PHOTONIC ENTANGLEMENT IN QUANTUM COMMUNICATION AND QUANTUM COMPUTATION

A. ZEILINGER*

Institute for Quantum Optics and Quantum Information IQOQI, , Austrian Academy of Sciences, and Faculty of Physics, University of Vienna, A-1090 Vienna, Austria

E-mail: anton.zeilinger@univie.ac.at

Since ISQM 05, entangled photons have been used in our laboratory for a number of novel experiments, both in the foundations of quantum mechanics and in quantum information. Because of the high quality of entanglement of photons, precision tests of a non-local realistic theory proposed by Leggett were possible. These experiments indicate that the concept to be abandoned in quantum mechanics is most likely that of objectivism or realism. In parallel experiments, many schemes of one-way quantum computation were performed. There, because of active feed-forward, one can realize an efficient quantum computer and eliminate the effect of the randomness of individual events. The most significant properties of all-optical quantum computation are the very short cycle time, which can easily be below 100 ns and the high fidelity of the operation. Finally, experiments on quantum entanglement over distances of up to 144 km not only confirmed that quantum communication with satellites is possible, they also allowed novel tests of Bell's inequality.

Keywords: Entanglement; quantum computation; quantum communication.

1. Introduction

The current ISQM Tokyo 08 may be an opportunity to look back 25 years to the *First International Symposium on the Foundations of Quantum Mechanics in the Light of New Technology* which took place in Tokyo in 1983. Back at that time, I was still interested in neutron interferometry, and ISQM 1983 gave us the opportunity to present some results in neutron interferometry where we searched for new physics beyond standard quantum mechanics [1].

While many of these ideas of neutron interferometry are now used routinely in experiments with cold atoms and Bose-Einstein-condensates, it is still most challenging to come up with good experiments testing quantum mechanics with matter waves. Indeed, it is still very difficult to design tests which do not run immediately into inconsistencies.

Back in 1983, this was witnessed by a comment by Professor Y. Nambu after my presentation, where he questions whether it is possible at all to form a consistent theory which would allow for one of the tests we did, namely, the search for a new gauge theory coupling to iso-spin. Luckily, Prof. C. N. Yang came to the rescue, pointing out that our experiment was setting a limit on any gauge theory which contains the iso-spin SU(2) independent of the structure of the entire group.

The reason I point this out is to reflect on the one hand on the enormous progress which has been made in the field, with numerous new experiments in matter wave interferometry of many different systems far beyond the neutron and on the other hand on the fact that, to date, no test theory exists which would allow us to perform broad classes of quantum mechanics without immediately running into internal contradictions or into contradictions with existing experiments.

Obviously, it is a great advantage that experimental progress since then has put many more tools into our hands for performing fundamental experiments on quantum mechanics. One of them is entanglement, which has achieved such a maturity that it can now be applied to various quantum communication and quantum computation protocols.

2. Entanglement - Fundamentals

When in 1935 Einstein, Podolsky and Rosen discussed entanglement for the first time [2], they already presented the apparent conflict with relativity theory because of the instantaneous collapse of the wave function for entangled systems irrespective of distance.

They could actually have referred to Isaac Newton [3] "that Entanglement should be innate, inherent an essential to Matter, so that one Body may act upon another at a Distance thro' a Vacuum, without the Mediation of any thing else … is to me so great an Absurdity that I believe no Man who has in philosophical Matters, a competent Faculty of Thinking can ever fall into it". All I did here was to replace Newton's originally used word "Gravity" by "Entanglement".

While Schrödinger already in 1935 pointed out [4] about entanglement "I would not call that one, but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." Despite this clear indication that entanglement is something very significant, the field lay essentially dormant until John Bell [5] discovered that there is an inherent contradiction between the predictions of quantum mechanics and those of any local realistic theory. This prediction is most striking for the case of entanglement between three or more qubits [6]. There, the situation may arise for the three-photon entangled state

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_1 |H\rangle_2 |H\rangle_3 + |V\rangle_1 |V\rangle_2 |V\rangle_3\right). \quad (1)$$

This state describes three entangled photons, each of them either horizontally (H) or vertically (V) polarized.

There, based on two measurements in a complementary basis, a local realist predicts for the third photon to be, say, vertically polarized while quantum mechanics predicts it to be horizontally polarized. This prediction was confirmed within experimental uncertainty

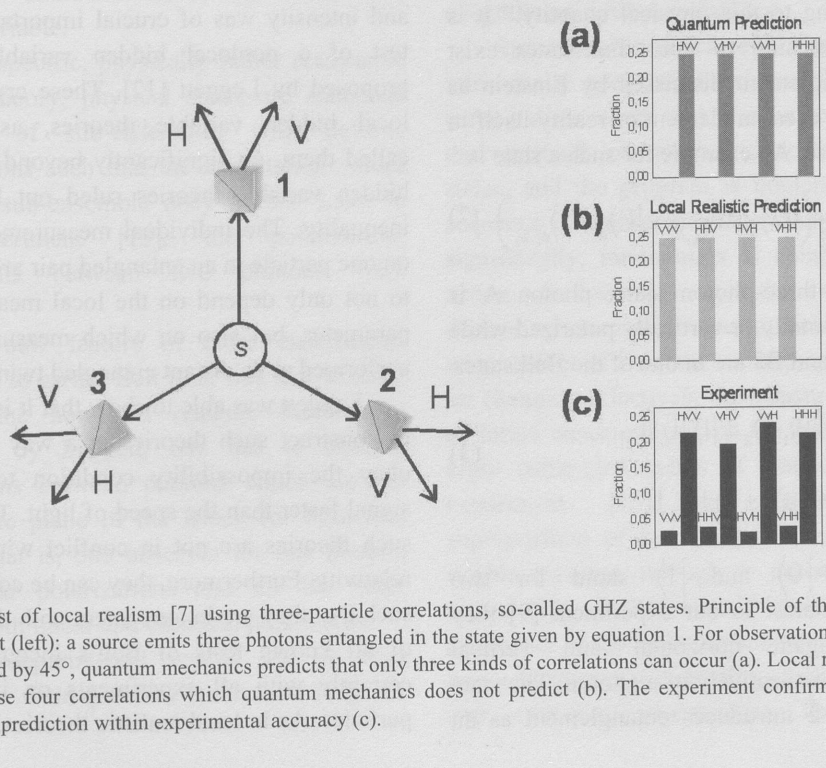

Fig. 1. Test of local realism [7] using three-particle correlations, so-called GHZ states. Principle of the experimental arrangement (left): a source emits three photons entangled in the state given by equation 1. For observation in a conjugate basis rotated by 45°, quantum mechanics predicts that only three kinds of correlations can occur (a). Local realism predicts exactly those four correlations which quantum mechanics does not predict (b). The experiment confirms the quantum mechanical prediction within experimental accuracy (c).

[7] (Fig. 1). It might be interesting to remark that, while such states and also other multi-particle entangled states, for example the so-called W-states [8] were invented just for pointing out fundamental features of quantum mechanics, they have now become central in many quantum computation protocols.

3. Entanglement and Reality

In their 1935 paper, EPR take issue with entanglement and, as they say at the end of the paper, "we believe, however, that such a theory is possible", by which they mean a theory which offers a more complete description of physical reality than quantum mechanics, in particular, it describes a realistic description of entanglement.

The starting point of their argument is the introduction of "elements of physical reality" which are defined in their famous statement "if, without in any way disturbing a system, we can predict with certainty (i.e. with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical quantity." It is therefore amusing to note that states exist where entanglement dismissed by Einstein as "spooky" is even an element of reality itself in the EPR sense. An example for such a state is

$$\left|\Phi^{-}\right\rangle_{a,b}=\frac{1}{\sqrt{2}}\left(\left|H\right\rangle_{a}\left|\phi^{-}\right\rangle_{b_1,b_2}-\left|V\right\rangle_{a}\left|\psi^{+}\right\rangle_{b_1,b_2}\right) \quad (2)$$

In this three-photon state, photon A is either horizontally or vertically polarized while photons B1 and B2 are in one of the Bell states

$$\begin{aligned}\left|\Phi^{\pm}\right\rangle_{12}&=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|0\right\rangle_2\pm\left|1\right\rangle_1\left|1\right\rangle_2\right)\\ \left|\Psi^{\pm}\right\rangle&=\frac{1}{\sqrt{2}}\left(\left|0\right\rangle_1\left|1\right\rangle_2\pm\left|1\right\rangle_1\left|0\right\rangle_2\right)\end{aligned} \quad (3)$$

where the $\left|0\right\rangle$ and $\left|1\right\rangle$ stand for two orthogonal states. In our experiment [9] they represent again horizontal and vertical polarization respectively of a photon. The state of equation 2 introduces entanglement as an element of reality because, depending on whether the polarization of photon a is horizontal or vertical, one may predict with certainty the entangled state for the other two photons. The experiment [9] not only confirms state 2 but also allows to observe the violation of a CHSH inequality for the case where for photon a, the measurement observable was linear polarization while for photons b1 and b2, it was a superposition of two different Bell states.

The recent experiments would not have been possible without significant progress in the development of sources for entanglement. An important step was the development of a source for collinear entangled photons using Sagnac geometry [10]. Recent development [11] allows to produce more than 1 million pairs per second for laser pump powers of a few tens of milliwatts.

4. Testing Nonlocal Realism

The fact that, as just mentiones, recent sources produce entanglement is of both very quality and intensity was of crucial importance for a test of a nonlocal hidden variable theory proposed by Leggett [12]. These crypto non-local hidden variable theories, as Leggett called them, go significantly beyond the local hidden variable theories ruled out by Bell's inequality. The individual measurement result on one particle in an entangled pair are allowed to not only depend on the local measurement parameter, but also on which measurement is performed at its distant entangled twin brother.

Leggett was able to show that it is possible to construct such theories in a way that they obey the impossibility condition to send a signal faster than the speed of light. Therefore, such theories are not in conflict with special relativity. Furthermore, they can be constructed such that they are in agreement with the results of all known tests of Bell's inequality and certainly with all experiments on individual particles. As in local realistic theories, the total

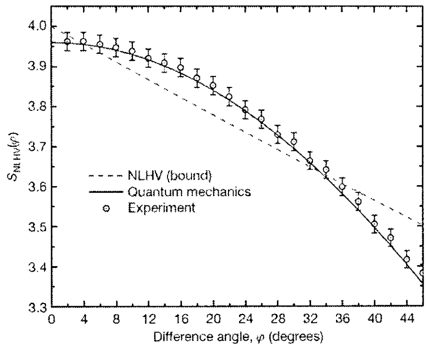

Fig. 2. Test of nonlocal quantum theory of the class proposed by Leggett [12]. The graph (from [13]) shows a specific parameter, a sum of correlations generalized from the original CHSH inequalities. The difference angle is that angle by which one has to go with the measurement of elliptical polarization of one photon out of the plane defined by the linear polarization of the other photon in the Poincaré sphere. The limit for a nonlocal hidden variable scheme is given by the dashed line. The experiment clearly violates this limit and thus rules out the theories of the class tested. It should be mentioned that in the same experiment, a violation of a CHSH inequality was also observed, thus ruling out not only the new nonlocal theories, but also local realism in the usual way.

ensemble of particles is divided into sub-ensembles characterized by distributions of hidden variable.

In a specific, physically rather reasonable type of theory, physical states are statistical mixtures of sub-ensembles with definite polarizations such that the expectation values for each sub-ensemble obey Malus' Law. In the experiment [13], the polarization-correlations between two photons were observed.

The new feature of these experiments compared to earlier Bell tests was that in order to test the non-local realistic theories as proposed by Leggett, one has to observe correlations between photons which are not within one plane of the Bloch (or Poincaré) sphere, that is, one observes for one photon, say, linear polarizations and for the other photon both linear and elliptical polarization.

The experimental results are in clear agreement with quantum mechanics (Fig. 2). This confirms that certain specific nonlocal variants of a realistic theory proposed by Leggett are not viable. While the theory ruled out was an intuitively rather reasonable alternative to quantum mechanics, the question is left open which more, possibly less intuitive nonlocal variants might also be ruled out in future experiments.

5. Quantum Computation with Entangled Photons

It is well known that due to the lack of effective photon-photon interactions, the implementation of quantum computation with photons only provides a significant challenge. As has been shown in the seminal paper by Knill, Laflamme and Milburn [14], one nevertheless can implement quantum computation using linear optical elements only. The essential idea here is to exploit the fact that the measurement process in quantum mechanics is outside the linear and unitary quantum evolution. Yet, the intrinsic randomness of quantum measurement implies a significant limit to scalability.

Raussendorf and Briegel [15] suggested an intrinsically non-unitary scheme for quantum computation where this can be overcome. In that approach, one starts with so-called cluster states, and the program is implemented by a sequence of measurements on that state. Most significantly, randomness is compensated by active feed-forward in the sense that, depending on earlier measurement results on some qubits of the state, unitary operations are set changing effectively the measurement bases of future measurements on the remaining, still higly enttangled qubits of that state. In the experiment [16], we used coherent superposition of two photon pairs created in double passage through a down-conversion crystal (Fig. 3). We were able to demonstrate [16] some of the most fundamental concepts of one-way quantum computing including single and two-qubit operations. The intrinsic

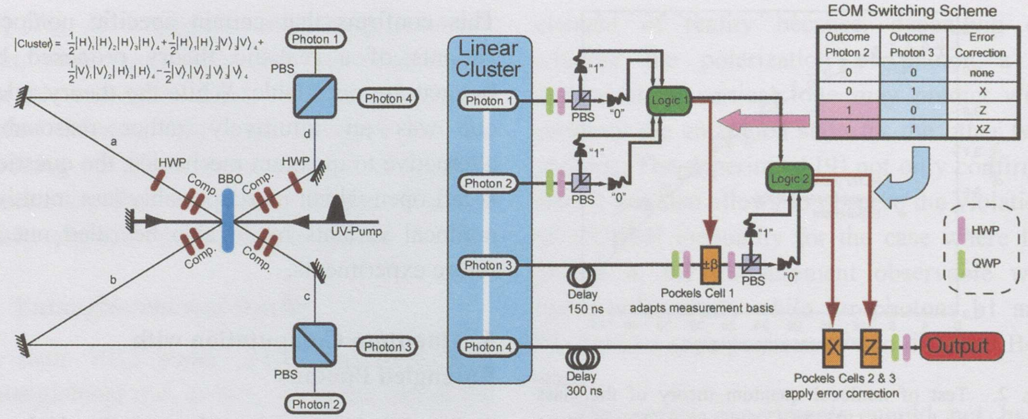

Fig. 3. Experimental one-way quantum computation. Left: A UV pulse passing twice through a nonlinear BBO crystal creates probabilistically two pairs of entangled photons. Coherent superposition of two photons each at the two polarizing beam splitters PBS create the cluster state shown under the condition that one photon each is detected in one of the four detectors. This set-up requires interferometric stability over a long time. The proper state is set by half-wave plates (HWP) at appropriate angles. Right: Linear optics quantum computation with active feed-forward. Depending on the measurement results of photon 1 and photon 2, the measurement basis for photon 3 is adapted using a Pockels cell which can implement a polarization rotation by the angle ±β. Finally, depending on the then obtained results on all three photons, Pauli errors can be corrected by applying the proper spin rotations, again with Pockels cells on photon 4. These two operations are the most basic building blocks for linear optics quantum computation with active feed-forward. The insert shows the logic of the switching scheme (from [16] and [18]).

quantum nature of the procedure was demonstrated by violating a cluster-state Bell inequality [17].

In a more recent experiment [18], active feed-forward was implemented. In the experiment, both rotations of the measurement basis and Pauli error corrections could be achieved using fast detectors, rapid electronics and Pockels cells. It should be noted that one such cycle from measurement all the way to the setting of the new parameter took less than 150 ns.

Our one-way quantum computation scheme was applied to a number of basic quantum computation protocols. These include the realization of Deutsch's algorithm [19], decoherence-free quantum information transfer [20], the realization of a quantum version of prisoner's dilemma [21] and of Grover's search algorithm [16]. Future challenges of all-optical quantum computation certainly include the development of efficient sources for multi-photon entangled states, of detectors with both higher efficiency and the ability to discriminate photon numbers, and of feed-forward schemes with even shorter time constants. All these goals seem to be within reach of technology in reasonable time.

6. Long-Distance Quantum Communication

In the time since the last ISQM, a significant part of the work of our group was to extend quantum communication both to larger distances and to higher data rates, higher fidelity and towards more technical applications. In terms of distance, we are routinely operating a quantum communication link between the Canary Islands of Tenerife and La Palma [22].

Typically, on La Palma, we implement a source generating entangled photons, and on Tenerife we utilize the telescope of the Optical Ground Station (OGS) operated by the European Space Agency ESA. As an example, we might discuss the transmission of one of two entangled photons. A source on La Palma generates an entangled pair, of which one photon is measured by Alice on La Palma and the other photon is transmitted through an optical telescope over to Tenerife. In parallel to the quantum link, we operate tracking lasers to correct for the atmospheric instability. This is done by readjusting both the sending and the receiving telescope continuously in real time. In the experiment mentioned, both photons are measured using polarizing beam splitters, one rotated by 45° relative to each other. This makes it possible to implement the BBM protocol of quantum cryptography.

Using this scheme, it was both possible to violate the Bell inequality for the photon locally measured and the transmitted photon as well as to establish a quantum cryptography key. It should be noted that the attenuation across the link between La Palma and Tenerife is comparable to the typical attenuation between a ground station and a satellite in low-earth orbit. In the long run, we intend to establish an entangled source on a satellite and transmit either one or both photons to ground stations on Earth [23].

7. Concluding Comments

After having been a philosophical curiosity in the 1930s, entanglement has significantly matured over the last 20 years as a resource for quantum communication and quantum computation. Photonic entanglement will certainly remain one of the most essential resources for long-distance quantum communication. Besides that, all-optical one-way quantum computation offers a very exciting perspective, paralleling quantum computation with other means.

Acknowledgments

This work was supported by the Austrian Science Funds FWF, by the European Commission (projects QAP and EMALI), by the IARPA-funded U.S. Army Research Office (QCCM) and by the European Space Agency.

References

1. A. Zeilinger, M.A. Horne and C.G. Shull, in *Proceedings of the International Symposium on Foundations of Quantum Mechanics in the Light of New Technology*, (S. Kamefuchi et al., Eds.), Phys. Soc. Japan, Tokyo, 289-293 (1983).
2. A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
3. Newton to Bentley, February 25, 1692 / 3.
4. E. Schrödinger, Proceedings of the Cambridge Philosophical Society **31**, 555 (1935).
5. J.S. Bell, Physics **1**, 195 (1964).
6. D.M. Greenberger, M.A. Horne, A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, (M. Kafatos, Ed.), Kluwer, Dordrecht, 69 (1989); arXiv: quant-ph 0712.0921.
7. J.W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, A. Zeilinger, Nature **403**, 515 (2000).
8. A. Zeilinger, M.A. Horne, D. Greenberger, in *Proceedings of the NASA Conference „Squeezed States and Quantum Uncertainty"*, NASA Conference Publication 3135, 73-81 (1992).
9. P. Walther, K. J. Resch, C. Brukner and A. Zeilinger, Phys. Rev. Lett. **97,** 020501 (2006).
10. T. Kim, M. Fiorentino and F. N. Wong, Phys. Rev. A **73**, 012316 (2006).
11. A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein and A. Zeilinger, Optics Express **15**, 15377-15386 (2007).
12. A.J. Leggett, Found. Phys. **33**, 1469 (2003).
13. S. Gröblacher, T. Paterek, R. Kaltenbaek, C. Brukner, M. Zukowski, M. Aspelmeyer and A. Zeilinger, Nature **446**, 871-875 (2007).
14. E. Knill, R. Laflamme and G. J. Milburn, Nature **409**, 46 - 52 (2001).

15. R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 - 5191 (2001).
16. P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, Nature **434**, 169 - 176 (2005).
17. P. Walther, M. Aspelmeyer, K.J. Resch, and A. Zeilinger, Phys. Rev. Lett. **95**, 020403 (2005).
18. R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhi, R. Kaltenbaek, T. Jennewein and A. Zeilinger, Nature **445**, 65 – 69 (2007).
19. M. S. Tame, R. Prevedel, M. Paternostro, P. Böhi, M. S. Kim and A. Zeilinger, Phys. Rev. Lett. **98**, 140501 (2007).
20. R. Prevedel, M. S. Tame, A. Stefanov, M. Paternostro, M. S. Kim and A. Zeilinger, Phys. Rev. Lett. **99**, 250503 (2007).
21. R. Prevedel, A. Stefanov, P. Walther and A. Zeilinger, New Journal of Physics **9**, 205 (2007).
22. 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, Nature Physics **3**, 481 - 486 (2007).
23. J. Perdigues Armengol, B. Furch, C. J. d. Matos, O. Minster, L. Cacciapuoti, M. Pfennigbauer, M. Aspelmeyer, T. Jennewein, R. Ursin, T. Schmitt-Manderbach, G. Baister, J. G. Rarity, W. Leeb, C. Barbieri, H. Weinfurter and A. Zeilinger, Acta Astronautica **63,** 165 – 178 (2008).