Summary

One of the most important achievements in physics in the course of this century is certainly the development of a theory, describing the behavior of single quanta. Since the beginning, quantum theory has given rise to endless discussions about its meaning and interpretation. Heisenberg's uncertainty relation and Einstein-Podolsky-Rosen paradox are typical examples of counter intuitive predictions. In the past few years, physicists began to realize that quantum physics is more than a radical departure from classical physics. In particular, it provides important new possibilities for information processing [1]. The key word of this new, rather fast evolving field is entanglement, a purely quantum mechanical property leading to non classical correlations between particles.

In this proposal, we present optical realizations of fundamental as well as applied research in the field of quantum information processing (also referred to as quantum communication) carried out within the frame of our Ph.D. thesis. We greatly benefited from the "traditional" experience of the Group of Applied Physics/Optics headed by Professor Gisin at the University of Geneva in the domain of optical telecommunications as well as in quantum key distribution based on polarization coding using single photons at telecommunication wavelength (1310 nm). Our experiments have in common the use of installed optical fibers cables lent by Swisscom, which allowed us to carry them out on scales of ten to twenty kilometers.

A new activity in our group is experiments with energy-time entangled photons. The strange quantum mechanical predictions for such particle pairs leads via the Einstein-Podolsky-Rosen paradox to the famous Bell inequalities, the set of mathematical relations that enables to test whether nature can be described by theories based on local hidden variables. During the last two years we developed the knowledge necessary to perform tests over long distances. This includes building a compact and transportable photon-pair source at telecommunications wavelength, solving problems caused by chromatic dispersion and birefringence in optical fibers, and increasing the performance of photon counting detectors [2,3]. Using a telecommunication fiber network, we could recently demonstrate quantum non-locality over more than 10 km, which is about three orders of magnitude more than in previous experiments [4-6]. In addition to fundamental interest, this directly shows the feasibility of entanglement based quantum key distribution. Beyond, together with a recent proposal how to use energy-time entangled photons instead of polarization entanglement for quantum communication [7], this opens the door to applications like quantum teleportation over large distances.

One of the most promising application of quantum information processing is quantum key distribution, often referred to as quantum cryptography [1, 8], a way to establish a secret key between two remote parties which can be used for encrypting a message. Quantum mechanics states that a measurement of an unknown system will in most cases disturb it. This property is exploited here to reveal a spy: if none of the transmitted bits, encoded in non-orthogonal bases, have been disturbed, it can be inferred that no unlegitimate person tried to listen in. In 1997, we proposed and tested a new set-up for quantum key distribution using faint laser pulses simulating single photons (in opposition to schemes based on entanglement) and exploiting phase coding [9-11]. In general, such interferometric systems suffer from problems caused by the mechanical stability and fluctuations of the state of polarization as encountered when guiding light in optical fibers. The new feature was the use of a self-balancing "time-multiplexed" interferometer in conjunction with so called "Faraday mirrors", which automatically compensates all birefringence in the fibers. Hence, this "plug & play" system does not need any adjustment, a major advantage compared to other systems. We achieved an excellent performance over 23 km of installed telecommunication fiber between Geneva and Nyon. This system, which was developed with the support of Swisscom, has since been patented. In order to further improve it, the transmission rate had to be increased. To do so, we developed new single photon detectors based on InGaAs avalanche photodiodes, which show a better performance than Germanium detectors which had been used before [12]. Recently, we tested this improved set-up and increased the key distribution rate by a factor of more than hundred. We also improved the driving electronics, allowing user-friendly operation of the system [13].

List of Publications

[1] Physics World, special issue on Quantum Information Theory, March 1998. It includes an article on Quantum Cryptography by W. Tittel, G. Ribordy, and N. Gisin.

[2] W. Tittel, J. Brendel, T. Herzog, H. Zbinden, and N. Gisin, "Non-local two-photon correlations using interferometers physically separated by 35 meters", Europhysics Letters **40** (6), pp. 595 - 600 (1997).

[3] W. Tittel, J. Brendel, B. Gisin, T. Herzog, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum correlations over more than 10 km", Physical Review A **57** (5), pp. 3229 - 3232 (1998).

[4] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Violation of Bell Inequalities by Photons More Than 10 km Apart", Physical Review Letters **81** (17), pp. 3563 - 3566 (1998).

[5] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, "Long –distance Bell-type tests using energy-time entangled photons", submitted to Physical Review A.

[6] N. Gisin, J. Brendel, W. Tittel, and H. Zbinden, "Quantum Correlations Over More Than 10 km", to appear in *Optics in 1998*, Optics & Photonics News, December 1998.

[7] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, "Pulsed energy-time entangled twin-photon source for quantum communication", submitted to Physical Review Letters.

[8] H. Zbinden, H. Bechmannn-Pasquinucci, N. Gisin, and G. Ribordy, "Quantum Cryptography", Applied Physics B **67** (6), pp. 743 - 748 (1998).

[9] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug & Play'" systems for quantum cryptography", Applied Physics Letters **70** (7), pp. 793 – 795 (1997).

[10] H. Zbinden, J.-D. Gautier, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Interferometry with Faraday mirrors for quantum cryptography", Electronics Letters **33** (7), pp. 586 – 588 (1998).

[11] B. Huttner, A. Muller, G. Ribordy, W. Tittel, H. Zbinden, and N. Gisin, "'Plug & Play' quantum cryptography", *Optics in 1997*, Optics & Photonics News, December 1997.

[12] G. Ribordy, J.-D. Gautier, H. Zbinden, and N. Gisin, "Performance of InGaAs/Inp avalanche photodiodes as gated-mode photon counters", Applied Optics **37** (12), pp. 2272 – 2277 (1998).

[13] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, "Automated 'plug & play' quantum key distribution", Electronics Letters **34** (22), pp. 2116 – 2117 (1998).

GMP-Preis-Preisträger

1999 Dr. Gregoire Ribordy und Dr. Wolfgang Tittel von der "Groupe de Physique Appliquée" der "Section de Physique" der Universität Genf

Die Arbeit von Grégoire Ribordy und Wolfgang Tittel beschäftigt sich zum einen mit Tests einer der grundlegenden und praktisch sämtliche Anwendungen durchziehenden Eigenschaft, der sogenannten Verschränkung. Solche Tests zeigen, dass das Verhalten von verschränkten, also quantenmechanisch korrelierten Teilchen nur mit Hilfe nichtlokaler Theorien erklärt werden kann – Theorien, die eine instantane Abhängigkeit des Ergebnisses der Messung an einem Teilchen vom Ergebnis der Messung an einem anderen, mit dem ersten verschränkten und von diesem im Prinzip beliebig weit entfernten Teilchen erlauben. Nachdem Tests der sogenannten Bell-Ungleichungen seit 25 Jahren immer wieder im Labor durchgeführt wurden, konnte die Genfer Gruppe die Distanz zwischen den beiden verschränkten Teilchen in einem, mit Hilfe des Swisscom Glasfasernetzes durchgeführten Experiment mehr als vertausendfachen und somit Verschränkung auch über grosse Entfernungen nachweisen.

Die am weitesten fortgeschrittene Anwendung der Quanten-Kommunikation ist die Quanten Kryptographie, die schon bald für die Datensicherheit bei der Nachrichtenübertragung über öffentliche Netze eine wichtige Rolle spielen könnte. Im Gegensatz zu den bisher meist eingesetzten, sogenannten public key Verschlüsselungsverfahren bieten nur auf geheimen Schlüsseln beruhende Methoden der Kodierung einen mathematisch bewiesenen Schutz gegenüber ungewünschten Lauschern. In der klassischen Kryptographie stellt jedoch die sichere Übermittelung solcher geheimen Schlüssel unüberwindliche Probleme dar, sofern er nicht bei einer direkten (physischen) Begegnung der Kommunikationspartner ausgetauscht werden kann. Die Quanten-Kryptographie schafft diesem Manko Abhilfe. Grob gesagt läßt sich die Tatsache benutzen, daß eine Messung eines quantenmechanischen Teilchens seinen Zustand im allgemeinen verändert : Sind Bits des Schlüssels, realisiert in Form von Quantenzuständen einzelner Photonen während der Übertragung verändert worden, so kann auf die Anwesenheit einer dritten Person geschlossen werden. Ein solches Quanten-Kryptographiesystem ist innerhalb der letzten drei Jahre an der Universität Genf u.a. von Grégoire Ribordy und Wolfgang Tittel entwickelt und erfolgreich unterhalb des Genfer Sees, erneut unter Benutzung des Telekommunikations Fasernetzes, getestet worden. Es zeichnet sich durch besonders grosse Unempfindlichkeit gegenüber möglichen Störungen der Photonen während der Transmission innerhalb der Glasfaser aus. Um den Kreis zwischen den beiden Aspekten der Arbeit „angewandte und fundamentale Physik" zu schliessen, sei noch angemerkt, dass nichtlokale Korrelationen zwischen verschränkten Teilchen ebenfalls für die Quanten Kryptographie einsetzbar sind, eine Idee, die aus dem Jahre 1991 stammt und bereits von den Genfer Forschern getestet wurde und in der Zukunft weiterverfolgt werden wird.

Quelle :

- Schweizerische Gesellschaft für Optik und Mikroskopie; Yearbook 2005