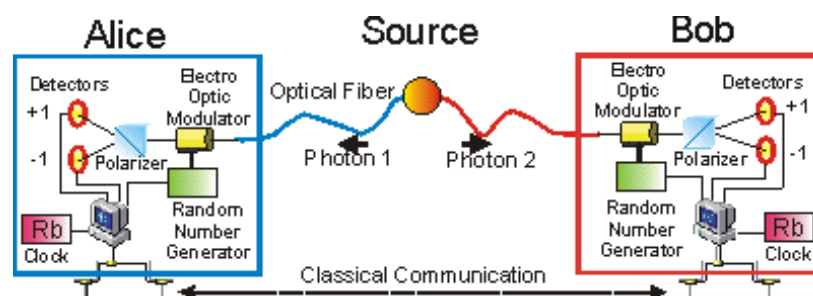


IST-1999 100 33 QuComm

Long Distance Photonic Quantum Communication



Deliverable D4

Half year progress report

Reporting period: from 2000-01-01 to 2000-06-30

Dissemination Level: Public

Prepared by

**KTH, LMU, EXPUNIVIE, Oxford, GAP,
LANL, TH LCR, DERA**

For further information on this report contact
A. Karlsson, KTH, email:andkar@ele.kth.se



1. Executive summary

The work in the QuComm project has started well. The project was launched off with a kick-off meeting at KTH Kista, Feb. 18-19, 2000. Most groups, however, had already started working earlier on the project work topics either themselves or in collaborations with other partners in the project. Among technical highlights we like in particular to mention:

- The realisation of time-bin entangled sources by P05 and their subsequent use in experiments on entanglement quantum cryptography and quantum secret sharing using pseudo GHZ-states.
- The entanglement based quantum cryptography demonstrator realised by P03 in collaboration with P02, including also the software for error correction and privacy amplification.
- The work of P05 and P06 on the investigations of the robustness of entanglement and entanglement purification.
- The free space quantum cryptography trials of P06 up to 1.6km. While not yet using entanglement schemes the trials are very important with respect to investigation quantum cryptography under field like situations.

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

2. Introduction

In the last few years, there has been a remarkable progress in the field of *Quantum Information Processing and Communication* - QIPC. QIPC promises new capabilities in computation and communication, for instance with fundamentally secure quantum cryptography systems, with quantum logic for reduced computational complexity in factoring and sorting, and with protocols such as quantum teleportation exploring entangled quantum states lacking classical counterparts. The **QuComm** project has the objectives

- To scale experimental quantum communication protocols, notably quantum teleportation, entanglement swapping and entanglement enhanced quantum cryptography, towards longer distances in particular to explore entangled states of multiple photons.
- To demonstrate novel quantum communication protocols. On the one hand, decoherence and noise effects will be minimised by implementing various methods for error correction in quantum transmission.
- 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.

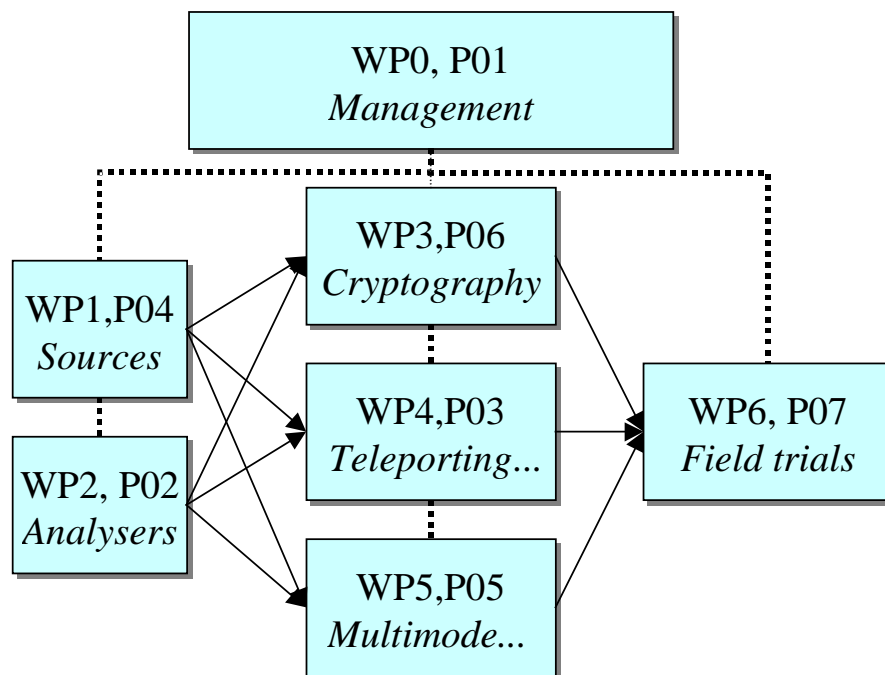


Table:
Division of work in workpackages.
 Partners are
 P01=KTH
 P02=LMU
 P03=EXPUNIVIE
 P04=Oxford
 P05=GAP
 P06=LANL
 P07=TH LCR
 P08=DERA

The work is divided into six workpackages (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 multimode and multistate protocols. In WP 6 the assembled work in earlier workpackages will be used to conduct trials outside the laboratory setting. The report will describe the work as divided per workpackage.



3. Description by workpackage

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.

On February 18-19 P01 (KTH) arranged the Kick-Off Meeting of the project at KTH Kista, Sweden, (P02,P03,P04,P05,P07,P08 participants, P06 sent all material for presentation and participated electronically). The meeting was very productive and there were many discussions and openings for new collaborations. In conjunction to the meeting a visit to ACREO AB (the joint company of the former Institute of Optical Research and the Swedish Industrial Microelectronics centre) was arranged. At the meeting we also discussed the setup of an industrial advisory group which is in progress.

The project Internet site (deliverable D2, T0+3) was officially launched in the beginning of February. We had intense, but fruitful discussions on what exactly to write in order to be both popular in presentation, yet precise in our statements.

An application was submitted to NATO/EURESCO for the arrangement of a Euroconference "*Quantum interference and cryptographic keys: novel physics and technologies (QUICK)*" with P08 as treasurer and P01 as responsible for public relations and secretary. This conference is the deliverable D6 of QuComm. Currently in June 2000, a first WWW site of QUICK (is under development).

There have been a few industrial contacts and reports in media of the work performed in the project. P01 has made presentations at CELO communications (a company dealing with Internet security), and also had visits from Perkin Elmer (former EG&G) and Ericsson Microelectronics (in both cases concerning detectors). P03 had a lab visit by William C. Topp of tvn (a venture capital company). Mr. Topp was interested in the state of quantum communication experiments. He said that they realise that there may be great potential in qc in the mid-range future. Concerning popular science, A Scientific American article by Anton Zeilinger appeared in the April 2000 issue.

With regards to media contacts, the Swedish science program NOVA (Swedish National TV Channel 1) visited P01 to make a 10-minute feature on quantum cryptography. The long distance teleportation project of P03 will be accompanied from now until completion by a journalist (and photographer) of a very serious Austrian weekly journal (FORMAT). On a first meeting Thomas Jennewein presented a very detailed schedule and workplan for this project.



For P03, P02, P05 and P06 there has also been considerable media coverage on quantum cryptography mentioning all three cryptography papers:

Source	Location	Date	Title
American Institute of Physics, Physics News Update #480	www.aip.org	24.04.00	Exploiting Quantum "Spookiness" To Create Secret Codes
American Institute of Physics, Physics News Graphics	www.aip.org	24.04.00	Image: Exploiting Quantum "Spookiness" to Encrypt an Image
American Institute of Physics, News Release	www.aip.org	29.04.00	You'd Have to Break the Laws of Physics to Break This Code
Nature Science Update	www.nature.com	03.05.00	Top Secret
The New York Times	www.nytimes.com	03.05.00	In The Quantum World, Keys to New Codes
Intelligence Newsletter	www.intelligenceonline.com	04.05.00	Cryptography-Progress in Quantum Technology
Süddeutsche Zeitung	www.sueddeutsche.de	09.05.00	Verschränkt und verschlüsselt
NRC Handelsblad, NL	www.nrc.nl	06.05.00	Onkraakare codes
Physics Today (Physics Update)	www.aip.org	06/2000	Quantum key distribution
Opto & Laser Europe	www.olemag.com	06/2000	R&D: Optical encryption secures transmission of data
Physikalische Blätter	www.wiley-vch.de	06/2000	Geheime Schlüssel mit verschränkten Photonen
Science & Vie	www.science-et-vie.com/actu2.html	07/2000	Discrètion absolue ... Entre voisins
Weltwoche	www.weltwoche.ch	06/2000	

In the June 2000 Physic Today issue, the three entangled state quantum key distribution experiments of P02 &P03, P05 and P06 are also mentioned in the "Physics Update" column.

WP 1 ENTANGLED STATE SOURCES

The objective of WP1 is to build the enabling quantum toolbox of compact and user-friendly sources of complex optical quantum states on demand, which are to be used in later WPs. During the six month reporting period considerable progress was made towards this goal. Most groups have had made progress independently, but crossflow of information has also taken place

WP1.1 Develop bright sources of entangled pair photons

- For telecom wavelengths 1330 and 1550nm, **P01** will develop a time-bin entangled source (similar to that of P05, but at 1550 nm) and have observed downconversion from 514 to the idler at 780nm, the signal 1500nm, will be found next. **P05** have constructed and tested a stable bulk interferometer for a fs time-bin-entangled n-photon-pair source. **P05** started to build the complete source based on the mentioned interferometer and parametric downconversion in a KNbO3 crystal pumped by a fs Ti:Sapphire laser. We theoretically investigated how to extend our ps time-bin-entangled photon-pair source as used in our crypto-experiment (PRL 84(20), 4737 (2000)) to create non-maximally entangled states.



- **P02** have observed first blue light from frequency doubled laser diodes (1 mW, 425nm). It is planned to enhance this output with a UV-build-up cavity, which was already demonstrated for 351nm from an Ar⁺ laser.
- **P04&P08** have been working on downconversion in periodically poled Lithium niobate (PPLN) started and very promising pair-photon creation in PPLN crystals has been observed). Work on periodically poled fibres completed, and started on periodically poled Lithium Niobate in collaboration with Oxford. The design of compact and portable entangled photon source for free space key distribution underway.
- **P06** have developed a source of ultrabright entangled pair photons which will be used in later WPs. Recently a systematic investigation was started of ways to improve the brightness, by which is meant the entanglement purity over large collection angles.
- The design work of the GaAs based photon pairs source at 1.55 microns of **P07** has made considerable progress. The requirements of the source have been precised during a visit of Dik Bouwmeester from **P04** at THOMSON-CSF LCR (wavelength of interest, power, etc). 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.

1) Most appropriate semiconductor material system.

In order to provide parametric fluorescence at 1.55 microns at degeneracy, the pump wavelength has to be around 775 nm. GaAsP/GaInP quantum wells and GaAs/AlGaAs quantum wells are possible for this purpose. GaAs/AlGaAs has the advantage of a better knowledge of the refractive indexes, which is a crucial point in the design. However, GaAsP/GaInP was preferred because of the higher quality of the Al-free lasers in this wavelength range.

Structures schemes.

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 polarised.
- 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 1.55 and higher order mode at 775 nm) has to be optimised.
- The efficiency of the transport of carriers (electrons and holes) toward the quantum well has to be considered, especially because high barriers are necessary.

Given these requirements, three possible structures have been designed:

- The first is a « step » waveguide, with the laser mode on the second order mode of the waveguide.

- The second is an asymmetric « double core » waveguide, with the laser mode on the second order mode of the waveguide.
- The third is a symmetric « double core » waveguide, with the laser mode on the third order mode of the waveguide. This solution presents a good non-linear overlap integral, but is very sensitive to variations of parameters. The two first solutions are shown in the figures. The final structure is under study.

2) EPR source in a waveguide. We have made experiments of surface emitting second-harmonic generation in semiconductor waveguides. Two pump beams (one TM and the other TE polarised) are counter propagating in a GaAs/AlGaAs waveguide. Two second harmonic beams (at 532nm in the experiment) are emitted on top of the waveguide, symmetrically with respect to the normal of the top surface. The angle of emission with respect to this normal is given by the waveguide birefringence. We propose now to perform the reverse experiment: To pump a semiconductor waveguide on its surface, and to observe the counter propagating emission of two signal and idler photons in the waveguide beams (one TM and the other TE polarised). In spite of the poor efficiency of the non-linear process (due to the very short interaction), the advantages of the method are the possibility to generate photons at 800 nm in the semiconductor (compared to 1.55 microns in the previous device), the simplicity of the technological approach, and the possibility of pig tailing directly the waveguide on both facets. This would lead to a very simple and compact fibered EPR source. Further work on the design will be done before the experimental implementation.

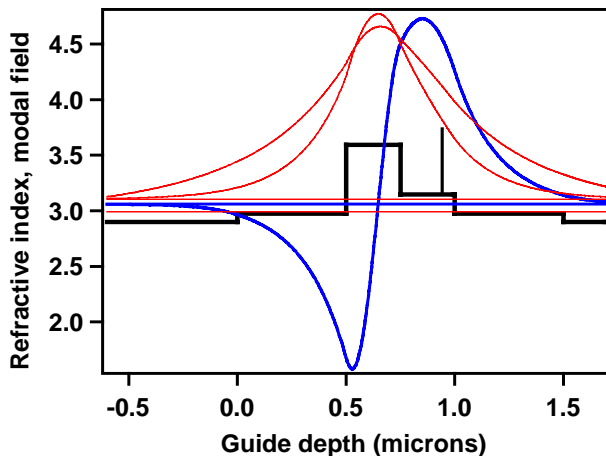


Figure 1: Example of « step » structure for the intracavity modal phase-matched quantum well laser OPO.

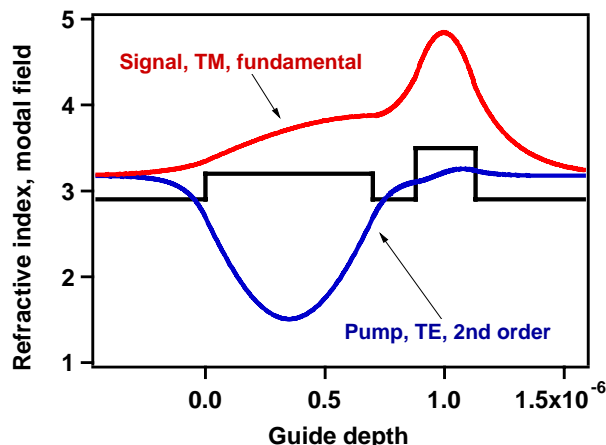


Figure 2 : Example of « double core » waveguide for the intracavity modal phase-matched quantum well laser OPO.

WP1.2 Generation of arbitrary two-photon states

- **P06** have in collaboration with Andrew White (University of Queensland) generated partially-mixed states, and have theoretically identified a new class of states that maximise the amount of entanglement for a fixed purity. A paper is in progress. We have begun investigating the methods to controllably produce arbitrary partially mixed and partially entangled polarisation states of two photons. In particular, we are identifying the necessary controls to adjust any of the 15 free parameters that define a given arbitrary density matrix.

WP1.3 Bright source of entangled multiphoton states

- **P02** is working on a pulsed source built on a MIRA laser, and the set-up of pulsed UV-source, 600mW, 390nm. In parallel **P04** and **P08** are working on Ar-ion modelocked laser for generation of GHZ (with mixing from weak coherent state started and have started work on Stimulated parametric downconversion work in Ti:Sapphire laser with regen amp. Work on this is also ongoing at **P03**, where a high yield 3-4 photon source based on Ti:Sapphire laser+ regenerative amplifier under study, this is of relevance for WP5. The regenerative amplifier system is running after many pump-laser problems, but there are still pulse-width considerations. New upconversion crystals have arrived. A publication on 3-state entangled systems is being prepared.

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

No work 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 workpackages.

- **P02** have been working on new coincidence count scheme on microproc. registers to be built (first tests done) . New detector mounts done with 4 fibre pigtailed SPCM avalanche diodes in single cooled block. A Bell state analyser will be built soon.
- **P03** have started building a fibre Bell state analyser.
- **P06 have for** two-photon tomography, made an analysis of the propagation of errors (both statistical, which is easy, and systematic, which is much harder), how they affect the derived density matrix, and how this in turn affects various measures like the Purity, the Entropy, the entanglement, etc. **P06** can now calculate the effect of counting statistics on various characterisation parameters, such as fidelity, purity, and “tangle”. We are now working to include the uncertainties in the various polarisation analysis settings. This is a non-trivial problem, which will be important for all future tomographic measurements. Related to this, we are developing a fitting method, by which all derived density matrices will necessarily have non-negative eigenvalues. **P05** have theoretically investigated how to adapt quantum state tomography as developed for polarisation entangled states to energy-time Bell states.

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 six-month period considerable progress was made by many partners setting the stage for early field trials.

- **P01** have been working both on the hardware-software interface, detector modules, as well as made on theoretical paper on authentication, see paper 3 in the publication list. Some problems with detectors have slowed down the experimental implementations.
- **P03**, together with H. Weinfurter from **P02** completed work on polarisation entangled quantum cryptography, see publication 4 below. See also the figures on the ensuing page. By realising a quantum cryptography system based on polarisation entangled photon pairs P03 established highly secure keys, because a single photon source was effectively realised and the inherent randomness of quantum measurements exploited. A novel key distribution scheme using Wigner's inequality to test the security of the quantum channel was implemented, and, alternatively, realise a variant of the BB84 protocol. The system has two completely independent users separated by 360 m, and generates raw keys at rates of 400 - 800 bits/s with bit error rates around 3 %.

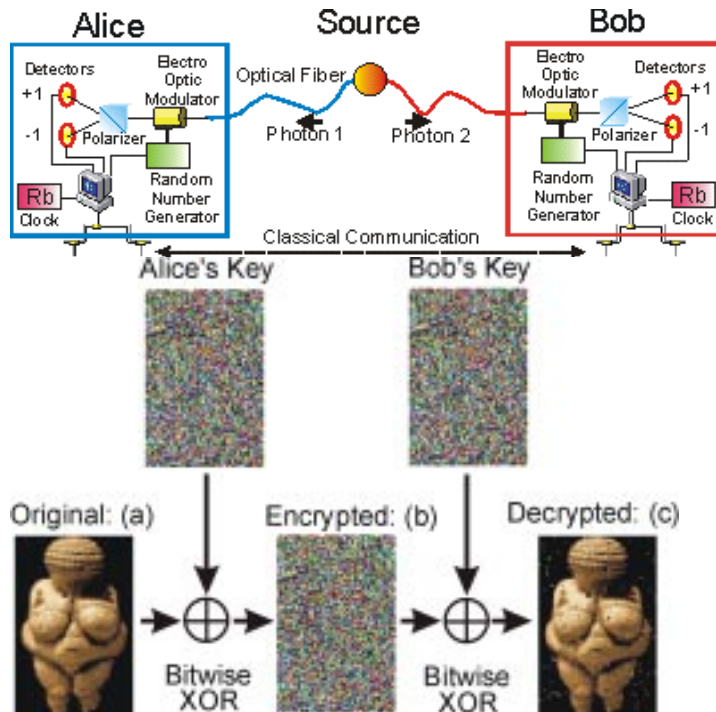


Figure: Schematics of experimental setup for polarisation entangled quantum cryptography reported by P03

The Image (a) of the "Venus von Willendorf" is encrypted by Alice via bitwise XOR operation with her key. She transmits the encrypted image (b) to Bob via the computer network. Bob decrypts the image with his key, resulting in (c) which shows only few errors due to the remaining bit errors in the keys.

The "Venus von Willendorf" was found in 1908 at Willendorf in Austria and presently resides in the Naturhistorisches Museum, Vienna. Carved from limestone and dated 24.000 - 22.000 BC, she represents an icon of prehistoric art.

- **P05** made considerable progress on quantum cryptography using time-bin entanglement with two photons at 1300nm, see publications 1 and 2 below. Furthermore, work on an energy-time entanglement based QC-experiment using a 532nm cw pump laser for creation of photon pairs at 800 and 1550nm was started with. Two polarisations multiplexed interferometers allowing the implementation of the BB84. A laboratory experiment over 8.5 km has been performed and a scientific article is currently under preparation.
- **P06** have implemented the Ekert (entangled state) protocol implemented + experimental simulation of eavesdropper, see the figure below for some examples of the effect of eavesdropping on the security parameter (test of violation of Bell Inequality) used to test the presence of an eavesdropper

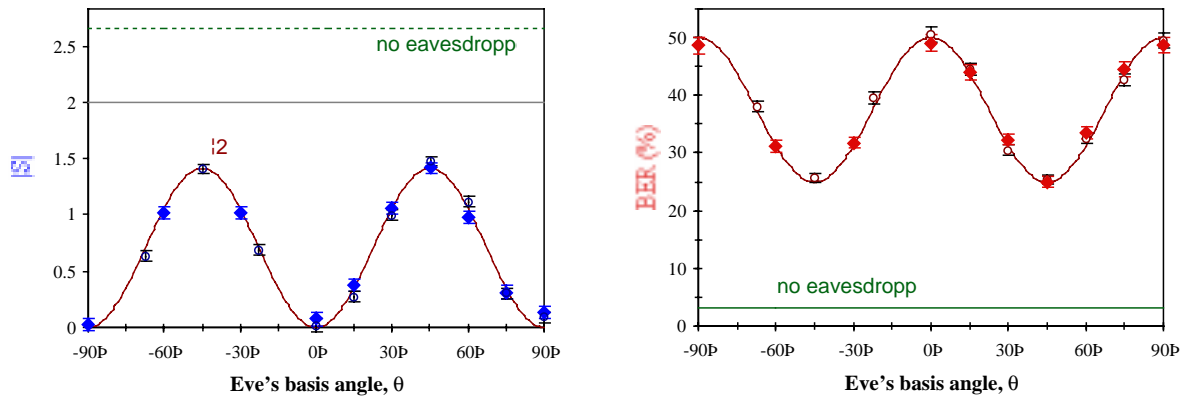


Fig. Data and theory (curves) showing the effect of an eavesdropper on the Bell parameter S and the BER, for a linear polarisation attack basis: $\cos\theta |H\rangle + \sin\theta |V\rangle$ (diamonds), and a QND measurement in the same basis (circles). Experiments by P06. The maximum value of $|S|$ for any local realistic theory is 2; with no eavesdropper we measured 2.66 ± 0.04 . Our bit error rate under these conditions was 3.1%.

- Furthermore, **P06** have conducted a free space 1.6 km quantum cryptography (B92 protocol) trial in daylight conditions done (published in PRL). **P06** have also designed our two-photon experiment to implement the 6-state quantum cryptography protocol, and started setting up to do this.
- **P08** have also conducted a Free space 1.2km QC with faint pulse sources. This is mainly for EQCSPOT, but clearly there will be a knowledge transfer for QuComm for entangled sources.

WP 4 TELEPORTING ENTANGLEMENT

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

- **P03** has been working on a tabletop experiment for teleportation and swapping started. The Entanglement swapping (High fidelity teleportation) was initially hindered by a Pump-laser firmware malfunction. Laser had to be sent back to the factory because the service technician was not able to repair it on site. This caused a 4-week shutdown of the work on that experiment. Work has resumed after laser shutdown. The experimental setup has been redesigned for higher stability and variability. The initial alignment phase is completed and data is already being taken.



WP 5 MULTI-MODE AND 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 the official start for WP5 is only T0+6 (i.e. June 2000), first progress in theory as well as in experiment has already been obtained and first results have been published or submitted to scientific journals.

WP5.1 Experimental multi-party cryptography and novel protocols:

- A **proof-of principle demonstration of quantum secret sharing** in a laboratory experiment has been reported by **P05 (GAP)**, see publication 2 below. In opposition to known implementations using three-particle GHZ states, pairs of entangled photons in so-called energy-time Bell states were used to mimic the necessary quantum correlation of three entangled qubits, albeit only two photons exist at the same time. This is possible thanks to the symmetry between the preparation device acting on the pump pulse and the devices analysing the down-converted photons: the data describing the emission of the bright pump pulse is equivalent to the data characterising the detection of a photon. Therefore, the emission of a pump pulse can be considered as a detection of a photon with 100% efficiency, and the scheme features a much higher coincidence count rate compared to the initially proposed “triple-photon” schemes. Further experimental investigations show that extensions towards transmission distances of tens of km are possible.
- In order to enable new protocols for quantum cryptography, **P02 (LMU)** started to build **tools for general polarisation measurement** of single photons. 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.
- The new setup for teleportation entanglement of P03 (EXPUNIVIE) has a 4-particle GHZ-state producing capability and will be used in that way.
- **P04 (OXFORD)** devised a novel **scheme for error-free quantum state transmission** through a noisy channel, rejecting single bit-flip errors, see publication 5 below. The particular feature is that, in contrast to existing quantum error-correction protocols, this scheme avoids the currently infeasible requirements for a controlled-NOT operation between single photons. Instead, it combines quantum-measurement properties of three-particle entangled (GHZ) states with properties of quantum teleportation, both already demonstrated experimentally.



WP5.2 Robustness of high-dimensional entanglement

- A first leitmotiv of WP5.2 is to study the robustness of partial entanglement between two qubits. **P06 (LANL)** demonstrated **entanglement concentration of non-maximally polarisation entangled states**. **P05 (GAP)** is currently preparing an experiment to investigate the **impact of distance on non-maximally entangled energy-time Bell states** using quantum state tomography as developed for polarisation entangled states.
- Another goal of WP 5.2 is to experimentally demonstrate **entanglement purification** protocols. As predicted by N.Gisin from GAP in 1996, this can be achieved by local filtering. This scheme has been demonstrated experimentally in collaboration between **P05 and P06 (GAP and LANL)**, with GAP's Ph.D student Andre Stefanov visiting LANL. To demonstrate the phenomenon of "hidden non-locality", certain partially-entangled, partially mixed states which do not violate Bell inequality were prepared utilising the polarisation entanglement source developed by LANL. It has been shown that the resulting states after a suitable local filtering operation violate Bell-CHSH inequalities. A scientific article is currently under preparation.

WP 6 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:

- **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.
- 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.



4. List of first year deliverables and milestones

<i>Ist year Deliverables & Milestones</i>			
	Originally	Current	Actual
Month	Planned	View	
Jan 00			
Feb 00		D2	D2
Mar 00	D2		
Apr 00			
May 00		D1 (early May)	
June 00	D3,D4	D3,D4	D3,D4
July 00			
Aug 00			
Sep 00			
Oct 00			
Dec 00	D5,D14,D16,M1,M2,M3,M11,M16,M17, M18	D5,D14,D16,M2,M3,M11, M16,M17, M18	

5. Deliverables and reports

1. D1 (T0+3) Popular project presentation (delayed one month), now on project www site.
2. D2 (T0+3) Project Internet Site <http://www.ele.kth.se/QEO/qucomm/> (the site is in operation officially since February 2000)
3. D3(T0+6) Dissemination and Use Plan, submitted to project officer June 30.
4. D4(T0+6) Half year progress report of year one (this deliverable)

In addition to the above, two bi-monthly progress reports (February, April) have been written and circulated among the projects partners as well as sent to the project officer at the Commission. The material for the report for June is directly included in the present deliverable.



6. Publications

Papers

1. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, "Quantum cryptography using energy-time entangled Bell states", *Phys. Rev. Lett.* **84**, 4737 (2000). Preprint at Los Alamos e-print archive, <http://xxx.lanl.gov/abs/quant-ph/9911109>
2. W. Tittel, H. Zbinden, N. Gisin, "Quantum Secret Sharing by GHZ states", Los Alamos e-print archive, <http://xxx.lanl.gov/abs/quant-ph/9912035>
3. D. Ljunggren, M. Bourennane and A. Karlsson, *Authority based user authentication in quantum cryptography*, *Phys. Rev. A*, accepted for publication March 2000.
4. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum Cryptography with Entangled Photons", *Physical Review Letters* Vol. 84, pp. 4729-4732 (2000)
5. D. Bouwmeester, "Error free optical quantum communication", Los Alamos e-print archive, <http://xxx.lanl.gov/abs/quant-ph/0006108>
6. "Demonstration of entanglement distillation and purification", P. G. Kwiat, S.-B. Lopez, A. Stefanov, and N. Gisin, to be submitted to Nature (2000).

Conferences

1. D. Ljunggren, M. Bourennane and A. Karlsson, *User authentication in quantum cryptography based on two-particle entanglement*, oral presentation at **Swedish-Russian Workshop on Entangled Quantum Systems**, St. Petersburg, Russia, May 19-21, 2000.
2. A. Karlsson, M. Bourennane, D. Ljunggren, F. Nilsson, J. Peña Císcar, F. Gibson, A. Hening, P. Jonsson and M. Mathes, *Fundamentally Secure Information Distribution Using Optical Quantum Cryptography*, oral talk OR9 at **Northern Optics 2000**, Uppsala, Sweden, June 5-8, 2000.
3. A. Karlsson, M. Bourennane, D. Ljunggren, F. Nilsson, J. Peña Císcar, M. Mathes, W. Fransson, A. Hening, F. Gibson and P. Jonsson, *Quantum Technologies for Cryptographic Key Distribution and Beyond...*, invited presentation at the **Information Optics Group (IOG) satellite meeting to Northern Optics 2000**, Uppsala, Sweden, June 5-8, 2000.
4. A. Karlsson, M. Bourennane, D. Ljunggren, F. Nilsson, J. Peña Císcar, M. Mathes, W. Fransson, A. Hening, F. Gibson and P. Jonsson, *Quantum Information and Single Photon Technologies*, invited presentation at **ROMOPTO 2000**, Bucharest, Romania, Sept 5-9, 2000
5. G. RIBORDY, "Cryptographie quantique expérimentale sous le Lac Lemán", 68ème congrès de l'Acfas, 16 may 16th 2000 in Montreal/Canada.
6. N. GISIN, "Linking classical and quantum key agreement : is there classical bound information?", at Royal Holloway College London, may 26th 2000.
7. G. RIBORDY, "Distribution quantique de clefs au moyen de paires de photons intriquées", Colloque "Information quantique", may 30 2000 in Orsay/France.



Other publications of relevance from P06 in year 2000, some completed before project start, hence do not explicitly reference QuComm. They are included because of discussions concerning whether LANL could acknowledge project for financial support or not. This issue is now resolved and further work within the project will explicitly acknowledge the project.

Papers

1. "Free-space quantum key distribution in daylight", R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, *J. Mod. Opt.* **47**, 549 (2000).
2. "Quantum key distribution over a 48-km optical fiber network", R. J. Hughes, G.L. Morgan, and C. G. Peterson, *J. Mod. Opt.* **47**, 533 (2000).
3. "Entangled state quantum cryptography: Eavesdropping on the Ekert protocol", D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, *Phys. Rev. Lett.* **84**, 4733 (2000).
4. "Free-space quantum cryptography in daylight", R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, *Proc. SPIE* **3932**, 117 (2000).
5. "Daylight quantum key distribution over 1.6 km", W. T. Buttler *et al.*, *Phys. Rev. Lett.* **84**, 5652 (2000).
6. "Quantum cryptography for secure satellite communications", R. J. Hughes, submitted to IEEE Aerospace 2000 Conference, Big Sky, Montana, March 14-25, 2000.
7. "Experimental verification of decoherence-free subspaces", P. G. Kwiat, A. J. Berglund, J. B. Altepeter, and A. G. White, submitted to *Science* (2000).

Talks

8. P. G. Kwiat, "Entanglement: The Good, the Bad, and the Ugly", Univ. of Toronto, Physics Colloquium, Jan. 27, 2000.
9. P. G. Kwiat, "Entangled photons for quantum information", Workshop on Quantum Entanglement, Stanford University, Mar. 20 -23, 2000.
10. P. G. Kwiat, "Entanglement concentration and hidden entanglement", APS DAMOP 2000 meeting, Storrs, Connecticut, June 14-17, 2000.
11. P. G. Kwiat, "Measuring entanglement and entanglement measures", Quantum Electronics Conference (CLEO/QELS '2000), San Francisco, CA, May 8-12, 2000.
12. P. G. Kwiat, "Entangled-photon quantum cryptography", Quantum Electronics Conference (CLEO/QELS '2000), San Francisco, CA, May 8-12, 2000.
13. P. G. Kwiat, "101 uses for a Schroedinger kitten", Fifth International Conference on Quantum Communication, Measurement & Computing, Capri, Italy. July 3-8, 2000.
14. P. G. Kwiat, R. J. Hughes, "Free-space quantum cryptography in daylight", SPIE Photonics West, San Jose, CA, January 2000.
15. R. J. Hughes, "Quantum Computing", invited talk, APS March Meeting, Minneapolis, MN, March 2000.
16. R. J. Hughes, "Experimental Quantum Cryptography systems", colloquium at IBM Almaden Research Center, San Jose, CA, April 2000.
17. R. J. Hughes, "Secure communications using quantum cryptography", keynote address, SPIE, AEROSENSE conference, Orlando, FL, April 2000.
18. R. J. Hughes "Daylight quantum key distribution over 1.6 km", APS DAMOP 2000 meeting, Storrs, CT, June 2000.