QUANTUM COMMUNICATION AND QUANTUM COMPUTATION WITH ENTANGLED PHOTONS

ANTON ZEILINGER

Institut fuer Experimentalphysik, Vienna University, Boltzmanngasse 5, A-1090 Vienna, Austria
IQOQI Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences,
Boltzmanngasse 3, A-1090 Vienna, Austria
E-mail: anton.zeilinger@univie.ac.at

Entangled photons provided the first evidence of a violation of Bell's inequality which implies a breakdown of the philosophical world-view of local realism. These experiments, having been extended over the years over ever longer distances, also provided the experimental foundation of the emerging field of quantum communication. There, quantum cryptography and quantum teleportation are key topics, which are already fairly advanced, being able to cover significant distances. Originally, it was thought that in a future quantum internet scheme, communication would be provided by photons while the local computers were to be realized with ions, atoms, atomic nuclei, solid state devices and the like. Interestingly, most recently the field of linear optics quantum computation has emerged with interesting possibilities and advantages.

Keywords: Quantum Communication; Quantum Computation; Entanglement.

1. Introduction

From a historical point of view, a most remarkable feature of entanglement is that it lay dormant for such a long time. There were very few reactions on the original Einstein-Podolsky-Rosen Paper[1], most remarkably those of Niels Bohr[2] and Erwin Schrödinger[3]. This may be seen for example by the number of citations which the EPR-Paper received (Fig. 1). The situation changed only in the 1960s and 1970s, after the discovery of Bell's theorem and after the first experiments[4] which were made possible by the invention of the laser.

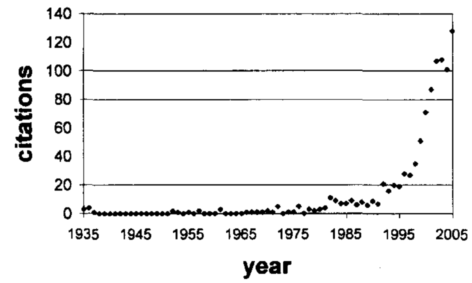

Fig. 1. Number of citations of the EPR-Paper per year. In the beginning, the article was apparently ignored. It has gained wide recognition world-wide today.

From an information theoretic point of view, the most remarkable feature of entanglement is the fact that in a maximally entangled state, all information is encoded in joint properties of the individual systems while the individuals themselves carry no information whatsoever. This may for example be seen in the case of the antisymmetric polarization-entangled state of two photons.

$$|\psi\rangle^{-} = \frac{1}{\sqrt{2}}\left(|H\rangle|V\rangle - |V\rangle|H\rangle\right) \quad (1)$$

Here and in the following, we assume the kets to be numbered from left to right. The state of equation 1 simply means that one has two photons, each one either horizontally (H) or vertically (V) polarized. They are orthogonal to each other in any basis, but before measurement, neither photon carries any information whatsoever.

2. Dense Coding and Cryptography

This property, that neither photon carries any polarization on its own, is essential in many applications, including entanglement-based quantum cryptography and quantum teleportation. The first application where this came to fruit is quantum dense coding[5] as proposed by Bennett and Wiesner[6]. There, one is able to switch around between all four different Bell states, the maximal entangled states of two photons, Alice's and Bob's, by just manipulating Bob's photon alone. Alice, as the receiver, may then identify which of the four messages was sent by performing a suitable Bell state measurement. That way, she is able to identify which of the four Bell states was produced by Bob's manipulation, and thus receive the two bits of information sent by Bob.

In the first experiment where entanglement was put to work to transmit information in a way not possible with classical means, polarization-entangled photons were produced by type II down-conversion[7]. There, Bob can transfer between the four Bell states using $\lambda/2$- and $\lambda/4$-plates and Alice can then identify the Bell states by suitable polarization coincidence measurements. Since complete Bell state analyzers for two photons are hitherto unavailable, Alice was able to discriminate in the experiment between three possibilities only. Nevertheless, taking into account inefficiencies of the experiment, these resulted in a channel capacity of 1.6 bit per photon manipulated by Bob, which is significantly larger than the classical limit of 1 bit.

A conceptually rather interesting feature of this experiment is the property that it also constitutes a situation of quantum cryptography. The point is that by measuring Bob's photon alone, an eavesdropper has no possibility whatsoever to identify which message was sent by Bob. This is because the density matrix of one photon alone represents a maximally mixed state. Therefore, as long as an eavesdropper has only access to Bob's channel, he has no possibility to identify the message sent.

3. Long-Distance Experiments

A most dramatic development in the time since the last ISQM is that quantum entanglement has left the laboratory. There exist now numerous different experiments utilizing quantum entanglement over large distances up to the order of 10 kilometers.

In terms of experimental stability, the most advantageous experiments are those where the entangled photons are distributed by glass fibers. This is because such fibers are usually put underground, and therefore such a communication is independent of external disturbances, in particular, the weather pattern. Distances of the order of 10 kilometers can easily be achieved as already demonstrated by the Geneva group[8] in a test of Bell's inequality. In an experiment where the glass fiber ran under the river Danube[9], quantum teleportation over a distance of 600 meters could be demonstrated (Fig. 2). In that experiment, the maximally efficient quantum teleportation protocol possible with linear elements only was performed. At the receiver station, the unitary operation was applied to the arriving photon fast enough to form the necessary transformation, as suggested in the original protocol[10].

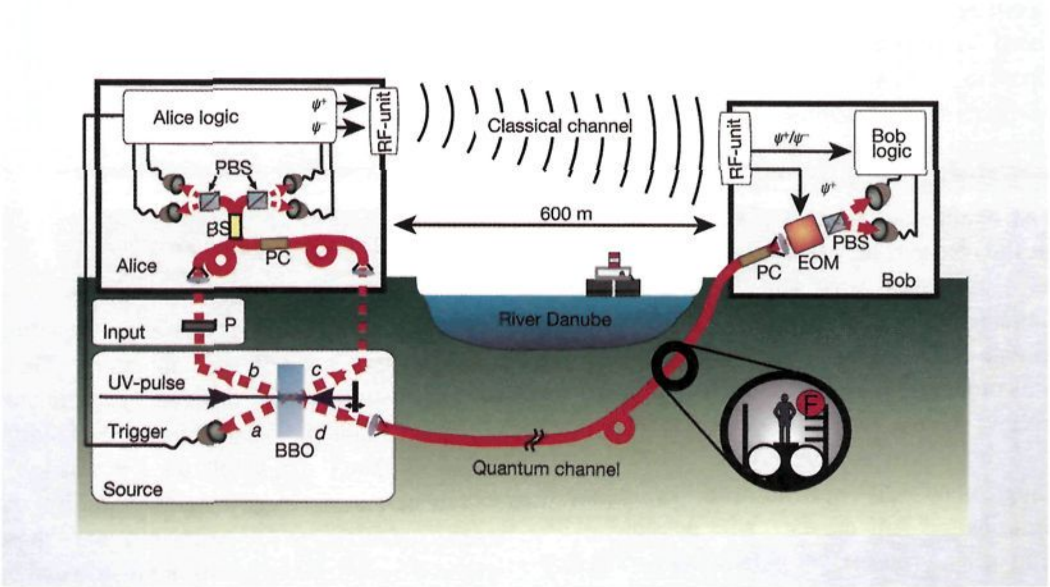

Fig. 2. Long-distance quantum teleportation across the River Danube[9]. The quantum channel (fiber F) rests in a sewage-pipe tunnel below the river in Vienna, while the classical microwave channel passes above it. A pulsed laser (wavelength, 394 nm; rate, 76 MHz) is used to pump a barium borate (BBO) crystal that generates the entangled photon pair c and d and photons a and b (wavelength, 788 nm) by spontaneous parametric down-conversion. The state of photon b after passage through polarizer P is the teleportation input; a serves as the trigger. Photons b and c each are guided into a single-mode optical-fiber beam splitter (BS) connected to polarizing beam splitters (PBS) for Bell-state measurement. Polarization rotation in the fibers is corrected by polarization controllers (PC) before each run of measurements. The logic electronics identify the Bell state as either ψ^- (bc) or ψ^+ (bc) and convey the result through the microwave channel (RF unit) to Bob's electro-optic modulator (EOM) to transform photon d into the input state of photon b.

Another recent application concerns the first bank transfer performed in the city of Vienna. There, all the information necessary to transmit during a banking transaction was encoded using a key generated by entangled photons. These photons were transmitted over underground optical fibers passing through the sewage system of Vienna.

An alternative for long distance quantum communication is sending the entangled photons through air via free-space links. The most promising avenue here is to finally exploit satellites. This is because then, one has to penetrate only a few kilometers of air, and the rest of the propagation is through vacuum. A distinct advantage of propagating through air is that there are no birefringent effects, that is, polarization is very well conserved during such communication. In a very recent experiment[11], it was actually possible to send an individual entangled photon over a distance of 144 kilometers between two Canary Islands. Using such a long-distance link, it was feasible to actually encode some information in a quantum cryptography scheme.

The final goal will be to establish a source of entangled photons on a satellite or on the International Space Station ISS, and thus provide the possibility of exchanging quantum cryptographic keys between two arbitrary locations on Earth.

4. All-Optical Quantum Computation

It is well known that one can build a general quantum computer using a combination of different single-qubit-gates and one sufficiently complex two-qubit gate. Such a two-qubit-gate could, for example, be a CNOT-gate. The essential feature of all such two-qubit-gates is that one needs significant interaction between two qubits. This means that the evolution of the second qubit must depend strongly on the quantum state of the first one.

While the quantum gates with interaction between two qubits are readily available in various atomic or solid state applications, this is not the case for photons. At present, no interaction exists between two photons which is strong enough, such that it can serve as the essential element in a two-qubit-gate. Nevertheless, it had been shown[12] that with linear optical elements alone, one can build any quantum computer. The problem there remains that in such a linear optics scheme, the behavior of the algorithm is probabilistic. This means that only in a small fraction of cases, the optical quantum computer returns the calculation result desired.

This limitation has been shown to be overcome in a scheme proposed by Raussendorf and Briegel[13]. What they showed is that measurement of individual qubits together with active feed-forward can turn such a linear optics quantum computer into a deterministic one. The computer itself is based on cluster states, a specific class of multi-qubit entangled states.

In a recent experiment[14], it was possible to demonstrate for the first time such cluster states for four qubits and implement some of the most basic schemes for one-way quantum computation. In that experiment, it was even possible to demonstrate successfully a Grover search algorithm[15], where one tagged element out of four different ones was identified.

5. Outlook

It will be interesting to see to which extent long-distance quantum communication can be established using satellites in the near future. From a fundamental point of view, such experiments are interesting because they would eventually provide a test of quantum nonlocality over distances over the order of thousands of kilometers, a distance over which entanglement has not been tested at all thus far.

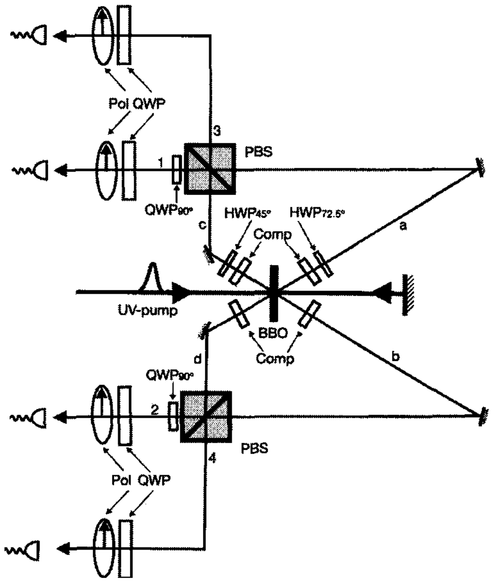

Fig. 3. Experiment on all-optical one-way quantum computation[14]. An ultraviolet laser pulse makes two passes through a nonlinear crystal (BBO), which is aligned to produce entangled photon pairs Φ^- in the forward direction in modes a and b, and Φ^+ in the backward direction in modes c and d. Compensators (Comp), consisting of a half-wave plate (HWP) and an extra BBO crystal, are placed in each path to counter walk-off effects. Including the possibility of double-pair emission and the action of the polarizing beam-splitters (PBS), the four components of the cluster state can be prepared. The incorrect phase on the HHVV amplitude can easily be changed by using a HWP in mode a. The amplitudes can be equalized by adjusting the relative coupling efficiency of those photon pairs produced in the backward pass as compared to the forward pass. Polarization measurements were carried out in modes 1 to 4 using quarter-wave plates (QWPs) and linear polarizers (Pol) followed by single-mode fiber-coupled single-photon counting detectors behind 3-nm interference filters.

All-optical one-way computers in the next generation will include active feed-forward of the measurement result in such a way that further parameters in the computation are set, depending on earlier results. It is obvious that the main challenge for all-optical quantum computers is the development of sources of highly entangled multi-photon quantum states of detectors with high efficiency, which also would allow discriminating between different numbers of photons.

Nevertheless, all-optical quantum computation provides the aspect of being extremely fast. Present technology would already allow one computational cycle, that is, one cycle of measurement and active feed-forward to be performed in less than 100 ns, and it is reasonable to expect that this can be pushed down into the 10 ns regime, which, if implemented on a grand scale, would imply a quantum computer with the order of 10^8 elementary calculations per second, a fascinating possibility.

Acknowledgments

This work was supported by the Austrian Science Fund (FWF) under project numbers SFB1520 and SFB1506, the European Space Agency under project QIPS, the European projects SECOQC and QAP, and by the ASAP program of the Austrian Space Agency (FFG).

References

1. A. Einstein, B. Podolsky and N. Rosen, *Phys. Rev.* **47**, 777 (1935).
2. N. Bohr, *Phys. Rev.* **48**, 696 (1935).
3. E. Schrödinger, *Die Naturwissenschaften* **23**, 807; 823; 844 (1935) [English translation by J. D. Trimmer, Proc. Am. Philos. Soc. **124**, 323 (1980).]
4. S. J. Freedman and J. F. Clauser, *Phys. Rev. Lett.* **28**, 938 (1972).
5. K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996).
6. C.H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
7. P. G. Kwiat, K. Mattle, H. Weinfurter and A. Zeilinger, *Phys. Rev. Lett.* **75**, 4337 (1995).
8. W. Tittel, J. Brendel, H. Zbinden and N. Gisin, *Phys. Rev. Lett.* **81**, 3563 (1998).
9. R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther and A. Zeilinger, *Nature* **430**, 849 (2004).
10. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
11. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter and A. Zeilinger, submitted for publication.
12. E. Knill, R. Laflamme, and G.J. Milburn, *Nature* **409**, 46 (2001).
13. R. Raussendorf and H.J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
14. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, *Nature* **434**, 169 (2005).
15. L.K. Grover, *Phys. Rev. Lett.* **79**, 325 (1997).