QUANTUM ENTANGLEMENT, PURIFICATION, AND LINEAR-OPTICS QUANTUM GATES WITH PHOTONIC QUBITS

PHILIP WALTHER AND ANTON ZEILINGER

Institut für Experimentalphysik, Universität Wien, Vienna, Austria
Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Vienna, Austria
E-mail: wspc@wspc.com

1. Entanglement

Strikingly, quantum information processing has its origins in the purely philosophically motivated questions concerning the nonlocality and completeness of quantum mechanics sparked by the work of Einstein, Podolsky and Rosen in 1935 [1]. In experiments using entanglement, the system of spin-$\frac{1}{2}$ particles is realized by the usage of single photons, whose properties are defined by their polarization. Considering the H/V bases, a logical $|0\rangle$ corresponds to a horizontally polarized photon $|H\rangle$, respectively a logical $|1\rangle$ corresponds to a vertically polarized photon $|V\rangle$. A single qubit can be written as a coherent superposition of the form $|\psi\rangle = \alpha|H\rangle + \beta|V\rangle$, where the the probabilities α^2 and β^2 sum up to $\alpha^2 + \beta^2 = 1$. For the two qubit case the four different maximally entangled Bell-states are defined as:

$$|\Phi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|H\rangle_2 \pm |V\rangle_1|V\rangle_2)$$

$$|\Psi^{\pm}\rangle_{12} = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)$$

The Bell states have the unique feature that all information on polarization properties is completely contained in the (polarization-)correlations between the separate photons, while the individual particle does not have any polarization prior to measurement. In other words, all of the information is distributed among two particles, and none of the individual systems carries any information. This is the essence of entanglement. At the same time, these (polarization-)correlations are stronger than classically allowed since they violate bounds imposed by local realistic theories via the Bell-inequality [2] or they lead to a maximal contradiction between such theories and quantum mechanics as signified by the Greenberger-Horne-Zeilinger theorem [3,4]. Distributed entanglement thus allows to establish non-classical correlations between distant parties and can therefore be considered the quantum analogue to a classical communication channel, a quantum communication channel.

The most widely used source for polarization-entangled photons today utilizes the process of spontaneous parametric down-conversion in nonlinear optical crystals [5]. Occasionally the nonlinear interaction inside the crystal leads to the annihilation of a high frequency pump photon and the simultaneous creation of two lower frequency photons, signal and idler, which satisfy the phase matching condition:

$$\omega_p = \omega_s + \omega_i \qquad \text{and} \qquad \vec{k}_p = \vec{k}_s + \vec{k}_i$$

where ω is the frequency and $\vec{k}$ the wavevector of the pump p, signal s and idler i photon. A typical picture of the emerging radiation is shown in Figure 1.

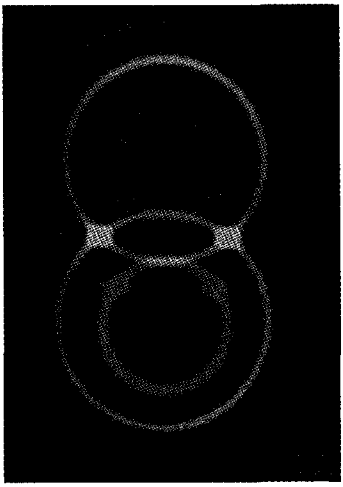

Figure 1. Photograph of the light emitted in type-II parametric down-conversion (false colours). The polarization-entangled photons emerge along the directions of the intersection between the white rings and are selected by placing small holes there

The possibility to establish such quantum communication channels over large distances offers the fascinating perspective to eventually take advantage of these novel communication capabilities in networks of increasing size. Naturally, non-trivial problems emerge in scenarios involving long distances or multiple parties. Experiments based on present fiber technology have demonstrated that entangled photon pairs can be separated by distances ranging from several hundreds of meters up to about 10 km [6,7,8], but no improvements by orders of magnitude are to be expected. Optical free-space links could provide a solution to this problem since they allow in principle for much larger propagation distances of photons because of the low absorption of the atmosphere in certain wavelength ranges. Single optical free-space links have been studied and successfully implemented already for several years for their application in quantum cryptography based on faint classical laser pulses [9,7]. We have recently demonstrated a next crucial step, namely the distribution of quantum entanglement via two simultaneous optical free-space links in an outdoor environment [11]. Polarization-entangled photon pairs have been transmitted across the Danube River in the city of Vienna via optical free-space links to independent receivers separated by 600m and without a line of sight between them (see Figure 2). A Bell inequality between those receivers was violated by more than 4 standard deviations confirming the quality of the entanglement:

$$S = |E(\phi_A, \phi_B) - E(\phi_A, \hat{\phi}_B) + E(\hat{\phi}_A, \phi_B) + E(\hat{\phi}_A, \hat{\phi}_B) \leq 2$$

where S is the "Bell parameter" and E the two photon visibility when polarizers are set to ϕ or $\hat{\phi}$ at receiver A or B. In this experiment, the setup for the source generating the entangled photon pairs has been miniaturized to fit on a small optical breadboard and it could easily be operated completely independent from an ideal laboratory environment.

Obviously, terrestrial free-space links are limited to rather short distances because they suffer from possible obstruction of objects in the line of sight, from atmospheric attenuation and, eventually, from the Earth's curvature. To fully exploit the advantages of free-space links, it will eventually be necessary to use space and satellite technology. By transmitting and/or receiving either photons or entangled photon pairs to and/or from a satellite, entanglement can be distributed over truly large distances. This would allow quantum communication applications on a global scale. From a fundamental point of view, satellite-based distribution of quantum entanglement is also the first step towards exploiting quantum correlations on a scale larger by orders of magnitude than achievable in laboratory and even ground-based experimental environments. State of the art photon sources and detectors would already suffice to achieve a satellite-based quantum communication link over some thousands of kilometers [12,13,14].

2. Quantum Key Distribution using Polarization Entangled Photons

The appeal of quantum cryptography is that its security is based on the laws of nature. In contrast to existing classical schemes of Key Distribution, Quantum (Cryptographic) Key Distribution does not invoke the transport of the key, since it is created at the sender and receiver site immediately. Furthermore, the key is created from a completely random sequence, which is in general an extremely difficult task in classical schemes. Finally, eavesdropping is easily detected due to the fragile nature of the qubits invoked for the quantum key distribution. Those features show that quantum cryptog-

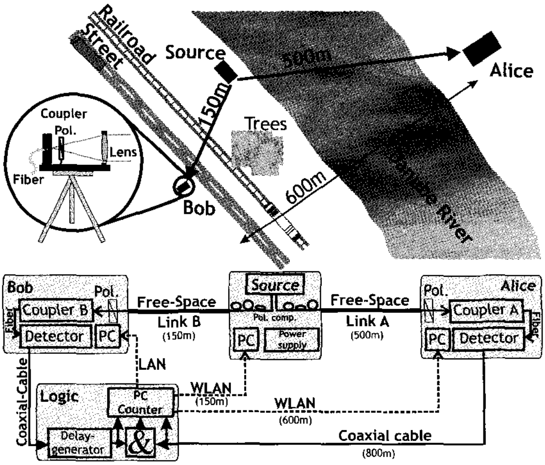

Figure 2. Free-space distribution of polarization-entangled photons [11]. The entangled-photon source was positioned on the bank of the Danube River. The two receivers, Alice and Bob, were located on rooftops and separated by approx. 600m, without a direct line of sight between each other. The inset shows the schematics of the telescopes consisting of a single-mode fibre coupler and a 5cm diameter lens. At the receiver telescopes, polarizers (Pol.) were attached to determine the polarization correlations and eventually violate a Bell-inequality. The lower figure shows a functional block diagram of the experiment. Detection signals from Alice were relayed to Bob using a long BNC cable. Singles and coincidence counting was performed locally at Bob and the results were shared between all three stations using LAN and Wave-LAN connections.

raphy is a superior technology which overcomes limitations and drawbacks of classical cryptographic schemes by utilizing the fascinating properties of quantum physics.

Cryptography (Quantum Key Distribution) allows two physically-seperated parties to create a random secret key without resorting to the services of a courier, and to verify that the key has not been intercepted. This is due to the fact that any measurements of incompatible quantities on a quantum system will inevitably modify the state of this system. This means that an eavesdropper (Eve) might get information out of a quantum channel by performing measurements, but the legitimate users will detect her and hence not use the key.

To ensure privacy of the key in advance, Alice and Bob do not use the quantum channel to transmit information, but only to establish a random sequence of bits, i.e.a key. The security of the key is determined by estimating the error rate after transmission and measuring the qubits. Quantum physics guarantees that any eavesdropping of the quantum channel will necessarily lead to errors in the key. If the key turns out to be insecure, then Alice and Bob simply discard it, and do not use it for encoding their message.

The utilization of entangled qubits for quantum cryptography has been proposed independently by Ekert [15] and by Bennett et al. [16]. As is indicated in Figure 3, Alice and Bob observe perfect anticorrelations of their measurements whenever they happen to have parallel oriented polarizers, leading to bitwise complementary keys. Alice and Bob will obtain identical keys if one of them inverts all bits of the key. Polarization entangled photon pairs offer a means to effectively realize a single photon situation, necessary for secret-sharing. Whenever Alice makes a measurement on her photon, Bob's photon is projected into the orthogonal state which is then analyzed by Bob, or vice versa. One immediately profits from the peculiar properties of entangled photon pairs, because the inherent randomness of quantum mechanical observations renders any analysis of the randomness of the keys or the encoded messages void.

After collecting the keys, Alice and Bob authenticate their keys by openly comparing (via classical communication) a small subset of their keys and evaluating the bit error rate. One advantage of using entangled photons is that the individual results of the measurements on entangled photons are purely random and therefore the randomness of the final key is ascertained . A further advantage is that the entangled photons represent a conditional single photon source, and the probability of having two photon pairs within the coincidence window can be very low.

Most recently an entangled state quantum cryptography prototype system in a typical application scenario was presented in Vienna [17]. It was possible to distribute secure quantum keys on demand between the headquarters of an Austrian bank and the Vienna City Hall using polarization-entangled photon pairs. The produced key was directly handed over to an application that was used to send a quantum secured online wire transfer from the City Hall to the headquarters of the bank.

The quantum cryptography system used (see Figure 4) consists of the source for polarization-entangled photons located at the bank, two combined polarization analysis and detection modules and two electronic units for key generation. These two quantum cryptography units which handled the five steps of secure key generation - real-time acquisition, key sifting , error estimation, error correction and privacy amplification - are based on an embedded electronic design and are compatible with classical telecommunication equipment. The quantum channel between Alice and Bob consists of an optical fiber that has been installed between the two experimental sites in the Vienna sewage system. The exposure of the fibers to realistic environmental conditions such as stress and strain during installation, as well as temperature changes were an important feature of this experiment, as it shows that our system not only works under laboratory conditions, but also in a realistic quantum cryptography scenario.

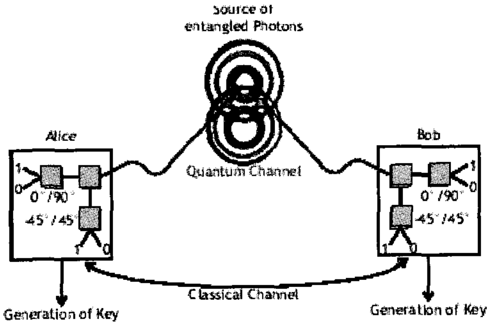

Figure 3. Quantum Cryptography using entangled photons

3. Purification of Entanglement

Owing to unavoidable decoherence in the quantum communication channel, the quality of entangled states generally decreases with the channel length. Entanglement purification is a way to extract a subset of states of high entanglement and high purity from a larger set of less entangled states - and is thus needed to overcome the decoherence of noisy quantum channels. We were able for the first time to experimentally demonstrate a general quantum purification scheme for mixed polarization-entangled two-particle states [18]. The crucial operation for a successful purification step is a bilateral conditional NOT (CNOT) gate, which effectively detects single bit-flip errors in the channel by performing local CNOT operations at Alice's and Bob's side between particles of shared entangled states. The outcome of these measurements can be used to correct for such errors and eventually end up in a less noisy quantum channel [19]. For the case of polarization entanglement, such a "parity-check" on the correlations can be performed in a straight forward way by using polarizing beamsplitters (PBS) [20] that transmit horizontally polarized photons and reflect vertically polarized ones, as seen in Figure 5.

Consider the situation in which Alice and Bob have established a noisy

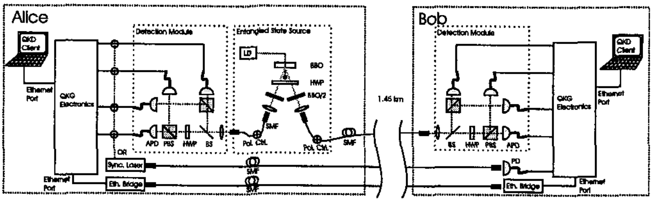

Figure 4. Sketch of the experimental setup. An entangled state source pumped by a violet laser diode at 405 nm produces polarization entangled photon pairs. One of the photons is locally analyzed in Alice's detection module, while the other is sent over a 1.45 km long single-mode optical fiber (SMF) to the remote site (Bob). Polarization measurement is done randomly in one of the two complementary bases ($|H\rangle/|V\rangle$ and $|45\rangle/|-45\rangle$), by using a beamsplitter (BS) which randomly sends incident photons to one of the two polarizing beamplsplitters (PBS). One of the PBS is defined to measure in the $|H\rangle/|V\rangle$ basesm the other in the $|45\rangle/|-45\rangle$ bases turned by a half-wave plate (HWP). The final detection of the photons is done in passively quenched silicon avalanche photodiodes (APD). When a photon is detected in one of Alice's four photodiodes an optical trigger pulse is created (Sync. Laser) and sent over a second fiber to establish a common time bases. at both sides, the trigger pulses and the detection events from the APDs are fed into an dedicated quantum key generator (QKG) device for further processing. This QKG electronic device is an embedded system, which is capable of autonomously doing all necessary calculations for key generation.

quantum channel, i.e. they share a set of equally mixed, entangled states ρ_{AB}. At both sides the two particles of two shared pairs are directed into the input ports a_1, a_2 and b_1, b_2 of a PBS (see Figure 6). Only if the entangled input states have the same correlations, i.e. they have the same parity with respect to their polarization correlations, the four photons will exit in four different outputs (four-mode case) and a projection of one of the photons at each side will result in a shared two-photon state with a higher degree of entanglement. All single bit-flip errors are effectively suppressed.

For example, they might start off with the mixed state

$$\rho_{AB} = F \cdot |\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F) \cdot |\Psi^-\rangle\langle\Psi^-|_{AB}$$

where $|\Phi^+\rangle = (|HH\rangle + |VV\rangle)$ is another Bell state. Then, only the combinations $|\Phi^+\rangle_{a_1,a_2} \otimes |\Phi^+\rangle_{b_1,b_2}$ and $|\Psi^-\rangle_{a_1,a_2} \otimes |\Psi^-\rangle_{b_1,b_2}$ will lead to a four-mode case, while $|\Phi^+\rangle_{a_1,a_2} \otimes |\Psi^-\rangle_{b_1,b_2}$ and $|\Psi^-\rangle_{a_1,a_2} \otimes |\Phi^+\rangle_{b_1,b_2}$ will be rejected. Finally, a projection of the output modes a_4, b_4 into the basis $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ is needed to create the new mixed state

$$\rho'_{AB} = F' \cdot |\Phi^+\rangle\langle\Phi^+|_{AB} + (1-F') \cdot |\Psi^-\rangle\langle\Psi^-|_{AB}$$

with probability $F' = F^2/[F^2 + (1-F)^2]$ for the pure states $|\Phi^+\rangle_{a_3,b_3}$ and

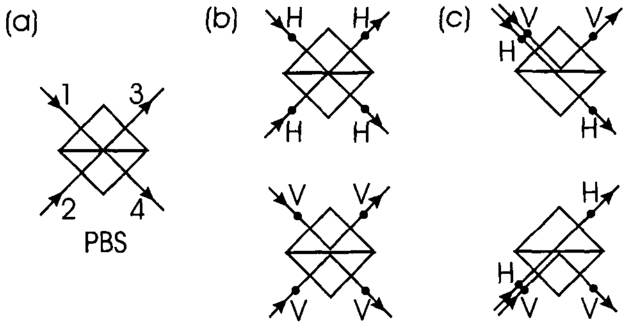

Figure 5. Using a polarizing beamplitter as a polarization comparer.a The polarizing beamsplitter (PBS) transmits horizontally polarized photons and reflects vertically polarized photons. If a vertically polarized photon incidents along mode 1, denoted by V, it will go out within mode 3. Similarly a horizontally polarized photon, denoted by H, which also incidents along mode 1, is transmitted into the mode 4. b Considering the case that two photons incident simultaneously, one in each input mode, then they will go out into different output modes, when both have the same polarization. For this case, where each output mode has to be occupied, the PBS acts like a party-checker c On the other hand, if the two incident photons have opposite polarization, then they will always go out along the same direction.

probability $1-F'$ for $|\Psi^+\rangle_{a_3,b_3}$, respectively. The fraction F' of the desired state $|\Phi^+\rangle$ becomes larger for $F > \frac{1}{2}$. In other words, the new state ρ'_{AB} shared by Alice and Bob after the bilateral parity operation demonstrates an increased fidelity with respect to a pure, maximally entangled state. This is the purification of entanglement.

Typically, in the experiment, one photon pair of fidelity 92% could be obtained from two pairs, each of fidelity 75%. Also, although only bit-flip errors in the channel have been discussed, the scheme works for any general mixed state, since any phase-flip error can be transformed to a bit-flip by a rotation in a complementary basis.

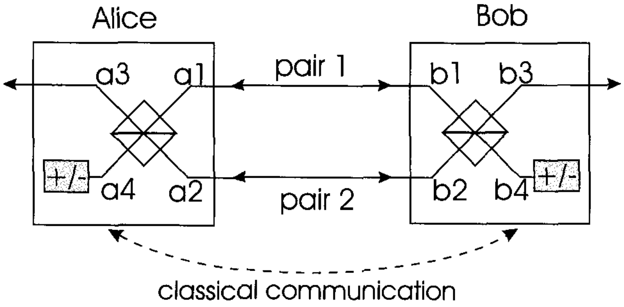

Figure 6. Scheme for entanglement purification of polarization-entangled qubits (from [18]). Two shared pairs of an ensemble of equally mixed, entangled states ρ_{AB} are fed in to the input ports of polarizing beamsplitters that substitute the bilateral CNOT operation necessary for a successful purification step. Alice and Bob keep only those cases where there is exactly one photon in each output mode. This can only happen if no bit-flip error occurs over the channel. Finally, to obtain a larger fraction of the desired pure (Bell-)state they perform a polarization measurement in the $|\pm\rangle$ basis in modes a4 and b4. Depending on the results, Alice performs a specific operation on the photon in mode a3. After this procedure, the remaining pair in modes a3 and b3 will have a higher degree of entanglement than the two original pairs.

References

1. A. Einstein, B. Podolsky, N. Rosen *Phys. Rev.* **75**, 777 (1935).
2. J. Bell *Physics* **1**, 195 (1964).
3. D. M. Greenberger, M. A. Horne, A. Zeilinger Bell's Theorem, Quantum Theory, and Conceptions of the Universe *Kluwer* (Dordrecht), (1989).
4. D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger *Am. J. Phys.* **58**, 1131 (1990).
5. P. G. Kwiat *et al. Phys.Rev.Lett.* **75**, 4337 (1995).
6. P. R. Tapster, J. G. Rarity, P. C. M. Owens *Phys. Rev. Lett.* **73**, 1923 (1994).
7. W. Tittel, J. Brendel, H. Zbinden, N. Gisin *Phys. Rev. Lett.* **81**, 3563 (1998).
8. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, A. Zeilinger *Phys. Rev. Lett.* **81**, 5039 (1998).
9. W. T. Buttler *et al. Phys. Rev. Lett.* **81**, 3283 (1998).
10. C. Kurtsiefer *et al. Nature* **419**, 450 (2002).
11. M. Aspelmeyer *et al. Science* **301**, 621 (2003).
12. M. Aspelmeyer *et al. European Space Agency (ESA)* 16358/02 (2003).
13. M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, A. Zeilinger *quant-ph/0305105* (2003).
14. R. Kaltenbaek *et al. quant-ph/0308174* (2003).
15. A. K. Ekert *Phys. Rev. Lett.* **67**, 661 (1991).
16. C. H. Bennett, G. Brassard, N. D. Mermin *Phys. Rev. Lett.* **68**, 557 (1992).
17. A. Poppe *et al. quant-ph/0404115 v2* (2004).
18. J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, A. Zeilinger, *Nature* **423**, 417 (2003).
19. C. H. Bennett *et al. Phys. Rev. Lett.* **76**, 722 (1996).
20. J.-W. Pan, C. Simon, C. Brukner, A. Zeilinger *Nature* **410**, 1067 (2001).