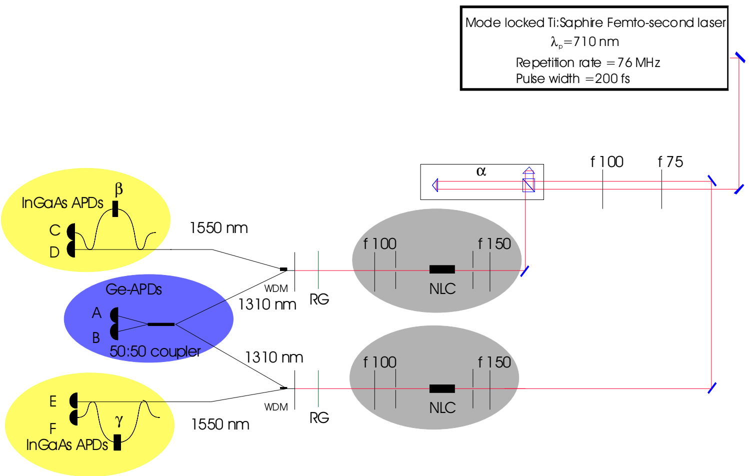
QuComm

IST-1999-10033

Long Distance Photonic Quantum Communication

Periodic Progress Report N°2, Deliverable D8

Covering period 1.1.2001-31.12.2001



Report Version: 1

Report Preparation Date: 2001-12-28

Classification: Public

Contract Start Date: 2000-01-01 Duration: 36 months

Project Co-ordinator: Professor Anders Karlsson, Kungliga Tekniska Högskolan, Sweden

Partners:
P01-KTH, Kungliga Tekniska Högskolan, Kista, Sweden
P02-LMU, Ludwig-Maximilians-Universität München, München, Germany
P03-EXPUNIVIE, Institut für Experimentalphysik der Universität Wien, Wien, Austria
P04-Oxford, University of Oxford, Oxford, United Kingdom
P05-GAP, University of Geneva, Group of Applied Physics, Geneva, Switzerland
P06-LANL, Los Alamos National Laboratory, Los Alamos, New Mexico, United States of America
P07-TH LCR, THALES, Courberville, France
P08-DERA, QinetiQ, Malvern, United Kingdom

Project Internet site: http://www.ele.kth.se/QEO/qucomm/

Project funded by the European Community under the "Information Society Technologies" Programme (1998-2002)

Table of Contents

Executive summary

The work in the QuComm project has continued in the second year with great enthusiasm. Two informal project meetings were held during the year, one in conjunction to the QUICK workshop (see below), a second in conjunction to the EU QIPC workshop in Torino.

Among technical highlights we like to mention (not in order of importance)

- The work of Oxford on stimulated emission into polarization entangled modes “entangled photon laser” and the use of the source in the first experimental demonstration of violation of a spin-1 Bell inequality.
- The free space quantum cryptography trials of LANL up to 10 km (Dec. 2001) and DERA (now QinetiQ) up to 1.2 km (most of the DERA work falls within EQCSPOT). While not yet using entanglement schemes the trials are very important with respect to investigation quantum cryptography under field like situations.
- The realisation of four-photon entangled state correlation by EXPUNIVIE.
- The work of Oxford and EXPUNIVIE on quantum error filtering/purification (presented in PRA and Nature), and of KTH and GAP on multilevel quantum cryptography
- The demonstration of third-order mode laser which is phase-matched for down-conversion by TH LCR (THALES)
- The succesful organization of the QUICK conference, April 7-13, 2001 in Cargese, Corsica, by KTH, DERA and Philippe Grangier of QuiCov and S4P. The conference attracted most of the prominent groups involved in quantum communication, notably in quantum cryptography, and gave an excellent overview of the international state-of-the-art.

Concerning the dissemination and use of results, the work in QuComm generated extensive media coverage worldwide. A number of publications and conference presentations (invited talks, regular talks, posters) where presented by QuComm members. Liaisons were also maintained with the IST OPTIMIST project (with QuComm presented at ECOC), as well as to the QUIPROCONE network. Following internal discussions in the consortium, it was decided that the industrial pick-up could be handled without the industrial reference committee originally planned. One reason for this is that several of the consortium members have already entered discussions with industrial interests concerning commercialisation of quantum information technologies.

Overall, the work follows the original project plan well, with mostly no delays in milestones and deliverables. Some shifts in milestones have also been decided based upon the results obtained in the scientific work.

.

Work progress overview

In the last few years, there has been a remarkable progress in the field of *Quantum Information Processing and Communication* - QIPC. The **QuComm** project deals with photonic quantum communication and has the objectives

– To scale experimental quantum communication protocols, notably quantum teleportation, entanglement swapping and entanglement enhanced quantum cryptography, towards longer distances.

– To demonstrate novel quantum communication protocols.

– To validate optical quantum communication technologies in an application context through various field tests of the developed concepts and technologies.

– To identify and transfer "spin off" results to industries or to industries-to-be.

Specific objectives during year two has been

- To make use of the user-friendly sources of entangled states developed during year one. This objective has been met.
- To study multi-photon entangled states theoretically and experimentally. This objective was met.
- Finally, on the management side the goal was to keep the collaborative atmosphere between all groups going. We believe this objective was met.

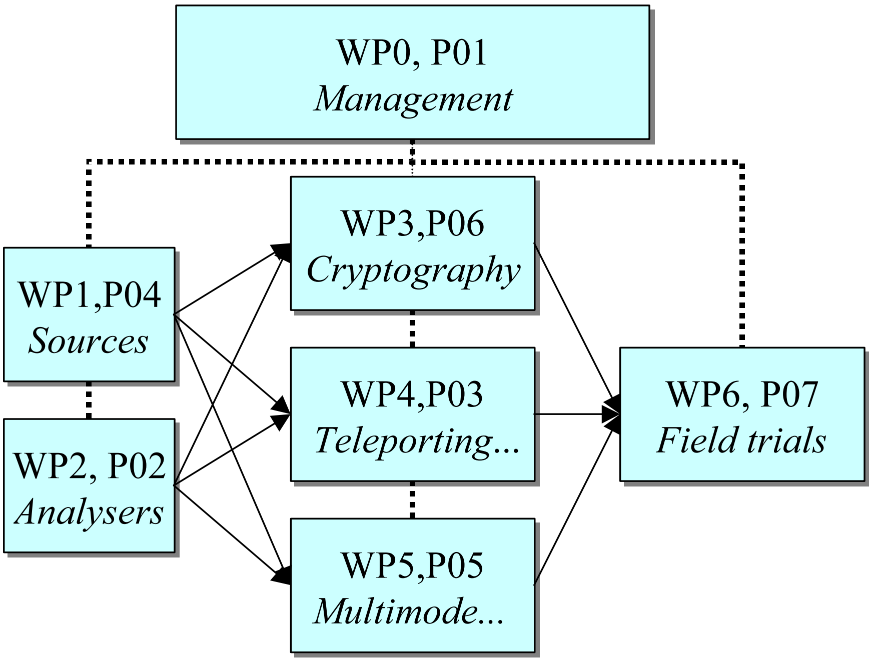


Table:
Division of work in work-packages.
Partners are
P01=KTH
P02= LMU
P03=EXPUNIVIE
P04=Oxford
P05=GAP
P06=LANL
P07=TH LCR
P08=DERA

The work in QuComm is divided into six work-packages (WPs), see figure above. WP0 is the management and dissemination WP. WP1 on sources, and WP2 on quantum state analysers, form the enabling building blocks for the subsequent work. Once the sources and detectors are available they will be transferred to the later WPs: WP3 on entanglement enhanced quantum cryptography, WP4 on teleporting entanglement, and WP5 on multi-mode and multi-state protocols. In WP 6 the assembled work in earlier work-packages will be used to conduct trials outside the laboratory setting.

Before describing the progress made per work-package in detail, we give first an updated simplified chart showing the overall status of deliverables and Milestones :

Deliverables & Milestones			
	Originally	**Actual**	**Comment**
Work-package	**Planned**	**Status (when reached)**	
WP0			
Deliverables	D6 (T0+18) D7 (T0+18) D8 (T0+24)	D6 (T0+18) D7 (T0+18) D8 (T0+24)	
Milestones	No milestones		
WP1			
Deliverables	D11 (T0+18) D12 (T0+24) D13 (T0+24)	D11 (T0+18) D12 (T0+24) D13 (T0+24)	
Milestones	M3 (T0+12) M4 (T0+18) M5 (T0+18) M6 (T0+24) M7 (T0+24) M8 (T0+24)	M3 (T0+18) M4 (T0+18) M5 (T0+18) M6 (T0+24) M7 (T0+24) ---	M3 partly met M4 partly met M5 met M6 partly met, see D13 M7 partly met M8 not yet met
WP2			
Deliverables	D15 (T0+18)	D15 (T0+18)	
Milestones	M11(T0+18) M12(T0+18) M13(T0+18)	M11(T0+18) --- M13(T0+18)	M11 not met M12 not yet met M13 partly met
WP3			
Deliverables	D16 (T0+18) D17 (T0+24)	D16 (T0+12) D17 (T0+24)	This will be final version
Milestones	M14 (T0+12) M17 (T0+18) M18 (T0+24)	M14 (T0+18) --- ---	M14 met M17 not yet met M18 not yet met
WP4			
Deliverables	D18 (T0+18)	D18 (T0+18)	
Milestones	M17 (T0+18)	M17 (T0+18)	M17 partly met
WP5			
Deliverables	D20 (T0+18)	D20 (T0+18)	
Milestones	M21 (T0+12) M22 (T0+18) M23 (T0+24)	--- --- M23 (T0+24)	M21 not met M22 not met M23 met
WP6			
Deliverables	No deliverables		
Milestones	No milestones		

WP0: MANAGEMENT, DISSEMINATION AND TAKE-UP OF RESULTS

The objective of WP0 is the management and co-ordination of the project, the dissemination of the results, and to assure the transfer and take-up of direct project results and/or spin-offs by industry at the earliest stage possible.

Deliverables

D6(T0+18): Joint IST FET workshop (P01, P02,P03,P04,P05, P06,P07 ,P08)

P01 (KTH) & P08 (DERA): Together with P. Grangier of QUICOV we organised the European High Level Scientific Conference *"Quantum interference and cryptographic keys: novel physics and technologies (QUICK)"* with **P08 (DERA)** as treasurer and **P01 (KTH)** as responsible for public relations and secretary. We believe the conference was quite successful, but it took much more time than anticipated to organise it. As we had attendance from all the groups of QuComm we also organised a small meeting to discuss the project progress.

D7 (T0+18): Half year progress report year 2 (P01, P02,P03,P04,P05,P06,P07,P08)

Delivered on time.

D8 (T0+24): Second year annual report (P01, P02,P03,P04,P05,P06,P07,P08)

Delivered on time.

Milestones

No milestones in this WP.

Further results of year two and work in progress

P01(KTH): M. Bourennane of KTH successfully defended his Ph.D. thesis *"Long-Wavelength Quantum Cryptography, Single-Photon Detection and Quantum Entanglement Applications"*. As the faculty opponent was Prof. Eugene Polzik, Århus (QUICOV). This is the second Ph.D. thesis with QuComm work, the first of Gregoire Ribordy from **P05 (GAP)**, took place in 2000, and was mentioned in the 2000 annual report.

P02 (LMU): Worked on and submitted as a coordinator a proposal for a research training network "PEQI- Photonic Entanglement and Quantum Information". The application was narrowly rejected.
The work on diode pumped generation of entangled photon pairs is described in the "Nature Physics Portal -Research Highlights" (6847-3), and in the German Bild der Wissenschaft Newsticker (13.8.01).
Introductory book article (P02, P03):
H. Weinfurter, A. Zeilinger: *Quantum Communication*, in 'Quantum Information - an introduction', (eds. G. Alber, H. Steiner), Springer, 2001.

P03(EXPUNIVIE) has written a review article for the "Entangled Photons Cryptography", which appear in a well renown german computer magazin:Thomas Jennewein, Gregor Weihs, Anton Zeilinger, "Schrödingers Geheimnisse", c't, No. 6/2001.

P05 (GAP) and P06 (LANL): The entanglement distillation paper (ref. 2) of LANL and GAP were commented upon in
"Cleaning Up Entangled Quantum States", Melissa Checker, Technical Insights (spring, 2001).
"Getting All Entangled Up", Tony Sudbery, Physics World, p. 24 (May, 2001)

Paul G. Kwiat of **P06 (LANL)** is from Jan. 2001 Professor of Physics at University of Illinois at Urbana-Champaign. The discussions concerning contractual issues were resolved in the simplest manner possible, with Richard Hughes of LANL taking over the formal responsability and Paul Kwiat remaining within the project through informal collaborations.

Concerning the consortium agreement, this is not yet signed. The latest version read and approved by most partners is currently with the legal contact person of the co-ordinator.

The collaboration between various nodes in QuComm has been good: there have been several visits between the nodes and there has even been transfer (loan) of equipment between nodes. In the description to follow the work is mainly described according to work-parts, but it is impossible to describe the work not also listing the individual partner contributions:

WP1: Entangled state sources

The objective of WP1 is to build user-friendly sources of optical quantum states, which are to be used in the later work-packages.

Deliverables

D11 (T0+18): Report on diode laser pumped non-linear crystal source for entangled states (P01, P05, P06).

Delivered on time.

D12 (T0+24): Prototype integrated GaAs laser photon pair source (P07)

This has not yet been achieved.

D13 (T0+24): Report on synchronisation of separate pair-photon sources (P02,P03)

Delivered on time

P02 (LMU): State-of-the-art of synchronization of mode-locked lasers was performed. As it turns out, recent developments, both for special applications in optical frequency synthesis and for commercial applications now supply the tools necessary for future concatenated long-distance quantum communication.

Milestones

M3 (T0+12): Prototype breadboard systems developed. Target: 10kHz coincidences and >95 % visibility of polarisation and interference fringes (P01, P02, P06, P08).

This milestone has been achieved for a system operating at 850/850nm by **P02 (LMU)** but research is still in progress to complete the 800/1500 and 1500/1500 breadboard systems. At **P05 (GAP)**, pumping a KNbO3 nonlinear crystal with a 100 mW frequency doubled yttrium aluminium garnet (YAG) laser emitting at 532 nm, more than 50 kHz of energy-time entangled photon pairs at 810 and 1550 nm wavelength have been detected using photon detectors based on silicon and InGaAs avalanche photodiodes, respectively. Two-photon interference fringes exhibit visibilities of up to 92%. This source has already been implemented for energy-time entanglement quantum cryptography (see WP3, M15).

Following work for M3, **P02 (LMU)** developed a prototype breadboard systems of polarisation entangled photon pairs, the published results found response in the scientific community. The system is currently redesigned to enable implementation of blue laser diodes. The work of P02 (LMU) and **P05 (GAP)** is reported in D11

P08 (DERA) has built a breadboard based pair photon source. A 3mW diode laser source has been characterised and we find it suitable for pumping parametric downconversion. Using a 3mm Type I BBO crystal we obtain coincidence rates of 4.5kHz with 15% detection efficiency into 9um core (three-mode) fibre We expect to optimise to better than 25% efficiency. A 5mm type II crystal and 2.5mm compensator crystal have been purchased but problems with diode laser has delayed measurement of entangled photons.

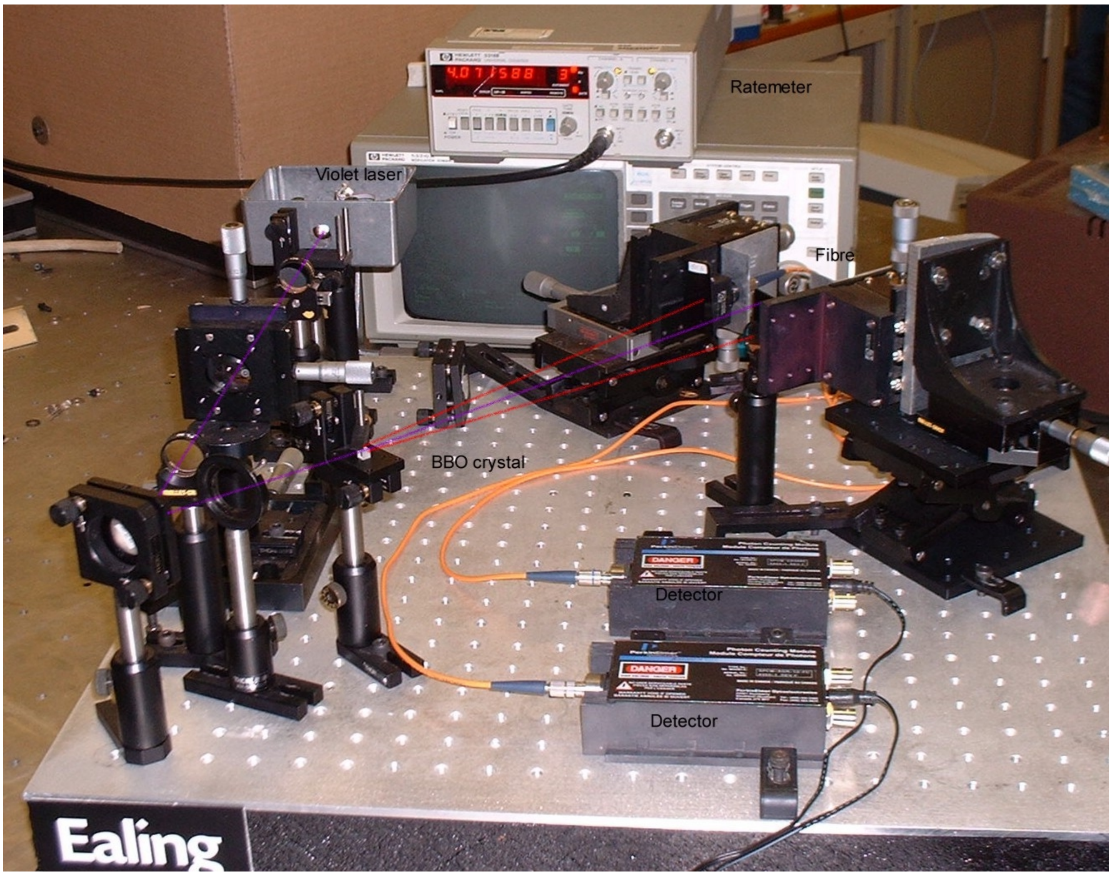


Figure caption: Entangled pair photon source on a 60cm square breadboard. The source is pumped by a CW diode laser (406nm) and will produce ~10K coincidences per second. At present detectors are local to the breadboard but year 3 realisation will be free space separated for QC demonstrations.

M4 (T0+18): Optical characterisation of non-linear lasers (P07).

This milestone has been achieved by TH LCR (P07), see their report below.

M5 (T0+18): Breadboard systems for 800/800 pairs done (P01, P06,P08).

This milestone has been achieved by LMU and DERA (LMU work reported in D11)

M6 (T0+24): Achieved synchronisation of two sources of entangled states (P02)

As described in D13, synchronisation of pulsed modelocked lasers, the core to synchronize sources, in the meantime became a commercial option. However, the laser available at LMU is not upgradeable and the recently bought new laser has different repetition rates and thus con not be synchronized with the other product at all. This laser was ordered due to its much improved specifications (output power >2 W) which are desperately needed for many experiments within QuComm. We thus propose to cancel this milestone as the essential (and at the time of the application novel) part of this task is now readily available.

M7 (T0+24): Generation of novel 2-photon states, including partially mixed and hyper-entangled states (P05,P06)

This milestone has partly been met.

.

M8 (T0+24): Delivery of packaged, pigtailed electrically pumped semiconductor laser module of twin photons (P07).

This milestone has not yet been met, see comment below.

Further results of year two and research in progress

WP1.1 Develop bright sources of entangled pair photons

At **P01 (KTH)**, Progress has been made on entangled pair generation using both a long-coherence-time frequency-doubled YAG laser and a picosecond modelocked Ti:sapphire laser as pump sources. In both cases type-II collinear downconversion is performed in a 12mm long BBO crystal.

In the case of the 532nm pumped system, generating pairs at 810nm and 1550nm for signal and idler respectively, the bare count rate for detection of the signal in a commercial silicon single photon counting module is of order 10^6 per second. The coincidence rate for the idler channel, using a home-made gated InGaAs SPAD (Epitaxx) is of order 1000 per second. Work is in progress to improve on this coincidence rate with better coupling into the single mode fibre.

Downconversion experiments pumped with the modelocked Ti:sapphire laser from 775nm to two degenerate, but orthogonally polarised, photons at 1550nm, is typically generating 1000 counts per second. Work is underway to again improve on the coupling efficiency to acheive a symmetric count in the two channels. Coincidence measurements will then be performed.

P05 (GAP) have demonstrated time-bin entanglement with ultrashort pulses with non-degenerate photon pairs at telecom wavelengths [35]. We use a Ti-Sapphire fs laser and a bulk interferometer to pump a $KNbO_3$ crystal, thus generating time-bin photons pairs at 1310/1550 nm (figure 1). Entanglement is shown by performing a Franson-type Bell test. Visibilities of up to 92 % have been observed. A scientific paper is in preparation [35].

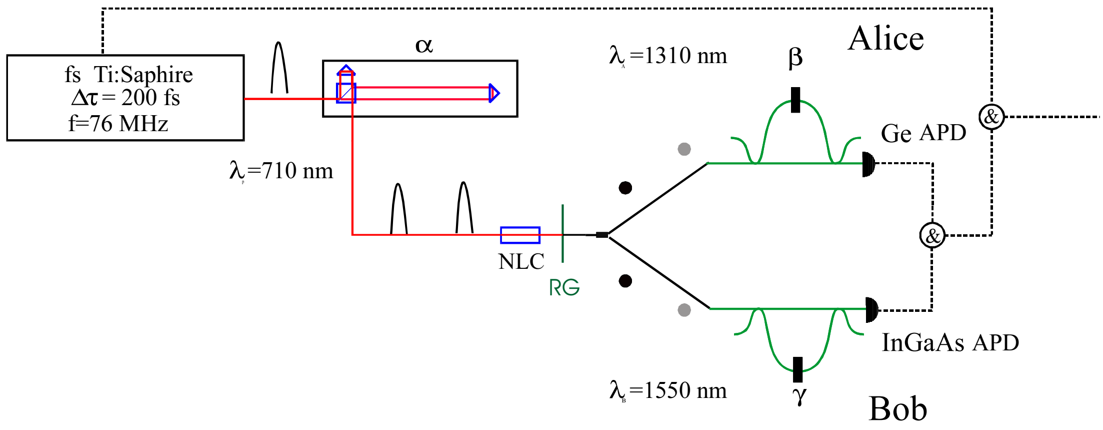


Figure 1 : Experimental setup used to demonstrate time-bin entanglement at telecom wavelength (1310-1550 nm) with ultrashort pulses.

We studied both theoretically and experimentally the creation of more than one pair in a laser pulse, and we developped a simple tool to quantify the probability of such events to happen [34,35]. The method is based on the study of side peaks due to the detections of photons coming from different laser pulses.

In WP 1.1**, P06 (LANL)** made investigations of ways to improve the entanglement purity over large collection angles.

Recently, a highly interesting development initated by **P05 (GAP)** is concerned with novel solutions for high efficiency down-conversion. Of particular interest could be quasi-phase matched (QPM) materials, and indeed the joint work of GAP and University of Nice. Of particular on down-conversion in QPM waveguides seems extremely promising, see [32,33,34].

Degenerate parametric down conversion at 1310 nm has been observed in quasi-phase matched Periodically Poled Lithium Niobate (PPLN) waveguides. An increase of the efficiency of the photon-pair creation of 4 orders of magnitude compared to bulk crystals has been reported [32]. Energy-time entanglement has been shown in the cw case with a Franson Bell test, and visibilities of up to 92 % (97% after noise substraction) have been observed [34].

During the period october-december 2001, The PPLN waveguide has been used together with a pulsed ps laser diode at 655 nm to generate time-bin entangled photons at 1300 nm. With a bulk pump interferometer, visibilities of up to 90 % have been observed, for very low pump powers (~10 µW). Tests with a fiber pump interferometer are under way.

Concerning such novel sources, PO8 (DERA) furthermore has collaborated with P04 on novel PPLN pair photon sources and P04/P06 on developing GaAs waveguide sources of photon pairs

P07 (TH LCR); Twin photon source based on parametric fluorescence in a semiconductor laser

The purpose of the work of TH LCR is mainly to develop an electrically pumped semiconductor laser of direct generation of twin photons at 1.55 microns.

The effort was mostly focused on the development of a laser diode emitting on the third order mode. The waveguide is designed in such a way that the third order laser mode is phase matched for parametric generation with the fundamental order modes at the signal/idler frequencies.

Such kind of source must meet several constraints arising from:

- the phase matching through compensation of the chromatic dispersion with modal dispersion.
- the optimisation of the overlap integral, hence the nonlinear conversion efficiency.
- The optimisation of injection of the generated carriers into the quantum well.

This requires a large dynamics in refractive index (form 2.9 to 3.5) , therefore the system Al(1-x)Ga(x)As is the natural choice. In particular, the cladding must provide a strong confinement, therefore AlAs is used, although a special care must be used to passivate the air-exposed surfaces of the final device. A special care must be paid to prevent the many interfaces, needed for the optimisation of the nonlinear interaction, making barriers for the carriers and hence degrading performances.

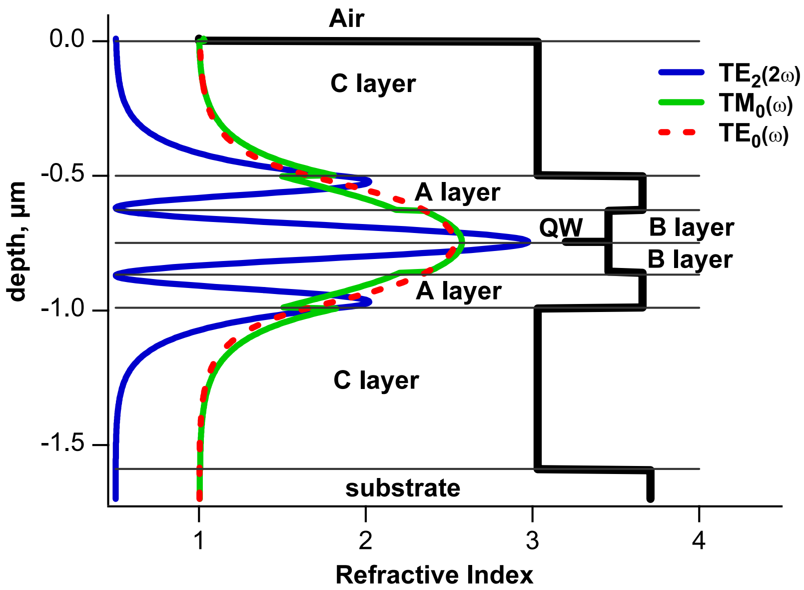


Figure 1

Optically pumped laser

An optically pumped third order mode laser was presented at the last QUCOMM meeting and in the last report. The sample structure meeting those requirements is illustrated in Fig. 1; the waveguide double core is composed by two $Al_{0.25}Ga_{0.75}As$ layers (A), two $Al_{0.50}Ga_{0.50}As$ spacer layers (B), and a $Al_{0.11}Ga_{0.89}As$ quantum well (QW). The waveguide core is sandwiched between two thick AlAs cladding layers (C). This structure was grown by MBE on a semi-insulating GaAs substrate.

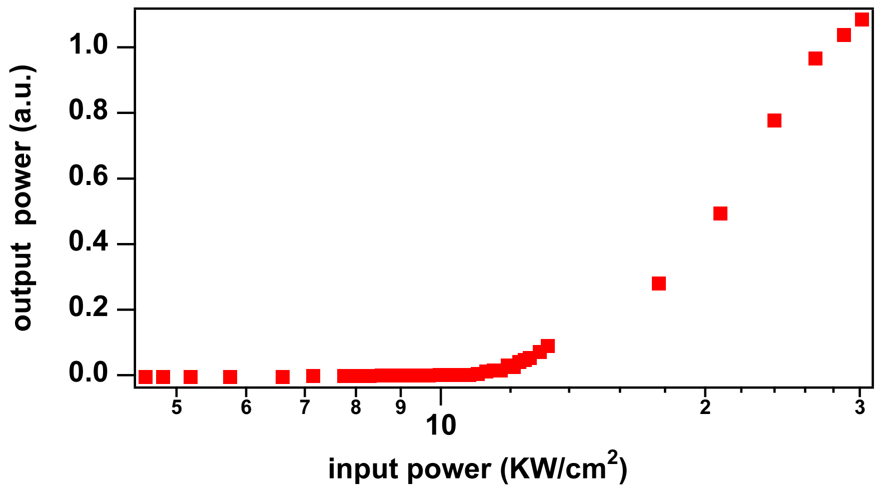


Figure 1: typical Pout-Pin plot.

The samples were optically pumped by a pulsed Nd :YAG laser (10 Hz, 6 ns). Laser emission from the QW was observed around 775 nm at room temperature, with threshold in the range 5 – 15 KW/ cm^2, i.e. 5 times the predicted threshold in the best samples.

The laser operates on the third order mode from 10K to room temperature. High temperature operations on the third order mode have been obtained as well, with negligible variation in slope efficiency. This is very important in order to tune the device over the widest range possible and thus meeting the phase-matching condition, despite of a possible non nominal epitaxy Figure 3.

The far field of the laser emission was measured by an angular scan on the vertical plane of the waveguide. Figure 2 shows the angular dependence of the far field (points), compared the calculated farfield corresponding to the 3rd order mode.

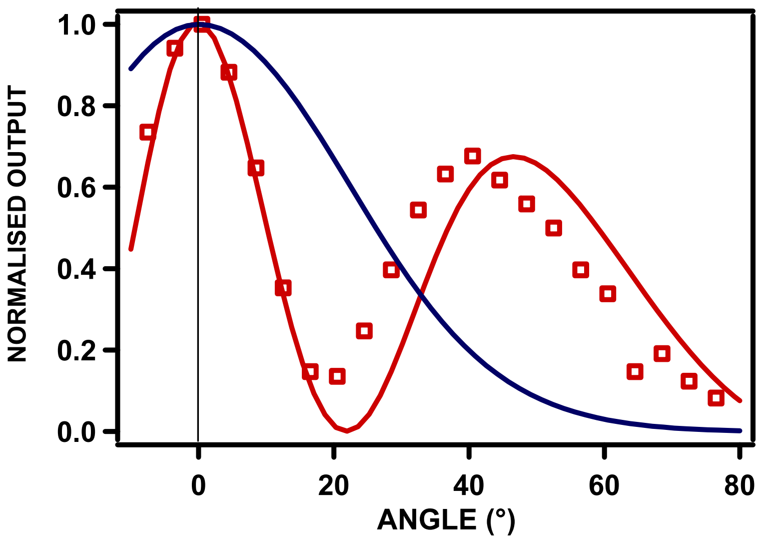


Figure 2: Emitted far field (markers) compared with the calculated pattern corresponding to a fundamental and a 3rd order mode.

The source developed meets all the preliminary requirements to produce parametric fluorescence through modal phase matching. In order to demonstrate parametric down conversion a brand new experimental set-up must be designed, meeting several conflicting requirements. The experiment must be carried on by varying the temperature, since the modal phase matching is expected to occur at a given temperature.

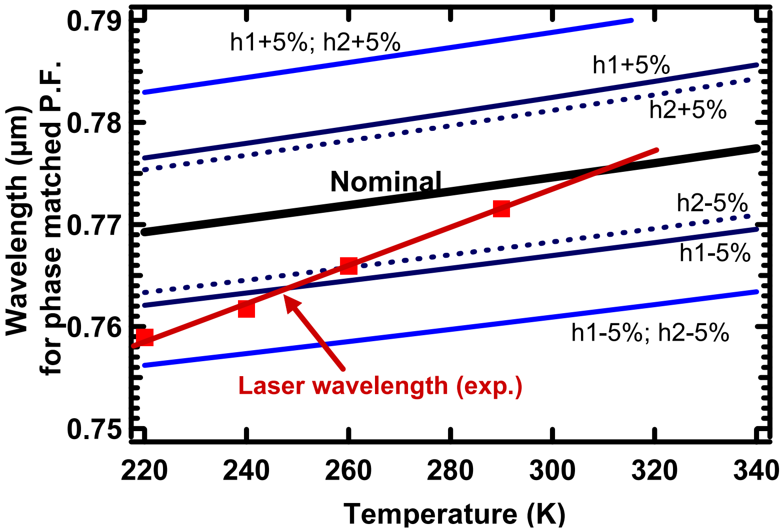


Figure 3: phase matching wavelength, tacking into account tolerances.

These results have been submitted to APL [36,37].

Electrically pumped laser

A sample was designed, grown and processed to make an electrically pumped device. The main difficulty of the design arises from the transport of carriers in the aluminium rich cladding, were the mobility is low. Moreover, the effect of the several barriers must be carefully taken into account, to prevent carriers being blocked by the barriers. Simulations with a proprietary code for vertical transport in heterostructures was used.

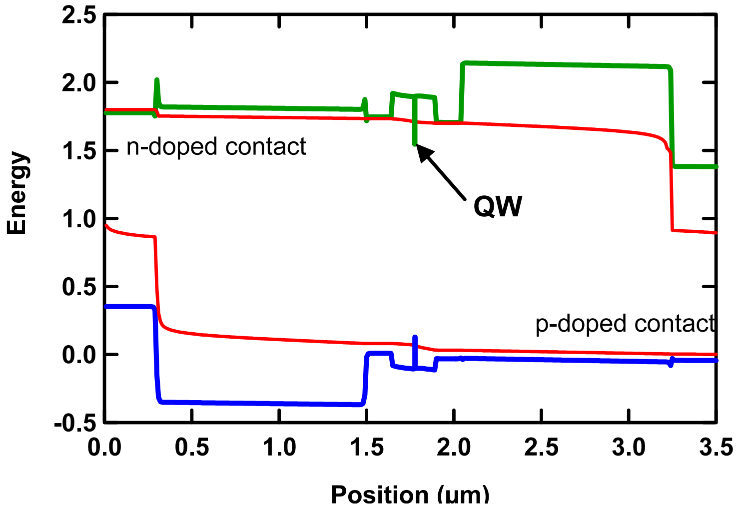


Figure 4: energy band diagrams for the electrically pumped laser at threshold.

According to simulation, the threshold is in the order of 500 A/cm^2, which is not far from the typical specifications of AlGaAs diode laser at the same wavelengths. The expected diode knee voltage around 1.5 V with a reasonable series resistance.

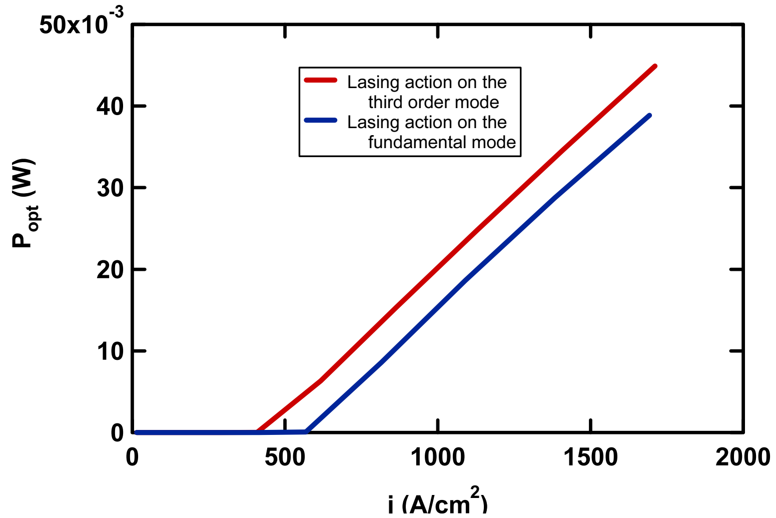


Figure 5: expected P vs I plots for the third order and fundamental mode. The expected threshold is 1.6 V

Sample after growth was technologically processed (photolithography, etching and metals thermal evaporation) to make laser 'ridges' with width in the order of 8 µm and contacts in order to apply current. **Figure 6** shows I-V characteristics measured by applying pulsed current: (a) 1kHz, 5µs and (b) 10 kHz, 3 µs.

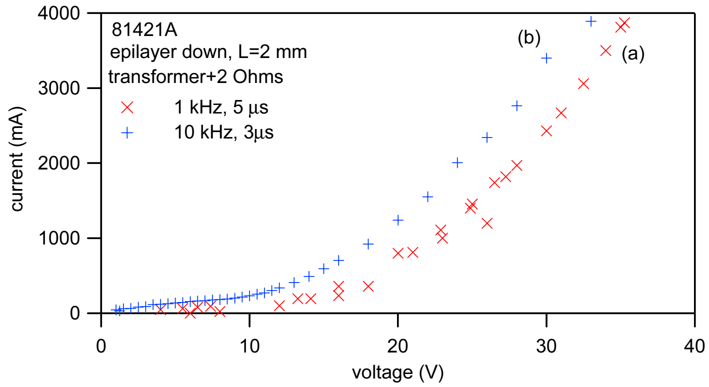


Figure 6: I-V characteristics

Electroluminescence spectra are shown in Figure 2 for several currents between 0.5A and 3.8A, which was the maximum current we could apply.

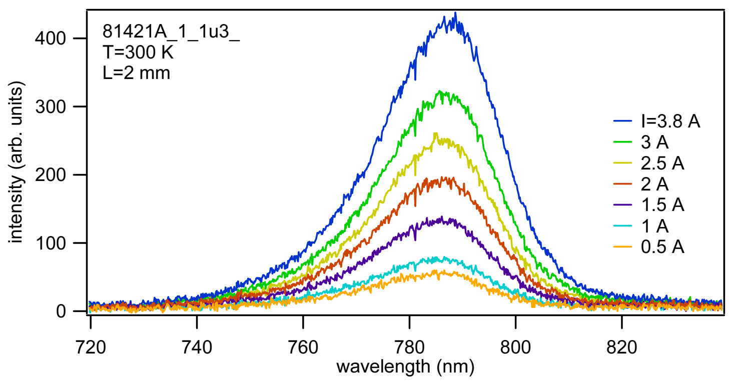


Figure 7: diode electroluminescence.

Preliminary results are not satisfactory at all. The electrically pumped device is severely affected by a huge series resistance. Threshold was not reached despite high voltages (20V) and high currents (4 A) used.
The peak is observed at 786-787 nm very close to the theoretically estimated e1-hh1 transition for the QW (777.50 nm at room temperature).
A huge resistivity was measured through the "p" type cladding, which is of a pseudo alloy type. The non optimal doping of this regions is probably at the origin of the observed blocking behaviour. A new sample based on a true alloy is going to be processed.

Twin photon source based on counterpropagating signal and idler interaction

An original source based on counterpropagating interaction has been proposed. The general analysis of such kind of interaction in waveguides is going to be published in Physics Review Letters [38]. The principle consist in exploiting a non collinear phase matching scheme in waveguides. Despite the weak interaction, this source has the advantage of being extremely simple, and to emit directly pairs of photons in the entangled state. Moreover, the emission has a very narrow linewidth.

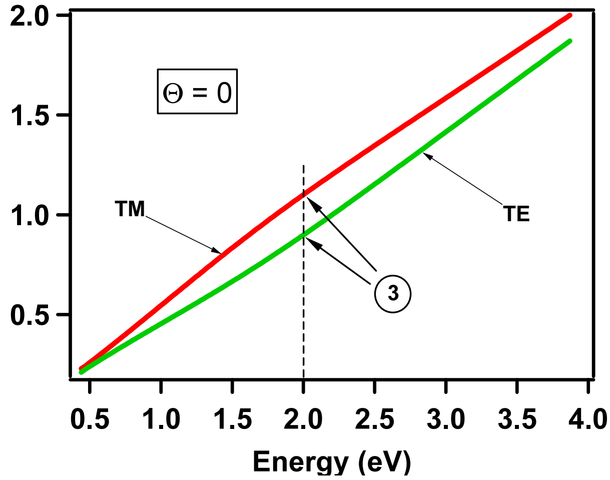


Figure 8: Tuning caracteristic of counterpropagating interaction with the pump perpendicular to the waveguide

A sample based on such interaction was grown and sent to Oxford for experiments.

WP1.2 Generation of arbitrary two-photon states

P03 (EXPUNIVIE) has finalized the construction of the platform for purification of arbitrary mixed states. Currently setting up the Ti:Sa laser and frequency doubling. Furthermore, work on photon statistics measurements on down-converison light from a high-energy pulsed laser. First results imply that on average on the order of 1 photon per pulse is created.

WP1.3 Bright source of entangled multi-photon states

P02 (LMU): Theoretical and experimental work on the entanglement of four-photon states as emitted by parametric down-conversion resulted in the observation of a highly entangled 4-photon state (Fig 1.). The good quality of the entanglement and the high stability of the source together with the multi-conicidence unit developed during year 1 of QuComm allowed elaborate analysis of the properties. The state, which is a superposition of a 4-photon GHZ-state and the product of 2 EPR-states, exhibits high symmetry with respect to observation in different polarisation bases (Fig. 2). The results between the four observers show perfect correlations for specific analysis directions and also a strong violation of a generalised Bell-inequality. This forms the basis fo its use in advanced multi-party quantum communication (see WP3).

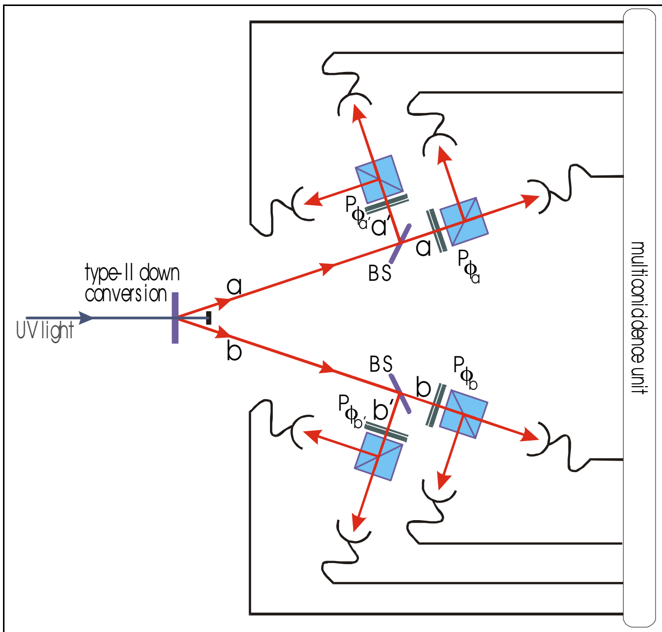


Fig. 1.1: Set-up for the observation of 4-photon polarisation entangled states as produced by parametric down-conversion.

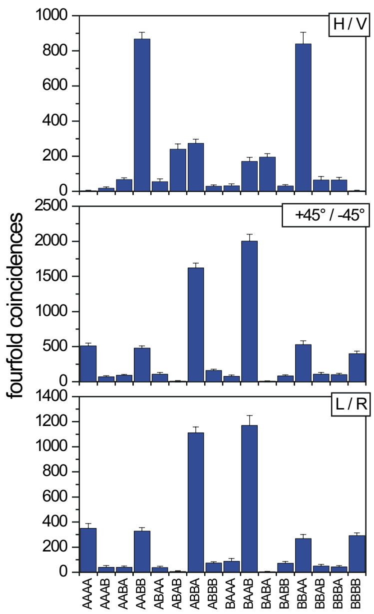


Fig. 1.2: Polarisation analysis of the four-photon state emitted by parametric down-conversion for different orientations of the four analysers.

P03 (EXPUNIVIE): We investigated a possible high intensity source for multi photonic entanglement using the "RegA"-System, a regenerative amplifier, as a pump laser for the down conversion. This laser system provided fs-pulses of several micro joule energy at a repetition rate of 250 kHz, which represent a 300-fold gain of the pulse energy, compared to the Mira systems presently in use.

However, our experimental results showed that this laser system is not useful for generating pure entangled photon pairs. The reason, which is supported by further numerical and theoretical analysis, is that the high pulse energy of the laser leads to a production of too many photon pairs at the same time and drastically reduces the visibility. The reduction of the power of the laser to an acceptable level leads to a net rate of 2-pair production, which is even below that of the (weaker) system currently used.

P04 (OXFORD): Inspired by laser operation, Oxford has addressed the question of whether stimulated emission into polarization entangled modes can be achieved. In [19], the new source is described and the state produced by stimulated emission of the singlet Bell state is analysed in [20]. Such an entangled-photon laser could be a very important tool for studying "mesoscopic quantum entanglement" bridging the gap between discrete and continous variable quantum information.

WP1.4 Synchronisation of independent sources of pulsed parametric down-conversion

P02 (LMU): Synchronization of mode-locked lasers is nowadays a commercial option. Even better stability and synchronicity was achieved in the realm of ultra precise measurements of optical frequencies. Thus, as it turns out, recent developments, both for special applications in optical frequency synthesis and for commercial applications, now supply the tools necessary for future concatenated long-distance quantum communication.

WP2: QUANTUM STATE ANALYSERS

The objective of WP2 is to build the quantum toolbox of efficient and easy-to-use analysers of complex photonic quantum states, notably entangled states. Quantum logic operations with linear optical elements are at the heart of these analysers and will be further developed for applications in other work-packages.

Deliverables

D15 (T0+18): Report on linear quantum logic and quantum error correction (P04, P06)

This has been prepared by **Oxford (P04),** containing work on the Oxford the bit-flip error-rejection scheme, [2], and from the Vienna group concerning the purification paper [14].

Milestones

M11 (T0+18): Quantum tomography performed on arbitrary polarisation quantum states of multiple photons, and on 2-photon states entangled in multiple degrees of freedom (P06)

This milestone has partly been achieved.

M12 (T0+18): Identification of all 4 polarization Bell-states of hyper-entangled states (P02, P06)

This milestone has not been achieved, yet. It was delayed due to work within WP5, which took unexpectedly long time, but recently (Jan. 2002) showed the first successful results.

M13 (T0+18): Linear quantum logic demonstration (P04, P06)

This milestone has been achieved in terms of theoretical proposals, deliverable D15

Further results of year two and research in progress

P03 (EXPUNIVIE) has built more detectors for both teleportation and purification experiments.

The full implications of the schemes, [2] and [26], devised by **P04 (OXFORD)** for error-free quantum state transmission through a noisy channel, rejecting single bit-flip errors and **P03 (EXPUNIVIE)** for entanglement purification of general mixed entangled states, both schemes avoiding the controlled-NOT gate operation and requiring only simple linear optical elements will be further studied.

WP3: ENTANGLEMENT BASED QUANTUM CRYPTOGRAPHY

The objective of WP3 is to demonstrate entanglement-based quantum cryptography protocols, featuring an enhanced security compared to faint-pulse quantum cryptography, and bring the technology from proof-of-principle (i.e., on lab benches, and in spooled optical fibre) to field demonstrations, to be conducted in WP6. Novel protocols, such as secret sharing or multi-mode/state quantum cryptography are also studied in WP5.

Deliverables

D16 (T0+18): Report on free-space entanglement enhanced quantum cryptography (P04, P06, P08)

A report was submitted as D16 at T0+12. This will be taken as the final version

D17 (T0+24): Report on entanglement enhanced quantum cryptography fiber system (P01,P03, P05,P06).

A report was submitted as D17.

Milestones

M14 (T0+12): First lab tests of free-space cryptography using near-infrared entangled photons

This has been realised by LANL and Univ. Illinois, details are given in D20.

P06 (LANL): Los Alamos free-space quantum key distribution over 10-km in daylight and at night.

During the October- December 2001 time period Los Alamos (work led by Richard Hughes) completed a long-distance (10 km) demonstration of free-space QKD, obtaining several hours of data in both daylight and at night on each of several days. Our transportable system uses weak attenuated laser pulses to implement the BB84 QKD protocol with a clock rate of 1 MHz, which is limited by the cryptographic randomizer source of random bits at the transmitter.

For this demonstration the transmitter (Alice) was located on a nearby mountain at an elevation of 2,760 m, and sent the QKD signals to the receiver (Bob) located to the ESE of the transmitter, near to our laboratory, at an elevation of 2,153m. The optical air path distance was 9.81 km.

As an example of our results, on 4 October during full daylight we transmitted 340 million bits with average photon numbers per pulse down to ~ 0.2. From these transmitted bits, 464,309 sifted key bits with a (quantum) bit error rate of 5.5% were generated. After reconciliation and privacy amplification, 186,669 error-free secret key bits were produced that passed both the FIPS 140-1 and 6-bit “Maurer” cryptographic randomness tests. At night, we were able to generate large quantities of key (hundreds of thousands of secret bits) at average photon numbers per pulse of ~ 0.1, with sifted bit rates of ~ 500 Hz and (quantum) bit error rates of ~ 2%.

Using polarization-entangled photons, Los Alamos (work led by Paul Kwiat) have implemented the "six-state" quantum cryptography protocol, whereby each photon is measured in one of *three* bases. See also work done by KTH and GAP in WP5 and [4,9]. This is in contrast with the "standard" BB84 protocol where two bases are used. The resulting eavesdropper-induced error rate, experimentally investigated for several attacks, is enhanced to 33% compared to 25% for BB84. This work also pertains to workpackage 5, and some more details is given in deliverable D20.

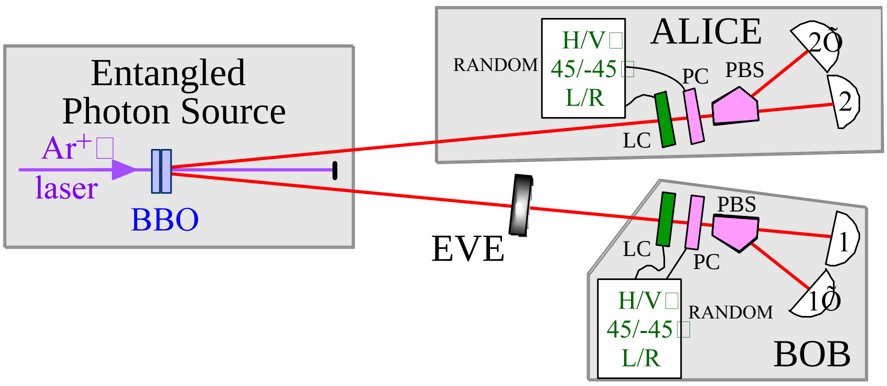


Fig. 1. Experimental setup for implementing the six-state cryptography protocol with polarization-entangled photons.

Since the main benefit of moving to the six-state protocol is an enhancement of the detectability of Eve, a primary goal was to experimentally realize an intervening eavesdropper. Given that one always assumes that Eve has perfect equipment, and in reality we do not, the best one can do is to simulate her presence in as non-invasive a fashion as possible. To this end, we implemented several different eavesdropping strategies. All of these were incoherent attacks (i.e., on each photon individually) of the intercept-resend variety. In these the eavesdropper intercepts a photon traveling to Bob, measures it, and sends on to Bob a photon with a polarization consistent with the measurement result (it obviously only makes things worse to send something other than what was measured).

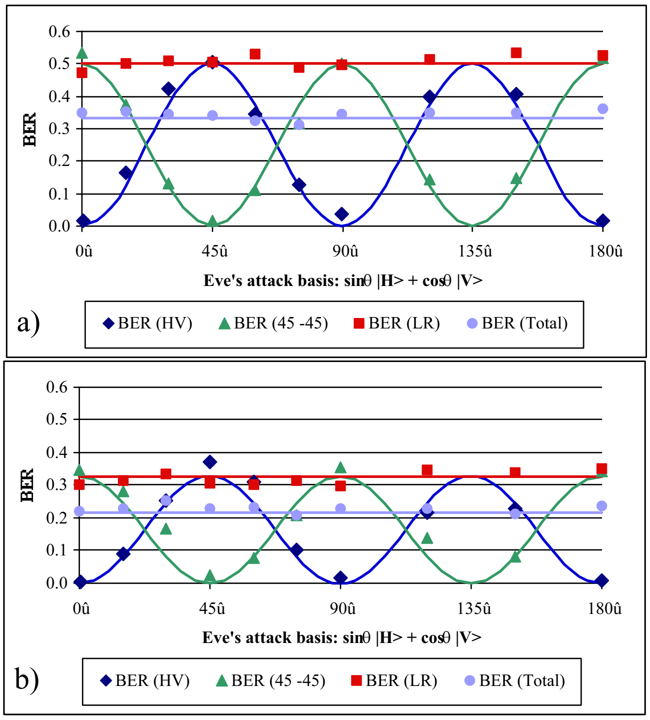


Fig. 2. Effect of an intermediate eavesdropper (measuring in a linear polarization basis) on the induced bit error rates in the various bases, and on the total BER. a). Eve simulated by making a strong measurement of the polarization on every photon. b). A partial quantum non-demolition attack, simulated with a partial decohering element.

The above implementation of the six-state protocol employed photons entangled in polarization. However, this need not have been the case -- one could imagine a system in which Alice sent single photons to Bob with one of six definite polarizations. Nevertheless, it seems that there are potential advantages to be gained by using the photons from parametric down conversion. First, it has been shown that, in comparison to the faint pulse sources actually employed in other experiments, the correlated photons in principle would allow secure key distribution over longer distances [WP3:1]. Second, the entangled photons have the feature that they automatically allow one to test the quality of the source [WP3:2]. Specifically, if photons with definite polarization are sent to Bob, it is conceivable that some other degree of freedom may also serve as a partial label for the polarization state. For example, if the photons with different polarizations originate in different lasers, they may have slightly different frequency spectra; such a difference would in principle allow an eavesdropper to gain free information, i.e., without affecting the BER. In contrast, if there is any information "leakage" to other degrees of freedom with entangled photons, then this will automatically manifest itself in the error rate detected by Alice and Bob. In other words, any attempted eavesdropping on *any* degree of freedom with which the polarization might be coupled will cause noticeable effects on the polarization correlations.

[WP3:1] N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution", Phys. Rev. A **61**, 052304-1-10 (2000).
[WP3:2] D. Mayers and A. Yao, " Quantum cryptography with imperfect apparatus", Proc. of the 39th IEEE Conf. of Found. of Computer Science; also on quant-ph/9809039.

M17 (T0+18): Rapid-switching violation of Bell's inequality over 10km optical fibre. (P03, P05, P06)

This milestone has not been achieved, although there are results, which are connected to this milestone.

The entanglement based quantum cryptography scheme over 8.5 km of optical fiber, reported in [8], corresponds with slightly modified setting parameters at Alice's and Bob's to a rapid switching violation of Bell's inequality. Here, the switching was not determined by an external random number generator, but is implemented using a passive choice. Two different analyzers are connected to each side of the two-photon source by means of a fiber optical coupler. Each photon chooses independently whether to be measured in one or the other analyzer. However, the analyzer settings used in the experiment were chosen in order to distribute a secret key and not to test a Bell inequality. It is known that quantum key distribution using the BB84 protocol is possible only if the noise on the quantum channel is low enough to allow a violation of CHSH Bell inequality [WP4:1,WP4:2].

Beyond, the aim of M17 is to demonstrate a violation of a Bell inequality while closing the locality loophole as has been done by EXPUNIVIE in 1998 over a distance of 360 meters [WP4:3]. Therefore, not only fast switching is required, but also a large distance between Alice's and Bob's analyzers as well as a symmetric setup where the source is roughly in the middle between both parties. The latter contrasts with the chosen asymmetric setup, optimized for quantum cryptography (Alice is directly connected to the source), and the modification of the crypto experiment in order to enable a Bell-test would have required changing the whole setup (wavelength, electronics). We therefore opted to focus only on the cryptographic experiment.

[WP4:1] N. Gisin and B. Huttner. Phys. Lett. A 228, 13 (1997)
[WP4:2] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres. Phys. Rev. A 56, 1163 (1997)
[WP4:3] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger. Phys. Rev. Lett. 81, 5039

M18 (T0+24): Demonstration of symmetric 1550/1550nm quantum cryptography system (P01) and 1300/1300nm system (P06)

This milestone has not been achieved.

Further results of year two and research in progress

P02 (LMU): The new results on multi-photon states (WP1) allow the formulation of novel quantum communication protocols, not foreseen when planning work within QuComm. The four-photon state as produced by parametric down-conversion exhibits strong correlations and high entanglement. Extending the basic scheme of entanglement quantum cryptography, these properties form the main ingredients for a multi-party secret sharing protocol. The signal to noise ratio of a first test was above 10% and thus is not yet sufficient for key exchange, tests with narrow filtering are now planed to improve the characteristics and also to evaluate a possible performance in view of the relative low detection rates of four-photon coincidences.

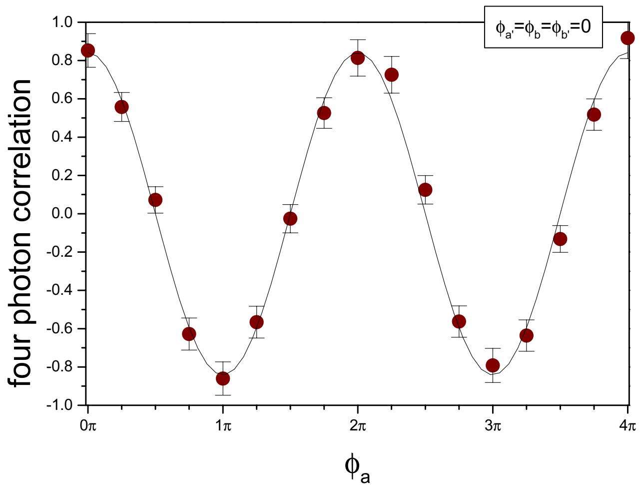


Fig. 3.1: Four-photon correlation when analyzing three outputs at 0° and varying the fourth analysis

Overall, the progress in this work-package has been beyond expectation, and as reported above several entanglement based quantum cryptography experiments were realised. Further work to realise the free space trials, as well as other field trials is ongoing.

WP4: Teleportation of entanglement

The objective of WP4 is to experimentally demonstrate efficient quantum teleportation and quantum information transmission. A special emphasis is put on the teleportation of entangled qubits as a means of distributing entanglement.

Deliverables

D18 (T0+18): Report on high fidelity qubit teleportation (P02,P03,P04,P05).

The report D18 was submitted on time.

Milestones

M19 (T0+12): Violation of Bell's inequality with photons that never interacted to demonstrate high fidelity of qubit teleportation (P03).

A further experiment related to this was achieved by **P03 (EXPUNIVIE).** By the use of fiber optic components, the teleportation fidelity allows the teleportation of an entangled photon with sufficiently high fidelity. Also, GAP is working towards entanglement swapping based on energy-time entanglement.

P03 (EXPUNIVIE) is presently working on the experiment. The necessary components are tested in the lab.

Further results of year two and research in progress

The activities in WP1 by **P02 (LMU)**, **P03 (EXPUNIVIE)**, **P04 (OXFORD),** and **P05 (GAP)** are setting the road towards M20 (T0+30), which will be an extremely challenging combination of only partly known technologies to perform quantum teleportation with unprecedented quality and efficiency. LMU's work on Bell-state analysis in WP2 will lead to higher efficiency, one of the prerequisites to M21.

P03 (EXPUNIVIE) has in WP4 performed an entanglement swapping experiment based on two independent pairs of polarization-entangled photons. The two independent photons were entangled with such high fidelity that a violation of Bell's inequality was shown. For the realization of this experiment several new technologies had to be implemented. The analysis of the photons, such as the Bell-state analysis and the polarization analysis, were performed with fiber optic components, allowing the achievement of better and independent collection alignment of the entangled photons produced by the downconversion, than in previous experiments. In order to enhance the rate of the photons the system generating the UV-laser pulses used for the downconversion was optimized. This was achieved by implementing astigmatic UV beam collimation after the second harmonic generation in order to obtain nearly a Gaussian-shaped beam profile, and focusing the UV-beam sharper into the downconversion crystal. Also, the long-time (24h) stability of the experiment was improved by implementing an active laser beam steering, keeping the UV-laser pulses strictly fixed in reference to the down conversion beam. The increased rate and temporal stability of the system allowed the use of narrower spectral filtering of the photons ($\Delta\lambda$=1nm instead of $\Delta\lambda$=3.5nm), leading to a significant increase of the fidelity of Bell-state analysis and consequently of the teleportation. After the entanglement swapping procedure, the entanglement between the two independent photons had a visibility better than 80%, which is well above the limit required for a violation of Bell's inequality. The experimental test of the CHSH-inequality was performed and gave a Bell-parameter of S=2.46 ±0.9, which clearly violates the classical limit of 2 by more than 4 standard deviations. The results are published in Physical Review Letters on January 7th, 2002 [24].

P03 (EXPUNIVIE) have also successfully demonstrated four-particle entanglement by using two independently created EPR pairs. In this experiment, we were able to observe four-particle entanglement with very high purity, which is an important step for entanglement purification [25].

In **P05 (GAP),** the setup that will be used to implement entanglement swapping with two spatially separated sources using time-bin entangled photons has been completely built (figure 1), including fiber interferometers for 1550 nm, new InGaAs APD's module and a new home made gating electronics for the InGaAs APD. We use the two outputs of a bulk pump interferometer to pump two spatially separated $KNbO_3$ non linear crystals with femtosecond pulses at λ= 710 nm. The down conversion process produces time-bin entangled photons at 1310 and 1550 nm. As a first step, the two sources have been tested independantly. The quality (i.e degree of entanglement and purity) of the Bell states has been characterized with Franson type Bell tests, where photons at 1.3 and 1.5 µm are sent to two different fiber interferometers (analyzers). Interference fringes with visibilities of up to 92 % have been observed for both sources, showing a high quality of entanglement [35]. The spectral distributions have also been measured.

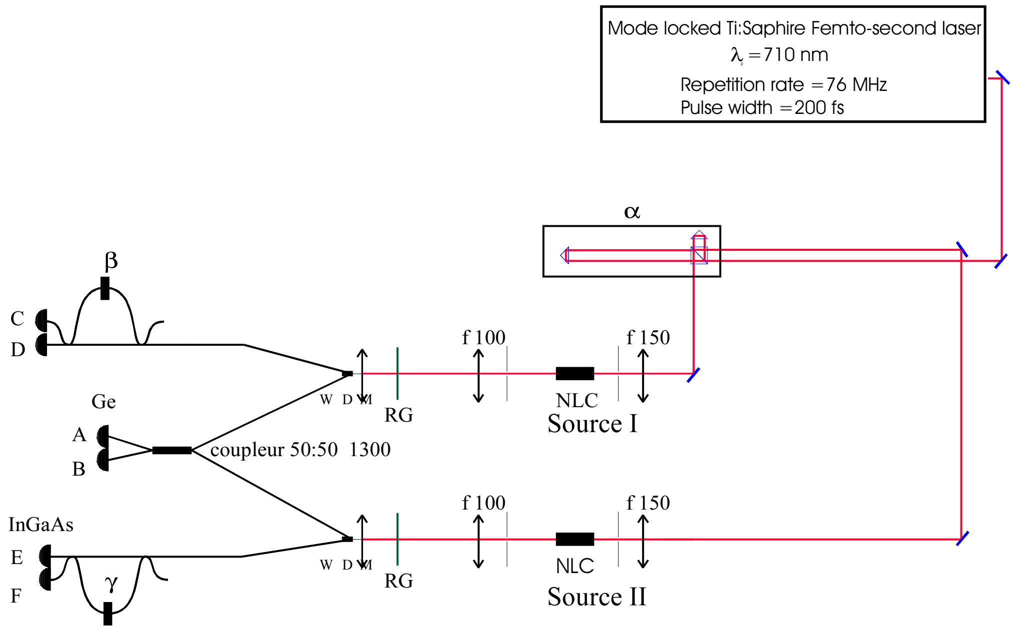


Figure 1 : Experimental setup for the implementation of entanglement swapping with spatially separated sources using time-bin entangled photons at telecom wavelength.

The measurements with the two spatially separated sources have started November- Dec. 2001 . We first detected coincidences between photons coming from different sources. Then the alignement was done so that two photons from different sources (photon at 1310 nm from each source) overlap exactly at the same time at a beam splitter. When varying the delay of one photon, we observe a decrease in the coincidence rate at zero delay (Mandel dip). If we record only 2-fold coincidences (2 detectors after the beam splitter), the visibility of this dip is theoretically limited to 50 %, because in this case we can not discard events where 2 pairs are created in the same crystal. We obtained experimentally a visibility of 45 % (figure 2). The way to recover 100 % visibility is to post-select events where one pair is created at the same time in the two crystals by detecting the four photons (4-fold coincidence). First observations of 4-fold coincidences with 1310-1550 nm photons pairs have been made.

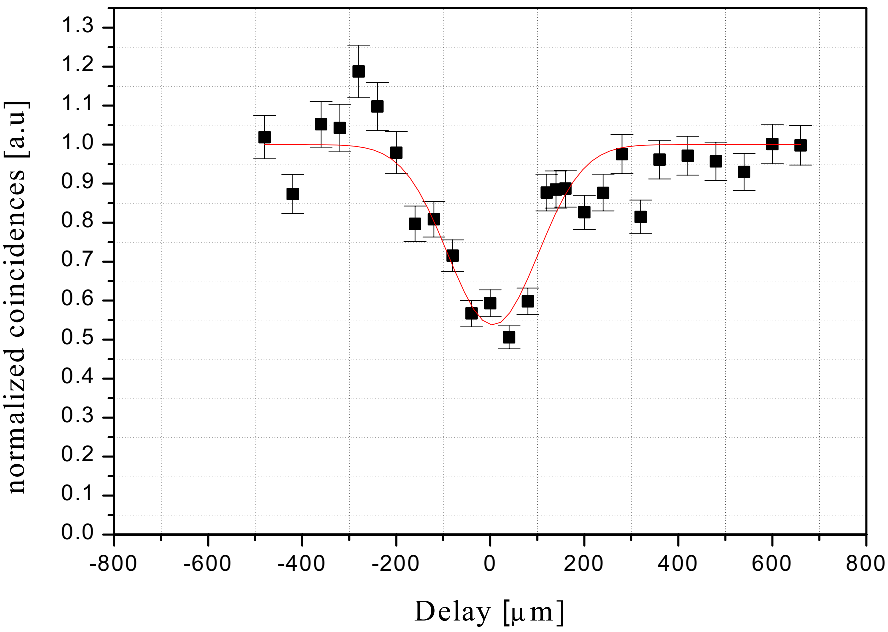


Figure 2: *Normalized 2-fold coincidences count rate as a function of the delay of one photon. The normalization is made with the product of single count rate at the 2 detectors. The FWHM is ~230 μm and the visibility is 45 %. The solid line is a gaussian fit.*

WP5 : Multi-mode & multi-state quantum communication

The objectives of **WP 5** are to devise and to demonstrate novel protocols for quantum communication, using multi-dimensional or multi-mode entangled states. This topic was virtually unexplored at the starting time of the QuComm project and no experiments had been reported before. Although milestone **M21 (T0+12)** has not been achieved yet, the progress in this work-package has been very good, and new results in theory as well as in experiment have been obtained and published or submitted to scientific journals. The demonstration of quantum secret sharing (milestone **M23 (T0+24)**) has been realised by **P05** (**GAP**) and published in Phys.Rev. A. One future milestone has already been realised, scheduled for T0+30. This is the demonstration of entanglement purification **M24 (T0+30)** by a collaboration of **P05 (GAP)** and **P06 (LANL)** + proposals of **P03 (EXPUIVIE)**. The collaboration between different nodes has been good, and joint experiments as well as common theoretical investigations can be reported.

Deliverables

D20 (T0+18): Report on multimode, multiparticle entanglement protocols (P01,P03,P04, P05,P06)

This report (handed in at T0+18) summarises the ongoing work in QuComm on the demonstration of novel quantum communication protocols, in particular multi-party protocols or protocols which use more than 2-states (or more than one qubit). Such new protocols will extend the capabilities of quantum communication by increasing the channel capacity, by making the systems less sensitive to channel noise. Examples of such protocols include multi-party quantum cryptography (using qutrits and systems with higher Hilbert-space dimension), encoding more than one qubit per photon, and the "entangled-photon laser".

Milestones

M21 (T0+12): Experimental demonstration of a quantum dense coding system which enhances the transmission capacity of a noisy channel (WP5.1; P02)

This milestone has not been achieved.

Lots of detector developments have been done and first tests of fibre bell-state analysis have already been realized. However, lack of man-power and delays with the other developments resulted in the hold-up of this milestone.

M22 (T0+18): Experimental demonstration of Quantum Zeno effect error correction system on a noisy quantum channel. (P02,P04)

This milestone has not yet been achieved

M23 (T0+24) Experimental demonstration quantum cryptography system between three parties

This milestone has been achieved by **P05(GAP)** in [1]

Further results of year two and research in progress

P02 (LMU) started to build tools for general polarisation measurement of single photons in order to enable new protocols for quantum cryptography. According to proposals by Vaidman, Aharonov and Albert, **P02 (LMU)** is going to demonstrate the feasibility of determining the results of possible non-commuting spin-observables by multi-mode entangled state analysis. Parts of the setup have already been tested, demonstrating good performance.

P03 (EXPUNIVIE) has been working on entanglement purification and on the entanglement of the angular orbital momentum states of photons

Entanglement purification is essential for long-distance quantum communication over noisy channels. Usually, entanglement purification is based on cnot-operations, which is difficult to implement experimentally. This year, we were able to find a theoretical scheme which is based on simple polarizing beam splitters [26]. We are now working on the experimental realization using a new technique to stabilize the experimental setup, which includes a stable platform, temperature control and beam monitoring.

We have been working on a theoretical scheme to realize a cnot-gate completely based on linear optics. Experimental realization is planned for next year. [27]

P03 (EXPUNIVIE) has further been working on the entanglement of the angular orbital momentum states of photons .There are two ways of generalizing the usual two particle two-dimensional entanglement. This can be done by involving more than two particles producing multi-particle entanglement or by creating higher-dimensional entanglement by making use of particles with multi-level states.

We focused on the latter and showed an experimental realization of a three-dimensional entangled state. This was done by making use of orbital angular momentum entangled states of photons, which were created in a type-I down-conversion crystal. First, we showed that the orbital angular momentum is conserved in the down-conversion process [28]. In a second step, by developing a method for creating and analysing superposition states of orbital angular momentum [29], we showed that the correlation between the two down-converted photons goes beyond classical correlation.

In a recent experiment we were able to prove the entanglement of a 3 dimensional orbital angular momentum entangled state by violating a corresponding CHSH type Bell's inequality. The results achieved in this experiment yielded to a violation of more than 18 standard deviations. This might be seen as a hint that higher dimensional entangled states are more resistant against noise. As a consequence, such states would be of great importance in all fields of quantum communication.

P05 (GAP) is preparing an experiment to investigate the impact of distance on non-maximally entangled energy-time Bell states. This experiment has been delayed, as the PPLN waveguide used for the creation of photon pairs was used in another experiment. **GAP** also started to work on the extension of time-bin qubits to higher dimension (qutrits). This extension involves the realisation of multi-branch interferometers. The construction of a 3-branch fiber interferometer has started.

WP6 : Field demonstrations

The objective WP6 is to bring together the accumulated know-how developed in WP1-WP5, and to use the technology demonstrated to conduct field trials of quantum communication protocols. Although the field experiments are planned to start first at T0 + 18, the various devices are currently being developed at a laboratory stage by the partners, and considerable work towards field tests are ongoing.

Deliverables

There are no deliverables due this reporting period.

Milestones

There are no milestones to be met this reporting period.

Further results of year two and research in progress

- **P03 (EXPUNIVIE)** is working on long distance teleportation: The hardware is being developed, such as the polarisation control scheme, source design, detectors, registration electronics and a microwave based classical channel. Further, the labs at the field site are presently being adopted for the teleportation experiment.
- **P04 (OXFORD)** and **P08 (DERA)** are making preliminary investigation of potential 1.2km and 1.9km free space trial sites in conjunction with EQCSPOT and QuComm. Experiments at DERA will be conducted before christmas 2001.
- The LANL **P06** free-space cryptography project published a paper demonstrating quantum key distribution over 1 mile horizontal distance. While not entanglement-based per se, the same optical difficulties (e.g., turbulence, background, etc.) will face any system attempting long-distance entanglement distribution, and therefore this result is an important proof of principle.

World-wide state of the art

At present nearly all the leading groups in the field of optical entanglement physics are in the QuComm consortium. Other physical realisations of entangled systems (ion traps, solid-state systems) are still at a much earlier stage of development, and most of them are – from the present point of view – not well suited for quantum communication purposes.

If we analyse the world-wide state-of-the-art in quantum communication, we find that most groups working on quantum cryptography still puts most emphasis on faint pulse systems. Several members of QuComm are also members of EQCSPOT, and outside EQCSPOT, excellent work is being done for instance within the EQUIS consortium, and in Europe notably in Norway, Denmark and France. Outside Europe, there is substantial ongoing work on quantum cryptography, notably in USA at IBM, MagiQ technologies, MITRE and BBN technologies, and most recently also in Japan in various labs.

Recently, EXPUNIVIE, together with an industrial research center (ARCS), has started to work towards an entanglement based quantum cryptography test system. Other members of QuComm might collaborate in the future.

Quantum information processing using light and linear optics has recently attracted a lot of attention. In a paper in Nature, Knill, Laflamme and Milburn have suggested that efficient quantum computing may be possible using only single-photon sources and linear optical elements. A first simple demonstration experiment in this context was recently performed by Pittman, Jacobs and Franson. The spirit of this work is similar to that of work within QuComm on realizing entanglement purification and error correction using linear optics only. Linear optics entanglement purification was also studied by a Japanese group (Koashi and Imoto).

Concerning entanglement manipulations and entangled state cryptography, there are not so many labs outside QuComm that are active experimentally in the area. In Europe, very interesting work has been done in the ATHESIT project headed by University of Rome (La Sapenzia), for instance on quantum teleportation. Very good work is also done e.g. at Maryland University, for instance in the recent teleportation experiment by Shi et al (quant-ph/0010046) showing how to do a complete (however, still very unefficient) Bell measurement. Excellent work is done also by the Quantum Imaging lab at Boston University, but most of their work does not overlap with QuComm activities.

On the technology side, however, there are some very interesting developments that we within QuComm must follow closely. On the long wavelength detector side, at the moment almost all groups have converged on using EPITAXX detectors (UNIPHASE), see [7,31]. While on one hand they do offer excellent performance, it is still not a very good situation to be dependent on a single manufacturer.

Appendix 1: Publications of Year two

Journal publications

1. W. Tittel, H. Zbinden, N. Gisin, *Experimental demonstration of quantum secret sharing*, Phys. Rev. A 63, 042301 (2001). Preprint quant-ph/9912035.
2. D. Bouwmeester, *Bit-flip-error rejection in optical quantum communication*, Phys. Rev. A 63, 040301(R) (2001). Preprint quant-ph/0006108.
3. P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, *Experimental entanglement distillation and 'hidden' non-locality*, Nature 409, 1014 (2001).
4. M. Bourennane, A. Karlsson and G. Björk, *Quantum key distribution using multilevel encoding*, Phys. Rev. A 64, 012306 (2001).
5. I. Ghiu, M. Bourennane, and A. Karlsson, *Entanglement-assisted local transformations between inequivalent classes of three-particle entangled states*, Phys. Lett. A 287, 12 (2001).
6. R. Asplund, G. Björk and M. Bourennane, *An expectation value expansion of Hermitian operators in a discrete Hilbert space*, J. Opt. B 3, 163 (2001). Preprint quant-ph/0011037.
7. M. Bourennane, A. Karlsson, J. Peña Císcar, and M. Mathes, *Single photon counters in the telecom wavelength region of 1550 nm for quantum information processing*, J. Mod. Opt., vol. 48, no. 13 - Special Issue on Technologies for Quantum Communications, pp. 1983-1995, 2001.
8. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, *Long-distance entanglement-based quantum key distribution*, Phys. Rev. A 63, 012309 (2001). Preprint quant-ph/0008039.
9. M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, *Quantum key distribution using multilevel encoding: security analysis*, quant-ph/0106049.
10. B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, *Universal unitary gate for single-photon 2-qubit states*, Phys. Rev. A 63, 032303 (2001).
11. Ch. Kurtsiefer, M. Oberparleiter, H. Weinfurter, *High-efficiency entangled photon pair collection in type-II parametric fluorescence*, Phys. Rev. A 64, 023802 (2001).
12. A. Beige, B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, *Cryptography with single-photon two-qubit states*, submitted to PRL.
13. C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, *Generation of correlated photon pairs in type-II parametric down conversion -- revisited*, submitted to J. of Mod. Opt.
14. M. Bourennane, *Long-Wavelength Quantum Cryptography, Single-Photon Detection and Quantum Entanglement Applications*, Ph.D. thesis, KTH, May 28, 2001.
15. Thomas Jennewein, Gregor Weihs, Anton Zeilinger, *Schrödingers Geheimnisse*, c't, No. 6/2001.

16. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum Cryptography*, quant-ph/0101098, accepted for publication in Rev. Mod. Phys.

17. R. J. Hughes et al., *Quantum key distribution in daylight*, Los Alamos report LA-UR-01-1535 (2001). Abstract submitted to "XV International Conference on Laser Spectroscopy" June 10-15, 2001, Snowbird, UT.

18. A. Lamas-Linares, C. Mikkelsen, J. C. Howell, D. Bouwmeester, *Interference enhanced entanglement: concept of an entangled photon laser*, submitted to PRL.

19. John C. Howell, Antia Lamas-Linares, Dik Bouwmeester, *Experimental violation of a spin-1 Bell inequality using maximally-entangled four-photon states*, quant-ph/0105132.

20. Gabriel A. Durkin, Christoph Simon, Dik Bouwmeester, *Multi-Photon Entanglement Concentration and Quantum Cryptography*, quant-ph/0109132.

21. Christoph Simon, Julia Kempe, *Robustness of Multi-Party Entanglement*, quant-ph/0109102.

22. Caslav Brukner, Jian-Wei Pan, Christoph Simon, Gregor Weihs, Anton Zeilinger, *Probabilistic Instantaneous Quantum Computation*, quant-ph/0109022.

23. Christoph Simon, Jian-Wei Pan, *Polarization Entanglement Purification using Spatial Entanglement*, quant-ph/0108063.

24. Jennewein, G. Weihs, J.-W. Pan, A. Zeilinger. *An experimental proof of nonlocality for Teleportation and Entanglement Swapping,* Phys. Rev. Lett. 88, (2002).

25. J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs and A. Zeilinger, *Experimental demonstration of four-photon entanglement and high-fidelity teleportation*, Phys. Rev. Lett. 86, 4435 (2001).

26. J.-W. Pan, C. Simon, C. Brukner and A. Zeilinger, *Entanglement purification for quantum communication*, Nature (London) 410, 1067 (2001).

27. T. Rudolph and J.-W. Pan, *A simple gate for linear optics quantum computing*, Quant-ph/0108056.

28. A. Mair, A. Vaziri, G. Weihs and A. Zeilinger,. *Entanglement of the orbital angular momentum states of photons*, Nature 412, 313 (2001).

29. A. Vaziri, G. Weihs and A. Zeilinger, *Superpositions of the Orbital Angular Momentum for Applications in Quantum Experiments,* quant-ph/0111033 (to appear in Journal of Optics B)

30. Wolfgang Tittel, Gregor Weihs, *Photonic entanglement for fundamental tests and quantum communication*, Quantum Information and Computation, vol. 1, no. 2, pp. 3-56 (2001).

31. D. Stücki, G. Ribordy, A. Stefanov, H. Zbinden, J.G. Rarity, T. Wall, *Photon counting for QKD with Peltier Cooled InGaAs/InP APD's*, to appear in Journal of Modern Optics, , J.Mod.Opt **48,** n°13 1967-1981 (2001)

32. S. Tanzilli, H. de Riedmatten ,W. Tittel, H. Zbinden, P. Baldi, M. de Micheli, D.B. Ostrowsky, N. Gisin, *Highly efficient photon–pair source using PPLN waveguide*, Electr. Lett. , **37** p28 (2001)

33. H. Zbinden, N. Gisin, G. Ribordy, D. Stücki, W. Tittel, *Experimental quantum communication*, to appear in the proceedings of the International School of Physics Enrico Fermi, Varenna, July 17-27, 2001.

34. S. Tanzilli, W. Tittel, H. de Riedmatten, H. Zbinden, P. Baldi, M. de Micheli, D.B. Ostrowsky, N. Gisin , *PPLN waveguide for Quantum Communication*, quant-ph/0107125, to be published in European Physical Journal D (special issue of the Quick conference).

35. I. Marcikic, H de Riedmatten, W. Tittel, H. Zbinden, N. Gisin, *Femtosecond time-bin entangled qubits for robust quantum communication,* to be submitted.

36. N. G. Semaltianos, B. Vinter, A. De Rossi, V. Berger, and V. Ortiz, *"Photoluminescence of a third order mode optically pumped semiconductor laser structure",* submitted to Applied Physics Letters.

37. A. De Rossi, N. G. Semaltianos, , V. Berger, E. Chiralis, B. Vinter, and V. Ortiz, *"Third order mode optically pumped semiconductor laser",* submitted to Applied Physics Letters.

38. A. De Rossi, V. Berger, *"Counterpropagating twin photons by parametric fluorescence",* to be published in Physics Review Letters.

39. N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin *"Security of quantum key distribution using d-level systems",* accepted for publication in Phys. Rev. Lett., also at http://arXiv.org/abs/quant-ph/0107130

40. A. Karlsson, M. Bourennane, D. Ljunggren, J. Peña Císcar, M. Mathes and A. Hening, *Quantum communication and single-photon technologies*, **Proc. SPIE**, vol. 4430 - ROMOPTO 2000: Sixth Conference on Optics (edited by V. I. Vlad), pp. 430-441, 2001.

41. M. Bourennane, A. Karlsson and G. Björk, *Quantum Key Distribution Using Multilevel Encoding*, pp. 295-298 in **Quantum Communication, Computing, and Measurement 3**, eds. P. Tombesi and O. Hirota, Plenum, New York, 2001.

42. D. Ljunggren, M. Bourennane and A. Karlsson, *Authority-Based User Authentication and Quantum Key Distribution*, pp. 299-302 in **Quantum Communication, Computing, and Measurement 3**, eds. P. Tombesi and O. Hirota, Plenum, New York, 2001.

Conferences

1. I. Ghiu, M. Bourennane and A. Karlsson, *Transformations between inequivalent classes of three-particle engtangled states*, poster at **Quantum Entanglement and Quantum Information (QuEnt)**, in Les Houches, France, March 19-30, 2001.

2. A. Karlsson, M. Bourennane and D. Ljunggren, *Long wavelength quantum cryptography: A discussion on some issues*, oral presentation SuM2 at **Quantum interference and cryptographic keys: novel physics and advancing technologies (QUICK)**, Cargèse, Corsica, France, April 7-13, 2001.
3. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and H. Zbinden, *A quantum key distribution with N-array encoding*, poster M5 at **Quantum interference and cryptographic keys: novel physics and advancing technologies (QUICK)**, Cargèse, Corsica, France, April 7-13, 2001.
4. A. Karlsson, *Technologies for Quantum Communication*, invited talk at **Workshop on (Not Only) Solid State Quantum Computing**, Warsaw, Poland, April 26-29, 2001.
5. A. Karlsson, M. Bourennane, D. Ljunggren, I. Ghiu and R. Viana Ramos, *Long wavelength quantum cryptography and entanglement manipulations*, invited talk QECCB2 at **International Conference on Quantum Information (ICQI)**, Rochester, New York, USA, June 10-13, 2001.
6. A. Karlsson, *Technologies for Quantum Communication*, oral presentation at **4th QNANO Workshop**, Nässlingen, Sweden, June 13-15, 2001.
7. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and N. J. Cerf, *Quantum key distribution using multilevel encoding: Security analysis*, poster at **2nd ESF QIT Conference - Quantum Information Theory and Quantum Computing**, Gdansk, Poland, July 10-18, 2001.
8. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and N. J. Cerf, *Quantum key distribution using multilevel encoding: Security analysis*, poster at **2nd ESF QIT Conference - Quantum Information Theory and Quantum Computing**, Gdansk, Poland, July 10-18, 2001.
9. M. Bourennane, A. Karlsson, M. Mathes and J. Peña Císcar, *Single Photon Counters in the Telecom Wavelength Region of 1550nm for Quantum Information Applications*, oral presentation WG2-2 at **CLEO/Pacific Rim 2001**, Chiba, Japan, July 15-19, 2001. .
10. A. Karlsson, *From quantum encryption to teleportation; an introduction to quantum communication with possible applications*, invited tutorial Th.M.3.1. at **27th European Conference on Optical Communication (ECOC'01)**, Amsterdam, Sept 30-Oct 4, 2001.
11. R. Viana Ramos, *Numerical Analysis of Eavesdropping Attacks in Quantum Cryptographic Systems using MATLAB*, oral presentation at **Nordic MATLAB conference**, Oslo, Norway, Oct 17-18, 2001.
12. A. Karlsson, *Entanglement manipulations and quantum communication*, oral presentation at **XXII International Solvay Conference in Physics - The Physics of Communication**, Delphi and Lamia, Greece, Nov 24-30, 2001
13. H. Weinfurter, *Falsification of Noncontextual Hidden Variable Theories*, Int. Workshop FRISNO X, Les Houches, France, 31.1.-3.2.2000.
14. H. Weinfurter, *Quantum Communication*, The IEEE-Symposium on Circuits and Systems, ISCAS 2000, Geneva, Switzerland, 28.5.-31.5.2000.
15. H. Weinfurter, *Recent developments in Quantum Communication*, Workshop on Quantum Information Processing - Theory and Experiment, Benasque, Spain, 2.7. - 7.7.2000.
16. H. Weinfurter, *Quantenkryptographie; Quantenteleportation*, Tutorials, Summerschool on Quantuminformation of the German Physical Society, Bad Honnef, Germany, 9.10. - 13.10.2000.
17. H. Weinfurter, *Quantum Cryptography and Teleportation*, Rank Prize Symposium on 'Application of low light level technologies', Grasmere, UK, 16.10. - 19.10.2000.

18. T. Jennewein, J.W. Pan, G. Weihs, A. Zeilinger: *Experimental Nonlocality proof for Entanglement Swapping*, poster, WE-Heraeus-Seminar Exploring Quantum Physics, Venice (Italy), 18. – 23. August 2001.
19. T. Jennewein, G. Weihs, A. Zeilinger. *An all-fiber Bell State Analyzer*, poster, CARGESE CORSICA April 7-13, 2001
20. A. Vaziri, *Verschränkung von Photonenzustände mit Bahndrehimpuls*, invited lecture, Ludwig Maximiliam Universität, Munich, Germany, March 2001.
21. A. Vaziri, G. Weihs, A. Mair and A. Zeilinger, *Entanglement and Superpositions of Photon States with Orbital Angular Momentum*, poster, Ecole de physique, Les Houches, France, March 2001.
22. A. Vaziri, G. Weihs, A. Mair and A. Zeilinger, *Entanglement of Photon States with Phase Singularities*, poster, CLEO/Europe-EQEC Focus Meeting 2001, Munich, Germany, June 2001.
23. A. Vaziri, G. Weihs, A. Mair and A. Zeilinger, *Entanglement of Photon States with Phase Singularities*, poster, 259. WE-Heraeus-Seminar Exploring Quantum Physics, Venice, Italy, August 2001.
24. A. Vaziri, G. Weihs and A. Zeilinger, *Entanglement and Quantum Superposition of the Orbital Angular Momentum of Photons*, poster, Quantum Optics EuroConference 2001 San Feliu de Guixols, Spain, October 2001.
25. G. Weihs, *Introduction to photonic entanglement*, Invited Tutorial,Seminaire Rhodanien, Dolomieu, France, February 2001.
26. G. Weihs, Photonic entanglement, *Bell's inequality and GHZ*, Invited Lecture, Les Houches Winter School, Les Houches, France, March 2001.
27. G. Weihs, Quantenkryptographie, Tuturial Lecture, Cryptology Seminar, St. Pölten, Austria, April 2001.
28. G. Weihs, *Photonic entanglement for quantum communication*, Physics/Applied Physics Colloquium, Stanford University, Palo Alto, USA, May 2001.
29. G. Weihs, *High-fidelity entanglement swapping*, Institut for theoretical Physics and Astrophysics, Gdansk, Poland, June 2001.
30. G. Weihs, *Photonic quantum communication*, Invited Talk, ERATO Quantum Computation and Information Project, Tokio, Japan, July 2001.
31. G. Weihs, *Higher photonic entanglements*, ISQM-Tokyo, Japan, August 2001.
32. G. Weihs, *Entanglement of the orbital angular momentum states of photons*, Invited Talk, International Symposium on Quantum Information, Tunxi, China, September 2001.
33. A. Zeilinger, *Information in der Quantenwelt*, Werner Heisenberg Vorlesung, Carl Friedrich von Siemens Stiftung, Munich, Germany, January17, 2001.
34. A. Zeilinger, *Quantum Physics: Finding Answers to Scientific Puzzles*, Forum Fellow at the Annual Meeting, World Economic Forum, Davos, Switzerland, January 25-30, 2001.
35. A. Zeilinger, *Quanteninformation - ein neues Konzept zur Informationsverarbeitung und Informationsübertragung*, Lecture at Siemens AG, Munich, Germany, February 19, 2001.
36. A. Zeilinger, *Quantum Experiments and the Foundations of Physics*, Distinguished Lectureship, Brookhaven National Laboratory (BNL), Islip, New York, U.S.A., February 28, 2001.
37. A. Zeilinger, *Quanteninformation und die Grundlage der Quantenmechanik*, Lecture, Nordrhein-Westfälische Akademie der Wissenschaften, Germany, April 4, 2001.
38. A. Zeilinger, *Was Quanten alles können: Von der Philosophie zu einer neuen Technologie*, Public Evening Lecture at the International Workshop on Coherent Evolution in Noisy Environments, Dresden, Germany, May 22-25, 2001.

39. A. Zeilinger, *Quantenphysik und Information*, Keplervorlesung, Tübingen, Germany, July 11, 2001.
40. A. Zeilinger, *Information and Quantum Mechanics Gordon Conference on Quantum Control of Atomic and Molecular Motion*, Mount Holyoke College, Boston, Mass., USA, July 29 – August 3, 2001.
41. A. Zeilinger, Q*uantum Entanglement, Classical Information and Physical Reality*, XXII International Solvay Conference in Physics on The Physics of Communication, Lamia and Delphi, Greece, November 24-30, 2001.
42. A. Zeilinger, *Quantum Interference, Uncertainty and Complementary in Experiments*, Heisenberg-Symposium, Ludwig Maximilians-Universität, Munich, Germany, December 5-7, 2001.
43. A. Zeilinger, *Classical Information, Quantum Entanglement and Photonic Communication,* Fondation Hugot du Collège de France, Paris, France, December 13-16, 2001.
44. Hugo Zbinden, *Experimental quantum Key Distribution*, 10th International Laser Physics Workshop, Moscow, Russia, July 3-7, 2001.
45. Hugo Zbinden, *Experimental quantum Communication*, International School of Physics Enrico Fermi, Varenna, Italy, July 17-27, 2001.
46. Hugo Zbinden, *Quantum Communication and computing*, NKT summer school, Copenhagen, Denmark, Aug 19-25, 2001.
47. N. Gisin, *Entanglement in relativistic configurations: theory and experiments*, Workshop on quantum information and space-time structure, Madrid, Spain, Sept 5, 2001.
48. N. Gisin, *Entanglement in relativistic configurations: theory and experiments*, invited talk at 10th conference on the foundations of quantum physics, Belfast, Northern Ireland, UK, Sept 11, 2001. .
49. H. ZBINDEN, "Cryptographie Quantique", at *Neuvième Séminaire Rhodanien de Physique, « Physique des états enchevêtrées »* in Dolomieu-France, February 25-March 3, 2001.
50. STEFANOV, "Quantum Cryptography", at *9. SSOM Fachkurs "Optical Communication"* in Engelberg/Switzerland, March 25 – 29, 2001.
51. N. GISIN, *"Quantum cryptography: from basic physics to applications",* at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
52. H. ZBINDEN, *"Faint laser versus entangled photons Quantum Key Distribution"*, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
53. W. TITTEL, *"Time-bin entangled photon pairs & applications in quantum cryptography",* at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
54. S. TANZILLI, *"Highly efficient photon-pair source using PPLN waveguide",* at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
55. STEFANOV ET AL., *"Plug & Play long distance quantum key distribution prototype",* poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
56. S. TANZILLI ET AL., *"Highly efficient photon-pair source using PPLN waveguide",* poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
57. N. GISIN at CLEO/EQELS: "Quantum Key Distribution : Faint laser pulses vs. entangled Photons", invited talk, May 10.
58. N. GISIN at CERN: *"Quantum Key Distribution : Faint laser pulses vs. entangled photons",* invited talk within the OPAL-project meeting, June 13.
59. H. ZBINDEN et al. at CLEO-Europe, *"Experimental Quantum Cryptography",* June 20st, 2001
60. I.MARCIKIC, H.de RIEDMATTEN, W.TITTEL, H.ZBINDEN and N.GISIN, *Femtosecond time bin entangled qubits for quantum communication*, poster at the QIPC Workshop, October 28-31, Torino, Italy

61. H.de RIEDMATTEN, I.MARCIKIC, W.TITTEL, H.ZBINDEN and N.GISIN, *Towards long distance entanglement swapping using time-bin entangled qubits*, poster at the QIPC Workshop, October 28-31, Torino, Italy

Appendix 2- Deliverables Table

Accumulated DELIVERABLES TABLE (in BF are due reporting period 2)

Project Number: *IST-1999-10033*

Project Acronym: **QuComm**

Title: ***Long Distance Photonic Quantum Communication***

Del. No.	Revision	Title	Type[1]	Classification[2]	Due Date	Issue Date
D1	**Final**	Popular Project Presentation	O	Pub	T0+3	T0+2
D2	**Final**	Startup of Project Internet Site	O	Pub	T0+3	T0+1
D3	**Final**	Dissemination and use plan	R	Pub	T0+6	T0+6
D4	**Final**	Half year progress report for first year	R	Pub	T0+6	T0+6
D5	**Final**	First year annual report	R	Pub	T0+12	T0+12
D6	**Final**	Joint IST FET workshop	W	Pub	**T0+18**	**T0+18**
D7	**Final**	Half year progress report year 2	R	Pub	**T0+18**	**T0+18**
D8	**Final**	Second year annual report	R	Pub	**T0+24**	**T0+24**
D11	**Final**	Report on diode laser pumped non-linear crystal source for entangled states	R	Pub	**T0+18**	**T0+18**
D12	**Not yet**	Prototype integrated GaAs laser photon pair source	P	Int	**T0+24**	**T0+30**
D13	**Final**	Report on synchronisation of separate pair-photon sources	R	Pub	**T0+24**	**T0+24**
D14	**Final**	Report on complete Bell -state characterisation	R	Pub	T0+12	T0+12

D15	**Final**	Report on linear quantum logic and quantum error correction	R	Pub	**T0+18**	**T0+18**
D16	**Final**	Report on free-space entanglement enhanced quantum cryptography	R	Int	T0+12	T0+12
D17	**Final**	Report on entanglement enhanced quantum cryptography fiber system	R	Int	**T0+24**	**T0+24**
D18	**Final**	Report on high fidelity qubit teleportation	R	Pub	**T0+18**	**T0+18**
D20	**Final**	Report on multimode, multiparticle entanglement protocols	R	Pub	**T0+18**	**T0+18**

1 *R: Report; D: Demonstrator; S: Software; W: Workshop; O: Other – Specify in footnote*

2 *Int.: Internal circulation within project (and Commission Project Officer + reviewers if requested)*
Rest.: Restricted circulation list (specify in footnote) and Commission SO + reviewers only
IST: Circulation within IST Program participants
FP5: Circulation within Framework Program participants, Pub.: Public document

Appendix 3 – Deliverable Summary Sheets of Year 2

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Joint IST FET workshop

Deliverable N°: D6

Due date: T0+18

Delivery Date: T0+18

Short Description:

Organisation of European High Level Scientific Conference *"Quantum interference and cryptographic keys: novel physics and technologies (QUICK)"* with **P08 (DERA)** as treasurer and **P01 (KTH)** as responsible for public relations and secretary

Downloadable from: http://www.ele.kth.se/QEO/QUICK/

Partners owning: P01, P08

Partners contributed: P01,P08

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Half year progress report for second year

Deliverable N°: D7

Due date: T0+18

Delivery Date: T0+18

Short Description:

Half year progress report for second year.

Downloadable from: http://www.ele.kth.se/QEO/qucomm/DelivD7QuComm_Halfyear2.pdf

Partners owning: P01

Partners contributed: All

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Second year annual progress report

Deliverable N°: D8

Due date: T0+24

Delivery Date: T0+24

Short Description:

Second year annual report

Downloadable from: http://www.ele.kth.se/QEO/qucomm/

Partners owning: All

Partners contributed: All

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Report on diode laser pumped non-linear crystal source for entangled states

Deliverable N°: D11

Due date: T0+18

Delivery Date: T0+18

Short Description:

This report summarises the ongoing work in QuComm on realising diode laser pumped non-linear crystal source for entangled states. In LMU a compact source of polarization entangled photon pairs at a wavelength of 856 nm is realized using a frequency doubled laser diode as pump source for cavity enhanced type-II spontaneous parametric down-conversion (SPDC). The LMU setup generates photon pairs with entanglement visibility of ≥95% and with countrates comparable to those of standard experiments based on large-frame ion lasers. At GAP extensive work has been devoted to the realization, characterisation and application of sources for time-multiplexed, or time-bin qubits and on entangled time-bin qubits. GAP works with photons at telecommunication wavelength in order to allow long-distance quantum communication protocols. Net single photon rates of 20 and 27 KHz, respectively, have been found in initial tests with visibilities of up to 94 %, demonstrating the high purity of the created entangled state. New collaborations, using quazi-phase matched waveguides have demonstrated four order of magnitude higher rates, and with similar visibilities

Downloadable from:

http://www.ele.kth.se/QEO/qucomm/DelD11QuComm.pdf

Partners owning: P05

Partners contributed: P02, P05

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Synchronisation of separate pair-photon sources

Deliverable N°: D13

Due date: T0+24

Delivery Date: T0+24

Short Description:

The report analyses the requirements for the synchronisation of independent photon pair sources and describes the available tools.

Dissemination and Use Plan.

public

Downloadable from:

http://www.ele.kth.se/QEO/qucomm/d13.pdf

Partners owning: P02

Partners contributed: P02,P03 P06

Made available to: Public

DELIVERABLE SUMMARY SHEET	
Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Linear quantum logic, quantum error correction and entanglement purification and distillation

Deliverable N°: D15

Due date: T0+18

Delivery Date: T0+18

Short Description:

The use of linear operations such as beam splitters and polarizing beam splitters plays a crucial role in various new ideas on quantum communication, quantum error correction and entanglement purification. Linear operations are of great interest in quantum communication and computation because they can be implemented comparatively easily and with high precision. Here we review the recent contributions from the Oxford/DERA group on linear quantum logic and bit-flip error rejection in optical quantum communication, from the Vienna group on entanglement purification with linear optics, and on entanglement distillationa and purification by LANL and GAP in collaboration.

Downloadable from:

http://www.ele.kth.se/QEO/qucomm/DelD15QuComm.pdf

Partners owning: P04

Partners contributed: P03, P04, P05, P06, P08

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Report on free-space entanglement enhanced quantum cryptography

Deliverable N°: D16

Due date: T0+12

Delivery Date: T0+12.

Short Description:

The performance requirements of free space quantum cryptography systems is discussed. The advantages of pair photon based cryptography are identified. Progress towards the system on several fronts is described For entangled state quantum cryptography initial experiments were begun using low loss fibre optics to allow long distances to be reached. This has culminated in fibre based entangled state quantum cryptography being demonstrated by groups in the QuComm consortium during this year. However the brightness of entangled state sources needed to be improved as it limits the range of these systems. Meanwhile progress made on faint pulse quantum cryptography systems has meant that free space ranges up to 2km are now achievable with loss budgets around 20dB. If we can solve the brightness limitation then such loss budgets will be within the capabilities of entangled state systems. The preliminary report explains the status of QuComm work on entangled state free-space quantum cryptography.

Partners owning: P04

Partners contributed: P04, P06, P08

Made available to: Project participants

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Report on entanglement enhanced quantum cryptography fiber system

Deliverable N°: D17

Due date: T0+24

Delivery Date: T0+24

Short Description:

This report summarises the ongoing work in QuComm on fiber based entanglement quantum cryptography.

Downloadable from: Internal to project members and the commission

Partners owning: P05

Partners contributed: P02,P03, P05, P06

Made available to: Internal

DELIVERABLE SUMMARY SHEET

Project Number:	*IST-1999-10033*
Project Acronym:	**QuComm**
Title:	Report on high fidelity qubit teleportation
Deliverable N°:D18	
Due date: T0+18	
Delivery Date: T0+18	

Short Description:

After quantum teleportation has been demonstrated for the first time in 1997 a discussion has been going on about potential measures and criteria for the performance of the various experimental teleportation schemes. One particular criterion is the fidelity or overlap between corresponding input and output states. If the fidelity was ideal every allowed input state would be teleported perfectly. Any real piece of apparatus is clearly far from ideal. Here we report on the activities to push the fidelity closer to ideal, which recently lead to the striking demonstration of a violation of Bell's inequality for teleported entanglement.

Downloadable from: http://www.ele.kth.se/QEO/qucomm/DelD18QuComm.pdf

Partners owning: P03

Partners contributed: P03, P05

Made available to: Public

DELIVERABLE SUMMARY SHEET

Project Number: *IST-1999-10033*

Project Acronym: **QuComm**

Title: Report on multimode, multiparticle entanglement protocols

Deliverable N°: D20

Due date: T0+18

Delivery Date: T0+18

Short Description:

This report summarises the ongoing work in QuComm on the demonstration of novel quantum communication protocols, in particular multi-party protocols or protocols which use more than 2-states (or more than one qubit). Such new protocols will extend the capabilities of quantum communication by increasing the channel capacity, by making the systems less sensitive to channel noise. Examples of such protocols include multi-party quantum cryptography (using qutrits and systems with higher Hilbert-space dimension), encoding more than one qubit per photon, "entangled-photon laser". Work concerning error correction and entanglement purification, although relevant for D20, are presented in D15.

Downloadable from: http://www.ele.kth.se/QEO/qucomm/DelD20QuComm.pdf

Partners owning: P01

Partners contributed: P01,P04, P05, P06

Made available to: Public

Appendix 4 (a)- Comparative Information on Resources (Person months)

Effort in person months for reporting period 1/1/2000 -31/12/2000

	KTH				LMU				EXPUNIVIE				Oxford				GAP			
	Period		Total		Period		Total		Period		Total		Period		Total		Period		Total	
WP/Task	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.
WP0	2	3	6	5	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0
WP1	8	11	16	22	3	10	6	11	3	3	4	4	3	2	9	12	5	11	14	19
WP2	0	0	0	0	2	3	9	7.5	4	4	6	6	3	3	6	6	0	0	0	0
WP3	5	4	13	9	0	2	0	2	0	0	3	3	5	5	6	6	5	1	10	11
WP4	0	0	0	0	4	0	5	0	8	8	14	14	3	1	6	3	10	10	10	14
WP5	2	5	15	8	3	4	6	4	2	4	4	6	3	0	7	8	5	3	10	9
WP6	0	0	16	0	0	0	0	0	5	5	5	5	0	0	0	0	0	0	0	0
Total	**17**	**23**	**64**	**44**	**12**	**19**	**24**	**24.5**	23	23	37	37	**17**	**11**	**34**	**35**	**25**	**25**	**44**	**53**

Period: Est.: estimated effort in contract for period Act.: effort actually spent in period
Total: Est.: estimated cumulative effort to date in contract Act.: cumulative effort to date actually spent

	LANL				TH LCR				DERA			
	Period		Total		Period		Total		Period		Total	
WP/Task	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.
WP0	0	0	0	0	0.33	0.33	0.66	0.66	0	0	0	0
WP1	1.5	2	1.5	2	14	13.3	26	24.9	2	3	2	3
WP2	0	0	0	0	0	0	0	0	0	0	0	0
WP3	4	4	4	4	0	0	0	0	0	0	0	0
WP4	0	0	0	0	0	0	0	0	0	0	0	0
WP5	1.5	2	1.5	2	0	0	0	0	0	0	0	0
WP6	6	12	6	12	0	0	0	0	2	3	2	3
Total	**13**	**20**	**13**	**20**	**14,33**	**13.63**	**26.66**	**25.56**	**4**	**6**	**4**	**6**

Period: Est.: estimated effort in contract for period — Act.: effort actually spent in period
Total: Est.: estimated cumulative effort to date in contract — Act.: cumulative effort to date actually spent

Appendix 4 (b) - Comparative Information on Resources (Costs)

Costs in euro for reporting period 1/1/2000 -31/12/2000

	KTH				LMU				EXPUNIVIE				Oxford				GAP (reimbursed from Suisse)			
	Period		Total		Period		Total		Period		Total		Period		Total		Period		Total	
Cost category	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.
Direct costs																				
1. Personnel	63266	72 555	126533	133121	54000	24000	54000	24000	43605	18777	86355	18777	38664	45113	72479	45113	0	0	0	0
2. Durable equipment	0	0,00	0		0	0	0	0	0	11445	26449	31631	0	0	0	0	0	0	0	0
3. Subcontracting	0	0,00	0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4. Travel and subsistence	7333	6 926	14667	13726	4000	4500	4000	4500	10000	1882	20000	4217	5533	5612	11066	10109	0	0	0	0
5. Consumables	6000	17 971	12133	27455	8000	8500	8000	8500	6800	3309	13600	6749	22333	51329	55833	64748	0	0	0	0
6. Computing	0	3 603	0	9659	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7. Protection of knowledge	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8. Other specific costs	0	0,00	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Subtotal	76599	101 055	153333	183961	66000	37000	66000	37000	60405	35413	146404	61374	66530	102054	139378	119970	0	0	0	0
Indirect costs																				
9. Overheads	13333	20 211	26000	34440	14000	7500	14000	7500	12081	7083	29281	12275	13306	20411	27876	23994	0	0	0	0
Total	**89993**	**121266**	**179333**	**218401**	**80000**	**44500**	**80000**	**44500**	**72486**	**42495**	**175685**	**73648**	**79836**	**122465**	**167254**	**143964**	**0**	**0**	**0**	**0**

Period: Est.: estimated costs in contract for period — Act.: actual costs in period

Total: Est.: estimated cumulative costs to date in contract — Act.: cumulative actual costs to date

	LANL (no EU funding)				TH LCR				DERA			
	Period		**Total**		**Period**		**Total**		**Period**		**Total**	
Cost category	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.	Est.	Act.
Direct costs												
1. Personnel	62000	76000	62000	76000	181088	181088	337913	337913	30864	33600	30864	33600
2. Durable equipment	10000	10000	10000	10000	0	0	0	0				
3. Subcontracting	0	0	0	0	0	0	0	0				
4. Travel and subsistence	3000	2000	3000	2000	4382	4382	8438	8438	2572	2000	2572	2000
5. Consumables	0	0	0	0	17660	17660	24896	24896	8000	4400	8000	4400
6. Computing	4000	3000	4000	3000	0	0	0	0	0	0	0	0
7. Protection of knowledge	0	0	0	0	0	0	0	0	0	0	0	0
8. Other specific costs	0	0	0	0								
Subtotal	79000	91000	79000	91000	203130	203130	371247	371247	41436	40000	41436	40000
Indirect costs												
9. Overheads	92000	106000	92000	106000	37326	37326	68136	68136	0	0	0	0
Total	**171000**	**197000**	**171000**	**197000**	**240456**	**240456**	**439383**	**439383**	**41436**	**40000**	**41436**	**40000**

Period: Est.: estimated costs in contract for period Act.: actual costs in period

Appendix 5 – Progress Overview Sheets

PROGRESS OVERVIEW SHEETS

Organisation: KTH (P01)

Workpackage/ Task	Planned effort[1]	Planned Date[2]		Actual Date[3]		Resources employed[2]	Cumulative Resources[2]
	Whole Project	Start	End	Start	End	This Period	Since start
WP 0		0	36	0	36	3	5
WP 1		0	30	0	30	11	22
WP 2		0	24	0	24	0	0
WP 3		0	24	0	24	4	9
WP 4		6	30	6	30	0	0
WP 5		6	36	4	36	5	8
WP 6		18	36	18	36	0	0
Total						20	44
One person month is equal to		140		Person hours			

Main contribution during this period

Workpackage/Task	Action
WP 0	Coordination and management of the project. Arrangement of the QUICK workshop.
WP 1	We have built a down-conversion source from 514nm to the idler at 780nm and 1550nm, and a second source to generate two photons at 1550nm. Different non-linear materials tested.
WP 2	No activity
WP 3	We have been working both on the hardware-software interface, detector modules, as well as made a theoretical paper on authentication.
WP 4	No activity.
WP 5	Theoretical studies of the encoding of information on N-state systems and investigated the use of this in quantum cryptography, and studies of various operator expansions in Hilbert space with possible application to state tomography.
WP 6	No activity

Deliverables due this period

Deliverable number	Title of Deliverable	Status (Draft Final, Pending)

Dissemination actions (articles, workshops, conferences etc.)

2001 Publications

1. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and N. J. Cerf, *Quantum key distribution using multilevel encoding: security analysis*, quant-ph/0106049, 8 June, 2001.
2. N. J. Cerf, M. Bourennane, A. Karlsson and N. Gisin, *Security of quantum key distribution using d-level systems*, quant-ph/0107130, 26 July, 2001.

[1] In person months (or in person hours)
[2] Project month when the activity was planned to be started or to be completed
[3] Project month when the activity was actually started or completed

3. M. Bourennane, A. Karlsson and G. Björk, *Quantum key distribution using multilevel encoding*, **Phys. Rev. A**, vol. 64, art. no. 012306/1-5, 2001.

4. M. Bourennane, A. Karlsson and G. Björk, *Quantum Key Distribution Using Multilevel Encoding*, pp. 295-298 in **Quantum Communication, Computing, and Measurement 3**, eds. P. Tombesi and O. Hirota, Plenum, New York, 2001.

5. D. Ljunggren, M. Bourennane and A. Karlsson, *Authority-Based User Authentication and Quantum Key Distribution*, pp. 299-302 in **Quantum Communication, Computing, and Measurement 3**, eds. P. Tombesi and O. Hirota, Plenum, New York, 2001.

6. I. Ghiu, M. Bourennane and A. Karlsson, *Entanglement-assisted local transformations between inequivalent classes of three-particle entangled states*, **Phys. Lett. A**, vol. 287, no. 1-2, pp. 12-18, 2001.

7. M. Bourennane, A. Karlsson, J. Peña Císcar and M. Mathes, *Single-photon counters in the telecom wavelengh region of 1550 nm for quantum information processing*, **J. Mod. Opt.**, vol. 48, no. 13 - Special Issue on Technologies for Quantum Communications, pp. 1983-1995, 2001.

8. A. Karlsson, M. Bourennane, D. Ljunggren, J. Peña Císcar, M. Mathes and A. Hening, *Quantum communication and single-photon technologies*, **Proc. SPIE**, vol. 4430 - ROMOPTO 2000: Sixth Conference on Optics (edited by V. I. Vlad), pp. 430-441, 2001.

2001 Conference Contributions

1. I. Ghiu, M. Bourennane and A. Karlsson, *Transformations between inequivalent classes of three-particle engtangled states*, poster at **Quantum Entanglement and Quantum Information (QuEnt)**, in Les Houches, France, March 19-30, 2001.

2. A. Karlsson, M. Bourennane and D. Ljunggren, *Long wavelength quantum cryptography: A discussion on some issues*, oral presentation SuM2 at **Quantum interference and cryptographic keys: novel physics and advancing technologies (QUICK)**, Cargèse, Corsica, France, April 7-13, 2001.

3. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and H. Zbinden, *A quantum key distribution with N-array encoding*, poster M5 at **Quantum interference and cryptographic keys: novel physics and advancing technologies (QUICK)**, Cargèse, Corsica, France, April 7-13, 2001.

4. A. Karlsson, *Technologies for Quantum Communication*, invited talk at **Workshop on (Not Only) Solid State Quantum Computing**, Warsaw, Poland, April 26-29, 2001.

5. A. Karlsson, M. Bourennane, D. Ljunggren, I. Ghiu and R. Viana Ramos, *Long wavelength quantum cryptography and entanglement manipulations*, invited talk QECCB2 at **International Conference on Quantum Information (ICQI)**, Rochester, New York, USA, June 10-13, 2001.

6. A. Karlsson, *Technologies for Quantum Communication*, oral presentation at **4th QNANO Workshop**, Nässlingen, Sweden, June 13-15, 2001.

7. G. Björk, J. Söderholm, A. Trifonov, P. Usachev and L. L. Sánchez-Soto, *Applications of entangled state interference*, invited talk WM5 at **XVII International Conference on Coherent and Nonlinear Optics (ICONO 2001)**, Minsk, Belarus, June 26-July 1, 2001. .

8. M. Bourennane, A. Karlsson, G. Björk, N. Gisin and N. J. Cerf, *Quantum key distribution using multilevel encoding: Security analysis*, poster at **2nd ESF QIT Conference - Quantum Information Theory and Quantum Computing**, Gdansk, Poland, July 10-18, 2001.

9. M. Bourennane, A. Karlsson, M. Mathes and J. Peña Císcar, *Single Photon Counters in the Telecom Wavelength Region of 1550nm for Quantum Information Applications*, oral

presentation WG2-2 at **CLEO/Pacific Rim 2001**, Chiba, Japan, July 15-19, 2001.

10. A. Karlsson, *From quantum encryption to teleportation; an introduction to quantum communication with possible applications*, invited tutorial Th.M.3.1. at **27th European Conference on Optical Communication (ECOC'01)**, Amsterdam, Sept 30-Oct 4, 2001.

11. R. Viana Ramos, *Numerical Analysis of Eavesdropping Attacks in Quantum Cryptographic Systems using MATLAB*, oral presentation at **Nordic MATLAB conference**, Oslo, Norway, Oct 17-18, 2001.

12. A. Karlsson, *Entanglement manipulations and quantum communication*, oral presentation at **XXII International Solvay Conference in Physics - The Physics of Communication**, Delphi and Lamia, Greece, Nov 24-30, 2001.

Deviations from the planned work schedule/reasons/corrective actions/special attention required
The work to realise the down-conversion source took much longer time than expected, partly due to lack of personell (one person was leaving), partly due to technology reasons. Now, the down-conversion set-ups are beginning to work well
Planned actions for the next period
The down-conversion towards applications has top priority.

Organisation: LMU (P02)

Workpackage/Task	**Planned effort**	**Planned Date**		**Actual Date**		**Resources employed**	**Cumulative Resources**
	Whole Project	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP 1	**6**	**0**		**0**		**10**	**11**
WP 2	**9**	**0**				**3**	**7.5**
WP 3	**0**	**0**		**0**		**2**	**2**
WP 4	**10**	**6**		**6**		**0**	**0**
WP 5	**10**	**6**		**0**		**4**	**4**
WP 6	**1**	**18**				**0**	**0**
Total	36					19	24.5
One person month is equal to	140			Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 1	
	• Polarization-entangled photon pairs at about 856nm have been obtained from a frequency-doubled laser diode and subsequent parametric fluorescence at the end of the first year. The performance of the system was documented and published, gaining interest in the scientific community. The system is currently under redesign to improve stability, and handling. • After set-up and optimization of pulsed down-conversion was finished the generation of four-photon entanglement directly from the don conversion was demonstrated. The high stability of the source allowed detailed measurement of correlation functions, the first four particle Bell inequality and effects of coherence/decoherence of the four photons. The results are currently prepared for publication. • Feasibility study of synchronising independent pair-photon sources was performed. Since by the time synchronisation became a commercial option for upgrading certain mode-locked lasers, we did not implement this system due to lack of novelty. For future use of concatenated communication systems, the tools are readily available.
WP 2	
Task 2.1	• Design of compact polarisation units: the stable design allows the utilisation in long-time measurements of four-photon Bell-inequalities.
WP 3	

Task 3.1	• Development of a multi-party quantum cryptography scheme based on the four photon results of WP1. The perfect correlations of the four photon measurements together with the observed violation of a Bell-inequality allows the generalisation of the Eckert-protokol for entanglement based quantum cryptography to 4 parties.
WP 5	
Task 5.1	• Demonstration of the "mean king" quantum game demonstrating the extended measurement possibilities of entangled particles as opposed to untentangled ones. (After finishing with this experiment, work on M10 and M21 can be resumed) • Developed new protocols for secure communication and for deterministic quantum cryptography based on the features of the "mean king" game.

Deliverables due this period

Deliverable number	Title of Deliverable	Status (Draft Final, Pending)
D13	Synchronisation of separate pair-photon sources	Final

Dissemination actions (articles, workshops, conferences etc.)

Articles:

Ch. Kurtsiefer, M. Oberparleiter, H. Weinfurter, *High efficiency entangled photon pair collection in type II parametric fluorescence*, Phys. Rev. A **64**, 023802 (2001).

H. Weinfurter, M. Zukowski, *Four-photon entanglement from down-conversion*, Phys. Rev. A 64, 010102(R), (2001).

J. Volz, Ch. Kurtsiefer, H. Weinfurter, *Compact All-Solid-State Source of Polarization Entangled Photon Pairs*, Appl. Phys. Lett. **79**, 869 (2001).

C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, *Generation of correlated photon pairs in type-II parametric down conversion – revisited*, Journal of Modern Optics **48**, 1997 (2001).

A. Beige, B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, *Cryptography with single-photon two-qubit states*, submitted to PRL.

H. Weinfurter, *Quantum Communication with entangled Photons*, Proceedings of the IX Seminaire Rhodanien, Winterschool on Quantum Information, Dolomieu, March 2001.

Ch. Kurtsiefer, M. Oberparleiter, J. Volz, H. Weinfurter, *Efficient generation of polarization entangled photon pairs with a laser diode source*, in 'Frontiers of Laser Physics', (ed. H. Figger, D. Meschede, C. Zimmermann), Springer, 2001.

H. Weinfurter, A. Zeilinger: *Quantum Communication*, in 'Quantum Information - an introduction', (eds. G. Alber, H. Steiner), Springer, 2001.

Talks:

Entanglement and Quantum Communication, Seminaire Rhodanien, Dolomieu, France, 25.2. - 1.3.2001.

Quanteninformation Lehrerfortbildung, Seeon, Germany, 12.3.2001.

Quantuminformation – Basics, Tutorial series, Workshop on *Coherent Evolution in Noisy Environments,* MPI-PKS-Dresden, Germany, 3.4.-6.4.2001.

Quantuminformation – Overview, Workshop 'German American Frontiers of Science', Bad Homburg, Germany, 8.6.-10.6.2001.

Four-Photon Entanglement from Parametric Down-Conversion, CLEO Europe Topical meeting, Munich, Germany, 20.6.-22.6.2001.

Quantenkryptographie und Quantenteleportation, Kolloquium Max-Planck-Institut for Polymerresearch and University of Mainz, Germany, 3.7.2001

Anwendungen der Quantenkommunikation, Kolloquium at "Physikalische Technische Bundesanstalt" – PTB, Braunschweig, Germany, 6.9.2001

Challenges in Quantuminformation, Workshop on "Challenges in Quantum Mechanics", Essen, Germany, 8.9.2001

Deviations from the planned work schedule/reasons/corrective actions/special attention required

- Work on M10, M21 was further delayed in favour of successfully finishing teh experiment on multi-state analysis of the "mean king" quantum game. These milestones, however, will attacked in the near future as the "mean king"-game now could be demonstrated with success rates well exceeding the rates possible without entanglement.

Planned actions for the next period

- Complete Bell-state analysis M10
- Quantum Dense Coding in noisy environment M21
- Demonstrate novel three-particle entangled state

Organisation: EXPUNIVIE (P03)

Workpackage /Task	**Planned effort**	**Planned Date**		**Actual Date**		**Resources employed**	**Cumulative Resources**
	Whole Project	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP 0	**2**	**0**	**36**	0		1	1
WP 1	3	0	30	0		3	4
WP 2	6	0	24	0		4	6
WP 3	6	0	24	0	24	0	3
WP 4	15	6	30	6		8	14
WP 5	4	6	36	6		4	6
WP 6	6	18	36			5	5
Total	42					25	39
One person month is equal to		140		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 1	• construction of the platform for purification of arbitrary mixed states (mainly contained in WP 5) • setting up of the Ti:Sa laser and frequency doubling • photon statistics measurements on down-conversion light from a high-energy pulsed laser. First results imply that on average of the order of 1 photon per pulse is created.
WP 2	• development of a scheme for entanglement purification of general mixed entangled states avoiding the controlled-NOT-gate operation and requiring only simple linear optical elements
WP 3	• No activity
WP 4	• performance of an entanglement swapping experiment based on two independent pairs of polarization-entangled photons. Two independent photons were entangled with

	such high fidelity that a violation of Bell's inequality was shown. For the realization of this experiment several new technologies had to be implemented (as described in the main text). The experimental test of the CHSH-inequality was performed and gave a Bell-parameter of S=2.46 ±0.9, which clearly violates the classical limit of 2 by more than 4 standard deviations. • EXPUNIVIE is presently working on the experiment. The necessary components are tested in the lab.
WP 5	• construction of a first test platform for purification of entangled states • observance of a violation of Bell's inequality for an angular momentum entangled state of photon pairs produced by Down-conversion
WP 6	• development of the hardware for long distance (560 m) teleportation, such as the polarisation control scheme, source design, detectors, registration electronics and a microwave based classical channel. • adaptation of the labs at the field site for the teleportation experiment

Deliverables due this period

Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**
D18	High fidelity quantum teleportation (lead partner)	OK
D15	Linear quantum logic and quantum error correction (contribution)	OK
D17	Entanglement enhance cryptography fiber system (contribution)	OK

Dissemination actions (articles, workshops, conferences etc.)

Articles

- Thomas Jennewein, Gregor Weihs, Anton Zeilinger, *Schrödingers Geheimnisse*, c't, No. 6/2001.
- Caslav Brukner, Jian-Wei Pan, Christoph Simon, Gregor Weihs, Anton Zeilinger, *Probabilistic Instantaneous Quantum Computation*, quant-ph/0109022.
- Christoph Simon, Jian-Wei Pan, *Polarization Entanglement Purification using Spatial Entanglement*, quant-ph/0108063.
- Jennewein, G. Weihs, J.-W. Pan, A. Zeilinger. *An experimental proof of nonlocality for Teleportation and Entanglement Swapping,* Phys. Rev. Lett. 88, (2002).
- J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs and A. Zeilinger, *Experimental demonstration of four-photon entanglement and high-fidelity teleportation*, Phys. Rev. Lett. 86, 4435 (2001).
- J.-W. Pan, C. Simon, C. Brukner and A. Zeilinger, *Entanglement purification for quantum communication*, Nature (London) 410, 1067 (2001).
- T. Rudolph and J.-W. Pan, *A simple gate for linear optics quantum computing*, Quant-ph/0108056.
- A. Mair, A. Vaziri, G. Weihs and A. Zeilinger,. *Entanglement of the orbital*

angular momentum states of photons, Nature 412, 313 (2001).

- A. Vaziri, G. Weihs and A. Zeilinger, *Superpositions of the Orbital Angular Momentum for Applications in Quantum Experiments,* quant-ph/0111033 (to appear in Journal of Optics B)
- Wolfgang Tittel, Gregor Weihs, *Photonic entanglement for fundamental tests and quantum communication*, Quantum Information and Computation, vol. 1, no. 2, pp. 3-56 (2001).

Talks and Posters

- T. Jennewein, J.W. Pan, G. Weihs, A. Zeilinger: Experimental Nonlocality proof for Entanglement Swapping, poster, WE-Heraeus-Seminar Exploring Quantum Physics, Venice (Italy), 18. – 23. August 2001.
- T. Jennewein, G. Weihs, A. Zeilinger. An all-fiber Bell State Analyzer, poster, CARGESE CORSICA April 7-13, 2001
- G. Weihs, *Introduction to photonic entanglement*, Invited Tutorial,Seminaire Rhodanien, Dolomieu, France, February 2001.
- G. Weihs, Photonic entanglement, *Bell's inequality and GHZ*, Invited Lecture, Les Houches Winter School, Les Houches, France, March 2001.
- G. Weihs, Quantenkryptographie, Tuturial Lecture, Cryptology Seminar, St. Pölten, Austria, April 2001.
- G. Weihs, *Photonic entanglement for quantum communication*, Physics/Applied Physics Colloquium, Stanford University, Palo Alto, USA, May 2001.
- G. Weihs, *High-fidelity entanglement swapping*, Institut for theoretical Physics and Astrophysics, Gdansk, Poland, June 2001.
- G. Weihs, *Photonic quantum communication*, Invited Talk, ERATO Quantum Computation and Information Project, Tokio, Japan, July 2001.
- G. Weihs, *Higher photonic entanglements*, ISQM-Tokyo, Japan, August 2001.
- G. Weihs, *Entanglement of the orbital angular momentum states of photons*, Invited Talk, International Symposium on Quantum Information, Tunxi, China, September 2001.
- A. Zeilinger, *Information in der Quantenwelt*, Werner Heisenberg Vorlesung, Carl Friedrich von Siemens Stiftung, Munich, Germany, January17, 2001.
- A. Zeilinger, *Quantum Physics: Finding Answers to Scientific Puzzles*, Forum Fellow at the Annual Meeting, World Economic Forum, Davos, Switzerland, January 25-30, 2001.
- A. Zeilinger, *Quanteninformation - ein neues Konzept zur Informationsverarbeitung und Informationsübertragung*, Lecture at Siemens AG, Munich, Germany, February 19, 2001.
- A. Zeilinger, *Quantum Experiments and the Foundations of Physics*, Distinguished Lectureship, Brookhaven National Laboratory (BNL), Islip, New York, U.S.A., February 28, 2001.
- A. Zeilinger, *Quanteninformation und die Grundlage der Quantenmechanik*, Lecture, Nordrhein-Westfälische Akademie der Wissenschaften, Germany, April 4, 2001.
- A. Zeilinger, *Was Quanten alles können: Von der Philosophie zu einer neuen Technologie*, Public Evening Lecture at the International Workshop on Coherent Evolution in Noisy Environments, Dresden, Germany, May 22-25, 2001.
- A. Zeilinger, *Quantenphysik und Information*, Keplervorlesung, Tübingen, Germany, July 11, 2001.
- A. Zeilinger, *Information and Quantum Mechanics Gordon Conference on*

Quantum Control of Atomic and Molecular Motion, Mount Holyoke College, Boston, Mass., USA, July 29 – August 3, 2001. • A. Zeilinger, Q*uantum Entanglement, Classical Information and Physical Reality*, XXII International Solvay Conference in Physics on The Physics of Communication, Lamia and Delphi, Greece, November 24-30, 2001. • A. Zeilinger, *Quantum Interference, Uncertainty and Complementary in Experiments*, Heisenberg-Symposium, Ludwig Maximilians-Universität, Munich, Germany, December 5-7, 2001. • A. Zeilinger, *Classical Information, Quantum Entanglement and Photonic Communication,* Fondation Hugot du Collège de France, Paris, France, December 13-16, 2001.
Deviations from the planned work schedule/reasons/corrective actions/special attention required
none
Planned actions for the next period
• setting up the long-distance teleportation experiment • implementation of an improved Bell state analyser and active switching for a higher efficiency teleportation experiment • feasibility tests of entanglement purification • development of protocols using multi level states, such as angular momentum of photons

Organisation: Oxford

Workpackage /Task	Planned effort	Planned Date		Actual Date		Resources employed	Cumulative Resources
	Whole Project	Star t	End	Star t	End	This Period	Since start
WP 1	12	00	30	00		2	12
WP 2	6	00	18	00		3	6
WP 3	6	00	24	00		5	6
WP 4	9	12	30	00		1	3
WP 5	10	00	30	00		0	8
WP 6	3	18	36			0	0
Total	46					11	35
One person month is equal to		145		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 1	
Task 1.1	We have studied the effective creation of twin-photons using PPLN structures.
Task 1.3	We have experimentally realized stimulated four-photon entanglement generation in parametric down-conversion.
WP 2	
Task 2.2	We have developed linear optics schemes for error correction and entanglement purification.
WP 3	
Task3.1	We have proposed a scheme for multiphoton-entanglement based quantum cryptography.
WP 4	
	See below
WP 5	
Task 5.2	We have theoretically studied the robustness of multiphoton entanglement under photon loss.
WP 6	

Deliverables due this period		
Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**
D15 (T0+18)	Report on linear quantum logic and quantum error correction	Final

Dissemination actions (articles, workshops, conferences etc.)
Invited talks in Gdansk, Rochester, Hangzhou, Seoul, Santa Barbara. Papers:

A. Lamas-Linares, J. C. Howell, D. Bouwmeester, *Stimulated Emission of Polarization Entangled Photons,* Nature 412, 887 (2001)

John C. Howell, Antia Lamas-Linares, Dik Bouwmeester, *Experimental violation of a spin-1 Bell inequality using maximally-entangled four-photon states*, quant-ph/0105132, to appear in Phys. Rev. Lett.

Gabriel A. Durkin, Christoph Simon, Dik Bouwmeester, *Multi-Photon Entanglement Concentration and Quantum Cryptography*, quant-ph/0109132.

Christoph Simon, Julia Kempe, *Robustness of Multi-Party Entanglement*, quant-ph/0109102.

Caslav Brukner, Jian-Wei Pan, Christoph Simon, Gregor Weihs, Anton Zeilinger, *Probabilistic Instantaneous Quantum Computation*, quant-ph/0109022.

Christoph Simon, Jian-Wei Pan, *Polarization Entanglement Purification using Spatial Entanglement*, quant-ph/0108063.

Deviations from the planned work schedule/reasons/corrective actions/special attention required
We have diverted resources from the study of teleporting entanglement (WP4) to the related experimental realization of quantum cloning by stimulated emission.
Planned actions for the next period
We will continue to study the generation and applications of multiphoton entanglement from parametric down-conversion, with an emphasis on applications that only require linear optical elements.

Organisation: GAP (P05)

Workpackage /Task	Planned effort	Planned Date		Actual Date		Resources employed	Cumulative Resources
	Whole Project	Star t	End	Star t	End	This Period	Since start
WP 1	**14**	**0**		**0**		**11**	**19**
Task 1.1						11	19
Task 1.2						0	0
Task 1.3						0	0
Task 1.4						0	0
WP 2	**0**	**0**				**0**	**0**
Task 2.1						0	0
Task 2.2						0	0
WP 3	**10**	**0**		**0**		**1**	**11**
Task 3.1						0	0
Task 3.2						0	10
WP 4	**20**	**6**		**6**		**10**	**14**
Task 4.1						0	0
Task 4.2						10	14
WP 5	**15**	**6**		**0**		**3**	**9**
Task 5.1						0	4
Task 5.2						3	5
WP 6	**10**	**18**				**0**	**0**
Task 6.1							
Task 6.2							
Task 6.3							
One person month is equal to		40		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 1	
Task 1.1	• Development of a bright time-bin entangled photon-pair source using a PPLN waveguide emitting photons at 1310 nm (for use in WP 3 and, in a modified version, in WP5) • Development of a femtosecond time-bin entangled photon pair source emitting non-degenerate photons at 1310/1550 nm (for use in WP4)
WP 3	
Dissemination	• Writing of a review article concerning quantum cryptography, accepted for publication in Rev.Mod.Phys. [16]
WP 4	
Task 4.2	• building setup for entanglement swapping with time-bin entangled photons using two spatially separated sources • testing entanglement quality of the 2 sources.

	• Observation of quantum interferences with photons coming from two spatially separated sources, with 2-photon detection • First observation of 4-photon detection at telecom wavelength
WP 5	
Task 5.2	• devising the setup to extend time-bin entanglement to 3 dimensions (qutrits). Start of the construction of a 3 branch interferometer.

Deliverables due this period

Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**
D4 **D5**	Half Year progress report First year progress report	OK OK

Dissemination actions (articles, workshops, conferences etc.)

Publications

- W. TITTEL, H. ZBINDEN, N. GISIN, *Experimental demonstration of quantum secret sharing*, Phys. Rev. A 63, 042301 (2001).

- G. RIBORDY, J. BRENDEL, J.-D. GAUTIER, N. GISIN, AND H. ZBINDEN, "Long distance entanglement-based quantum key distribution", Phys. Rev. **A** 63, 012309. Preprint quant-ph/0008039

- N. GISIN, G. RIBORDY, W. TITTEL, and H. ZBINDEN, *Quantum Cryptography*, quant-ph/0101098, accepted for publication in Rev. Mod. Phys.

- P. G. KWIAT, S. BARRAZA-LOPEZ, A. STEFANOV, and N. GISIN, *Experimental entanglement distillation and 'hidden' non-locality*, Nature 409, 1014 (2001).

- Wolfgang TITTEL, Gregor WEIHS, *Photonic entanglement for fundamental tests and quantum communication*, Quantum Information and Computation, vol. 1, no. 2, pp. 3-56 (2001).

- D. STÜCKI, G. RIBORDY, A. STEFANOV, H. ZBINDEN, J.G. RARITY, T. WALL, *Photon counting for QKD with Peltier Cooled InGaAs/InP APD's*, J.Mod.Opt **48,** n°13 1967-1981 (2001)

- S. TANZILLI, H.de RIEDMATTEN ,W. TITTEL, H. ZBINDEN, P. BALDI, M. de MICHELI, D.B. OSTROWSKY, N. GISIN, *Highly efficient photon–pair source using PPLN waveguide*, Electr. Lett. , **37** p28 (2001)

- H. ZBINDEN, N. GISIN, G. RIBORDY, D. STÜCKI, W. TITTEL, *Experimental quantum communication*, to appear in the proceedings of the International

School of Physics Enrico Fermi, Varenna, July 17-27, 2001.

- S. TANZILLI, W. TITTEL, H. de RIEDMATTEN, H. ZBINDEN, P. BALDI, M. de MICHELI, D.B. OSTROWSKY, N. GISIN , *PPLN waveguide for Quantum Communication*, quant-ph/0107125, to be published in European Physical Journal D (special issue of the Quick conference).

- I. MARCIKIC, H de RIEDMATTEN, W. TITTEL, H. ZBINDEN, N. GISIN, *Femtosecond time-bin entangled qubits for robust quantum communication,* to be submitted.

Presentations, Posters

- W. TITTEL, "Quantenkryptographie über große Entfernungen: von der Idee zur Anwendung" presentation at *Siemens*, München, Germany, February 19th, 2001.

- H. ZBINDEN, "Cryptographie Quantique", at *Neuvième Séminaire Rhodanien de Physique, « Physique des états enchevêtrées »* in Dolomieu-France, February 25- March 3, 2001.

- STEFANOV, "Quantum Cryptography", at *9. SSOM Fachkurs "Optical Communication"* in Engelberg/Switzerland, March 25 – 29, 2001.

- N. GISIN, "Quantum cryptography: from basic physics to applications", at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- H. ZBINDEN, "Faint laser versus entangled photons Quantum Key Distribution", at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- W. TITTEL, "Time-bin entangled photon pairs & applications in quantum cryptography", at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- S. TANZILLI, "Highly efficient photon-pair source using PPLN waveguide", at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- STEFANOV ET AL., "Plug & Play long distance quantum key distribution prototype", poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- S. TANZILLI ET AL., "Highly efficient photon-pair source using PPLN waveguide", poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.

- V. SCARANI, "Quantum cryptography, from foundations to application", at *foyer d'étudiants*, Zürich, April 4^{th}, 2001.

- N. GISIN, "Entanglement, from paradoxes to applications", at *foyer d'étudiants*, Zürich, April 4^{th}, 2001.

- N. GISIN at CLEO/EQELS: "Quantum Key Distribution : Faint laser pulses vs.

entangled Photons", invited talk, May 10.

- N. GISIN at GDR : "La Cryptographie Quantique », présentation invitée dans le cadre du lancement de ce nouveau programme français, Mai 18.

- N. GISIN at University of Barcelone : "Quantum Key Distribution : Faint laser pulses vs.entangled photons", colloquium May 31.

- N. GISIN at CERN: "Quantum Key Distribution : Faint laser pulses vs. entangled photons", invited talk within the OPAL-project meeting, June 13.

- G. RIBORDY et al. at CERN :"Single-Photon Detection at Telecommunication Wavelengths: Performance and Applications to Classical and Quantum Communications" . June 5th, 2001.

- H. ZBINDEN et al. at CEA Grenoble, "Cryptographie quantique expérimentale". June 12th, 2000.

- H. ZBINDEN et al. at CLEO-Europe, "Experimental Quantum Cryptography", June 20st, 2001

- Hugo ZBINDEN, *Experimental quantum Key Distribution*, 10th International Laser Physics Workshop, Moscow, Russia, July 3-7, 2001.

- Hugo ZBINDEN, *Experimental quantum Communication*, International School of Physics Enrico Fermi, Varenna, Italy, July 17-27, 2001.

- Hugo ZBINDEN, *Quantum Communication and computing*, NKT summer school, Copenhagen, Denmark, Aug 19-25, 2001.

- N. GISIN, *Entanglement in relativistic configurations: theory and experiments*, Workshop on quantum information and space-time structure, Madrid, Spain, Sept 5, 2001.

- N. GISIN, *Entanglement in relativistic configurations: theory and experiments*, invited talk at 10th conference on the foundations of quantum physics, Belfast, Northern Ireland, UK, Sept 11, 2001.

- I.MARCIKIC, H.de RIEDMATTEN, W.TITTEL, H.ZBINDEN and N.GISIN, *Femtosecond time bin entangled qubits for quantum communication*, poster at the QIPC Workshop, October 28-31, Torino, Italy

- H.de RIEDMATTEN, I.MARCIKIC, W.TITTEL, H.ZBINDEN and N.GISIN, *Towards long distance entanglement swapping using time-bin entangled qubits*, poster at the QIPC Workshop, October 28-31, Torino, Italy

Deviations from the planned work schedule/reasons/corrective actions/special attention required

- The demonstration of robustness non-maximally time-bin entangled states

over large distances has been delayed, because the PPLN waveguide used as downconverter was used for another experiment
Planned actions for the next period
• Demonstration of robustness of non-maximally time-bin entangled states over large distances • Demonstration of two-photon correlations after swapping of time-bin entanglement

Organisation: LANL (P06)

Workpackage /Task	**Planned effort**	**Planned Date**		**Actual Date**		**Resources employed**	**Cumulative Resources**
	Whole Project	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP 0	0					0	0
WP 1	6	0	30	0		2	2
WP 2	4	12	24	12		0	0
WP 3	6	6	24	6		4	4
WP 4	0					0	0
WP 5	4	6	36	0		2	2
WP 6	18	12	36	0		12	12
Total	38					20	20
One person month is equal to		150		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 0	No activity
WP 1	Begun detailed calculations to optimize techniques to permit strong polarization-entanglement for *all* emitted pairs of photons. We have demonstrated the basic principle of the technique.
WP 2	No activity
WP 3	Performed two free-space polarization-entanglement based quantum cryptography experiments. In the first (which appeared along with GAP and EXPUNIVE in PRL), we implemented Ekert's protocol, including tests of Bell's inequalities, and also experimental implementation of simple eavesdropping strategies. In the second, we have set up an experiment, and obtained preliminary results, implementing a six-state protocol, in which the presence of an eavesdropper is made 33% more visible. A variety of eavesdropping attacks are being explored.
WP 4	No activity
WP 5	First demonstration of entanglement distillation and the phenomenon of hidden nonlocality (along with GAP); results to appear in Nature.
WP 6	Constructed a transportable free-space quantum key distribution that uses the BB84 protocol. An active beam control system is designed to allow unattended operation throughout the day and night over terrestrial paths of up to 10 km. Laboratory testing was completed during this performance period and field tests will be carried out in early 2001.

Deliverables due this period		
Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**

Dissemination actions (articles, workshops, conferences etc.)

1. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, *"Entangled state quantum cryptography: Eavesdropping on the Ekert protocol"*, Phys. Rev. Lett. **84**, 4733 (2000).
2. R. J. Hughes et al., "*Free-space quantum key distribution in daylight"* Journal of Modern Optics **47**, 549 (2000).
3. R. J. Hughes et al., "*Free-space quantum cryptography in daylight"*, Proc. SPIE **3932**, 117 (2000).
4. W. T. Buttler et al., "*Daylight quantum key distribution over 1.6 km"*, *Physical Review Letters* **84**, 5652 (2000).
5. P. G. Kwiat, S. Lopez, A. Stefanov, and N. Gisin, *"Demonstration of entanglement distillation and purification"*, to appear in Nature (2001).
6. R. J. Hughes, *Free-space quantum cryptography in daylight*, SPIE Photonics West, San Jose, CA, January 2000.
7. R. J. Hughes, *Secure communications using quantum cryptography*, keynote address, SPIE AEROSENSE conference, Orlando, FL, April 2000.
8. P. G. Kwiat, *Entangled-photon quantum cryptography*, contributed paper, CLEO/QELS 2000 conference, San Francisco, CA, May 2000.
9. P. G. Kwiat, *Entanglement concentration and hidden entanglement*, contributed paper, APS DAMOP 2000 meeting, Storrs, CT, June 2000.
10. R. J. Hughes, *Daylight quantum key distribution over 1.6 km*, contributed paper, APS DAMOP 2000 meeting, Storrs, CT, June 2000.
11. P. G. Kwiat, *101 Uses for a Schrödinger Kitten*, invited talk at 5th Int. Conf. on Quantum Communication, Measurement & Computing, Capri, Italy July 2000.
12. R. J. Hughes, Earth to space quant*um key distribution*, invited talk at NASA-DoD workshop on Quantum Clock Synchronization, Glendale, CA, September 2000.

Deviations from the planned work schedule/reasons/corrective actions/special attention required

None

Planned actions for the next period

We will complete the six-state quantum cryptography protocol experiment, including analysing the effect of various sorts of eavesdroppers. We will further develop the free-space experiment, so that when the appropriate sources of entangled photons become available, they can be readily incorporated into the system.

Organisation: THOMSON-CSF LCR (P07)

Workpackage/ Task	**Planned effort**	**Planned Date**		**Actual Date**		**Resources employed**	**Cumulative Resources**
	Whole Project	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP 0	1	T0	T0+36	T0		0.33	0.66
WP 1							
Task 1.1	26	T0	T0+24	T0		13.3	24.9
WP 6	1	T0+18	T0+36	T0+18		0	0
Total	28					13.63	25.5
One person month is equal to		143		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 0	Management of TH-LCR contribution to the project
WP 1	
Task 1.1	• An optically pumped semiconductor laser for direct generation of twin photons at 1.55 microns has been processed. Laser operation at 775 nm in the third order mode of the guiding structure has been shown. The measurement of the parametric fluorescence is on going (Partner 01). • An electrically pumped semiconductor laser for direct generation of twin photons at 1.55 microns has been processed. No laser operation has been shown at the moment due to an unexpected huge resistivity. Effort is being pursued to produce an improved sample. • A structure aiming at producing conterpropagating twin photons has been processed. Test is ongoing at partner 04.

Deliverables due this period

Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**
D12	Prototype integrated GaAs laser photon pair source	Delayed, work ongoing

Dissemination actions (articles, workshops, conferences etc.)

Publications :

43. N. G. Semaltianos, B. Vinter, A. De Rossi, V. Berger, and V. Ortiz, *"Photoluminescence of a third order mode optically pumped semiconductor laser structure",* submitted to Applied Physics Letters.

44. A. De Rossi, N. G. Semaltianos, , V. Berger, E. Chiralis, B. Vinter, and V. Ortiz, *"Third order mode optically pumped semiconductor laser",* submitted to Applied Physics Letters.

45. A. De Rossi, V. Berger, *"Counterpropagating twin photons by parametric fluorescence",* to be published in Physics Review Letters.

Conference :
Participation to the Cargese QIPC Workshop

Deviations from the planned work schedule/reasons/corrective actions/special attention required

Work delayed during year two because several key people in the technology left the laboratory. Unexpected technical difficulty with the electrically pumped sample.
Planned actions for the next period
Continuing effort will be devoted to the improvement of the semiconductor structure in order to produce a sample fulfilling the requirements of Deliverable 12.

Organisation: DERA (P08) (now renamed QinetiQ)

Workpackage /Task	**Planned effort**	**Planned Date**		**Actual Date**		**Resources employed**	**Cumulative Resources**
	Whole Project	**Start**	**End**	**Start**	**End**	**This Period**	**Since start**
WP 1	12	0	36	5	36	5	8
WP6	12	0	36	0	36	2	5
Total							
One person month is equal to		120		Person hours			

Main contribution during this period	
Workpackage/Task	**Action**
WP 1	We have built a breadboard based pair photon source. A 3mW diode laser source has been characterised and we find it suitable for pumping parametric downconversion. Using a 3mm Type I BBO crystal we obtain coincidence rates of 4.5kHz with 15% detection efficiency into 9um core (three-mode) fibre We expect to optimise to better than 25% efficiency. A 5mm type II crystal and 2.5mm compensator crystal have been purchased but problems with diode laser has delayed measurement of entangled photons. Collaboration with P04 on novel PPLN pair photon sources and P04/P06 on developing GaAs waveguide sources of photon pairs.
WP6	200m, 1.2km and 1.9km and 23.4km trials sites identified. A free space key exchanged is planned this year. Trials of faint pulse systems (to 1.9km and 23.4km) are reported in the EQCSPOT consortium. Although not directly relevant to QuComm these trials will provide a sound basis for entangled state trials in year 3. The software developed for key sifting and error correction are certainly applicable.

Deliverables due this period		
Deliverable number	**Title of Deliverable**	**Status (Draft Final, Pending)**
D16	Progress towards an entangled state free-space quantum cryptography system	Final

Dissemination actions (articles, workshops, conferences etc.)
Co-organisers of the QUICK conference. Editors of Special Issue of Journal of Modern Optics: JMO 48 (13) 2001, Technologies for Quantum Communications. 3 papers from QUCOMM work included. Exhibitors at Dusseldorf IST Exhibition, Dec 2001 with EQCSPOT & QUIPROCONE.

Deviations from the planned work schedule/reasons/corrective actions/special attention required
Deliverable D16 was slightly delayed to TO+15. We expect a delay of a two months in preparing entangled state experiment due to diode laser failure.
Planned actions for the next period
WP6: Free space key exchange experiment (collaborations with P02,P06). WP4: Studies of quantum logic arrangements. WP1: High brightness three photon source experiment in collaboration with P04. Experimental testing of counter-propagating 1.55um GaAs source in collaboration with P04 and P07