Quantum Noise and Quantum Communication

Thomas Jennewein[a], Anton Zeilinger[*a,b]

[a]Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Boltzmanngasse 3, A-1090 Vienna, Austria

[b]Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Vienna, Austria

ABSTRACT

We show how the probabilistic interpretation of quantum mechanics leads to unavoidable quantum noise, even for deterministic evolution of the quantum state. Far from being a nuisance, this consequent quantum randomness is at the heart of new concepts in technology. We discuss explicitly the quantum random number generator based on the partitition noise at the beam splitter. Another application of quantum noise is quantum cryptography, where the randomness of the detection event leads to the generation of a random cryptographic key at two locations without the necessity of transporting that key from A to B. Finally, we will show how quantum noise is an intrinsically important part of quantum teleportation, and we conclude with a brief discussion of the possibilities of free-space quantum communication.

Keywords: quantum noise, quantum communication, quantum information, entanglement, quantum teleportation

1. INTRODUCTION

It appears that very early in the development of quantum mechanics, it was realized that randomness plays a new role which transcends its role in classical physics. Witness for example Albert Einstein, who expressed his misgivings about the new role of chance in quantum physics as early as 1908. He more explicitly expressed the same feeling in his famous 1917 paper, where he introduced the concepts of induced transition and spontaneous transition between atomic levels. Einstein explicitly says there: „Die Schwäche der Theorie liegt ... darin, dass sie Zeit und Richtung des Elementarprozesses dem „Zufall“ überlässt.“ (“The weakness of the theory lies ... in the fact, that it leaves time and direction of the elementary process to “chance”, translation by A. Zeilinger)”[1].

Far from removing randomness from the theory, chance and probability have been raised to playing a pivotal role in the interpretation of the mathematical formalism by Born’s rule, where he explicitly states that the square of the wave function $|\psi|^2$ gives directly the probability for, say, finding a particle somewhere or for some electronic transition etc.

[*]zeilinger-office@ap.univie.ac.at; phone +43 (1) 4277 51201; fax +43 (1) 4277 9512, www.quantum.univie.ac.at

Fluctuations and Noise in Photonics and Quantum Optics II, edited by Peter Heszler, Derek Abbott, Julio R. Gea-Banacloche, Philip R. Hemmer, Proceedings of SPIE Vol. 5468 (SPIE, Bellingham, WA, 2004) 0277-786X/04/$15 · doi: 10.1117/12.561308

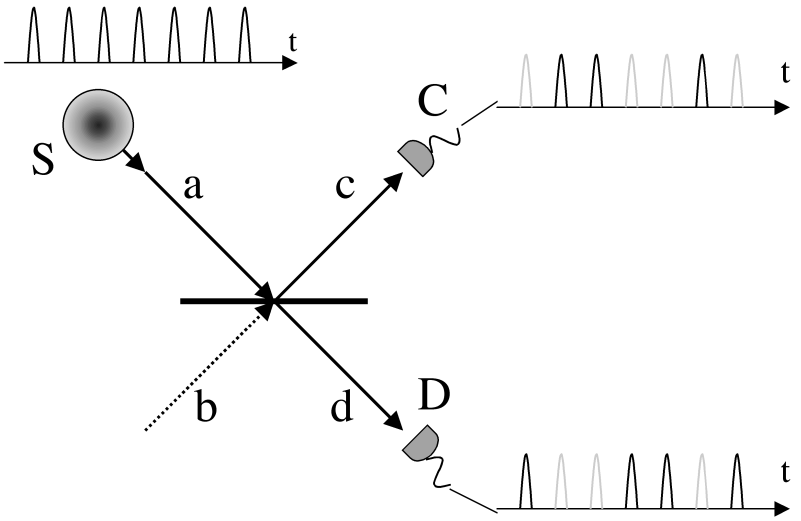

Figure 1. A train of single particles from a source *S* is split up on a semi-reflecting beam splitter. We consider individual particles (photons, electrons, atoms, molecules…) incident on the beam splitter. The probability to find the particle in each output port is then just 1/2. Thus, an ordered sequence of incident particles gives rise to random sequences of detection "clicks" in both output ports.

To discuss the nature of randomness in quantum mechanics more explicitly, let us consider a simple experimental setup (Fig. 1), a semi-reflecting beam-splitter. Let us first analyze such a beam splitter from a classical point of view. An incident light wave is split by the beam splitter in two halves, such that each of the two outgoing beams carries half the energy. Clearly, this is easily understood. Let us now consider the quantum situation. We assume that we have one, and only one, particle at a time incident on the beam splitter, from, say, port *a*. We describe this by using the symbol $|a\rangle$, which is a vector in Hilbert space employing that the individual particle is in beam *a*, and analogously, $|b\rangle$, $|c\rangle$, $|d\rangle$ describes the state of a particle being in the respective beams. The beam splitter then acts on the incident state in the following way:

$$|a\rangle \rightarrow \frac{1}{\sqrt{2}}\left(i|c\rangle + |d\rangle\right) \tag{1}$$

Here, we have assumed that the reflected wave picks up a phase jump of $\pi/2$ upon reflection. The general rules describing beam splitter behaviour are slightly more complicated[2]. According to Born's rule, the probability to find the particle in beam *c* or in beam *d* is then just the absolute square of the corresponding probability amplitudes, i.e.

$$p(c) = \left|i/\sqrt{2}\right|^2 = 1/2, \quad p(d) = \left|1/\sqrt{2}\right|^2 = 1/2 \tag{2}$$

that is, just as expected, we find a particle with the equal probability of 50% in either beam *c* or *d.* Yet, nothing in quantum theory whatsoever allows us to make any predictions about the individual event, that is, no prediction about in which of the outgoing beams the individual particle will be registered. We also note that the particles could be photons, electrons, neutrons, atoms, molecules etc.

Therefore, an incident stream of particles, be it regular or not, gives raise to random output at a beam splitter, which can actually be used to build a random number generator. We note two more points. Firstly, the quantum state after the beam splitter, as described in equation 1, is actually a coherent superposition of the two possibilities of finding the particles in beam *c* and *d*. Thus, before the performance of an actual measurement, designed such that the path *c* or *d* is determined, the state does not contain any path information. Performing the measurement is actually necessary to obtain

randomness. We might, secondly, understand the importance of superposition by assuming that the incident beam is in a superposed state of beams *a* and *b*. An example is

$$|\psi\rangle_{incident} = \frac{1}{\sqrt{2}}\left(|a\rangle + i|b\rangle\right), \quad |\psi\rangle_{outgoing} = i|c\rangle \tag{3}$$

Then, all particles end up with probability 1 in beam *c* and none in beam *d*.

We conclude that the measurement of the output ports of a beam splitter results in noise even if the incident radiation is perfectly structured for example, when the particles come at equal time intervals (see Fig. 1). The resulting noise, often also somewhat misleadingly called partition noise, is, as we have shown above, not a consequence of individual particles taking either way, but a consequence of the probability interpretation of quantum mechanics and of the fact that an incident quantum state is divided into two. In other words, while there is quantum noise upon detection, the evolution of the quantum state as described by the Schrödinger equation is always deterministic.

2. QUANTUM NOISE AND RANDOM NUMBER GENERATION

It is straight forward to exploit the inherent randomness of quantum noise observed after the semi-reflecting mirror to generate random signals and numbers. We have developed and used such devices[3] for a fundamental experiment on quantum entanglement[4]. The requirement for these random signal generators was that they were a) physical, b) very fast, i.e. the random signals have a correlation time of less than about 100 ns. This difficult requirement was easily achieved with a device based on the quantum noise generated by measuring single photons after a semi-reflecting mirror (Fig 1), with two photo multiplier tubes as detectors, and a dimmed light emitting diode as the source of photons. The principle of the quantum noise signal generation is to combine the signals of detectors C and D (Fig. 1) in a RS-flip-flop, where a "click" in detector C triggers the Set-input, i.e. the flip-flop is set to "1" and detector D triggers the Reset-input, i.e. the output of the flip-flop is set to "0". This system was built in a small compact housing and finally produced a digital random signal with an autocorrelation time of about 11 ns. The next step was to sample this random digital signal with a regular clock in order to generate strings of random numbers at a rate of up to 1 Mbit/second. The analysis of 80 Mbit samples showed the high quality of the quantum randomness, which was also confirmed by tests performed by independent institutions[5], who tested sample random numbers generated with our quantum random number generator.

The intriguing feature of a quantum number generator based on a beam-splitter is the simplicity and clarity of the source of randomness, as well as the possibility to scale up its speed which is finally limited by the speed of the detectors and the electronics. Such devices are already in use in commercial quantum communication systems, but quantum randomness could well be used in classical areas such as computing, cryptography or even lottery machines, where good random numbers are a necessity.

3. QUANTUM NOISE AND INFORMATION

Let us recall an interesting observation when discussing the behaviour of an individual quantum system at the beam splitter as shown in Fig. 1. There are two extreme situations. If the incident quantum system occupies only one mode, *a* or *b*, then, as described in Eq. 1, there is equal probability to find it in either output mode. In other words, if the incident state is noiseless, we obtain maximum noise in both outputs.

On the other hand, if the incident state is in a superposition, as described by Eq. 3, that is, the incident quantum system occupies both modes, *a* and *b*, with equal probability and with the proper phase, then the output system will definitely be found in one mode only, in that case, mode *c*. We remark that this phenomenon depends on the relative phase $\pi/2$. If the phase were $-\pi/2$, then the output mode *c* would be occupied, and if it had another, arbitrary value, λ, the situation is somewhat more complicated, but it is always possible to define an observable with definite value. So, we conclude, that

in the situation described by Eq. 3, we have maximum noise at the input of the beam splitter (if a measurement of the state were performed) and no noise at the output.

It does therefore appear that the noise during evolution of the quantum system passing through the beam splitter – which serves as the simplest possible example of a quantum device – is unavoidable. We can either choose to have the noise appear in the output or in the input. Also, not discussed explicitly here, an intermediate situation with partial noise at the input and at the output is also possible. This is a consequence of the observation that the individual quantum system in that situation can be described as carrying one bit of information only[6] and it is up to the experimenter by choosing the input state, that is, by choosing the appropriate apparatus for preparing the quantum system, whether this one bit of information carried by the system defines the input state perfectly, without noise, or the output state perfectly. Then, if the single bit available is used up, other observations are random by necessity. We conclude that quantum noise is a consequence of the finiteness of information carried by a quantum system.

4. QUANTUM NOISE AND ENTANGLEMENT

A conceptually interesting situation arises when one considers quantum states describing two or more systems. It was first realized by Einstein, Podolsky and Rosen (EPR)[7] that systems which once interacted stay connected in a very interesting way. More precisely, it may appear that measurement on one system defines the quantum state of the other system, no matter how far it is away. Erwin Schrödinger, who coined the notion "entanglement" for that situation, wrote explicitly: "In particular, there exists at all times the one-to-one entanglement of all variables together with its evil consequences." [8]. We now discuss the salient features of entanglement with the help of a two-photon interferometer (Fig. 2). There, we have a source *S* which can emit two particles, one to the left and one to the right. For particle 1, two beams, i.e. two modes of propagation, are available, *a* and *b*. These two modes are recombined at a beam splitter of exactly the kind we discussed above. Finally, the particle may be registered in the outgoing modes by detectors *A* and B. Similarly, particle 2 propagating to the right has modes *c* and *d* available, which are also mixed at the beam splitter and the particle may be detected in detectors *C* and *D*. We might first discuss the situation where particle 1 is emitted somehow into its modes *a* and *b* independent of particle 2 and vice versa. Then, exactly the same reasoning as above applies. If the particle is emitted into either of these modes, then we have maximum noise at detectors *A* and *B*, if it is emitted into the proper superposition, we can have the situation where no noise at the detectors arises. The same situation applies for particle 2.

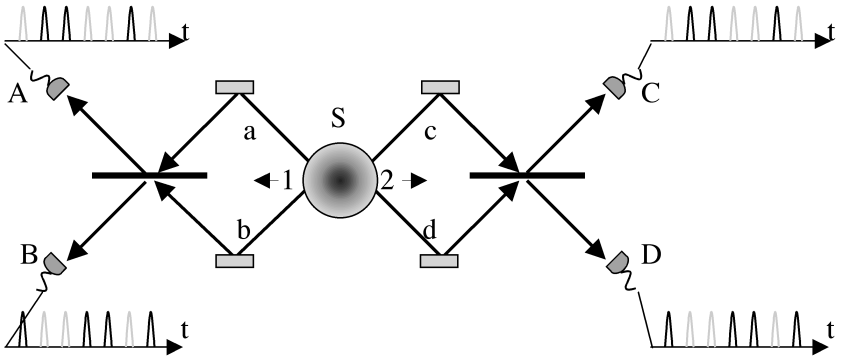

Figure 2. The mode entanglement strictly correlates the detection result of the two particles, although each particle is sent through a semi reflecting beam splitter. If particle 1 is found in detector *A*, then particle 2 will be found in detector *C*.

We now consider a situation where the two particles are emitted into the entangled state.

$$|\psi\rangle_{initial} = \frac{1}{\sqrt{2}}\left(|a\rangle|d\rangle_2 + |b\rangle_1|c\rangle_2\right) \tag{4}$$

This is a maximally mode-entangled state. Its meaning simply is that particle 1 might be emitted either into mode *a* or *b* and particle 2 into mode *c* or *d*, just as we discussed before, but now, the two particles are completely correlated. If particle 1 is emitted into mode *a*, then particle 2 is emitted into mode *d* and vice versa. Also, if particle 1 is emitted into mode *b*, then particle 2 is emitted into mode *c* and vice versa. But this state does not describe a mixture of the two possibilities, but a coherent superposition. The consequence of this superposition will be seen if we analyze the detector responses. It can readily be seen that the output state after both beamsplitters is

$$\frac{i}{\sqrt{2}}\left(\left|A\right\rangle_1\left|C\right\rangle_2+\left|B\right\rangle_1\left|D\right\rangle_2\right) \tag{5}$$

where, for example, $|A\rangle$ describes the state of a particle in the mode leading to *A*. Let us now leave the formalism behind and discuss the detector responsibilities and the quantum noise in that experiment by analyzing the experimental consequences of the states of Eq. 4 and Eq. 5.

At first, we realize that, should we decide to place detectors into any of the modes *a, b, c* or *d*, then each of these detectors will fire with 50% probability. That is, maximal noise results. Yet, let us now look at the situation when detectors placed into these modes fire together. We immediately realize that the detector in mode *a* will always fire together with the detector in mode *d*, and the detector in mode *b* will always fire together with the detector in mode *c*. This means that the noise in either of these modes, conditioned on the detection of a particle in the other mode disappears. The reason is simply correlation, the fact that the particles are emitted together in pairs from the source. This might still be understood in a classical way, assuming that the source emits the particles half in the modes *a*-*d* and half in the modes *b*-*c*.

This picture breaks down when we analyze the counts in the detectors *A, B* and *C, D* behind the beamsplitters. There, we realize that a similar correlation is obtained. Each of the four detectors fires randomly with the same probability of 50%. Again, we have maximal noise in these outputs. On the other hand, we have perfect correlation, that is, if we know that detector *A* fired, we know definitely that detector *C* also fired. So, the noise conditioned on detection of one particle on one side disappears. Why does this contradict the possibility that the particles emitted by the source are in an incoherent mixture, as we just discussed? Let us focus on the ensemble of photons emitted as pairs, one in mode *a* and the other one in mode *d*. The photon in mode *a* has a 50/50 chance to trigger detector *A* or *B*, likewise, the photon in mode *d* has a 50/50 chance to trigger the detector *C* or *D*. Evidently, these are completely uncorrelated, and therefore, the noise conditioned on detection on one side does not disappear. It is only the quantum entanglement in Eq. 4 which results in the suppression of the conditional noise.

Interestingly, quantum noise and quantum entanglement recently led to novel concepts in communication. Of those, Dense Coding[9] was the first one to find experimental realization[10]. Other very interesting applications of quantum noise and entanglement are quantum cryptography and quantum teleportation, which we will discuss in the following.

5. QUANTUM NOISE AND QUANTUM CRYPTOGRAPHY

While the randomness of the individual quantum event, that is, quantum noise, has for a long time been viewed as a limitation of the possibility for an experimentalist, it has recently found a number of applications in communication. The most interesting one is quantum cryptography[11].

In entanglement-based quantum cryptography[12], one uses entangled states very similar to the situation of Fig. 2. For practical reasons, instead of employing a two-particle interferometer, one can use photon states entangled in polarization[13]. But the basic physics and the conceptual situation are the same. The idea is to utilize the perfect correlations between the detectors on both sides *A, B* and *C, D* to establish a random key. It has been known since Vernam[14] that a random key which is only used once ("one-time pad") provides a method to encrypt information in a way that its safety is guaranteed by the laws of physics. If we assign to a detector click in detectors *A* and *C* the bit values "1" and to a detector click in detectors in *B* and *D* the bit values "0", then, obviously, because of the perfect

correlation, Alice on the right-hand side and Bob on the left-hand side obtain the same sequence of random numbers. This sequence is secure against eavesdropping because any eavesdropper who tries to intercept the propagating photons between both sides can easily be detected, as she would destroy the perfect correlations. More details might be found elsewhere. From a conceptual point of view, we underline that the interesting feature of entanglement-based quantum cryptography is that the key, which is used by Alice and Bob, does not have to be transported between the two sides anymore, but it only comes into existence by the measurements performed by the two players. This means that the severe security problem of key distribution disappears.

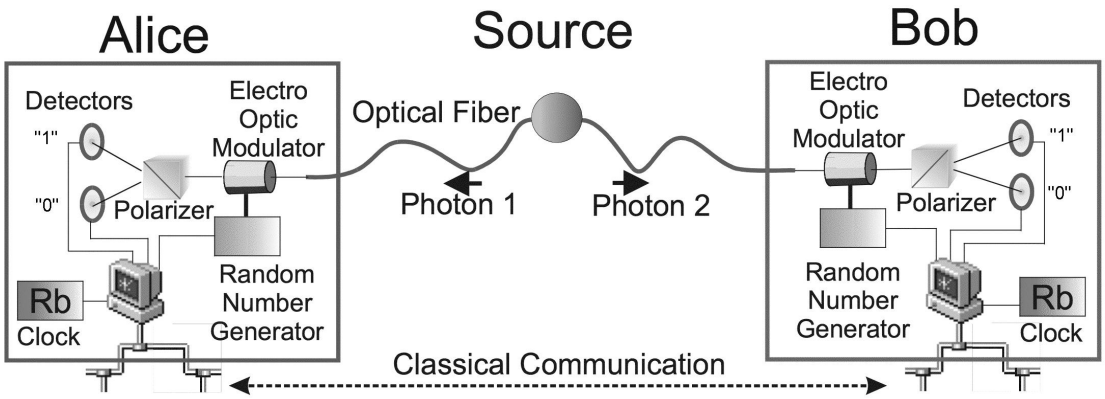

Figure 3. Quantum Cryptography based on polarization-entangled photons. Alice and Bob both measure the polarization of their photon. Due to the entanglement, they will generate identical but perfectly random sequences of measurement results[13].

6. QUANTUM NOISE AND QUANTUM COMMUNICATION

A conceptually rather striking application of entanglement is quantum teleportation[15]. Thereby (Fig. 4), one teleports the quantum state of an unknown system using an additional entangled pair. Alice, who wants to teleport the original state, subjects the original photon and one of the two photons from the entangled pair to a so-called Bell-state measurement. This is a measurement which entangles the photon whose state is to be teleported and her member of the entangled pair. That measurement projects Bob's photon immediately into a state which is uniquely related to the original such that, in principle, it contains already all the information. Yet most interestingly, in a Bell state measurement of two-state systems[16], as signifies all experiments performed so far, four possible results for the Bell-state measurement exist. According to the specific result, Bob has to perform a unitary operation on his photon. We note that in one of the four possible results, Bob's photon is immediately in the original state. This might appear to imply a violation of Einstein locality, i.e. signalling faster than the speed of light. Yet, it is now the existence of quantum noise which actually prohibits such a violation. It turns out that the four measurement results for Alice's Bell state measurement are completely random, that is, there is maximal noise in the output of the Bell state analyzer. This implies that on Bob's side, the four states in which his photon ends up are also completely randomly distributed and therefore taken together do not contain any information. Bob has to await receiving a signal from Alice, telling him which specific result was obtained for which specific photon allowing him to put his photon back into the exact initial state of the original.

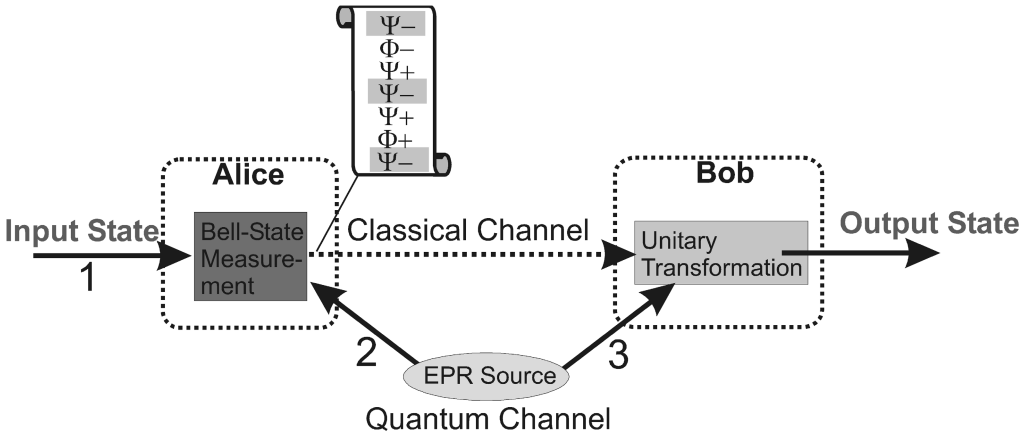

Figure 4. The basic concept of quantum teleportation. Alice and Bob can transfer a quantum state from particle 1 to particle 3 via a quantum channel and a classical channel. The information conveyed by the two channels separately is purely random, but by combining the two, Bob obtains a perfect replica of the input state.

Conceptually most striking is the case of quantum teleportation an entangled state is teleported, also called entanglement swapping[17] (Fig. 5). Future quantum computers are expected to use quantum teleportation for internal and external communication.

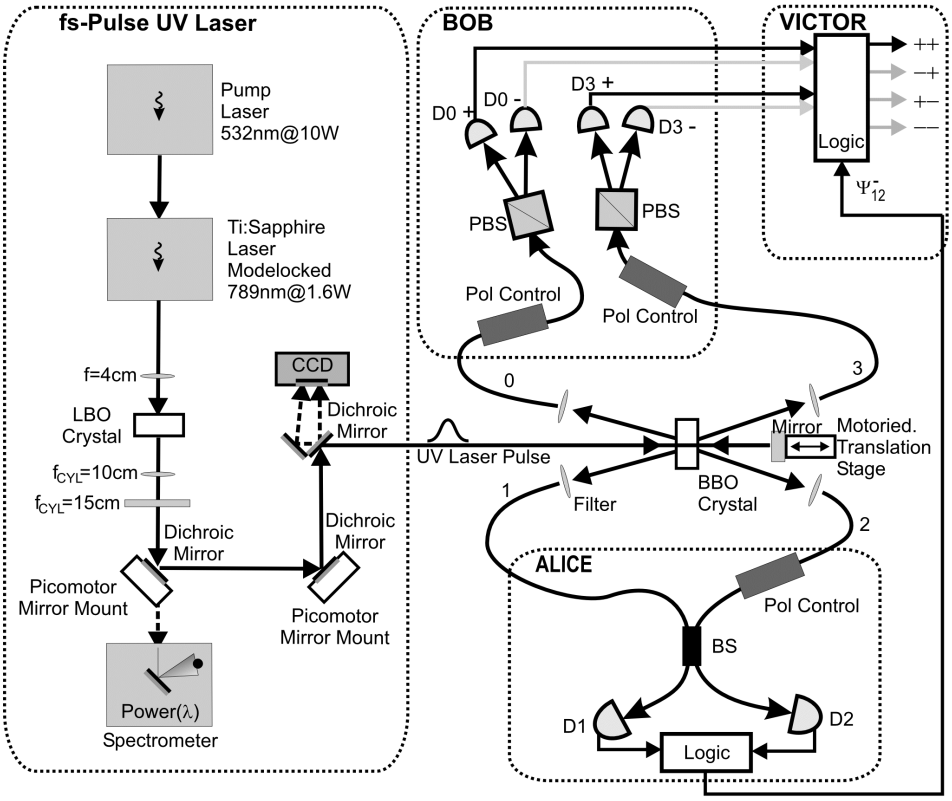

Figure 5. Experimental setup of the teleportation of entanglement[17].

Another interesting question is over how large distances quantum communication can be established. A significant limitation arises because quantum states cannot be amplified without disturbing the state. Therefore, quantum

communication is presently limited by the unavoidable loss of photons. The limit both in free-space communication and in communication using glass fibres is of the order of a few tens of kilometres. Therefore, quantum communication via satellites provides an interesting possibility for reaching distances even on a global scale. In a recent experiment[18], quantum entanglement was established in a realistic environment over significant distances of 600 m (Fig.6). Worldwide quantum communication becomes feasible once satellites are employed to carry sources for entangled photons. Then, the photons have to propagate only through a few kilometres of atmosphere and the consequent attenuation is technically acceptable.

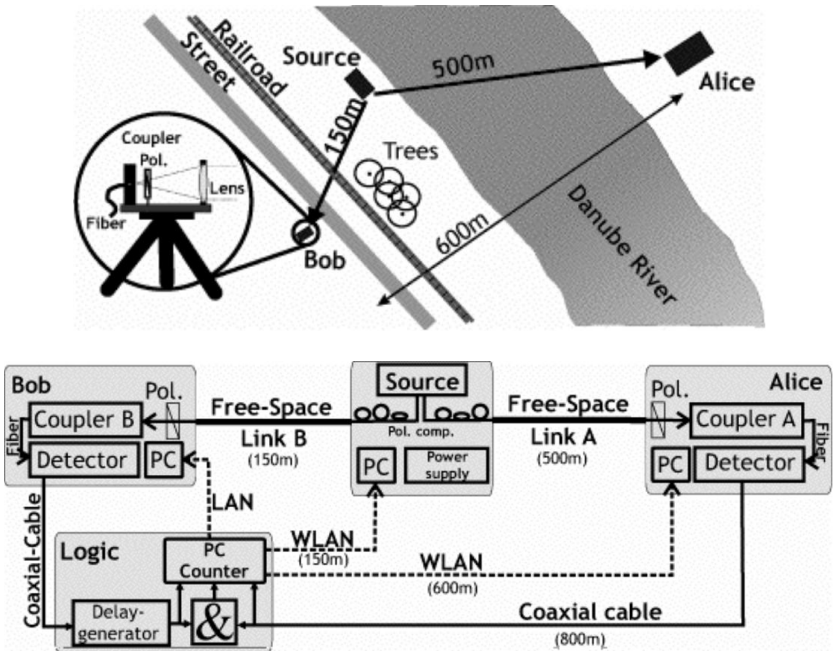

Figure 6: Experimental arrangement of free-space distribution of entanglement across large distances[18].

ACKNOWLEDGMENTS

This work was supported by the Austrian Science Foundation (FWF), project number SFB 015 P20 and the European Commission, contract number IST-2001-38864 (RAMBOQ).

REFERENCES

1 A. Einstein "Zur Quantentheorie der Strahlung" (On the Quantum Theory of Radiation), *Physika Zeitschrift* , *Volume 18*, 121-128, 1917.

2 A. Zeilinger “General properties of lossless beam splitters in interferometry”, *Am. J. Phys. 49,* 882, 1981.

3 T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger "A fast and compact quantum random number generator" *Rev. Sci. Inst. 71*, 1675-1680, 2000.

4 G. Weihs, T. Jennewein, Ch. Simon, H. Weinfurter, A. Zeilinger "Violation of Bell's inequality under strict Einstein locality conditions" *Phys. Rev. Lett. 81,* 5039 (1998).

5 1) Dr. Joop M. Houtkooper, Institut fuer Psychobiologie und Verhaltensmedizin, Justus-Liebig-Universitaet Giessen, (email communication, 8. July 2002). 2) Stefan Pyka, Siemens AG, CT IC 3, D-81730 Muenchen,

(email communication, 15.April 2002). 3) Peter Hellekalek, Institut fuer Mathematik, University Salzburg, A-5020 Salzburg / Austria (email communication, 12.December.2002).

6 A. Zeilinger, "A Foundational Principle for Quantum Mechanics", *Found. Physics Vol. 29 no. 4,* (1999) 631; C. Brukner and A. Zeilinger "Young's experiment and the finiteness of information", *Phil. Trans. R. Soc. Lond. A 360,* 1061 (2002).

7 A. Einstein, B. Podolsky, and N. Rosen. "Can quantum-mechanical description of physical reality be considered complete?" *Phys. Rev. 47,* 777–780, 1935.

8 E. Schrödinger, "Die Gegenwärtige Situation in der Quantenmechanik", *Naturwissenschaften 23,* 807--812, 823--828, 844--849, 1935.

9 C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett., vol. 68,* p. 557, 1992.

10 K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," *Phys. Rev. Lett., vol. 76,* p. 4656, 1996.

11 C. H. Bennett and G. Brassard, in *Proceedings of the InternationalConference on Computer Systems and Signal Processing,* Bangalore, 1984, p. 175; C. H. Bennett, G.Brassard, and A. Ekert, *Sci. Am. 267,* 26 1992.

12 A. K. Ekert, "Quantum cryptography based on Bell's theorem" *Phys. Rev. Lett. 67,* 661 1991.

13 T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger "Quantum Cryptography with Polarization Entangled Photons", *Phys. Rev. Lett. 84,* 4729-4732 2000.

14 G. S. Vernam, *J. Am. Inst. Elec. Eng. 55,* 109, 1926.

15 C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K.Wootters. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels" *Phys. Rev. Lett. 70 (13),*1895–1899, 1993.

16 D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature, vol. 390,* p. 575, 1997.

17 M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "Eventready-detectors Bell experiment via entanglement swapping," *Phys. Rev. Lett. vol. 71, no. 26,* pp. 4287–4290, 1993; T. Jennewein, G. Weihs, J.W. Pan, and A. Zeilinger, "Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping", *Phys. Rev. Lett., vol. 88,* p. 017903, 2002.

18 M. Aspelmeyer, H. R. Bohm, T. Gyatso, T. Jennewein, R. Kaltenbaek, M.Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, "Long-distance free-space distribution of quantum entanglement," *Science, vol. 301,* p. 621, 2003.