



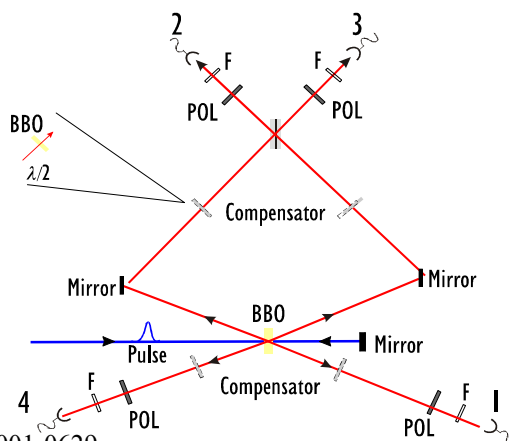
QuComm

IST-1999-10033

Long Distance Photonic Quantum Communication

Periodic Progress Report N°3, Deliverable D7

Covering period 1.1.2001-30.6.2001



Report Version: 1

Report Preparation Date: 2001-0629

Classification: Public

Contract Start Date: 2000-01-01

Duration: 36 months

Project Co-ordinator: Associate 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, Defence Evaluation and Research Agency, 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

TABLE OF CONTENTS.....	2
EXECUTIVE SUMMARY.....	3
WORK PROGRESS OVERVIEW	4
WP 0 MANAGEMENT, DISSEMINATION AND TAKE UP OF RESULTS	6
WP1: ENTANGLED STATE SOURCES.....	7
DELIVERABLES	7
MILESTONES	7
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	12
WP 2 QUANTUM STATE ANALYSERS.....	13
DELIVERABLES	13
MILESTONES	13
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	13
WP 3 ENTANGLEMENT BASED QUANTUM CRYPTOGRAPHY	14
DELIVERABLES	14
MILESTONES	14
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	16
WP 4 – TELEPORTATION OF ENTANGLEMENT.....	16
DELIVERABLES	16
MILESTONES	16
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	17
WP5 : MULTI-MODE & MULTI-STATE QUANTUM COMMUNICATION	17
DELIVERABLES	17
MILESTONES	18
<i>This milestone has not yet been achieved.....</i>	<i>18</i>
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	18
WP6 : FIELD DEMONSTRATIONS	19
DELIVERABLES	19
MILESTONES	19
FURTHER FIRST HALF YEAR RESULTS OF YEAR TWO AND RESEARCH IN PROGRESS.....	19
APPENDIX 1: PUBLICATIONS OF FIRST HALF YEAR OF YEAR TWO.....	20
JOURNAL PUBLICATIONS	20
CONFERENCES	21
APPENDIX 2- DELIVERABLES TABLE.....	23

Executive summary

The work in the first half of the second year of the QuComm project has progressed according to plan.

Among technical highlights we like to mention in particular

- The work of Oxford and Vienna on quantum error filtering/purification (presented in PRA and Nature), and of KTH and GAP on multilevel quantum cryptography
- 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 1.9km and DERA up to 1.2 km. 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 succesful organization of the QUICK conference by KTH, DERA and Philippe Grangier of QuiCov and S4P. The conference attracted most of the prominent group involved in quantum communication, notably quantum cryptography, and gave an excellent overview of the international state-of-the-art.

Concerning the dissemination and use of results, a number of publications and conference presentations (invited talks, regular talks, posters) where presented by QuComm members.

Overall, the work follows the original project plan well, with mostly no delays in milestones and deliverables expected.

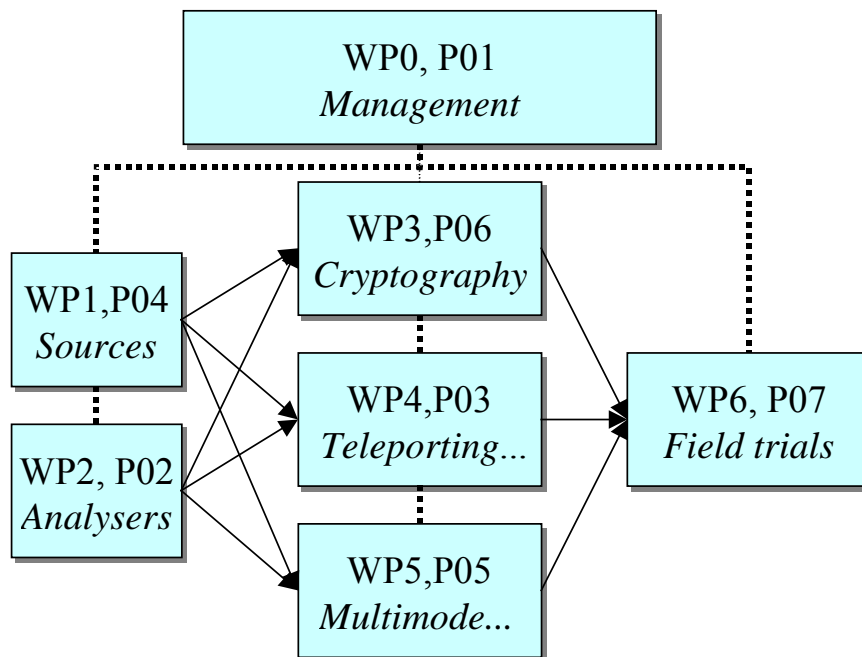
Work progress overview

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 the first part of year two has been

- To begin to use the developed user-friendly sources of entangled states. 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 maintain momentum in the work



*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 :

<i>Deliverables & Milestones</i>			
	Originally	Actual	Comment
Work-package	Planned	Status (when reached)	
WP0			
Deliverables	D7 (T0+18)	D7 (T0+18)	
Milestones	No milestones		
WP1			
Deliverables	D11 (T0+18)	D11 (T0+18)	
Milestones	M3 (T0+12) M4 (T0+18) M5(T0+18)	M3 (T0+18) M4 (T0+18) M5(T0+18)	M3 partly met M4 partly met M5 met
WP2			
Deliverables	D15(T0+18)	D15 (T0+18)	
Milestones	M11(T0+18) M12(T0+18) M13(T0+18)	M11(T0+18) M12(T0+18) M13(T0+18)	M11 not met M12 not met M13 partly met
WP3			
Deliverables	No deliverables		
Milestones	M14 (T0+12)	M14 (T0+18)	M14 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	M22 (T0+18)	M22 (T0+18)	M22 not met
WP6			
Deliverables	No deliverables		
Milestones	No milestones		

WP 0	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.

P01: 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 of GAP, took place in 2000, and was mentioned in the 2000 annual report. At KTH, A. Karlsson was also awarded a six year grant (one of 20 from all fields of science) on Quantum Information Technologies from the Swedish Foundation of Strategic research- SSF. Two Post-Docs and a graduate student, who will be engaged in the QuComm project work, will be hired. On the management side, KTH also very late submitted the cost claims for year one.

P01 & P08: 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** as responsible for public relations and secretary. We believe the conference was quite successful, but it took much more time than anticipated to organise the meeting. At the conference, we had attendance from all the groups of QuComm, and we also took the opportunity to organise a small meeting to discuss the project progress.

P02: Worked on and submitted as a coordinator a proposal for a research training network "PEQI- Photonic Entanglement and Quantum Information". This network, if accepted, will be important to help to solve the issue of finding good postdocs and provide adequate training in the area of QuComm.

P03: We have written a review article for the "Entangled Photons Cryptography", which appeared in a well renowned German computer magazine: Thomas Jennewein, Gregor Weihs, Anton Zeilinger, "Schrödingers Geheimnisse", c't, No. 6/2001.

P05 and P06: 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. Discussions are ongoing concerning contractual issues.

Concerning the consortium agreement, this is yet under discussion. The latest version read and approved by most partners is currently with the legal contact person of the coordinator. Due to some personnel changes the legal section at KTH, it has taken some time to have all procedures concerning R&D contracts running again.

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 other work-packages. The collaboration between various nodes 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:

Deliverables

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

Delivered on time.

Milestones

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

This milestone has been partly achieved by TH LCR (P07):

Twin photon source based on parametric fluorescence in a semiconductor laser

The purpose is to develop an electrically pumped semiconductor laser of direct generation of twin photons at 1.55 microns. During the first 12 months, we have worked on the design of such a source. The most appropriate semiconductor material has been selected, and three different structure schemes have been studied. This work has also led to the proposal of an original source of counter propagating photons generated in a semiconductor waveguide.

This source is based on the parametric down conversion of an internally generated laser mode due to the quadratic nonlinearity in bulk III-V semiconductors . The design of the structure has to take into account the following requirements :

- The quantum well laser wavelength has to be between 770 and 775 nm.
- The quantum well laser emission must be TE polarized.
- The quantum well laser emission must be on a high order mode of the waveguide (second order or third order)
- The phase matching condition for the intracavity parametric fluorescence must be fulfilled, with a parametric fluorescence at 1.55 microns in the fundamental mode of the waveguide.
- The nonlinear overlap integral between the interacting modes (fundamental mode at 1550 and higher order mode at 775 nm) has to be optimized.
- The efficiency of the transport of carriers (electrons and holes) toward the quantum well has to be considered, especially because high barriers are necessary for the waveguide design.

For the sake of simplicity of the technological process, optically pumped laser was initially developed, an electrically pumped device is going to be designed.

From the beginning, the design had to take into account all the needs of an electrically pumped system. In particular, the compatibility with a doped structure was considered.

Initially, different possible structures were considered: a) A « step » waveguide, with the laser mode on the second order mode of the waveguide; b) An asymmetric « double core » waveguide, with the laser mode on the second order mode of the waveguide; c) A symmetric « double core » waveguide, with the laser mode on the third order mode of the waveguide.

The latter solution was preferred because of the much better overlap between the pump (laser) mode and the signal modes (at $1.55\mu\text{m}$), which is a strict requirement for nonlinear conversion efficiency. The structure is thus *imposed by the need to obtain the modal phase matching* between the interacting modes, i.e. $k_{\text{pump}} = k_{\text{signal}} + k_{\text{idler}}$, *preserving a good mode overlap*. The sample structure meeting those requirements is illustrated in Fig. 1; the waveguide double core is composed by two $\text{Al}_{0.25}\text{Ga}_{0.75}\text{As}$ layers (A), two $\text{Al}_{0.50}\text{Ga}_{0.50}\text{As}$ spacer layers (B), and a $\text{Al}_{0.11}\text{Ga}_{0.89}\text{As}$ 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.

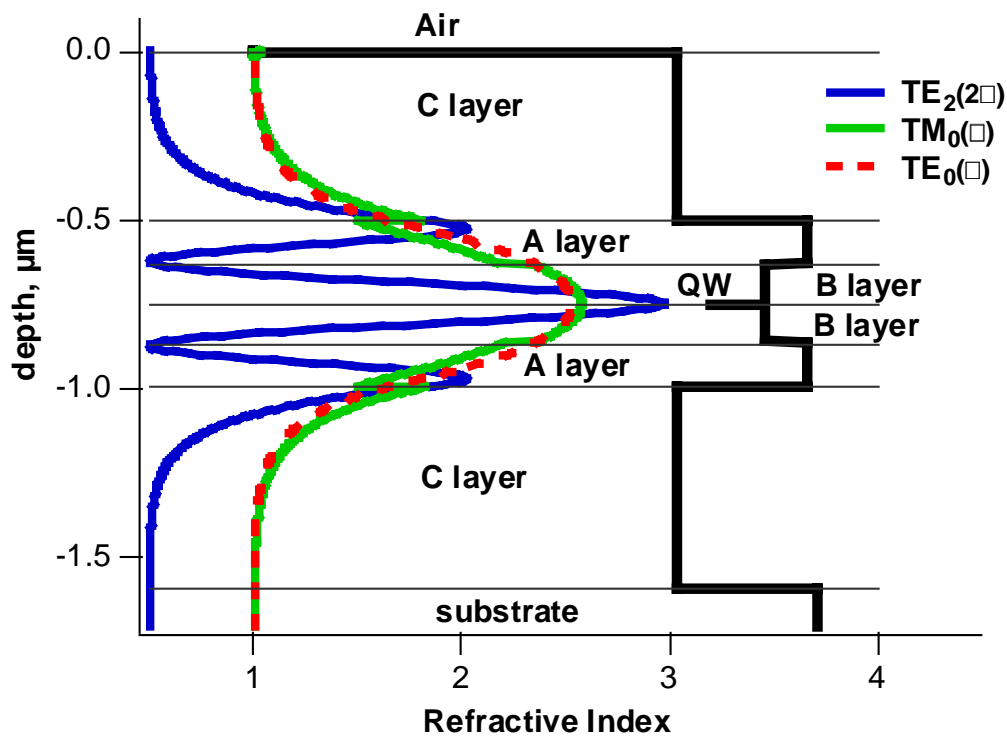


Figure 1

The optimisation of mode overlap in the nonlinear interaction need the introduction of the spacer layer, introducing a barrier separating the $\text{Al}_{0.25}\text{Ga}_{0.75}\text{As}$ layer (A), where the carriers are generated by optical pumping, from the quantum well. This results in a potential degradation of the carrier transport toward the quantum well. However, simulation of the carriers transport in this structure confirmed the possibility of yielding the required emission on the third order mode with a reasonable pump threshold power

Photoluminescence, lasing operation and far field were characterised before looking at the nonlinear operations. A typical PL spectrum at room temperature is shown in Fig. 2 (dashed line) by using a low power CW He:Ne laser. The peak at 770 nm is due to the

recombination transition between the first excited state of the conduction band electrons to the first excited state of the valence band heavy holes of the quantum well, while the peak at 1.706 nm is due to the luminescence of the absorbing layer. At room temperature, the luminescence peak of the QW is twice as stronger as the 706 nm peak, meaning that more than 50 % of the carriers generated in the absorbing layer recombine in the QW, the efficiency of transport of carriers (electron and holes) toward the QW is quite high thus despite of the existence of the spacer layer.

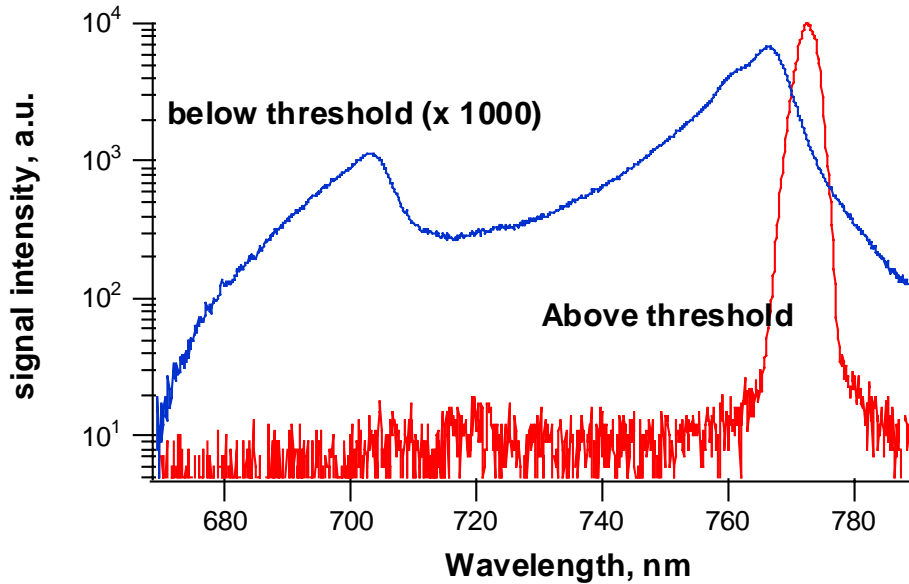


Figure 2

Waveguides ridges of 10 μ m have been etched chemically and samples as long as 1 mm were cleaved. The samples were optically pumped by a pulsed Nd :YAG laser (10 Hz, 6 ns). Laser emission from the QW was observed between 772 and 775 nm at room temperature (shown by the solid line in Fig. 2). The FWHM of the laser peak is around 2 nm at room temperature and around 1 nm at low temperatures. The measured laser threshold was 1.89 MW/cm² at 290 K and 0.25 MW/cm² at 20 K for L=1.44 mm cavity. A collimated beam was used to get rid of alignment of the beam with the waveguide, thus several laser were operating at the same time. Threshold pump power versus the sample temperature are shown in Fig. 3. A characteristic temperature T_0 of 117 K was estimated by exponential fit. This value is comparable to III-V lasers. Laser peak position versus temperature is also shown in Fig. 3 and it follows the theoretically calculated (by using a simple model assuming infinite barriers) energy of the transition $e_1 \rightarrow hh_1$ in the QW. The power input – output curves at different temperatures are also plotted in figure 4.

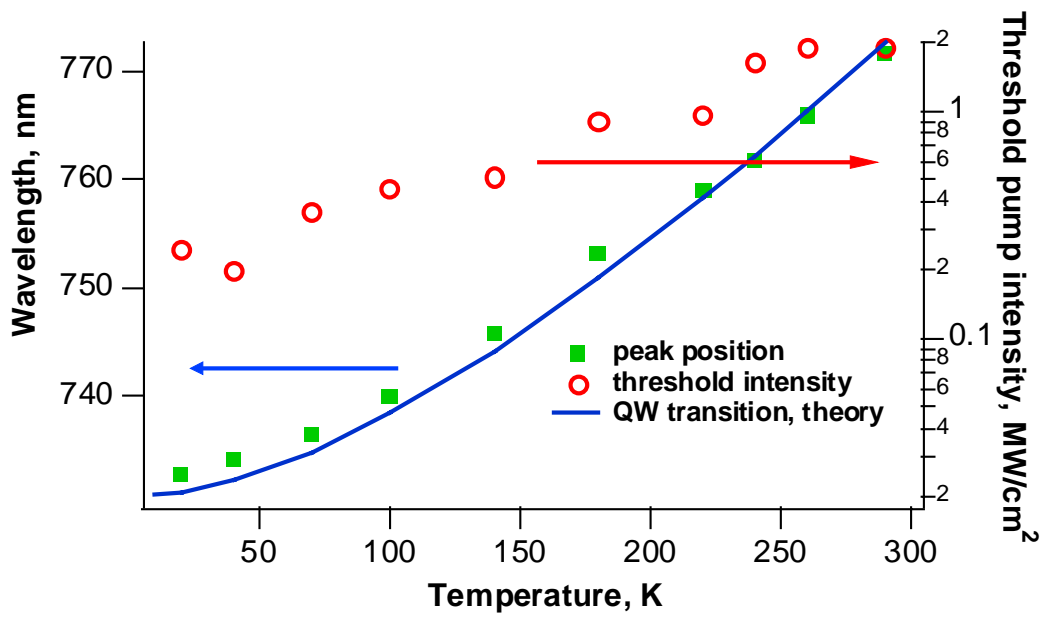


Figure 3

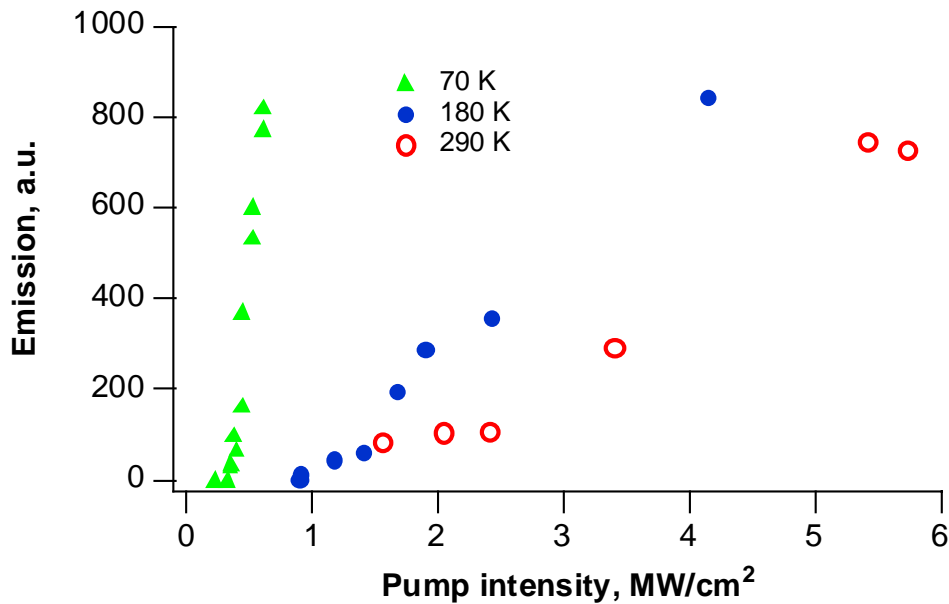


Figure 4

To check that the emission is actually on the 3rd order mode, the far field of the laser emission was measured by an angular scan on the vertical plane of the waveguide. Fig. 5 shows the angular dependence of the far field (points), compared the calculated farfield corresponding to the 3rd order mode. The agreement is qualitative, and, in particular, the minima at about 25° is the “signature” of the 3rd order mode. Quantitative discrepancies are due to the use of a microscope objective to collect enough power into the detector (the duty cycle is extremely low), and to the difficulty of measuring at very wide angles.

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. Precision in epitaxial growth, uncertainty in the optical constants of III-V alloy are such that it is not possible to obtain a nominal sample, i.e. simultaneously emitting at 775 nm and phase matched at that wavelength and at room temperature. A Peltier cell or even a cryostat need to be used. On the other hand, efficient collection of light generated by this source is difficult, due to the huge numerical aperture of the waveguide. Microscope objectives are required, which makes it complicated to use with a cryostat. Finally, the expected twin photon signal is extremely low, in this optically pumped configuration. In fact, pulsed pumping is imposed by the fact the threshold is quite high, making the average power level of the QW laser quite low. A time resolved detection system using quite sensitive and fast detectors is required. However, all these difficulties can be solved.

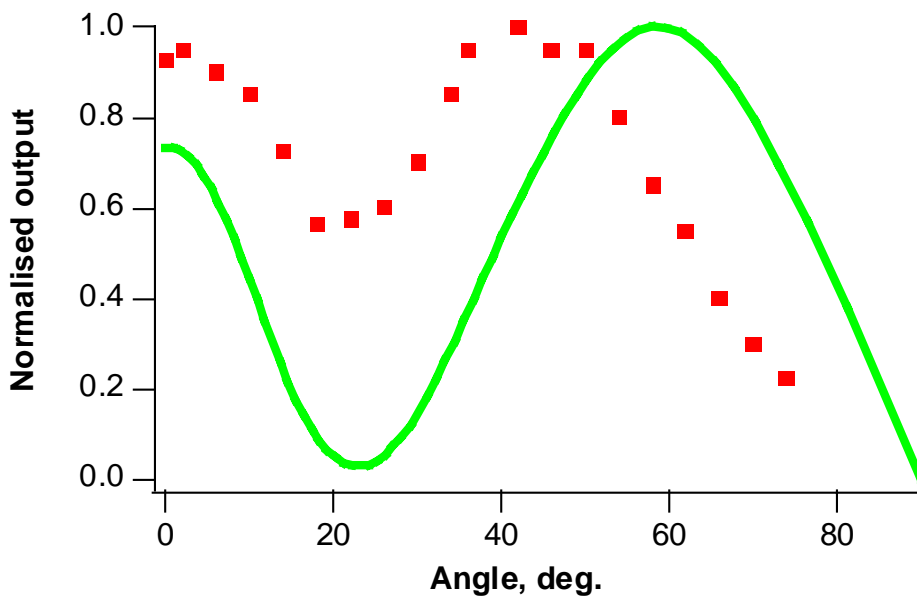


Figure 5

Thanks to all the information collected from experiments of the optically pumped sample, the design of an electrically pumped source is now in progress.

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)

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 800/800nm but research is still in progress to complete the 800/1500 and 1500/1500 breadboard systems. At **P05**, 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).

Further first half year results of year two and research in progress

WP1.1 Develop bright sources of entangled pair photons

Concerning down-conversion to telecom wavelengths, this was the work of **P01** and **P05**. Observation of down conversion from 514nm to the idler at 780nm (the corresponding 1500nm photons are still to be observed) was done by **P01**. The work of **P02** and **P05** is reported in D11. In WP 1.1, **P06** have been conducting Investigations of ways to improve the entanglement purity over large collection angles. Finally, concerning non-linear crystal based sources **P08**, **DERA** made work on the optimisation of free-space emission of entangled photons and study of photon pair creation using a violet diode laser.

WP1.2 Generation of arbitrary two-photon states

P03 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-conversion 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

P04: Inspired by laser operation, Oxford has addressed the question of whether stimulated emission into polarization entangled modes can be achieved. In ref. 13, the new source is described and the state produced by stimulated emission of the singlet Bell state is analysed in ref. 14. Such an entangled-photon laser could be a very important tool for studying “mesoscopic quantum entanglement” bridging the gap between discrete and continuous variable quantum information.

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

No work to be reported.

WP 2 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, ref. 1, 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)

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

This milestone has not been achieved.

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

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

Further first half year results of year two and research in progress

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

The full implications of the schemes, ref. 1 and 14, 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.

WP 3 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. During the first year considerable progress was made by many partners setting the stage for early field trials.

Deliverables

D16 (T0+12): Report on free-space entanglement enhanced quantum cryptography (P04, P06, P08)

A report was submitted as D16.

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: Using polarization-entangled photons, we have implemented the “six-state” quantum cryptography protocol, whereby each photon is measured in one of *three* bases. 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.

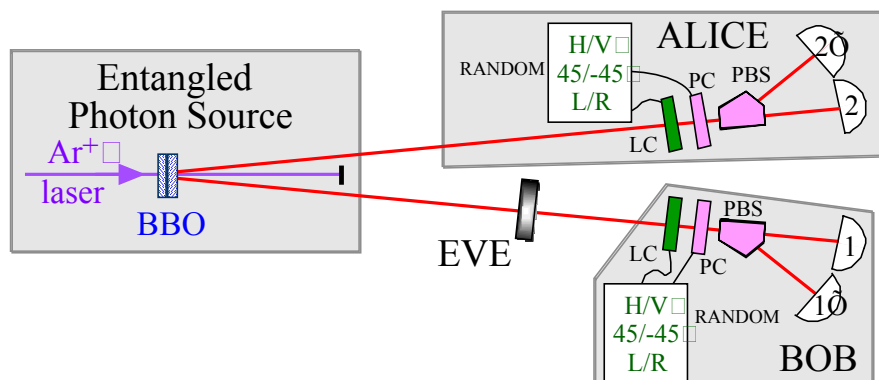


Fig. 1. Experimental setup for implementing the six-state cryptography protocol with polarization-entangled photons.

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 which 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).

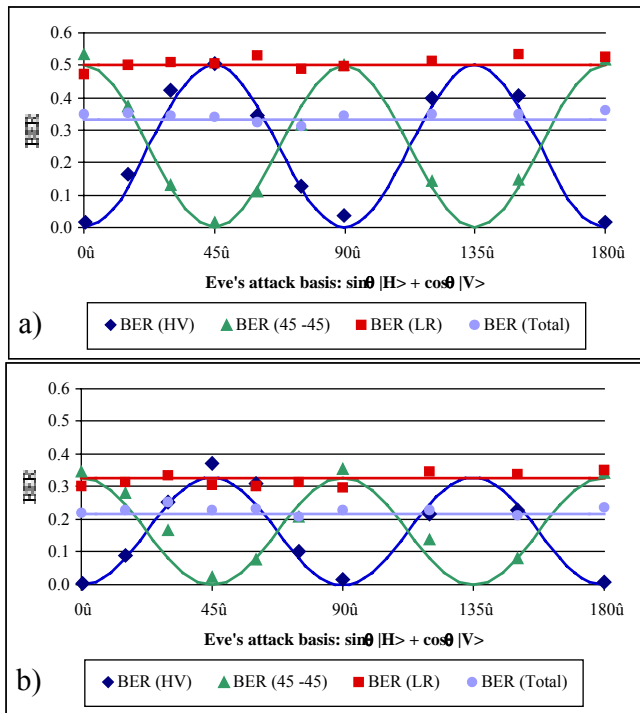


Fig. 2. Effect of an intermediate eavesdropper (measuring in a linear polarization basis) on the induced bit error rates in the various bases, and on the total BER. a). Eve simulated by making a strong measurement of the polarization on every photon. b). A partial quantum non-demolition attack, simulated 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 [1]. Second, the entangled photons have the feature that they automatically allow one to test the quality of the source [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.

[1] N. Lutkenhaus, “Security against individual attacks for realistic quantum key distribution”, Phys. Rev. A **61**, 052304-1-10 (2000).

[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.

Further first half year results of year two and research in progress

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.

WP 4 – 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 is submitted together with this report

Milestones

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 [1], 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, and 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, although 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 [2,3].

Beyond, the aim of M17 is to demonstrate a violation of a Bell inequality while closing the locality loophole as has been done by UNIVIE in 1998 over a distance of 360 meters [4]. 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.

- [1] G. Ribordy, J. Brendel, J.D. Gautier, N. Gisin and H. Zbinden. Phys. Rev. A 63, 012309 (2001)
- [2] N. Gisin and B. Huttner. Phys. Lett. A 228, 13 (1997)
- [3] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres. Phys. Rev. A 56, 1163 (1997)
- [4] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger. Phys. Rev. Lett. 81, 5039 (1998)

Further first half year results of year two and research in progress

The activities in WP1 by P02, P03, P04, and P05 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. GAP constructed two sources, generating one pair per source, however, two pairs (from different sources) at the same time. Two fiber-optical interferometers working at 1.5 μm wavelength have been build and tested with classical light. Furthermore, they are now employed to characterize the output light from the downconversion sources. First Franson-type tests with photon pairs at 1.3 and 1.5 μm wavelength (from the same source) have been performed, yielding visibilities of above 70%.

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. Two future milestones have already been realised, scheduled for T0+24 and T0+30, respectively. These are the demonstration of quantum secret sharing **M23 (T0+24)** by **P05 (GAP)** and the demonstration of entanglement purification **M24 (T0+30)** by a collaboration of **P05 (GAP)** and **P06 (LANL)**. 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

Further first half year 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** 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.

P05 (GAP) is preparing an experiment to investigate the impact of distance on non-maximally entangled energy-time Bell states using quantum state tomography as developed for polarization entangled states.

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 first half year results of year two and research in progress

- **P03** are working on long distance teleportation: Hardware is being developed. Polarisation control scheme, source design, detectors, and registration electronics.
- **P04** and **P08** 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.

Appendix 1: Publications of first half year of year two

Journal publications

1. D. Bouwmeester, “*bit-flip error rejection in optical quantum communication*”, Phys. Rev. A 63, 040301 (2001), also at Los Alamos e-print archive, <http://xxx.lanl.gov/abs/quant-ph/0006108>
2. P. G. Kwiat, S. Lopez, A. Stefanov, and N. Gisin, “*Experimental entanglement distillation and ‘hidden’ nonlocality*”, Nature **409**, 1014 (2001).
3. M. Bourennane, A. Karlsson, and G. Björk, “*Quantum cryptography using multilevel encoding*”, Phys. Rev. A. 64, 012306 (2001).
4. Lamas. C. Mikkelesen, J. Howell D. Bouwmeester, “*Interference enhanced entanglement: concept of an entangled photon laser*”, submitted to PRL.
5. I. Ghiu, M. Bourennane, and A. Karlsson, “*Transformations between inequivalent classes of three particle entangled states*” Submitted to Phys. Lett. A.
6. M Bourennane, A. Karlsson, J. P. Ciscar, and M. Mathes “*Single photon counters in the telecom wavelength region of 1550 nm for quantum information processing*”, Accepted for publication in J. Mod. Opt.
7. M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. Cerf, “*Quantum key distribution with multilevel encoding: Security Analysis*” submitted, also at Los Alamos e-print archive, <http://xxx.lanl.gov/abs/quant-ph/0106049>.
8. B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, *Universal unitary gate for single-photon 2-qubit states*, Phys. Rev. A, **63**, 032303 (2001).
9. Ch. Kurtsiefer, M. Oberparleiter, H. Weinfurter, *High efficiency entangled photon pair collection in type II parametric fluorescence*, submitted to PRA.
10. A. Beige, B.-G. Englert, Ch. Kurtsiefer, H. Weinfurter, *Cryptography with single-photon two-qubit states*, submitted to PRL.
11. C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, *Generation of correlated photon pairs in type-II parametric down conversion -- revisited*, submitted to Journal of Modern Optics,
12. M. Bourennane, “*Long-Wavelength Quantum Cryptography, Single-Photon Detection and Quantum Entanglement Applications*”, Ph.D. thesis, KTH, May. 28, 2001.
13. Antia Lamas-Linares, Christian Mikkelsen, John C. Howell, D. Bouwmeester, “*Interference enhanced polarization entanglement and the concept of an Entangled-Photon Laser*”, submitted to PRL November 2000, quant-ph/0103056
14. 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
15. 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), quant-ph/0011037.
16. Thomas Jennewein, Gregor Weihs, Anton Zeilinger, “*Schrödingers Geheimnisse*”, c’t, No. 6/2001.
17. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “*Quantum Cryptography*”, quant-ph/0101098, submitted to Rev. Mod. Phys.
18. Pan, J.-W., Simon, C., Brukner, C. & Zeilinger, “*A. Feasible entanglement purification for quantum communication.*” Nature 410, 10671070 (2001)

19. 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.

Conferences

1. W. Tittel, “Quantenkryptographie über große Entfernungen: von der Idee zur Anwendung” presentation at *Siemens*, München, Germany, February 19th, 2001.
2. H. Zbinden, “Cryptographie Quantique”, at *Neuvième Séminaire Rhodanien de Physique*, « *Physique des états enchevêtrés* » in Dolomieu-France, February 25- March 3, 2001.
3. Stefanov, “Quantum Cryptography”, at 9. *SSOM Fachkurs “Optical Communication”* in Engelberg/Switzerland, March 25 – 29, 2001.
4. N. Gisin, “Quantum cryptography: from basic physics to applications”, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
5. H. Zbinden, “Faint laser versus entangled photons Quantum Key Distribution”, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
6. W. Tittel, “Time-bin entangled photon pairs & applications in quantum cryptography”, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
7. S. Tanzilli, “Highly efficient photon-pair source using PPLN waveguide”, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
8. Stefanov et al., “Plug & Play long distance quantum key distribution prototype”, poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
9. S. Tanzilli et al., “Highly efficient photon-pair source using PPLN waveguide”, poster, at *QUICK* workshop in Cargèse-France, April 7-13, 2001.
10. V. Scarani, “Quantum cryptography, from foundations to application”, at symposium Schrödinger, Zürich, April 4th, 2001.
11. N. Gisin, “Entanglement, from paradoxes to applications”, symposium Schrödinger, Zürich, April 4th, 2001.
12. Paul Kwiat, "Entangled Photons for Quantum Information", Plenary Talk at the APS 2001 April meeting, Washington D.C.
13. Paul G. Kwiat, “101 uses for a Schrödinger kitten-embryo”, colloquium at Argonne National Lab, May 11, 2001.
14. Paul G. Kwiat, “Entangled Photons for Quantum Communication”, 7th Annual Symposium on German-American Frontiers of Science, Bad Homburg, Germany, June 7-10, 2001.
15. Paul G. Kwiat, “Experimental six-state quantum cryptography”, International Conference on Quantum Information (ICQI), Rochester, New York, June 11-14, 2001.
16. R. J. Hughes, *Free-space quantum key distribution*, invited talk at the “Quantum Interference and Cryptographic Keys” conference, Cargese, Corsica, France, April 2001
17. M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and H. Zbinden, “*Quantum key distribution using multilevel encoding: Security Analysis*” poster at Quantum interference and cryptographic keys: novel physics and advancing technologies conference, Cargese, April 2001.
18. M. Bourennane, A. Karlsson, M. Mathes, and A. Hening, “*Single-photon counters in the telecom wavelength region of 1550nm for quantum information applications*”, accepted for presentation at CLEO Pacific Rim 2001, Chiba, Japan, July 15-19, 2001.
19. I.Ghiu, M. Bourennane, and A. Karlsson, “*Transformations Between Inequivalent Classes of Three Particle Entangled States*”, poster presented a EUROPEAN HIGH LEVEL SCIENTIFIC CONFERENCE, "QuEnt" Quantum Entanglement and Quantum Information”, Les Houches, France, March 19-30, 2001
20. A. Karlsson, M. Bourennane, and D. Ljunggren, “*Long Wavelength Quantum Cryptography* ”, Invited presentation at the Quantum interference and cryptographic keys: novel physics and advancing technologies conference, Cargese, April 2001
21. A. Karlsson, “*Technologies for Quantum Communication*”, invited talk at the “Workshop on (Not Only) Solid State Quantum Computing”, Institute of Physics, Polish Academy of Sciences, Warsaw, Poland, April 26-29, 2001
22. A. Karlsson, M. Bourennane, D. Ljunggren, F. Nilsson, J. Pena Ciscar, and M. Mathes, “*Long Wavelength Quantum Cryptography and Single Photon Technologies* ”, Invited presentation at International Conference on Quantum Information (ICQI), Rochester, New York, June 10-13, 2001
23. A. Karlsson, M. Bourennane, D. Ljunggren, F. Nilsson, J. Pena Ciscar, M. Mathes, W. Fransson, A. Hening, F. Gibson, and P. Jonsson, “*Quantum Information and Single Photon Technologies* ”,

- Invited presentation at Swedish- Japanese Quantum Nanoelectronics workshop- QNANO, Stockholm, Sweden, June 13-16, 2001
24. N. Gisin at CLEO/EQELS: “*Quantum Key Distribution : Faint laser pulses vs. entangled Photons*”, invited talk, May 10, 2001
 25. N. Gisin at GDR : “*La Cryptographie Quantique* », présentation invitée dans le cadre du lancement de ce nouveau programme français, Mai 18, 2001
 26. N. Gisin at University of Barcelone,, “*Quantum Key Distribution : Faint laser pulses vs entangled photons*”, colloquium May 31, 2001
 28. N. Gisin at CERN: “Quantum Key Distribution : Faint laser pulses vs. entangled photons”, invited talk within the OPAL-project meeting, June 13, 2001
 29. G. Ribordy et al. at CERN :“Single-Photon Detection at Telecommunication Wavelengths: Performance and Applications to Classical and Quantum Communications”. June 5th, 2001
 30. H. Zbinden et al. at CEA Grenoble, “Cryptographie quantique expérimentale”. June 12th, 2000.
 31. H. Zbinden et al. at CLEO-Europe, “Experimental Quantum Cryptography”, June 20st, 2001

Appendix 2- Deliverables Table

DELIVERABLES TABLE

Project Number: *IST-1999-10033*
 Project Acronym: **QuComm**
 Title: *Long Distance Photonic Quantum Communication*

Del. No.	Rev	Title	Type ₁	Classi ²	Due Date	Issue Date
D6		Joint QuComm IST FET workshop	O	Pub	T0+18	
D7		Half year progress report year 2	R	Pub	T0+18	
D11		Diode laser pumped user friendly non-linear crystal source for entangled states	R	PP	T0+18	
D15		Linear quantum logic and quantum error correction	R	Pub	T0+18	
D18		High fidelity qubit teleportation	R	Pub	T0+18	
D20		Multimode, multiparticle entanglement protocols	R	Pub	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