Entanglement Based Quantum Communication

H. Weinfurter[1,2], Ch. Kurtsiefer[1]

[1] Sektion Physik der Universität München, 80799 München, Germany
[2] Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany

Abstract

Fundamental quantum effects lie at the heart of new proposals for quantum communication and computation, like Quantum Cryptography and Quantum Teleportation. Here we describe the experimental status of quantum communication schemes, which improve existing classical methods or add new features to the world of communication.

Keywords: quantum communication, quantum teleportation

1. INTRODUCTION

The new field of quantum information shows the fascinating features of new methods for secure and efficient communication and new algorithms exploiting the capability of quantum computers [1]. While the latter needs entanglement between a number of quantum systems, the basic quantum communication schemes only rely on entanglement between the members of a pair of particles and thus can be demonstrated already in todays state-of-the-art experiments. The basic version of quantum cryptography only requires attenuated laser pulses and prototypes for commercial applications are therefore already under development.

In the present work we report on the first experimental realizations of quantum communication schemes using entangled photon pairs as produced by parametric down-conversion. The ready use of these violently nonclassical states of light has proven its usability in a number of experiments on the foundations of quantum mechanics [2]. Here we describe how to make communication secure against eavesdropping using quantum cryptography, how to increase the information capacity of a quantum channel by quantum dense coding and how to communicate quantum information itself in the process of quantum teleportation. Finally, we report on the development of new tools for the development of prototypes for secure quantum key distribution.

2. QUANTUM COMMUNICATION SCHEMES

Cryptography enables two parties (lets call them ALICE and BOB) to mask confidential messages such, that they are illegible to any unauthorized institution (called Eve). However in principal, any *classical* key distribution can be intercepted without being detected. The recent development of quantum key distribution can cover this major loophole of classical cryptography and allows to detect any eavesdropping attack upon this quantum channel, since nature does not allow to gain information on the state of a quantum system without disturbing it [3].

Quantum Cryptography with entangled photon pairs [4] is an intriguing application of Bell's theorem. This theorem states [5], that the results of certain correlation measurements on entangled photon pairs violate an inequality, which is derived under the assumption that the results of all possible measurements are predetermined, and that relativistic locality is satisfied. Now, if eavesdropping attacks along the lines between the two observers ALICE and BOB try to obtain information about the quantum state of the photons, information about this state becomes available and the results of the two observers are partly predetermined! Thus the security of a quantum channel between ALICE and BOB can be tested, since any interception of the connection leads to a reduced degree of violation of a Bell-type inequality. When utilizing the peculiar

properties of entangled photon pairs produced by parametric down-conversion, one immediately profits also from the inherent randomness of quantum mechanical observations and obtains truly random, non-deterministic keys.

Various experiments with entangled photon pairs have already demonstrated that the entanglement can be observed with high signal to noise ratio and also that it can be preserved over distances as large as 10 km [6]. Here we describe how the peculiar quantum properties for the first time could be applied for secure generation of random keys.

The key distribution system (Figure1a) starts with distributing polarization entangled photon pairs described by the state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right)$$

where we denote horizontal and vertical polarization of the photon by H and V, respectively, and where photon A is sent to ALICE and photon B to BOB. This state is rotationally invariant and thus shows perfect anti-correlation for polarization measurements with two channel polarizers done by ALICE and BOB with parallel, but arbitrarily oriented settings. The perfect anti-correlations will be used for generating the quantum keys. The security of the quantum channel then is ascertained by evaluating either subsets of the key (BB84-protocol) or a Bell inequality.

A particularly suited Bell-inequality is due to E.P. Wigner [7], which bounds the probabilities for $(+_A,+_B)$ events, i.e. both observers register a click in the "+" detector of a polarization analyzer oriented along an angle α,β, or γ, by

$$p_{++}(\alpha_A,\beta_B) + p_{++}(\beta_A,\gamma_B) - p_{++}(\alpha_A,\gamma_B) \geq 0 .$$

In order to implement quantum key distribution, ALICE and BOB each vary their analyzers randomly between two angles, ALICE: -30°, 0° and BOB: 0°, 30°. Because ALICE and BOB operate independently, four possible combinations of analyzer settings will occur, of which the three oblique settings allow a test of Wigner's inequality and the remaining combination of parallel settings (ALICE: and BOB both at 0°) allows to establish the quantum key. If the measured probabilities violate Wigner's inequality, fundamental laws of physics guarantee the security of the key shared by ALICE and BOB.

Classical communication uses two-state systems to encode a single bit, if one wants to send a certain amount of information one consequently has to physically transfer the corresponding amount of such systems. The question now arises whether one can use quantum systems to communicate classical information more efficiently. And also whether it is possible to transfer quantum information itself, and if so, which resources are needed. In two proposals [8, 9] it was realized, that the foremost requirement for the sender and receiver then is to first share an entangled pair of particles. As can be seen in Figure 1b and 1c, both methods use similar ingredients: firstly, the source for entangled pairs of particles, secondly, a component (U) performing unitary operations on a two-state quantum particle given one of four classical messages, and finally, the so called Bell-state measurement (BSM) projecting a pair of two-state particles onto the Bell-state basis given by four maximally entangled, orthogonal states.

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right)$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B + |V\rangle_A|H\rangle_B\right)$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|H\rangle_B - |V\rangle_A|V\rangle_B\right)$$
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B\right)$$

Quantum dense coding uses the peculiar feature, that just by manipulating *one* of the two particles, each of the four two-particle states can be transformed into any other. This enables the sender (ALICE) to encode one out of *four* messages, i.e. 2 bits of information, in only one two-state system. After transmission, the receiver (BOB) can read this message by projecting the two-particle state onto the Bell-

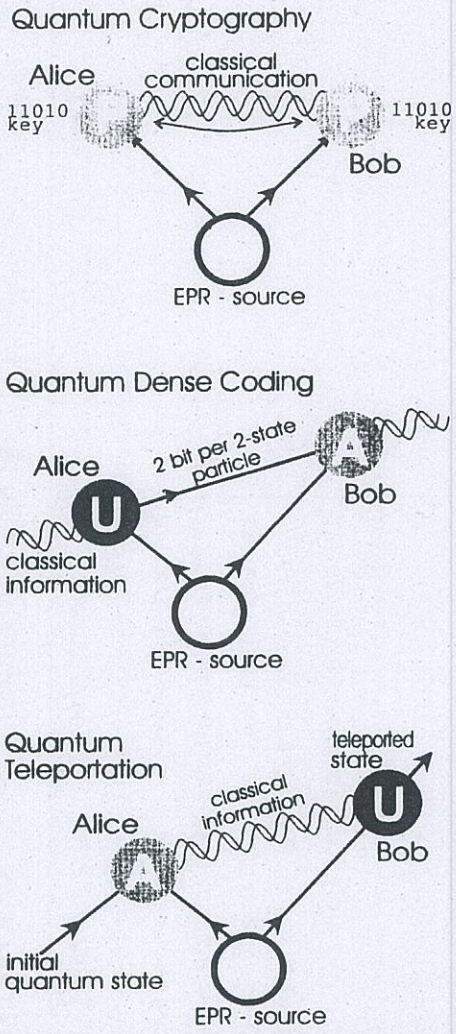

Figure 1. Schemes of quantum communication methods: (a) for guaranteeing secure communication (quantum cryptography), (b) for efficiently transmitting classical information (quantum dense coding), and (c) for transferring quantum states (quantum teleportation, c). (P polarization measurement, U...unitary transformation, BSM...Bell-state analysis)

basis. We want to stress the fact that, as in the classical case, two two-state particles are needed, yet due to the particular properties of the Bell-vectors, 2 bits of information can be transferred via only one of the two particles provided there is no encoding performed on the second one.

In classical physics any object is fully determined by its properties which can be determined by measurement. If one knows all that properties, in principle, one can make a copy at a distant location and thus does not need to send the object itself. Quantum information of a system is given by the state of a quantum system. However, according to Heisenberg's uncertainty relation one can not fully determine this state by a measurement. Any attempt to gain knowledge about quantum information causes a collapse of the quantal wavefunction and thus reduces the amount of accessible information. This is closely related to the no-cloning theorem and seems to bring the idea of transferring quantum properties to a halt. Surprisingly, it is a measurement which does not give any information about the quantum system at all, which shows the way out.

For the teleportation of a quantum state, ALICE first measures one of the entangled particles together with the particle carrying the state to be transferred. If the measurement projects the state of the two particles onto an entangled state, then the initial properties of each of the two particles can not be inferred anymore. Yet, due to the original quantum correlations the state of the second particle of the pair is correlated with the result of the measurement. The corresponding unitary transformation can restore the quantum state on BOB's particle once he received the result via classical communication.

3. EXPERIMENTAL REALIZATION

For the experimental demonstrations of entanglement based quantum communication schemes polarization entangled photons were produced by type-II down-conversion in a nonlinear BBO crystal. A UV-beam (either λ=351.1 nm from an argon-ion laser or pulse with a duration of 200 fs and λ=490 nm) is down-converted into pairs of photons with equal wavelength but orthogonal polarization [10]. For polarized photons state analysis can be performed with high signal to noise ratio and the necessary unitary transformations are especially easy to perform. One quarter-wave and one half-wave retardation plate are sufficient to perform the necessary spin-flips or polarization dependent phase-shifts to either-

encode the message or to transform into the teleported state.

The set-up of the quantum key distribution system is sketched in figure 2. The photons of a pair are each coupled into 500m long optical fibers and transmitted to ALICE and BOB, respectively, who are separated by 400m. ALICE and BOB both have Wollaston calcite polarizers and electro-optic modulators in front of the analyzers which rapidly switch the axis of analysis, controlled by quantum random signal generators [11]. Photons are detected by Silicon avalanche photo diodes, and their arrival time is registered together with the analyzer settings and detection results to enable key sifting. Overall the system allowed to establish a key at a rate of 420bit/sec with a quantum bit error rate less than 3.4%[12].

For quantum dense coding and quantum teleportation Bell state analysis turned out to be the most crucial task to be performed. Conditional state changes, e.g., due to strong coupling or interaction between two quantum particles, would be needed, but are unfortunately not feasible with current technology. Here we employ two-photon interferometry allowing a partial solution of the problem [13]. In this technique polarization and coincidence analysis in the output modes of a beamsplitter can uniquely identify two of the four states with the other two giving a third result.

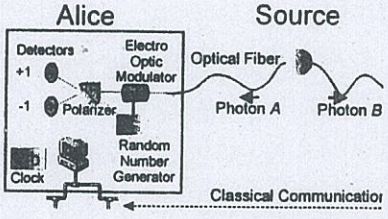

Figure 2. Scheme of the set-up for Quantum Cryptography where the two users, ALICE and BOB, are separated by ~400m and connected

This allows to transmit one of three messages in one two-state system [16]. Since we now can read 3 different messages, the stage is set for the 1.58-bit quantum dense coding transmission. Figure 3 shows the various coincidence rates when sending the ASCII codes of "KM°" (i.e. codes 75, 77, 179) in only 15 trits instead of 24 classical bits.

For quantum teleportation [15], the interferometric approach for Bell-state analysis requires specific timing conditions for two independent incoming photons on ALICE's Bell-state analyzer to erase path information [14]. This was achieved using pulsed down-conversion radiation together with narrow filtering at the detectors. Adjusting for zero delay of the two photons at the Bell-state analyzer, one can transfer the state of the initial photon – in this case the polarization – onto a third photon. Fig. 4 shows two scans for different initial polarization. At zero delay. the polarization state could be reproduced on the third photon with a fidelity of more than 80%. Demonstrating that also entanglement between photons can be teleported, one can prove the ability to teleport not only pure states, but any arbitrary quantum state of a qubit [16].

4. THE NEXT STEPS

In this contribution we presented the initial proof of principle experiments for new communication schemes. They either guarantee perfect security against eavesdropping, increase the channel capacity of communication or allow, for the first time, to transfer quantum properties from one particle onto another one.

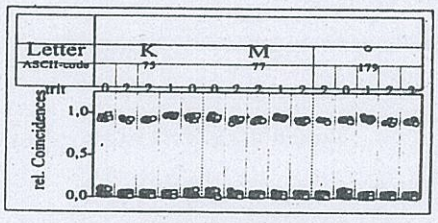

Figure 3. "1.58 bit per photon" quantum dense coding: The ASCII-codes for the letters "KM°" are encoded in 15 trits instead of the 24 bits usually necessary. The data for each type of transmitted state are normalized to the maximum coincidence rate for that state.

Obviously, photons are the choice for any communication techniques, especially when using standard telecom fibers to transmit the light to distant locations.

For any realistic application the experiments have to be completely redesigned in order to enable easy handling and to guarantee high stability at the same time. Most important, the costly laser systems needed for the generation of polarization entangled photon pairs have to be replaced. Recently, we could employ diode pumped down-conversion for efficient production [17]. This first test set-up will be further improved with new laser-diodes already emitting blue light with a output power of more than 10mW. This should allow one to design fully integrated sources of polarization entangled photon pairs and to increase the key rates of secure quantum cryptography.

5. Acknowledgements

We acknowledge the inspiring collaboration with our co-workers and financial support from the Deutsche Forschungsgemeinschaft and under the EU-IST-FET project QuComm.

REFERENCES

[1] Bennett, C. H. "Quantum Information", *Physics Today*, **48**(10):24, 1995. Bouwmeester, D., Ekert, A., and Zeilinger, A., editors. *The Physics of Quantum Information*, Springer, 2000.

[2] Greenberger, D. M., Horne, M. A., and Zeilinger, A. "Multi-particle Interferometry and the Superposition Principle". *Phys. Today*, p. 22, August 1993; for detailed overviews see Chiao, R. Y., Kwiat, P. G., and Steinberg, A. M., in ***Advances in Atomic, Molecular and Optical Physics,*** **Vol. 34**, B. Bederson and H. Walther, ed., Academic Press, 1994; Weinfurter, H. *ibid.* **Vol. 39**, 1999.

[3] Bennett, C. H., Brasssard, G. "Quantum Cryptography: Public Key Distribution and Coin Tossing", *Proc. IEEE Int. Conf. Computer Systems and Signal Processing*, Bangalore, India, IEEE, New York, pp.175, (1984).

[4] Ekert, A. "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.*, **67**:661-664, 1991.

[5] Bell, J. S., "On the Einstein Podolsky Rosen paradox", *Physics* (Long Island City, N.Y.) 1:195, 1965.

[6] Tittel, W., Brendel, J, Zbinden, H., and Gisin, N. *Phys. Rev. Lett.*, **81**:3563-3567, 1998.

[7] Wigner, E. P. "On hidden variables and quantum mechanical probabilities", *Am. J. Phys.*, **38**:1005-1009, 1970.

[8] Bennet, C. H., Wiesner, S. *Phys. Rev. Lett.*, **69**:2881-2884, 1992.

[9] Bennet, C. H., Brassard, G., Crépeau, C., Josza, R., Peres, A., Wootters, W.K. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". *Phys. Rev. Lett.*, **70**:1895-1899, 1993.

[10] Kwiat, P. G., Mattle, K., Weinfurter, H., Zeilinger, A., Sergienko, A. V., Shih, Y. H. "New High-Intensity Source of Polarization-Entangled Photon Pairs". *Phys. Rev. Lett*, **75**:4337-4341, 1995.

[11] Jennewein, T., Weihs, G., Weinfurter, H., and Zeilinger, A., "A compact quantum random number generator", *Rev. Sci. Instr.*, 41:16751680 (2000).

[12] Jennewein, T., Simon, Ch., Weihs, G., Weinfurter, H., and Zeilinger, A. "Quantum Cryptogrpahy with polarization entangled photons". *Phys. Rev. Lett.*, **84**:4729-4732 (2000).

[13] Weinfurter, H. "Experimental Bell-state Analysis", *Europhys. Lett.*, 25:559, 1994. Zukowski, M., Zeilinger, A., and Weinfurter, H., "Entangling Photons Radiated by Independent Pulsed Sources", *Ann. N.Y. Acad. Science*, **755**:91-97, 1995. Rarity, J. G., *ibid.* p.624-628.

[14] Mattle, K., Weinfurter, H., Kwiat, P. G., and Zeilinger, A. "Dense Coding in Experimental Quantum Communication". *Phys. Rev. Lett.*, **76**:4656-4660, 1996.

[15] Bouwmeester, D., Pan, J.-W., Mattle, K., Eibl, M., Weinfurter, H., and

Zeilinger, A. "Experimental Quantum Teleportation". *Nature*, **390**:575, 1997.

[16] Pan, J.-W., Bouwmeester, D., Weinfurter, H., and Zeilinger, A. *Phys. Rev. Lett.*, **80**:3891-3895, 1998.

[17] J. Volz, Ch. Kurtsiefer, H. Weinfurter: "Compact All-Solid-State Source of Polarization Entangled Photon Pairs", *Appl. Phys. Lett.*, **79**:869871 (2001).

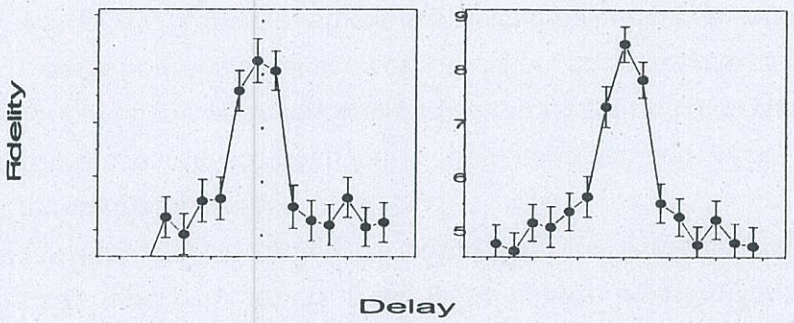

Figure 4. Fidelity of quantum teleportation: the two data show the results for teleportaion of the polarization state of photons originally prepared at 45° (left, (a)) and at 0° (right(b)). These results for teleportation of two non-orthogonal states prove the possibility to teleport the quantum state of a single photon.