Scientific Report

Object : **Continuous Variables Quantum Information Processing workshop**
Aix en provence (France)
11th to 14th of April 2003
web : www.iota.u-psud.fr/~grangier/VariablesContinues/IntroCVQIP.html

QUIPROCONE funding application n° 0038

I. Scientific content of the event

This workshop has been focused on the use of continuous-spectrum quantum variables in quantum informational processes, a topic which has attracted a lot of attention over the last three years. The workshop managed to gather a quite large part of the scientists who have been involved in these recent developments at the European scale. Both the theoretical and experimental aspects have been discussed.

Quantum information theory has developed dramatically over the past few years, driven by the prospects of quantum-enhanced communication and computation systems. It exploits the intrinsic parallelism and large space capacity of quantum mechanics to perform tasks unrealisable with classical physics. Among the most striking successes, one finds for example the discovery of quantum factoring, quantum key distribution, or quantum teleportation. Most of these concepts were initially developed for discrete quantum variables. Recently, however, a lot of attention has been devoted to investigating the use of continuous variables in quantum informational or computational processes.

Continuous-spectrum quantum variables, for example the quadrature components of light modes, may be easier to manipulate than quantum bits. It is actually sufficient to process squeezed states of light into linear optics circuits in order to perform various quantum information processes over continuous variables. Variables with a continuous spectrum have been shown to be useful to carry out quantum teleportation, quantum error correction, or even quantum computation. The concepts of quantum cloning or entanglement purification have also been extended to continuous variables, and several quantum key distribution schemes relying on continuous key carriers have been proposed, which may be interesting in some applications. Another significant advantage of this new paradigm is the fact that, unlike discrete atomic spins, distant atomic continuous-variable systems can be entangled and that light-atoms quantum state exchange can be performed at the level of continuous variables.

II. Final Programme

The programme below is just intended to help readers fix ideas on the general timing and organization of the meeting. It only shows the speaker name together with the title of his presentation.

A full version of the final programme, including full-length abstracts of talks and poster presentations can be found in Appendix A at the end of this document.

Friday, April 11th
15:00 Conference opening
16:00 **Nicolas Treps** Quantum information processing in optical images
16:40 **Jens Eisert** Feasible distillation of continuous-variable entanglement
17:20 Organizationnal details
Free dinner

Saturday, April 12th
9:00 **Ignacio Cirac** Gaussian entanglement measures
9:40 **Geza Giedke** Entanglement of Formation for Gaussian States
10:20 Poster session
12:20 Lunch
14:00 **Philippe Grangier** Quantum cryptogaphy with coherent states
14:40 **Nicolas Gisin** The role of photon-numbers in coherent pulse quantum cryptography
15:20 Coffee break & posters
16:00 **Norbert Luetkenhaus** Quantum Key Distribution with Strong Reference Pulses
16:40 **Gerd Leuchs** Advances in quantum communication with intense light pulses
17:20 End
Free dinner

Sunday, April 13th
9:00 **Klaus Molmer** Discrete and continuous variable approaches to measurement induced entanglement.
9:40 **Eugene Polzik** Light-atoms quantum interface with continuous variables
10:20 Coffee break & posters
11:00 **Nicolas Cerf** Optimal quantum non gaussian cloning of a coherent state
11:40 **Natalja Korolkova** Quantum communication with classical and non-classical polarization states
12:20 Lunch
14:00 **Konrad Banaszek** Engineering correlated photons for quantum information processing applications
14:40 **Jaromir Fiurasek** Conditional generation of entangled states of light violating the Bell inequalities based on homodyne detection
15:20 Coffee break & posters
16:00 End
19:30 Conference dinner

Monday, April 14th
9:00 **Peter Van Loock** Projective measurements using linear optics - discrete versus continuous variables
9:40 **Matteo Paris** Two and three mode CV entanglement in optical and BEC systems
10:20 Coffee break & posters
11:00 **Vincent Josse** Polarization squeezing and quadrature entanglement using cold atoms
11:40 Lunch buffet

III. Assessment of the results, contribution to future direction

Quantum cryptography

The use of specific quantum states (as for instance squeezed or entangled states) has somehow been let apart, focussing most of the discussions on the use of coherent pulses (quasi-classical Glauber states). These coherent states are easier to manipulate experimentally. The study of coherent states protocols opens up new breakthroughs : links between security and entanglement, unconditional proofs of security, new eavesdropping strategies…

Optimal quantum non gaussian cloning

Non-gaussian quantum cloning machines specifically dedicated to coherent states duplication have been investigated, deriving an upper bound on the fidelity of this class of quantum cloning machines. Proposals for experimental set ups have been discussed.

Specific quantum states generation – applications to quantum communication

Different theoretical proposals together with experimental realisations have been discussed. A lot of attention has been devoted to generation of arbitrary multimode entangled states of light having a finite decomposition in Fock basis. Such states have been shown to present much interest for quantum communication purposes (use of entanglement, violation of Bell inequalities). Reported experimental realisations were focused on the generation of squeezed and entangled beams from several physical processes (OPO, optical fibre, cold atoms). Pros and cons together with limitations of such experiments have been discussed.

Entanglement measures

Several quantum entanglement measures have been investigated, together with their experimental implementation. In particular, the “entanglement of formation” has been newly introduced for gaussian states.

Entanglement distillation

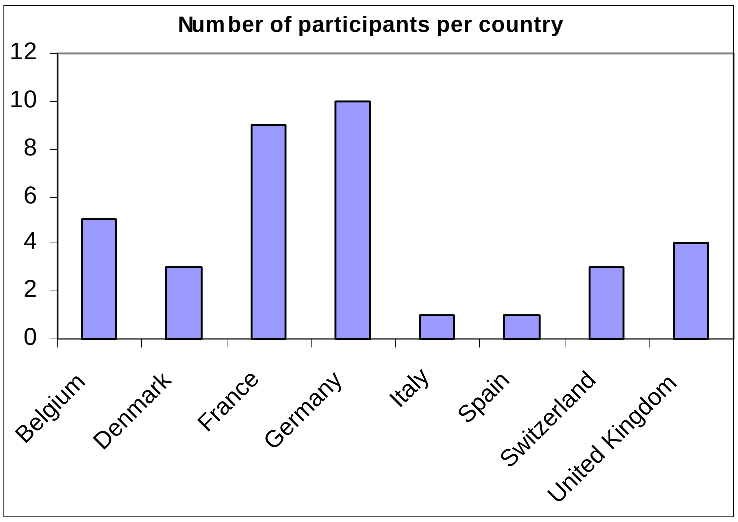
Several procedures using linear optical elements and photodetectors have been discussed to extract maximally entangled states from an ensemble of weakly entangled states. This method may also provide a new process for quantum cryptography.

Quantum memories and light-atoms interactions : towards quantum computation

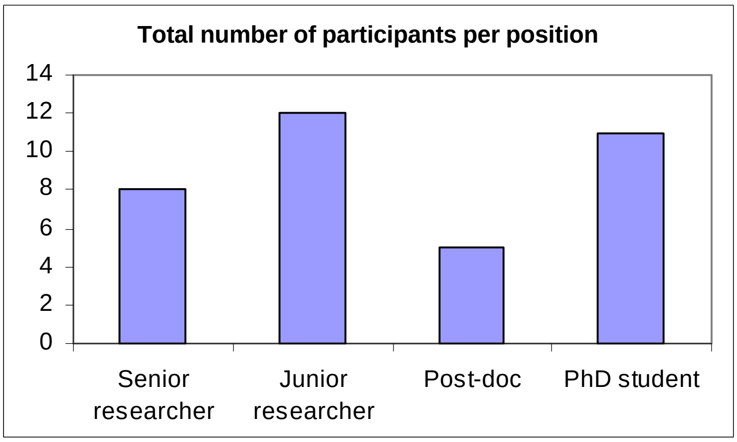
The progress in light-atoms quantum interface experiments using cold atoms and room temperature gazes have been presented. Quantum continuous variables offer major advantages in quantum computation, as for instance entanglement at distance between light and atomic ensembles appears realizable.

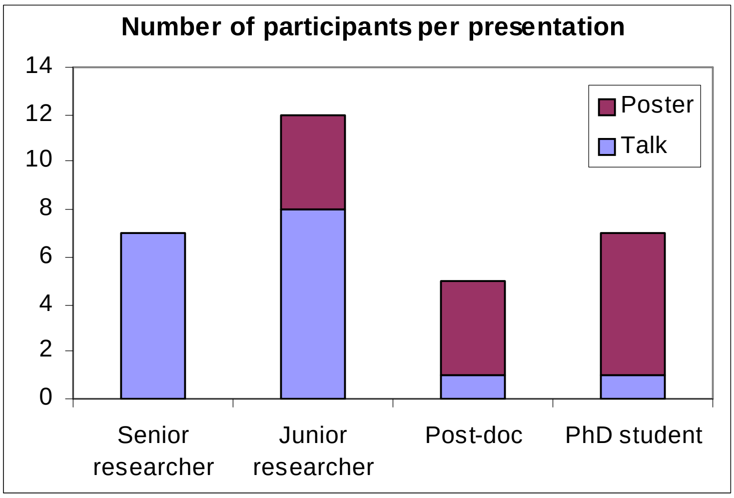
IV. Statistical information on participants

The total number of participants (including paying participants) was of 36 originating from 8 European countries. The histogram below shows their geographical repartition.



The workshop tried to retain a reasonable balance between senior and younger researchers, letting as many young researchers as possible give talks. The two histograms below detail the age repartition of the participants, together with their presentation. Let us point out that there was a total of 16 (44%) non-permanent researchers (PhD and post-docs).





V. Final list of participants

Name	Institution	E-mail
Antonio Acin	University Geneva Switzerland	antonio.acin@physics.unige.ch
Konrad Banaszek	University Oxford United Kingdom	k.banaszek1@physics.ox.ac.uk
Kamel Bencheikh	LPN France	kamel.bencheikh@lpn.cnrs.fr
Dan Browne	Imperial College United Kingdom	d.browne@ic.ac.uk
Nicolas Cerf	University Brussels Belgium	ncerf@ulb.ac.be
Ignacio Cirac	Max Planck Garching Germany	ignacio.cirac@mpq.mpg.de
Thierry Debuisschert	Thales LCR France	thierry.debuisschert@thalesgroup.com
Michaël Drewsen	University Aarhus Denmark	drewsen@ifa.au.dk
Jens Eisert	Imperial College United Kingdom	jense@ic.ac.uk
Jaromir Fiurasek	University Brussels Belgium	jfiurase@ulb.ac.be
Geza Giedke	Zürich ETH Switzerland	geza@giedke.de
Nicolas Gisin	University Geneva Switzerland	nicolas.gisin@physics.unige.ch
Oliver Gloeckl	University Erlangen Germany	gloeckl@kerr.physik.uni-erlangen.de
Philippe Grangier	Institut d'Optique France	philippe.grangier@iota;u-psud.fr
Frédéric Grosshans	University Brussels Belgium	frederic.grosshans@ulb.ac.be
Otfried Guehne	University Hannover Germany	guehne@itp.uni-hannover.de
Klemens Hammerer	Max Planck Garching Germany	klemens.hammerer@mpq.mpg.de
Vincent Josse	Lab. Kastler Brossel France	vincent.josse@spectro.jussieu.fr
Natalia Korolkova	University Erlangen Germany	korolkova@kerr.physik.uni-erlangen.de
Julien Laurat	Lab. Kastler Brossel France	laurat@spectro.jussieu.fr
Gerd Leuchs	University Erlangen Germany	leuchs@physik.uni-erlangen.de
Jérome Lodewyck	Institut d'Optique France	jerome.lodewyck@ens.fr

Stefan Lorenz	University Erlangen Germany	lorenz@kerr.physik.uni-erlangen.de
Norbert Lütkenhaus	University Erlangen Germany	luetkenhaus@kerr.physik.uni-erlangen.de
Christoph Marquardt	University Erlangen Germany	marquardt@kerr.physik.uni-erlangen.de
Klaus Mölmer	University Aarhus Denmark	moelmer@ifa.au.dk
Patrick Navez	University Brussels Belgium	patrick.navez@ulb.ac.be
Matteo Paris	University Pavia Italy	paris@unipv.it
Eugene Polzik	Niels Bohr Institute Denmark	polzik@phys.au.dk
Christine Silberhorn	University Oxford United Kingdom	silberhorn@physics.ox.ac.uk
Lluis Torner	University Barcelona Spain	torner@tsc.upc.sp
Nicolas Treps	Lab. Kastler Brossel France	nicolas.treps@spectro.jussieu.fr
Rosa Tualle-Brouri	Institut d'Optique France	rosa.tualle-brouri@iota.u-psud.fr
Gilles Van Assche	University Brussels Belgium	gvanassc@ulb.ac.be
Peter Van Loock	University Erlangen Germany	vanloock@kerr.physik.uni-erlangen.de
Jérôme Wenger	Institut d’Optique France	jerome.wenger@iota.u-psud.fr

VI. Conclusion

The organizing committee of this workshop would like to thank Mrs Christine Lane for her very efficient help realising this event.

All the texts and programmes of the workshop mentioned the help provided by the QUIPROCONE network, indicating clearly on each document the Quiprocone logo.

We would also like to specify that there is no publication plan resulting from the workshop, but we enclose below the abstract of each contribution – talks and posters.

Looking forward to having the pleasure to collaborating again soon with the Quiprocone network,

Yours sincerely,

Jérome Wenger **Philippe Grangier**
(on behalf of the organizing committee)

Appendix A. Detailed programme and abstracts

Friday 11 April 2003

15.00 Conference opening - coffee

Chair: Philippe Grangier
Institut d'Optique, Orsay, France

16.00 **Nicolas Treps**
Laboratoire Kastler Brossel, Paris, France

Quantum information processing in optical images

Optical images can be considered as multichannel communication devices. Therefore, the manipulation of their quantum properties allow the realisation of quantum information protocols in a multichannel configuration. We have realised two experiments, based on optical parametric oscillators (OPO) and amplifiers (OPA), that illustrate two different approaches to the general problem of "quantum imaging". These systems can be used to do quantum information processing and, also, to increase the sensitivity in optical resolution.

16.40 **Jens Eisert**
Imperial College, London, United Kingdom

Feasible distillation of continuous-variable entanglement

In this talk I will present a procedure that is capable of distilling Gaussian two-mode states from a supply of weakly entangled mixed states. This procedure makes use of passive optical elements and photon detectors distinguishing the presence and the absence of photons. On the one hand abstract issues of identifying the fixed points of the iteration map and its convergence properties will be considered. In particular, necessary and sufficient criteria for convergence to a pure Gaussian state will be presented. On the other hand, practical issues related to an actual implementation of such a procedure will be discussed, assuming non-unit detection efficiencies. The use of this method as a starting point for quantum key distribution will be outlined.

17.20 **Jérome Wenger**
Institut d'Optique, Orsay, France
Various organizationnal details

Free dinner

Saturday 12 April 2003

Chair: Eugene Polzik
Niels Bohr Institute, Copenhagen, Denmark

09.00 **Ignacio Cirac**
Max Planck Institute, Garching, Germany

Entanglement of Formation for Gaussian States
J.I. Cirac, G. Giedke, O. Krueger, R.F. Werner, and M.M. Wolf

We determine the entanglement of formation of symmetric Gaussian states and show that the optimal decomposition consists of pure Gaussian states.

09.40 **Geza Giedke**
Institute für Quantenelektronic, Zürich, Switzerland

Gaussian entanglement measures
M. Wolf, R. Werner, U. Krüger, G. Giedke, and J.I.Cirac

We introduce the Gaussian entanglement of formation and calculate it for two-mode Gaussian states. We discuss its additivity properties and compare it to other practical entanglement measures for Gaussian states.

10.20 **Poster session**

12.20 Lunch

Chair: Gerd Leuchs
University of Erlangen, Germany

14.00 **Philippe Grangier**
Institut d'Optique, Orsay, France

High-rate quantum key distribution using Gaussian-modulated coherent states
F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N.J. Cerf and P. Grangier

In the field of quantum information processing, a stimulating question is whether quantum continuous variables may provide a valid alternative to the usual quantum key distribution (QKD) schemes based on single photon counting. Here we demonstrate a novel QKD protocol based on the transmission of coherent states, containing a few hundred photons on average. The scheme relies on Gaussian-modulated coherent states and homodyne detection, and achieves high secret-key rates without requiring squeezed or entangled beams. It remains, in principle, efficient for any value of the line transmission by use of a "reverse reconciliation" technique, which is shown to be secure against individual attacks based on entanglement and quantum memories. The experimental implementation of our protocol is followed by the complete secret key extraction, yielding a net key rate of about 1.7 Mbps for a lossless line and 75 kbps for 3.1 dB on-line losses.

14.40 **Nicolas Gisin**
University of Geneva, Switzerland

The role of photon-numbers in coherent pulse quantum cryptography

Coherent pulses in one or several modes can be described as statistical mixtures of photon numbers, each photon being in superposition of the various modes. In the usual 2-mode case, each photon carries a qubit. Hence, continuous variable quantum cryptography is equivalent to protocols using a statistical number of qubits (with large mean qubit-number). This equivalence suggests new questions for large pulse protocols. It suggests also new protocols for weak pulse protocols.

15.20 Coffee break and posters

Chair: Nicolas Gisin
University of Geneva, Switzerland

16.00 **Norbert Lütkenhaus**
University of Erlangen, Germany

Quantum Key Distribution with Strong Reference Pulses
N. Lutkenhaus, Ch. Silberhorn, N. Korolkova, T.C. Ralph and G. Leuchs

Quantum Key Distribution is the most prominent example demonstrating the power of quantum communication. We know that these protocols can be implementet using weak coherent pulses even along channels with strong loss (10-20dB). In order to extend the range and the rate of key creation over this scheme new protocols are being developed. These schemes present new challenges in the analysis and processing of correlations established between sender and receiver. We present an approach to extract a secure key out of the correlations using post-selection procedures.

16.40 **Gerd Leuchs**
University of Erlangen, Germany

Advances in quantum communication with intense light pulses

Intense light pulses may exhibit quantum properties such as entanglement. Experiments are reported in which the quantum properties of intense optical soliton pulses are controlled via their non-linear interaction with the material. The wavelength used is within the 1.5 micrometer optical communication wavelength range and the optical non-linearities of standard waveguide structures are exploited. The quantum properties are enhanced when operating the pulses in the soliton regime. The conjugate quantum variables used to describe the quantum solitons are amplitude and phase quadratures or conjugate Stokes parameters. The latter approach has the advantage that direct detection is sufficient. It is, however, more complex because the commutator of the Stokes operators is an operator itself. The experimental progress towards the implementation of quantum communication protocols will be discussed.

17.20 End

Free dinner

Sunday 13 April 2003

Chair: Ignacio Cirac
Max Planck Institute, Garching, Germany

09.00 **Klaus Moelmer**
University of Aarhus, Denmark

Discrete and continuous variable approaches to measurement induced entanglement.

Atomic systems can be entangled by Quantum Non Demolition measurements of collective observables. We present theoretical analyses of two processes :
1. The entanglement of the continuous collective spin variables of large atomic samples are discussed in terms of state vectors conditioned on discrete single photon detection events. This analysis offers new insights and enables novel proposals for entanglement and teleportation operations.
2. Entanglement is obtained by detection of the optical transmission of a cavity containing a single pair of atoms. For this process, continuous measurements on coherent fields are superior over discrete measurements on number state fields.

09.40 **Eugene Polzik**
Niels Bohr Institute, Copenhagen, Denmark

Light-atoms quantum interface with continuous variables

Quantum interface between light and atoms is the basis for quantum memory for light, for generation of entanglement between distant atomic objects and for teleportation, to name a few applications. Continuous variables proved to be extremely suitable for these purposes. The progress in developing the light-atoms quantum interface using room temperature gases and cold atoms will be discussed.

10.20 Coffee break and posters

Chair: Philippe Grangier
Institut d'Optique, Orsay, France

11.00 **Nicolas Cerf**
Ecole Polytechnique, Brussels, Belgium

Non-gaussian cloning of gaussian states
N.J. Cerf and P. Navez

The concept of gaussian quantum cloning machines will be summarized. These cloning machines duplicate all coherent states with a fidelity of 2/3 and are known to be optimal over the set of gaussian operations. Here, we will investigate whether non-gaussian cloning transformations may beat this 2/3 fidelity limit for coherent states. Then, the application to non-gaussian attacks of continuous-variable quantum key distribution will be discussed.

11.40 **Natalia Korolkova**
University of Erlangen, Germany

Quantum communication with "classical" and non-clasical polarization states
N. Korolkova, S. Lorenz, J. Heersink, O. Gloeckl, N. Luetkenhaus and G. Leuchs

The use of continuous polarization variables in quantum communication is discussed. The generation and characterization of polarization squeezed and entangled states is reported. Their specific properties and applications for teleportation and cryptography are envisaged. A quantum key distribution scheme using coherent polarization states is presented as an alternative approach to squeezing/entanglement cryptography.

12.20 Lunch

Chair: Klaus Moelmer
University of Aarhus, Denmark

14.00 **Konrad Banaszek**
University of Oxford, United Kingdom

Engineering correlated photons for quantum information processing applications
A. B. U'Ren, E. Mukamel, K. Banaszek, and I. A. Walmsley

We analyse means to control spatio-temporal characteristics of photons generated in the process of spontaneous parametric down-conversion. Such control is necessary to achieve high-visibility interference in multiple-pair experiments without deleterious effects of filtering. It also offers a possibility to generate continous-variable entanglement in the spectral and the spatial degrees of freedom. In this context, we present our recent experiment to determine the transverse spatial coherence in the Wigner representation, and discuss its extension which can be used to probe spatial entanglement of photon pairs.

14.40 **Jaromir Fiurasek**
Ecole Polytechnique, Brussels, Belgium

Conditional generation of arbitrary multimode entangled states of light with linear optics
J. Fiurasek, S. Massar, and N. J. Cerf

We propose a scheme for probabilistic generation of an arbitrary multimode entangled state of light with finite expansion in Fock basis. The suggested setup involves passive linear optics, single photon sources, strong coherent laser beams, and photodetectors with single-photon resolution. As an interesting application of the present scheme, we will briefly discuss the generation of two-mode entangled states that yield a strong violation of Bell inequalities, when using balanced homodyne detection and root binning.

15.20 Coffee break and posters

19.30 **Conference Dinner** at restaurant "La Vieille Auberge", 63 rue Espariat (*rendez-vous* at 19.30 there)

Monday 14 April 2003

Chair: Nicolas Cerf
Ecole Polytechnique, Brussels, Belgium

09.00 **Peter Van Loock**
University Of Erlangen

Projective measurements using linear optics - discrete versus continuous variables

We give simple criteria to decide when arbitrary projective (von Neumann) measurements are possible solely by means of linear optics. These criteria highlight the differences between the discrete-variable and the continuous-variable approaches to measurements needed for quantum communication.

09.40 **Matteo Paris**
University of Pavia, Italy

Two and three mode CV entanglement in optical and BEC systems

We address optical CV two-mode entangled states (twin-beam) as a resource for precision measurements, state engineering, and characterization of devices, and analyze the degradation and the restoration of such entanglement in noisy channels. We then discuss the generation of three-mode CV entangled states and analyze possible applications in cloning and teleportation protocols. We consider bilinear interactions in second order nonlinear crystals, and collective atomic recoil in BE condensates.

10.20 Coffee break and posters

11.00 **Vincent Josse**
Laboratoire Kastler Brossel, Paris, France

Polarization squeezing and quadrature entanglement using cold atoms
V. Josse, A. Dantan, L. Vernac, A. Bramati, M. Pinard and E. Giacobino

We study the interaction of a nearly resonant linearly polarized laser beam with a cloud of cold atoms in a high finesse opical cavity. The Cross-Kerr effect due to the saturation of the optical transition produces quadrature squeezing on both the mean field and the orthogonally polarized vacuum mode. An interpretation of this vacuum squeezing as *polarization squeezing* is given and a method for measuring the quantum Stokes operator is developed. On the other hand, we generate two non separable beam, which entanglement is measured using the criterion for continous variables derived by Duan *et al* and Simon.

11.40 Lunch buffet

14.00 Departure

Poster presentations

Antonio Acin
University of Geneva, Switzerland

Quantum key distribution protocols more robust against photon number splitting attacks

We describe a new class of quantum key distribution (QKD) protocols that are robust against the most general photon number splitting attacks in a weak coherent pulse implementation. The eavesdropper (Eve) is supposed to have unlimited technological power while the honest parties (Alice and Bob) use present day technology, in particular an attenuated laser as an approximation of a single-photon source. The non-orthogonality of quantum states is exploited for decreasing the information accessible to Eve in the multi-photon pulses accidentally produced by the imperfect source. An implementation of some of these protocols using present day technology allow for a secure key distribution up to distances of 150 km. Moreover, they open the possibility for a connection from finite- to infinite-level QKD schemes.

Kamel Bencheick
Lab. de Photonique et Nanostructures, Marcoussis, France

Quantum key distribution with continues variables: The first steps towards the experimental demonstration

K. Bencheikh, T. Symul, A. Jankovic and J.A. Levenson

We will report on the ongoing experimental work dedicated to the demonstration of a quantum cryptography protocol based on entangled continues variables [1].
The protocol suggests the use of entangled quadratures of two electromagnetic fields (signal and idler) generated by phase sensitive parametric amplification (PSA). The signal being distributed to Alice and the idler is sent to Bob. The random bits of the secret key are naturally constructed by measuring the instantaneous quantum fluctuations of the correlated quadratures.
We will present the protocol for quantum key distribution and the experimental setup under construction. For the experimental demonstration, two identical PSAs are used. Each of which is based on a type-II KTP crystal pumped by a frequency doubled Nd:YLF laser emitting at 1054 nm. High speed InGaAs detectors and Boxcar averager will be used for the measurement of the instantaneous quantum fluctuations.

Dan Browne
Imperial College, London, United Kingdom

Gaussification with linear optics

D.E. Browne, J. Eisert, S. Scheel and M.B. Plenio

Entangled Gaussian states cannot be distilled using Gaussian operations, i.e. those which map Gaussian states to Gaussian states, alone. Therefore any distillation protocol for such states must consist of at least two stages. First a non-Gaussian step which generates an intermediate supply of more highly entangled non-Gaussian states, and then a "Gaussification" step which distills (ideally even more entangled) approximately Gaussian states from this intermediate supply. In this poster we summarise a possible non-Gaussian initial step and then describe a Gaussification protocol which uses linear optical elements. Together these steps form an entanglement distillation protocol for Gaussian states.

Thierry Debuisschert
Thalès TRT, Orsay, France

4 states protocol for time coding quantum key distribution
T. Debuisschert and W. Boucher

Coherent one photon pulses are sent with four possible time delays with respect to a reference. Ambiguity of the photon time detection resulting from pulses overlap combined with interferometric measurement allows for secure key exchange. The security is evaluated as a function of the QBER and of the contrast of the interferometer.

Michaël Drewsen
University of Aarhus, Denmark

Towards a quantum memory for photons based on an ion Coulomb crystal

An experimental project to use a two-species ion Coulomb-crystal inside an optical cavity as a medium for storage of quantum states of light is described. The ions in the nearly cylindrical shaped core of the ion bi-crystal will be situated within the TEM00 mode volume of a high-finesse optical cavity and serve as the storage medium, while the outer ion species will be laser cooled and indirectly cool the “memory” ions. The concept of the storage process follows the initial idea of Ref. [1] involving dynamical cavity impedance matching and electromagnetic induced transparency. The presentation will include recent experimental progress on several part of the project.

[1] M. D. Lukin, S. F. Yelin, and M. Fleischhauer, “Entanglement of atomic ensembles by trapping correlated photon states”, Phys. Rev. Lett. 84, 4232-4235 (2000).

Oliver Gloeckl
University of Erlangen

Interference of two intense entanglement sources: entanglement swapping and multi-partite correlation
O. Gloeckl, S. Lorenz, C. Marquardt, J. Heersink, P. van Loock, N. Korolkova and G. Leuchs

We present a protocol for performing continuous variable entanglement swapping with intense pulsed beams. In a first step, the generation of amplitude correlations between two systems that have never interacted directly is demonstrated. This is verified in direct detection with electronic modulation of the detected photocurrents. The measured correlations are better than expected from a classical reconstruction scheme by 1.77dB. In the entanglement swapping process, a highly correlated four–partite state is generated. We show experimentally that the amplitudes of these four optical modes are quantum correlated 3 dB below shot noise. A theoretical analysis indicates that these correlations are due to four–party entanglement.

Frédéric Grosshans
Université Libre de Bruxelles, Belgium

Virtual Entanglement in Coherent States Quantum Cryptography

We have proposed [1] and experimentally demonstrated [2] quantum key distribution (QKD) protocols using coherent states. Since entangled Gaussian states are multimode squeezed states, the lack of squeezing in our protocols implies no entanglement is present during such protocols. However, it is possible to exhibit an entanglement based protocol equivalent to the coherent states protocol. This is in agreement with our study of reverse reconciliation protocols [3], which allow key distribution over lossy channels. The conclusion of this approach is that, if entanglement is not actually needed for QKD, the possibility that the two partners could have used it is crucial. In some sense, even if no actual entanglement is needed, ``virtual entanglement'' is necessary for QKD.

[1] F. Grosshans and Ph. Grangier, Continuous Variable Quantum Cryptography using Coherent States, Phys. Rev. Let. 88:057902 (2002). E-print quant-ph/0109084.
[2] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf and Ph. Grangier, High-Rate Quantum Key Distribution using Gaussian Modulated Coherent States, Nature 421:238 (2003)
[3] F. Grosshans and Ph. Grangier, Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables, in Proc. of the 6th Int. Conf. on Quantum Communications, Measurement, and Computing (QCMC'02, Boston, July 2002). E-print quant-ph/0204127.

Klemens Hammerer
Max Planck Institute, Garching, Germany

Quantum control of light/matter interaction: quantum memory for light
K. Hammerer and J. I. Cirac

Continuous variable quantum states can be transmitted easily by means of light pulses while atomic spin states on the other hand are capable of coherent storage of these states. Recent experiments [1] show that off-resonant light/matter interaction in a warm atomic ensemble can be used for the purpose of such a quantum memory. Within the setting of these experiments we analyze from a control theoretic point of view how the given interaction between light and matter can be employed optimally to map the quantum state of light onto atoms and vice versa.

[1] Julsgaard B, Kozhekin A, Polzik ES, NATURE, 413 (6854): 400-403 2001

Natalja Korolkova
University of Erlangen, Germany

Novel nonclassical polarization effects
J. Heersink, T. Gaber, S.Lorenz, O. Gloeckl, N. Korolkova and G. Leuchs;

We report on the generation of polarization squeezing and polarization entanglement of intense, short light pulses using an asymmetric fiber Sagnac interferometer. The Kerr non-linearity of the fiber is exploited to produce independent amplitude squeezed pulses. The experimental results for a single amplitude squeezed beam are compared to the case of two phase-matched, spatially overlapped amplitude squeezed pulses. For the latter, noise variances of -3.4 dB below shot noise in the S0 and the S1 and of -2.8 dB in the S2 Stokes parameters were observed, which is comparable to the input squeezing magnitude. Polarization squeezing, that is squeezing relative to a corresponding polarization minimum uncertainty state, was generated in S1. Polarization entanglement was generated by interference of the polarization squeezed field with a vacuum on a 50:50 beam splitter. The two resultant beams exhibit strong quantum noise correlations in S1 and S3. The sum noise signal of S3 was at the respective shot noise level and the difference noise signal of S1 fell -2.9 dB below this value.

Julien Laurat
Lab. Kastler Brossel, Paris, France

Bright EPR beams with a self-phase-locked non-degenerate OPO
J. Laurat, L. Longchambon, T. Coudreau and C. Fabre

In standard continuous type II phase matched Optical Parametric Oscillator (OPO) above threshold, the orthogonally polarized signal and idler waves show large quantum intensity correlations (twin beams) and also phase anti-correlations. However, due to a classical phase diffusion phenomenon, the measurement of phase properties is impossible. We describe theoretically the steady regime and the quantum properties of an OPO containing a birefringent plate. Such a linear coupling allows a frequency degenerate operation as well as phase locking between the signal and idler modes. This system is expected to be a reliable light source of continuous quadrature entanglement. The experiment is in progress and we will report the first achieved steps.

Squeezed State Generation using Conditional Measurement
J. Laurat, T. Coudreau, N. Treps, A. Maitre and C. Fabre

Conditional state reduction via quantum correlations plays a key role in a large number of discrete variables quantum optics experiments. Single photon Fock state producing by conditional measurement on photon pairs is perhaps the most widely used example. If this general procedure has been intensively studied in the photon counting regime, no scheme has been suggested so far to generate non classical bright beams. We will present a new and simple method to conditionally prepare a bright intensity squeezed beam.
The requiste correlations between a signal and a trigger are produced by a non degenerate Optical Parametric Oscillator above threshold. When the "twin beams" are detected, the photocurrents exhibit very strong correlations. We keep only the time intervals for wich the trigger's photocurrent is within a given band around the mean value. The signal is thus reduced to a squeezed state and the Fano factor of the resulting light beam is twice the remaining noise on the intensity difference. The measurements are in good agreement with theoretical calculations as well as numerical simulations.

Jérôme Lodewyck
Institut d'Optique, Orsay, France

Quantum bit commitment with continuous variables

Bit commitment is a basic cryptographic protocol which enables toss-up between two untrustworthy actors, Alice and Bob. Alice commits a bit to Bob. The protocol has to be "binding" (Alice cannot change her commit) and "concealing" (Bob cannot know the bit before a given phase of the play). Since Mayers (95), it is widely believed that secure quantum bit commitment is impossible. However, cheating requires extraordinary high quantum computing power. Hence, an experimental demonstration based on continuous variables is possible.

Stefan Lorenz
University of Erlangen

Quantum cryptography with intense beams of light
S. Lorenz, Ch. Silberhorn, O. Gloeckl, N. Luetkenhaus, J. Schneider, C. Marquardt, N.Korolkova and G. Leuchs.

We present a quantum key distribution scheme which relies only on the polarization uncertainty of coherent states. Four overlapping non-orthogonal states are used to generate correlations between two parties. By evaluating his measurement results of the states sent by Alice properly, the receiving party (Bob) can retain only the results which give him an information advantage over a potential eavesdropper. We present preliminary results on the experimental realization of the state generation (Alice) and measurement (Bob) apparatus. The four states to be transmitted are generated by modulating the polarization of a weak cw laser beam. The detection consists of a polarization analyser using a balanced photodetector and an electro-optical modulator to switch between different measurement bases. Results on state generation and discrimination at moderate bit rates are shown.

Patrick Navez
Université Libre de Bruxelles, Belgium

Coherent state quantum cryptography by means of intensity measurement

We propose a two-mode quantum cryptographic protocol in which two coherent signals are sent from Alice and received by Bob who performs a simple intensity measurement rather than a homodyne detection. The protocol is such that Bob measures the intensity either on the two modes, or on linear combination of the modes resulting from a 50:50 beam splitter attack. Directe or reverse reconcilation procedure in the post treatement of information allows Alice and Bob to exchange a secret key.

Christine Silberhorn
University of Oxford, United Kingdom

Quantum key distribution with continuous variable entangled beams for lossses beyond 3 dB

It was shown recently [1], that the apperent 3 dB loss limit of for quantum key distribution with coherent states implied by a beamsplitting eavesdropper attack can be overcome by an appropriate post-selection of the measured data by Alice and Bob. Here we show, that actually the post-selection is not restricted to continuous variable quantum key distribution with coherent states, but can also be applied for a squeezed or entangled state protocol.

[1] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. 89, 167901, (2002).

Rosa Tualle-Brouri
Institut d'Optique, Orsay, France

Maximal Violation of Bell Inequalities using Continuous Variables Measurements
J. Wenger, M. Hafezi, F. Grosshans, R. Tualle-Brouri and P. Grangier

We present a whole family of quantum states allowing a maximal violation of Bell inequalities using quadrature phase homodyne detection. In order to get the binary results involved in the CHSH inequality, we use a binning process called root binning. The influence of losses is considered, and the possibility to synthesize such states is also explored.

Gilles Van Assche
Université Libre de Bruxelles, Belgium

Security Aspects of QKD Protocols Using Coherent States

We analyze the security of a continuously-modulated QKD protocol using coherent states and homodyne detection. This protocol is examined from both a physical and a classical processing point of view, and is shown to be robust against non-Gaussian attacks. This is done by generalizing sliced error correction to an entanglement distillation procedure.