Quantum key distribution employing geometric rotating of the quantum polarisation of bright coherent light

Rubens Viana Ramos

Abstract — **Quantum polarisation is an important property that has extensively being used for quantum communication purposes. In this work, initially, the mixture of an unpolarised two-mode state and a two-mode pure state is analysed. Such mixture is controlled by a single parameter, the degree of purity. The quantum polarisation of the two-mode mixed state is discussed using quantum Stokes parameters. After, a quantum key distribution set-up using geometric rotating of the quantum polarisation of coherent light pulses is proposed and analysed using both pure and mixed states.**

Keywords — **Quantum polarisation, Stokes parameters, quantum key distribution.**

I. Introduction

Quantum polarisation is an important and useful property that permits the designing and implementation of protocols of quantum communication. The firsts quantum key distribution (QKD) set-ups were implemented using single-photon light polarisation [1-3]. The main problem in those set-ups was the hardness to keep the polarisation unchanged during channel propagation. More recently, long distance QKD using polarisation of bright coherent pulses was proposed and successfully implemented [4,5]. Such scheme has the advantage of reaching high bit rates, since single-photon pulses and detectors are not used. Basically, in the scheme using bright pulses the information is modulated in S_3 Stoke parameter, hence, it requires phase modulators. However, it is also possible to implement a similar QKD scheme where the information is carried in the S_1 and S_2 parameters. In this case, instead of phase modulators, polarisation rotators are used, since only linear polarisation states are employed. In this work, a set-up for QKD employing geometric rotating of bright coherent pulses is proposed. Initially the set-up is analysed using only pure states. In this case, the error rate depends only on the quantum uncertainty of the states. However, pure states are not easy to produce or maintain. Hence, a mixed polarised state is also analysed. The mixed state is a mixture of an unpolarised state and a pure state and the mixture is controlled by a unique parameter, the degree of purity. The effect of the use of the mixed state analysed in the QKD set-up is considered. Since the error probability depends also on the purity of the quantum states used, one can obtain a direct relationship between the error probability and the quantum purity degree of polarisation. This work is outlined as follow: In Section II, the main concepts of quantum polarisation used in this work are reviewed. In Section III, the mixture of two-mode unpolarised and pure states is introduced and analysed. In Section IV, the quantum key distribution set-up employing geometric rotating of bright coherent pulses is proposed and the use of the mixture of two-mode unpolarised and pure states in that system is studied. At last, in Section 5 the conclusions are presented.

II. Quantum Polarisation and Quantum Stokes Parameters

The most used mathematical tool when quantum polarisation is considered, is the quantum version of the Stokes parameters [6,7]:

$$\hat{S}_0 = \hat{a}_1^+\hat{a}_1 + \hat{a}_2^+\hat{a}_2 \quad (1)$$

$$\hat{S}_1 = \hat{a}_1^+\hat{a}_1 - \hat{a}_2^+\hat{a}_2 \quad (2)$$

$$\hat{S}_2 = \hat{a}_1^+\hat{a}_2 + \hat{a}_2^+\hat{a}_1 \quad (3)$$

$$\hat{S}_3 = i\left(\hat{a}_2^+\hat{a}_1 - \hat{a}_1^+\hat{a}_2\right) \quad (4)$$

$$\left[\hat{S}_2,\hat{S}_3\right] = i2\hat{S}_1 \quad (5)$$

Equation (5) and its cyclic versions imply that it is not possible to know, with total accuracy, any pair of Stokes parameters simultaneously. In order to apply a phase shift ϕ between two linearly polarised modes, the unitary operator $U_\phi = \exp\left(i0.5\phi\hat{S}_1\right)$ is used. When applied, for example, to two-mode coherent states, $\left|\alpha_x,\beta_y\right\rangle$, the output modes are $\left|\alpha e^{i\phi/2}{}_x,\beta e^{-i\phi/2}{}_y\right\rangle$. On the other hand, a geometric rotating of θ in the polarisation is achieved by the application of the unitary operator $U_\theta = \exp\left(i\theta\hat{S}_3\right)$. When applied, for example, to two-mode coherent states, $\left|\alpha_x,0_y\right\rangle$, the output modes are $\left|\alpha\cos(\theta)_x,\alpha\sin(\theta)_y\right\rangle$. For this linearly polarised light, the mean values and the variances of the Stokes parameters are:

$$\left\langle S_1\right\rangle = |\alpha|^2\cos(2\theta);\left\langle S_2\right\rangle = |\alpha|^2\sin(2\theta);\left\langle S_3\right\rangle = 0 \quad (6)$$

$$V_{S_1} = V_{S_2} = V_{S_3} = |\alpha|^2 \quad (7)$$

Hence, quantum polarisation cannot be represented by only a point on the Poincaré sphere. An interesting question is how good we can distinguish between two linear polarisation states having a dephasing of θ between them.

This work was supported by the Brazilian agency CNPq. Rubens Viana Ramos is with Dept. of Teleinformatic Engineering, UFC, Campus do Pici, bloco 710, C.P. 6007, 60455-760, Fortaleza. Email: rubens@deti.ufc.br.

This measure is given by the dot product and, without loss of generality, let us consider one of the polarisations the linear horizontal state. The dot product is then given by:

$$D = \left|\left\langle \alpha_x, 0_y \left| \exp\left(i\theta \hat{S}_3\right)\right| \alpha_x, 0_y \right\rangle\right|^2 = \exp\left(-2|\alpha|^2 \sin^2(\theta)\right) \quad (8)$$

$$0 \le D \le 1$$

So, D=0 implies perfectly distinguishable polarisation states, while D=1 implies indistinguishable states.

Classically, a light pulse is unpolarised if its Stokes parameters vanish. When considering quantum light, that condition (in average) is necessary but not sufficient. In fact, from a quantum optics point of view, a light beam can be considered unpolarised if its observable properties remain unchanged after an application of a geometric rotating and/or a phase shift between the two linearly polarised components. These conditions are mathematically described by [8]:

$$\left[\rho, \hat{S}_3\right] = \left[\rho, \hat{S}_1\right] = 0 \tag{9}$$

The most general form of an unpolarised state was given in [9,10]:

$$\rho = \sum_n p_n \frac{1}{n+1} \sum_{k=0}^{n} |k\rangle|n-k\rangle\langle k|\langle n-k| \tag{10}$$

where p_n is the probability distribution of the photon number considering both modes.

III. Mixture of Unpolarised and Pure Quantum Light States

Let us now consider the controlled mixture of unpolarised and pure states:

$$\rho(\xi) = \xi\rho^{(M)} + (1-\xi)\rho^{(P)}, \tag{11}$$

where $\rho^{(M)}$ represents the two-mode unpolarised state given in (10) and $\rho^{(P)}$ is any two-mode pure state. The parameter ξ controls the mixture and, hence, ξ is a kind of degree of purity. The state (10)-(11) is similar to the state introduced in reference [11], the differences are the mixed state used in the mixture and only single-mode states were considered there. If we consider single-photon pulses, (10)-(11) can be of the type:

$$\rho = \xi \frac{\left[|01\rangle\langle 01| + |10\rangle\langle 10|\right]_{xy}}{2} + (1-\xi)|\psi\rangle\langle\psi| \tag{12}$$

$$|\psi\rangle = \cos(\theta)|01\rangle_{xy} + e^{i\phi}\sin(\theta)|10\rangle_{xy} \tag{13}$$

that has a similar mathematical structure of a mixed qubit state. The application of a geometric rotating or phase shift between the modes in (11) produces the following state:

$$\begin{aligned} e^{i\hat{S}_m\theta}\rho(\xi)e^{-i\hat{S}_m\theta} &= \xi e^{i\hat{S}_m\theta}\rho^{(M)}e^{-i\hat{S}_m\theta} + \\ (1-\xi)e^{i\hat{S}_m\theta}\rho^{(P)}e^{-i\hat{S}_m\theta} &= \xi\rho^{(M)} + (1-\xi)e^{i\hat{S}_m\theta}\rho^{(P)}e^{-i\hat{S}_m\theta} \end{aligned} \tag{14}$$

since the application of a geometric rotating or phase shift does not change the unpolarised part. The Stokes parameters' average and variance of states (11) are given by [11]:

$$\left\langle S_i(\rho(\xi))\right\rangle = \xi\left\langle S_i\left(\rho^{(M)}\right)\right\rangle + (1-\xi)\left\langle S_i\left(\rho^{(P)}\right)\right\rangle \tag{15}$$

$$\begin{aligned} V_i(\rho(\xi)) = {} & \xi V_i\left(\rho^{(M)}\right) + (1-\xi)V_i\left(\rho^{(P)}\right) + \\ & \xi(1-\xi)\left[\left\langle S_i\left(\rho^{(M)}\right)\right\rangle - \left\langle S_i\left(\rho^{(P)}\right)\right\rangle\right]^2 \end{aligned} \tag{16}$$

where V_i is the variance given by $\left\langle S_i^2(\rho)\right\rangle - \left\langle S_i(\rho)\right\rangle^2$. Furthermore, $\left\langle S_i\left(\rho^{(M)}\right)\right\rangle = 0$ and $V_i\left(\rho^{(M)}\right) = \left\langle S_i^2\left(\rho^{(M)}\right)\right\rangle = .$ $\left(\left\langle n^2\right\rangle + 2\langle n\rangle\right)/3$. Since $V_i\left(\rho^{(M)}\right) \ge V_i\left(\rho^{(P)}\right)$, the minimal value of the variance $V_i(\rho(\xi))$ is obtained when ξ=0. Hence, the presence of the unpolarised part increases the uncertainty of the Stokes parameters and the polarisation becomes less defined.

IV. Quantum Key Distribution Using Two-Mode Coherent States and Polarisation Rotation

Quantum key distribution set-ups using single-photon pulses, in 1550 nm telecommunication window and for long distances, up to the moment, have presented a quite low effective data transmission rate. Aiming to overcome this problem, a different set-up employing the polarisation of multiphoton pulses was proposed [4,5]. In this scheme, the information is modulated in the Stokes' parameter S_3. For the optical set-up proposed here, and shown in Fig. 1, the information is modulated in the Stokes' parameters S_1 and S_2.

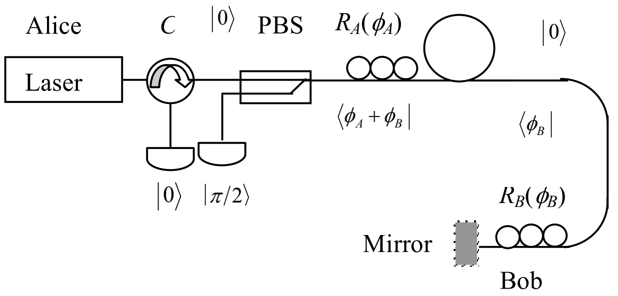

Fig. 1 – Optical set-up for QKD employing multi-photon pulses.

In Fig. 1, C is a circulator, PBS is a polarisation beam splitter and R_A and R_B are polarisation rotators. The functioning of the QKD set-up shown in Fig. 2 is as follows: The transmitter, Alice, produces a bright coherent pulse with polarisation $|0\rangle$ ($|\alpha_x,0_y\rangle \Rightarrow \langle S_1\rangle=|\alpha|^2$ and $\langle S_2\rangle=\langle S_3\rangle=0$). This pulse is sent to the receiver, Bob. At this last, a geometric rotating of ϕ_B is applied and the optical pulse, having now polarisation $|\phi_B\rangle$ ($|\alpha_x\cos(\phi_B),\alpha_x\sin(\phi_B)_y\rangle \Rightarrow \langle S_1\rangle=|\alpha|^2\cos(2\phi_B)$ and $\langle S_2\rangle=|\alpha|^2\sin(2\phi_B)$ and $\langle S_3\rangle=0$) is reflected back to Alice by the mirror. When the optical pulse arrives at Alice's place, it suffers a second geometric rotating of ϕ_A and, according to its final polarisation $|\phi_B+\phi_A\rangle$ ($|\alpha_x\cos(\phi_B+\phi_A),\alpha_x\sin(\phi_B+\phi_A)_y\rangle \Rightarrow \langle S_1\rangle=|\alpha|^2\cos(2(\phi_B+\phi_A))$ and $\langle S_2\rangle=|\alpha|^2\sin(2(\phi_B+\phi_A))$ and $\langle S_3\rangle=0$), the pulse will be, or not be, split by the polarisation beam splitter (PBS), that resolves its input pulse in the polarisations linear horizontal $|0\rangle$ and vertical $|\pi/2\rangle$. The set of possible values of ϕ_A and ϕ_B is $k\pi/2+j\delta$, where $\delta=(\pi/2)/\mathrm{W}$, where W, an odd number, is the number of words of the code. Besides that, $j\in\{0, 1, 2,\ldots, \mathrm{W}-1\}$, $k = 0$ for Alice and $k = 0$ or 1 for Bob. Two extra codification are used:

$$C_1 = \begin{cases} j\text{ even} \Rightarrow \left|\alpha\cos(j\delta)_x, \alpha\sin(j\delta)_y\right\rangle \Rightarrow \text{bit } 0 \\ j\text{ even} \Rightarrow \left|\alpha\cos(0.5\pi + j\delta)_x, \alpha\sin(0.5\pi + j\delta)_y\right\rangle \Rightarrow \text{bit } 1 . \end{cases}$$

$$C_2 = \begin{cases} j\text{ odd} \Rightarrow \left|\alpha\cos(j\delta)_x, \alpha\sin(j\delta)_y\right\rangle \Rightarrow \text{bit } 1 \\ j\text{ odd} \Rightarrow \left|\alpha\cos(0.5\pi + j\delta)_x, \alpha\sin(0.5\pi + j\delta)_y\right\rangle \Rightarrow \text{bit } 0 \end{cases}$$

The codification C_1 and C_2 can be seen in Fig. 2.

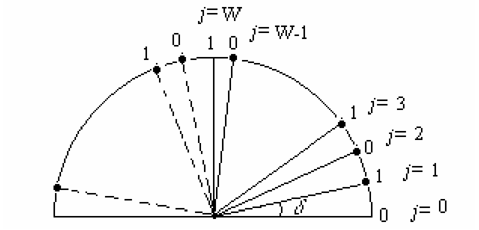

Fig. 2. Codification C_1 and C_2 for the protocol of quantum key distribution.

Hence, in order to implement an understandable communication between Alice and Bob, both of them must know in advance which values of polarisation rotation (j's value) they must apply in each optical pulse and which coding is being used for each particular pulse, C_1 or C_2. These information are provided in advance for both users [4,5], that is, Alice and Bob must share in advance a bit sequence that will indicate j value and C code used for each pulse sent. Further, as can be seen in Fig. 2, the bits are encoded such that neighbours polarisation states represent different bits. If the eavesdropper tries to identify the polarisation state sent by Alice measuring the photon number in both modes, the independence of the photon number distribution of both modes guarantees the security [4,5]. In fact, the security of the system is based on (8), where δ must be low enough in order to make D close to1. A brute force attack is also possible. Since the optical pulse is assumed to have too many photons, Eve can split it in 2W+1 parts (the number of different possible values for the polarisation angle ϕ_B and one more that Eve amplifies and sends to Alice) and she uses the same apparatus used by Alice, for each split part, applying a different value for ϕ_A in each of them. If Eve has perfect detectors, the following cases are possible:

1) Eve has detection in both detectors. In this case she knows that the phase applied is wrong.
2) Eve has no detection at all. In this case she does not gain any information.
3) Eve has detection in only one detector. In this case there are two possibilities:
   3.1) The polarisation angle applied is correct.
   3.2) The polarisation angle applied is wrong but one of the modes arriving at the photodetectors has zero photons.

If the optical pulse sent by Alice has a photon number much larger than the number of words (number of different phases) of the code used by Alice and Bob, Eve will, with high probability, get the correct phase applied by Alice. However, since it is assumed that Eve does not know which codification is being used, C_1 or C_2, she will not obtain any useful information.

Let us now suppose that Alice is not able to produce pure states, but she can produce mixed states of the type given in (14). So the question that arises is: How much error will be introduced for Eve and Bob? If instead of pure two-mode coherent states, two-mode mixed states are used, then, one the following states will arrive at the Alice's PBS input, depending on the previous shared bit sequence:

$$\rho(\xi) = \xi\left[\sum_n p_n\left(\frac{1}{n+1}\right)\sum_{k=0}^{n}\left|k_x,(n-k)_y\right\rangle\left\langle k_x,(n-k)_y\right|\right] + (1-\xi)\begin{cases}\left(\left|\alpha_x,0_y\right\rangle\left\langle\alpha_x,0_y\right|\right) \\ \left(\left|0_x,\alpha_y\right\rangle\left\langle 0_x,\alpha_y\right|\right)\end{cases} \quad (17)$$

since, according to (14), the mixed part and the degree of purity are not affected by the local unitary operations realised during the pulse propagation from Alice to Bob and back to Alice. From (17), where it should have vacuum state there is, according to the previous shared bit sequence, one of the states:

$$\rho_x(\xi) = \xi\left[\sum_n p_n\left(\frac{1}{n+1}\right)\sum_{k=0}^{n}\left|k_x\right\rangle\left\langle {}_x k\right|\right] + (1-\xi)\left|0_x\right\rangle\left\langle 0_x\right| \quad (18)$$

$$\rho_y(\xi) = \xi\left[\sum_n p_n\left(\frac{1}{n+1}\right)\sum_{k=0}^{n}\left|(n-k)_y\right\rangle\left\langle (n-k)_y\right|\right] + (1-\xi)\left|0_y\right\rangle\left\langle 0_y\right| \quad (19)$$

Hence, the presence of the mixed part introduces, for Alice using ideal detectors, an error rate (probability of having one or more photons in the mode) given by:

$$E = \xi\left(1 - \sum_n \frac{p_n}{n+1}\right) \tag{20}$$

Obviously, if p_0=1 and p_i=0 $\forall\ i \neq 0$, the error rate vanishes.

V. Conclusions

The quantum polarisation of a mixture of an unpolarised two-mode state and a two-mode pure state was analysed using quantum Stokes parameters. Such mixture is controlled by a single parameter, the degree of purity. It was demonstrated that the introduction of the unpolarised part makes the total state less polarised. After, a quantum key distribution set-up employing geometric rotating of polarisation of a bright coherent light was proposed. The set-up was described using pure and mixed states. In this last case, a relation between the error rate and the degree of purity of the mixed states used was found.

References

[1] J. Breguet, A. Muller e N. Gisin, "Quantum cryptography with polarized photons in optical fibres: Experimental and Practical limits", *J. of Mod. Opt.*, 41, 12, pp. 2405-2412, 1994.

[2] J. Breguet, A. Muller e N. Gisin, "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km", *Europhys. Lett.*, 23, pp. 383-388, 1993.

[3] J. D. Frasson e H. Ilves, "Quantum cryptography using optical fibers", *Appl. Opt.*, 33, 14, pp. 2949-2954, 1994.

[4] E. Corndorf, P. Kumar, C. Liang, G. A. Barbosa, and H. P. Yuen, Efficient quantum cryptography with coherent-state light in optical fibers at Gbps rates, Report Northwestern University, EUA, 2004.

[5] G. A. Barbosa, E. Corndorf, P. Kumar and H. P. Yuen, "Secure communication using mesoscopic coherent states", *Phys. Rev. Lett.*, 90, 227901, 2003.

[6] Robson, B. A., 1974, *The Theory of Polarisation Phenomena*, Claredon Press, Oxford.

[7] P. Usachev, J. Söderholm, G. Björk and A. Trifonov, "Experimental verification of differences between classical and quantum polarisation properties", *Opt. Commun.*, 193, pp. 161-173, 2001.

[8] G. S. Agarwal, J. Lehner and H. Paul, 1996, "Invariances for states of light and their quasi-distributions", *Opt. Commun.*, 129, 369, 1996.

[9] H. Prakash and N. Chandra, "Density operator of unpolarised radiation", *Phys. Rev. A*, **4**, 796, 1971.

[10] J. Lehner, U. Leonhardt and H. Paul, Unpolarized light: Classical and quantum states", *Phys. Rev. A*, **53**, 2727, 1996.

[11] B. Baseia, A. R. Gomes, and V. S. Bagnato, "Intermediate pure mixed states of the quantized radiation field", *Brazilian J. of Phys.*, 27, 276, 1997.