

Entangled State Quantum Key Distribution and Teleportation

A. Poppe (1), A. Fedrizzi (1), H. Hübel (1), R. Ursin (1), A. Zeilinger (1,2)

1 : Institut fuer Experimentalphysik, Universitaet Wien, Boltzmannngasse 5, 1090 Wien, Austria
andreas.poppe@univie.ac.at

2 : Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences,
Boltzmannngasse 3, 1090 Wien, Austria

Abstract *To achieve highest security in quantum cryptography, entanglement must be implemented. The generation and distribution of polarization entangled photon pairs will be discussed as the basis for quantum key distribution, teleportation and quantum repeater.*

Introduction

Quantum physics has excited and fascinated people for the last century. However it is only in the last decades that novel applications were found, that would make explicit use of the fundamental principles of quantum mechanics. The field of quantum information emerged. The information is encoded on single quantum states called qubits. This allows extending the rules of quantum physics to information science. In contrast to classical bits, the quantum mechanical approach can exhibit features like superposition or entanglement of qubits and therefore of the information, which gives rise to many interesting and valuable applications. Today many experimental implementations exist in the laboratory and some are already on the way to commercialization [1].

Entanglement plays a decisive role in many quantum communication and quantum computation schemes. As a physical resource for these protocols it is important to be able to generate, manipulate and distribute entanglement as accurate and efficient as possible.

Classical communication

Nowadays classical communication via optical fibres is very well established. An enormous amount of data is transferred to almost every place of the world having deep impact to the economic and political situation. The sender encodes all data, whether it is highly secure data or spam, in bits and corresponding optical pulses which are sent over the fibre system. At a transmission rate of GBit/s at the wavelength of 1550nm the typical pulse energy is in the pJ level. That corresponds to many million photons per bit and subsequently the receiver electronics is possible to make a decision between "0" and "1" for all incoming photon bursts.

The absorption of the fibre simply lowers the number of photons per bit, but with the help of optical amplifiers it is possible to restore a too low photon number. At the end, it is only important that the eye-diagram is not totally closed and the bit error rate (BER) will be only a small fraction of the overall transmitted data.

On the other hand, due to the high amount of photons

per bit, a possible adversary can easily get full information out of the transmission system. Moreover, the eavesdropper (subsequently called Eve) can use amplifiers and it is impossible to detect her attack neither by the users nor by the operator of the optical network.

Quantum communication

The goal of quantum communication is to transfer qubits from the sender (Alice) to the receiver (Bob). One way to handle qubits in photonics is to control the polarization states of single photons. Subsequently and in large contrast to the aspects of classical communication above, in quantum communication applications Alice prepares qubits as single photons and sends them to Bob, who uses an optical measurement apparatus and tries to detect single photon events.

An important issue of quantum mechanics is the impossibility to copy quantum states. Due to the so called "**no-cloning-theorem**" one qubit can not be duplicated in that way that full information from the original quantum state of a photon is copied to another photon [2].

The key-point of quantum cryptography is concluded from a consequence of the "no-cloning-theorem": It is forbidden with fundamental laws of physics to measure or copy the information of the qubit without disturbing the quantum system. Luckily this is also true for a possible eavesdropper. This effect can be used to detect an adversary by the users Alice & Bob.

Unfortunately, another important consequence for quantum communication is the lack of amplifiers and the forbidden usage of the classical repeater stations that are used nowadays. Contrarily to classical communication, if due to absorption one photon is lost, the qubit fails to be transmitted. As an important consequence, the loss of photons reduces the transmission rate of qubits and in combination on the impossibility to amplify qubits, quantum communication via optical fibres is limited to approx. 100km.

Entanglement

Quantum entanglement, a term originally coined by the Austrian physicist Erwin Schrodinger, is the essence of quantum physics. Two entangled particles can only be described by their joint behaviour. This has the intriguing consequence that measurements on the individual particles will always lead to random results although perfect correlations are observed for measurement outcomes of both particles – no matter how far apart the two particles are.

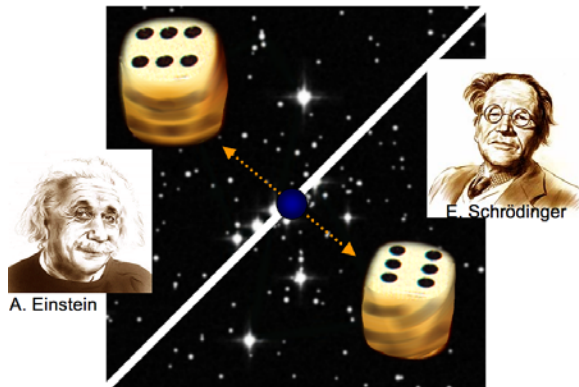


Fig. 1. Example of two (imaginary) "entangled dices" to explain entanglement: If both dices would be perfect entangled and be separated, they would show remarkable behaviour. Both players would recognize total random results between 1 and 6 when they throw their dices, but both dices will always show the same result. They are perfectly correlated.

Albert Einstein called this astonishing behavior "spooky action at a distance". In theory, these correlations should be maintained over arbitrary distances, but the practical limitation for fibre based entanglement distribution is the absorption and decoherence due to polarization mode dispersion.

Generation of polarization entangled photon pairs

Nonlinear optical media are widespread used to efficient double the wavelength of lasers (i.e. green 532nm lasers). The reverse effect – spontaneous parametric downconversion SPDC - to convert visible photons into the infrared is very inefficient. Only approx. 1 out of 10^6 pump photons decay into a signal and idler photon. Depending on the cut of the crystal, both photons have the same polarization (type-I) or different polarizations (type-II). The wavelength and the direction of propagation of the new wavelength are determined by the energy and momentum conservation relations [3]. This leads to a cone-like emission from the signal and idler photons. The selection of different wavelength with filters leads to the ring structure on a CCD camera or a photographic plate as depicted in fig. 2.

If the polarization of one photon is strictly linked to another property of a photon, entanglement is not possible. The photons indicated by the rectangular

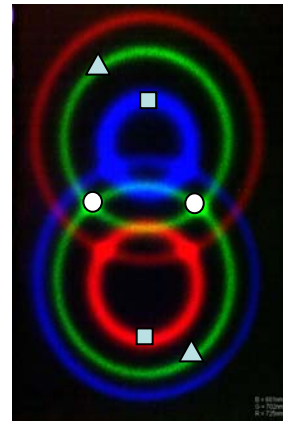


Fig. 2. The two ring system of this type-II BBO crystal is formed by the vertical signal and horizontal idler photons on the top and bottom part, respectively. The colour indicate different wavelength. The sum of the photon energies of both photons correspond to the pump energy and the direction is determined by the momentum conservation.

position in fig. 2 have different wavelengths and are distinguishable. Even when both pair-photons are degenerated, i.e. having the same wavelength, but different emission angles, the polarization is determined by the position. Only for the intersection region of both cones with the same wavelength, the photons are entangled. This is indicated by the filled circles in fig. 2. Figure 3 again clearly shows the emission cones and the direction of the polarization entangled photon pairs.

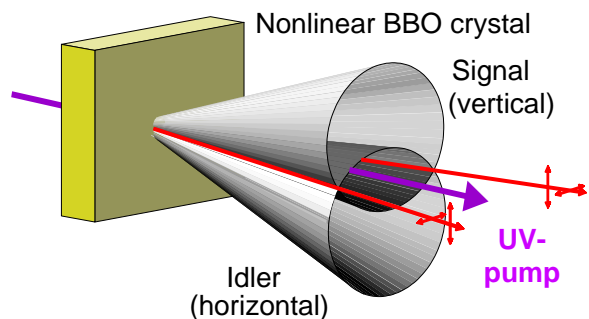


Fig. 3. Nonlinear BBO crystal with the degenerate signal and idler cones. Only the photons emitted in the direction of the intersection lines are polarization entangled.

We lost the knowledge of the propagation cone of the signal and idler photons and subsequently unpolarized light is generated at the intersection lines. There is no way determining the polarization of the photons except making a measurement. Using a type-II crystal and preparing a special state, both photons carry a polarization tilted by 90° with respect to each other. Only if one photon is measured in one polarization direction (i.e. 45°), the other photon is immediately polarized at the other direction (i.e. 135°), no matter the distance in between. This is the so called "spooky action at a distance".

QKD with entangled photons

The entangled particles are sent to the trusted parties Alice and Bob respectively. This can be arranged, if the source is located in the middle of them. It is even possible to shift the source to Alice and sending the other photon to Bob. The principle is shown in fig. 4.

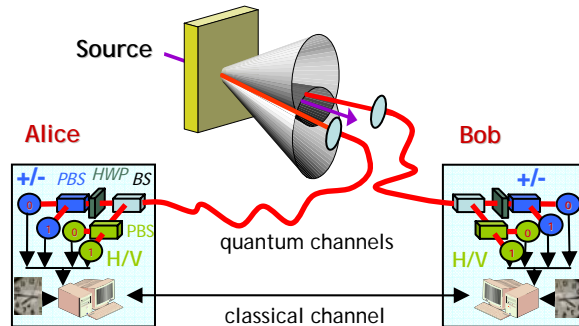


Fig. 4. Arrangement of all parties of a QKD setup with entangled photons. The photons are produced at the source and distributed to Alice and Bob. There, a set of beamsplitters transform the polarization state of the qubits into output ports for measurement.

Alice and Bob receive photons and measure their polarization in one of the two polarization basis (H for horizontal, V for vertical and + for 45°, - for 135°) [4]. Both receivers choose their bases independently either with active switching [5, 6, 7] or passively [8] as shown in fig. 4. If both photons of a pair are detected in the same basis (in H/V or +/-) and entangled photons were used, then we know that the outcomes will always be correlated due to the “spooky action”. Measurements in different bases must be discarded.

For this so called sifting procedure, Alice and Bob need to find out if the corresponding pair-photon has reached the other party. They can time-stamp all events from their detectors (implied in fig. 4) or compare the arrival time with a stable time reference (see fig. 5). Only the basis, but not the result of the different measurements are announced publicly and Alice and Bob exactly knows which photon pair can be used further.

Possible attacks from Eve

There are many potential attacks for Eve, the potential eavesdropper. But still quantum mechanics comes into play and guarantees a secure transmission of the key [9, 10]:

- Eve can try to take over the source in the middle and prepare photon pairs with distinct polarization, however Alice and Bob can perform tests of the entanglement. If the Bell inequality is violated then the source really emits entangled pairs which could have not been tampered with by Eve.
- Eve cannot copy the quantum state of the photon perfectly and then wait for basis reconciliation to measure in the appropriate basis. The non cloning

theorem in quantum mechanics prohibits such actions.

- If Eve decides to measure and resend the photon, she will only half of the time pick the right basis. In the other cases Eve will get random information and the photon she sends to Bob is necessarily also uncorrelated to the photon prepared by Alice. Eve therefore introduces an error between otherwise perfectly correlated events and she can be detected. Using the intercept-resend strategy, Eve's tampering will amount to 25% qubit error rate (QBER). More elaborate attacks can reduce the error bound to 11%, above which no secure communication is any longer possible.

In quantum cryptography all errors due to the potential eavesdropper and/or imperfections in the setup must be rectified. Therefore both parties use classical error correction protocols and “privacy amplification” and additionally all messages must be authenticated to achieve highest security [9]. The price to pay for this highest possible (unconditionally) security is a low bit rate in the order of 1000 bits per second or below.

A real world experiment

In April 2004, a bank transfer, secured by a quantum key, was successfully accomplished. The aim of this demonstration was to implement all steps of QKD including a possible future application not under laboratory conditions but to demonstrate a real-world scenario. The choice of location fell to the Vienna City Hall and the headquarters of a national bank.

The setup used is shown in fig 5. Alice's side (bank) consisted of a compact source of entangled photons, a BB84 detection unit and QKD-hardware. A similar type-II SPDC setup as described above was used to produce entangled photon pairs with a central wavelength of 810 nm and a FWHM bandwidth of 5.6 nm. With a 16 mW pump laser about 8200 pairs could be detected locally.

The fibre used for the quantum channel was single mode for 810 nm and showed an overall attenuation of 6 dB. Beside the quantum channel, 3 additional standard telecom fibres were used to handle the synchronization pulses and classical data transfer. The whole fibre bundle was installed in the Vienna sewage system, where it was subjected to environmental influences like temperature fluctuations.

The polarization rotation induced by the fibre was compensated using polarization controllers at the source. Once the controllers were adjusted, the polarization proved to be stable for hours and no active compensation was necessary during key

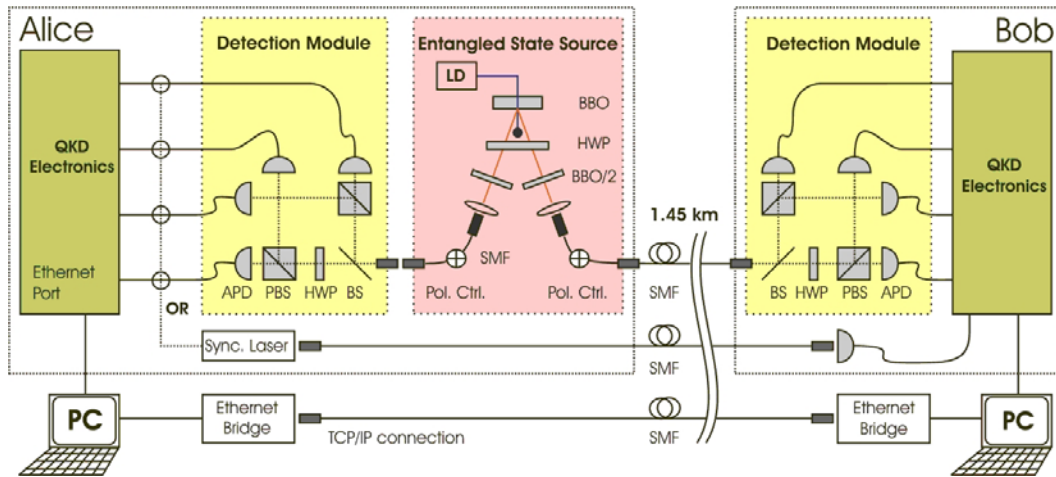


Fig. 5. Sketch of the polarization entangled QKD setup (from [8]). A SPDC source, located at Alice, produces entangled photon pairs. One photon is directly analyzed at Alice. The other photon is transmitted to Bob over a 1.45 km single mode fibre. At both detection units, the incoming photon chooses randomly between the H/V and +/- basis. Once a photon is measured at Alice, an optical trigger pulse is sent to Bob to establish a time reference. The detector events and synchronization pulses are fed on both sides into an electronic hardware which performs all necessary QKD operations to yield the secure key.

exchange. For longer operation an active control will be necessary but only for long time scales (few hours).

The idea of the QKD-hardware is to have all the steps required for a full automated QKD exchange on an embedded electronic board which is compatible with conventional telecommunication standards. Moreover, the electronics was recently extended not only to handle the secret key as a resource for a one-time pad, but also to symmetrically expand the key to increase the encrypted data rate (with slight reduction in the security of the key).

During a typical 18 minute long key exchange a total of 250 kbits of sifted key was recorded. 25% of the bits were publicly compared to estimate the QBER. An average error value of 6.3% was found in this way. The final secure quantum key after privacy amplification amounted to 79 kbits. This corresponds to an average secure key of 76 bits/s

Teleportation and Quantum Repeater

Entanglement is also a unique resource for novel quantum protocols. The initial state of an additional photon is transferred to the teleported state (fig. 6), if a successful joint measurement with a photon of an entangled photon pair is performed ("BSM" in fig. 6). No information transformation faster than the speed of light is possible, because Bob needs to do some transformations ("U" in fig. 6) on the second photon to get out exactly the same state as the initial state. And therefore more classical information about the measurement result of "BSM" is needed from Alice to teleport a quantum state successfully.

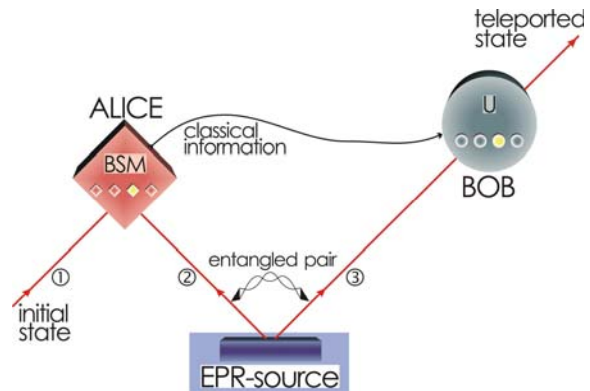


Fig. 6. Teleportation scheme using a source of entangled photon pairs (EPR-source) to transfer the initial state to the teleported state.

Using a photon from an additional entangled pair as the "initial state", entanglement swapping can be performed. This is the basic working principle of a future quantum repeater.

References

- 1 N. Gisin et al., Rev. Mod. Phys. **74** (2002), 145
- 2 W.K. Wootters et al., Nature **299** (1982), 802
- 3 P. Kwiat et al., Phys. Rev. Lett. **75** (1995), 4337
- 4 C.H. Bennet et al., Int. Conf. Computers, Systems & Signal Processing, India (1984), 175
- 5 A. Ekert, Phys. Rev. Lett. **67** (1991), 667
- 6 C.H. Bennet et al., Phys. Rev. Lett. **68** (1992), 557
- 7 T. Jennewein et al., Phys. Rev. Lett. **84** (2000), 4729
- 8 A. Poppe et al., Optics Express **12** (2004), 3865
- 9 N. Luetkenhaus, Phys. Rev. A **61** (2000), 052304
- 10 E. Waks et al., Phys. Rev. A **65** (2002), 052310
- 11 C.H. Bennett et al., Phys. Rev. Lett. **70** (1993), 1895