We discuss the use of these correlations in several four-dimensional key distribution protocols.

DOI: 10.1103/PhysRevA.73.040301 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Dv, 42.65.Lm

Photon pairs obtained from parametric down-conversion have played a crucial role in the experimental investigation of the fundamentals and applications of quantum mechanics [1]. On the one hand, most experiments in quantum information and computation use photon pairs entangled in the polarization degree of freedom (DOF) [2,3]. On the other hand, position-momentum entanglement has been investigated and utilized for more than ten years in the context of quantum imaging [4–6] and, more recently, it was shown that down-converted photon pairs are indeed entangled in position-momentum [7,8] through the violation of a separability criterion [9,10]. Photons are the obvious choice for communication-based applications such as quantum key distribution (QKD), due to the ease in which approximate single-photon pulses or entangled photon pairs can be produced, manipulated, and transmitted. To date, there are many QKD protocols [11], beginning with the seminal work of Bennett and Brassard [12], commonly known as the BB84 protocol. While BB84 uses single particles, also well known is the Ekert protocol [13], which utilizes entangled pairs to distribute a random and secure key. Bennett, Brassard, and Mermin (BBM) have adapted the BB84 protocol to entangled particles, and shown that the BB84 and Ekert protocols are essentially equivalent [14]. Using entangled photons, QKD has been demonstrated using polarization [15,16], time-bin [17], and transverse position-momentum [18]. In principle, it should be possible to use two or more of these, or other DOF, simultaneously in a QKD protocol.

Here, we show that it is possible to create and measure downconverted photons which are simultaneously entangled in both polarization and transverse position-momentum. Entanglement in position-momentum is very robust and it is, in fact, actually difficult to produce downconverted photon pairs that are not entangled in position-momentum [23]. Most of the sources of polarization entangled photons, which generally rely on the superposition of two emission cones [2,3], already produce entanglement in position-momentum. A difficulty arises in that this superposition is obtained in the far field, so that by performing a position measurement by imaging one or both photons creates distinguishability in the form of “which cone” information. Thus, in order to utilize both position-momentum and polarization correlations in a QKD protocol, it is necessary to develop a position-momentum measurement scheme which does not destroy polarization entanglement. Here, we demonstrate experimentally that the quantum correlations between position-momentum and polarization of photon pairs can be produced and detected simultaneously.

We then show that these simultaneous correlations could be used to implement QKD protocols based on four-dimensional states, which enhance the transmission rate per photon pair as well as the sensitivity to eavesdropping, two important goals in QKD. For example, for the $d=4$ case (qu-quarts), using a generalized BBM protocol, the transmission rate would be improved from 1/2 (for qubits) to 1 bit per photon photon pair, while the error rate due to eavesdropping based on the intercept-resend strategy would also increase from 1/4 to 3/8, therefore improving the security [19,20]. With simultaneous correlations in multiple DOF, we are at liberty to choose between a number of protocols. We provide three possibilities: A parallel protocol with average transmission rate 1 bit/photon pair and error rate of 1/4, a qu-quart protocol with average transmission rate 1 bit/photon pair and error rate of 3/8, and a deterministic skewed qu-quart protocol with transmission rate 1 bit/photon pair and error rate 1/4.

The experimental setup is shown in Fig. 1. A He–Cd laser was used to pump two 2 mm long lithium iodate crystals arranged with their optic axes perpendicular, creating downconverted signal and idler photons, as reported in Ref. [3]. The signal and idler photons were sent to detection systems $A$ and $B$, respectively. Coincidence counts were registered using SPCM single-photon counting modules (SPCM) equipped with 12 nm FWHM bandwidth interference filters and 0.3 mm diameter detection apertures. Coincidence and single counts were registered using coincidence electronics and a personal computer.

It is well known that this source can be used to create photon pairs in a maximally entangled polarization state [3]. The polarization of the pump beam was adjusted using half- and quarter-wave plates so that the photon pairs were in the state $|\phi^+\rangle=(|HH\rangle−|VV\rangle)/\sqrt{2}$. With the lens systems removed, the polarization entanglement was initially verified by performing the usual polarization interference measurements using linear polarization analyzers consisting of half-wave plates and polarizing beam splitters, where one of the analyzers is kept fixed at 45° and the other is rotated. Interference curves with visibilities above 95% were typically observed in the coincidence counts, while the single-count rates remained approximately constant, indicating a high degree of entanglement.

*Electronic address: swalborn@if.ufrj.br
Due to phase matching in spontaneous parametric down-conversion (SPDC), anticorrelation is observed in transverse momentum measurements. That is, if one detects a signal photon with momentum $p$, one finds an idler photon with momentum $-p$. One can measure momentum by creating the Fourier transform of the field at the source on the detection plane. This is achieved using a lens placed so that the image and object planes each lie in the focal plane of the lens, therefore mapping the transverse momentum distribution of the photons at the crystal face onto positions in the detection plane. Figure 1(b) shows our lens system consisting of a lens with focal length $F=500$ mm. The detectors were placed 1 m from the source. It is thus possible to choose detector positions that exhibit a high spatial anti-correlation. Figure 2(a) shows coincidence counts for two sets of detector positions which display high momentum anticorrelations. Positions $A_{p1}$ and $A_{p2}$ correspond to positions of detector $A$, and likewise $B_{p1}$ and $B_{p2}$ for detector $B$. Also shown is a diagram of the detector positions, from which it can be seen that when one photon is detected in the upper position, the other is detected in the lower position, illustrating the anticorrelation in momentum measurements. The polarization analyzers were orientated at $\theta_1=45^\circ$ and $\theta_2=45^\circ$ to ensure that we collected photons from both crystals. The error rate [18] derived from our experimental results is about 1.5%, well below the limit necessary for successful QKD [11].

Position measurements can be performed by creating the image of the source at the detection plane [7,8]. Using an imaging system, we see position correlations: If the signal photon is detected at position $x$, the idler photon is found at the same position $x$. Position correlations in downconverted photons are due to the fact that the photons are “born” at the same position in the crystal. However, simply imaging the crystal face will destroy the polarization entanglement present in this two-crystal source, since it has been shown that a two-crystal source displays interference that is analogous to a two-photon double-slit experiment [21]. Thus, imaging the crystal face provides which-crystal information that destroys polarization interference. In order to overcome this difficulty, we developed a slightly more complex position measurement system, shown in Fig. 1(c). First, a lens is used to image the crystal face at an intermediate plane $P$. We define an upper and lower spatial region by placing a thin blade in $P$ such that it blocks the lower or upper half of the image, respectively. In this way, passage through plane $P$ determines whether the photon originates from the upper or lower half of the crystal face. We then used a second lens to implement the Fourier transform of plane $P$, which removes the which-path information. In all configurations, the detector remained fixed at the center of the Fourier plane.

Using this detection system, we measured the position correlations, which are shown in Fig. 2(b). For each detection system, we defined positions $A_{x1}$, $A_{x2}$, $B_{x1}$, and $B_{x2}$ of the blade in the image plane $P$. The diagram shows the positions of the blades corresponding to each measurement, which indicates that in this case we have position correlations instead of anticorrelations as in the momentum-momentum case. Here, the error rate is about 10%, still within the bounds for successful QKD [11].

Since position and momentum are complementary observables, there is a complete absence of correlation when systems $A$ and $B$ perform measurements in different bases. Figure 3 shows measurement results when $A$ implements a momentum measurement and $B$ implements a position measurement. There is roughly the same detection probability for all detector combinations, which shows that there is no correlation between the detection positions.

In order to use polarization entanglement along with po-
Simultaneous Observation of Correlations in bars

...indicating that the polarization correlations are nonclassical with visibilities ranging from 82% to 92% were observed, measurement systems were the same. Interference curves... configurations. Having established adequate position and momentum detection systems, we then performed polarization interference measurements in order to confirm that polarization-momentum correlations to establish a random key-scheme.

Experimental results for position-momentum measurements. Also shown is a diagram of the measurement scheme.

Polarization correlation measurements for the case where A measures position and B measures momentum, while A measures momentum, and B measures position. The insets in Figs. 4 and 5 show polarization interference curves. All experimental results show that polarization correlations can be observed in parallel to position-momentum correlations. It is thus possible to use these DOF to implement QKD protocols.

Let us briefly analyze some possible protocols which could be implemented with position-momentum and polarization. One first possibility is to run two parallel and independent BBM protocols; one using polarization entanglement and the other using position-momentum correlations. Since the two protocols are independent, Alice and Bob choose randomly between polarization bases as well as position and momentum bases. In this case, an average transmission rate of one bit per photon pair is achieved, since 1/4 of the time they choose the same basis in both DOF and establish 2 bits, 1/2 of the time they choose the same basis in only one DOF and establish 1 bit, and 1/4 of the time they choose different bases in both DOF. The error rate due to intercept-resend eavesdropping is the same as a single BBM protocol: 1/4.

A second possibility is encoding in qu-quarts instead of qubits. A four-dimensional alphabet can be defined using position-momentum and polarization. For instance, let us define \( a = H, X_1 \), which stands for one photon with linear polarization \( H \) at position \( X_1 \), \( b = H, X_2 \), \( c = V, X_1 \), and \( d = V, X_2 \). A complementary alphabet would be: \( \alpha = +, P_1 \).
which stands for one photon with linear polarization $+45^\circ$ and momentum $P_1$, $\beta = +P_2$, $\gamma = -P_1$ and $\delta = -P_2$. Alice and Bob then both choose between two sets of measurements: The roman letter basis, consisting of $H/V$ polarization and $X$ measurements, or the greek letter basis, comprised of $+/-$ polarization and $P$ measurements. Here, the transmission rate is again 1 bit per photon pair, since 1/2 of the time they choose the same basis and establish two random bits, while the other 1/2 of the time they choose different bases and establish no random bits. In addition to the increase in the transmission rate, the error rate due to intercept-resend eavesdropping would be improved from 1/4 to 3/8, since Eve chooses the wrong basis with probability 1/2 and consequently has a 3/4 probability to send the wrong state.

A third possibility is for Alice and Bob to skew their combined measurements. For example, suppose Alice chooses between (i) $H/V$ polarization and $X$ measurements and (ii) $+/-$ polarization and $P$ measurements, while Bob chooses between (i) $H/V$ polarization and $P$ measurements and (ii) $+/-$ polarization and $X$ measurements. Skewing the measurement bases guarantees that Alice and Bob always agree on a basis in one DOF. This protocol is deterministic, in the sense that Alice and Bob establish one random bit for every photon pair sent, and thus every photon pair contributes to the sifted key.

We note that this last example is similar to a recent proposal for deterministic QKD where security is provided by AVN tests of local realism [22]. In the protocol proposed in Ref. [22], Alice and Bob choose randomly between three groups of measurements. Two of the measurement groups are analogous to the skewed basis above. It is possible to implement QKD based on AVN with polarization and position-momentum, however, our experimental results are not sufficient to demonstrate such a protocol. One measurement required is a single-photon Bell state measurement, which could be realized with linear optics [22]. The transmission rate QKD based on AVN is still one bit per photon pair. The error rate was not analyzed in Ref. [22], but we conjecture that it would be increased, since the three groups of measurements are analogous to three bases.

In summary, we have experimentally observed the simultaneous entanglement between polarization and position-momentum of photon pairs from parametric downconversion. Our results show that four-dimensional quantum key distribution can be implemented using these DOFs, enhancing the transmission rate and error rate induced by eavesdropping.

The authors would like to acknowledge fruitful discussions with L. Davidovich, K. Dechoun, R. L. de Matos Filho, D. Jonathan, A. Z. Khoury, and C. H. Monken. Financial support was provided by the Brazilian funding agencies CNPq, CAPES and FAPERJ and the Brazilian Millennium Institute for Quantum Information.