Quantum Information and Computation, Vol. 17, No. 15&16 (2017) 1277–1291

QUANTUM COMMUNICATION WITH CONTINUUM SINGLE-PHOTON, TWO-PHOTON AND COHERENT STATES

F. FRANKLIN S. RIOS[a]
Department of Teleinformatic Engineering, Federal University of Ceará - DETI/UFC, C.P. 6007 Campus do Pici Fortaleza, Ceará - 60455-970, Brazil.

A. GEOVAN DE A. H. GUERRA[b]
Quantum Information Group, Lab. of Quantum Information Technology, C.P. 6007 Campus do Pici Fortaleza, Ceará - 60455-970, Brazil.

R. VIANA RAMOS[c]
Quantum Information Group, Lab. of Quantum Information Technology, C.P. 6007 Campus do Pici Fortaleza, Ceará - 60455-970, Brazil.

Received August 16, 2016
Revised September 28, 2017

In this work, we analyze the behavior of continuum single-photon, two-photon and coherent states in some quantum communication schemes. In particular, we consider the single-photon in a Mach-Zenhder interferometer, the Hong-Ou-Mandel interference, the quantum bit commitment protocol and a new protocol for secure transmission of sampled analog signals. Furthermore, it is shown an equation for estimating the spectral distribution of the single-photon produced by a heralded single-photon source using four-wave mixing in an optical fiber.

Keywords: Continuum light states, Two-photon interference and Quantum bit commitment
Communicated by: I Cirac & G Milburn

1 Introduction

Since the beginning of the quantum information era several quantum tasks using single-photon, entangled two-photon and coherent states have been proposed. For example, the single-photon interference is a crucial tool for experimental realization of quantum communication, quantum computation and quantum metrology schemes. Teleportation requires two-photon entangled states while several quantum key distribution setups use weak coherent states. However, in general, their descriptions are based on single-frequency optical pulses. Usually, the single-photon interference is analyzed as if the photons were produced by a single-frequency optical source, their propagation in optical fibers was free of dispersive effects and the behavior of the optical devices, like beam splitters, polarization rotators and phase modulators, were not frequency-dependent. These are, obviously, simplifications of

[a]frfranklin.rios@gmail.com
[b]geovanguerra@gmail.com
[c]rubens.viana@pq.cnpq.br

the real situation. A single-frequency source would violate the Heisenberg uncertainty principle and, hence, it does not exist. Moreover, optical devices are made of glass and the refractive index is frequency dependent. For example, the photon propagation in dispersive optical fibers results in an additional phase term of the type ($\beta L + 1/2\beta_2\omega^2 L$-$1/6\beta_3\omega^3 L$) [1] where β is the constant of propagation, β_2 is the group velocity dispersion (GVD), β_3 is the third order dispersion (usually considered when $\beta_2 \sim 0$) and L is the fiber's length propagated. Furthermore, real beam splitters, polarization rotators and phase modulators are frequency-dependent devices. Hence, a more realistic analysis of quantum communication schemes requires the consideration of continuum fields [2]. In this direction, the present work discusses the use of continuum optical fields in some quantum optical setups and quantum communication protocols. In particular, the spectral distribution of single-photons produced by a heralded single-photon source using four-wave mixing in optical fibers is analyzed and an optical setup for secure transmission of sampled analog states is presented, as well we discuss the security of quantum bit commitment when continuum entangled two-photon states are used. This work is outlined as follows: In Section 2 the discretization of the continuum single-photon state is reviewed. Following, the single-photon interference, the two-photon interference (HOM experiment) and the single-photon propagation in a birefringent channel are discussed. In Section 3 the discussion of the spectral width of the single-photons produced by four-wave mixing in optical fibers is presented. In Section 4 the security of quantum bit commitment protocol using continuum two-photon entangled states is considered. In Section 5, an optical setup for secure transmission of sampled analog signals is described and the conclusions are drawn in Section 6.

2 Quantum communication with continuum single-photon state

In this section, we consider the effect of the spectral width of single-photons in three situations: single-photon interference, interference between two single-photons coming from different sources (Hong-Ou-Mandel experiment) and single-photon propagation in a birefringent channel. The single-photon continuum state is given by [2]

$$|1_\omega\rangle = \int_0^\infty \sigma(\omega)\hat{a}^+(\omega)d\omega\,|0_\omega\rangle \tag{1}$$

$$\int_0^\infty |\sigma(\omega)|^2\, d\omega = 1 \tag{2}$$

The state $|0_\omega\rangle$ is the continuum vacuum state and, hence, $\hat{a}(\omega)\,|0_\omega\rangle = 0$, where $\hat{a}(\omega)$ is the continuum annihilation operator. Furthermore, $|\sigma(\omega)|^2$ gives the probability of the frequency of the photon to belong to the interval $(\omega, \omega + d\omega)$. In order to work with the continuum single-photon in quantum communication schemes, we firstly make its discretization. Let us start by writing $\sigma(\omega)$ in the basis of sinc functions (the discretization using the sinc functions makes easier the calculation of the important probabilities considered in the error rate and security analysis) [3]:

$$\sigma(\omega) = \sum_{k=-\infty}^{\infty} \sigma(k\omega_s)\mathrm{sinc}[(\omega - k\omega_s)/\omega_s] \tag{3}$$

$$\mathrm{sinc}(x) = \sin(\pi x)/\pi x \tag{4}$$

In (3) ω_s is the step of discretization in the frequency domain. Thus, $\sigma(k\omega_s)$ is the value of $\sigma(\omega)$ in $\omega = k\omega_s$ where k is an integer number. Using the orthogonality of the sinc function,

$$\frac{1}{\omega_s}\int_{-\infty}^{\infty} \text{sinc}\left[\frac{(\omega - k\omega_s)}{\omega_s}\right] \text{sinc}\left[\frac{(\omega - m\omega_s)}{\omega_s}\right] d\omega = \delta_{km} \tag{5}$$

and the fact that $\sigma(\omega)$ zero for negative frequencies, one has that

$$\int_0^{\infty} |\sigma(\omega)|^2 \, d\omega = \int_{-\infty}^{\infty} |\sigma(\omega)|^2 \, d\omega = \sum_{k=1}^{\infty} |\sigma(k\omega_s)|^2 \, \omega_s = 1 \tag{6}$$

Equation (6) shows us how to make discrete the continuum single-photon state:

$$|1_\omega\rangle = \sum_{k=1}^{\infty} \sigma(k\omega_s)\sqrt{\omega_s}\, |0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots \tag{7}$$

According to (7), the continuum single-photon state can be approximated by a superposition of the tensor product of discrete oscillators. Each discrete oscillator works in a single-frequency. For example, the state $|0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots$ means one photon in the frequency $k\omega_s$ and zero photons in the other frequencies. The number of discrete oscillators is equal to the number of samples of $\sigma(\omega)$ and the amplitude of probability of k-th term in the superposition is given by $\sigma(k\omega_s)(\omega_s)^{1/2}$. Now, if $\sigma(\omega)$ vanishes for $\omega > N\omega_s$, then one has just a finite number of oscillators:

$$|1_\omega\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\, |\tilde{1}\rangle_k \tag{8}$$

$$|\tilde{1}\rangle_k = |0\rangle_1 \otimes \cdots \otimes |1\rangle_k \otimes \cdots \otimes |0\rangle_N \tag{9}$$

Now, in order to study the single-photon interference, we will consider the behavior of the quantum state given in (8) in a Mach-Zehnder interferometer (MZI) whose phase modulators are frequency-dependent (to include the frequency dependence of the beam splitters is just an algebra exercise). The MZI is composed by two lossless beam-splitters having transmittance $T = 1/2^{1/2}$(and reflectance $R = i1/2^{1/2}$), and one phase modulator in each arm, $\phi_A(\omega)$ and $\phi_B(\omega)$. Such interferometer is useful in quantum key distribution (QKD) setups. The input state is $|\, 1_\omega\rangle \,|\, 0_\omega\rangle$. The scheme is shown in Fig.1.

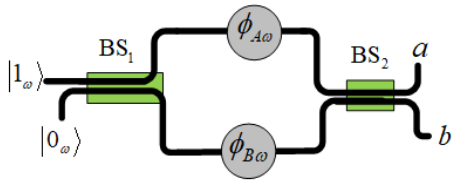

Fig. 1. Mach-Zehnder interferometer with lossless balanced beam splitters and frequency-dependent phase modulators ($\phi_{A\omega} \rightarrow \phi_A(\omega)$,$\phi_{B\omega} \rightarrow \phi_B(\omega)$).

After some algebra one gets the following total quantum state at the interferometer output

$$|\psi_\omega\rangle = \sum_{k=1}^{N} \sigma\left(k\omega_s\right)\sqrt{\omega_s}|0\rangle_1|0\rangle_1 \otimes ... \otimes |\xi_\omega\rangle_k \otimes ... \otimes |0\rangle_N|0\rangle_N \tag{10}$$

$$|\xi_\omega\rangle_k = ie^{i\Omega_k}\left\{\cos\left(\Delta_k\right)|1\rangle_k^a|0\rangle_k^b + \sin\left(\Delta_k\right)|0\rangle_k^a|1\rangle_k^b\right\} \tag{11}$$

$$\Omega_k = \left[\phi_A\left(k\omega_s\right) + \phi_B\left(k\omega_s\right)\right]/2;\ \Delta_k = \left[\phi_A\left(k\omega_s\right) - \phi_B\left(k\omega_s\right)\right]/2. \tag{12}$$

Hence, the probabilities of the photon to emerge at the outputs a and b of the interferometer are given by

$$p_a = \sum_{k=1}^{N} \cos^2\left[\frac{\phi_A(k\omega_s)-\phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2\omega_s \tag{13}$$

$$p_b = \sum_{k=1}^{N} \sin^2\left[\frac{\phi_A(k\omega_s)-\phi_B(k\omega_s)}{2}\right]\left|\sigma\left(k\omega_s\right)\right|^2\omega_s \tag{14}$$

or, returning to the continuous case,

$$p_a = \int_0^\infty \cos^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega \tag{15}$$

$$p_b = \int_0^\infty \sin^2\left[\frac{\phi_A(\omega)-\phi_B(\omega)}{2}\right]\left|\sigma\left(\omega\right)\right|^2 d\omega. \tag{16}$$

Observing (15)-(16) one sees that the frequency-dependence can increase the error rate of a QKD protocol (this error can be taken into account through the visibility of the interferometer) or it can be designedly used to increase the security of a quantum cryptographic protocol.

Now, let us consider the HOM experiment, the interference between two continuum single-photon pulses, coming from different single-photon sources, impinging in a beam splitter at the same time and with the same polarization. The total state at the beam splitter's output is

$$[U_{BS}|1_\omega\rangle|1_\omega\rangle = U_{BS}\left(\sum_{k=1}^{N}\sigma\left(k\omega_s\right)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k\right)\otimes\left(\sum_{l=1}^{N}\xi\left(l\omega_s\right)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_l\right) = \sum_{k,l=1}^{N}\sigma\left(k\omega_s\right)\xi\left(l\omega_s\right)\omega_s U_{BS}\left|\tilde{1}\right\rangle_k\left|\tilde{1}\right\rangle_l \tag{17}$$

In (17) $U_{BS}(\omega)$ is the unitary operation of the frequency-dependent beam splitter. Its transmittance and reflectance are, respectively, $\cos(\theta(\omega))$ and $i\sin(\theta(\omega))$. Thus,

$$U_{BS}\left|\tilde{1}\right\rangle_k\left|\tilde{1}\right\rangle_l = \begin{cases} |0\rangle_1^a|0\rangle_1^b \otimes ... \otimes |\mu\rangle_k \otimes ... \otimes |\mu\rangle_l \otimes ... \otimes |0\rangle_N^a|0\rangle_N^b & \text{if } k \neq l \\ |0\rangle_1^a|0\rangle_1^b \otimes ... \otimes |\lambda\rangle_k \otimes ... \otimes |0\rangle_N^a|0\rangle_N^b & \text{if } k = l \end{cases} \tag{18}$$

$$|\mu\rangle_{r=k,l} = \cos\left(\theta\left(r\omega_s\right)\right)|1\rangle_r^a|0\rangle_r^b + i\sin\left(\theta\left(r\omega_s\right)\right)|0\rangle_r^a|1\rangle_r^b \tag{19}$$

$$|\lambda\rangle_k = \sin\left(2\theta\left(k\omega_s\right)\right)\frac{|2\rangle_k^a|0\rangle_k^b + |0\rangle_k^a|2\rangle_k^b}{\sqrt{2}} + i\cos\left(2\theta\left(k\omega_s\right)\right)|1\rangle_k^a|1\rangle_k^b \tag{20}$$

In (18)-(20) a and b are the beam splitter's output modes. Using (17)-(20), one gets the coincidence probability

$$p_{coin} = \sum_{\substack{k,l=1 \\ k\neq l}}^{N} \left|\sigma\left(k\omega_s\right)\xi\left(l\omega_s\right)\right|^2\omega_s^2\left[\cos^2\left(\theta\left(k\omega_s\right)\right)\cos^2\left(\theta\left(l\omega_s\right)\right) + \sin^2\left(\theta\left(k\omega_s\right)\right)\sin^2\left(\theta\left(l\omega_s\right)\right)\right]$$
$$+\sum_{k=1}^{N}\left|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)\right|^2\omega_s^2\cos^2\left(2\theta\left(k\omega_s\right)\right) \tag{21}$$

If the beam splitter is not frequency-dependent and balanced ($\theta = \pi/4$) (21) reduces to

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\sum_{k=1}^{N}\left|\sigma\left(k\omega_s\right)\xi\left(k\omega_s\right)\right|^2\omega_s^2 \tag{22}$$

or, returning to the continuous case,

$$p_{coin} = \frac{1}{2} - \frac{1}{2}\int\int_D \left|\sigma\left(\omega_1\right)\right|^2\left|\xi\left(\omega_2\right)\right|^2 d\omega_1 d\omega_2 \tag{23}$$

where $D = \{(\omega_1,\omega_2) \in \mathrm{R}^2{}_{\geq 0} : \omega_1 = \omega_2\}$. As one may note in (22)-(23), the coincidence probability will be zero only when the spectral distributions are $\sigma(\omega) = \xi(\omega) = \delta(\omega\text{-}\omega_0)$, that is, both photons having the same single-frequency ω_0 (and zero spectral width). This happens because, due to the spectral distribution, one cannot guarantee that both photons will be in the same frequency, even if they have the same spectral distributions. On the other hand, the coincidence probability is equal to 1/2 only when the spectral distributions of the photons do not have any overlap. However, in practice, if frequency information cannot be gained by the detectors used in the experiment, that is, if the detectors' bandwidth is wider than photons spectral distribution, then photons with different frequencies become indistinguishable and a perfect Hong-Ou-Mandel interference can be achieved.

At last, we consider the continuum single-photon light propagating in a frequency-dependent phase-damping channel as discussed in [4, 5]. Initially, at the channel's input, the quantum state is

$$|\psi\rangle = |1_\omega\rangle \otimes (a|H\rangle + b|V\rangle) = \sum_{k=1}^{N}\sigma\left(k\omega_s\right)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k \otimes (a|H\rangle + b|V\rangle) \tag{24}$$

Therefore, for the initial state frequency and polarization are not entangled. The channel's propagation effect is modeled by the unitary operator $U(\omega) = \lambda_H(\omega)|H\rangle\langle H| + \lambda_V(\omega)|V\rangle\langle V|$ (H

and V mean, respectively, horizontal and vertical modes, the eigenvalues depend on the frequency while the eigenstates are constant). Hence, the state at channel's output is

$$|\psi_{out}\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k U(a|H\rangle + b|V\rangle) = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}\left|\tilde{1}\right\rangle_k (a\lambda_H(k\omega_s)|H\rangle + b\lambda_V(k\omega_s)|V\rangle) \quad (25)$$

$$\rho = |\psi_{out}\rangle\langle\psi_{out}| = \sum_{k,l=1}^{N} \sigma(k\omega_s)\sigma^*(l\omega_s)\omega_s\left|\tilde{1}\right\rangle_{kl}\langle\tilde{1}| \otimes \begin{pmatrix} |a|^2 \lambda_H(k\omega_s)(\lambda_H(l\omega_s))^* |H\rangle\langle H| \\ +|b|^2 \lambda_V(k\omega_s)(\lambda_V(l\omega_s))^* |V\rangle\langle V| \\ +ab^*\lambda_H(k\omega_s)(\lambda_V(l\omega_s))^* |H\rangle\langle V| \\ +a^*b(\lambda_H(l\omega_s))^* \lambda_V(k\omega_s)|V\rangle\langle H| \end{pmatrix} \quad (26)$$

In order to get only the polarization information, the frequency variable is traced out in (26). Using $Tr_\omega\left(\left|\tilde{1}\right\rangle_{kl}\langle\tilde{1}|\right) = {}_l\langle\tilde{1} \mid \tilde{1}\rangle_k = \delta_{kl}$ and (6) one gets for the final output state

$$\rho = \begin{bmatrix} |a|^2 & ab^* \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \lambda_H(k\omega_s)(\lambda_V(k\omega_s))^* \\ a^*b \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s (\lambda_H(k\omega_s))^* \lambda_V(k\omega_s) & |b|^2 \end{bmatrix} \quad (27)$$

For this birefringent channel, one has eigenvalues of the form

$$\lambda_{H,V}(k\omega_s) = e^{i\left(\frac{n_{H,V}k\omega_s L}{c}\right)}, \quad (28)$$

where $n_{H,V}$ are the refractive index in the orthogonal directions, c is the light velocity and L is the channel's length. The fidelity between the input and output state is given by

$$F = \langle\psi|\rho|\psi\rangle = |a|^4 + |b|^4 + 2|a|^2|b|^2 \sum_{k=1}^{N} |\sigma(k\omega_s)|^2 \omega_s \cos\left(\frac{n_H - n_V}{c} k\omega_s L\right) \quad (29)$$

or, returning to the continuous case,

$$F = |a|^4 + |b|^4 + 2|a|^2|b|^2 \int_0^\infty |\sigma(\omega)|^2 \cos\left(\frac{n_H - n_V}{c}\omega L\right) d\omega. \quad (30)$$

As expected, if the medium is not birefringent, $n_H = n_V$, then $F = 1$. In order to gain some physical insight, let us consider the simple case of a rectangular spectrum with width $\Delta\omega$ and centered in the frequency ω_0: $\sigma(\omega) = \sigma_0$in the interval [$\omega_0$ - $\Delta\omega/2$, ω_0 + $\Delta\omega/2$] and zero otherwise. In this case, the fidelity is simply given by

$$F = |a|^4 + |b|^4 + 2|a|^2|b|^2 \frac{2c}{(n_H - n_V)L} \sin\left(\frac{(n_H - n_V)L}{c}\frac{\Delta\omega}{2}\right) \cos\left(\frac{(n_H - n_V)L}{c}\omega_0\right). \quad (31)$$

One may note that, if $|\psi\rangle = (|H\rangle + |V\rangle)/2^{1/2}$, then F =1/2 when $L = 2c\pi/[(n_H - n_V)\Delta\omega]$. As expected, the shorter the spectral width the longer the photon can travel. In Fig. 2 one can see the variation of F versus L for an input state with a Gaussian spectrum having ω_0= $8.3.10^{14}$ [rad/s] (λ = 1550 nm) and $\Delta\omega = 1.33.10^{10}$ [rad/s]. The other parameters values are $n_H = 1.46$, $n_V = 1.465$.

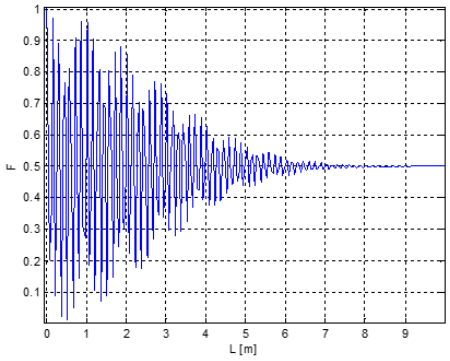

Fig. 2. Fidelity given by Eq. (31) versus channel's length L. Input state $(|H\rangle + |V\rangle)/2^{1/2}$ and Gaussian spectrum.

As one can notice in Fig. 2 the birefringence is very harmful for quantum states that are superposition of $|H\rangle$ and $|V\rangle$. On the other hand, since the channel considered is a phase damping channel, the input states $|H\rangle$ and $|V\rangle$ do not suffer any kind of perturbation ($F = 1$).

3 Spectral distribution of a single-photon produced by a four-wave mixing-based two-photon Source

The two-photon states are mostly produced by parametric down conversion and spontaneous or stimulated four-wave mixing in optical fibers. Thus, the frequencies of the created photons have to obey the energy conservation law. For the four-wave mixing, for example, two photons from the pump beam (ω_p) are annihilated while two new photons, named signal (ω_{sig}) and idler (ω_{id}), are created. The relation $2\omega_p$=ω_{sig}+ω_{id} must be obeyed. For this case, the signal and idler annihilation $(\hat{a}_s, \hat{a}_i)$ and creator $\left(\hat{a}_s^\dagger, \hat{a}_i^\dagger\right)$ operators are governed by the following coupled differential equations [1, 6]

$$\frac{d\hat{a}_s}{dz} = i\left(\delta/2\right)\hat{a}_s + 2i\gamma A_p^2 \hat{a}_i^\dagger \tag{32}$$

$$\frac{d\hat{a}_i}{dz} = i\left(\delta/2\right)\hat{a}_i + 2i\gamma A_p^2 \hat{a}_s^\dagger. \tag{33}$$

In (32)-(33), z is the spatial coordinate, γ is the fiber nonlinearity coefficient, A_P^2 is the pump power and δ is the phase mismatch given by

$$\delta = \beta\left(\omega_{sig}\right) + \beta\left(\omega_{id}\right) - 2\beta\left(\omega_p\right) + 2\gamma A_p^2. \tag{34}$$

The equations (32)-(33) do not take into account the spontaneous Raman scattering (SRS) [7]. In practice, the SRS is reduced by choosing ω_{sig}- ω_i far from $2\pi\cdot$13THz [8] or cooling the fiber in order to decrease the phonon population [9]. The solutions of (32)-(33) are [1, 6]

$$\hat{a}_s\left(z\right) = k_1 \hat{a}_s\left(0\right) + k_2 \hat{a}_i^\dagger\left(0\right) \tag{35}$$

$$\hat{a}_i(z) = k_1 \hat{a}_i(0) + k_2 \hat{a}_s^{\dagger}(0) \tag{36}$$

$$k_1 = \cosh(gz) + (i\delta/2g)\sinh(gz) \tag{37}$$

$$k_2 = i(\gamma/g) A_p^2 \sinh(gz) \tag{38}$$

$$g = \sqrt{\gamma^2 A_p^4 - \delta^2/4}. \tag{39}$$

The two-photon source, in practice, can produce multiphoton pulses. Hence, the quantum state produced is of the form $|\psi\rangle = \sum_n c_n |n,n\rangle$, having equal individual states $\rho = \sum_n |c_n|^2 |n\rangle\langle n|$. The photon number distribution of the signal and idler modes are equal to [10]

$$p_n = \frac{2}{(\Delta k_+ + 1)} \left[\frac{(\Delta k_+ - 1)}{(\Delta k_+ + 1)}\right]^n \tag{40}$$

$$\Delta k_+ = \left(|k_1|^2 + |k_2|^2\right) = \cosh^2(gz) + \left[\frac{\delta^2}{4g^2} + \frac{\gamma^2}{g^2} A_p^4\right] \sinh^2(gz). \tag{41}$$

Considering that the idler mode is detected by an ideal photon counter, the single-photon state at the signal mode (conditioned to single-photon detection in the idler mode and for a monochromatic pump field) is given by $\prod_a^b$

$$|1_\omega\rangle = \sum_{k=1}^{N} \sigma(k\omega_s)\sqrt{\omega_s}|\tilde{1}\rangle_k = \sum_{k=1}^{N} \left[\frac{p_1(k\omega_s)\prod_{\substack{l=1\\ l\neq k}}^{N} p_0(l\omega_s)}{\sum_{k=1}^{N} p_1(k\omega_s)\prod_{\substack{l=1\\ l\neq k}}^{N} p_0(l\omega_s)}\right]^{1/2} |\tilde{1}\rangle_k \tag{42}$$

$$N\omega_s = \omega_p - \omega_s \tag{43}$$

where, according to (40),

$$p_0(k\omega_s) = \frac{2}{(\Delta k_+ + 1)} \tag{44}$$

$$p_1(k\omega_s) = \frac{2}{(\Delta k_+ + 1)} \left[\frac{(\Delta k_+ - 1)}{(\Delta k_+ + 1)}\right]. \tag{45}$$

Furthermore, the phase mismatch is

$$\delta = \beta(k\omega_s) + \beta([2(N+1) - k]\omega_s) - 2\beta((N+1)\omega_s) + 2\gamma A_p^2. \tag{46}$$

According to (41)-(46), δ plays a crucial role in the spectral width of the single-photon state produced by a heralded single-photon source using four-wave mixing in optical fiber. Without knowing the formula of $\beta(\omega)$ is not possible to go beyond, however, one can clearly see that the optical power of the pump beam is important not only to keep small the amount of multiphoton pulses ($\gamma A_p^2 L_f << 1$), but it also has implications on the spectral width of the generated single-photon pulses: The variation of A_p^2 makes a variation in Δk_+ that, by its turn, changes p_0 and p_1 in (42).

4 Quantum bit commitment using continuum two-photon states

Now, let us consider the implications of continuum states in the quantum bit commitment (QBC) protocol. It has been shown that QBC protocols without any restriction cannot be unconditionally secure [11]. Attempts of producing unconditional QBC protocols with some restrictions have been proposed [12, 13]. Here, we consider the Lo-Chau's QBC protocol (LC-QBC) from a practical point of view, aiming to show that, at least in principle, Alice's cheating strategy may be noticed by Bob with a probability larger than zero. The practical conditions considered are: the entangled photons have a spectral distribution and the quantum gates are frequency-dependent. The LC-QBC protocol can be explained in the following way: Alice and Bob agree that the states $|0_L\rangle = (|00\rangle+|11\rangle)/2^{1/2}$ and $|1_L\rangle = (|01\rangle+|10\rangle)/2^{1/2}$ represent, respectively, the logical bits '0' and '1'. In the commitment stage, Alice prepares the state $|0_L\rangle$ and she sends the second qubit to Bob. In the unveil stage two situations are possible: 1) Alice decides to keep the choice '0'. She measures her qubit using the $\{|0\rangle,|1\rangle\}$ basis and informs to Bob the values of the bit committed ('0') and the result of her measurement. Bob, by his turn, measures his qubit in the same basis and compares the result with that one announced by Alice. If the results of the measurements are the same, Bob thinks that Alice acted honestly. 2) Alice changes her mind and decides to unveil the value '1'. She applies the NOT gate X and realizes a measurement in her qubit. Alice informs to Bob the values of the bit committed ('1') and the result of her measurement. Bob, by his turn, measures his qubit and compares the result with that one announced by Alice. If the measurement results are different, Bob thinks that Alice acted honestly. Since Alice can always change from '0' to '1' (by applying the X gate in her qubit) without being noticed, she can always cheat Bob with zero probability of being caught cheating. This scenario changes when we consider real entangled states whose photons have non-zero spectral width. Let us consider that Alice and Bob will run the LC-QBC protocol using the following entangled state

$$|0_L\rangle = \int_0^\infty d\Omega\sigma\left(\Omega\right)\frac{|\omega_0+\Omega,\omega_0-\Omega\rangle_{HH}+|\omega_0+\Omega,\omega_0-\Omega\rangle_{VV}}{\sqrt{2}}. \tag{47}$$

The discretization of the state (47) using (3)-6 is

$$|0_L\rangle = \sum_{\substack{k,l=1\\k+l=M}}^{N} \sigma\left(k\omega_s,l\omega_s\right)\sqrt{\omega_s}\left[\frac{\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H+\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V}{\sqrt{2}}\right]. \tag{48}$$

$$M\omega_s = 2\omega_0. \tag{49}$$

According to (48), with probability $|\sigma(k\omega_s,l\omega_s)|^2\omega_s$ the photons in the frequencies $k\omega_s$ and $l\omega_s$ ($k\omega_s + l\omega_s = M\omega_s = 2\omega_0$) are in the entangled state $(|HH\rangle+|VV\rangle)/2^{1/2}$. The NOT gate, by its turn, is a frequency-dependent polarization rotator. It is represented by $R[\theta(\omega)]$, where $\theta(\omega_c) = \pi/2$ in the central frequency ω_c. When Alice tries to cheat applying $R[\theta(\omega)]$, she produces the quantum state

$$R\left[\theta\left(\omega\right)\right]\left|0_L\right\rangle = \sum_{\substack{k,l=1 \\ k+l=M}}^{N} \sigma\left(k\omega_s, l\omega_s\right)\sqrt{\omega_s} \times \left[\begin{array}{l} \cos\left[\theta\left(k\omega_s\right)\right]\frac{\left(\left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^H - \left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}} \\ +\sin\left[\theta\left(k\omega_s\right)\right]\frac{\left(\left|\tilde{1}\right\rangle_k^V\left|\tilde{1}\right\rangle_l^H + \left|\tilde{1}\right\rangle_k^H\left|\tilde{1}\right\rangle_l^V\right)}{\sqrt{2}} \end{array}\right]. \quad (50)$$

An error in Bob denouncing Alice's cheating strategy will occur when Alice informs that she chose bit '1' and Bob gets in his measurement the same result as Alice got in her measurement. Using the state in (50) one gets the following error probability

$$PE = \sum_{\substack{k,l=1 \\ k+l=M}}^{N} \left|\sigma\left(k\omega_s, l\omega_s\right)\right|^2 \cos^2\left[\theta\left(k\omega_s\right)\right]\omega_s \quad (51)$$

or, returning to the continuum case,

$$PE = \int_0^\infty d\Omega \left|\sigma\left(\Omega\right)\right|^2 \cos^2\left[\theta\left(\omega_0+\Omega\right)\right]. \quad (52)$$

In (52) it is assumed that Alice (Bob) kept the photon with central frequency ω_0+Ω (ω_0-Ω). Hence, once one takes into account the spectral distribution and the frequency dependence of optical devices, one may note that Alice's strategy may cause an error in Bob, revealing her cheating strategy.

5 Quantum communication using continuum coherent states

Optical schemes for quantum secure direct communication using continuum coherent states have been proposed in [14]. In this section, we describe an optical setup for secure transmission of sampled analog signals using continuum coherent states. However, before describing the optical setup proposed, let us start by describing the continuum coherent state used. It is defined as [2]

$$\left|\alpha_\omega\right\rangle = \exp\left[\int\left[\alpha\left(\omega\right)a^\dagger\left(\omega\right) - \alpha^*\left(\omega\right)a\left(\omega\right)\right]d\omega\right]\left|0_\omega\right\rangle \quad (53)$$

$$\left\langle n\right\rangle = \int_0^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega. \quad (54)$$

In (54) $\langle n\rangle$ is the mean photon number of the state $|\alpha_\omega\rangle$, where $\alpha(\omega)$ is the complex amplitude of the field. Now, using (3)-(6) in the discretization of (53) one gets

$$\left|\alpha_\omega\right\rangle = \prod_{k=1}^{N}\left|\alpha\left(k\omega_s\right)\sqrt{\omega_s}\right\rangle. \quad (55)$$

$$\left\langle n\right\rangle = \int_0^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega = \int_{-\infty}^\infty \left|\alpha\left(\omega\right)\right|^2 d\omega = \sum_{k=1}^{N}\left|\alpha\left(k\omega_s\right)\right|^2\omega_s. \quad (56)$$

In (55)-(56) it is considered that $\alpha(\omega)$ vanishes for $\omega > N\omega_s$. Equation (55) shows that the continuum coherent state can be approximated by a tensor product of single-frequency discrete oscillators in coherent states [3]. Due to the decomposition in sinc functions, the number of discrete oscillators is equal to the number of samples taken from the field's envelope. Each discrete oscillator is in a (single-frequency) coherent state and the amplitude of the k-th oscillator is equal to the product of the k-th sample of $\alpha(\omega)$ and the square root of ω_s.

In a Mach-Zehnder interferometer with frequency-dependent phase modulators, the mean photon numbers at the interferometer's outputs are [14]

$$\langle n_1 \rangle = \sum_{k=1}^{N} |\alpha(k\omega_s)|^2 \cos^2\left(\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right)\omega_s \tag{57}$$

$$\langle n_2 \rangle = \sum_{k=1}^{N} |\alpha(k\omega_s)|^2 \sin^2\left(\frac{\phi_A(k\omega_s) - \phi_B(k\omega_s)}{2}\right)\omega_s \tag{58}$$

or, returning to the continuous case,

$$\langle n_1 \rangle = \int_0^{\infty} \cos^2\left[\tfrac{\phi_A(\omega)-\phi_B(\omega)}{2}\right] |\alpha(\omega)|^2 \, d\omega \tag{59}$$

$$\langle n_2 \rangle = \int_0^{\infty} \sin^2\left[\tfrac{\phi_A(\omega)-\phi_B(\omega)}{2}\right] |\alpha(\omega)|^2 \, d\omega. \tag{60}$$

The optical setup that implements the secure transmission of sampled analog signals scheme is shown in Fig. 3.

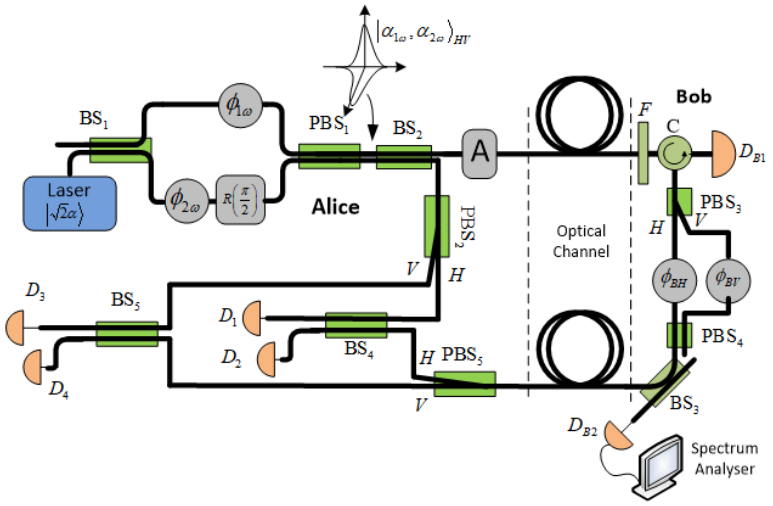

Fig. 3. Optical setup for secure transmission of sampled analog signals. BS – beam splitter, PBS – polarizing beam splitter, C – optical circulator, R – polarization rotator, F – optical filter, D – detector, A – optical attenuator, ϕ - phase modulator and ϕ_ω - frequency-dependent phase modulator.

In Fig. 3, $\phi_{1\omega}$ and $\phi_{2\omega}$ (ϕ_{BH} and ϕ_{BV}) are (not) frequency-dependent phase-modulators while A is an optical attenuator. The filter F avoids a spy (Eve) to use optical signals in a frequency range not seen by Bob's detectors. The circulator C and detector D_{B1} makes the setup one-directional. Light detected in D_{B1} implies the existence of an attack. At last, the set BS_3-D_{B2}-Spectrum analyzer works as a watch-dog avoiding Eve to send strong signals to Bob aiming to read them at the output [15, 16]. As it can be noted, the optical scheme in Fig. 3 uses the frequency-dependent phase modulation, only known by Alice, to hide Bob's phase-modulation. Since the pulse sent by Alice has low mean photon number, Eve cannot determine the functions $\phi_{1\omega}$ and $\phi_{2\omega}$. Considering the beam splitters obey the relation

$$U_{BS}|\xi,\lambda\rangle = \left|\frac{\xi+\lambda}{\sqrt{2}}, \frac{-\xi+\lambda}{\sqrt{2}}\right\rangle, \tag{61}$$

the equations that explain the functioning of the setup in Fig. 3 are the following: The quantum states at PBS_2's and at the channel's inputs are, respectively,

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_1 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{62}$$

$$\left|\alpha_2 e^{i\phi_1(\omega)}, \alpha_2 e^{i\phi_2(\omega)}\right\rangle_{HV} \tag{63}$$

$$\alpha_2 = \alpha_1 10^{-\frac{\varepsilon[dB]}{10}}. \tag{64}$$

In (64), ϵ (in dB) is the loss of the attenuator A. The total state at Bob' output is

$$\left|\alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}, \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}\right\rangle_{HV} \tag{65}$$

$$\alpha_3 = t_B \alpha_2. \tag{66}$$

In (66) t_B is the transmissivity of BS_3. Returning to Alice, the quantum states at beam splitters BS_4 and BS_5 inputs are

$$\left|\alpha_1 e^{i\phi_1(\omega)}, \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}\right\rangle \tag{67}$$

$$\left|\alpha_1 e^{i\phi_2(\omega)}, \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}\right\rangle. \tag{68}$$

Now, using (61), the states at beam splitters BS_4 and BS_5 outputs are

$$\left|\frac{\alpha_1 e^{i\phi_1(\omega)} + \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_1(\omega)} + \alpha_3 e^{i[\phi_1(\omega)+\phi_{BH}]}}{\sqrt{2}}\right\rangle_{12} \tag{69}$$

$$\left|\frac{\alpha_1 e^{i\phi_2(\omega)} + \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}}{\sqrt{2}}, \frac{-\alpha_1 e^{i\phi_2(\omega)} + \alpha_3 e^{i[\phi_2(\omega)+\phi_{BV}]}}{\sqrt{2}}\right\rangle_{34}. \tag{70}$$

Hence, the photocurrents in D_1, D_2, D_3 and $D_4$are, respectively,

$$I_{1,2} = R\left[\frac{\alpha_1^2+\alpha_3^2}{2} \pm \alpha_1\alpha_3\cos(\phi_{BH})\right] \tag{71}$$

$$I_{3,4} = R\left[\frac{\alpha_1^2 + \alpha_3^2}{2} \pm \alpha_1\alpha_3 \cos\left(\phi_{BV}\right)\right]. \tag{72}$$

In (71)-(72) R is the responsivity of the detectors. Now, making $I = (I_1\text{-}I_2) + (I_3\text{-}I_4)$ one has

$$I = 2R\alpha_1\alpha_3\left[\cos\left(\phi_{BH}\right) + \cos\left(\phi_{BV}\right)\right]. \tag{73}$$

Here we will assume a sampled analog modulating signal, hence, $\phi_{BH} = mS_H(kT)$ and $\phi_{BV} = mS_V(kT)$, where m ($<<1$) is the modulation index, k is an integer number and T is the time step, equal to the time separation between consecutive optical pulses generated by the laser. Obviously, in order to satisfy the Nyquist theorem, the maximal frequency components of S_H and S_V are lower or equal to $1/(2\,T)$. For a small value of m one has $\cos(\phi_{BH}) \sim 1+\phi_{BH}$ $= 1 + mS_H(kT)$ and, similarly, $\cos(\phi_{BV}) \sim \ 1 + mS_V\ (kT)$. Substituting these expressions in (73) one finally gets

$$I \approx 2R\alpha_1\alpha_3\left\{2 + m\left[S_H\left(kT\right) + S_V\left(kT\right)\right]\right\}. \tag{74}$$

Thus, according to (74), using a low-pass filter, Alice can recover the signal $S(t) = \mathrm{S}_H(t)$ $+ S_V(t)$ sent, in a secure way, by Bob.

One may note that, the best that Eve can do is to use a beam splitter with reflectivity equal to the loss between Alice and Bob and to change the fiber between Alice and Bob by a lossless fiber. At Bob's output, Eve uses the same apparatus of Alice. Thus, Eve would get

$$I \approx 2R\alpha_2\alpha_3\left\{2 + m\left[S_H\left(kT\right) + S_V\left(kT\right)\right]\right\}. \tag{75}$$

Since $\alpha_2 << \alpha_1$, the signal obtained by Eve would be very weak and not detectable. Furthermore, due to (59)-(60), Eve would not have enough information to reconstruct $\phi_{1\omega}$ and $\phi_{2\omega}$ and to resend the correct state to Alice. At last, the security of the scheme in Fig. 3 can be even improved by the usage of thermal states [14, 16].

6 Conclusions

The present work showed that considering the spectral distribution of single-photons, two-photon entangled states and coherent states is an important issue in the analysis of quantum error rate and security of quantum communication protocols. In fact, a quantum protocol can be considered unconditionally secure or insecure only if all conditions required by physical laws are taken into account in the security analysis, this includes, obviously, the non-zero spectral distribution of the optical pulses and frequency dependence of optical devices. In this direction, the present work provided

(i) Analytical equations for single-photon interference when the phase modulators are frequency-dependents, and two-photon interference (HOM experiment) when the two single-photons at the beam splitters' inputs have different spectral distributions.
(ii) An equation for estimating the spectral distribution of single-photons, produced by a source based on four-wave mixing in optical fibers, versus the optical power of the pump beam.

(iii) A formula for the probability of Alice being caught cheating in a quantum bit commitment protocol realized with entangled photons, when real conditions are considered.

(iv) An optical setup for secure transmission of a sampled analog signal. The spectral width and the frequency-dependence of the phase-modulators were used to provide the security of the system.

Acknowledgements

This work was supported by the Brazilian agencies CAPES and CNPq via Grant no. 307062/2014-7. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

[1] G. P. Agrawal (2007). *Nonlinear fiber optics*. Academic press.

[2] D. J. Santos, R. Loudon, and F. J. Fraile-Peláez (1997). Continuum states and fields in quantum optics. *American Journal of Physics*, Vol. 65(2), pp. 126–132.

[3] R. V. Ramos and R. F. Souza (2001). Simulations of continuum coherent states and its use in quantum cryptographic systems. *Journal of Modern Optics*, Vol. 48(6), pp. 989–1003.

[4] A. J. Berglund (2000). Quantum coherence and control in one-and two-photon optical systems. *arXiv preprint quant-ph/0010001*.

[5] Y.-X. Gong, Y.-S. Zhang, Y.-L. Dong, X.-L. Niu, Y.-F. Huang, and G.-C. Guo (2008). Dependence of the decoherence of polarization states in phase-damping channels on the frequency spectrum envelope of photons. *Physical Review A*, Vol. 78(4), pp. 042103.

[6] G. Agrawal. *Applications of nonlinear fiber optics*. Academic press, 2007.

[7] Q. Lin, F. Yaman, and G. P. Agrawal (2006). Photon-pair generation by four-wave mixing in optical fibers. *Optics letters*, Vol. 31(9), pp. 1286–1288.

[8] X. Li, J. Chen, P. Voss, J. Sharping, and P. Kumar (2004). All-fiber photon-pair source for quantum communications: Improved generation of correlated photons. *Optics express*, Vol. 12(16), pp. 3737–3744.

[9] H. Takesue and K. Inoue (2005). 1.5-μm band quantum-correlated photon pair generation in dispersion-shifted fiber: suppression of noise photons by cooling fiber. *Optics express*, Vol 13(20), pp. 7832–7839.

[10] D. B. de Brito and R. V. Ramos (2010). Analysis of heralded single-photon source using four-wave mixing in optical fibers via wigner function and its use in quantum key distribution. *IEEE Journal of Quantum Electronics*, Vol. 46(5), pp. 721–727, 2010.

[11] H.-K. Lo and H. F. Chau (1997). Is quantum bit commitment really possible? *Physical Review Letters*, Vol. 78(17) pp. 3410.

[12] H. P. Yuen (2003). How to build unconditionally secure quantum bit commitment protocols. *arXiv preprint quant-ph/0305144*.

[13] G. Murta, M. T. Cunha, and A. Cabellov(2013). Quantum nonlocality as the route for ever-lasting unconditionally secure bit commitment. *measurements*, pp. 16:17.

[14] A. G. d. A. H. Guerra, F. F. S. Rios, and R. V. Ramos (2016). Quantum secure direct communication of digital and analog signals using continuum coherent states. *Quantum Information Processing*, Vol. 15(11), pp. 4747–4758.

[15] P. V. P. Pinheiro and R. V. Ramos (2015). Two-layer quantum key distribution. *Quantum Information Processing*, Vol. 14(6), pp. 2111–2124.

[16] F. A. Mendonça, D. B. De Brito, and R. V. Ramos (2012). An optical scheme for quantum multi-service network. *Quantum Info. Comput.*, Vol. 12(7-8), pp. 620–629.