Optical transmission of frequency-coded quantum bits with WDM synchronization

Thiago Ferreira da Silva and Jean Pierre von der Weid

Abstract—**Quantum-key distribution enables absolutely secure communication between two parts, making them able to share a secret that will be used in the posterior message encryption. Here we shall report the experimental implementation of an optical qubits transmission system compatible with the BB84 protocol. Photons are prepared and measured by a double-modulation process according with the relative phase of a wavelength-division multiplexed synchronized radiofrequency signal, in the way that the qubits are coded in the optical sidebands. A filtering scheme is applied to further sidebands selection, delivering the qubits to the single-photon detector.**

Keywords—**QKD; quantum-key distribution; quantum cryptography; frequency coding; BB84 protocol.**

I. INTRODUCTION

Several communication sections have the need of confidentiability as the main feature. For this purpose, modern cryptographic systems make use of the advent of the key. In this way, the public key systems are widely implemented, making parties able to share information easily. On the other hand, as this kind of code is not proved as absolutely secure, one could discover an efficient algorithm to break the key. Another possibility refers to the private key systems. In Vernam cipher, per example, if both parts share a common random sequence, they are able to code a message that no one that does not have the key can decipher. Such a scheme is proved as absolutely secure if each key is used once and only once [1]. Quantum cryptography rises as a relatively new and interdisciplinary area that, grounded in the quantum physics laws, promises to solve the major challenge in the actual symmetric classical cryptography, the key distribution.

First proposed by Bennett and Brassard in 1984 [2], the quantum-key distribution (QKD) protocol starts with a random sequence of bits that one part, say Alice, wants to share with other one, called Bob. For each bit, Alice prepares, also randomly, a quantum bit (qubit) in one of four states of two non-orthogonal bases in a Hilbert space. In this way, the photons are coded in some degree of freedom and sent to Bob, who chooses for each of them, again randomly, the basis at his measurement apparatus. Depending on this choice, the photon is routed to one of two single-photon detectors (SPD), which represents bit zero and bit one. If the measurement basis is compatible (coincident) with that chosen by Alice, the qubit will be projected in the correct autovector and detected by the correct SPD, that fires a count. If the bases disagree, the qubit will be projected in one of the two vectors of the measurement base with equal probability, resulting in a random bit and a random SPD count. So, this raw key has 75% of correct bits.

After transmission, the communicating parties perform the basis reconciliation. Bob tells Alice through a classical channel in which instants photons were detected and in which basis they were measured. If Alice's preparation basis agree, they keep the bit; if not, they discard it, resulting in a sifted key composed from 50% of the received bits in mean.

An eavesdropper (Eva) could be present at any point of the link and it is assumed to be able to perform any kind of (physically possible) measurement. So Alice and Bob must determine the quantum bits error rate (QBER) of the system. They choose some bits and publicly reveal them to each other. If the error is above a specific value, too much information could have been eavesdropped and they stop the protocol. If not, they perform an error correction step. After this, a privacy amplification protocol can be used to reduce Eva's information to an arbitrary low value, letting Alice and Bob with a secure key and able to communicate [3].

This paper reports the experimental implementation of an optical QKD system with frequency coding by amplitude and phase double-modulation process and wavelength-division multiplexing (WDM) synchronization. Such frequency coding technique agrees with the BB84 protocol, as like to other four- or two-states discrete-variables ones, like B92 or SARG04 [4]. According to phase difference between transmitter and receiver, the qubits will be found in the sidebands (SB) of an optical signal. A selective photon counting at these wavelengths can reveal or not the transmitted bit.

The mean theoretical foundations of the frequency coding scheme are introduced in section II. Section III shows the filtering scheme applied to the photon selection after qubit decoding, as like the characterization measurements of such devices. A description of the implemented system is presented in section IV. Section V shows the results of quantum measurements, followed by some conclusions in section VI.

II. FREQUENCY CODING

As verified by [5,6], an amplitude and phase double-modulated optical signal can exhibit sideband suppression if it is properly adjusted. It is due to the fact that amplitude

Thiago Ferreira da Silva and Jean Pierre von der Weid, Telecommunication Studies Center – CETUC, Pontifical Catholic University of Rio de Janeiro – PUC-Rio, Rio de Janeiro, Brazil, E-mails: thiago@cetuc.puc-rio.br, vdweid@cetuc.puc-rio.br. This work has been supported partially by CNPq and by FAPERJ.

modulated (AM) signals present identical sidebands at the same spectral distance and phase relative to the carrier. On the other hand, a phase modulated (PM) signal may present the same equally spaced sidebands, but with inverse phase relative to each other. Combining them through a double-modulation scheme, one sideband can be then suppressed, regarding the modulating signals and modulation depths are the same, and the correct AM bias voltage is established.

Depending on the phase difference between AM and PM signals, left SB, right SB, or neither of them will be suppressed [6]. It occurs in a complementary way, according to the right (I_+) and left (I_-) SB intensities bellow:

$$\begin{aligned} I_+ &= \frac{E_0^2}{8}\left[\frac{m_A^2}{4} + m_B^2 - m_A m_B sen\left(-\frac{n}{c}\Omega L - \phi_A + \phi_B\right)\right] \\ I_- &= \frac{E_0^2}{8}\left[\frac{m_A^2}{4} + m_B^2 + m_A m_B sen\left(-\frac{n}{c}\Omega L - \phi_A + \phi_B\right)\right] \end{aligned} \qquad (1)$$

where E_0 is the amplitude of the carrier wave, m_A and m_B refers to amplitude and phase modulation depths respectively, *n* is the fiber refractive index, *c* is the velocity of the light, Ω is the radiofrequency (RF), *L* is the propagation distance and ϕ_A and ϕ_B are the RF phases.

Two non-orthogonal bases, each one composed by two orthogonal states, can be defined in a Hilbert space. They are associated to the signal phases ϕ_A and ϕ_B as in Table I.

TABLE I
PHASE RELATIONS FOR THE FREQUENCY CODE CODIFICATION TECHNIQUE

Alice			Bob				
Base	**Bit**	**Φ_A**	**Φ_B**	**ΔΦ**	**P(|ω$_0$-Ω⟩)[a]**	**P(|ω$_0$+Ω⟩)**	**Bit**
α	0	0	0	0	0	1	1
		0	π/2	π/2	0,5	0,5	0 or 1
	1	π	0	π	1	0	0
		π	π/2	π/2	0,5	0,5	0 or 1
β	0	π/2	0	π/2	0,5	0,5	0 or 1
		π/2	π/2	0	0	1	1
	1	3π/2	0	π/2	0,5	0,5	0 or 1
		3π/2	π/2	π	1	0	0

[a] P stands for the probability of the correct bit detection after Bob's basis choice. Left (-) and right (+) sidebands are represented by $\omega_0 \pm \Omega$, that is, the frequency difference and sum of optical carrier and modulating RF signal.

As can be seen, if the preparation and measurement bases difference equals zero or π, the photon will ideally be in one and only one of the sidebands, represented by states $|\omega_0 \pm \Omega\rangle$, with hundred percent probability. On the other hand, if the bases disagree (difference of π/2), the qubit state cannot be deterministically determined, and will be a coherent superposition of both states in the form

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|\omega_0 + \Omega\rangle + |\omega_0 - \Omega\rangle\right). \qquad (2)$$

Thus the measured qubit will collapse to one of these states at detection, firing one of the SPD, what results in a random zero or one bit value.

III. FILTERING SCHEME

As the single-photon detector has no spectral filter, all the wavelengths matching its responsivity would be detected, as the whole signal would be integrated. As the decoded qubit are found only in the sidebands after Bob's base choice, the optical carrier must be suppressed. To avoid this source of noise, a filtering scheme is need. Following this, the sidebands have to be separated and sent to different SPDs, what requires another filter or interleaver. To insert the synchronism channel a multiplexer-demultiplexer pair is required.

A. *Bragg-gratings Fabry-Perot filter*

To suppress the carrier, as it carries no more information, a Fabry-Perot cavity was projected, acting as a notch filter. It was designed with two specifically spaced (5mm) Bragg gratings, in the way that the optical sidebands of the input signal are reflected back to a circulator and then to output R, while the carrier is transmitted to output T, as in Fig. 1.

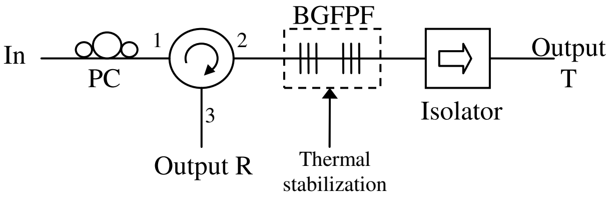

Fig. 1. Bragg-gratings Fabry-Perot (BGFPF) filter scheme.

A polarization controller (PC), like "Mickey ears", was set at the input, while an optical isolator after the cavity grants no undesired back-reflection of fiber termination. The gratings were thermally stabilized as their small thermal mass make the spacing length very unstable. For this purpose, a PID controller, a thermistor and a thermoelectric device were used. A proper temperature change leads to a fine spectral tuning.

The transmission spectra from input to output T and to output R were measured and are shown in Fig. 2. The Fabry-Perot peaks are spaced by 20GHz and the Bragg gratings centered at 1548.5nm.

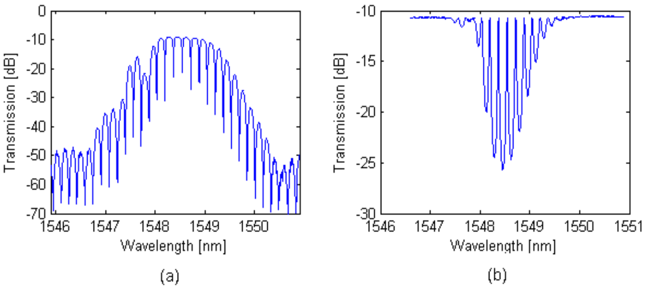

Fig. 2. Bragg-gratings Fabry-Perot filter transmission spectra from input to (a) reflected output and to (b) transmitted output.

B. *Mach-Zehnder interferometer*

Sideband selection was achieved by an interleaver. Two optical couplers were carefully spliced in order to construct a Mach-Zehnder interferometer (MZI), as in Fig. 3.

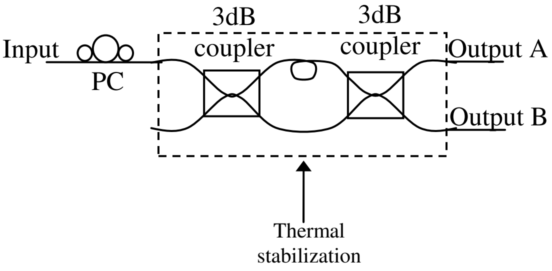

Fig. 3. Mach-Zehnder interferometric interleaver scheme.

The arms unbalance leads to the interference of the two propagating portions of the optical field as they acquire a relative phase. The wavelength dependent sinusoidal interference term with 40GHz pattern was achieved with a difference of 20mm in the paths. Putting one SB at some transmission peak of the device while the other one is placed at an adjacent valley, which corresponds to a transmission peak for the complementary output, grants the desired desegregation of the spectral signal components.

Again, a "Mickey ears" polarization controller was set at the input port, because the fields must not be orthogonal to interfere [7]. A thermal stabilization similar to the previous BGFPF was necessary, for the same reasons.

The complementary interleaving pattern can be seen in the transmission measurements from input to outputs A and B at Fig. 4. An extinction rate around 20dB was achieved.

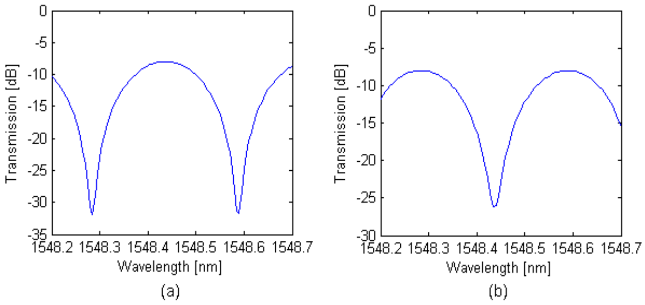

Fig. 4. Mach-Zehnder interferometer transmission spectra from input to output (a) A and (b) B.

C. *WDM MUX-DEMUX*

The synchronism channel was inserted in the system with the WDM technique. The multiplexer (MUX) and demultiplexer (DEMUX) devices were characterized, as in Fig. 5, to assure this classical channel would not interfere to the quantum one.

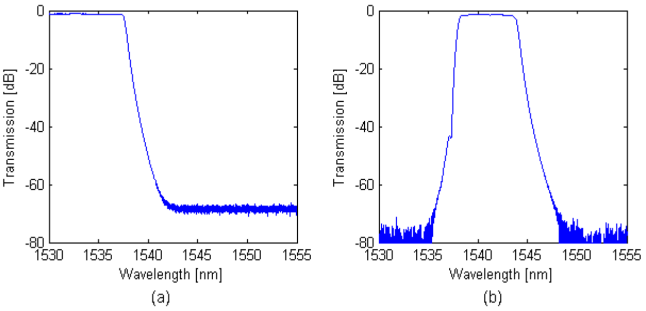

Fig. 5. MUX-DEMUX transmission spectra from common input to channels (a) 1 and (b) 2. The last one has been chosen for the synchronization channel.

As seen, the best isolation measured was better than 75dB, determining the choice of the channel number 2, against the other one, to establish the synchronization, as the quantum channel had been placed at 1548.5nm.

IV. General System Description

In the optical frequency-coded qubits transmission reported, Alice has a poissonian photon source, obtained with a faint laser, set around 1548.5nm and with a mean photon number in the sidebands near 0.2 per 2.5 ns gate. For each zero or one bit to be transmitted, the amplitude of an optical tone is modulated by a RF signal at 10.308GHz. The signal phase must be chosen according with Table I, which links it to the two non-orthogonal quantum bases. The basis selection results in one of the four quantum states per qubit. This choice was implemented over the RF by a quadrature phase-shift keying (QPSK) modulator and applied to the photons through a Mach-Zehnder optical modulator.

At the receiving side, Bob must choose between the two bases, changing his modulating RF signal phase with another QPSK modulator. He then modulates the phase of the incoming optical signal, determining the photon spectral position. Next, he must apply the filtering scheme.

Bob's RF signal is identical to Alice's one and have been sent to him through the same fiber of the qubits, but in another WDM channel, modulated over other wavelength. Both this classical and he quantum channel are subjected to the same transmission path variation, what achieves the system phase stability.

After the carrier filtering and sidebands separation, the system output was connected to a SPD by an optical switch. The detector was an InGaAs commercial one, properly cooled and set up in Geiger mode with 2.5ns trigger pulses at 100kHz repetition rate. Its dark counts was measured as 1.4×10^{-4} counts per Hz.

V. Quantum Measurements and Results

The optical frequency-coded qubits transmission system was gradually implemented. The first measurement determined the system RF operation and was necessary to adjusting the AM-PM electro-optic propagation lengths. Then the phase keying was set and, at last, the synchronization channel was configured.

A. *Frequency-swept system*

In this setup, Alice and Bob use the same RF generator to their amplitude and phase modulation, as in Fig. 6.

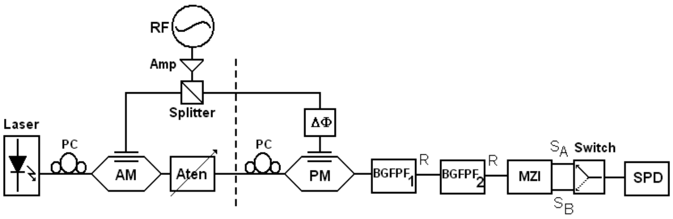

Fig. 6. Frequency sweep system.

The frequency was swept in order to vary the relative signal phase between Alice's and Bob's modulated signals. As the electro-optic lengths are kept constant, the frequency change leads to a wavelength change. It will affect the phase of the arriving electrical and optical signals at Bob's PM. A fine phase adjust was obtained by the delay shift ΔΦ.

The resulting sinusoidal pattern for both system outputs can be seen in Fig. 7, relating the RF (relative phase) to the photon counts, as like the detector dark counts.

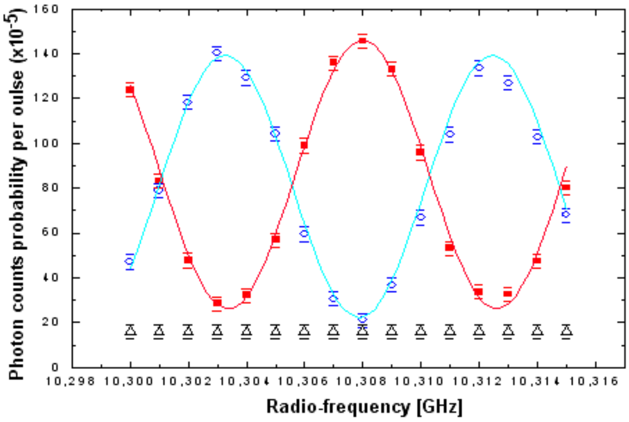

Fig. 7. Photon counts according to the phase difference induced by radio-frequency sweep for both outputs A (unfilled circles) and B (filled squares) with the standard deviation bars. Triangles represent detector dark counts.

One can see the complementary behavior of the system outputs. The peaks of one curve match to the valley of the other, corresponding to the cases of bases agreement and photon determined presence at some SB. The curves interception points correspond to the cases of ambiguity presence in sidebands, when the bases disagree.

The system visibility can be calculated from the photon counts, being equal to the difference between the maximum and the minimum counts at some setting point divided by their sum. At the maximum contrast point, obtained at RF 10.308GHz, the visibility is 75%. As the detector dark counts were measured as 1.4×10^{-4} per pulse at 2.5ns width – a large value, it was reduced by one order of magnitude, resulting in a common commercial value. So, the resulting visibility is 91%.

B. *Phase-shifted system*

Keeping the RF at 10.308GHz, the QPSK modulators were inserted, as Fig. 8. Now the phases can be discretely chosen, between the four values by Alice (0 or π; π/2 or 3π/2), and the two bases by Bob (0 or π/2).

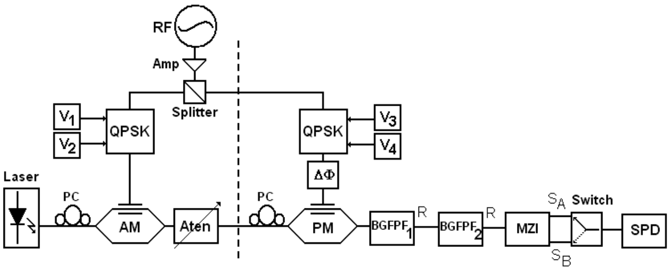

Fig. 8. Phase-shift system by the QPSK modulators.

The photon counts were performed for all the eight phases combination possibilities and grouped in the two graphics of Fig. 9.

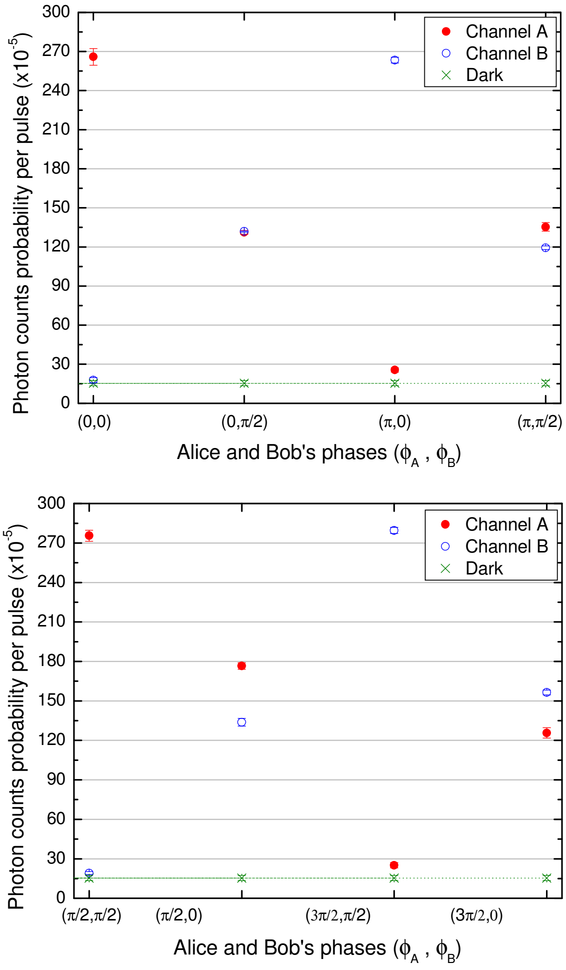

Fig. 9. Photon counts according to Alice and Bob's phases (ϕ_A, ϕ_B). In the upper figure, Alice can choose between states 0 and π of the first base and, in the lower one, between π/2 and 3π/2 of the second base. Bob can choose between 0 and π/2 (one statebof each base) in both cases. Red filled and blue unfilled circles represent system outputs A and B, respectively, with the corresponding standard deviation bars. The green dashed line represents SPD the dark counts.

The total QBER is related to visibility and calculated according to [3]

$$QBER_{total} = \frac{1-V}{2}\,. \qquad (3)$$

For the maximum extinction rate points, corresponding to the coincident preparation and measurement bases, visibility and QBER are shown in Table 2 (1st and 2nd columns).

TABLE II
VISIBILITY AND QBER FOR THE PHASE-SHIFTED SYSTEM

Output	V_{meas}	$QBER_{total}$	$QBER_{det}$	$QBER_{dev}$	V_{better}	$QBER_{total}$	$QBER_{det}$	$QBER_{dev}$
A	83,0%	8,5%	4,3%	4,2%	90,6%	4,7%	0,5%	4,2%
	82,7%	8,6%	4,4%	4,2%	90,6%	4,7%	0,5%	4,2%
B	88,0%	6,0%	4,6%	1,4%	96,2%	1,9%	0,5%	1,4%
	86,4%	6,8%	4,8%	2,0%	94,9%	2,6%	0,5%	2,0%

V_{meas}: measured visibility; $QBER_{total}$: total QBER; $QBER_{det}$: detector QBER; $QBER_{dev}$; devices QBER; V_{better}: visibility corrected as the detector had one magnitude order better dark counts.

By subtracting photodetector dark counts from the total counts, we obtain the QBER imposed by the system devices ($QBER_{dev}$), and subtracting it from the total one, the detector QBER ($QBER_{det}$). Assuming the use of a better detector, with dark counts one magnitude order lower, the values were recalculated, resulting in the 6th to 9th columns in table II.

C. *WDM synchronized system*

Finally, the common RF generator was replaced by the synchronism channel, as in Fig. 10.

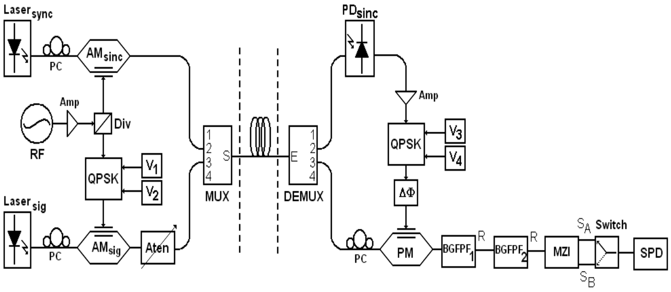

Fig. 10. Qubits transmission system with synchronization channel.

Now only Alice has the RF generator. She divides this signal and modulates the synchronism laser. The classical optical signal is coupled to the fiber through the WDM MUX and disaggregated at Bob's side by the WDM DEMUX. A p-i-n diode recovers the RF signal that, after amplification, passes through the QPSK modulator and drives the optical PM.

The channels crosstalk was first measured. With the quantum channel laser turned off, the power of the synchronism laser was varied, while Bob's classical received power and photon counts were monitored. For a received power at Bob's synchronism photodiode varying up to -1dBm, no changes were observed at the photon counts, indicating that no leakage has taken place.

The last measurement is similar to the one in section V-b and is shown in Fig. 11.

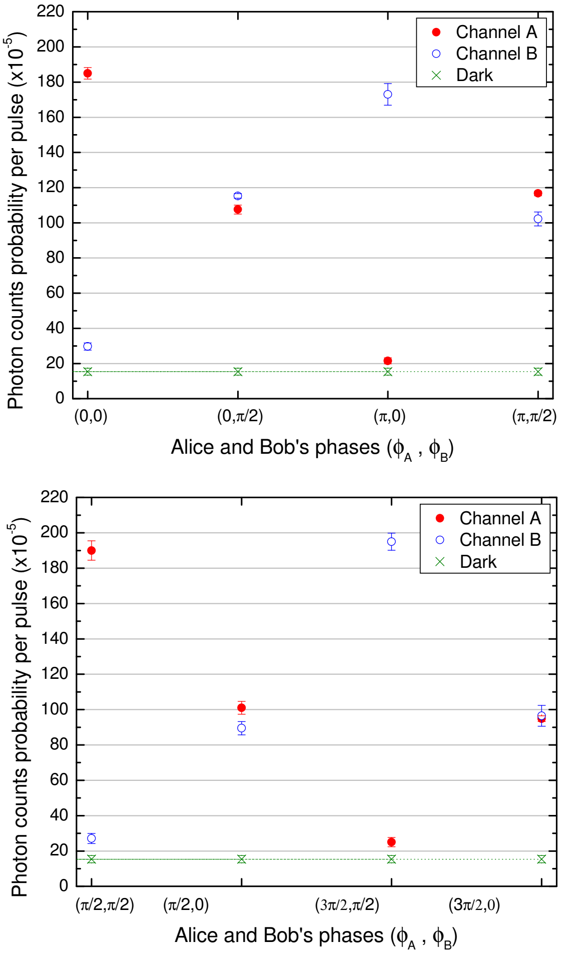

Fig. 11. Photon counting according to Alice and Bob's phases (ϕ_A, ϕ_B). In the upper figure, Alice can choose between states 0 and π of the first base and in, the lower one, between π/2 and 3π/2 of the second base. Bob can choose between 0 and π/2 (one of each base) in both cases. Red filled and blue unfilled circles represent system outputs A and B, respectively, with the corresponding standard deviation bars. The green dashed line represents SPD the dark counts.

The photon counts were grouped according to Alice's bases, and the results for both Bob's choices are shown in Table III in a similar way to section V-b.

TABLE III
VISIBILITY AND QBER FOR THE WDM-SYNCHRONIZED SYSTEM

Output	V_{meas}	$QBER_{total}$	$QBER_{det}$	$QBER_{dev}$	V_{better}	$QBER_{total}$	$QBER_{det}$	$QBER_{dev}$
A	73,6%	13,2%	5,2%	8,0%	82,9%	8,6%	0,6%	8,0%
	73,0%	13,5%	5,9%	7,6%	83,5%	8,2%	0,7%	7,6%
B	80,1%	10,0%	6,1%	3,8%	91,0%	4,5%	0,7%	3,8%
	76,7%	11,6%	5,7%	5,9%	86,9%	6,5%	0,7%	5,9%

The results here are inferior if compared with the RF generator shared setup. The RF power amplifier (at Bob's side) noise figure broadened the optical spectrum at the phase modulator, in such a way that the filtering lost efficiency. Furthermore, the power budget was not the better possible, i.e., PM modulation depth was slightly different from AM one as result of the low power achieved.

VI. Conclusions

A double-modulated AM-PM frequency-coded qubits transmission system with WDM synchronization [5], agreeing with BB84 (four-states discrete-variables protocols) [6] was implemented. It worth mentioning that, if two AM or two PM modulator were used, only the two-state protocol (B92) would be compatible [6]. This degree of freedom of the qubits is in principle justified to avoid the required interferometers stabilization of the phase coding and the high fiber induced decoherence in polarization coding systems [3].

The results reported have shown a correct systemic behavior, assessing its possibility as a QKD system. It can be seen that the measured QBER is lower than the general upper threshold of 12,4% [8], what enables further error correction, privacy amplification and the agreement on a secure key. However, some aspects must be mentioned. The polarization dependence of both amplitude and phase modulators displaces the system optimum operating point with time, as consequence of the polarization-mode dispersion. The same problem is faced by the Mach-Zehnder interferometer and even by the Bragg-gratings Fabry-Perot filters, leading thus to the difficulty of adjusting all system parameter and maintaining them at the optimum set point. Polarization insensitive filters and modulators are suggested to face such a problem, or even an active polarization control solution.

References

[1] D. Bouwmeester, A. Ekert and A. Zeilinger, *The Physics of Quantum Information: Quantum Cryptography*, Quantum Teleportation, Quantum Computation. Berlin: Springer, 2000.

[2] C. H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*. Proceedings of IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, pp. 175-179, December, 1984.

[3] N. Gisin et al, *Quantum Cryptography*. Reviews of Modern Physics, volume 74, January 2002.

[4] Scarani et al – *A framework for practical quantum cryptography.* ArXiv:0802.4155v1 [quant-ph], February 28th 2008.

[5] J. Mérolla et al, *Single-photon interference in sideband of phase-modulated light for quantum cryptography*. Physical Review Letters, Vol. 82, No. 8, 22 February 1999.

[6] G. B. Xavier and J. P. von der Weid, *Modulation schemes for frequency coded quantum key distribution*, Electronics Letters, Vol. 41, Issue 10, 12 May 2005.

[7] G. P. Agrawal, *Fiber-optic communication systems*. New York: Wiley & Sons, 2002.

[8] B. Kraus, N. Gisin and R. Renner, *Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication*. Phys. Rev. Lett., Vol. 95, 080501, August 19th 2005.