

Stable polarization coded quantum communication through single mode optical fibers

G. B. Xavier, G. Vilela de Faria, G. P. Temporão, J. P. von der Weid, H. Zbinden and N. Gisin

Abstract — We perform a transmission of polarization encoded quantum bits through 16 km of single mode optical fiber in the 1550 nm window. The polarization drift caused by the changing birefringence of the fiber is kept stable through the use of a polarization control system we developed. This system employs 2 classical reference signals with 0.8 nm spacing from the quantum channel. We also send through the same fiber an extra reference classical signal used to trigger the single-photon detector. To the best of our knowledge this is the first time a quantum channel is multiplexed with 3 classical signals in the same optical fiber.

Keywords — Quantum Information, Optical Communications, Quantum Key Distribution.

I. INTRODUCTION

Quantum Information Theory (QIT) [1] stands in the intersection between classical information theory and quantum physics. Quantum communication is the branch of QIT that concerns the generation, transmission and detection of quantum information. It includes quantum cryptography [2] and quantum teleportation [3], which have both seen considerable advances in the last years. For all quantum communication schemes, the information is coded into two-level quantum systems, known as quantum bits or qubits. The quantum entity generally used for quantum communications is the single photon, due to its natural characteristics for transmission.

Usually the information is coded in either polarization [4] or phase [5] of a single photon. Polarization coding was only used extensively in the beginning of experimental optical fiber quantum communication. Fiber birefringence varies randomly along an optical fiber, causing a phenomenon well known in classical optical communications called Polarization Mode Dispersion (PMD) [6]. The State of Polarization (SOP) of an optical signal will also vary randomly along the fiber, because of the changing birefringence. Because of these reasons it has been considered non-practical to perform polarization coding outside of the lab. Phase coding has since then taken over [2]. In fact most commercial quantum cryptography systems (also called Quantum Key Distribution or QKD for short) currently employ phase coding [7].

G. B. Xavier, G. Vilela de Faria, G. P. Temporão and J. P. von der Weid, Center for Telecommunication Studies, Pontifical Catholic University of Rio de Janeiro, Rua Marquês de São Vicente, 225 Gávea – Rio de Janeiro – Brazil, Email: guix@opto.cetuc.puc-rio.br Tel +55 21 3527 1684.

H. Zbinden and N. Gisin, GAP-Optique, University of Geneva, rue de l'Ecole-de-Médecine 20, CH-1211 Geneva 4, Switzerland.

This work was partially financed by CAPES and CNPq.

However it is still desirable to perform quantum communication employing polarization coding. Phase coding systems require very good stabilization of the interferometers used, making polarization coding simpler in principle. There are other cases where polarization coding will be needed such as hyperentanglement [8]. In this paper we perform a stable transmission of polarization coded qubits, over 16 km of optical fiber and show the results.

II. THE BB84 PROTOCOL

We shall perform here a very brief review of the most widely used protocol in QKD, BB84 [4], since it will be illustrative to show why non-orthogonal states are needed. In order to keep trend with the literature, we will also employ the terms Alice and Bob for the transmitter and receiver respectively, and Eve for the eavesdropper. For a more comprehensive explanation please refer to [2].

The BB84 protocol consists of two distinct parts: the quantum transmission in itself and a classical reconciliation procedure. This classical procedure consists of Alice and Bob talking to each other via a classical communication channel, which is of course, passive of eavesdropping. The only requirement is that the information on the channel is not modifiable.

Alice randomly generates a key for transmission. For each bit she intends to transmit she randomly chooses between two transmission bases, $+$ and X . Base $+$ consists of two orthogonal polarization states. We shall use horizontal and vertical ($|0^\circ\rangle$ and $|90^\circ\rangle$) linear polarization states for their representation. These two states are vectors in a 2-dimensional Hilbert space, and they form an orthonormal base for this vector space. Thus, they are distinguishable from each other, as any two orthogonal states in quantum physics. Base X also consists of two other orthogonal states that form another orthonormal base in the same 2-dimensional Hilbert space. We will use the two diagonal polarizations, $|+45^\circ\rangle$ and $|-45^\circ\rangle$ for base X . Therefore the two orthogonal states of base X are also readily distinguishable from each other. However, states belonging to base $+$ cannot be deterministically distinguished from states of base X , because they are non-orthogonal [4]. What gives QKD its security is this idea of using two random bases for each transmitted qubit.

Alice therefore randomly chooses between both bases for transmission of each bit. Bob uses a polarization beam-splitter (PBS), a device that can reliably distinguish between

two orthogonal polarization states. At the end of each arm of the PBS, there is a single photon detector. So, if Alice uses base $+$, and Bob aligns his PBS with a polarization controller in respect to this base, then he will know which state was sent, $|0^\circ\rangle$ or $|90^\circ\rangle$, according to the result of his detectors. However if Alice sends a state using base X and Bob has aligned his PBS with respect to base $+$, the photon will have a 50% probability of going into either arm of the PBS, and as such, Bob will not be able to know which polarization was sent. He can only guess, but it is not a good strategy, since he will be wrong for half of his attempts. If Bob aligns his PBS with respect to base X , and Alice sends the qubit using base X , then Bob will now be able to correctly distinguish between $|+45^\circ\rangle$ and $|-45^\circ\rangle$. Every time they use the same base, then the qubit can be correctly distinguished, and every time they disagree on the basis used, the qubit cannot be correctly measured.

Bob will then, also choose randomly, and independently of Alice between bases $+$ and X for each qubit that he measures. He will record the results of his single-photon detectors and which base he used for each measurement. Alice also records for herself which base she employed for each transmitted qubit. After some time they stop the transmission and communicate using the classical channel, revealing publicly which base they used for each qubit. Bob does not, at any time, reveal the results of his measurement, i. e., which detector accused a count for each qubit. Every time they disagree on the base choice, they discard that qubit, which should be 50% of all the sent qubits. The other half they keep as a raw key, which will be further distilled. Now, apart from errors in the system, they can be certain of the results of the raw key, since they both used the same base for each of these qubits, and therefore Bob can reliably measure them.

This procedure of using two random and independent base choices for transmission and detection is what gives QKD its security. The simplest strategy Eve may choose to use is the intercept-resend attack, in which case she must also guess the basis in which to measure the qubits, therefore introducing a 25% error rate in the transmitted key if she attempts to measure every single qubit [2]. So, shortly after Alice and Bob obtain the raw key, they discard some bits to measure the error rate. If they obtain a 25% error rate, they know that Eve listened in on all the transmitted qubits. After the error rate verification Bob and Alice follow on to perform error correction and privacy amplification procedures [4].

III. THE EXPERIMENT

We use the idea of employing classical side channels as a polarization reference for the channel carrying the quantum information (henceforth called the quantum channel) [9]. We employ two side channels, one at a shorter, and the other at a longer wavelength than the quantum channel. They are also placed as close as possible to the quantum channel according to our simulations [10].

Our experimental setup is shown in Fig. 1. We chose to use the standard ITU-T grid for the wavelength of our channels, in order to be able to use standard off-the-shelf telecom components. Our quantum channel was chosen to be placed at $\lambda_Q = 1546.12$ nm. According to our simulations, a distance of 0.8 nm from the classical channels to the quantum channel will suffice for typical QKD transmission distances [10]. Therefore we used the immediate below and above channels in the grid, $\lambda_1 = 1545.32$ nm and $\lambda_3 = 1546.92$ nm respectively. These two channels will be used in a counter propagating way, to minimize noise contribution from imperfect filtering. We also use a 4th channel, at $\lambda_4 = 1547.72$ nm, to use as a synchronism channel for the SPAD.

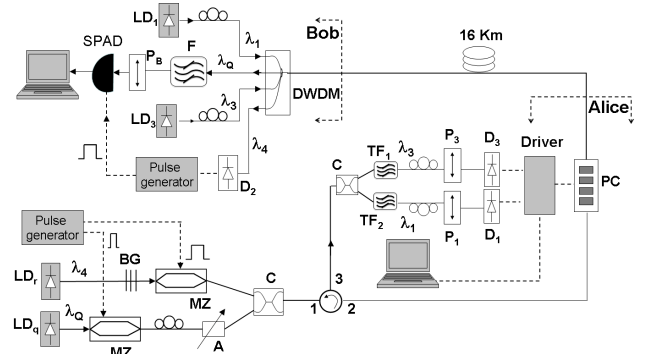


Fig. 1. Experimental setup: LD: Laser diodes, MZ: Mach-Zehnder modulators, BG: Bragg grating, A: Variable optical attenuator, C: Couplers, TF: Tunable filters, P: Polarizers, PB: Polarizing beam splitter, D: Photodetectors, DWDM: Multiplexer, F: Optical filter, SPAD: Single Photon Avalanche Detector. Both classical channels SOPs are set at 45° difference at the fiber input.

The pseudo-single photons were generated by means of an attenuated Distributed Feedback (DFB) laser at $\lambda_q = 1546.12$ nm, modulated with an external Mach-Zehnder (MZ) modulator with 10 ns pulses at a frequency of 100 kHz.

The DFB laser along with a calibrated optical attenuator (A), and a MZ modulator, generating the single photon states is within Alice's setup. The attenuator was adjusted such that there is an average of 0.2 photons per pulse in the input of the fiber.

All the automated control system is also inside Alice's station. She employs a Lithium Niobate (LiNbO_3) polarization controller (PC - our system response time is of ~ 40 kHz). Both side channels, which provide the feedback information for the control loop are split with a 50/50 coupler and analyzed with a polarizer each (P_1 and P_3 set at 45° apart). A tunable filter (TF_1 and TF_2) is used at each arm to separate the 2 side channels. They are both converted to electrical signals with p-i-n photodetectors (D_1 and D_3), and they are fed into the computer for processing. We use a circulator to couple the single photons into the fiber, and the side channels in the filters.

The reference laser ($\lambda_4 = 1547.72$ nm) is also modulated by a pulse generator (50 ns pulses) in order to create the timing signal for the SPAD. The same generator drives both modulators. We use a narrowband Bragg grating at the output of the reference laser (0.3nm full width at half maximum) to

remove the amplified spontaneous emission emitted at the quantum channel wavelength from the reference laser. The power level of the side channels is set at the minimum possible level in such a way to mitigate the noise contribution, and not compromise the control system at the same time.

The Single Photon Avalanche Detector (SPAD) is located in Bob's setup. We used a 20 ns detection window to be compatible with the optical pulse we used (10 ns). The results shown in Figure 2 have been corrected assuming a 2.5 ns detection window and a 1 ns optical pulse have been used.

The filtering scheme consists of 2 DWDM multiplexers with 100GHz (0.8 nm) ITU-T channel spacing, with over 50 dB extinction ratio between adjacent channels. The first multiplexer (DWDM) is used to separate and couple the channels, with the second multiplexer only connected as an additional filter for the SPAD, and is represented in Fig. 1 by the band-pass filter F. Manual polarization controllers (shown in the figure) are used at each side channel since they need to be launched with their SOPs separated by 45° in order for the control scheme to function properly [9]. A polarizing beam splitter (P_B) is placed before the SPAD to function as an analyzer for the polarization state. The transmission fiber (two spools of 8 km of DS fiber each) is connected after the multiplexer as shown in the figure.

After being split at the DWDM, the reference channel λ_4 containing the triggering pulses for the SPAD is detected by the p-i-n photodiode D_2 . The electrical signal is formatted by a pulse generator and then sent to the SPAD. Electrical delays are adjusted at both pulse generators to correctly match the arriving single photon with the detection window. In order to avoid cross-talk noise from the co-propagating reference channel inside the quantum channel band, the modulation at λ_4 and the delay is adjusted such that the output classical power is minimum when the single photon is being transmitted.

IV. RESULTS

We transmitted 3 single photon states through our optical fiber link ($|+0^\circ\rangle$, $|+45^\circ\rangle$ and $|+90^\circ\rangle$) using our control system, and verified that the states remained constant throughout the experiment running time (Fig. 2). For a comparison of what we can expect if we attempt a quantum transmission without any type of control system, we plotted a measurement without controlling the polarization in the same figure. Clearly we can observe that the polarization drift would make transmission impossible, as we begin with $|+45^\circ\rangle$ and end up with almost $|+90^\circ\rangle$ close to the end of the measurement.

As can be observed from Figure 2 the counts are stable throughout the whole transmission time (a bit less than two hours). The small discontinuity for the $|+0^\circ\rangle$ state occurred due to a reset in the control system. Similarly the small variation at the beginning of the $|+90^\circ\rangle$ curve was due to a long settling time the system experienced.

The reason why those three states were particularly shown is because of the BB84 protocol. As was mentioned in section II, 4 states are used in BB84 divided in two bases. Those

states are fully represented by the three states shown, since for a PBS aligned with respect to the $+$ base such as our case, -45° and $+45^\circ$ will yield the same count probability.

The results shown are the net results, with dark and noise from classical channel counts removed. The measured visibility is 94.7%, which will generate a Quantum Error Bit Rate (QBER) of 2.6% after 16 km of fiber. This result clearly shows the effectiveness of our scheme.

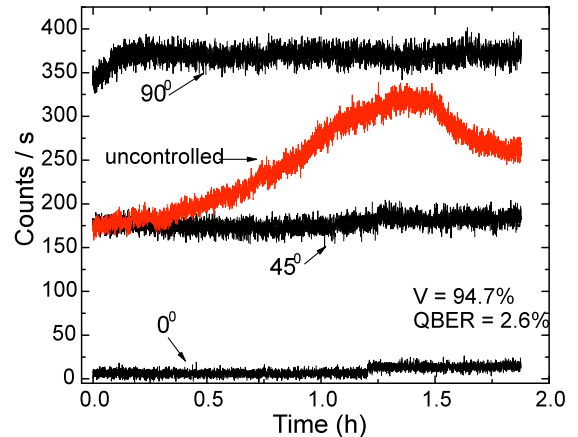


Fig. 2. Experimental net results. The value of QBER was calculated from the visibility, and shows that our system does not add substantially to the error rate. Results have been corrected to a 2.5 ns detection window.

We have performed a stable quantum transmission of single photon states over 16 km of optical fiber. We also compared these results with an uncontrolled scheme, and demonstrated that our system is effective. The experiment took place with 3 classical channels present with small wavelength separation from the quantum channel (0.8 nm spacing). To the best of our knowledge this is the first experiment performed with 3 classical channels propagating simultaneously in the same optical fiber as the quantum channel.

REFERENCES

- [1] C. H. Bennett and P. W. Shor, "Quantum Information Theory", IEEE Transactions on Information Theory, Vol. 44, Issue 6, pp. 2724-2742, 1998.
- [2] N. Gisin et al, "Quantum Cryptography", Rev. of Mod. Phys., V. 74 pp. 145-195, 2002.
- [3] C. H. Bennett et al, "Teleporting an unknown state via dual classical and Einstein-Podolsky-Rosen channels", Phys. Rev. Lett. 70, pp. 1895-1899, 1993.
- [4] C. H. Bennett et al, "Experimental Quantum Cryptography" J. Cryptology, V. 5, pp. 3-28, 1992.
- [5] C. H. Bennett, "Quantum Cryptography using any two non-orthogonal states" Phys. Rev. Lett. V. 68, pp. 3121-3124, 1992.
- [6] N. Gisin, J. P. von der Weid and J. -P. Pellaux, "Polarization mode dispersion of short and long single-mode fibers", Journal of Lightwave Tech. Vol. 9 Issue 7, pp. 821-827, July 1991.
- [7] A. Muller et al, "Plug and Play" Systems for Quantum Cryptography", Applied Phys. Lett. 70 pp. 793-795, 1997
- [8] J. T. Barreiro, N. K. Langford, N. A. Peters, P. G. Kwiat, "Generation of Hyperentangled Photon Pairs", Phys. Rev. Lett., 95, 260501, 2005.
- [9] G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express 16, 1867-1873 (2008).
- [10] G. Vilela De Faria et al, "Polarisation control schemes for fibre-optics quantum communications using polarisation encoding," Electronics Letters, vol.44, no.3, pp.228-229, January 31 2008.