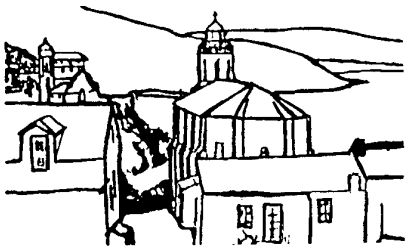


The European Commission

High-level Scientific Conferences

INSTITUT D' ÉTUDES SCIENTIFIQUES DE CARGÈSE
20130 Cargèse, Corse (France)
http://cargese.univ-corse.fr

This conference is supported by the European Commission (High Level Scientific Conference), QUIPROCONE (Network of Excellence), CNRS, DGA, the U.S. Army Research Laboratory (European Research Office), and the USAF European Office of Aerospace Research and Development.

QUICK

Quantum interference and cryptographic keys: novel physics and advancing technologies

CARGÈSE, CORSICA, FRANCE, April 7-13, 2001

Organising committee :

Philippe Grangier (CNRS/IOTA, Orsay, France)
John Rarity (DERA, Malvern, United Kingdom)
Anders Karlsson (KTH, Stockholm, Sweden)

R&D 9073-PH-02
N68171-01-M-5350

Conference WWW site: **http://www.ele.kth.se/QEO/QUICK/**

The I.E.S.C. is affiliated to Centre National de la Recherche Scientifique, Université de Corse and Université de Nice-Sophia Antipolis. It is sponsored by MENESR, CNRS and CTC.
Director : Élisabeth Dubois-Violette, tel. : (33) 1 69 15 61 01, dubois-violette@physol.lps.u-psud.fr
Institute phone number : tel. : (33) 4 95 26 80 40 or (33) 4 95 26 80 48, fax : (33) 4 95 26 80 45

Welcome to Cargèse

The conference "Quantum interference and cryptographic keys : novel physics and advancing technologies (QUICK)" has been organised at the initiative of the european Quantum Cryptography projects QuComm, S4P, QuiCov, EQUIS and EQCSPOT, in the framework of the European Union IST/FET/QIPC program.

Its goal is to provide a forum for scientific exchanges for one hundred researchers and students, from academia and industry, working world-wide on the physics, implementations, and applications of quantum communications.

We acknowledge specific support for this conference, which has been granted by the European Commission (High Level Scientific Conference), QUIPROCONE (Network of Excellence), CNRS, DGA, the U.S. Army Research Laboratory (European Research Office), and the USAF European Office of Aerospace Research and Development.

The conference format consists of general talks (40 mn + 5 mn discussions), invited talks (25 mn + 5 mn discussions), and two poster sessions for contributed papers. Ample time is provided for informal discussions during the afternoons.

We hope you will enjoy the conference in the special working and cooperative atmosphere of Cargèse. In case you have any questions do not hesitate to contact one of us.

Philippe Grangier

John Rarity

Ander Karlsson

DAY	9:00 - 9:45	9:45 - 10:30	10:30 - 11:00	11:00 - 11:45	11:45 - 12:15	12:15 - 16:00	16:00 - 16:30	16:30 - 17:00	17:00- 17:30	17:30 - 18:00	18:00 - 18:30	18:30-19:00 (+ evening)
Saturday			TRAVEL							Welcome - Apéritif		
	Quantum Cryptography : basics (P. Grangier)						Quantum Cryptography : technology and implementations (A. Karlsson)					
Sunday	open N. Gisin	A. Karlsson	Coffee Break	H. Zbinden	G. Buller	LUNCH & Discussion	C. Kurtseifer	G. Bonfrate	Coffee Break	J.P. Goed-gebuer	D. Bethune	V. Berger
	Cavity QED and trapped particles (E. Giacobino)						New ideas in quantum communications 1 (N. Gisin)					
Monday	M. Brune	G. Rempe	Coffee Break	J. M. Gérard	P. Grangier	LUNCH & Discussion	N. Lütken-haus	N. Imoto	Coffee Break	V. Vedral	D. Mayers	Posters 1 Buffet Supper
	New ideas in quantum communications 2 (J. Rarity)											
Tuesday	J. Shapiro	H. Yuen	A. Kent	Coffee Break	H. Aschauer	P. Dumais	LUNCH and Free Afternoon					Conference Dinner
	Free space cryptography (H. Zbinden)						Parametric processes and fluorescence (E. Polzik)					
Wednesday	R. Hugues	J. Rarity	P. Edwards	Coffee Break	G. Gilbert	W. Tittel	LUNCH & Discussion	D. Bouw-meester	A. Sergienko	Coffee Break	S. Tanzilli	A. Lvovsky	Posters 2 Buffet Supper
	Quantum continuous variables (J. Shapiro)						Single photon sources (J. Rarity)					
Thursday	E. Polzik	E. Giacobino	Coffee Break	G. Leuchs	N. Cerf	LUNCH & Discussion P. Zarda	R. Brouri	B. Barnes	Coffee Break	B. Gayral	M. Pelton	V. Zwiller
Friday						TRAVEL						

Saturday April 7 : Arrival day	
17 :30-20 :00	Welcome + aperitif

Sunday April 8	
Session 1 : Quantum Cryptography basics (Chairman : P.Grangier)	
9:00 - 9:15	Conference opening
9 :15 - 10:00 *SuM1*	Quantum cryptography : from basic physics to applications N. Gisin
10:00 - 10 :30 *SuM2*	Long Wavelength Quantum Cryptography A. Karlsson
10:30 - 11:00	**Coffee break**
11:00 - 11:45 *SuM3*	Faint laser versus entangled photons Quantum Key Distribution H. Zbinden
11:45 - 12:15 *SuM4*	Enabling technologies for Quantum Key Distribution systems Gerald Buller
12:15 - 16:00	**Lunch and free time for discussions**
Session 2 : Quantum Cryptography : technology and implementations (A. Karlsson)	
16:00 - 16:30 *SuA1*	Technologies for quantum cryptography C. Kurtseifer
16:30 - 17:00 *SuA2*	Asymmetric Mach-Zehnder channel waveguide interferometers for Quantum communication system G. Bonfrate
17:00 - 17:30	**Coffee break**
17:30 - 18:00 *SuA3*	Single Side Band Modulation of Light For Quantum Key Distribution J.P. Goedgebuer
18:00 - 18:30 *SuA4*	An Autocompensating Quantum Cryptography System D. Bethune
18:30 - 19 :00 *SuA5*	Semiconductor twin photon sources : towards integrated quantum optics V.Berger
19 :00 -	**Free evening**

Monday April 9	
Session 3 : Cavity QED and trapped particles (Chairman : E. Giacobino)	
9 :00 - 9 :45 *MoM1*	Entanglement engineering with quantum gates in a cavity QED experiment M. Brune
9 :45 - 10 :30 *MoM2*	Towards quantum communications with strongly coupled atoms G. Rempe
10:30 - 11:00	**Coffee break**
11:00 - 11:45 *MoM3*	Quantum dots in 3D microcavities: CQED effects and application to single photon sources J.M. Gérard
11:45 - 12:15 *MoM4*	Single atoms in microscopic dipole traps : towards quantum gates ? P. Grangier
12:15 - 16:00	**Lunch and free time for discussions**
Session 4 : New ideas in quantum communications 1 (Chairman : N. Gisin)	
16:00 - 16:30 *MoA1*	Practical quantum key distribution and security analysis N. Lütkenhaus
16:30 - 17:00 *MoA2*	Quantum technology and protocols other than QKD N. Imoto
17:00 - 17:30	**Coffee break**
17:30 - 18:00 *MoA3*	Entanglement purification in quantum cryptography V. Vedral
18:00 - 18:30 *MoA4*	Unconditional security in quantum cryptography D. Mayers
18:30-	**Poster Session I + Buffet Dinner**

Tuesday April 10	
Session 5 : New ideas in quantum communications 2 (J. Rarity)	
9 :00 - 9 :45 *TuM1*	Architectures for Long-Distance Quantum Communication J. Shapiro
9 :45 - 10 :15 *TuM2*	Unconditionally Secure Quantum Bit Commitment H. Yuen
10:15 - 10:45 *TuM3*	Relativistic cryptography FAQ's A. Kent
10:45 - 11:15	**Coffee break**
11:15 - 11:45 *TuM4*	Unconditionally secure quantum communication using entanglement-based quantum repeaters H. Aschauer
11:45 - 12:15 *TuM5*	Quantum bit commitment from any quantum one-way permutation. P. Dumais
12:15 - 18:00	**Lunch and conference excursion**
19:30-	**Conference dinner**

Wednesday April 11	
Session 6 : Free space cryptography (Chairman : H. Zbinden)	
9 :00 - 9 :45 *WeM1*	Atmospheric Quantum Key Distribution in Daylight: ground-based experiments and prospects for satellite communications R. Hughes
9 :45-10 :15 *WeM2*	Free space quantum cryptography J. Rarity
10:15 - 10 :45 *WeM3*	Free-space QKD trials at Mt Stromlo, Australia P. Edwards
10:45 - 11:15	**Coffee break**
11:15 - 11:45 *WeM4*	High speed quantum cryptography SATCOM G. Gilbert
11:45 - 12:15 *WeM5*	Time-bin entangled photon pairs & applications in quantum cryptography W. Tittel
12:15-16:00	**Lunch and free time for discussions**
Session 7 : Parametric processes and fluorescence (E. Polzik)	
16:00-16:30 *WeA1*	An entangled photon laser : prospects and applications D. Bouwmeester
16:45-17:15 *WeA2*	Hyperentanglement in Parametric Down-Conversion A. Sergienko
17:15-17:30	**Coffee break**
17:30-18:00 *WeA3*	Highly efficient photon-pair source using PPLN waveguide S. Tanzilli
18:00-18:30 *WeA4*	Synthesis, manipulation and measurement of highly non-classical photon states A. Lvovsky
18:30-	**Poster Session II + Buffet Dinner**

Thursday April 12	
Session 8 : Quantum continuous variables (J. Shapiro)	
9 :00 - 9 :45 *ThM1*	Entanglement and communication via teleportation between macroscopic atomic spin samples E. Polzik
9 :45 - 10 :30 *ThM2*	Quantum state transfer from light fields to atomic ensembles E. Giacobino
10:30 - 11:00	**Coffee break**
11:00 - 11:45 *ThM3*	The generation of bright entangled light and its applications G. Leuchs
11:45 - 12:15 *ThM4*	Optimal Cloning and Anticloning of continous quantum variables N.Cerf
12:15 - 15:30	**Lunch and free time for discussions**
Session 9 : Single photon sources (J. Rarity)	
15:30 - 16:00 *ThA1*	An all-solid state source for single photons P. Zarda
16:00 - 16:15 *ThA2*	Photon antibunching from diamond microcrystallites R. Brouri
16:15 - 16:45 *ThA3*	Collecting the 'one photon' B. Barnes
16:45 - 17:15	**Coffee break**
17:15 - 17:45 *ThA4*	Single photons from single quantum boxes B. Gayral
17:45 - 18:15 *ThA5*	Triggered single photons and entangled photons from a quantum dot microcavity M. Pelton
18:15 - 18:45 *ThA6*	Antibunched emission from single self-assembled quantum dots V. Zwiller

Friday 13 : Departure day

Poster Session 1 : Monday April 9

M 1	Alves Carolina	Quantum correlations between two trapped electrons
M 2	Angelakis Dimitris	Testing Bell Inequalities in Photonic Crystals
M 3	Atature Mete	Hyperentanglement in parametric down-conversion
M 4	Beveratos Alex	Single Photon source from NV centers in diamond
M 5	Bourennane Mahamed	Quantum key distribution with N-array encoding
M 6	Castelletto Stefania	Experimental limits in QC systems based on polarization entangled photons
M 7	Couteau Christophe	Twin photon production by quasi phase matching with PPLN
M 8	Curty Marcos	Secure Authentication of classical messages with a 1-ebit quantum key
M 9	Durkin Gabriel	Exploring Multi-Photon Entanglement
M 10	Eibl, Marcus	New Entangled Multiphoton state
M 11	Grosshans Frederic	Quantum noise analysis using pulsed quantum tomography methods
M 12	Hennrich Marcus	Vacuum stimulated photon generation in a high finesse optical cavity
M 13	Hiskett Phil	80km transmission test of a quantum cryptography receiver at 1.55mm
M 14	Hunter Kieran	General 3 element POM for light polarisation measurements
M 15	Iblisdir Sofyan	Optimal M-to-N cloning and phase conjugation for continous variables
M 16	Jennewein Thomas	A Fiber Optic Bell State Analyzer
M 17	Jonsson Per	Dye molecules in a microcavity - photostability and extraction efficiency
M 18	Josse Vincent	Spin squeezing in atomic systems
M 19	Korolkova Natalia	Continuous Variable Polarization Entanglement and Key Distribution

Poster Session 2 : Wednesday April 11

W 1	Lamas-Linares Antia	Stimulated Parametric Down-Conversion
W 2	Ljunggren Daniel	Abstract missing
W 3	Longchambon Laurent	Production of EPR beams using self-phase locking
W 4	Lorenz Stefan	Squeezed State Entanglement for Free Space Quantum Cryptography
W 5	Makarov Vadim	High speed quantum key distribution experiment
W 6	Mueller-Quade Joern	Quantum Secure multiparty computations
W 7	Navez Patrick	Quantum public key scheme using continuous variables
W 8	Orlowski Arkadius	Teleportation of entanglement
W 9	Orlowski Arkadius	Quantum visual cryptography
W 10	Parker Steve	Abstract missing (Simulating Entanglement in Shor's algorithm)
W 11		withdrawn
W 12	Pellegrini Sara	Characterisation of InGaAs/InP APDfor Quantum Cryptography Systems
W 13	Rallan Luke	Abstract missing
W 14	Robert Isabelle	Single InAs/GaAs Quantum dot in Pillar Microcavities
W 15	Schori Christian	Frequency tunable EPR-correlated optical fields
W 16	Stefanov Andre	Plug&Play long distance quantum key distribution prototype
W 17	Tanzilli Sebastien	Highly efficient photon-pair source using a PPLN waveguide
W 18	Varoutsis Spyros	Long wavelength single photon sources from InGaAs quantum dots.
W 19	Virmani S S	How to optimally distinguish two pure states locally
W 20	Zwiller Valery	Antibunched photon emission from single self assembled quantum dots

TALKS

Quantum Cryptography: from basic physics to applications

Nicolas Gisin, GAP, Geneva

The landscape of quantum cryptography extends from basic questions in quantum physics to real life applications. Physicists, working in the field, enjoy thus a magnificent view, but also have to face the difficulties inherent to any multidisciplinary research field. For example, questions on the security of quantum cryptography have to be analyzed from different perspectives, depending whether one is primary interested in the foundations or in their applications. In this overview talk, several open questions ranging from abstract to concrete QC will be discussed.

Long Wavelength Quantum Cryptography : A discussion on some issues

Anders Karlsson, Mohamed Bourennane and Daniel Ljunggren

KTH, Sweden

For quantum cryptography to be extended to long distances, beyond 50 km, we need to work in the long wavelength telecom window of 1550nm. Several labs, among them labs represented at the QUICK meeting are adressing this problem and slowly, but steadily progress is being made. The main limitation so far has been the not-too-good performance of InGaAs APDs at 1550nm, and here we will discuss some of our results on evaluating InGaAs APDs from various manufacturers, as well as present some systems results. In the presentation, to fuel further discussions at the meeting, we will also discuss quantum cryptography in a more general context, adressing "ultimate" limits on the extension of quantum cryptography, security issues as well as issues pertaining to a possible commercialisation of quantum cryptography in a near term context.

Faint laser vs. entangled photon QKD : An analysis taking into account "realistic" eavesdroppers.

Hugo Zbinden, GAP, Geneva

Faint laser QKD has been demonstrated by several groups and user-friendly prototypes will be available soon. However, it has been argued that multi-photon pulses are a serious threat on the security of those systems.

In this talk, we first present a QKD-setup relying on energy-time entangled photon pairs in optimised for long distance transmission. It is based on a Franson type set-up and uses a protocol analogous to BB84. We show that this system is immune to multi-photon attacks. We examine the noise sources and practical difficulties associated with entangled states systems.

Secondly, we discuss the technological possibilities of a realistic eavesdropper. Eavesdropping strategies taking profit of multi-photon pulses in faint laser QKD are presented. We conclude that as long as storage of Qubit is technically impossible, faint laser QKD is not limited by security issues, but mostly by the detector noise.

Enabling Technologies for Quantum Key Distribution Systems

Gerald S. Buller

Department of Physics
Heriot-Watt University
Riccarton
Edinburgh EH14 4AS
United Kingdom

G.S.Buller@hw.ac.uk

This paper will describe enabling technologies for quantum key distribution systems and their implementation in several demonstrator experiments. Such work has been the basis of the European collaborative EQUIS programme and results from several laboratories will be reported.

We will describe progress in the use of single-photon counting detectors in terms of spectral coverage, jitter, efficiency, dark noise and repetition rate limitations. This discussion will include commercially-available linear multiplication avalanche diodes operated in Geiger mode as well as devices specifically designed for single photon detection. Other vital issues such as such as sources, data acquisition cards, planar waveguide interferometers and clocking techniques will be presented.

Other spin-off applications of these enabling technologies will be discussed: including ultra-sensitive time-resolved fluorescence measurements and time-of-flight ranging using photon-counting techniques.

Tools for practical Quantum cryptography

Ch. Kurtsiefer, S. Mayer, M. Halder, P. Zarda, and H. Weinfurter
Sektion Physik der LMU Muenchen
Max-Planck-Institut fuer Quantenoptik, Garching, Germany

Since the introduction of quantum cryptography by Bennet et al. [1], a large number of experimental realizations were reported, both for the originally proposed scheme of encoding information into the polarization of single photons as well as coding schemes into different degrees of freedom [2]. Also, protocols using entangled photon pairs have been suggested [3] and demonstrated experimentally [4,5]. Although all these techniques offer various technical advantages, the original proposal seems still the simplest realization of a secure key exchange technique.

In this contribution, we want to report on an experimental realization of a BB84-type cryptography system, where the aim was to reduce size and adjustment needs to an absolute minimum. The source is comprised by four laser diodes, each generating faint light pulses for a particular polarization containing a fraction of a photon, which are sent along the the optical channel -- either a single mode optical fiber or a free space propagation mode [6]. Thereby we not only avoid the need for fast modulators, but also were able to reduce the size of the transmitter to several cm^3, compatible with nowadays communication equipment. On the receiver side, we use a 'coin-tossing' beam splitter [7] to randomly choose a detection basis (HV or +-45°) for the photon, and a parallel detection scheme to register photon events in all four base states H, V, +45°, and -45°. This allowed us to reduce the receiver optical setup to an equally small size. Whereas the random choice on the detection base in the receiver is provided by the physical property of a beam splitter, there is still a need for a fast local source of random numbers on the transmitter side in a BB84 protocol. In our setup, we use a physical process to create random bits with a rate of 20 MHz. These bits determine the settings of the polarization of the transmitted photons by choosing which of the four laser diodes is switched on for each pulse.

[1] C.H. Bennet, G. Brassard, Proc. Int. Conf. Computer Systems and Signal Processing, Bangalore, pp. 175 (1984).
[2] A. Muller et al, Appl. Phys. Lett. 70, 793 (1997).
[3] A.K. Ekert, Phys. Rev. Lett., 67, 661 (1991).
[4] A.K. Ekert et al, Phys. Rev. Lett., 69, 1293 (1992).
[5] T. Jennewein et al, Phys. Rev. Lett., 84, 4729 (2000).
[6] S. Chingga, P. Zarda, T. Jennewein, H. Weinfurter, Appl. Phys. B 69, 389 (1999).
[7] J.G. Rarity, P.C.M. Owens, P.R. Tapster, J. Mod. Optics 41, 2345 (1994).

Asymmetric Mach-Zender channel waveguide interferometers for Quantum Key Distribution Systems

Gabriele Bonfrate*, Mike Harlow, Colin Ford, Graeme Maxwell, and Paul D Townsend

Corning Research Centre, Adastral Park, Martlesham Heath
Ipswich, Suffolk, IP5 3RE, UK
**Electronic Address: bonfrateg@corning.com*

Quantum Cryptography, or as they are more properly called Quantum Key Distribution (QKD) systems, enable two legitimate parties to securely generate and share a secret key that can be used for the encryption, and subseqsuent decryption, of sensitive data transmitted over an open communication channel [1]. Although it is in principle possible to realise Quantum Cryptography using entangled particles, practical implementations of QKD to date have mainly comprised schemes based on the quantum properties of single photons or weak coherent states which are transmitted along an optical fibre: typically the key is encoded in the polarisation or the phase of the photons.

In the case of optical fibre based QKD systems, phase encoding, employing Mach-Zender type interferometers, has been generally implemented [2,3,4]. However these interferometers are typically expensive, bulky and relatively complex devices to fabricate. In addition, Mach-Zender designs often show a limited environmental stability due to the relatively long separate fibre paths employed (typically several metres) [2,4]. Fibre-based interferometers may not be suitable candidates, therefore, for practical QKD systems.

In this presentation we describe a new miniaturised version of channel waveguide Asymmetric Mach-Zender (AMZ) interferometers, which are suitable for the afore mentioned phase encoding in an integrated rather than an optical fibre structure, with improved compactness, stability and ruggedness. The device design and fabrication process will be discussed, addressing the advantages and the novelties involved.

Each AMZ was carefully characterized from the point of view of insertion loss, which may limit the QKD system span, and some were also linked in pairs in a combined interferometric system suitable for the implementation of the B92 protocol [5]. The fringe visibility of the system, related to the QBER performance, was then measured using a fast PIN receiver and an InGaAs APD operated in Geiger mode, obtaining values as high as 99% and typically 98%, for an estimated QBER of 1-2%.

[1] C.H. Bennett and G. Brassard, Proceedings of the IEEE international conference on computers, systems and signal processing, 1984, Page 175-179

[2] C. Marand and P.D. Townsend, *"Quantum key distribution over distances as long as 30km"*, Optics Letters, **20** (16), Page 1695-1697, (1995)

[3] G. Ribordy, J-D Gautier, N. Gisin, O. Guinnard and H. Zbinden, *"Automated 'plug & play' quantum key distribution"*, Electronics Letters, **34** (22), Page 2116-2117, (1998)

[4] R.J. Hughes, G.G. Luther, G.L. Morgan and C. Simmons, *"Quantum cryptography over 14km of installed optical fibre"*, in Proc. 7th Rochester Conf. On Coherence and Quantum Optics (J. H. Eberly, L. Mandel and E. Wolf, Eds.), pp. 103-112, Plenum Press, New York, 1996

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, *"Experimental quantum cryptography"*, Journal of Cryptology, 5 (1), Page 3-28, (1992)

Single-photon interference with a single sideband modulation scheme.

J. -M. Merolla, L. Duraffourg, J. -P. Goedgebuer[1].

GTL-CNRS Telecom, Georgia-Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France.

[1]Lab. Optique P.M. Duffieux, UMR CNRS 6603, Université de Franche-Comté, 25030 Besançon Cedex, France.

The practical quantum key distribution schemes, allowing transmissions more than 20 km reported thus far, have their technical basis in the polarization of photons [1] or in the use of optical delays [2]. We propose a new approach, based on a single-sideband (SSB) modulation scheme, that allows the BB84 protocol to be used in a robust scheme for quantum cryptography and eliminates both polarization and path-delay maintenance problems. In this method, the sender, Alice, uses an unbalanced integrated Mach-Zehnder modulator with a $\lambda/4$-optical path difference bias. This modulator is driven by a voltage-controlled oscillator (VCO) for which the electrical phase alternates randomly between four values that form two non-orthogonal bases (BB84 scheme). At the receiver, Bob uses a second unbalanced integrated Mach-Zehnder modulator MZ_2 with a $3\lambda/4$-optical path difference bias driven by a second VCO with two other phases. We have demonstrated that single-photon interference can occur in the sidebands produced by the two modulators and that the probability of detecting a photon in these two sidebands are complementary, depending on the relative phase difference between the sender and the receiver. The many potential advantages of SSB modulation and of the use of integrated optics technology make the method described a very promising alternative to other schemes. Such a scheme provides high mechanical stability against environmental perturbations and can be made polarization-independent by use of a polarization-independent-modulator at the receiver.

[1] C. H. Bennett, F. Bessette, G. Brassard, and L. Salvail, J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, vol. 3, no 5, pp. 3-28, 1992 ; A. Muller, H. Zbinden, N. Gisin, "Quantum cryptography over 23 km in installed under-lake telecom fibre", *Europhysics Letters*, 33, pp.335-339, 1996.

[2] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Single photon interference in 10 km long optical fibre interferometer" ; C. Marand and P. D. Townsend, "Quantum cryptography over distances as long as 30 km", *Optics Letters*, vol. 20, no 16, p.1695, 1995.

An Autocompensating Quantum Cryptography System

Donald S. Bethune and William P. Risk

IBM Almaden Research Center, 650 Harry Road, K13/D1 San Jose, A 95120-6099

Electronic addresses: bethune@almaden.ibm.com / risk@almaden.ibm.com

We have improved the hardware and software of our autocompensating system for quantum key distribution by replacing bulk optical components at the end stations with fiber-optic equivalents and implementing software that synchronizes end-station activities, communicates basis choices, corrects errors, and does privacy amplification over a local area network. Autocompensating systems[1,2] send light on a round-trip through the fiber so that quantum information can be coded in a fashion that is unaffected by random variations in the fiber properties. The all- fiber-optic arrangement provides stable, efficient and high-contrast routing of the photons. The low bit error rate leads to high error correction efficiency and minimizes data sacrifice during privacy amplification. The system currently generates privacy amplified key data at rates >1 kbit/s over a 10 km single-mode fiber link.

Our modified system is shown in Figure 1. Generally, the custom bulk-optic components used in our original implementation[2] have been replaced with polarization-maintaining (PM) fiber-optic components. The use of such components in Bob's delay loop substantially reduces losses and enhances the stability of the system, and eliminates the need for polarization adjusters in the phase-sensitive parts of the optical path. The main improvement at Alice's station is the replacement of the bulk-optical polarizer with a 2x2 fiber-optic polarizing beamsplitter (similar to Bob's PBS2). This polarizing coupler allows Alice to impart equal phase shifts to *both* polarization components of an *arbitrarily polarized* arriving pulse using a standard $LiNbO_3$ phase modulator, Mod_A, which transmits only one polarization. Data showing the raw, error-corrected, and privacy amplified data rates obtained is shown in Figure 2.

Key issues for future applications of quantum cryptography are overall loss and detector efficiency and noise. Single-photon detectors are crucial for this application, and currently are a serious problem. Our system employs Fujitsu InGaAs APD's cooled to 118 K. Using a novel pulse biasing scheme to minimize average current through the devices, we have characterized and compared these devices to several other APD's. The performance of the various APD's is summarized in Fig. 3, which shows the BER and quantum efficiencies obtained as the DC bias voltage applied to the devices was varied. Even devices of the same type from the same manufacturer are seen to vary widely, indicating the pressing need for APD's specifically tailored for single photon detection at low temperatures. This is perhaps not surprising since none of these devices are designed for low temperature operation, and their low temperature characteristics are neither controlled for nor documented by the manufacturers.

At longer distances backscattering in a continuously pulsing round-trip system becomes intolerable. We have recently carried out preliminary experiments on a scheme to avoid backscatter noise by frequency shifting the photons at Alices's station and employing a narrowband filter in front of the detectors to discriminate between the shifted and backscattered photons. We find that the high contrast routing is retained, even with a 2 GHz frequency shift.

[1] G. Ribordy, J.D. Gautier, N. Gisin, O. Guinnard and H. Zbinden, "Automated 'plug & play' quantum key distribution," *Electron. Lett.* **34**, 2116-2117 (1998).
[2] D. S. Bethune and W.P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light," *IEEE J. Quant. Electron.* **36**, 340-347 (2000).

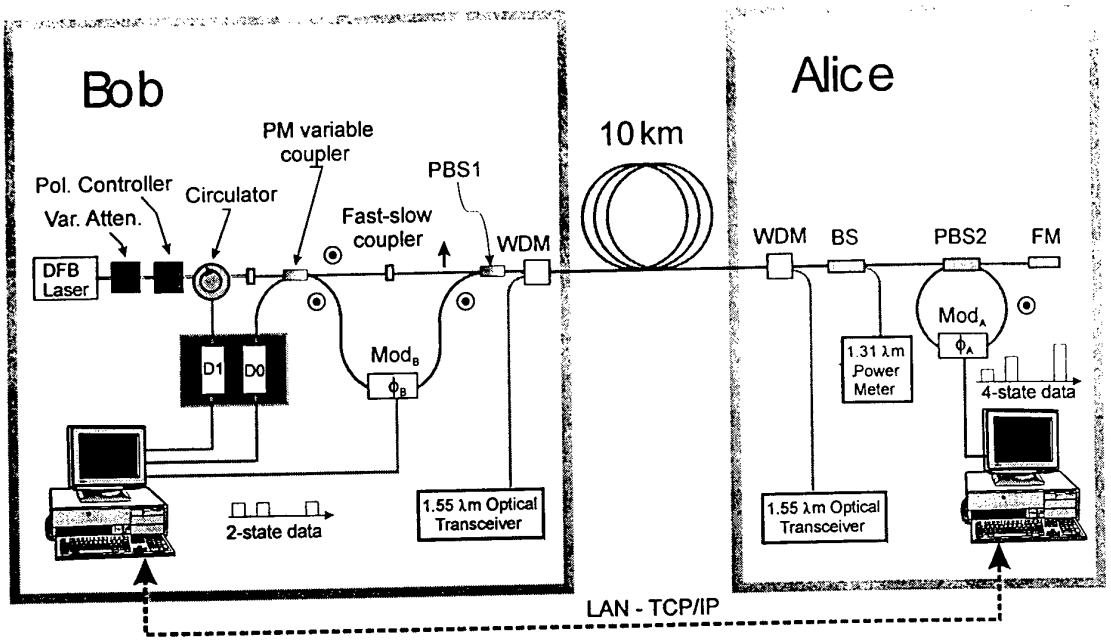


Figure 1. DFB laser emits 50 ps pulses at 1 MHz rate. PBS1,2 – polarizing beamsplitters; WDM – wavelength division multiplexers for 1.31 and 1.55 μm; Mod$_{A,B}$ – phase modulators; FM – Faraday Mirror; BS – fiber

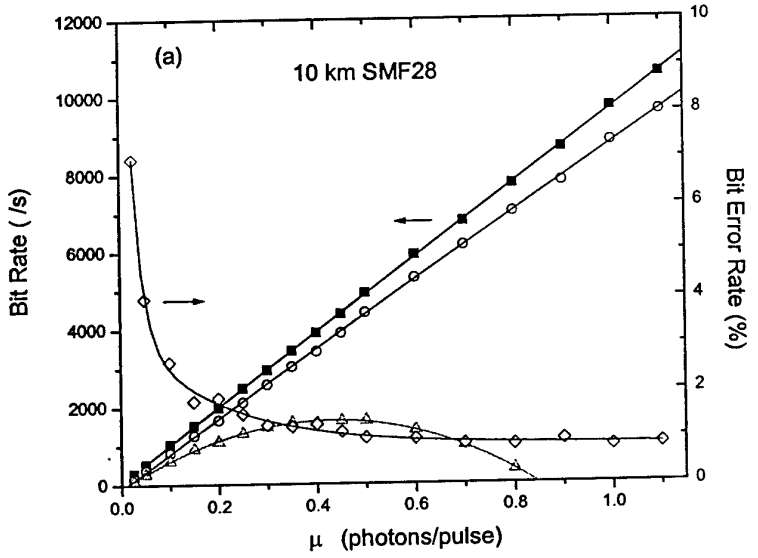


Figure 2. a) Data for 10 km fiber. Raw (■), error corrected (O) and privacy amplified (Δ) bit rates, and measured bit error rates (◊), vs. the mean number of photons/pulse, μ, leaving Alice's station. The leakage rate to Eve is estimated using the original BB84 formula for privacy amplification. All curves are simple fits provided as guides to the eye.

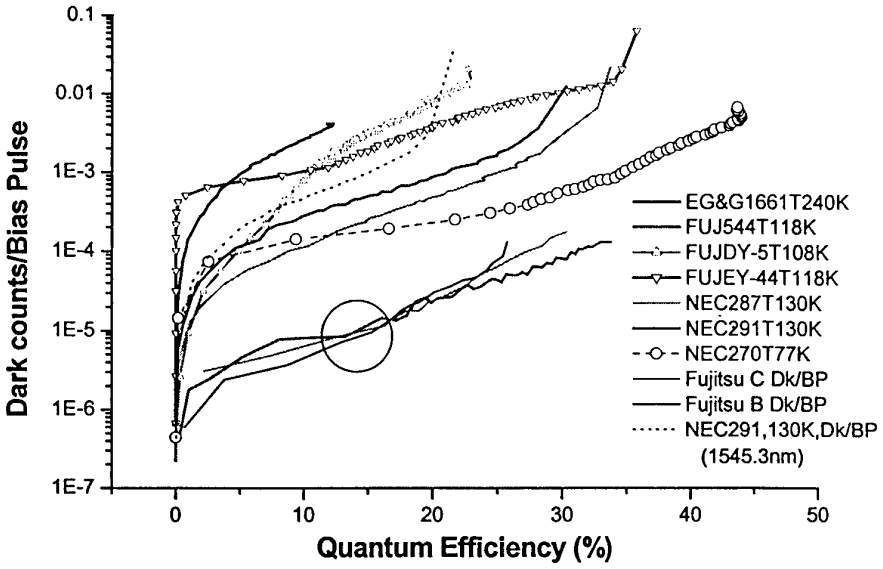


Figure 3. Bit Error Rates and quantum efficiencies for various APD's at their optimum temperatures as the DC bias voltage is varied (approaching their reverse breakdown voltages). All of the devices are based on InGaAs with the exception of the NEC270 device, which is a Ge APD.

Semiconductor twin photon sources : towards integrated quantum optics

V. Berger, A. De Rossi
THALES
Laboratoire Central de Recherches
91400 ORSAY, FRANCE

Recent work at Thales-LCR is devoted to the generation of twin photons by parametric fluorescence in semiconductor waveguides. Several different types of phase matching schemes are investigated:

- form birefringence phase matching
- modal phase matching
- counterpropagating signal and idler photons

A review of this work will be proposed, with a comparison of these different approaches. Perspectives of new devices (micro-optical parametric oscillators, fibered semiconductor sources of twin photons) will be given.

This work is supported by the European Community under "OFCORSE II" and "Qucomm" projects.

Entanglement engineering with quantum gates in a cavity QED experiment

M. Brune

Laboratoire Kastler Brossel
Département de physique de L'Ecole Normale Supérieure,
24 Rue Lhomond - 75005 Paris - France

The preparation of simple entangled quantum systems and the demonstration of their non-classical properties is a challenging goal since the early days of quantum mechanics and the famous Einstein Poldolsky Rosen (EPR) paper. Manipulation of tailored entangled states also seats at the heart of the physics of quantum information. Using "circular Rydberg atoms" strongly interacting one by one with a zero or one photon field stored in a high finesse microwave superconducting cavity, we prepare a tailored three particle entangled state [1] in a controlled sequence of quantum gate operation.

In our experiment, the entanglement originates from the Rabi [2] oscillation experienced by a single excited atom emitting a photon in an initially empty cavity. By adjusting the atom-cavity interaction time so that atoms experience a $\pi/2$, π or 2π pulse, we realize various quantum logic operation. The π pulse allows to write or detect a 0 and 1 photon superposition field state in the cavity. The $\pi/2$ pulse prepares a maximally entangled atom-cavity EPR pair. The 2π pulse provides the conditional dynamic corresponding to the operation of a two qubit quantum phase gate or equivalently of a C-Not gate.

We have prepared a three qubit (two atoms and a 0 or 1 photon field) "Greenberger Horne Zeilinger" entangled state by using a programmed sequence of resonant atom cavity interactions [1]. The method generalizes to the entanglement of larger number of particles.

By using the non-resonant atom-field interaction, new quantum gates are realized. In this way, atoms can be directly entangled without emission of a photon in the cavity. The interaction of a single atom with two non-degenerate cavity modes also allows to operate a three qubit Tofoli gate in a single operation. Application of these new gates will be discussed.

[1] Rauschenbeutel, G. Nogues, S. Osnaghi, P. Bertet, M. Brune, J.M. Raimond and S. Haroche: "Step-by-Step Engeneering Multiparticle Entanglement", Science, 288, 2024(2000).

[2] M. Brune, F. Schmidt-Kaler, A. Maali, J. Dreyer, E. Hagley, J. M. Raimond and S. Haroche: "Quantum Rabi oscillation: a direct test of field quantization in a cavity". Phys. Rev. Lett. 76, 1800 (1996).

Towards quantum communications with strongly coupled atoms

Gerhard Rempe,

Max-Planck Institute for Quantum Optics,

Garching,

Germany

Abstract:

Atoms strongly coupled to a single-mode field of an optical cavity exhibit radiation properties different from those in free space. This opens up new possibilities for experiments with single atoms and single photons. For example, the motion of an atom can be observed with high spatial and temporal resolution, and an atom can be trapped in a light field containing only one photon on average. Moreover, an atom passing through a cavity can be stimulated to emit one photon into a well-defined spatial mode with, in principle, near-unity efficiency. Such a single-photon light source might have interesting applications in quantum communications.

Quantum dots in 3D microcavities: CQED effects and application to single photon sources

J.M. Gérard, E. Moreau, I. Robert, I. Abram, L. Manin and V. Thierry-Mieg
CNRS/Laboratoire Photonique et Nanostructures, 196 av. Henri Ravera, 92220 Bagneux
Tel : 33 1 42317156 Fax : 33 1 42534930 jeanmichel.gerard@rd.francetelecom.fr

The development of efficient solid-state single-photon sources is an important prerequisit for a large scale implementation of secure telecommunication systems based on quantum crytography. Various solid-state emitters including molecules, F-centers, semiconductor nanocrystals and self-assembled quantum dots (QDs) emit under proper excitation conditions antibunched light. QDs at low temperature present some important assets in this context : QDs exhibit 1) a good stability (no photobleaching, no blinking), 2) a quantum efficiency very close to one, 3) a short radiative lifetime (1 ns), 4) a quasi-monochromatic emission (< 25 μeV at 4K), which allows to exploit CQED effects to tailor their emission properties, and 5) can be easily inserted inside semiconductor microcavities. We discuss recent advances toward the fabrication of an optically pumped single photon source based on isolated InAs QDs in pillar microcavities, following the operation principle we proposed few years ago [1].

. A QD containing two -or more- electron-hole (e-h) pairs may emit two photons within an arbitrarily short delay, so that a specific excitation/collection scheme must be used. Our protocol uses the strong Coulomb interaction between trapped carriers in the QD, which entails a large spectral separation of the QD emission lines corresponding to different numbers of trapped e-h pairs. After a pulsed injection of several e-h pairs, the spectral selection of one of these lines is enough to ensure that single photons are collected. We present detailed microphotoluminescence data and photon correlation experiments obtained on single QDs under pulsed excitation, which confirm the preparation of single photon pulses using this scheme.

. For practical applications, it is essential to collect efficiently these single photons ; this can be obtained by placing the QD in a 3D microcavity, such that the QD emission line of interest is on resonance with a single cavity mode. Thanks to the selective enhancement of the QD spontaneous emission rate into this resonant cavity mode (Purcell effect), a large fraction of the QD emission is funnelled into this single mode (β>0.9) [1]. Besides being efficiently collected, the single photons are also prepared in a given quantum state (same spatial mode, same polarisation), which is very interesting in practice. Until recently however, the Purcell effect had been observed only on collections of QDs. We present here the study of isolated QDs inside truly monomode micropillars with an elliptical cross-section. A comparison of the optical properties of QDs either in resonance or out of resonance with the cavity mode (including time-resolved and polarization-resolved experiments on single QDs) allows a clear observation of a strong Purcell effect (> x10 enhancement) for single QDs in resonance. The results of photon correlation experiments on the complete single photon source (QD emitter+ microcavity output coupler) at 8K are also presented.

We finally discuss several other important issues, such as the operation of QD based single photon sources at higher temperatures, and the prospects for the generation of entangled photon pairs, or entangled exciton-photon states [2] using single QDs in 3D cavities.

[1] J.M. Gérard et al, J. Lightwave Technology, 17, 2089 (1999); Phys.Rev.Lett 81, 1110 (1998)
[2] L.C. Andreani et al, *Phys. Rev. B.* 60, 13276 (1999), J.M. Gérard et al, *Physica* E 9, 131 (2001)

Single atoms in microscopic dipole traps : towards quantum gates ?

Nicolas Schlosser, Georges Reymond, Igor Protsenko and Philippe Grangier
Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS,
B.P. 147, F91403 Orsay Cedex - France.

Trapped neutral atoms are a possible candidate for implementing quantum gates. The proposed schemes may involve either direct coupling between two atoms, or cavity-mediated coupling, or coupling between an atom and a photon. Most of these schemes would highly benefit from the ability to trap and address individual atoms with high spatial resolution.

Here we present an experiment which aims at loading and detecting individual atoms in an optical dipole trap with a sub-micrometer size. We will also discuss the possibilities for trapping, adressing and coupling several atoms in separate traps, for applications to quantum information processing.

Practical Quantum Key Distribution and Security Analysis

Norbert Lütkenhaus

MagiQ Technologies, Inc.,
275 Seventh Avenue, 26th Floor, New York, NY 10001-6708

Practical quantum key distribution [QKD] involves the use of existing technology for sources and detectors to distribute a key which is secure against an eavesdropping attack using superior technology. Some of the imperfections of signal source and receiver put severe restrictions on the secure bit rate and distance over which a secure key can be established. The corresponding positive security proof can be established against a eavesdropper limited only by the rules of quantum mechanics. [Mayers, Inamori] Note that the availability of technology matching the conservative security condition has been demonstrated by many groups; most of them are represented at this conference.

It is very important to remember that we are still make assumptions in modeling the QKD protocol. However, by now we expect to have captured the dominating effects of the imperfections which takes the shape of the probability that the source emits several photon in the signal state rather than a single photon. [NL] Note that even signals from single photon devices contain multi-photon components which eventually limits the performance of the QKD system.

The secure rate and distances guaranteed by the positive security proofs differ from those in experimental papers. This can be explained by a different security notion commonly employed. Most articles deal with multi-photon components of the signals using the so-called beam-splitting attack. However, security against beam-splitting attacks is not a well-defined security level. We have shown [Dusek] that a system can be secure against beam-splitting attacks while one can think of a simple scheme employing only measurements, transfer of classical states and state preparation to break this scheme using *unambiguous state discrimination.* Such a scheme has been earlier proposed by Yuen [Yuen] to show the limitations of QKD.

[Mayers] D. Mayers, in *Advances in Cryptology - Proceedings of Crypto '96* Springer, Berlin (1996), 343-357; D. Mayers, quant-ph/9802025v4.
[Inamori] H. Inamori, D. Mayers, N. Lütkenhaus, in preparation.
[NL] N. Lütkenhaus, PRA **61** (2000) 052304.
[Dusek] M. Dušek, M. Jahma, N. Lütkenhaus, PRA **62** (2000) 022306.
[Yuen] H. P. Yuen, Quantum Semiclass. Opt. **8** (1996) 939-949.

Quantum information processing without strong nonlinear interactions

N. Imoto

SOKEN(The Graduate University for Advanced Studies), Hayama, Kanagawa 240-0193, Japan
CREST, JST(Carrier Interaction Research Program)
Department of Applied Physics, Universtity of Tokyo

A strong nonlinearity is necessary to form qubit-qubit entanglement, which is essential in the fundamental functions such as controlled NOT. Is entanglement, then, indispensable in quantum information processing? The answer is of course yes, but sometimes "no" for the users of quantum information processing. To see this, let us consider three cases: (1) Single-party calculation, (2) Multi-party processing (with no attack), and (3) Multi-party processing (with attack). Examples are as follows: (1) Computing, Database search, (2) Communication, Teleportation, and (3) Cryptography and Magic protocols such as discrete comparison, zero knowledge proof, and bit commitment. (Most of the quantum versions of these work but some do not in principle.) In category (3), there are the legitimate user and a cheating party. Entanglement is necessaty to explain what is going on in the whole system including the legitimate user and the cheating party. For the legitimate user only, however, there is no necessity of using entanglement, sometimes. This is why there are some quantum key distribution schemes which apparently do not require full quantum technology for Alice and Bob but still effectively prevent an eavesdropper from performing any quantum attack including not only individual attacks but also collective or coherent attacks.

We investigate those quantum information processing schemes which do not require entanglement for the legitimate users [1]. Also some schemes we proposed are included in the case of "individual" entanglement processing but not a large scale collective manipulation [2]. This type of entanglement can be obtained by a beam splitter and photon counting. We discuss the erformance of this kind of devices for the case that there are imperfections in each device [3]. Also, entanglement purification using incmpletely entangled pairs is [4]. There are also some interesting ideas other than QKD [5] with photon twins and also with a simple entanglement induced by a beam splitter [6]. The attainable amount of entanglement for various configurations of qubits have also been investigated [7].

[1] N. Imoto et al., in Proceedings of ISQM'98.
[2] A. Karlsson, et al., Phys. Rev. A59, 162(1999).
[3] S. Ozdemir, et al., in preparation.
[4] T. Yamamoto et al., to appear in Phys. Rev. A.
[5] K. Shimizu, et al., Phys. Rev. A59, 1092(1999).
[6] K. Shimizu, et al., Phys. Rev. A62, 054303(2000).
[7] M. Koashi et al., Phys. Rev. A62, 050302(R)(2000).

Entanglement purification in cryptographic schemes

Vlatko Vedral

In my lecture I will introduce the notion of entanglement purification between two and more parties involved in a quantum communication protocol. I will first present two examples of such protocols for bi-partite systems in terms of very simple quantum computational networks. Then I intend to show how these generalise straightforwardly to multi-partite systems. I will discuss fundamental limits to the efficiency of all such protocols resulting from the principle that "entanglement cannot inclease under local operations andwith the aid of classical communication". Finally, I will give examples of concrete realisations of purification protocols involving entangled photons. Implications to secure quantum cryptography are discussed throughout.

Unconditional security and quantum cryptography

Dominic Mayers

Unconditional security means a security which hold against a cheater with unlimited computational power, quantum or classical. This may seem only of theoretical interest, but it makes quantum cryptography a viable alternative in the long run: one may wonder if it is worth it to invest into a technology that might become obsolete in the future. Furthermore, in addition to an unconditional security, we want a security that works with imperfect apparatus. There are two levels to consider. At the lower level, we tolerate imperfections but requires assumptions about how bad the imperfections are. For example, for a protocol that ideally requires only one photon per pulse, we tolerate multi-photons per pulse, but we require that there is an upper bound on the number of photons. At the highest security level, the security of the protocol should not depend upon such an unproven upper bound. Again, this may seem only of theoretical interest, but it makes quantum cryptography more interesting even from an practical angle. In this talk, we will consider protocols and security proofs with regard to these security aspects.

Architectures for Long-Distance Quantum Communication

Jeffrey H. Shapiro
Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, U.S.A.
Electronic address: jhs@mit.edu

The preeminent obstacle to the development of quantum information technology is the difficulty of transmitting quantum information over noisy and lossy quantum communication channels, recovering and refreshing the quantum information that is received, and then storing it in a reliable quantum memory. A team of researchers from the Massachusetts Institute of Technology and Northwestern University (MIT/NU) is developing a singlet-based quantum communication approach [1] that uses a novel ultrabright source of polarization-entangled photon pairs [2], and a trapped-atom quantum memory [3] whose loading can be nondestructively verified and whose structure permits all four Bell-state measurements to be performed. This talk will first review the primitives for the MIT/NU architecture: the dual optical parametric amplifier (OPA) source of polarization entanglement; low-loss entanglement transmission over standard telecommunication fiber using quantum frequency conversion [4] to interface with the 795 nm line of the trapped Rubidium atom memory and time-division multiplexing [5] to avoid the ill-effects of fiber birefringence; and a clocked communication protocol whose loss-limited performance analysis shows that a throughput as high as 500 entangled-pairs/sec with 95% fidelity can be achieved over a 50 km path when there is 10 dB of fixed loss in the overall system and 0.2 dB/km of propagation loss in the fiber. An additional primitive—the type-II degenerate optical parametric amplifier—will then be added. This source, which is less complicated than the dual-OPA arrangement, is somewhat less effective in long-distance singlet-state teleportation. It can be used, however, within the MIT/NU architecture to perform long-distance transmission and storage of Greenberger-Horne-Zeilinger (GHZ) states via an alerted detection system akin to that in [6]. The addition of a heralded single-photon source primitive can be used to both eliminate the need for alerted detection in this GHZ-state transmission scheme, and to greatly increase its throughput.

[1] J. H. Shapiro, "Long-distance high-fidelity teleportation using singlet states," to appear in *Quantum Communication, Measurement, and Computing 3*, O. Hirota and P. Tombesi, eds., (Kluwer, New York, 2001).
[2] J. H. Shapiro and N. C. Wong, "An ultrabright narrowband source of polarization-entangled photon pairs," J. Opt. B vol. **2**, pp. L1–L4 (2000).
[3] S. Lloyd, M. S. Shahriar, and P. R. Hemmer, "Long distance, unconditional teleportation of atomic states via complete Bell state measurements," submitted to Phys. Rev. Lett.
[4] P. Kumar, "Quantum frequency conversion," Opt. Lett. **15**, pp. 1476–1478 (1990); J. M. Huang and P. Kumar, "Observation of quantum frequency conversion," Phys. Rev. Lett. vol. **68**, pp. 2153–2156 (1992).
[5] K. Bergman, C. R. Doerr, H. A. Haus, and M. Shirasaki, "Sub-shot-noise measurement with fiber-squeezed optical pulses," Opt. Lett. vol. **18**, pp. 643–645 (1993).
[6] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon Greenberger-Horne-Zeilinger entanglement," Phys. Rev. Lett. vol. **82**, pp. 1345–1349 (1999).

UNCONDITIONALLY SECURE QUANTUM BIT COMMITMENT

Horace Yuen

Northwestern University

Evanston Illinois,USA

Bit commitment involves the submission of evidence from one party to another so that the evidence can be used to confirm a later revealed bit value by the first party, while the second party cannot determine the bit value from the evidence alone. It is widely believed that unconditionally secure quantum bit commitment is impossible due to quantum entanglement cheating, which is codified in a general impossibility theorem. The limited scope of this theorem will be exhibited. Three quantum bit commitment protocols will be presented which can be proved to be unconditionally secure. The first, QBC1, involves the use of anonymous states and was presented at the 2,000 Capri meeting without a correct security proof to be presented in detail here. Qualitatively, the unconditional security derives from the fact that the cheating transformation is unknown due to the unknown anonymous states. The second protocol utilizes anonymous BB84 states and the third does not employ any anonymous state; their security proofs will be briefly described. The possibility of a practical implementation of QBC1 with large-energy coherent states will be presented. An expanded, revised version of quant/ph 0006109 on this topic will be made available before this meeting.

Relativistic Cryptography FAQ

Adrian Kent[1,2]

Quantum Information Processing Group, Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ,U.K.

[1] *On leave from: DAMTP, Centre of Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, U.K.*

[2] *Electronic addresses:* Adrian_Kent@hp.com, A.P.A.Kent@damtp.cam.ac.uk

Most physics-based cryptographic protocols studied to date rely on the properties of quantum information to guarantee security. However, special relativity – specifically, Minkowski causality – gives another way of guaranteeing security, which for some tasks is more powerful.

This talk reviews results in relativistic cryptography to date, focussing in particular on recently proposed relativistic protocols for bit commitment. The security assumptions required are discussed, and it is shown that no trust between the parties is required when arranging timings and locations, so that the protocols fall within the standard cryptographic scenario for information exchange between mistrustful parties. I explain why the protocols are not covered by the bit commitment no-go results of Mayers and Lo-Chau and are not susceptible to Mayers-Lo-Chau type attacks. Finally, I review the data transmission rates required for relavistic bit commitment, and show that its practical implementation is well within the capabilities of existing technology.

Unconditionally secure quantum communication using entanglement-based quantum repeaters

Hans Aschauer and Hans J. Briegel
Theoretical Physics, University of Munich (LMU),
Theresienstr. 37, 80333 München, Germany

We give a security proof of quantum cryptography based entirely on entanglement purification [1]. Our proof applies to all possible attacks (individual or coherent) and implies the security of quantum communication when entanglement-based quantum repeaters are used. We show that any eavesdropper gets factored out under the action of standard two-way entanglement purification protocols (EPP), even when Alice and Bob use imperfect apparatus. This means that under EPP the state of the ensemble converges to a final state (exponentially fast) where any residual entanglement is with the local apparatus rather than with the eavesdropper. This also proves the security of the entire *quantum channel*, which may not only be used for quantum key distribution but also for secure transmission of quantum information.

[1] H. Aschauer and H.J. Briegel, quant-ph/0008051, submitted to Phys. Rev. Lett.

Quantum Bit Commitment from any Quantum One-Way Permutations

Paul Dumais (Université de Montréal, Canada),
Louis Salvail (Århus University, Danemark) and Dominic Mayers (NEC Research Institute, Princeton, NJ).

Quantum cryptography has been mainly concerned with quantum key distribution (QKD) protocols so far. QKD is a useful cryptographic tool that allows two participants that trust each other to exchange a secret key through a conversation over a public line. But cryptographers are also interested in protocols that involve two or more participants that *do not* trust each other, but still they want to compute a function of their private inputs. A voting scheme is a typical example of such a task. To achieve such a feat we generally need a computational assumption, a problem that is believed to be hard to solve by computation, whether quantum or classical. For example, in the classical world, "factoring large integers is hard" is a well known computational assumption. Hence, in this work, we are interested in computationally based cryptography, as opposed to information theoretically based cryptography.

"Bit commitment" is a fundamental primitive in cryptography and it is a key building block for many cryptographic protocols. Although unconditionally secure quantum bit commitment has been shown impossible, it is still relevant to inquire into the possibility of basing this primitive upon (quantum) computationnal assumptions.

We show that quantum bit commitment can be based on the assumption that any family of quantum one-way permutations exists. Informally, a permutation is said to be one-way if it can be easily computed but is hard to invert on average. A one-way permutation is a "quantum one-way permutation" if it hard to invert even on a quantum computer.

Hence, even though quantum computers can be used to break classical assumptions like the factoring assumption mentionned earlier, there is still hope that computationally based cryptography continues to exist in the presence of quantum computers.

Atmospheric Quantum Key Distribution in Daylight: ground-based experiments and prospects for satellite communications

Richard J. Hughes, George L. Morgan, Jane E. Nordholt, Charles G. Peterson,
Los Alamos National Laboratory,
Los Alamos, NM 87545

In quantum key distribution (QKD) single-photon transmissions generate the shared, secret random number sequences, known as cryptographic keys, that are used to encrypt and decrypt secret communications. Because the security of QKD is based on principles of quantum physics an adversary can neither successfully tap the key transmissions, nor evade detection (eavesdropping raises the key error rate above a threshold value). We have developed an experimental QKD system that uses the four-state "BB84" protocol with non-orthogonal photon polarization states and lowest-order adaptive optics to generate shared key material over multi-kilometer atmospheric, line-of-sight paths. I will present results of a daylight demonstration of this system. Key material is built up using the transmission of a photon-pulse per bit of an initial secret random sequence. I will describe the design and operation of the system, present an analysis of the system's security, efficiency, error rate, and secret key rate, as well as cryptographic testing of the key bits produced. I will describe the prospects for longer-distance applications of free-space QKD, particularly for satellite communications.

FREE SPACE QUANTUM CRYPTOGRAPHY AND SATELLITE SECURE KEY DISTRIBUTION

John G. Rarity, P. Gorman and P.R. Tapster
DERA, St. Andrews Road, Malvern, Worcs. WR14 3PS
Tel: 44-1684-895031; Fax: 44-1684-896270; Email: rarity@dera.gov.uk

We have designed and built a free space quantum cryptography system [1]. It operates using weak laser pulses with polarisation modulation by acousto-optic switching. The system also incorporates full key sifting and error correction between computers connected by a serial port. We have used this system to exchange keys over ranges up to 1.9km with absolute security. The system is robust against transmission (and diffraction) losses up to 20dB.

The bread-board system (figure 1) uses an attenuated pulsed visible laser diode (635nm) at 10MHz repetition rate. The four polarisations 0, 90^0, 45^0, 135^0 encoding key bits in two non-orthogonal measurement bases are selected by acousto-optic switches. The receiver uses a passive 50/50 beamsplitter to set a measurement basis of 0^0 or 45^0. The beams are then recombined with 3ns time delay in a polarisation beamsplitter before detection in one of two photon-counting detectors. The passive beamsplitting technique randomly selects the measurement basis and the time delay allows discrimination of the two measurement bases [2].

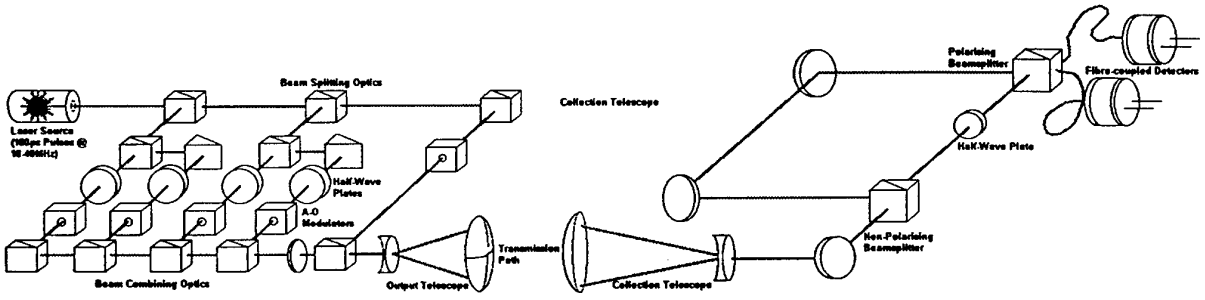


Figure 1: *Free space quantum cryptography system*

Send and receive optical boards are interfaced to two separate computers. A large number of random bits are sent and photon arrival times and bit values are digitised in the receiver. Arrival time information is used to synchronise clocks to sub-nanosecond as well at to determine the measurement basis. Key sifting involves sender and receiver ascertaining which sent bits have arrived and which bits were encoded and decoded using the same measurement basis. The key sifting and secure error correction operate over a standard modem-telephone link between the computers. In a demonstration experiment we have been able to exchange kilobit keys over a distance of 1.9km.

Using this system we have shown that a 20dB transmission loss can be tolerated when background counts are below 1Kcps (night operation). The key performance limit arises from errors due to dark counts appearing in the 1ns timing gate. Reducing the gate width and dark count rate will allow a 30dB loss tolerance. In our experiment losses were high because of air turbulence induced beam wander. In better air conditions we expect to reach tens of kilometres range.

The talk will describe initial feasibility studies for extending this system to upload keys to satellites. In a possible downlooking key exchange system with range >1000km we estimate ~30dB losses. This is possible simply by improving our existing system. However the tracking of a satellite with 10's of microradian beamwander will require sophisticated closed loop active pointing systems.

[1] J.G. Rarity et al, *Secure Key Exchange Over A 1.9km Free-space Range Using Quantum Cryptography*, Electronics Letters April 2001.

[2] J.G.Rarity, P.C.M.Owens and P R Tapster, *Quantum Random Number Generation and Key Sharing*, J.Mod Opt 41 (1994) 2435-2444.

Free-Space QKD Research at the Mt Stromlo Satellite Laser Ranging Observatory

Paul J Edwards

Centre for Advanced Telecommunications and Quantum Electronics Research, University of Canberra ACT 2601 Australia
Electronic address: paule@ise.canberra.edu.au

Free-space terrestrial paths provide a natural propagation medium in which to investigate the viability of earth/space single-photon QKD transfer. Satellite laser ranging observatories currently used for tracking geodetic satellites provide an ideal platform from which to extend these point-to-point terrestrial studies towards quantum key transfer via earth satellite.

In collaboration with colleagues at DERA (Malvern) and a number of Australian universities we are developing an optical free-space range based on a satellite laser ranging observatory instrumented for this purpose[1,2].

The 6.3 km horizontal path extends from the 805 m altitude Mt Stromlo satellite laser ranging station of the Australian Surveying and Land Information Group operated by EOS Pty Limited. The test range uses the 750mm Coude observatory telescope as the light collector for a dual-polarisation single-photon counting receiver with 10 nanosecond range gate resolution and 100 microradian FOV.

A binary non-orthogonally polarised single-photon transmitter with beam collimated to 20 microradians located at the observatory provides a 12.6 km folded-path capability and can also be operated remotely for single pass studies.

We are developing receiver-based active optics to compensate for turbulence-induced wavefront tilt leading to beam wander and consequent image excursion outside the field of view of the receiver.

We are also planning a 5 km terrestrial point-to-point free-space QKD demonstration link between a local telecommunications tower and our laboratory at the University of Canberra. This will employ GPS-based frame and bit synchronisation.

A photon-counting receiver is under construction for installation at Mt Stromlo for the acquisition of 10 photon/bit infra-red (835 nm) Manchester-coded binary pulse position modulated 400 baud data from a recently launched earth satellite. This project will provide information on data acquisition and tracking problems arising from atmospheric refraction, seeing and scintillation.

Data obtained from these three links will address the feasibility of ground to satellite and satellite to ground QKD systems.

Other QKD related projects include the evaluation of unconditional single photon sources in collaboration with the Yamamoto group at Stanford and an investigation of conditional [3] single-photon twin and multiplet beam sources. We show that the use of correlated multiplet photon sources permits efficient identification and rejection of multiple photon emissions with relaxed detector quantum efficiencies.

[1] EDWARDS P J, et alia, A free-space test range for global quantum key distribution feasibility studies, Paper QThD, IQEC 2000, Conference papers p97.

[2] CHEUNG W N et alia, Implementation of a quantum cryptographic key distribution system, Proc IEEE Tencon 2000, Kuala Lumpur, Malaysia, 24-27, Sep 2000, 3, pp. 374-378.

[3] EDWARDS P J et alia, A note on quantum key channel efficiency and security using correlated photon beam transmitters, quant-ph/0008013, Aug 2000.

High-Speed Quantum Cryptography SATCOM

Gerald Gilbert*

Quantum Information Science Group
The MITRE Corporation
12 Christopher Way, Eatontown, NJ 07724 USA
**Electronic address: ggilbert@mitre.org*

The requirements and prospects for high-speed free-space quantum cryptography implemented via ground-satellite, aircraft-satellite and satellite-satellite links are described. In connection with this we present the results of a comprehensive analysis of the secrecy capacity of practical quantum key distribution systems [1]. This is the first demonstration of the secrecy of the BB84 protocol that accounts for all of the following effects simultaneously: the finite length of individual blocks of key material, effects due to the presence of multi-photon pulses in a practical source, errors in polarization detection, the efficiency of the detectors, attenuation processes in the transmission medium, and losses due to error correction, privacy amplification, and continuous authentication. Of particular importance is the first derivation of the *necessary and sufficient* amount of privacy amplification (rather than just a sufficient amount) to protect against the loss of secret key material which would otherwise occur when an eavesdropper makes optimized individual attacks on pulses containing multiple photons. We also give the first explicit calculation (rather than just order of magnitude estimates) of the total number of bits that must be sacrificed to carry out continuous authentication. Also calculated are the complete classical communications bandwidth and computational resource requirements associated to carrying out the quantum cryptographic protocol. Our analysis includes a detailed, explicit analysis of all systems losses due to errors and noises, including turbulent and static atmospheric propagation losses, optics package losses, intrinsic channel losses, *etc.* We obtain predictions for maximal rates that can be achieved with practical system designs under realistic environmental conditions, taking into account our results for total system losses and loads. The analysis addresses eavesdropping attacks on individual photons rather than collective attacks in general. We propose a specific quantum cryptography system design that includes the use of a novel method of high-speed photon detection that may be able to achieve very high throughput rates for actual implementations in realistic environments. Aspects of the MITRE Quantum Information Science program are briefly described.

[1] G. Gilbert and M. Hamrick, "Practical Quantum Cryptography: A Comprehensive Analysis (Part One)," *arXive e-print* quant-ph/0009027, MITRE Technical Report 00W0000052 (2000).

Time-bin entangled photon pairs and its applications for quantum cryptography

Wolfgang Tittel, Hugo Zbinden, Nicolas Gisin
Group of Applied Physics - Optique, University of Geneva
20, Rue de l'Ecole-de-Médecine, 1211 Geneva 4, Switzerland
**Electronic address: wolfgang.tittel@physics.unige.ch*

Qubits and entangled states can be realized using different physical properties. We report on the creation of entangled qubits based on the superposition of different *time-bins* [1], and we present first applications for quantum key distribution [2] and quantum secret sharing [3].

Time-bin qubits can be realized using an interferometer with a path-length difference which is large compared to the photon's coherence length (Fig. 1, upper left part). α and β denote the normalized probability amplitudes for passing via the (s)hort and the (l)ong arm, respectively. Time-bin qubits can be represented graphically on the qubit sphere shown in the lower left part. Entangled time-bin qubits are created in a similar way by pumping a nonlinear crystal with two subsequent (classical) light pulses (upper right part).

The right-hand picture of Fig 1. also shows the setup for quantum key distribution. After separating the photons forming a pair in a maximally entangled Bell state, each photon is analyzed using an interferometer (at (A)lice's and (B)ob's), introducing the same travel-time difference as the "(p)ump"-interferometer. Depending on the arm chosen by a photon and the phase introduced between l and s, it is measured in a basis spanned either by discrete times as represented on the poles of the qubit-sphere, or in a basis spanned by two orthogonal states represented on the equator of the sphere. If Alice and Bob perform the same measurements, they get correlated results – if no third person tried to get any information about the state sent. Thanks to the symmetry between the preparation device and the analyzers of the entangled qubits, the same setup can also be used for quantum secret sharing, the extension of "traditional" two-party quantum key distribution to three parties.

[1] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. 82, 2594-2597 (1999).
[2] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. 84, 4737-4740 (2000).
[3] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A, 63, 042301 (2001).

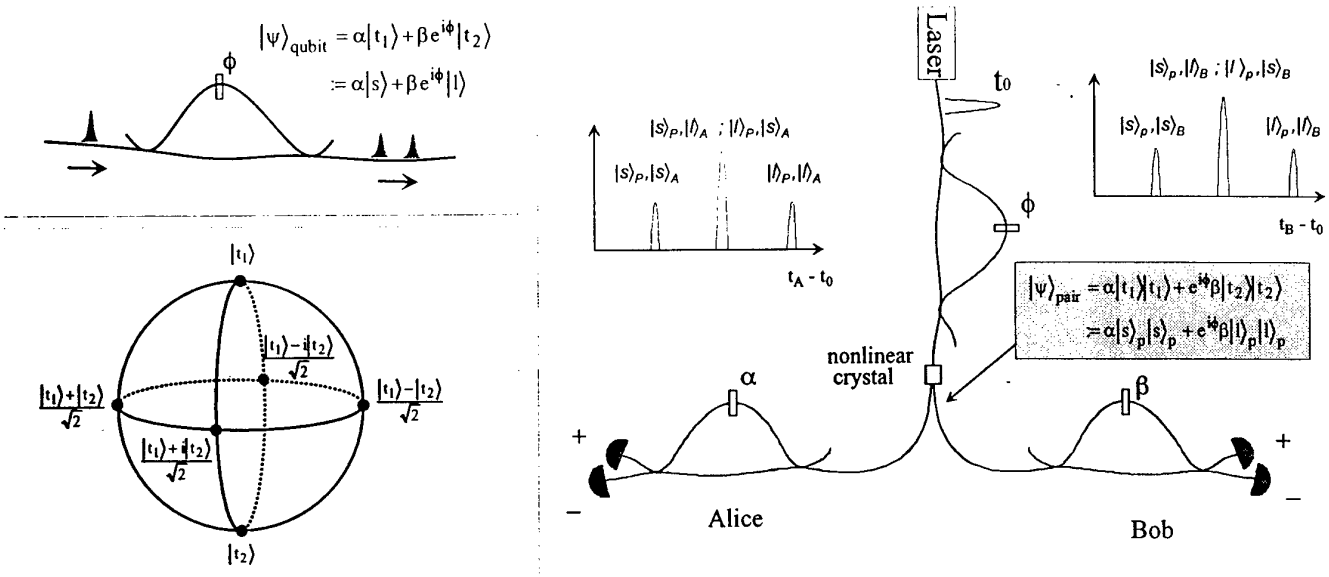


Figure 1: The left-hand part shows the creation of a time-bin qubit and its representation on the qubit sphere, the right-hand part the generation of entangled qubits and the use for quantum cryptography and quantum secret sharing.

An Entangled Photon Laser: Prospects and Applications

Dik Bouwmeester

Centre for Quantum Computation,
Clarendon Laboratory, University of Oxford
Parks Road OX1 3PU Oxford, United Kingdom

We introduce the notion of laser-like operation for polarisation entangled photons. The proposed device has a two-mode output which contains quantum correlations both between the polarisation degree of freedom for particles in seperate modes and between the photon numbers in the modes. The proposed lasing device will operate in the new and virtually unexplored regime of many-particle entanglement. We present the design and provide experimental data in support of the main operation mechanism. In particular we show the generation of a rotational symmetric four-photon entangled state obtained by stimulated emission of the familiar antisymmetric two-particle Bell state.

Hyperentanglement in Parametric Down-Conversion

A.V. Sergienko, M. Atature, G. Di Giuseppe, M. D. Shaw,
B. E. A. Saleh, and M. C. Teich

Quantum Imaging Laboratory, Dept of Physics and Dept of Electrical and Computer Engineering, Boston University, 8 Saint Mary's Street, Boston, MA 02215, USA

Abstract

Entanglement is, undoubtedly, one of the most fascinating features of quantum mechanics. Spontaneous parametric down-conversion (SPDC) a nonlinear optical phenomenon, has been one of the most widely used sources of entangled quantum states. In this process, pairs of photons are generated in a state that can be entangled in frequency, momentum, and polarization when a laser beam illuminates a nonlinear optical crystal. The experimental arrangement for producing entangled photon pairs is simple both in conception and in execution.

Ironically, a significant number of experimental efforts designed to verify the nonseparability of entangled states, the hallmark of entanglement, are carried out in the context of models that fail to access the overall relevant Hilbert space, but rather are restricted to only a single kind of entanglement, such as polarization entanglement \cite{Polarization}. Inconsistencies in the analysis of down-conversion quantum-interference experiments can emerge under such circumstances, as highlighted by the failure of the conventional theory of ultrafast parametric down-conversion to characterize quantum-interference experiments.

In this paper we present a complete quantum-mechanical analysis of entangled-photon state generation via SPDC, considering simultaneous entanglement (hyperentanglement) in momentum, frequency, and polarization at the generation, propagation, and detection stages. As an important example of the application of this approach, we use it to describe new, and previously obtained, results of SPDC experiments with a femtosecond pump. Our analysis confirms that the inconsistencies between existing theoretical models and the observed data in femtosecond down-conversion experiments can indeed be attributed to a failure of considering the full Hilbert space spanned by the simultaneously entangled quantum variables. Femtosecond SPDC models have heretofore considered only a single wavevector, which does not incorporate the previously demonstrated angular spread of the down-converted light. The approach presented here is suitable for Type-I, as well as Type-II, spontaneous parametric down-conversion.

Highly efficient photon-pair source using a Periodically Poled Lithium Niobate waveguide

S. Tanzilli[1*], H. De Riedmatten[2], W. Tittel[2], H. Zbinden[2], P. Baldi[1], M. De Micheli[1], D.B. Ostrowsky[1], and N. Gisin[2]

(1) LPMC-CNRS UMR 6622, Université de Nice - Sophia Antipolis, Parc Valrose, 06108 Nice Cedex 2.
(2) GAP, Université de Genève, 20, rue de l'école de médecine 1211 Genève 4, Switzerland.

In the beginning of the 80's Alain Aspect [i] performed his famous tests of Bell-inequalities to verify quantum non-locality [ii], using a complicated two-photon source based on a double atomic cascade transition. Since then, more and more Bell-tests have been reported [iii], taking advantage of more efficient and handy sources exploiting spontaneous parametric down-conversion (PDC) in second order ($\chi(2)$) non-linear bulk crystals. Such sources have become an essential tool for fundamental and applied quantum optical. Although a lot of important results have been obtained, always confirming theoretical predictions, more sophisticated experiments like quantum teleportation suffer from low photon-pair production leading to low signal-to-noise ratios and long measurement times. Here, we report on a new kind of twin-photon source taking advantage of an active optical waveguide integrated on a Periodically Poled Lithium Niobate (PPLN) substrate [iv], in opposition to bulk crystals used until now. Thanks to the confinement of the pump wave over the entire length of the sample and the use of Quasi-Phase-Matching (QPM), this leads to an improvement of the pair generation efficiency by four orders of magnitude.
Measurements are made on a 3.2 cm long sample with a 12.1 μm poling period. Using a pump laser of a few μW at 657 nm, we generate degenerate photon-pairs at 1314 nm. The output of the guide is coupled to a 50/50 single mode fiber optics beam splitter used to separate the twin photons. Using LN_2 cooled Germanium-APDs and a time-to-amplitude converter (TAC), the coincidence rate (R_c) is counted. The efficiency of the source is unprecedented: we obtain an average of around 1550 coincidences/s (c/s) for a guided pump power of only 1 μW. Furthermore, taking into account the 50% loss at the directional coupler, we can estimate a pair production rate of 7.5 MHz, corresponding to a conversion efficiency of about $2*10^{-6}$ per pump photon. To our knowledge, this result is at least 4 orders of magnitude higher than any other source reported before. Note that high efficiency for twin-photon production is especially important for experiments needing more than one photon pair at a time or high signal to noise ratios.

i A. Aspect, P. Grangier, and G. Roger
"Experimental test of realistic theories via Bell's inequality"
Phys. Rev., **47**, pp. 460-465 (1981)

ii J.S. Bell
"On the Einstein-Podolsky-Rosen Paradox"
Physics (Long Island City, N.Y.), **1**, pp. 195-200 (1964)

iii W. Tittel, J. Brendel, H. Zbinden, and N. Gisin
"Violation of Bell inequalities by photons more than 10 km apart"
Phys. Rev. Lett., **81**, 17, 3563-3566 (1998)
Phys. Rev. Lett., **82**, 7, pp. 1345-1349 (1999)

iv L. Chanvillard, P. Aschieri, P. Baldi, D.B. Ostrowsky and M. De Micheli; L.Huang, and D.J. Bamford
"Soft Proton Exchange on PPLN: a simple waveguide fabrication process for highly efficient non-linear interactions"
Applied Physics Letters, **76**, 9, pp. 1089-1091 (2000)

* e-mail : tanzilli@unice.fr

Synthesis, manipulation and measurement of highly non-classical optical states

A. I. Lvovsky*, H. Hansen, T. Aichele, O. Benson, J. Mlynek, and S. Schiller[1]

Fachbereich Physik, Universitt Konstanz, D-78457 Konstanz, Germany
[1] *Institut für Experimentalphysik, Universität Düsseldorf, D-40225 Düsseldorf, Germany*
**Electronic address: Alex.Lvovsky@uni-konstanz.de*

We present a research program dedicated to developing techniques of production, manipulation and characterization of complex quantum states of the light field. A successful completion of this program would mark a step towards developing *quantum technology of nonclassical light*, a new branch in the rapidly developing field of quantum technology.

As the first step, we have applied the technique of optical homodyne tomography to the single photon Fock state $|1\rangle$ prepared by conditional measurements on a photon pair produced in parametric down-conversion [1]. In our experimental setup (Fig.1) we employ a mode-locked Ti:Sapphire-laser in combination with a pulse picker to obtain transform-limited 1.6-ps pulses at 790 nm. Most of the radiation is single-pass frequency doubled in an LBO-crystal and passed on to a BBO crystal for down-conversion. The down-converter is operated in a type I frequency degenerate, but spatially non-degenerate configuration. A single-photon counter is placed in one of the emission channels — labeled trigger — to detect photon pair creation events and to trigger the readout of a homodyne system placed in the other emission channel — labeled signal. In this way only those pulses are selected for homodyne measurements where a photon has been emitted into the signal channel, thus conditionally preparing single photon Fock states. The latter are then subject to a homodyne measurement using a small fraction of the original laser power as a local oscillator.

The statistical distribution of the pulsed homodyne detector output was then used to reconstruct the Wigner function (Fig. 2). The latter exhibits a well at the center reaching a classically impossible negative value. Various experimental imperfections (such as non-ideal spatial and temporal mode matching, losses in the signal beam path, dark counts etc.) have caused an admixture of the vacuum $|0\rangle$ to the measured state, reducing the depth of the well.

Based on this experience, we are developing an experiment on production and characterization of *arbitrary* single-mode quantum-optical states. This is achieved via repeated two-photon down-conversion in a chain of nonlinear crystals with a set of coherent seed pulses fed into the trigger channel of each crystal [2]. The quantum state emerging in the common signal mode of the down-converting chain is determined by the choice of amplitudes and phases of the seed states and is conditioned upon simultaneous firing of single-photon counters placed into the trigger channel of each down-converter. The maximum number of terms in the output state's Fock representation is determined by the number of crystals in the chain.

In a separate effort, we intend to characterize, via the technique of quantum homodyne tomography, the entangled two-mode state $|\Psi^+\rangle = |1\rangle|0\rangle + |0\rangle|1\rangle$, generated by a photon incident on a 50/50 beamsplitter. The quantum states emerging from both beamsplitter output ports are subjected to balanced homodyne detection. By studying the correlations between the two homodyne detector outputs one can obtain the Wigner function $W(X_1, P_1, X_2, P_2)$ of $|\Psi^+\rangle$ and see interference effects demonstrating its nonlocal character in an entirely new fashion [3].

[1] A. I. Lvovsky *et al.*, quant-ph/0101051
[2] J. Clausen *et al.*, quant-ph/0007050
[3] K. Jacobs and P. L. Knight, Phys. Rev. **A 54**, 3738 (1996)

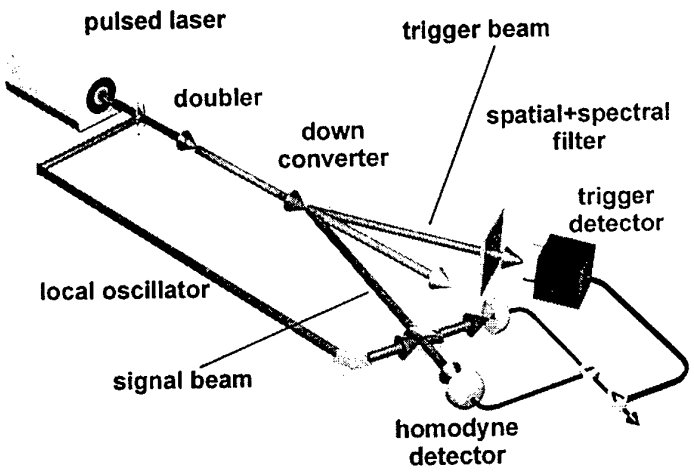


Figure 1: Simplified scheme of the experimental setup

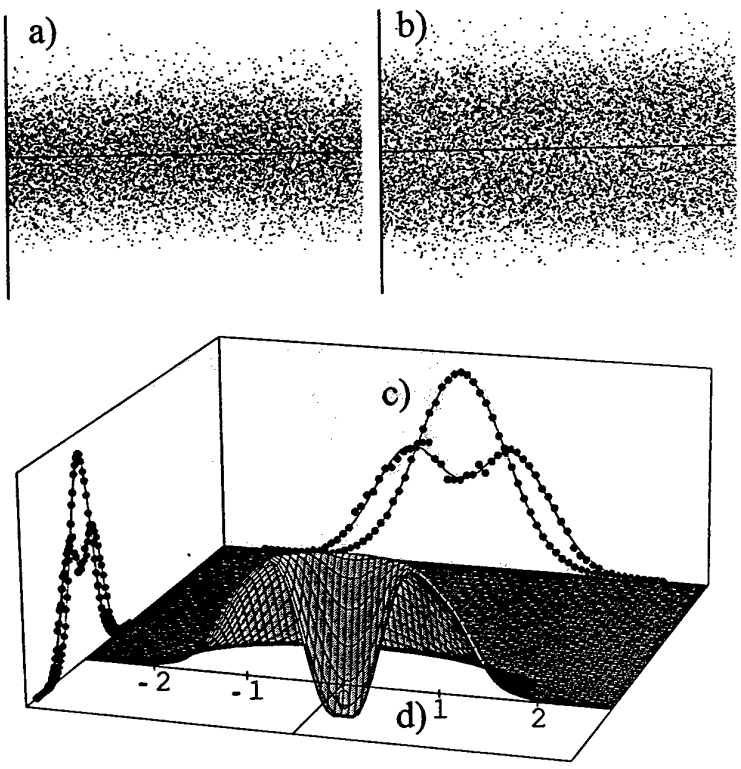


Figure 2: Experimental results of the quantum state measurement. Top: raw quantum noise data for the vacuum state (a) and the Fock state (b). Bottom: histograms of the data which correspond to the phase-randomized marginal distributions of the measured vacuum (green) and Fock (red) states (c); reconstructed Wigner function (d) is negative near the origin point. A measurement efficiency of 55% is achieved.

Entangled macroscopic atomic objects.

E. S. Polzik
University of Aarhus
Denmark

Abstract
We report on the progress with generation of the EPR state of spins of two separate atomic samples. The entanglement is generated via interaction of the samples with an off-resonant pulse of light. The life time of the correlated state around 1 millisecond has been observed.

Quantum state transfer from light fields to atomic ensembles

Laurent Vernac, Michel Pinard, Elisabeth Giacobino*,

Laboratoire Kastler Brossel, Université Pierre et Marie Curie, 4 place Jussieu, F75252 Paris Cedex 05 France *Electronic address: elg@spectro.jussieu.fr*

For quantum information processing as well as for high precision measurements in atomic physics, it is highly desirable to be able to engineer the quantum state of either individual atoms or atomic ensembles. In order to realize quantum registers or quantum memories for the information carried by light, one should be able to map the quantum state of light onto a material system. To reduce the quantum projection noise in measurements, one can consider putting the atoms in squeezed atomic states that exhibit reduced fluctuations for the measurement of interest[1, 2, 3].

Atomic ensembles have a variety of superposition states, that can be manipulated by the interaction with light fields. In the case of large enough ensembles, the components of the total polarization of the system, or of its equivalent collective spin, can be considered as a continuous variable, in the same way as the quadrature components of a light field. As was shown by other authors previously, one can get squeezed atomic states by having the atomic ensemble interact with a squeezed field[4, 5, 6, 7]. We have shown that this operation can be treated completely analytically while keeping a full quantum treatment if the incoming field is extremely weak. Moreover the resulting atomic state can be correlated at a quantum level with the light input state, leading to EPR-type correaltions.

In order to deal with such a system, we consider a model system made of an ensemble of 2-level atoms in an optical cavity interacting with a very weak squeezed field. We show that if the mean value of the field is zero, the system is fully equivalent to two coupled harmonic oscillators, an atomic one and a field one. This is also true for the quantum Langevin equations, taking into account all the noise sources. The equations can then be solved in a simple analytical way.

We derive the conditions for obtaining optimal squeezing transfer from a field to an atomic ensemble and we calculate the correlations between the atomic state and the field input state.

References

[1] W.M. Itano, J.C. Bergquist, J.J. Bollinger, J.M. Gilligan, D.J. Heinzen, F.L. More, M.G. Raizen, D.J. Wineland, Phys. Rev. A 47, 3554 (1993)

[2] M. Kitagawa and M. Ueda, Phys. Rev. A 47, 5138 (1993)

[3] D.J. Wineland, J.J. Bollinger, W.M. Itano, D.J. Heinzen, Phys. Rev. A 50, 67 (1994)

[4] J.M. Courty and S. Reynaud, Europhys. Lett. 10, 237 (1989)

[5] G. S. Agarwal and R. R. Puri, Phys. Rev. A 41, 3782 (1990)

[6] A. Kuzmich, K. Molmer and E.S. Polzik, Phys. Rev. Lett. 79, 4782 (1997)

[7] L. Vernac, M. Pinard, E. Giacobino, Phys. Rev. A, 62, 063812 (2000)

Quantum techniques using continuous variables of light

G. Leuchs, C. Silberhorn, P.K. Lam*, N. Korolkova

Zentrum für Moderne Optik,
Universität Erlangen-Nürnberg
*Australian National University, Canberra

Quantum entangled light pulses are basic requisites for quantum communication systems. A realisation using optical fibre solitons is presented. It is straight forward to extend the experimental set-up for the detection of quantum phase correlations of the two entangled beams to demonstrate quantum dense coding. The scheme can also be interpreted as a squeezed light interferometer with two intense amplitude squeezed beams at the two input ports resulting in an enhancement of the interferometric sensitivity corresponding to the degree of squeezing.

Optimal Cloning and Anticloning of Continuous Quantum Variables

Nicolas J. Cerf*

Ecole Polytechnique, CP 165/56, Université Libre de Bruxelles, 50 av. F. D. Roosevelt, B-1050 Brussels, Belgium

**Electronic address: ncerf@ulb.ac.be*

The cloning of continuous quantum variables is investigated. We consider a Gaussian 1-to-2 cloning machine, which duplicates optimally (and with a same fidelity) two conjugate variables such as the quadrature components of a light mode [1]. The resulting cloning fidelity for coherent states (namely $F = 2/3$) is shown to be optimal, and the extension to optimal N-to-M continuous cloners is discussed [2]. The possibility of implementing these cloners using a phase-insensitive amplifier and a network of beam splitters is considered [3]. Then, a phase-conjugated inputs (N, N')-to-(M, M') cloner is presented, which yields M clones and M' anticlones from N replicas of a coherent state and N' replicas of its phase conjugate (with $M' - M = N' - N$) [4]. Interestingly, this is a first example of a continuous-variable quantum information-theoretic process for which no qubit analogue has been found yet. For well chosen input asymmetries $(N' - N)/(N' + N)$, this cloner yields better fidelities than the standard N-to-M cloner. The special case of the balanced cloner ($N = N'$) is analyzed in detail, and shown to be optimal.

[1] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[2] N. J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000).
[3] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, to appear in Phys. Rev. Lett. (2001); see also quant-ph/0012046.
[4] N. J. Cerf and S. Iblisdir, quant-ph/0102077.

Stable Solid-State Source of Single Photons

Patrick Zarda[1,*], Christian Kurtsiefer,[2] Christoph Braig,[2] Sonja Mayer,[2] and Harald Weinfurter[1,2]

[1] *Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, 85748 Garching, Germany*

[2] *Ludwig-Maximilians-Universtität München, Sektion Physik, Schellingstr. 4/III, 80799 München, Germany*

**Electronic address: patrick.zarda@physik.uni-muenchen.de*

The controlled generation of single photons is mandatory for new applications of quantum communication, in particular for truly secure quantum cryptography [1]. Various solutions based on the fluorescence of single atom, ions or organic molecules have been demonstrated already [2]. However, they are either rather difficult to perform, need expensive equipment or can generate only a very limited number of emissions. Here, we present an all-solid-state solution promising low costs and unprecedented stability [3].

Compared to other candidates for single photon generation, single nitrogen-vacancy (NV) centers in type Ib diamond have a number of advantageous properties: The fluorescence cycle has a radiant efficiency of close to one, particularly at room temperature, and the wavelength range from 637 to 800 nm fits to the requirements of many applications like free space quantum cryptography. But foremost, the center shows no photo-bleaching and does not degrade or escape like single trapped atoms, ions or single organic dye molecules. In our experiment, single NV centers were observed over days without change of the emission characteristics.

The set-up of the single photon source is shown in the Figure 1: A cw pump laser beam at λ=532 nm is focused onto a single NV center. The red to NIR fluorescence light emerging from the excited center is collected into a single mode optical fiber. The confocal geometry allows to address individual centers separated by several 10 μm in our diamond sample.

For the demonstration of the non-classical features of the fluorescence the intensity correlation was measured in a Hanbury-Brown–Twiss configuration with silicon APD detectors behind a beam splitter (see Figure 2). The significantly reduced probability for detecting two photons simultaneously is a clear indication of the single photon character of the emitted light. The finite visibility is compatible with background counts and the limited time resolution of 1.5 ns of the single photon detectors.

Our experiment shows that NV centers, together with pulsed excitation schemes and optimized fluorescence collection, are a promising single photon source for practical applications.

[1] C.H. Bennett, G. Brassard: in *Proc. if IEEE Internat. Conf. on Computers, Systems and Signal Processing* (IEEE, New York 1984), pp. 175; G. Brassard et al., preprint quant-ph/9911054

[2] F. Diedrich, H. Walther, PRL. **58**, 203 (1987); Th. Basche et al., PRL **69**, 1516 (1992); W.P. Ambrose e al., Science **265**, 364 (1994); F. De Martini et al., PRL **76**, 900 (1996); Ch. Brunel et al., PRL **83**, 2722 (1999).

[3] C. Kurtsiefer, S. Mayer, P. Zarda and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000)

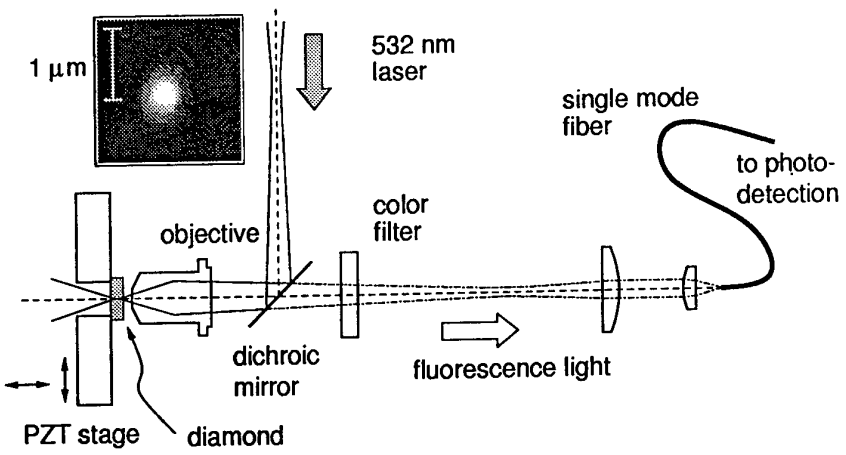


Figure 1: Confocal microscope setup. The inset shows a 2D-mapping of the fluorescence from the center with a FWHM of 650 nm.

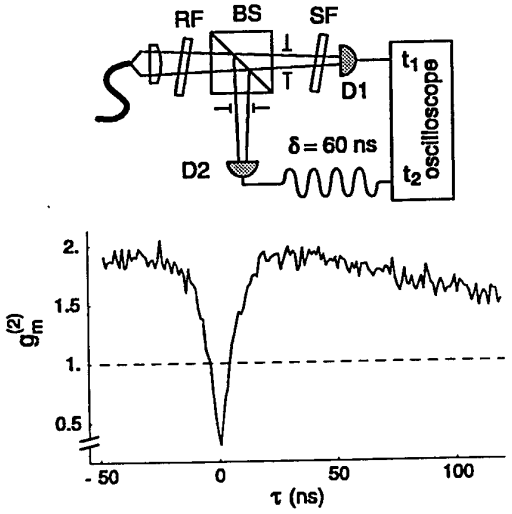


Figure 2: Pair-correlation function for a $g^{(2)}$ measurement on NV centers in diamond.

Nonclassical radiation from diamond nanocrystals

Rosa Tualle-Brouri

Institut d'Optique, BP147, 91402 Orsay Cedex

The quantum properties of the fluorescence light emitted by diamond nanocrystals containing a single nitrogen-vacancy (NV) colored center is investigated. We have observed photon antibunching with very low background light. This system is therefore a very good candidate for the production of single photon on demand. In addition, we have measured larger NV center lifetime in nanocrystals than in the bulk.

Collecting the one photon

Bill Barnes

School of Physics, University of Exeter, Exeter, EX4 4QL, UK, (w.l.barnes@ex.ac.uk)

Experimental demonstrations of single photon sources have been made by various authors in recent years. These have included sources based on quantum dots [1], terrylene molecules [2], and from defect centres in diamond [3]. In general the efficiency with which these photons have been collected is rather low. This low efficiency is deleterious in quantum cryptographic systems since it leads to a large proportion of the single photon pulses being dark.

A variety of ways have been explored to improve collection efficiency, notably that of placing the emitter within a microcavity [4]. The utility of this approach will be discussed, together with its limitations. An alternative will also be suggested, in which surface plasmon rather than microcavity modes are used as a way to enhance the radiative efficiency. This alternative may be adventageous when the emission spectrum of the source is broad, as is the case for terrylene molecules and the NV defect in diamond.

References.

1 P. Michler, A. Kiraz, C. Becher, et al., Science **290**, 2282 (2000).
2 B. Lounis and W. E. Moerner, Nature **407**, 491 (2000).
3 C. Kurtseifer, S. Mayer, P. Zarda, and H. Weinferter, Phys. Rev. Lett. **85**, 290 (2000).
4 S. C. Kitson, P. Jonsson, J. G. Rarity, and P. R. Tapster, Phys. Rev. A. **58**, 620 (1998).

Enhancement of a single dot spontaneous emission by coupling to a microdisk resonant mode

Bruno Gayral,* Alper Kiraz, Christoph Becher, Peter Michler, Winston Schoenfeld,[2] Pierre Petroff,[1,2] Lidong Zhang, Evelyn Hu,[1,2] and Atac Imamoğlu.[1,3]

[1] *Department of Electrical and Computer Engineering, University of California, Santa Barbara, California 93106,*

[2] *Materials Department, University of California, Santa Barbara, California 93106*

[3] *Department of Physics, University of California, Santa Barbara, California 93106,*

* *bruno@xanadu.ece.ucsb.edu*

Single photon states play a major role in current quantum cryptography and quantum computation proposals. Still, the realization of a good single photon source remains a challenge. Whatever "good" single photon source means, it is fair to say that for most applications a high "useful single photons" rate is desirable. In this context, one of the promising solutions is to use a single semiconductor quantum dot (QD). As was proposed [1] and recently demonstrated [2], the discrete energy level structure of a single QD, combined with the strong carrier-carrier interactions within the QD, allow a single QD to act as a converter from a non-resonant pulsed laser to single photon pulses at the same repeating frequency ($\sim 100\,MHz$). One issue with this source is that due to total internal reflection, most of the emitted photons never exit from the semiconductor and are lost. Moreover, coupling of these photons to a fiber is highly desirable, thus requiring a low NA output for the single photons. One way of dealing with these issues is to couple the QD to a high quality factor (Q) mode of a microcavity. The so-called Purcell effect then leads to an enhancement of the spontaneous emission rate of the emitter into this mode, in which most of the photons are thus fed. Beyond the aforementioned application prospects, the single dot/single mode system is a good test-bench for cavity quantum electrodynamics experiments in the solid-state.

The experiments we report here are microphotoluminescence experiments on a single InAs/GaAs quantum dot, at low temperature. The emission of the dot is around $1.33\,eV$, and is pumped non resonantly by a femtosecond Ti:sapphire laser (repetition rate $82\,MHz$) emitting at $1.6\,eV$. The dot emission is sent via a grating spectrometer to a standard time-correlated photon counting set-up (resolution $420\,ps$). We can thus access, within our time-resolution, the dynamics of the photoluminescence (rise and decay time) for the several spectral lines of the dot emission. The quantum dot is located in a $5\,\mu m$ diameter GaAs microdisk sustaining high Q whispering gallery modes (WGM). At a temperature of $4\,K$, the quantum dot is not on-resonance with a high Q WGM. In that case, we measure a radiative lifetime of $1.7\,ns$, the rise-time is resolution limited. A very important feature of this experiment is that great care has to be taken to work in the low excitation regime, for which on average about 1 or less electron-hole pair is created in the dot per pulse. In the high excitation regime, shelving of excess carriers in the excited states of the dot mask the recombination dynamics. By raising the temperature, the dot transition is red-shifted, allowing to tune the single exciton transition on resonance with a high Q (~ 6000) WGM at $T = 32\,K$. In that case, while still making sure that we are in the low excitation regime, the radiative lifetime of the QD drops to $850\,ps$. At even higher temperature ($50\,K$) when the QD transition is clearly detuned from the mode, the lifetime of $1.7\,ns$ is recovered, showing that in this temperature range, the lifetime does not vary with temperature. We thus attribute the lifetime shortening at $32\,K$ to the Purcell effect induced by the coupling with the WGM.

[1] J.-M. Gérard, B. Gayral, *J. Lightwave Technol.* **17**, 2089 (1999).
[2] P. Michler *et al.*, *Science* **290**, 2282 (2000).

Triggered single photons and entangled photons from a quantum dot microcavity

Matthew Pelton*, Charles Santori, Glenn Solomon,
and Yoshihisa Yamamoto[1]

Quantum Entanglement Project, ICORP, JST, Edward L. Ginzton Laboratories, Stanford University, Stanford, CA 94305

[1] *and NTT Basic Research Laboratories, 3-1 Morinosoto-Wakamiya, Atsugi, Karagawa, 243-01, Japan*

* *Electronic address: pelton@stanford.edu*

A single quantum dot (QD) can serve as a novel source of non-classical states of light, including triggered single photons and entangled photon pairs. This device may have important applications to practical implementations of quantum cryptography, allowing secure communication at reasonable rates over longer distances than is possible using attenuated coherent light sources or photon pairs from parametric downconversion.

Our QD's are made by growing InAs in a GaAs matrix using molecular-beam epitaxy (MBE). Nanometer-scale islands form by a strain-induced process. The sample is then patterened into an array of mesas with sub-micron diameter using electron-beam lithography and ECR dry etching. Each mesa contains, on average, less than one dot.

Excitation with a laser pulse creates excitons within the QD. The wavelength of photons emitted by recombination of these excitons is uniquely determined by the number of carriers in the dot. It is thus possible to isolate the one-exciton emission line through spectral filtering. At this wavelength, there will be only one photon emitted for each incident laser pulse. This was verified with Hanbury Brown-Twiss-type measurement of the photon autocorrelation function. Fig. 1 shows that large antibunching was seen, reflecting a strong reduction of the two-photon probability as compared to Poissonian light.

If the last two photons are collected instead, the resulting photon pair will have a high probability of being polarization-entangled. The biexcitonic state in the quantum dot consists of correlated electrons and holes with opposite spins. The selection rules for transitions in cubic crystals translates the anticorrelation of the carrier spins into an anticorrelation in polarization of the emitted photons.

The utility of the QD light source is limited by its efficiency. In the first experiments, only 0.03% of the emitted photons were ultimately detected, primarily because of the isotropic emission from the QD. To improve the collection efficiency, the QD can be placed in an optical microcavity. The microcavity is made by growing GaAs / AlAs distributed Bragg reflectors (DBR's) above and below the QD layer in a single MBE growth process. The entire sample is etched into sub-micron posts, as before; see Fig. 2. As well as isolating the QD's, this serves to confine light in the transverse direction by waveguiding. The discrete QD emission line is thus coupled to a single three-dimensionally confined optical mode, leading to significant enhancement of the spontaneous emission rate into this cavity mode. Up to 78% of the light emitted from the dot is captured in a single Gaussian-like mode, and can then be efficiently coupled into downstream optical components.

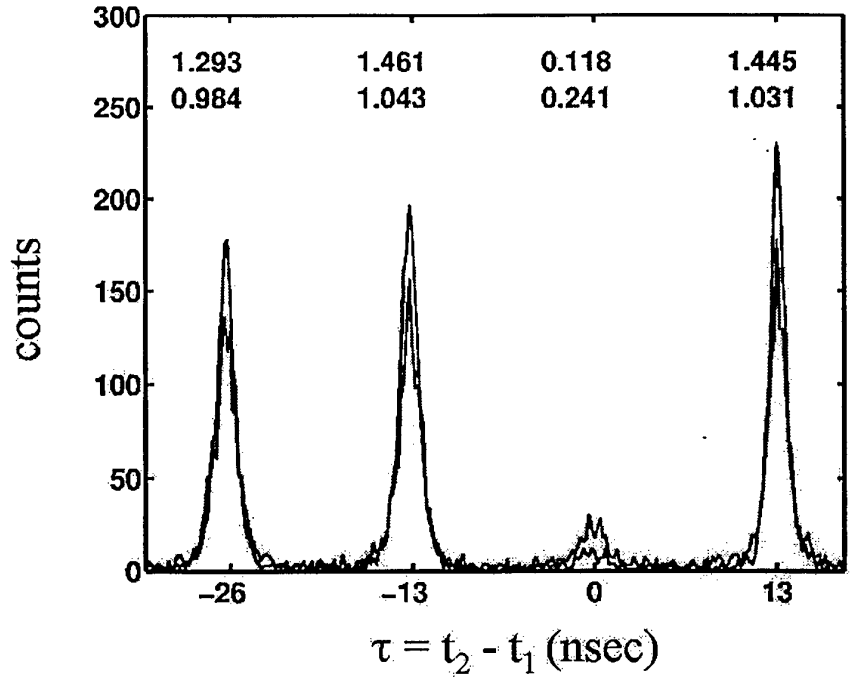


Figure 1: Photon autocorrelation function for pulsed one-exciton emission from a single quantum dot, showing strong suppression of the two-photon probability

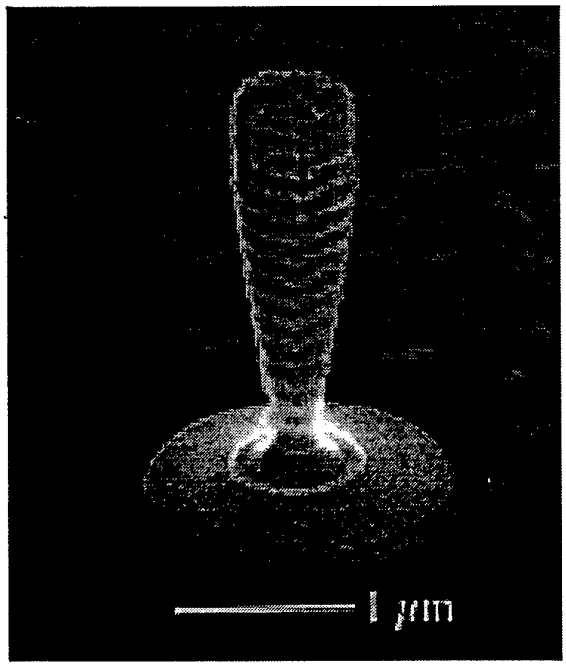


Figure 2: SEM micrograph of a micropost microcavity containing a single quantum dot

Antibunched photon emission from single self assembled quantum dots

Valery Zwiller*, Nikolay Panev, Soren Jeppesen, Mats-Erik Pistol, Lars Samuelson

Department of Solid State Physics, Lund University, Box 118, SE-221 00 Lund, Sweden

Hans Blom, Per Jonsson, Gunnar Björk

Department of Electronics, Royal Institute of Technology, SE-16440 Kista, Sweden

* *Electronic address: Valery.Zwiller@ftf.lth.se*

We report on antibunching measurements performed on a single self assembled quantum dot[1]. The quantum dots were obtained by epitaxial deposition (Chemical Beam Epitaxy) of 1.6 monolayers of InAs on GaAs. The low density of quantum dots with an average spacing of several micrometers enabled single dot investigations using a confocal microscope assisted by a solid immersion lens to increase light collection from the high refractive index sample. A Hanbury-Brown-Twiss interferometer was used to measure the correlation function using two sensitive avalanche photodiodes and a correlation card with a time resolution of around 0.5 ns.

The correlation function was measured under both continuous and pulsed excitation. In both cases, the excitation intensity was adjusted so that only a single sharp line due to the exciton recombination was observed. Under continuous excitation, a dip was observed in the correlation function. The pulsed excitation experiment was performed using a Ti:Sapphire laser emitting 150 fs pulses at 80 MHz, the correlation function shows a weaker peak for t=0 implying that single quantum dots could be used as triggered single photon sources.

The possibility of generating and detecting entangled photon pairs emitted by a single quantum dot will be discussed as well as different schemes to increase light collection efficiency from single quantum dots using microcavities of various designs.

[1] V. Zwiller, H. Blom, N. Panev, P. Jonsson, S. Jeppesen, T. Tsegaye, E. Goobar, M.-E. Pistol, L. Samuelson, G. Björk, submitted to APL

POSTERS

Quantum correlations between two trapped electrons

Carolina M. Alves, Ana M. Martins

Centro de Fisica de Plasmas, Instituto Superior Tecnico,
P-1096 Lisboa Codex, Portugal

Quantum entanglement is one of the most intriguing aspects of quantum mechanics. It is the essence ofthe Einstein-Poldosky-Rosen paradox and of the related problems of non-locality. More recently the interest in quantum entanglement gained a new breath when it was shown that this peculiar behaviour of the quantum world could be relevant to quantum computation [1], and quantum information transfer [2].

In this work we are concerned with the entanglement between position and momenta of two electrons confined intwo Penning-traps (PT) [3], which can be coupled through their axial currents. Initially the coupling bettween the PT is switched off and the electrons are disentangled. Their total wave function is given by the direct product of the wavefunctions of each electron. When the coupling between the two PT is switched on, their quantum state is governed bythe following Hamiltonean [4]

$$H = 3D\hbar\omega_1\left(a_1^\dagger a_1 + \frac{1}{2}\right) + \hbar\omega_2\left(a_2^\dagger a_2 + \frac{1}{2}\right) + \frac{\hbar g^2}{\omega_1\omega_2}\left(a_1^\dagger a_2 + a_1 a_2^\dagger + a_1 a_2 + a_1^\dagger a_2^\dagger\right), \qquad (1)$$

where a_i and $a_i^\dagger$ are the usual anhilation and creation operators for the axial oscillation of electron i ($i\omega_1$ and ω_2 are their axial frequencies, and g is the coupling constant. The last term of this Hamiltonean is the one describing the coupling between the electron axial currents. There is an obvious analogy between the coupling of these two massive oscillators (the electrons) and twolinear optical devices used to couple different modes of the electromagnetic field. The term$(a_1^\dagger a_2 + a_1 a_2^\dagger)$ is the analog of a beam splitter and the term$(a_1 a_2 + a_1^\dagger a_2^\dagger)$ is associated to a nodegenerate parametric amplifier.

We show that, for uncorrelated vacuum inputs (corresponding to the ground state of the axial oscillators in both PT),it is possible to squeeze the momentum or the position quadratures of the axial oscillators, and that this is afunction of the interaction time.

The axial coupling is also a source of quantum entanglement between the axial quantum states. This can be shownby computing the correlation functions between the axial positions and momenta of the two electrons.

We also propose some measurement procedures to determine the above refered properties.

This preliminar work suggests us that it would be, in principle, possible to use two spatially separated trappedelectrons to transfer quantum information between them. In particular such a system could be used to teleport the quantum state of a massive particle. To owr knowledge, no such experiment as yet been performed.

[1] D.DEUTSCH, Proc. R. Society of London, Ser.A 400, 97 (1985).
[2] C.H.BENNETT, G.BRASSARD, C.CREPEAU, R.JOSZA, A.PERES and W.K.WOOTERS, Phys.Rev.Lett.70,1895(1993).
[3] L.S. BROWN and G. GABRIELSE, Rev. Mod. Phys.58, 233 (1986).
[4] D. J. HEINZEN and D. J WINELAND, Phys. Rev.A 42,2977(1990).

Testing Bell Inequalities in Photonic Crystals

D.G. Angelakis and P.L. Knight
Optics Section, Blackett Laboratory, Imperial College, London SW7 2BW, England

We show how entangled atomic pairs can be prepared in order to test the Bell Inequalities[1]. The scheme is based on the interaction of the atoms with a highly localized field mode within a photonic crystal[2]. The potential of using optically separated transitions and the stability of the entangled state to spontaneous emission can in principle close both the communication and the detection loopholes appearing in experiments so far.

In photonic crystals the regions in which photon localization occurs can be viewed as spherical "bubbles". These can be arranged in lines through which an excited atom can be fired. Our system consists of two three level atoms, the first of which is initially prepared in the upper of two optically separated states, denoted by $|e_1\rangle$ and the second in the lower one $|g_2\rangle$. The two atoms propagate sequentially in orthogonal directions through the defect region of the crystal(see Fig. 1). The defect mode is initially prepared in the vacuum state $|0\rangle$ and it is on resonance with the atomic transition $|e_i\rangle \rightarrow |g_i\rangle$.

In Fig. 2 we show contour plots of the strength of the correlations versus the velocities. The values of the parameters correspond to the case of Rb atoms traveling through a defect in an optical photonic crystal (e.g., GaP) at thermally-accesible velocities ($v \sim 150 - 400m/s$). The extend of the defect mode is assumed to be equal to the lattice constant a and $a = 0.8\lambda$. The coupling constant has maximum value of $1.1 \times 10^{10} rad/sec$ at the center of the defect. The dashed lines in the plot represent to $|S| = 2.2, 2.4, 2.6, 2.8$, whereas the solid line corresponds to $S = 2$, i.e., the maximum value allowed by local realistic theories.

As the transitions here are optically separated, decoherence due to spontaneous emission would potentially be a problem during the flight from the crystal to the analyzers/detectors(inside the crystal spontaneous emission is competely inhibited[2]). To tackle this problem through a properly engineered line defect we inject a coherent light field into the crystal which crosses the atom's path. This field is resonant with the $|e\rangle \rightarrow |g'\rangle$ transition. By adjusting the field intensity properly we can apply a Π pulse between $|e\rangle$ and $|g'\rangle$ transferring any population from $|e\rangle$ to $|g'\rangle$(see Fig. 1). The transition $|g'\rangle \rightarrow |g\rangle$ is dipole non-allowed and thus can be considered stable for our purposes(lifetime$\sim$1 sec)

We also calculate the robustness of our scheme as a function of the spread in the atomic velocities. In Fig. 3 we plot $\bar{S}$ as a function of Δv for the case of $\bar{v}_1 = 231$m/s and $\bar{v}_2 = 270$m/s. As we show the violation is quite strong even in the case of ± 25m/ which is easily within the limits of curent velocity selection technology.

Detection efficiency (we detect optically separated transitions) can be as high as 95%. This would close the detection loophole. The communication loophole can be also closed, as our entangled state stays alive for seconds which as we show is enough to prevent any kind of subluminal communication between the analyzers/detectors.

[1]A. Aspect et al., Phys. Rev. Lett. **47**, 460 (1981);P. Kwiat et al., *ibid.* **74**, 4763 (1995); A. Kuzmich et al., *ibid.* **85**, 1349;W. Tittel et al.,Phys. Rev. A **57**, 3229 (1998); G. Weihs et al., Phys. Rev. Lett. **81**, 5039 (1998). D. G. Angelakis et al., submitted.

[2]D. Angelakis et al., Phys. Rev. A **61**, 055802;A. Blanco et al., Nature **405**, 437 (2000); E. Yablonovitch et al., Phys. Rev. Lett **58**, 2059 (1987);

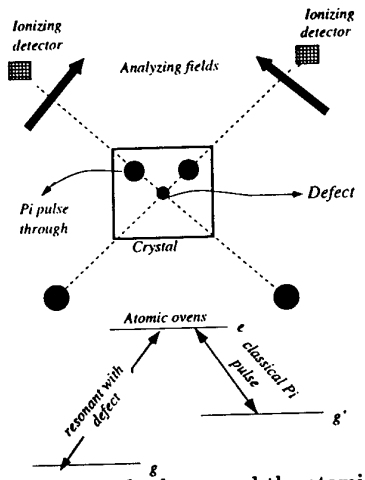


FIG. 1. The proposed scheme and the atomic system consideration

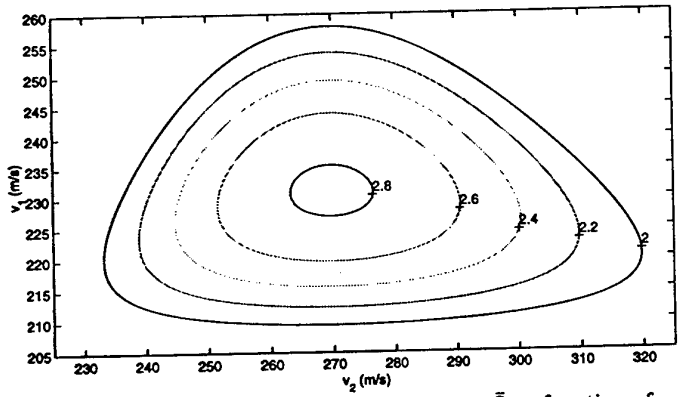


FIG. 2. Contour plot of Bell's parameter $\bar{\mathcal{S}}$ as function of the atomic velocities v_1, v_2

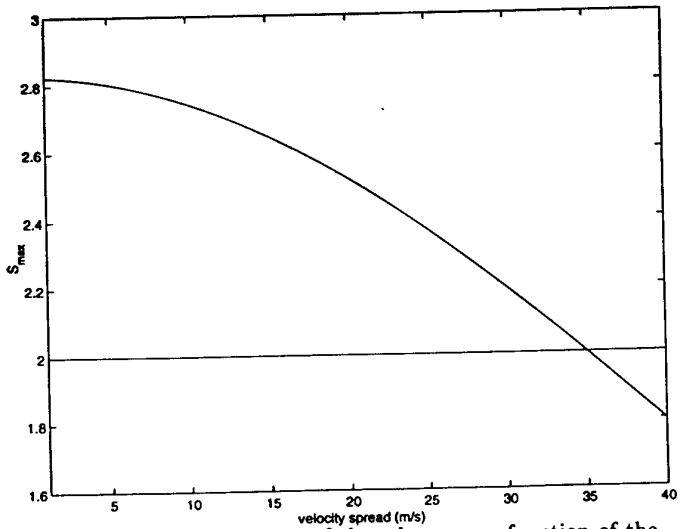


FIG. 3. The sensitivity of the scheme as a function of the spread in the atomic velocities. The vertical axis is the value the quantum mechanical sum $\bar{\mathcal{S}}$ and the horizontal the atomic velocity spread Δv . A violation of Bell's Inequality is predicted as long as $\Delta v \leq 34$m/s.

The Role of Hyperentanglement in Quantum Interferometry

M. Atatüre, G. Di Giuseppe, M. Shaw, A. V. Sergienko*, B. E. A. Saleh, M. C. Teich

Department of Electrical and Computer Engineering, Boston University,
8 Saint Mary's St., Boston, MA 02215, USA
** Electronic address: AlexSerg@bu.edu*
Homepage: http://www.bu.edu/qil/

Entanglement has proven to be an important resource in generating completely new optical states that can be used in quantum information processing, secure communication, and precise optical measurement. The transition from this theoretical notion to experimental reality is often a challenging step, however. One of the most accessible sources of entangled-photon states is a nonlinear optical process called spontaneous parametric down-conversion (SPDC), in which an optical crystal illuminated by a laser beam spontaneously generates pairs of photons. Each generated pair is simultaneously entangled in momentum, frequency, and polarization. The quantum state generated via down-conversion provides a hyperentangled state in an infinite-dimensional Hilbert Space. One can exploit the richness of this state in many powerful ways that range from probing the fundamental ideas of quantum mechanics via Bell's inequalities and GHZ tests, to practical applications including metrology, quantum imaging, and secure communications.

The use of entangled states lies at the heart of quantum information processing and SPDC has been established as the best source of entanglement in optics. Femtosecond parametric down-conversion must be used to demonstrate counterintuitive effects such as quantum teleportation and entanglement swapping, as well as to generate multi-photon entangled states. It has been shown previously that dispersion effects arising from the use of ultra-short femtosecond laser pulses in SPDC result in the dramatic degradation of entanglement. Previous attempts to describe this phenomenon have been based on separate analyses of frequency, momentum, and space-time variables and, as such, have failed to provide a comprehensive theory that accords with experimental observations.

We present a formalism that incorporates the hyperentangled nature of the quantum state generated via SPDC. The key to providing an adequate physical description of parametric down-conversion is to consider the initial entangled state in its entirety, including the interplay among the different quantum variables. To cover a broad range of experiments the theory is kept general and comprises three fundamentally distinct steps: generation, propagation, and measurement. In proceeding thusly we refrain from imposing the characteristics of a particular measurement apparatus onto the structure of the quantum state. Depending on the intended application it is now possible to design an optimal experimental system that modifies the quantum state in accordance with the desired aim of a particular experiment. The validity of our model is confirmed by its total agreement with various pulse- and cw-pumped SPDC experiments carried out in our laboratory.

Single photon source from single NV centers in diamond

Alexios Beveratos, Rosa Tualle-Brouri,Jean-Philippe Poizat, Philippe Grangier

Laboratoire Charles Fabry de l'Institut d'Optique,
UMR 8501 du CNRS, B.P. 147, F91403 Orsay Cedex - France,

Quantum cryptography relies on the fact that single quantum states can not be cloned. In this way coding information on single photons would ensure a secure transmission of encryption keys. First attempts for quantum cryptography systems were based on attenuated laser pulses. However the poissonian distribution of the photon number does not guarantee both the uniqueness of the emitted photon and a high bit-rate. Therefore a key milestone for efficient and secure quantum cryptography systems is the development of single photon sources.

Several pioneering experiments have already been realized in order to obtain single photon sources. Among these attempts one can cite twin-photons experiments, coulomb blockade of electrons in quantum confined heterojunctions, or fluorescence emission from single molecules. Up to now interesting results were obtained, but considerable work is still needed to design a reliable system, working at room temperature with a good stability and well-controlled emission properties. More recently several systems have been proven to be possible candidates for single photon sources. Antibunching was indeed observed in CdSe nanospheres, thereby proving the purely quantum nature of the light emitted by these sources. In the same way photon antibunching in Nitrogen-Vacancy (N-V) colored centers in diamond was reported by our group [1] and by Kurtsiefer et al [2]. A remarkable property of these centers is that they do not photobleach at room temperature: the fluorescence level remains unchanged after several hours of continuous laser irradiation of a single center in the saturation regime. These centers are therefore very promising candidates for single photon sources.

We will report on our recent progress towards this goal using a single NV colored center in diamond as emitting dipole.

The experimental set-up consists of two parts. A home built confocal microscope allows us to collect the fluorescence coming only from a small volume within the diamond. The excitation laser can be either a 514nm Argon, or 532nm YAG, with maximum power of 40mW. The second part is a standard Hanbury Brown - Twiss set-up with 2 avalanche photodiodes, which allows us to realise photon correlation experiments with ns resolution.

With our system we are able to scan across the bulk diamond in a region of 10 by 10 micrometers. After choosing the center we want to study, a servo-locked program allows us to collect the fluorescence light emitted by the dipole. The analysys of the fluorescence light shows antibunching wich confirms the uniqueness of the defect center. We also analyzed the system dynamics through the measurement of the autocorrelation function, showing the existence of a shelving effect which reduces the counting rate of the fluorescence emission, and gives rise to photon bunching. We study the dependence of this behavior on the pumping power, and we compare the experimental results with the predictions of a three-level model using rate equations.

Further results towards achieving triggered single photon source will be presented.

[1] R.Brouri, A.Beveratos, J.-P. Poizat, P.Grangier, Opt.Lett. 25,1294-1296 (2000)
[2] C.Kurtsiefer, S.Mayer, P.Zarda, H.Weinfurter, PRL 85, 290-293 (2000)

A Quantum Key Distribution with N-array Encoding

M. Bourennane, A. Karlsson, G. Björk,
Department of Microelectronics and Information Technology,
Royal Institute of Technology (KTH),
Electrum 229, SE-164 40 Kista, Sweden.
N. Gisin, and H. Zbinden
GAP-Optique, Universite de Geneve, 20 rue de
l'Ecole de Medecine, 1211 Geneve 4, Switzerland

Quantum cryptography provides an unconditionally secret key distribution between two parties Alice and Bob, followed by secret key cryptography to encrypt a message sent over the public channel. In the original protocol proposed by Bennett and Brassard (BB84)[1], Alice and Bob choose randomly between two complementary bases and the information is encoded using two orthogonal states (qubits). An extension to six state (3 complementary bases) protocol shows that Eve's information gain is lower than in the BB84 protocol[2]. Very recently Bechmann-Pasquinucci and Peres have considered scheme using 3 states with 4 mutually complementary bases[3].

We propose new protocol for quantum key distribution that is based on higher dimensional quantum systems in N-dimensional Hilbert space. We consider two cases. In the first we use only two bases as in the original BB84 protocol, in the second case we use $N+1$ mutually complementary bases and N orthogonal quantum states in each basis. We have followed Wootters construction method for $N = p^k$, (where p is a prime and k an integer) to find the $N+1$ mutually complementary bases, where the quantum states satisfy $|\langle \psi_i^\alpha \mid \phi_j^\beta \rangle| = 1/\sqrt{N}$.

We study the mutual information between Alice and Bob, and Eve's information gain and the disturbance she causes. We have analysed different incoherent eavesdropping attacks as a function of the dimension of the Hilbert space such as (a) intercept/resend, intermediate bases, and Universal Quantum Cloning Machine eavesdropping attacks. As in the qubit case, the fidelity of the optimal incoherent eavesdropping strategy turns out to be identical to the Universal Quantum Cloning Machine [5]. We have consider coherent attacks in which Eve process several quNits jointly. We will give the upper limits for Bob's error rate when Eve uses incoherent and coherent eavesdropping attacks. Finally, we will discuss realistic quantum key distribution systems by considering the dark count of the detectors.

[1]C.H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), p.175.
[2] D. Bruss, Phys. Rev. Lett **81**, 3018 (1998)and H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[3] H. Bechmann-Pasquinucci and Asher Peres, quant-ph/0001083.
[4] W. K. Wootters and B. D. Fields, Ann. Phys., **191**, 363, (1989).
[5] M. Bourennane, A. Karlsson, and Gunnar Bjrk, accepted for publication Phys. Rev. A.

Submission for poster presentation

Effects of Experimental limits in Quantum Cryptography Systems based on polarization entangled photons

Stefania Castelletto[1], Ivo Pietro Degiovanni[2] and Maria Luisa Rastello

Department of Photometry Istituto Elettrotecnico Nazioanle G. Ferraris (IEN), strada delle Cacce 91, 10135 Turin, Italy

[1] *Electronic address: castelle@ien.it*

[2] *Electronic address: degio@ien.it*

Entangled photons, generated by spontaneous parametric down-conversion in nonlinear crystals (SPDC), had been proved largely and successfully in fields such as quantum communication, quantum radiometry, as well as, more recently, quantum cryptography key distribution (QCKD)[1-5]. Particularly, after the first proposal of Bennett and Brassard and later Ekert protocol invoking entangled states, various systems of QCKD have been implemented and tested by groups around the world. In this trend, it is only recently that some research groups [3,4] performed the first QCKD experiments based on polarization entangled photon pairs and Brassard *et al.* [6] proved theoretically that SPDC-based QCKD schemes offer enhanced performances mostly in terms of security with respect to the one based on weak coherent pulses.

In this communication, we investigate the effects of some experimental limits inducing perturbation in the ideal polarization entanglement in SPDC and yielding errors in the transmitted bit sequence. Since all SPDC-based QCKD schemes rely on the measurement of coincidence to assert the bit transmission between the two parties, we developed a statistical model to calculate the accidental coincidences that might contribute to errors in the raw key, otherwise not completely accounted for by simple experimental means. This model considers firstly that, the practical deviation from maximally entangled states, due either to a trivial misalignment or a pump polarization residual impurity, may originate true coincidences but possibly some errors in the bit sequence transmission. We therefore calculate, for all possible choices of polarization analyzers settings, the probability distributions of coincidence counts, arising either from authentically entangled pairs or accidental photons, the latter due to different photon rates and degree of correlation generally present in the two-photon channels selected, as well as dark counts, stray light, optical losses, non-unitary quantum efficiency of detectors, electronic dead times and the finite temporal coincidence window. Eventually we discuss how all these unwanted effects modify Bell's inequalities expected results. Furthermore this model predicts precisely the quantum bit error rate (QBER) and the raw keys and guarantees a method to compare different security criteria of the hitherto proposed QCKD protocols.

This model may provide an objective assessment of performances and advantages of different systems.

[1] A. V. Sergienko, M. Atature, Z. Walton, G. Jaeger, B. E. A. Saleh, M. C. Teich Phys. Rev. A , **60**, 2622 (1999)

[2] T. Jennewein, C. Simon, G. Weihs, H. Weinfurther, A. Zeilinger Phys. Rev Lett. **84** 4729 (2000)

[3] D. Naik, C. Peterson, A. White, A. Berglund, P. Kwiat Phys. Rev Lett. **84** 4733 (2000)

[4] W. Tittel, J. Brendel, H. Zbinden, N. Gisin Phys. Rev. Lett. **84** 4737 (2000)

[5] G. Brassard, N. Lutkenhaus, T. Mor, B. Sanders Phys. Rev. Lett. **85** 1330 (2000)

Twin photon production by quasi phase matching with PPLN.

Christophe Couteau*, Christian Mikkelsen, John Rarity, Dik Bouwmeester.

Centre for Quantum Computation, Clarendon Laboratoty, University of Oxford, Oxford OX1 3PU

* *Electronic address: christophe.couteau@qubit.org*

Entangled photons play a crucial role in the schemes for quantum cryptography and quantum communication. Unfortunately, most of the currently used pair photon sources, such as type I and type II BBO crystals, have a very low efficiency which is a serious limitation for any commercial applications.
Recently, new ways have been proposed to produce bright sources of photon pairs using artificial crystal configurations that can be fabricated with modern solid state / semiconductor techniques. We will report on our collaboration with manufactures of these novel devices. In particular, we present the production of pair photons using periodically poled materials like lithium niobate (PPLN) that have been produced by the Optoelectronics Research Centre at the University of Southampton.
As a first step, we plan to characterise the conversion-efficiency and the bandwidth of the coherence length and the two photon coherence length of a pulsed PPLN source.
Furthermore, we will discuss ideas on how to modify the pair photon sources in order to produce pulsed polarisation entangled photon pairs as many as possible.

Secure authentication of classical messages with a one-ebit quantum key

Marcos Curty and David J. Santos*

Abstract

Although secret communication, in the form of quantum cryptography, is arguably the most studied context on which to apply quantum information processing techniques, message authentication, i.e. certifying the identity of the message originator and the integrity of the message sent, can also benefit from these techniques. In classical symmetric cryptosystems the security of the message authentication procedure relies on the length of the secret authentication key employed. In the case of a key just a few bits long, brute-force attacks make these methods particularly vulnerable. In this paper we propose a quantum authentication procedure that, making use of just one ebit as the authentication key, allows the authentication of classical messages in a secure manner.

*Marcos Curty and David J. Santos are with the Departamento de Tecnologías de las Comunicaciones, Universidad de Vigo, Campus Universitario s/n. E-36200 Vigo (Spain).

Exploring Multi-Photon Entanglement

Gabriel Durkin, Antia Lamas, John Howell, Dik Bouwmeester

Centre for Quantum Computation, Department of Physics, Oxford University, Clarendon Laboratory, Parks Road, Oxford OX1 3PU, United Kingdom

A proposal is made to investigate the possibilities for many correlated photon signals in quantum communication. Experimentally, new techniques are employed to increase the signal strength of such many photon entanglements. We consider a scheme which relies on the stimulated emission of polarisation entangled pairs. The state created by this process is characterised by

$$|\psi\rangle \sim \sum_{n=0}^{\infty} \frac{r^n}{\sqrt{n!(n-1)!}} \times \left(\sum_{m=0}^{n} (-1)^m |(n-m), m; m, (n-m)\rangle \right), \quad (1)$$

where n is the number of photon pairs produced in the down conversion process, and 'r' defines the non-linear interaction strength. We used the shorthand notation $|i,j;k,l\rangle$ for $|i\rangle_{ah}|j\rangle_{av}|k\rangle_{bh}|l\rangle_{bv}$ and $|0\rangle$ represents $|0,0;0,0\rangle$.('a' and 'b' are the two distinct down-converted spatial modes , and 'v' and 'h' refer to the polarisations, vertical and horizontal.) Projecting this state onto a fixed value of n produces purified entanglement. We describe ways of exploiting this feature for secure information transfer. Experimental techniques to perform this projection onto a particular 'n' state are discussed, comprising both post-selection and other approaches. We then propose to use these purified states for secure quantum key distribution, using an approach more robust against eavesdropping than the well known one photon pair protocol.

New entangled multiphoton state

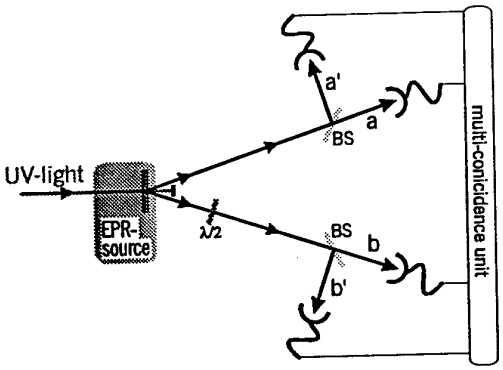
Manfred Eibl[1], Sascha Gaertner[2], Christian Kurtsiefer[2], Harald Weinfurter[1,2] and M. Zukowski[3]

[1] *Max-Planck-Institut für Quantenoptik (MPQ)*
MPQ, Hans-Kopfermann-Str.1, 85748 Garching, Germany

[2] *Ludwig Maximilian Universität (LMU)*
LMU München, Sektion Physik, Schellingstrasse 4/III, 80799 Munich, Germany

[3] *Instytut Fizyki Teoretyczney i Astrofizyki, Uniwersytet Gdanski, PL-80-952 Gdansk, Poland*

Multiphoton entanglement is the basis of new quantum communication schemes like quantum cloning, quantum secret sharing and teleportation of entanglement. Moreover it is the cornerstone of new studies of local realistic theories and the study of novel features of multiparticle entanglement and decoherence.
Among the multiphoton states until today only the three and four photon GHZ-states [1,2,3] are experimentally realized. We describe the generation of a new entangled multiphoton state with pulsed type II parametric downconversion. In cw-downconversion one usually produces pairs of polarization-entangled photons. For pulsed downconversion sources there is a non-negligible propability to get two pairs emitted simultaneously. We use 'pair-bunching' to generate new partially entangled 4-photon-states.



The 4 photon state is observed with a nonpolarizing beamsplitter in each arm of the down-conversion source. Conditioned on detection in the four outputs of the beamsplitters we get the state

$$\Psi = \frac{1}{\sqrt{3}}(\sqrt{2}GHZ_4 + EPR_2 \otimes EPR_2)$$

This new state is a superposition of a 4 photon GHZ-state and a product of two Bell-states. Whereas a 4-photon GHZ-state exhibits pure 4 particle entanglement this new state has in addition entanglement between photons in the same arm. Although Ψ is only partially entangled it strongly violates a generalized 4-particle Bell inequality.

[1] D.Bouwmeester, J.W. Pan, M.Daniell, H.Weinfurter, A.Zeilinger, PRL 82, 1345 (1999)
[2] A. Zeilinger, M. Horne, H. Weinfurter, M. Zukowski, PRL 78, 3031 (1997)
[3] private communication J.W. Pan, M. Daniell, G. Weihs, A. Zeilinger

Quantum teleportation of continuous variables, physical meaning of various criteria.

Frédéric GROSSHANS
I.O.T.A.
F91403 ORSAY CEDEX
France

Quantum teleportation, a concept introduced by Bennett et al. in 1993 for qubits, allows to construct an exact replica of an unknown quantum state. As pointed by Bennett et al., "the original state is destroyed during this process, as it must be to obey the no cloning theorem".

We discuss the criteria used for evaluating the efficiency of quantum teleportation shemes for continuous variables and their physical meaning. If a perfect teleportation with unity fidelity F=1 is not reachable, two limits have been proposed for succesful teleportation. If a fidelity higher than 1/2 is sufficient to make a copy of the initial state better than any classical copy and to allow quantum entanglement transfer, a fidelity higher than 2/3 is required to guarantee the destruction of the original state.

Vacuum-stimulated photon generation in a high-finesse optical cavity

Markus Hennrich, Thomas Legero, Axel Kuhn and Gerhard Rempe

Max-Planck-Institute for Quantum Optics,
Hans-Kopfermann-Str. 1, D-85748 Garching, Germany

Many attempts to realize elementary quantum-logic gates as well as the feasible schemes for quantum cryptography and quantum teleportation are based on the availability of a single photon in a well defined mode of the radiation field. However, most employed schemes used for photon generation rely on spontaneous processes or on parametric down conversion and produce photons at more or less random times. Only recently, different photon generation schemes have been demonstrated, like a single-photon turnstile device, based on the Coulomb blockade mechanism in a quantum dot, the fluorescence excitation of a single molecule or the excitation of single colour centers or quantum dots. All these new schemes emit photons upon an external trigger event. However, the photons are spontaneously emitted into many modes of the radiation field and usually show a broad energy distribution.

In contrast to these, our scheme leads to a photon emission into a single mode of the electromagnetic field of a high-Q optical cavity. It's loosely based on a proposal by Law et al. [1], but basically relies on stimulated Raman scattering involving adiabatic passage [2]. We present our results on vacuum-stimulated Raman scattering from Lambda-type three level atoms in a high-finesse optical cavity [3]. An excitation scheme similar to the well known "stimulated Raman scattering involving adiabatic passage" (STIRAP) process is realized here, but the stimulating laser is replaced by the interaction of the atoms with the vacuum field of a high-finesse optical cavity.

The Raman pump transition is excited by a laser beam crossing the cavity transverse to its axes, and the stimulated transition is resonant to the TEM00 mode of the empty cavity surrounding the atom. The vacuum field of the cavity stimulates a Raman transfer, which inevitably places photons into the former empty cavity mode. These photons are counted as soon as they are transmitted by one of the cavity mirrors. The characteristic dependence of the photon production rate from the cavity- and the pump laser detuning is a clear evidence for a stimulated Raman process and cannot be attributed to enhanced spontaneous emission. In addition, we see that the excitation spectrum is of sub-natural line width. Therefore the atom must follow a dark state throughout the interaction, thus avoiding any electronic excitation, i.e. line broadening by spontaneous emission cannot occur.

[1] C.K. Law and H.J. Kimble, J. Mod. Opt. **44**, 2067-2074 (1997).
[2] A. Kuhn, M. Hennrich, T. Bondo and G. Rempe, Appl. Phys. B **69**, 373-377 (1999).
[3] M. Hennrich, T. Legero, A. Kuhn and G. Rempe, Phys. Rev. Lett. **85**, 4872-4875 (2000).

80km transmission test of an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55μm

*Phil Hiskett, Gerald Buller and Paul Townsend**

Department of Physics, Heriot-Watt University, Edinburgh, UK, EH14 4AS.

**Corning Research Centre, Ipswich, UK, IP5 5RE.*

A polarisation-based quantum cryptography receiver incorporating an InGaAs/InP single photon avalanche photodiode (SPAD) has been constructed to investigate the potential for increasing the transmission distance in long wavelength QKD systems beyond the 40-50km range that has been reported to date [1,2]. The experimental set up was used to investigate two different approaches towards the achievement of system timing and synchronisation: spatial multiplexing and wavelength division multiplexing (WDM).

The first version of the system (figure 1) employed 40km of dispersion shifted optical fibre (Corning DS). Two optical sources emitting pulses at 100 kHz repetition rate were used in the system: a 1.55μm wavelength DFB laser that was highly attenuated so that each pulse contained, on average, only 0.1 photons and a synchronously triggered 1.3μm wavelength DFB laser for timing purposes. A combination of WDM couplers and filters was used to combine and separate the two wavelength channels at the transmitter and receiver ends of the system respectively. The SPAD was normally biased just below breakdown. Upon detection of the 1.3 μm wavelength pulse a gate generator applies a voltage pulse to the SPAD to bias it above breakdown synchronously with the arrival of the weak 1.55μm signal. The system was operated in gated mode, a technique now widely used in photon-counting and in particular in QKD [2,3], where the width of the gate pulse was restricted to 3.5ns to limit the effects of afterpulsing.

The quantum bit error rate (QBER) of this system was measured for the 40km transmission fibre and for different settings of Attn#2 corresponding to higher loss and therefore simulating longer transmission distances. The results in figure 2 show that the QBER remains below 15%, the theoretical upper limit for secure communication with an ideal single photon source [4], up to a (simulated) distance of 96km. In a successive experiment the 40km reel of optical fibre was replaced by a 51km reel, but longer transmission distances were prevented by the relatively high loss in the timing channel (0.4dB/km at 1.3μm vs. 0.25dB/km at 1.55μm). In a second version of the experiment the timing channel wavelength was changed to 1.55μm and was transmitted over a separate fibre (i.e. spatial multiplexing). The transmission distance could then be increased to 80km and the QBER measurement repeated. As shown in figure 2 this result (QBER = 5%) is in good agreement with the predicted values obtained using optical variable attenuators, confirming both negligible cross talk in the WDM scheme and negligible dispersion penalties at the increased 80km transmission distance in the spatial multiplexing scheme. The results confirm the potential for increasing the transmission distance to the 80km range in quantum cryptography systems based on InGaAs/InP SPADs

[1] P.D. Townsend, *"Quantum cryptography on optical fibre networks", Optical Fibre Technology, 4 (4), Page.345-70, (1998)*

[2] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Jonsson, T. Tsegaye, D. Ljunggren and E. Sundberg, *"Experiments on long wavelength (1550nm) 'plug and play' quantum cryptography systems"*, Optics Express, **4** (10), Page 383-387, (1999)

[3] G. Ribordy, J-D Gautier, N. Gisin, O. Guinnard and H. Zbinden, *"Automated 'plug & play' quantum key distribution"*, Electronics Letters, **34** (22), Page 2116-2117, (1998)

[4] N. Lutkenhaus, *"Security against eavesdropping in quantum cryptography"*, Physical Review A, **54** (1), Page 97-111, (1996)

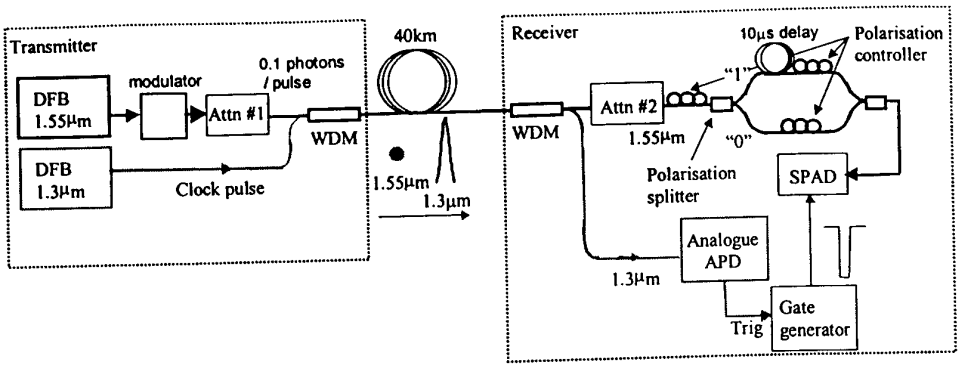


Figure 1 The QC system containing the InGaAs/InP SPAD. The increase in length of optical fibre can be simulated by further increasing the attenuation at the second attenuator (Attn#2). The clock pulse in the system is a 1.3μm wavelength pulse from a DFB laser. Both the 1.3μm and 1.55μm laser were operated at 100kHz, however, a modulator was used to divide the frequency of the 1.55μm laser by a factor of two.

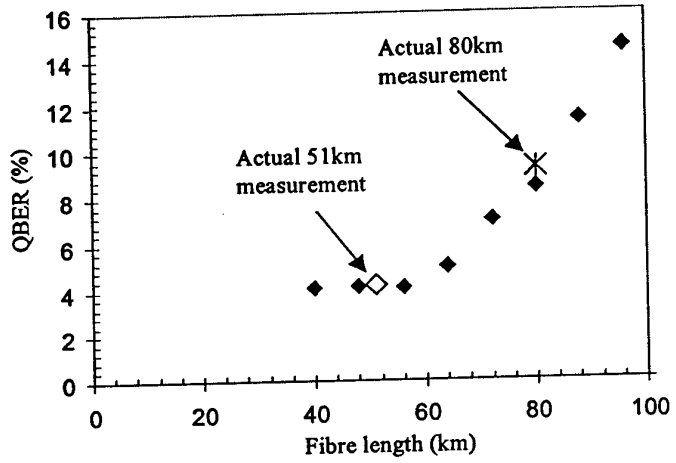


Figure 2 The graph of QBER against fibre length. The main curve was taken for a 40km system and the extra fibre lengths simulated by using a second attenuator. The 40km fibre reel was replaced by a 51km and 80km reel and the QBER was measured at these two actual distances.

General 3 element POM for light polarisation measurements

Kieran Hunter
University of Strathclyde

Abstract:

A von Neumann measurement on a system corresponds to a projection onto some set of basis states of the system. This is not, however, the most general measurement on the system which can be performed.

A general measurement corresponds to a projection onto a set of complete or overcomplete states, and is described by a set of operators, called a probability operator measure (POM). A von Neumann measurement is a special case of a POM where all of the elements are orthogonal.

In discrimination amongst a set of non-orthogonal or overcomplete states, von Neumann measurements do not generally represent the optimal measurement strategy, and the form of the general measurement must be used.

We have obtained the general from for a 3 element POM in a space of 2 basis states, stated in the formalism of the polarisation states of light.

We have used the parameters of this POM to propose an experimental scheme for resolving a general 3 element polarisation POM.

Optimal N-to-M cloning and phase-conjugation for continuous quantum variables

Sofyan Iblisdir
Ecole Polytechnique, CP 165/56, Universite Libre de Bruxelles
50 avenue F. D. Roosevelt, B-1050 Bruxelles, Belgium

Abstract:

Abstract:

The N-to-M symmetric cloning of continuous quantum variables is investigated. An argument based on state estimation is used to derive the maximum possible cloning fidelity of a coherent state: F=MN/(MN+M-N). A scheme achieving this bound is presented. It only requires a phase-insensitive linear amplifier, and a network of beam-splitters.

Besides cloning, the question of phase conjugation is also discussed. It is shown that it can be performed optimally using a fully classical procedure (just as for flipping quantum bits). A related result is that more information can be encoded into a pair of phase-conjugated coherent states than in two replicas of a same coherent state.

An all-fiber Bell State Analyzer for Quantum State Teleportation

T. Jennewein, G. Weihs, A. Zeilinger
Institute of Experimental Physics, University of Vienna,
Boltzmanngasse 5, A 1090 Wien, Austria

We have devised an all-fiber bell state analyzer as the element necessary for realizing experiments on quantum state teleportation, entanglement swapping and experiments towards quantum computation with photons. The advantage of using fiber optic components over free space components is the confinement of the photons in the fiber. A first experiment on entanglement swapping using the all-fiber bell state analyzer has shown a high visibility. Next steps will include the realization of a more complete bell state analyzer, which will allow to identify two of the four bell states for controlling a very fast polarization modulator in order to achieve more efficient teleportation as well as first steps towards quantum computation with linear elements.

Investigation of dye molecules in a microcavity – photostability and extraction efficiency

P Jonsson, J. G. Rarity [1], P. R. Tapster [1] and S. C. Kitson [1]

Department of Electronics, Royal Institute of Technology (KTH), Electrum 229, SE-164 40 Kista, SWEDEN
Phone +46-8-752 1206, Fax +46-8-752 1240, Electronic address: perj@ele.kth.se

[1] *DERA, St. Andrews Road, Malvern, Worcs., WR14 3PS, UK*

This paper presents the latest progress in our work towards the development of a high efficiency source of single photons for quantum optics applications. We aim to do this by isolating a single dye molecule thus limiting the emission per pump pulse to a single photon. We are placing the dye molecules in a microcavity to achieve a better collection efficiency of the spontaneous emission. The main technological problems are those of increasing the average number of emission cycles from a single dye molecule before it undergoes irreversible photobleaching, and of efficiently collecting and tailoring the fluorescence from the dye molecules. To date we have only been able to study dye solutions where the dye molecules are replaced by diffusion before they undergo irreversible photobleaching. The diffusion makes the number of emitters fluctuate and the antibunching we see is therefore super-Poissonian and not sub-Poissonian as needed for single-photon generation. However, the investigations show that dye molecules could be used as single-photon emitters if the bleaching problem is overcome.

A substantial part of the paper is devoted to means of reducing the bleaching rate. It is a common belief that singlet oxygen, produced in the quenching process of the dye metastable triplet-state, is the main promoter of bleaching. Therefore, we have studied routes to reduce the bleaching by lowering the oxygen concentration in the dye solution and by adding an alternative triplet-state quencher, cyclooctatetraene. We have analysed our systems by measuring the intensity correlation function, $g^{(2)}(\tau)$, of the fluorescent light over a time scale ranging from nanoseconds to seconds [1]. The correlation function gives information about the dye molecule dynamics, such as the excited state lifetime and the triplet-state lifetime and population. Our investigations show that the method to reduce the bleaching rate by adding triplet-state quenchers in an oxygen-free solution is more complicated than expected and that no reduction in the bleaching rate has yet been seen.

The paper also explores the possibility of controlling the spontaneous emission from the dye molecules with a microcavity. Our microcavity consists of two planar dielectric mirrors, made from alternating layers of silica (SiO_2, n =1.50) and tantalum pentoxide (Ta_2O_5, n = 2.27). The peak reflectivity of the mirrors is designed to be at a wavelength of 560 nm, which corresponds to the fluorescence peak of the dye molecules. The top layer of each mirror is silica, deliberately grown 20 nm thinner than the Bragg condition, $\lambda/4n$, and the microcavity is formed by placing a drop of the dye solution on one mirror and then pressing the two mirrors together. The resulting structure is a $\lambda/2n$ thick microcavity with an incorporated dye layer, approximately 50 nm thick in the centre. We are achieving a modest 4 % geometric collection efficiency and 0.5 % overall detection probability. The main advantage of the microcavity is the narrowing of the bandwidth of the collected emission (10 nm) compared to the free space emission (25 nm), which makes the discrimination of the fluorescence from the pump light easier.

[1] S. C. Kitson, P. Jonsson, J. G. Rarity, and P. R. Tapster, Phys. Rev. A 58, 620 (1998).

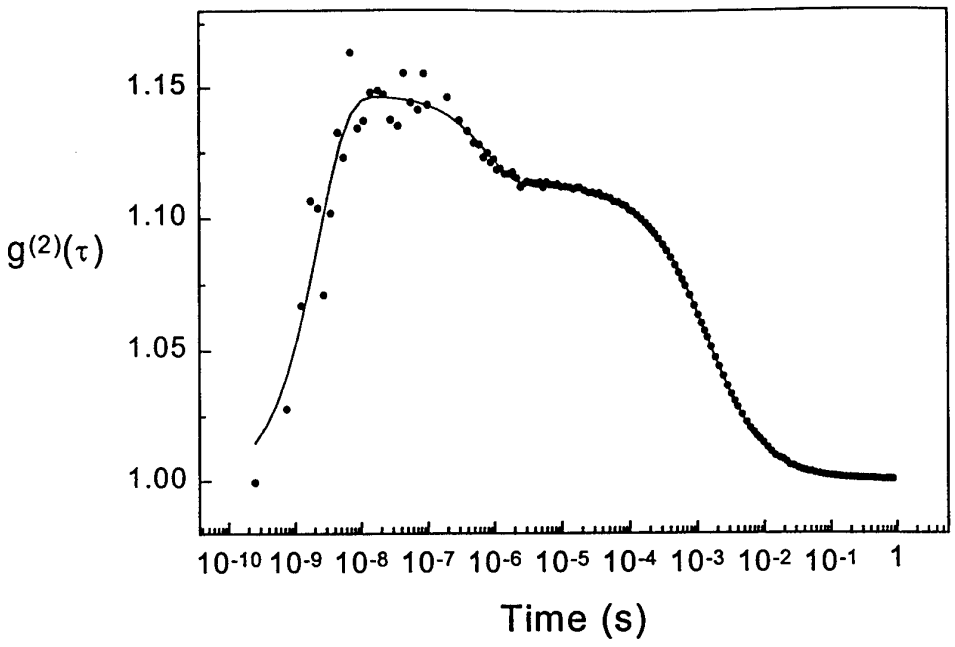


Figure: Experimental data (dots) and theoretical fit (red line) of the intensity correlation function, $g^{(2)}(\tau)$, obtained with the microcavity containing a solution of 10^{-9} Molar Rhodamine 6G in Propylene Carbonate.

Spin squeezing in atomic systems

V. Josse, L. Vernac, M. Pinard, E. Giacobino

Laboratoire Kastler-Brossel, Université P. et M. Curie, case 74, F-75252, Paris Cedex 05, France- Tel: 00 33 1 44 27 43 93 – Fax: 00 33 1 44 27 38 45
e-mail: josse@spectro.jussieu.fr

In high-precision atomic experiments such as atomic interferometry, the accuracy is ultimately limited by the so-called quantum projection noise, due to the fact that the atoms are not in an eigenstate of the measured quantity. In an ensemble of N independent atoms, fluctuations proportional to $N^{-1/2}$ result from this effect. A few years ago, it was shown that using squeezed atomic states would allow to reduce these fluctuations, in the same way as squeezed states of light allow to obtain noise reduction in measurements of the electromagnetic field. Recently, it was proposed to use absorption of squeezed light by atoms in single pass to produce spin squeezing.

We have investigated an alternative method in which a cold cesium atoms cloud interacts with light in an optical cavity. Under our experimental conditions, the cold atoms behave like a Kerr medium. It has been known for a long time that a Kerr medium can reduce the fluctuations of light below the standard quantum limit, transforming a coherent state into a squeezed state. The interaction with such squeezed state can in turn modify the atomic fluctuations. Indeed we have theoretically shown rigorously for the first time that, in the same conditions, the collective spin of the atomic ensemble is squeezed.

We have also obtained squeezing of a collective atomic spin by having it interact with incident squeezed light in an optical cavity. Here the optimal conditions for a transfer of squeezing from the incoming pump light to the atoms correspond to a non saturating light intensity, in the strong coupling regime. These results are conceptually very important since they show that it is possible to create quantum correlations within an ensemble of atoms in an optical cavity, in spite of the inevitable coupling to the vacuum fluctuations.

In order to make an experimental demonstration of spin squeezing, we propose the following scheme : the incoming pump (the field that is squeezed by non linear interaction) is linearly polarized and nearly resonant with the atomic closed transition 6S(1/2) F=4 – 6P(3/2) F=5 . Then the fluctuations of the e.m perpendicular to the mean field (that is called the « polarization noise ») of a weak linearly polarized probe beam is assumed to be sensitive to the atomic fluctuations. By setting the frequency of the probe near resonance with the atomic transition 6P(3/2) F'=5 – 6D(5/2) F''=6 (or 6S(1/2) F=4 – 6P(3/2) F'=5) we should observe the fluctuations relative with the excited (or ground) levels and determine if they are squeezed or not.

As the pump have to be polarized we focused until now on the study of its proper fluctuations. The polarization of the pump transmitted by the cavity exhibits an unstable behaviour, since it can be circular for certain values of detuning between laser and cavity. We observed squeezing for both « usual » quantum noise (the noise of the quadrature of the e.m of the mean field) (about 5%) and « polarization noise » (about 10%). To explain this preleminary results on the « polarization noise », we derived a four level model. The analyse of the optical pumping and the experimental behaviour of the polarization of the beam transmitted by the cavity are both in good agreement with our four level approach, if we assumed an important relaxation rate between the excited levels. Under the same condition, this model can also explain all our experimental results for the fluctuations.

We are now working on the set up of the probes beams in order to show the production of a collective spin squeezing.

Continuous Variable Polarization Entanglement and Quantum Key Distribution

Natalia Korolkova[1], Christine Silberhorn[1], Timothy C. Ralph[1,2], Rodney Loudon[1,3] and Gerd Leuchs[1]

[1] *Zentrum für Moderne Optik, Universität Erlangen Nürnberg, Staudtstr. 7/B2,D-91058 Erlangen, Germany*
[1] *Electronic address: korolkova@kerr.physik.uni-erlangen.de*

[2] *Department of Physics, University of Queensland, St Lucia, QLD 4072, Australia*

[3] *Electronic Systems Engineering Department, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK*

Continuous variable polarization entanglement [1] is related to the quantum correlations of the uncertainties of quantum Stokes operators which determine a polarization of a quantum state. This type of entanglement can be generated by linear interference of two polarization squeezed beams in analogy to the successful interference scheme for bright EPR-entanglement of amplitude and phase [2]. Hereby the notion of polarization squeezing implies the reduction of an uncertainty of one of the Stokes operators below that of the coherent light at the cost of growing uncertainty in other Stokes parameters [1]. The important advantage of such non-classical polarization states is the possibility to determine fully experimentally the relevant conjugate variables of a polarization-squeezed or a polarization-entangled field in direct detection only, using linear optical elements.

We present here the definition of continuous variable polarization entanglement and a way to generate it. Towards the experimental quantum communication, we consider an experimental characterization of continuous variable entanglement: polarization entanglement and entanglement of field quadratures. The notions of squeezed-state, EPR-, and QND-entanglement are introduced and their mutual relations are discussed.

As an application of squeezed-state- and EPR-entanglement for communication purposes, we propose a quantum key distribution (QKD) scheme using continuous EPR-like correlations of bright optical beams. For binary key encoding, the continuous quantum information is discretized in a novel way by associating a respective measurement, amplitude or phase, with a bit value "1" or "0". The implementation of the QKD scheme on the basis of continuous variable polarization entanglement avoids a cumbersome phase measurement and enables us to operate the key distribution with direct detection only making advantage of stable and efficient bright entanglement source.

[1] N. Korolkova, G. Leuchs, R. Loudon, T. C. Ralph, and Ch. Silberhorn. "Polarisation Squeezing," in preparation; N. Korolkova and G. Leuchs: *Multimode Quantum Correlations*, in "Coherence and Statistics of Photons and Atoms", J. Peřina (ed.), John Wiley & Sons, Inc., 2000, in press.
[2] Ch. Silberhorn, P. K. Lam, O. Weiß, F. König, N. Korolkova, and G. Leuchs, "Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fibre," submitted (2000).

Stimulated parametric down-conversion

Antia Lamas Linares

Center for Quantum Computation - University of Oxford
phone: 01865 282203 - fax: 01865 272400
a.lamas@qubit.org

The process of stimulated parametric down-conversion is used to exponentially enhance the probability of emission of polarisation entangled photons.

In particular we produce the many-photon equivalent of the antisymmetric Bell state and use its detection as a signature of laser-like operation. We will present experimental results that show the onset of lasing operation and discuss the many potential applications of this source in quantum information and fundamental tests of quantum mechanics.

LJUNGGREN Daniel

EPR-type entangled beams production using self-phase locked OPO

L. Longchambon, N. Treps, S. Ducci, A. Matre, T. Coudreau, C. Fabre *Laboratoire Kastler Brossel, Universit Pierre et Marie Curie Case 74,75252 Paris Cedex 05, France*

Abstract

It is well known that spontaneous parametric down-conversion produces EPR states for photon pairs in the directions where the two cones of spontaneous parametric fluorescence intersect. This situation has strong analogies with what occurs in some circumstances with Optical Parametric Oscillators(OPO's), which are likely to oscillate simultaneously on two pairs of signal and idler modes. It can be shown that the bright output beams of the OPO have in this case strong quantum correlations on different continuous observables.

A type II OPO comprising a birefringent plate oscillates in some circumstances in a locked regime[?, ?], where the ordinary and the extraordinary beams generated by the parametric effect are at the same frequency and are phase-locked to each other in a way that one circular mode oscillates. We will show that this system generates EPR-type entangled beams which can be used in quantum teleportation experiments.

References

[1] C. Fabre, E.J. Mason, N.C. Wong, *Theorical analysis of self-phase locking in a type II phase-matched optical parametric oscillator*, Opt. Comms. **170**, 299(1999)

[2] E.J. Mason, N.C. Wong, *Observation of two distinct phase states in a self phase-locked type II phase-matched optical parametric oscillator*, Opt.Letters **23**, 1733(1998)

Squeezed State Entanglement for Free Space Quantum Cryptography

Stefan Lorenz, Christine Silberhorn, Michael Langer,
Natalia Korolkova and Gerd Leuchs

Zentrum für moderne Optik, Universität Erlangen-Nürnberg,
Staudtstr. 7 / B2, D-91058 Erlangen, Germany
email: stefan.lorenz@physik.uni-erlangen.de

Quantum key distribution is on the verge of commercial applications as means of establishing secure data transmissions. While most of the existing experiments use single photons, we intend to utilize EPR-entangled multi-photon pulse pairs. They can be generated at a higher repetition rate, leading to decreased key distribution times. The entanglement can be produced by interference of two quadrature squeezed pulses at a beamsplitter. To produce the quadrature squeezed pulses we will use an asymmetric fiber Sagnac interferometer [1]. The nonlinear Kerr effect in the Sagnac interferometer can be exploited to produce amplitude squeezed pulses of high quality [2].

In contrast to existing experiments, we use a microstructured fiber [3] instead of a standard single mode fiber in the interferometer. This fiber has a very small mode field diameter leading to enhanced nonlinearity. Therefore the fiber length can be reduced, minimizing other noise producing effects such as e.g. guided acoustic wave brillouin scattering (GAWBS). In addition, the zero dispersion wavelength of the fiber lies at about 800nm, giving us the possibility to produce bright entangled pulses at a wavelength which is suited for free space transmission. The results of our experiment can therefore be used to build secure optical free space data links.

[1] S. Schmitt et al., Phys. Rev. Lett. **81**, 2446 (1998)
[2] Ch. Silberhorn et al., „Generation of continuous variable Einstein-Podolsky-Rosen entanglement via the Kerr nonlinearity in an optical fibre", Phys. Rev. Lett., submitted (2000)
[3] J.K. Ranka et al., Optics Letters **25**, No. 11, 796 (2000)

High-Speed Quantum Key Distribution Experiment

Vadim Makarov(1), Dag R. Hjelme(1), Andre Mlonyeni(2), Kirill Vylegjanine

(1)NTNU, Trondheim
(2)Telenor R&D, Kjeller (Oslo)

Abstract:

The quantum key distribution experiment uses Townsend interferometer structure with polarization maintaining fiber at 1300nm and BB84 protocol. Afterpulse blocking technique is utilized in APD-based single photon detector to achieve high pulse rate.

The latest experimental results will be presented.

Quantum Secure Multiparty Computations

J. Müller-Quade

Arbeitsgruppe QC Prof. Beth, IAKS, Fakultät für Informatik, Universität Karlsruhe, Am Fasangarten 5, 76 128 Karlsruhe, Germany

**Electronic address: muellerq@ira.uka.de*

In this contribution we present the advantages quantum secure multiparty computations have over classical secure multiparty computations. We focus on the three party case, the simplest case where these advantages can be seen. The capabilities of quantum secure multiparty computations are compared with what can be achieved in the private channel model or with an oblivious transfer channel between any two players.

For secure multiparty computations two cheating strategies of possible collusions can be distinguished. Whenever a collusion of players deviates from the protocol in a way that no honest player can detect any cheating we call this type of faulty beaviour a *Byzantine fault.* Deviations of the protocol which can be noticed by the honest players are called a *Non-Byzantine faults.* The known results about classical multiparty computations can, for the three party case, be summarized as follows:

Theorem 1

- *For three players who are by pairs connected by private and authenticated channels and have access to a broadcast channel all functions can be computed by multiparty secure computations if two players are honest and only Byzantine faults occur.*
- *For three players who are by pairs connected by private and authenticated oblivious transfer channels and have access to a broadcast channel all functions can be computed by multiparty secure computations if only Byzantine faults occur.*
- *Non-Byzantine faults cannot be tolerated in the above situations. of the protocol.*

For quantum secure multiparty computations we can prove:

Theorem 2

- *For three players who are by pairs connected by private and authenticated quantum channels and have access to a broadcast channel all functions can be computed by multiparty secure computations if two players are honest and only Byzantine faults occur.*
- *After termination such a protocol can additionally become robust against Byzantine faults of one collusion of two players.*
- *Non-Byzantine faults in the above situation can be tolerated if two players are honest.*

The basic idea of the proof is to use secret sharing to force honest measurements. After these measurements the possibilities of cheating are less and one more collusion can be tolerated. In our protocols Non-Byzantine faults always yield a conflict between two players. To continue with the protocol in case of a conflict between two players one lets the third player arbitrate between the players in conflict. The third player forwards the quantum information from one player to the other such that the receiver cannot distinguish between quatum states of the other two players. This way it becomes obvious for the arbiting party who is cheating. But as he has to forward the quantum information before he gets to know the bases used the arbiting party is unable to obtain any information from the other players.

So for three party protocols and byzantine faults the cryptographic strength of a quantum channel lies strictly between the strength of a private channel and that of oblivious transfer.

Quantum public key based cryptographic scheme using continuous variables

Patrick Navez, Alessandra Gatti, Luigi A. Lugiato

INFM, Dipartimento di Scienze CC FF MM,
Universita degli Studi dell'Insubria, Via Valleggio 11,
I-22100 COMO, Italy
**Electronic address: navez@mi.infn.it*

By analogy to classical cryptography, we develop a "quantum public key" based cryptographic scheme in which both the public and private keys consist in each of two entangled beams of squeezed light. An analog message θ is encrypted by modulating the phase of the beam sent in public. The knowledge of the degree of non classical correlation between the beam quadratures measured in private and in public allows only Bob to decrypt the message. The two quadratures measured by Bob and Alice can be expressed in terms of the field operators describing each beam:

$$\hat{Z}_{1'} = e^{-i\theta_A}\hat{a}_1 + e^{i\theta_A}\hat{a}_1^\dagger \quad (1)$$

$$\hat{Z}_2 = e^{-i\theta_B}\hat{a}_2 + e^{i\theta_B}\hat{a}_2^\dagger , \quad (2)$$

where $\theta_A = \phi_A + \theta$. ϕ_A and θ_B are the phases of the local oscillators used by Alice and Bob, respectively, in their homodyne measurements and determine which quadrature they select for their measurements. θ_B must remain private to Bob whereas ϕ_A must be communicated in public to Bob. Bob decrypts the message by measuring the noise associated to the quadratures difference ($\hat{Z}_- = \hat{Z}_{1'} - \hat{Z}_2$):

$$\langle\Psi|\delta^2\hat{Z}_-|\Psi\rangle = 2\left[\cosh 2r - \cos(\theta_A + \theta_B)\sinh 2r\right] \quad (3)$$

$$\overset{r\gtrsim 1}{\to} 4\sinh 2r \sin^2\frac{(\theta_A + \theta_B)}{2} \quad (4)$$

where r is the squeezing parameter. Fig.1 depicts a possible setup. The two EPR "q-private" and "q-public" beams are generated through a nondegenerate parametric down conversion process. They result from the fluorescence of a pump beam passing through a type II crystal acting also as an optical parametric amplifier (OPA). The quadratures components are measured in a homodyne detection with the help of local oscillators fields (LO). The pump field, which generates the two EPR beams via parametric down conversion, is obtained by one intermediate second harmonic (SHG) step as usual. While Bob carries out the homodyne detection of one quadrature of beam 2 for phase θ_B, Alice encrypts the message θ by modulating the beam 1 phase (e.g. by means of an electro-optical modulator), before carrying out the measurement of the quadrature ϕ_A.

Finally in a view towards absolute security, we formally prove that any external intervention of Eve makes her vulnerable to any subsequent detection. Furthermore, we describe how Bob can detect the presence of Eve provided he keeps the knowledge of the squeezing parameter r private. In contrast to single photon system where r does not exist, this parameter plays in our scheme an important role in the context of security aspects.

[1] P. Navez, A. Gatti, L.A. Lugiato, preprint

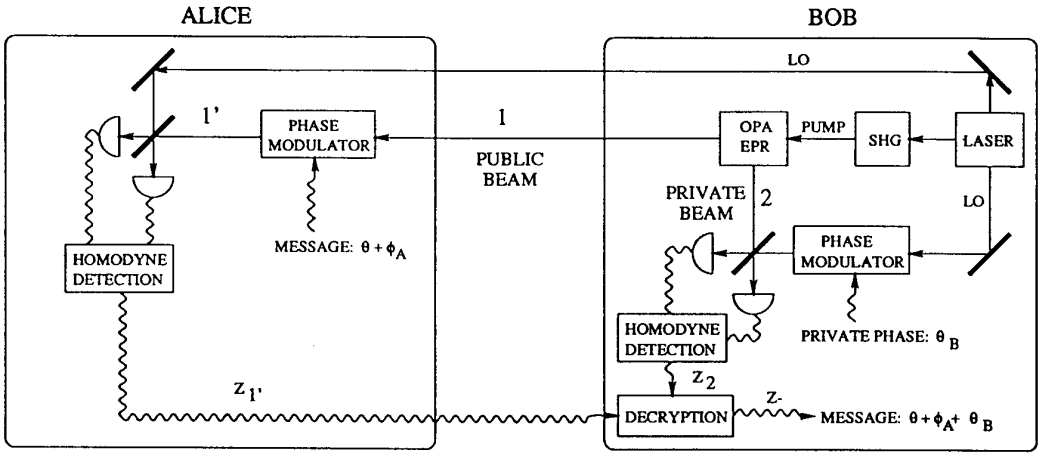


Figure 1: Schematic set-up for the "quantum public key" based cryptography with continous variables

Teleportation of Entanglement

Arkadiusz Orlowski

Instytut Fizyki PAN, Aleja Lotnikow 32/46, 02-668 Warszawa, Poland

Entanglement belongs to the fundamental resources used in quantum information processing. Once established via interaction it has to be carefully protected from environmental disturbances. In this paper a problem of faithful dissemination of entangled states is studied. Various schemes of generalized teleportation methods to teleport entangled states are discussed. The question of optimum teleportation, i.e., the minimum requirements (resources) necessary to teleport two-(and-more)-qubit entangled states, is raised and answered. A related problem of how to quantify the degree of entanglement for more than two qubits is considered. Possible applications in quantum cryptography are suggested.

Quantum Visual Cryptography?

Arkadiusz Orlowski

Instytut Fizyki PAN, Aleja Lotnikow 32/46, 02-668 Warszawa, Poland

Visual cryptography, recently devised by Naor and Shamir [1], is a novel scheme of encryption of pictures, writings, and graphics. It can also be considered as a scheme for sharing of visual secrets. After reviewing various implementations of visual (both black-and-white and color) cryptography some speculations about quantum versions of the problem are given.

[1] M. Naor and A. Shamir, "Visual Cryptography", *Advances in Cryptology – EUROCRYPT'94*, Lecture Notes in Computer Science **950** (Springer-Verlag, Berlin, 1995) pp. 1-12.

PARKER Steve

Characterisation of InGaAs/InP SAGM Avalanche Photodiodes for Quantum Cryptography Systems

Sara Pellegrini*, Phil A. Hiskett, Jason M. Smith, Paul .D.Townsend[1] and Gerald S. Buller

Department of Physics, Heriot-Watt University, Riccarton, EH14 4AS Edinburgh, U.K.

[1]*Corning Research Centre, Adastral Park, Martlesham Heath, Ipswich IP5 3RE, U.K.*

**Electronic address: s.pellegrini@hw.ac.uk*

The development of long span Quantum Key Distribution (QKD) requires systems operating in the low loss window of silica optical fibres Although Si based photon counting modules are now commercially available, single-photon detectors operating at around 1.55μm are still far from being off-the-shelf components. Currently, the most promising candidate for this role is the InGaAs/InP seperate absorption, grading and multiplication (SAGM) avalanche photodiodes (APD's) [1,2] which, although initially developed and now readily available as linear multiplication devices, can be biased above avalanche breakdown and operated in photon counting (Geiger) mode.

We report here the results of an extensive characterisation of commercially available SAGM avalanche photodiodes operated as photon counters. Since these detectors are not designed for such a regime, a full Geiger mode characterisation must be made in order to select the best device. The selection is based on some criteria which will be presented and discussed. One of the key parameters determining the suitability of the detectors for use in quantum cryptography systems is after-pulsing, consisting in the slow release of charges trapped during previous avalanches. Results will be presented describing the origin of this problem, how it affects the devices performance and how the use of different gating techniques can help overcome it (see figure overleaf). For QKD systems, a good figure of merit is the QBER (Quantum Bit Error Rate), which depends upon the optical system (e.g. interferometer visibility) as well as the detectors performance (e.g. detection efficiency, dark counts) [3]. For a quantum cryptography system to be secure, the QBER must be <15% [4] (ideally substantially less than this value to avoid significant bit loss during error correction and privacy amplification). The SPADs were assessed by gating the devices at the maximum frequency allowed by afterpulsing at the chosen operating temperature. The results obtained, taking into account the fibre loss of ~0.25dB/km at 1.55μm, showed the selected devices could potentially achieve QBERs of around 4% at transmission distances of 80km. These estimates were subsequently confirmed in tests on a prototype polarisation based QKD receiver [5].

[1] RIBORDY G., GAUTIER J.D., ZBINDEN H. and GISINN, "Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters", Applied Optics, **37** (12), Page 2272-2277, (1998)

[2] HISKETT P.A., BULLER G.S., LOUDON A.Y., SMITH J.M., GONTIJO I., WALKER A.C., TOWNSEND P.D.and ROBERTSON M.J., " Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55μm, Applied Optics, **39** (36) (Dec. 2000)

[3] TOWNSEND P.D. "Quantum Cryptography on Optical Fiber Networks", Optical Fiber Technology **4**, 345-370 (1998)

[4] LUTKENHAUS, "Security against eavesdropping in quantum cryptography", Phys. Rev. A, **54** (1), 97 (1996)

[5] HISKETT P.A., BULLER G. S. AND TOWNSEND P. D., these proceedings

RALLAN Luke

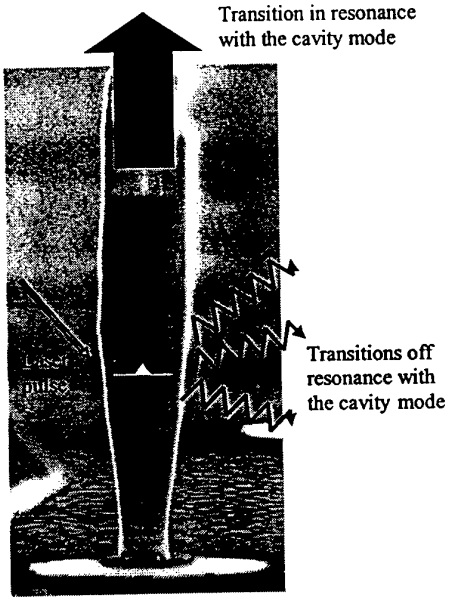
Dynamical Properties of the Emission from a Single InAs/GaAs Quantum dot in Pillar Microcavities : Towards a Single Photon Source

Emmanuel Moreau, Isabelle Robert, Bruno Gayral, Jean-Michel Gérard and Izo Abram

Laboratoire de Photonique et Nanostructures (LPN), CNRS,
196 avenue Henri Ravera, F-92225 Bagneux cedex, France
Electronic address: isabelle.robert@rd.francetelecom.fr

Over the past few years, the generation of trains of light pulses each containing one and only one photon synchronized on an external clock has attracted much interest. Indeed, the security of quantum cryptography relies on the fact that each bit of information is coded on a single photon. An efficient source of single photons is thus in demand.

Many solutions have been proposed for the engineering of such "anti-bunched" sources. The one we propose uses a single quantum dot under pulsed excitation as a source of a regulated photon stream [1]. In order to insure a good light collection efficiency, the InAs/GaAs quantum dot is placed in an elliptical cross-section pillar microcavity bounded by Bragg mirrors. The collection efficiency relies on CQED effects and in particular on the strong Purcell effect in this cavity (10-fold enhancement of the luminescence lifetime expected) and the concomitant directionality of the emission The potentiality of our system is underscored by the possibility to generate true single photon states with a high collection efficiency (up to 70 % [2]) and the possibility of light injection into a fiber (thanks to the directionality of the emission).



The measurement of the photon statistics emitted by our samples uses the standard Handburry-Brown and Twiss coincidence set-up, under non-resonant pulsed excitation at a temperature of 4K. With the use of this HBT-type correlation photon set-up, we can measure both the second-order coherence function $g^{(2)}(\tau)$ and the radiative lifetime which gives us access to the Purcell factor. Indeed, the luminescence lifetime of a quantum dot embedded in a micropillar can be measured via the same experimental set-up acting as a time-resolved photon counting set-up (the t_{start} is given by the laser pulse). The estimation of the spontaneous emission rate enhancement results from the comparison between the lifetimes measured on a dot in resonance and a dot off resonance with the cavity mode.

In this poster, we will present the first experimental observation of the Purcell effect on an isolated quantum dot and our preliminary results on the quantum correlation among photons from a single quantum dot placed in a pillar cavity.

[1] J. M. Gérard and B. Gayral, J. Lightwave Technol. **17**, 2089 (1999)
[2] J.M. Gérard *et al*, Phys. Rev. Lett. **81**, 1110 (1998)

Frequency tunable EPR-correlated optical fields.

Christian Schori, Jens Lykke Sørensen, Olivier Arcizet and Eugene Polzik
Institute of Physics and Astronomy, University of Aarhus, Denmark

A frequency tunable source of non-classical light based on a frequency non-degenerate optical parametric oscillator below threshold has been constructed. The progress in observing the Einstein-Podolsky-Rosen correlations between the signal and idler fields separated in frequency by 800 MHz is presented. Either the signal or the idler field can be tuned around Cs resonance at 852 nm making the source suitable for the future experiments with the quantum memory read-out via atom-to-light teleportation [1].

1. A. Kuzmich and E. S. Polzik, Phys. Rev. Lett. (2000) 85, 5639.

Plug&Play long distance quantum key distribution prototype

Andre Stefanov, Damien Stucki, Olivier Guinnard, Laurent Guinnard,
Grégoire Ribordy, Hugo Zbinden, Nicolas Gisin
GAP-Optique, University of Geneva
20, rue de l'école-de-médecine
CH-1211 Geneva 4, Switzerland

Abstract:

We present an user-friendly prototype realisation of the plug&play system for QKD. It is a fiber optic long distance system at 1550 nm, using Peltier-cooled InGaAs photon counters. Alice and Bob's apparatus are standalone connected to a PC via the USB port and fit in 19 inch boxes. The choice of the plug&play design permits simplicity and stability due to the self-alignement.

Highly efficient photon-pair source using a Periodically Poled Lithium Niobate waveguide

S. Tanzilli[1*], H. De Riedmatten[2], W. Tittel[2], H. Zbinden[2], P. Baldi[1], M. De Micheli[1], D.B. Ostrowsky[1], and N. Gisin[2]

(1) LPMC-CNRS UMR 6622, Université de Nice - Sophia Antipolis, Parc Valrose, 06108 Nice Cedex 2.
(2) GAP, Université de Genève, 20, rue de l'école de médecine 1211 Genève 4, Switzerland.

In the beginning of the 80's Alain Aspect [i] performed his famous tests of Bell-inequalities to verify quantum non-locality [ii], using a complicated two-photon source based on a double atomic cascade transition. Since then, more and more Bell-tests have been reported [iii], taking advantage of more efficient and handy sources exploiting spontaneous parametric down-conversion (PDC) in second order ($\chi(2)$) non-linear bulk crystals. Such sources have become an essential tool for fundamental and applied quantum optical. Although a lot of important results have been obtained, always confirming theoretical predictions, more sophisticated experiments like quantum teleportation suffer from low photon-pair production leading to low signal-to-noise ratios and long measurement times. Here, we report on a new kind of twin-photon source taking advantage of an active optical waveguide integrated on a Periodically Poled Lithium Niobate (PPLN) substrate [iv], in opposition to bulk crystals used until now. Thanks to the confinement of the pump wave over the entire length of the sample and the use of Quasi-Phase-Matching (QPM), this leads to an improvement of the pair generation efficiency by four orders of magnitude.
Measurements are made on a 3.2 cm long sample with a 12.1 μm poling period. Using a pump laser of a few μW at 657 nm, we generate degenerate photon-pairs at 1314 nm. The output of the guide is coupled to a 50/50 single mode fiber optics beam splitter used to separate the twin photons. Using LN_2 cooled Germanium-APDs and a time-to-amplitude converter (TAC), the coincidence rate (R_c) is counted. The efficiency of the source is unprecedented: we obtain an average of around 1550 coincidences/s (c/s) for a guided pump power of only 1 μW. Furthermore, taking into account the 50% loss at the directional coupler, we can estimate a pair production rate of 7.5 MHz, corresponding to a conversion efficiency of about $2*10^{-6}$ per pump photon. To our knowledge, this result is at least 4 orders of magnitude higher than any other source reported before. Note that high efficiency for twin-photon production is especially important for experiments needing more than one photon pair at a time or high signal to noise ratios.

i A. Aspect, P. Grangier, and G. Roger
"Experimental test of realistic theories via Bell's inequality"
Phys. Rev., **47**, pp. 460-465 (1981)

ii J.S. Bell
"On the Einstein-Podolsky-Rosen Paradox"
Physics (Long Island City, N.Y.), **1**, pp. 195-200 (1964)

iii W. Tittel, J. Brendel, H. Zbinden, and N. Gisin
"Violation of Bell inequalities by photons more than 10 km apart"
Phys. Rev. Lett., **81**, 17, 3563-3566 (1998)
Phys. Rev. Lett., **82**, 7, pp. 1345-1349 (1999)

iv L. Chanvillard, P. Aschieri, P. Baldi, D.B. Ostrowsky and M. De Micheli; L.Huang, and D.J. Bamford
"Soft Proton Exchange on PPLN: a simple waveguide fabrication process for highly efficient non-linear interactions"
Applied Physics Letters, **76**, 9, pp. 1089-1091 (2000)

* e-mail : tanzilli@unice.fr

Long wavelength single photon sources from InGaAs quantum dots

Spyros D. Varoutsis[(1)], Judy Rorison[(1)],
Dave Taylor[(2)], Paul Tapster[(2)] and John G. Rarity[(2)].
[(1)] Electrical and Electronic Engineering Department,
Bristol University. UK BS8 1UB
And
[(2)] DERA, Malvern Worcestershire, UK WR14 3PS
e-mail: sv7724@bris.ac.uk

This project is a preliminary investigation of the feasibility of Quantum Dot (QD) single photon sources beyond 1000nm. The system used consisted of single sheets of InGaAs quantum dots in GaAs with concentrations up to 6.10^{10} dots/cm^2. The experimental work was focused on developing the necessary detecting equipment and subsequently analysing the sample's photoluminescence spectra. In order to detect single photons at around 1200nm, which was the emission wavelength of the QD sample, we had to build a detector based on a germanium avalanche photodiode. The actual characterisation of the germanium detector was a major part of the project, since it suffered from high dark count rates and quite severe after-pulsing effects. The PL-spectra was done at 2K, while the micro-PL was done at room temperature. This led to differences between results obtained at wavelengths beyond 1050nm. In order to get the full micro PL-spectrum we used a silicon detector for measurements up to 1000nm and the germanium detector for measurements from 1000nm to around 1300nm.

Although this investigation is by no means conclusive, it has shown that isolating a single dot and resolving its emission spectra by filtering out the undesired higher order exitonic emissions might be possible at low temperatures. Another approach that might facilitate the isolation of a single dot would be to create pillars of sub-micron diameter (diameter dependent on density of dots) by etching. We show a QD sample etched into three by three array of pillars with diameters ranging from 500nm to 200nm. We expect less than four dots in the smallest diameter pillars. For future experiments a low temperature micro-PL experiment is being set up and improvements to the detection scheme are being investigated.

Optimal Inconclusive Discrimination of Two Pure States

Shashank Virmani, Massimiliano Sacchi,[1] Martin Plenio, Damian Markham

QOLS, Blackett Laboratory, Imperial College of Science Technology and Medicine
Prince Consort Road, South Kensington, London SW7 2BW, England

[1] *Dipartimento di Fisica 'A. Volta', Università di Pavia and Unità INFM, via A. Bassi 6, I27100 Pavia, Italy .*

In the field of Quantum Information, it has become important to try and determine what restrictions apply when Alice and Bob are only allowed to act locally on a shared quantum state. Of particular interest is the local distinguishability of quantum states, which is likely to have a bearing upon the distillation of entanglement and the sharing of quantum secrets. Several authors have recently begun to investigate this issue. In particular [1] have presented a basis of orthogonal product pure states that cannot be distinguished perfectly locally, and [2] present examples of orthogonal mixed states with the same property. On the more positive side, Walgate et. al. [3] have demonstrated that any two *orthogonal* multipartite pure states can be optimally distinguished using only local operations.

In this work [4] we utilise the results of [3] to show that this is true for *any* two multiparty pure states, in the sense of inconclusive discrimination . There are also certain regimes of conclusive discrimination for which the same also applies, although we can only conjecture that the result is true for all conclusive regimes.

We also discuss sets of states that can be locally optimally distinguished according to *any* figure of merit. These states have the property that local operations performed by Alice or Bob can be used to recreate the states that they share entirely on Alice's side. This means that Alice can apply any global protocol to discriminate them, and hence the optimal global procedure can be achieved locally. An interesting consequence of this is that any two maximally entangled states can optimally be distinguished locally according to *any* discrimination measure.

[1] C.H. Bennett, D.P. DiVincenzo, C.A. Fuchs, T. Mor, E. Rains, P.W. Shor, J.A. Smolin, W.K. Wootters, Phys. Rev. A. **59**, 1070 (1999).
[3] B. Terhal, D.P. DiVincenzo, D. Leung, quant-ph/0011042
[2] J. Walgate, A. Short, L. Hardy and V. Vedral, Phys. Rev. Lett.**85**, 4972 (2000)
[4] quant-ph/0102073

Antibunched photon emission from single self assembled quantum dots

Valery Zwiller*, Nikolay Panev, Soren Jeppesen, Mats-Erik Pistol, Lars Samuelson

Department of Solid State Physics, Lund University, Box 118, SE-221 00 Lund, Sweden

Hans Blom, Per Jonsson, Gunnar Björk

Department of Electronics, Royal Institute of Technology, SE-16440 Kista, Sweden

* *Electronic address: Valery.Zwiller@ftf.lth.se*

We report on antibunching measurements performed on a single self assembled quantum dot[1]. The quantum dots were obtained by epitaxial deposition (Chemical Beam Epitaxy) of 1.6 monolayers of InAs on GaAs. The low density of quantum dots with an average spacing of several micrometers enabled single dot investigations using a confocal microscope assisted by a solid immersion lens to increase light collection from the high refractive index sample. A Hanbury-Brown-Twiss interferometer was used to measure the correlation function using two sensitive avalanche photodiodes and a correlation card with a time resolution of around 0.5 ns.

The correlation function was measured under both continuous and pulsed excitation. In both cases, the excitation intensity was adjusted so that only a single sharp line due to the exciton recombination was observed. Under continuous excitation, a dip was observed in the correlation function. The pulsed excitation experiment was performed using a Ti:Sapphire laser emitting 150 fs pulses at 80 MHz, the correlation function shows a weaker peak for t=0 implying that single quantum dots could be used as triggered single photon sources.

The possibility of generating and detecting entangled photon pairs emitted by a single quantum dot will be discussed as well as different schemes to increase light collection efficiency from single quantum dots using microcavities of various designs.

[1] V. Zwiller, H. Blom, N. Panev, P. Jonsson, S. Jeppesen, T. Tsegaye, E. Goobar, M.-E. Pistol, L. Samuelson, G. Björk, submitted to APL

QUICK: List of Attendees

ABRAM Izo, Dr.
Lab de Photonique et nanostructures LPN/CNRS
BP29, 196 Avenue Henri Ravera
92222 Bagneuex Cedex, France
Tel +33 1 42 31 73 32
Fax: +33 2 42 53 49 30
email: izo.abram@rd.francetelecom.fr

ANGELAKIS, Dimitris
Laser Optics and Spectroscopy,
Physics Department,
Imperial College,
Prince Consort Road,
London, SW7 2BZ, UK
Phone: +44 (0)171 594 7728
FAX: +44 (0)171 823 8376
E-mail: d.angelakis@ic.ac.uk

ASCHAUER Hans, Ph.D. student
Theoretische Physik
Ludwig-Maximilians-Universität
Theresienstraße 37
D-80333 München
Phone: ++49 89 2394 4172
Fax: ++49 89 280 5248
email: Hans.Aschauer@Physik.uni-muenchen.de

ATATURE Mete
BOSTON UNIVERSITY
PHYSICS DEPARTMENT
590 Commonwealth Avenue Room 255
Boston, MA 02215
USA
Tel:+1 (617)-353-9956
Fax: (617) 353-9393
email: ataure@buphy.bu.edu

BARNES, Bill, Dr. Reader in Photonics
University of Exeter,
Stocker Road, Devon,
Exeter, EX4 4QL, UK
tel +44 1392 264135
fax +44 1302 264111
Email: W.L.Barnes@exeter.ac.uk

BENCHEIKH Kamel, Dr.
Laboratoire de Photonique et de Nanostructures CNRS
(UPR20)
196, Ave. Henri Ravera, BP29
92222 Bagneux, France
Tel: +33 (0) 1 42317414, +33 (0) 1 42317227
Fax: +33 (0) 42534930
email: kamel.bencheikh@rd.francetelecom.fr

BERGER Vincent, Dr
THALES Laboratoire Central de Recherches
Domaine de Corbeville
914000 Orsay, France
Tel: +33 1 69 33 90 84,
Fax: +33 1 69 33 07 40
email: vincent.berger@lcr.thomson-csf.com

BETHUNE, Donald, Dr
IBM Almaden Research Center
650 Harry Rd K13/D1
San José, CA 95120-6099, USA
Tel: +1 408 927 2480
Fax: +1 408 927 2100
email: bethune@almaden.ibm.com

BEVERATOS Alex - Optique Quantique
Institut d'Optique Théorique et Appliquée
Batiment 503 - BP 147, 91403 Orsay CEDEX, France
Tel : +33 (0) 1 69 35 88 67, + 33 (0) 1 69 35 87
Fax : +33 (0) 1 69 35 87 00
Email: alexios.beveratos@iota.u-psud.fr

BOUCHER, William, Dr.
THALES Laboratoire Central de Recherches
Domaine de Corbeville
914000 Orsay, France
Fax: +33 1 69 33 07 40
email: Boucher@lcr.thomson-csf.com

BONFRATE, Gabrielle, Dr.
Corning Research Centre
B55 Adastral Park
Martlesham Heath
Ipswich, Suffolk , IP5 3RE
UK
Tel: +44 (0)1473 663228
Tel: +44 (0)1473 663295
email: BonfrateG@corning.com

BOURENANNE Mohamed, Ph.D.Student
Department of Microelectronics and Information
Technology, Electrum 229, SE-164 40 Kista, Sweden
Tel: +46 8 752 1117,
Fax: +46 8 752 1240
email : boure@ele.kth.se

QUICK: List of Attendees

BOUWMEESTER, Dik, Dr.
Clarendon Laboratory
Parks Road
Oxford OX1 3PU
United Kingdom
Office +44 (0) 1865 282205
Lab. (room 201): +44 (0) 1865 272357
Lab. (room 221): +44 (0) 1865 272329
Email: dik.bouwmeester@qubit.org

BRUNE, Michel, Professor
Laboratoire Kastler Brossel
Departement de Physique de l*E.N.S.
24, rue Lhomond, 75231 Paris Cedex 05, France
Tel: +33 1 44 32 33 65,
Fax: +33 1 44 32 34 34
email: brune@lkb.ans.fr

BULLER Gerald, Prof.
Department of Physics
Heriot-Watt University, Riccarton
Edinburgh EH14 4AS, United Kingdom
Tel +44 (0)131 451 3069
Fax: +44 (0)131 451 8063
email: PHYGSB@phyfsa.phy.hw.ac.uk

CERF, Nicholas, Prof.
Ecole Polytechnique, ULB
Service d'Electronique, Microélectronique et
Télécommunications, Faculté des Sciences Appliquées
Université Libre de Bruxelles
50 avenue F. D. Roosevelt - CP 165/56
B-1050 Bruxelles - Belgique
Tel: +32-2-650-2858,
Fax: +32-2-647-7108
Email: ncerf@ulb.ac.be

CHENEVAS-PAULE Andre
CEA-LETI DOPT/SCOPI
CEA-G 17 Rue des Martyrs
38054 Grenoble Cedex
tel: (33)476884044
fax: (33)476885157
email: achenevaspaule@cea.fr

CODREAU Thomas, Prof.
Laboratoire Kastler Brossel
Université Pierre et Marie Curie
Case 74, Tour 12, 4, Place Jussieu
F-75252 Paris CEDEX 05
France
Tel :33 1 44 27 43 94
Fax :33 1 44 27 38 45
Email: coudreau@spectro.jussieu.fr

COTEAU Christophe, Ph.D. student
Centre for Quantum Computation
Clarendon Laboratory
Parks Road
Oxford, OX1 3PU
United Kingdom
phone: +44-1865-272*** (work)
fax: +44-1865-272387 (work)
email: christophe.couteau@qubit.org

CURTIS Jonathan
Quantum Confidential Inc.
817 Chehalem Road
LaCanada, CA. 91011
USA
Fax:+1 818790 2035
email: jcurtis@quantum-confidential.co.uk

CURTY Alonso Marcos, Ph.D.Student
E.T.S.I. Telecomunicación. Campus Universitario s/n.
36200 Vigo (España)
Tel: +34 - 986 812 664
Fax: +34 - 986 812 116
email: mcurty@com.uvigo.es

DEBUISSCHERT Thierry , Dr.
THALES, Laboratoire Central de Recherches
Domaine de Corbeville
91404 Orsay Cedex, France
Tel: +33 1 69 33 91 85,
Fax: +33 1 69 33 91 27
email: thierry.debuisschert@thalesgroup.com

DUMAIS Paul, Dr.
Laboratoire d'informatique théorique et quantique
Département d'informatique et de recherche
opérationnelle
Université de Montréal
C.P. 6128 succursale Centre-ville
Montréal (Québec) H3C 3J7 Canada
Tel: (514)398-7071, poste 0345 (ou 0699)
Fax: (514) 343-5834
email: dumais@iro.umontreal.ca

DURKIN Gabriel, Ph.D. student
Centre for Quantum Computation, Room 311
The Clarendon Laboratory
Parks Road
Oxford OX1 3PU, United Kingdom
Tel: +44 7790 585171
email: g.durkin1@physics.oxford.ac.uk,
gabriel.durking@qubit.org

QUICK: List of Attendees

EDWARDS Paul, Professor
School of Electronics and Telecommunications Engineering
Centre for Advanced Telecommunications and Quantum Electronics Research
University of Canberra ACT 2601, Australia
Tel +61 26 201 2515/2516/2411
Fax: +61 26 201 5041
email: paule@ise.canberra.edu.au

GAYRAL, Bruno, Dr.
ECE Department
University of California
Santa Barbara, CA, 93106-9560, USA
Tel : +1(805) 893 8664
Fax : +(805) 893 3262
email : bruno@xanadu.ece.ucsb.edu

GIACOBINO, Elisabeth, Prof. E.
Laboratoire Kastler Brossel
Université Pierre et Marie Curie
Case 74, Tour 12, 4, Place Jussieu
F-75252 Paris CEDEX 05
France
Tel :33 1 44 27 43 94
Fax :33 1 44 27 38 45
Email: elg@spectro.jussieu.fr

GISIN, Nicolas, Prof.
Université de Genève
GAP-Optique
Rue de l'École-de-Médecine 20, CH-1211
Genève 4, Suisse / Switzerland
Tel: +41 22 702 65 95 (GAP secratary's office)
Fax: +41 22 781 09 80
Email: *Nicolas.Gisin@physics.unige.ch*

GORMAN Phil, Dr.
Lasers and Photonics
DERA
Andrews Rd
Malvern, Worcs UK WR14 3PS
Fax 44-1684-896270
Email: gorman@dera.gov.uk

GROSSHANS Frederic, Ph.D.Student
Institut d'Optique
B.P. 147 - F91403 Orsay cedex - France
email: frederic.grosshans@iota.u-psud.fr

EIBL Mandred, Ph.D.Student
Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Straße 1
D-85748 Garching
phone: +49-(0)89-32905-732
fax: +49-(0)89-32905-200
email: m.eibl@mpq.mpg.de

GERARD Jean-Michel, Dr
Lab de Photonique et nanostructures LPN/CNRS
BP29, 196 Avenue Henri Ravera
92222 Bagneuex Cedex, France
Fax: +33 2 42 53 49 30
email: jeanmichel.gerard@rd.francetelecom.fr

GILBERT Gerald, Dr
Quantum Information Science Group
The MITRE Corporation
Tel: +1 732 935 5595
Fax: +1 732 389 6761
email: ggilbert@mitre.org

GOEDGEBUER, Jean-Pierre, Professor
Laboratorie d*optique, UMR CNRS 6603
Universite de Franche-Comte
25030 BESANCON Cedex, France
Tel: +33 (3) 3 81 66 64 23
Fax: +33 (0) 3 81 66 64 00
email: jean-pierre.goedgebuer@univ-fcomte.fr

GRANGIER Philippe, Prof.
Institut d'Optique
B.P. 147 - F91403 Orsay cedex - France
Tel : +33 (0)1 69 35 87 66 ou/or (33) (0)1 69 35 87 32
Fax : +33 (0)1 69 35 87 00 ou/or (33) (0)1 69 35 88 07
email: philippe.grangier@iota.u-psud.fr

GRUSKA, Jozef, Prof.
Faculty of Informatics
Department Department of Computer Science
Office Number B401 (Botanick 68a, 602 00 Brno)
Chech Republic
Phone +420-5-4151 2358
Fax: +420-5-41 212 568
Email: gruska@qci.jst.go.jp,
gruska@informatics.muni.cz

QUICK: List of Attendees

HENNRICH Marcus
Max-Planck-Institut für Quantenoptik
Abteilung für Quantendynamik
Hans-Kopfermann-Straße 1
D-85748 Garching
Germany
Tel ++49 - 89 - 32905 145
Fax ++49 - 89 - 32905 395
e-Mail M.Hennrich@mpq.mpg.de

HISKETT, Phil, Dr.
Department of Physics
Herio-Watt University, Riccarton
Edinburgh EH14 4AS, United Kingdom
Fax: +44 (0)131 451 8063
Email: p.a.hiskett@hw.ac.uk

HOWELL, Jonathan, Ph.D. student
Centre for Quantum Computation
Clarendon Laboratory
Parks Road
Oxford, OX1 3PU
United Kingdom
Email: j.howell@qubit.org

HUGHES Richard, Dr
Physics Division, P-23, MS H803
Los Alamos National Laboratory
Los Alamos, NM 87545, USA
Tel: +1 505 667 3876,
Fax: +1 505 665 4121
email: hughes@lanl.gov

HUNTER Kieran, Ph.D.Student
Department of Physics and Applied Physics
University of Strathclyde
John Anderson Building
107 Rottenrow, Glasgow G4 0NG.
UK
Tel: 0141 548 3174
FAX: 0141 552 2891
E-mail: kieran@phys.strath.ac.uk

IBLISDIR Sofyan, Ph.D.Student
Ecole Polytechnique, CP 165/56
Université Libre de Bruxelles
50 avenue F.D. Roosevelt
B-1050 Bruxelles, Belgium
Tel: +32 2 650 2875,
Fax: +32 2 650 2941
email: siblisdi@ulb.ac.be

IMOTO, Nobuyuki, Prof.
School of Advanced Science, SOKEN
Shonan Village, Hayama, Kanagawa 240-0193, Japan
Tel: 0468-58-1557,
Fax: 0468-58-1542
E-mail: imoto@soken.ac.jp

JENNEWEIN Thomas, Ph.D Student
Institute for Experimental Physics
University of Vienna
Boltzmanngasse 5
A-1090 Vienna
Tel: +43/1/4277-51211
Fax: +43/1/4277-9512
Email: thomas.jennewein@univie.ac.at

JONSSON Per, Ph.D.Student
Department of Microelectronics and Information Technology, Electrum 229, SE-164 40 Kista, Sweden
Tel: +46 8 752 1206,
Fax: +46 8 752 1240
email : perj@ele.kth.se

JOSSE Vincent, Ph.D.Student
Laboratoire Kastler-Brossel, Université P. et M. Curie, case 74, F-75252,
Paris Cedex 05, France-
Tel: 00 33 1 44 27 43 93
Fax: 00 33 1 44 27 38 45
email: josse@spectro.jussieu.fr

KARLSSON Anders, Associate Professor
Department of Microelectronics and Information Technology, Electrum 229, SE-164 40 Kista, Sweden
Tel :+46-8-7521272,
FAX :+46-8-7521240
email: andkar@ele.kth.se

KASHEFI Elham, Ph.D. student
Centre for Quantum Computation, Room 311
The Clarendon Laboratory
Parks Road
Oxford OX1 3PU, United Kingdom
Email: e.kashefi@qubit.org

QUICK: List of Attendees

KENT, Adrian, Dr.
Quantum Information Processing Group, HP Labs
Filton Road, Stoke Gifford, Bristol BS34 8QZ, U.K.
tel +44 (0)117 3129051
fax +44 (0)117 3129870
email Adrian_Kent@hp.com

KNIGHT, Paul, Dr.
Lasers and Photonics
DERA
Andrews Rd
Malvern, Worcs UK WR14 3PS
Fax 44-1684-896270
email: prknight@scs.dera.gov.uk

KOROLKOVA Natalia, Dr
Quantum Information Group, Lehrstuhl für Optik
Universität Erlangen-Nürnberg
Staudstrasse 7/B2, 91058 Erlangen, Germany
Tel: +49 9131 8528954
Fax: +49 9131 13508
email: korolkova@kerr.physik.uni-erlangen.de

KURTSIEFER Christian, Dr
Sektion Physik der LMU Muenchen
Schellingstr 4/III, 80799 Muenchen, Germany
Tel: +49 89 2180 3942
Fax: +49 89 2180 5032
email: Christian.Kurssiefer@physik.uni-muenchen.de

LAMAS-LINARES Antia, Ph.D. student
Center for Quantum Computation
University of Oxford
Tel: +44 01865 282203
Fax: +44 01865 272400
email: a.lamas@qubit.org

LEDOUX-RAK, Isabelle, Prof.
Laboratoire de Photonique Quantique et Moléculaire
Ecole Normale Supérieure de Cachan, pièce 109bis
61 avenue du Président Wilson
94235 Cachan, Cedex
FRANCE
Tel 01 47 40 55 60
Fax 01 47 40 55 67
e-mail isabelle.ledoux@lpqm.ens-cachan.fr

LEUCHS, Gerd, Prof.
Lehrstuhl für Optik, Physikalisches Institut V
Universität Erlangen
Staudtstr. 7 / B2
D-91058 Erlangen
Tel.: 09131 / 85 2 8371
Fax: 09131 / 13508
email: leuchs@physik.uni-erlangen.de

LJUNGGREN Daniel, Ph:D.Student
Department of Microelectronics and Information
Technology, Electrum 229, SE-164 40 Kista, Sweden
Tel: +46 8 752 1400,
Fax: +46 8 752 1240
email : daniellj@ele.kth.se

LONGCHAMBON Laurent, PhD student
Laboratoire Kastler Brossel
Université Pierre et Marie Curie
Case 74, Tour 12, 4, Place Jussieu
F-75252 Paris CEDEX 05
France
Tel :+33 1 44 27 43 94
Fax :+33 1 44 27 38 45
Email: longcham@spectro.jussieu.fr

LORENZ Stefan, Ph.D. student
Lehrstuhl für Optik, Physikalisches Institut V
Staudtstr. 7 / B2
D-91058 Erlangen
Tel.: 09131 / 85 2 8955
Fax: 09131 / 13508
email: stefan.lorenz@physik.uni-erlangen.de

LUTKENHAUS, Norbert, Dr.
MagiQ Technologies
275 Seventh Avenue, 26th Fl.
New York, NY 10001-6708
Email: norbert@magiqtech.com

LVOVSKY Alexander, Dr.
Fakultät für Physik M696, Universität Konstanz
D-78464 Konstanz, Germany
Tel: +49 7531-883827 (office), -883834 (lab)
Fax: +49 7531 883072
email: Alex.Lvovsky@uni-konstanz.de

QUICK: List of Attendees

MAGNIEZ Frederic, Dr.
CNRS-LRI, Bâtiment 490
Université Paris-Sud
F-91405 Orsay cedex Orsay,
France
Tel: +33 1 69 15 70 82
Fax: +33 1 69 15 65 86
email: magniez@lri.fr

MAKAROV Vadim, Ph.D.Student
Norges teknisk-naturvitenskapelige universitet
O.S. Bragstads Plass 2A
7034 TRONDHEIM
Telefon: 73 59 44 00
Fax: 73 59 14 41
email: makarov@fysel.ntnu.no

MASSEY Paul Stephen, Dr.
CESG
Room 2/0609, CESG, P.O. Box 144, Cheltenham,
GL52 5UE, United Kingdom.
Tel : 01242 221 491 xt4686
email: paul.masey@cesg.gsi.gov.uk

MAYERS, Dominic Professor/ Consultant Maharishi
University of Management/ NEC
Computer Science/Physical Division
Maharishi University of Management Computer
SCience Department Fairfield, IA 52556
Phone:(641) 470-1356 (641) 470-1994
Fax:(641) 472-1103
E-mail:mayers@reserach.nj.nec.com

MEROLLA, Jean-Marc, Dr.
Laboratorie d*optique, UMR CNRS 6603
Universite de Franche-Comte
25030 BESANCON Cedex, France
Tel: +33 (3) 3 81 66 64 23
Fax: +33 (0) 3 81 66 64 00
email: merolla@univ-fcomte.fr

MINOT, Christophe
Laboratoire LPN-CNRS
196, avenue Henri Ravera, BP 29
92222 Bagneux Cedex, France
Tel : +33 (0)1 42 31 73 20
Fax : +33 (0) 1 42 53 49 30
email : christophe.minot@francetelecom.fr

MOURA ALVES Carolina, Ph.D.Student
Centro de Fisica de Plasmas, Instituto Superior Tecnico
P-1096 Lisboa Codex
Portugal
email: heisenberg@clix.pt

MÜLLER-QUADE, Jörn, Dr.
Universität Karlsruhe
Institut für Algorithmen und Kognitive Systeme
Am Fasanengarten 5
D-76128 Karlsruhe
phone: +49 721 608 6309
fax: +49 721 696893
email: muellerq@ira.uka.de

NAVEZ Patrick
Istituto Nazionale per la Fisica della Materia (INFM)
Dip di Scienze Chimiche, Fisiche & Matematiche
Universita degli Studi dell'Insubria
via Valleggio, 11, I-22100 COMO, ITALY
Tel:+ 39/031-238-6222
Fax:+ 39/031-238-6119
Email : navez@mi.infn.it

NEMOTO Kae, Dr.
School of Informatics, Bangor University, LL57 1UT,
United Kingdom.
tel: (+44) (0) 1248 38-2808
fax: (+44) (0) 1248 36-1429
email: nemoto@sees.bangor.ac.uk

ORLOWSKI Arkadius, Assoc. Prof.
PolishAcademy of Sciences
Institute of Physics
Aleja Lotnikow 32/46
02-668 Warszawa
Poland
Tel: 48 22 843-70-01 ext. 3224
Fax:+ 48 22 843-09-26
Email: orlow@ifpan.edu.pl

OSTROWSKY Dan, Professor
UNSA/LPMC/CNRS
Parc Valrose
06108 Nice Cedex 2, France
Tel +33 492 07 67 53,
Fax: +33 492 07 67 54
email: Dan.Ostrowsky@unice.fr

QUICK: List of Attendees

PARKER Steve, Ph.D. student
Quantum Optics and Laser Science
Blackett Laboratory
Imperial College
Prince Consort Road
London SW7 2BZ
UK
Phone; +44 20 759 47642
Fax: + 44 20 7594 7714
Email: s.parker@ic.ac.uk

PELLEGRINI Sara, Dr.
Department of Physics, Heriot-Watt University,
Edinburgh EH14 4AS, UK
Telephone: +44 (0)131 451 8085
Fax: +44 (0)131 451 8083
E-mail: S.Pellegrini@hw.ac.uk

PELTON, Matthew, Dr.
Department of Applied Physics
Stanford University
316 via Pueblo Mall
Stanford, CA 94305-4090
U.S.A.
Tel: (650) 725-7698
Fax: (650) 723-5320
E-mail: pelton@stanford.edu

POLZIK Eugene, Professor
Institute of Physics and Astronomy
Aarhus University, 8000 Aarhus, Denmark
Tel: +45 89423745
Fax: +45 86120740
email: polzik@ifa.au.dk

RALLAN Luke, Ph.D. student
Centre for Quantum Computation
Clarendon Laboratory
Parks Road
Oxford OX1 3PU
United Kingdom
email: luke.rallan@physics.oxford.ac.uk

RARITY, John G., Prof
Lasers and Photonics
DERA
Andrews Rd
Malvern, Worcs UK WR14 3PS
Tel 44-1684-895031 St Fax 44-1684-896270
Email: rarity@dera.gov.uk

REMPE Gerhard., Prof
Max-Planck-Institut für Quantenoptik
Hans-Kopferman-Strasse 1
D-5748 Garching, Germany
Tel: +49 89 32905 711, Fax: +49 89 32905 311
email: gerhard.rempe@mpq.mpg.de

RIBOULET-DEYRIS Emmanuel, Dr.
Laboratorie de Mathématiques Emlie Picard
CNRS-UMR 5580
Université Paul Sabatier UFR MIG
118 route de Narbonne,
31062 Toulouse Cedex 04
Tel: +33 (0)1 69 35 87 86
Fax: +33 (0) 1 69 35 8700
email: riboulet@picard.ups-tlse.fr

ROBERT Isabelle, Dr.
Lab de Photonique et nanostructures LPN/CNRS
BP29, 196 Avenue Henri Ravera
92222 Bagneuex Cedex, France
Tel +33 1 42 31 73 32
Fax: +33 2 42 53 49 30
Email: isabelle.robert@rd.francetelecom.fr

SCHORI Christian, Ph.D.Student
University of Aarhus
Institute of Physics and Astronomy
Ny Munkegade, Bygning 520
DK-8000, Aarhus C., Denmark
Tel +45 89 42 37 37
Fax: +45 86 12 07 40
email: Schori@ifa.au.dk

SERGIENKO, Alexander, Professor
Dep of Electrical & Computer Engineering and Dep of Physics, Boston University
8 Saint Mary's Street
BOSTON MA 02215-2421, USA
Tel: Office +1 617 353 6564, Lab +1 617 353 9943
email: AlexSerg@bu.edu

SHAPIRO, Jeffrey H., Prof.
Room 35-213
77 Massachusetts Avenue
Massachusetts Institute of Technology
Cambridge, MA 02139-4307
Tel: +1 (617) 253-4179
email: JHS@MIT.EDU

QUICK: List of Attendees

SIMON Christoph, Dr
Centre for Quantum Computation
Clarendon Laboratory
Parks Road
Oxford OX1 3PU
United Kingdom
e-mail: Christoph.Simon@qubit.org

STEFANOV Andre, Ph.D.Student
Group of Applied Physics
Université de Genève
20, rue de l'Ecole de Medecine
CH-1211 Genève 4, Suisse
Tel: +41 22 702 6883,
Fax: +41 22 781 0980
email: Andre.Stefanov@physics.unige.ch

STUCKI Damien, Student
University of Geneva
Group of applied physics
37 chemin des Ambys, 1247 Anières, Switzerland
Tel +41 22 702.68.83
Fax +41 22 781.09.80
email : stucki6@etu.unige.ch

TANZILLI Sebastien
UNSA/LPMC/CNRS
Parc Valrose
06108 Nice Cedex 2, France
Tel +33 492 07 67 53,
Fax: +33 492 07 67 54
Email: tanzilli@unice.fr

TITTEL, Wolfgang, Dr.
Group of Applied Physics
Université de Genève
20, rue de l'Ecole de Medecine
CH-1211 Genève 4, Suisse
Phone: +41 22 702 69 29
Fax: +41 22 781 0980
email: *Wolfgang.Tittel@physics.unige.ch*

TRIFONOV Alexei, Dr
Ioffe Institute
26 Polytekhnicheskaja,
194021 St. Petersburg,
RUSSIA
Fax: +1-617-3549844.
email: a.trifonov@worldnet.att.net

TUALLE-BROURI Rosa, Dr.
Institut d'Optique
B.P. 147 - F91403 Orsay cedex – France
Tel: +33169358813
Fax: +33169358800
email: rosa.tualle-brouri@iota.u-psud.fr

VAROUTSIS, Spyros, Ph.D. student
UNIVERSITY OF BRISTOL
ELECTRICAL&ELECTRONIC ENGINEERING
68 ST PAUL'S ROAD,
CLIFTON,
BS8 1LP
UK
Email: sv7724@bris.ac.uk

VEDRAL, Vlatko, Dr.
Quantum Optics and Laser Science
Blackett Laboratory
Imperial College
Prince Consort Road
London
SW7 2BZ
Phone; +44 20 7594 7724
Fax: + 44 20 7594 7714
email: v.vedral@ic.ac.uk

VIRMANI, Shashank, Ph.D. student
Quantum Optics and Laser Science
Blackett Laboratory
Imperial College
Prince Consort Road
London
SW7 2BZ
Phone; +44 20 759 47642
Fax: + 44 20 7594 7714
email: s.virmani@ic.ac.uk

WILLIAMS, Colin P Associate Prof.
Principal Scientist (Jet Propulsion Laboratory) / Acting Associate Professor (Stanford) Computer Science Department Gates Building, Room 201 Stanford University Stanford, CA 94305-2140
Tel: (650) 723 8784
Fax: (650) 725 7411
Email: cpw@cs.stanford.edu, Colin.P.Williams@jpl.nasa.gov

WONG Franco, Dr.
MIT, Rm 36-473
Cambridge MA 02139, USA
Tel: +1 627 253 8131, Fax: +1 617 258 7864
email: franco@ncw2.mit.edu

QUICK: List of Attendees

YUEN Horace, Professor
Electrical and Computer Engineering
Northwestern University
Evanston, IL 60208-3118
Phone: (847) 491-7335
Fax: (847) 491-4455
email: yuen@ece.nwu.edu

ZBINDEN, Hugo, Dr.
Université de Genève
GAP-Optique
Rue de l'École-de-Médecine 20, CH-1211 Genève 4
Suisse / Switzerland
Phone: +41 22 702 68 83
Fax: +41 22 781 09 80
email: Hugo.Zbinden@physics.unige.ch

ZARDA, Patrick, P
Max-Planck-Institut für Quantenoptik
Hans-Kopfermann-Straße 1
D-85748 Garching
phone: +49-(0)89-32905-732
fax: +49-(0)89-32905-200
email: patrick.zarda@physik.uni-muenchen.de

ZWILLER Valery, Ph.D.Student
Solid State Physics
Lund University
Box 118, SE-22100 Lund
Sweden
Fixed phone: +46 (0)46 222 03 37
Mobile phone: +46 (0)7 3687 8377
Fax: +46 (0)46 222 36 37
email: Valery.Zwiller@ftf.lth.se