

Guilherme Barreto Xavier

**Practical Assets for Fiber Optical Quantum
Communications**

TESE DE DOUTORADO

**Thesis presented to the Postgraduate Program in Electrical
Engineering of the Departamento de Engenharia Elétrica, PUC-
Rio as partial fulfillment of the requirements for the degree of
Doutor em Engenharia Elétrica**

Advisor: Prof. Jean Pierre von der Weid

**Rio de Janeiro
March 2009**



Guilherme Barreto Xavier
Recursos Práticos para Comunicações Quânticas em
Fibras Ópticas

Tese apresentada como requisito parcial para obtenção do título de Doutor pelo Programa de Pós-Graduação em Engenharia Elétrica do Departamento de Engenharia Elétrica do Centro Técnico Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Dr. Jean Pierre von der Weid

Orientador

Centro de Estudos de Telecomunicações - PUC-Rio

Dr. Hugo Zbinden

Université de Genève

Dr. Paulo Henrique Souto Ribeiro

UFRJ

Dr. Guilherme Penello Temporão

Centro de Estudos de Telecomunicações - PUC-Rio

Dra. Patrícia Lustoza de Souza

Centro de Estudos de Telecomunicações - PUC-Rio

Stephen Patrick Walborn

UFRJ

Djeisson Hoffmann Thomas

Centro de Estudos de Telecomunicações - PUC-Rio

Prof. Jose Eugenio Leal

Coordenador(a) Setorial do Centro Técnico Científico - PUC-Rio

Rio de Janeiro, 04 de Março de 2009

All rights reserved

Guilherme Barreto Xavier

Guilherme B. Xavier graduated in Electrical Engineering at Pontifical Catholic University of Rio de Janeiro (PUC-Rio) in mid-2003, moving on to obtain the degree of Mestre in Engenharia Elétrica in 2005, in the field of modulation schemes for frequency encoded quantum key distribution. After starting his PhD, he went to KTH in Stockholm staying for one and a half years as an exchange PhD student. After return in the end of 2007, he carried on research in PUC-Rio to complete work for the PhD thesis. His research interests include (but are not limited to) quantum communications, quantum optics, and optical telecommunications metrology.

Bibliographic data

Xavier, Guilherme Barreto

Practical Assets for Fiber Optical Quantum Communications / Guilherme Barreto Xavier; advisor: Jean Pierre von der Weid. – 2009.

129 f. : il. ; 30 cm

Tese (Doutorado em Engenharia Elétrica)–Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2009.

Inclui bibliografia

1. Engenharia Elétrica – Teses. 2. Comunicações quânticas. 3. Distribuição Quântica de Chaves. 4. Fibras Ópticas. 5. Geração Quântica de Números Aleatórios. 6. Codificação em Polarização I. Weid, Jean Pierre von der. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Engenharia Elétrica. III. Título.

CDD: 621.3

Acknowledgements

To my advisor Jean Pierre von der Weid, for all the help, advice, friendship and discussions we had over these four years.

To Anders Karlsson, for welcoming me with open arms at KTH, and for all the nice talks and patiently explaining lots of cool stuff about entanglement and Sweden.

To my best friend and wife, Bruna, who has had the patience to endure me through the PhD, and who gave me priceless support.

A special thanks to my family specially my parents Alvaro and Luiza and my brother Bernardo, who always supported what I did and understood the sacrifices I had to make to get this work finally completed.

Many thanks to the people from the Optoelectronics group from CETUC/PUC-Rio: Djeisson, Janaína, Andy, Rogério, Tarcísio, Fernando, Marçal, Gustavo, Tito, Daniela and Douglas. Many thanks to Thiago, Giancarlo and Temporão who directly contributed to many of the results. A final thanks to Amalia, for all the help with the bureaucracy.

To the colleagues from KTH who received me very well, for providing a great working environment and who were always there for a friendly chat, Marcin, Qin, Christian, Simeon, Sebastian, Isabel, Maria, Johan, Rahul and Prof. Gunnar Bjork. A special thanks to Sèbastien for being a good friend, for advising me through the day-to-day work and for all the help settling in. A nice tap on the back to my new colleagues from Hefei, Wei and Tao. Last but not least, thanks to Walter from ACREO always ready to lend us equipment when we needed the most, specially the fiber splicer.

To Nino from the University of Geneva for the measurements done for the polarization-encoded QKD experiment. Many thanks to Profs. Hugo Zbinden and Nicolas Gisin for the helpful discussions and for the single-photon counting

module lent.

To all my friends who understood my absence during many months towards the end of the thesis. A special thanks to my sister-in-law Paula.

To everyone from LabSem in PUC-Rio, and to all the Professors and staff from CETUC and the Electrical Engineering department.

To CAPES and CNPq for the financial support.

This thesis was not a one-man work. A special thanks again to all those that contributed directly and indirectly to the results presented here!

Resumo

Guilherme Barreto Xavier. **Recursos Práticos para Comunicações Quânticas em Fibras Ópticas**. Rio de Janeiro, 2009. 129p. Tese de Doutorado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

As comunicações quânticas estão rapidamente integrando-se às redes de fibras ópticas, entretanto muitos desafios de engenharia ainda existem para essa aglutinação. Esta tese discute algumas soluções práticas para a melhoria de aplicações reais em comunicações quânticas em fibras ópticas. No primeiro experimento uma fonte de pares de fótons emaranhados não-degenerados, de banda-estreita, empregando conversão espontânea paramétrica descendente (CEPD) é utilizada para demonstrar a viabilidade da distribuição quântica de chaves (DQC) através de 27 km de fibras ópticas, com o canal de sincronismo presente na mesma fibra com uma separação de 0.8 nm em comprimento de onda. A outra demonstração utilizou uma fonte heráldica de fótons únicos também baseada em CEPD para a realização de DQC através de 25 km de fibras ópticas com a utilização do protocolo de decoy states pela primeira vez. Houve também um estudo dos impactos gerados por ruído Raman espontâneo causado por um canal óptico clássico presente na mesma fibra que o canal quântico. Um protocolo para gerar números verdadeiramente aleatórios em um sistema de DQC independente da taxa de transmissão do sistema é proposto, e um experimento prova-de-princípio demonstra a idéia. Finalmente um sistema de controle automático de polarização é utilizado para a realização de uma sessão de DQC através de 16 km de fibras ópticas utilizando codificação em polarização, mesmo sob a presença de um embaralhador rápido do estado de polarização.

Palavras-chave

Comunicações Quânticas, Distribuição Quântica de Chaves, Fibras Ópticas, Geração Quântica de Números Aleatórios, Codificação em Polarização.

Abstract

Guilherme Barreto Xavier. **Practical Assets for Fiber Optical Quantum Communications**. Rio de Janeiro, 2009. 129p. Tese de Doutorado - Departamento de Engenharia Elétrica, Pontifícia Universidade Católica do Rio de Janeiro.

Quantum communications is quickly becoming integrated within fiber optical networks and still many engineering challenges remain towards this interweaving. This thesis deals with some practical solutions toward improving real-world applications in quantum communications within optical fibers. In the first experiment, a non-degenerate narrowband entangled pair single-photon source based on spontaneous parametric down-conversion (SPDC) is used to show the feasibility of performing quantum key distribution (QKD) through 27 km of optical fiber, with the synchronization channel wavelength multiplexed in the same fiber with a channel spacing of just 0.8 nm. A second experiment uses a heralded single-photon source also based on SPDC to perform QKD over 25 km of optical fiber with the decoy state modification for the first time. Then there is a study of the problems caused by spontaneous Raman induced noise due to the presence of a classical signal in the same fiber as the quantum channel. A protocol to generate truly random numbers in a QKD setup independent of the system's transmission rate is proposed, and a proof-of-principle experiment demonstrates the idea. Finally an automatic polarization control system is used to perform a QKD session over 16 km of optical fiber using polarization encoding, even in the presence of a fast polarization scrambler.

Keywords

Quantum Communications, Quantum Key Distribution, Fiber Optics, Quantum Random Number Generation, Polarization Encoding.

Summary

1	Introduction	18
2	An Introduction to Quantum Communications	20
2.1.	Introduction	20
2.2.	Quantum physics and information	21
2.3.	Qubits	23
2.4.	Single-photon sources	25
2.4.1.	Non-linear optics	27
2.4.2.	Entangled single-photon pair sources	31
2.4.3.	Generation of single-photon pairs in optical fibers	35
2.5.	Single-photon detectors	36
2.6.	The quantum communication channel	39
2.6.1.	Optical fibers	41
2.7.	Quantum Key Distribution	44
2.7.1.	No-cloning theorem	47
2.7.2.	BB84	49
3	Integration within Classical Networks and the Decoy State Implementation	53
3.1.	Narrowband entangled photon pair source used in a DWDM environment	53
3.2.	Experimental QKD with a Heralded Single-Photon Source and the Decoy State Modification	62
4	Raman Noise and Random Number Generation	76
4.1.	Simultaneous Classical and Quantum Communications in Optical Fibers	76
4.2.	Quantum Random Number Generation Protocol	85

5	Transmission of Polarization Encoded Qubits in Optical Fibers	99
5.1.	Introduction	99
5.2.	Control theory	100
5.3.	The experiment	101
6	Conclusions and future developments	111
7	Bibliography	114

Figure list

- Figure 1 - Typical elements of a communication system. Information (represented here in its most usual form, binary digits) is modulated into an appropriate form for transmission through a communication channel by Alice. Bob demodulates it obtaining the same information Alice transmitted (in the absence of errors). 21
- Figure 3 - Two optical fields with frequencies ω_1 and ω_2 combining in a non-linear medium to produce ω_3 . 28
- Figure 4 - A periodically poled crystal. The signs indicate where the non-linearity $\chi^{(2)}$ is negative and positive. Shown are also the input optical field ω_p and the outputs ω_s and ω_t . 30
- Figure 5 - Generation of the maximally entangled state $|\psi\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle + e^{i\phi}|V\rangle|H\rangle)$ employing two non-linear crystals, with the pump polarization oriented at 45° . 33
- Figure 6 - Scheme for a Franson-type interferometry setup. EPS: Entangled photon source; L and S: Long and short interferometer arms respectively; D_x : Single photon detectors; ϕ_x : Phase shifters. 35
- Figure 7 - Part a) shows the circuit used to detect single photons in passive mode, while part b) is the circuit for passive gated mode operation. Capacitor C_g in part b) is used to decouple the DC voltage between the circuit and the pulse generator. 38
- Figure 8 - Typical current-voltage curve for an avalanche photo-diode. V_A is the breakdown voltage and V_G is the amplitude of the gate pulse applied. The red circle shows where the diode is placed for the gate pulse's duration. 39
- Figure 9 - Basic optical fiber structure. The protection coatings have been omitted from the figure. Right part is simply the profile view of the fiber. 42
- Figure 10 - Birefringence in an optical fiber is a function of mechanical stresses and temperature fluctuations along its length, causing random polarization

- rotations of an input polarization state. We see in the figure for example, a vertical state randomly transforming into a circular state after propagation. 44
- Figure 11 - Scheme of Vernam's cipher. Note that we used a trusted courier as the secure channel here, which in principle is not a good choice. Adapted from [72]. 46
- Figure 12 - BB84 protocol. PBS: Polarizing beam splitter. Adapted from [72]. 51
- Figure 13 - Entangled single-photon pair source used in the DWDM experiment. HWP: Half-wave plate; BSF: Band-stop filter; DM: Dichroic mirror; BS: Beamsplitter; PBS: Polarizing beamsplitter; FC: Fiber coupler. 55
- Figure 14 - Complete experimental setup. SPAD: Single photon avalanche detector; DG: Delay generator; DFB-EA: Distributed feedback laser with electro-absorption modulator; FBG: Fiber Bragg grating; WDM: Wavelength division multiplexer; SMF: Single-mode fiber; PC: Polarization controller; PD: Photo-diode; TDC: Time-discriminator circuit. Black lines represent optical fibers, red lines account for electrical connections, and the blue one is free-space. 58
- Figure 15 - Spectrum for the 1555 nm down-converted photons, obtained for horizontal polarization without conditional gating at 809 nm. The FWHM is approximately 0.8 nm. Background is the noise level from the optical spectrum analyzer. 60
- Figure 16 - Visibility curves using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal photons (H, V, D and A). Curves show a best fit. 61
- Figure 17 - Visibility curves after 27 km of single-mode fiber using coincidence counts as a function of the idler half-wave plate setting for each of the four polarization states of the signal (H, V, D and A). Curves show a best fit. 62
- Figure 18 - PNS attack scheme. Adapted from [72]. 64
- Figure 19 - Heralded single photon source used in the experiment. PPLN: Periodically-poled lithium niobate crystal; DM: Dichroic mirror; F: Filter; FC: Fiber coupler with aspheric lens and multi-axis translation stage; TC: Time chopper; CP: Counter and processing. Green, blue and red arrows represent pump, signal (809 nm) and idler (1555 nm) respectively. A HWP is used to adjust the pump polarization before the crystal (not shown). 67

- Figure 20 - Picture of part of the source. The pump laser, electronics and detectors are not shown. 70
- Figure 21 - Numerical simulation for the key generation rate vs total loss for the following schemes: a) WCS source without decoy state; b) HSPS without decoy state; c) WCS with decoy state method (optimal values for used for each point); d) HSPS with decoy state with $P^{cor} = 30\%$, $\mu = 5.88 \times 10^{-4}$ and $\mu' = 5.53 \times 10^{-3}$, values taken from our source characterization; e) HSPS with decoy state and with $P^{cor} = 70\%$, and μ and μ' values as before; f) the ideal single-photon source. 70
- Figure 22 - Complete experimental setup of QKD with an HSPS using the decoy state method. AOM: Acousto-optical modulator; PPLN: Periodic poled lithium niobate; WDM: Wavelength division multiplexer; OS: Optical switch; TC: Time chopper; BS: Beam splitter; PM: Phase modulator; FM: Faraday mirror; CB: Control board; DL: Delay line; SPD Single photon detector. 71
- Figure 23 - Spectrum of the down-converted idler photons with (red) and without (black) WDM filter. 73
- Figure 24 - Theoretical curves for the coincidence count rate (dotted blue line) and final secure key rate (dashed red line). The dots and squares are the experimental results at a total loss of 31 (optical fiber removed) and 36 dB (25 km of spooled SMF-28 fiber connected). 75
- Figure 25 - Experimental setup to investigate noise generated from Raman spontaneous scattering. SPAD: Single photon avalanche detector; DWDM: Dense wavelength division multiplexer. The Bragg grating center wavelength is 1546.12 nm. 77
- Figure 26 - Count probability per 1 ns gate for 1 mW (0 dBm) of input CW optical power as a function of the tunable laser wavelength. Dark counts have been subtracted. 79
- Figure 27 - Count probability per 1 ns gate for the counter propagating setup for 8 km of DS fiber as a function of input power and wavelength. 80
- Figure 28 - Spectra of each DWDM channel measured with a tunable laser source and an optical spectrum analyzer. 81
- Figure 29 - Setup for characterizing co-propagating Raman noise. 82

- Figure 30 - Count probability per 1ns gate for 1mW (0dBm) of input CW optical power as a function of the tunable laser wavelength. Dark counts + counts from cross-talk have been subtracted. 83
- Figure 31 - Scheme for QKD with an entangled-photon source based on the E91 protocol. PBS: Polarization beam splitter; PM: Polarization modulator; EPS: Entangled photon source. 88
- Figure 32 - Schematics of our proposal applied to the Ekert (E91) protocol. Black arrows represent optical connections, while blue and red ones depict electrical cables. EPS - Entangled photon source; PM - Polarization modulator; PBS - Polarizing beam splitter; SPCM - Single photon counting module. The master clock synchronizing Alice and Bob, as well as QKD electronics are omitted for the sake of clarity. b) Illustrative representation of the waveforms from the detection and clock pulses. 89
- Figure 33 - Measured histogram of the number of time slots between two consecutive successful detections for $\mu = 0.1$. 93
- Figure 34 - Normalized auto-correlation for the random sequence generated from the distribution from Fig. 33. 94
- Figure 35 - Experimental setup: ATT: Optical attenuator; HWP: Half-wave plate; M: Mirror; L: Lens; PPLN: Periodically-poled lithium niobate; P: Prism; FC: Fiber coupler, here consisting of a multi-axis translation stage (not shown here), RG 715 high-pass filter, 11 mm focal length aspheric lens and fiber holder; SMF: 780 nm single mode optical fiber; APD: Avalanche photon detector; A/D: Analog to digital converter. The green, red and blue arrows represent the pump, idler and signal beams respectively. The dashed lines represent electrical cables. 96
- Figure 36 - P-values plotted for the NIST test suite individual tests for the 20 million bit generated sequence after bias removal. Each dot represents a run of 1 million bits for a particular test. The results are all above the confidence value for cryptography applications. The tests are: 1 - Frequency; 2 - Block frequency; 3 - Cumulative-sums forward; 4 - Cumulative-sums reverse; 5 - Runs; 6 - Longest runs; 7 - Rank; 8 - DFFT; 9 - Universal; 10 - Approximate entropy; 11 - Serial 1; 12 - Serial 2; 13 - Linear complexity. 97

Figure 37 - Schematics showing the I_TU-T frequency grid (dashed black lines), the control channels (red) and the quantum channel (blue). 101

Figure 38 - Experimental setup for the polarization encoded QKD experiment. QKD-A and QKD-B: Alice and Bob's computers; FPGA: Field programmable gate array; D_S , D_1 and D_3 : Classical detectors; FBG: Fiber Bragg grating; PC-A and PC-B: Alice and Bob's LiNbO₃ polarization controllers; ATT: Optical attenuator; DWDM: Dense wavelength division multiplexer; P_1 and P_3 : Polarizers; BPF: Band-pass filter; PBS: Polarizing beam splitter; SPCM: Single photon counting module. APCS: Automatic polarization control system. Solid lines represent optical fibers, while dashed ones are electrical connections. The direction of pulses is indicated in the figure. 102

Figure 39 - Picture of the prototype. Clearly visible are the optical components: The polarization controllers, polarizers, detectors and the DWDMs. The electronics (power supplies, drivers and control CPU) are underneath the optics and thus not shown. 103

Figure 40 - Emission spectra of the two polarization control lasers (red), quantum channel laser (blue) and synchronization laser (black) aligned to 4 adjacent channels of the ITU-T band between 1545.32 and 1547.72 nm. The transmission spectra of the respective DWDM channels are shown as grey lines. Measurement performed by N. Walenta. 104

Figure 41 - Zoomed version of Fig. 27. The three arrows at the bottom represent the classical and quantum channels. 105

Figure 42 - Intensity measurements of a polarization pulse (black), and the quantum channel signal (red), operating on classical power levels. The polarization pulse was taken after a polarizer, with a CW laser, while switching the SOP between two orthogonal values, and back to the original. The quantum channel pulse is included here as a reference, showing that it is much narrower than the polarization bit. Measurement performed by N. Walenta. 106

Figure 43 - The optical share $QBER_{opt}$ as a function of the scrambling frequency demonstrating the stabilization capability of the control system under rapid polarization changes. Each value is averaged over 50 measurements, with 1

million photon pulses sent per measurement. Measurement performed by N. Walenta. 109

Figure 44 - QBER as a function of time under different conditions. a) No polarization scrambling. b) Polarization scrambling with active stabilization. c) Polarization scrambling without stabilization system. d) Re-stabilization after the system is reactivated. Each point corresponds to 1 million sent qubits. Black and red points distinguish measurements in different bases at Bob (see text for details). Measurement performed by N. Walenta. 109

Abbreviation list

ADSL - Asynchronous Digital Subscriber Line
AOM - Acousto-Optical Modulator
APD - Avalanche Photo-Diode
APCS - Automatic Polarization Control System
ASE - Amplified Spontaneous Emission
AWG - Array Waveguide Grating
BSF - Band Stop Filter
CHSH - Clauser Horne Shimony Holt
CW - Continuous Wave
DFB - Distributed Feedback
DG - Delay Generator
DM - Dichroic Mirror
DPSS - Diode Pumped Solid State
DS - Dispersion-Shifted
DWDM - Dense Wavelength Division Multiplexing
EA - Electro-Absorption
EPR - Einstein Podolsky Rosen
FBG - Fiber Bragg Grating
FC - Fiber Coupler
FM - Faraday-Michelson
FPGA - Field Programmable Generator Array
FWM - Four Wave Mixing
FWHM - Full Width at Half-Maximum
GHZ - Greenberger Horne Zeilinger
HSPS - Heralded Single Photon Source
HWP - Half Wave Plate
MZ - Mach-Zehnder
PBS - Polarizing Beam Splitter
PCF - Photonic Crystal Fiber
PD - Photo Diode
PMF - Polarization Maintaining Fiber
PNS - Photon Number Splitting

PPLN - Periodically Poled Lithium Niobate
QBER - Quantum Bit Error Rate
QIT - Quantum Information Theory
QKD - Quantum Key Distribution
QRNG - Quantum Random Number Generator
SOP - State of Polarization
SPAD - Single-Photon Avalanche Diode
SPDC - Spontaneous Parametric Down-Conversion
TC - Time Chopper
TDC - Time-Discriminator Circuit
WCP - Weak Coherent Pulse
WCS - Weak Coherent State
WDM - Wavelength Division Multiplexing
XPM - Cross Phase Modulation