



QuComm IST-1999-10033

Long Distance Photonic Quantum Communication

QuComm Deliverable D17

Dissemination level: Internal

DELIVERABLE D17 (REPORT)

Entanglement enhanced quantum cryptography fiber systems

Christian Kurtsiefer, Harald Weinfurter

Sektion Physik, University of Munich, Max-Planck-Institute for Quantum Optics, Garching

Hugues de Riedmatten, Wolfgang Tittel, Hugo Zbinden, Gregoire Ribordy and Nicolas Gisin
GAP Optique

Th. Jennewein, Ch. Simon, G. Weihs, and A. Zeilinger,

Institut für Experimentalphysik, Vienna University

D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat*

Los Alamos National Laboratory and * University of Illinois, Urbana-Champaign

ABSTRACT

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

Report Version: 1

Report Preparation Date: 2002-01-05

Classification: Internal



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



Introduction

The possibility to use entangled photon pairs for quantum cryptography (QC) was first proposed by Ekert in 1991 [1]. Although almost all tests of Bell inequalities can be seen as experiments of quantum cryptography, systems specifically designed to meet the special requirements of QC, like quick change of bases, were first implemented only recently. In 2000, three group members of Qucomm reported in the same issue of Phys. Rev. Lett.[2,3,4] quantum cryptography based on the properties of entangled photons.

On one hand, using photon pairs for QC has some potential advantages:

- 1) A first advantage lies in the fact that one can remove empty pulses, since the detection of one photon of a pair reveals the presence of a companion. In principle, it is thus possible to have a probability of emitting a non-empty pulse equal to one. It is beneficial only because presently available single-photon detectors feature high dark count probability. The difficulty to always collect both photons of a pair somewhat reduces this advantage.
- 2) One frequently hears that photon-pairs have also the advantage of avoiding multi-photon pulses, but this is not correct. For a given mean photon number, the probability that a non-empty pulse contains more than one photon is essentially the same for weak pulses and for photon pairs. However, the fact that passive state preparation can be implemented prevents multiphoton splitting attacks [5,6], since the different photon pairs are independent. So, even if multiple photon pairs don't increase Eve's information, they lead to an increase in the QBER [5].
- 3) Using entangled photons pairs prevents unintended information leakage in unused degrees of freedom [7]. Observing a QBER smaller than approximately 15 %, or equivalently that Bell's inequality is violated, indeed guarantees that the photons are entangled and so that the different states are not fully distinguishable through other degrees of freedom.
- 4) Entangled photons offer interesting possibilities in the context of cryptographic optical networks. The photon pairs source can indeed be operated by a key provider and situated somewhere in between potential QC customers. In this case, the operator of the source has no way to get any information about the key obtained by Alice and Bob.

On the other hand, entanglement based systems are far more complex than faint laser pulses set-ups. Current experimental key creation rates obtained with these systems are at least one order of magnitude smaller than those obtained with faint laser pulses set-ups. Decoherence is more serious when using photon pairs, because of the larger spectral width. For example, for a spectral width of 5 nm FWHM -- a typical value, equivalent to a coherence time of 1 ps -- and a fiber with a typical PMD of 0.2 [ps/ \sqrt{km}], transmission over a few kilometers induces significant depolarization. In case of polarization-entangled photons, this gradually destroys their correlation. Hence, although perfectly fine for free-space QC, polarization entanglement is thus not adequate for QC over long optical fibers. A similar effect arises when dealing with energy-time entangled photons. Here, the chromatic dispersion destroys the strong time-correlations between the photons forming a pair. However, it is possible to passively



compensate for this effect using either additional fibers with opposite dispersion, or exploiting the inherent energy correlation of photon pairs.

Recent studies suggest that faint laser QC is secure over distances of about 50 km that are possible with the detectors available today [8]. Hence in the short term entangled photons won't be used for the realization of industrial prototypes.

In the following, we shortly describe the four experiments performed by the QUCOMM consortium [2,3,4,5]. For a closer look refer to the attached reprints.

The group of Anton Zeilinger (EXPUNIVIE), demonstrated a crypto-system using polarization-entangled photon pairs of 702 nm, including error correction [1]. Two-photon source was located near the center between the two analyzers separated by a distance of 360 meters. Special optical fibers, designed for guiding only a single mode at 700 nm, were used to transmit the photons to the two analyzers. The results of the remote measurements were recorded locally and the processes of key sifting and of error correction implemented at a later stage, long after the distribution of the qubits. Two different protocols were implemented: one based on Wigner's inequality (a special form of Bell inequalities), and the other one following BB84.

Los Alamos National Labs (LANL) demonstrated the Ekert protocol [2]. This experiment was a table-top realization with the source and the analyzers separated by a few meters. The quantum channel consisted of a short free space distance. Different eavesdropping strategies were simulated as well. As predicted by the theory, a rise of the QBER was observed together with an increase of the information obtained by the eavesdropper. Moreover, they also recently implemented the six-state protocol and observed the predicted QBER increase to 33%.

The main advantage of polarization entanglement is the fact that analyzers are simple and efficient. It is therefore relatively easy to obtain high contrast. Naik and co-workers, for example, measured a polarization extinction of 97 %, mainly limited by electronic imperfections of the fast modulators. In addition, the constraint on the coherence length of the pump laser is not very stringent. As mentioned above, polarization is indeed not robust to decoherence in optical fibers. In addition, the polarization state transformation induced by an installed fiber frequently fluctuates, making an active alignment system absolutely necessary.

A scheme taking advantage of energy-time entangled photon pairs was realized by GAP. The two-photon source (a KNbO₃ crystal pumped by a cw doubled Nd-YAG laser) produces photons at non-degenerate wavelengths - one around 810 nm, the other one centered at 1550 nm. This choice allows detecting the photon of the lower wavelength with high efficiency silicon based single photon counters. The high transmission loss at this wavelength in optical fibers doesn't matter as the distance between the source and the corresponding analyzer is kept very short. The other photon, at the wavelength where fiber losses are minimal, is sent via an optical fiber to Bob's interferometer and is then detected by InGaAs APD's. The BB84 protocol was implemented with 2 birefringent interferometers, with polarization multiplexing of the two bases. Interference visibilities were typically 92% over. Mbit's of key were distributed through 8.5 km fiber on a spool, at a rate of about 100 Hz. For this scheme, the laser frequency and the rather bulky interferometers must remain stable during a key



exchange session. For this reason, it is not well suited for the development of a prototype, despite of its promising performance.

Finally, GAP also implemented a scheme using phase-time coding with a pulsed, energy-time bin source, creating photons at 1300nm [4]. A contrast of approximately 93% was obtained.

REFERENCES:

- [1] A.K. Ekert, *Quantum Cryptography based on Bell's theorem*, Phys. Rev. Lett. **67**, 661-661 (1991).
- [2] Th. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, *Quantum Cryptography with Entangled Photons*, Phys. Rev. Lett **84** 4729 (2000)
- [3] 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)
- [4] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Quantum Cryptography Using Entangled Photons in Energy-Time Bell States*, Phys.Rev. Lett, **84** 4737 (2000)
- [5] G. Ribordy, J. Brendel, J.D. Gautier, N. Gisin, H. Zbinden, *Long distance entanglement based quantum key distribution*, Phys. Rev. A **63**, 012309 (2001).
- [6] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders, *Limitations on practical Quantum Cryptography*, Phys. Rev. Lett. **85**, 1330 (2000).
- [7] D. Mayers and A. Yao, *Quantum Cryptography with imperfect Apparatus*, Proc. of the 39th IEEE Conf. on Found. of Computer Science (1998).
- [8] Stéphane Félix, N. Gisin, A. Stefanov, H. Zbinden, *Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses*, J. of Mod. Optics, **48** (13), 2009-2021 (2001).