Long-Distance Quantum Cryptography with Entangled Photons

Anton Zeilinger* [a]
[a] IQOQI Institute for Quantum Optics and Quantum Information,
Austrian Academy of Sciences, Boltzmanngasse 3, A-1090 Vienna, Austria

ABSTRACT

Entanglement-based quantum cryptography has the appealing advantage of intuitively more evident security. While originally, weak laser pulse schemes were implemented earlier as technologically simpler, it is now possible to build entanglement-based quantum key distribution systems on a technically equally advanced level. The existing polarization-based systems as developed in Vienna now cover distances of the order of 100 km in fiber and of 144 km in free space. In a recent fiber experiment, an asymmetric source is used such that one photon at the 1.550 nm telecom wavelength is transmitted to Bob, while the other photon at 810 nm is locally measured by Alice. It turns out that polarization entanglement is rather robust, certainly over distances of 100 km in fibers. In a recent long-distance free-space experiment, one photon was sent over 144 km from the Canary Island of La Palma to the island of Tenerife, while again the other photon was measured locally. The receiving station uses the OGS telescope operated by the European Space Agency ESA. This experiment opens up the possibility for future quantum key distribution using satellites.

Keywords: entanglement, quantum cryptography, quantum communication, optical communication

1. INTRODUCTION

Quantum cryptography with entangled photons [1] circumvents in a most elegant way the key distribution of classical cryptography. There, the random key has to be sent either from Alice to Bob or it has to be distributed between the various partners by a central authority. Even in the case of quantum cryptography based of transmission of individual qubits as in the BB84 protocol [2], qubits in well-defined quantum states have to be transmitted in the key distribution protocol. This feature clearly also holds for the case of quantum money [3], which is the first ever proposal using quantum states to encrypt information. In contrast, in entanglement-based quantum cryptography, the key does not have to be transported between different locations. Rather, it comes into existence at different locations simultaneously due to measurements on the individual members of an entangled quantum system.

Consider, for example, the maximally entangled state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2\right). \quad (1)$$

*anton.zeilinger@oeaw.ac.at; phone +43 1 4277 51201; fax +43 1 4277 29552; www.quantum.at

Quantum Communications Realized
edited by Yasuhiko Arakawa, Masahide Sasaki, Hideyuki Sotobayashi,
Proc. of SPIE Vol. 6780, 67800B, (2007) · 0277-786X/07/$18 · doi: 10.1117/12.740268

Here, $|0\rangle$ and $|1\rangle$ are the two basis states of the qubit in a specifically chosen basis. The subscripts 1 and 2 refer to two different qubits. State (1) describes the situation where either both qubits are in the state "0" or in the state "1". Therefore, measurements on either qubit in that measurement basis results either in "0" or in "1" with the other qubit exhibiting the same result due to the perfect correlation described by state (1). Most importantly, the result on either qubit is completely random. Therefore, if one performs such measurements on many pairs, one obtains random sequences of "0" and "1". Due to the perfect correlations, these random sequences are the same on both sides. Furthermore, for the state (1), these same perfect correlations between "0" and "1" hold for any measurement within one given plane of the Poincaré sphere, in other words, for any other basis which results out of the original basis by a simple rotation such that the phase factors stay real. This fact can be utilized to exclude an eavesdropper. This is done by both participants, Alice and Bob, switching around randomly between different bases. Then, if they happen to have chosen the same basis, they get perfect correlations and, furthermore, an eavesdropper is at loss because he has no chance to properly guess the basis chosen for any given pair.

In the first experimental realization [4] of entanglement-based quantum cryptography, polarization-entangled photons were utilized in the anti-symmetric state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B\right), \tag{2}$$

where H and V refer to horizontal and vertical polarization respectively, and A and B refer to Alice's and Bob's photon respectively. In the experiment, the photons A and B were generated by the process of spontaneous type-II parametric down-conversion [5] and sent to two different measurement stations separated by 360 m. In order to switch between different bases, quantum random number generators were used (Fig. 1).

In that experiment, the security of the quantum cryptography connection was established using Wigner's inequality [6], which is a variant of Bell's original inequality [7] based on set theoretical arguments. In that experiment, visual information in the form of a picture was encrypted and transmitted securely from Alice to Bob (Fig. 2).

The publication of experiment [4] was immediately followed by presentations of entanglement-based quantum cryptography experiments by the groups of Kwiat [8] and Gisin [9] in the same issue of Physical Review Letters, because the authors of [4] delayed publication in order to make joint publication possible.

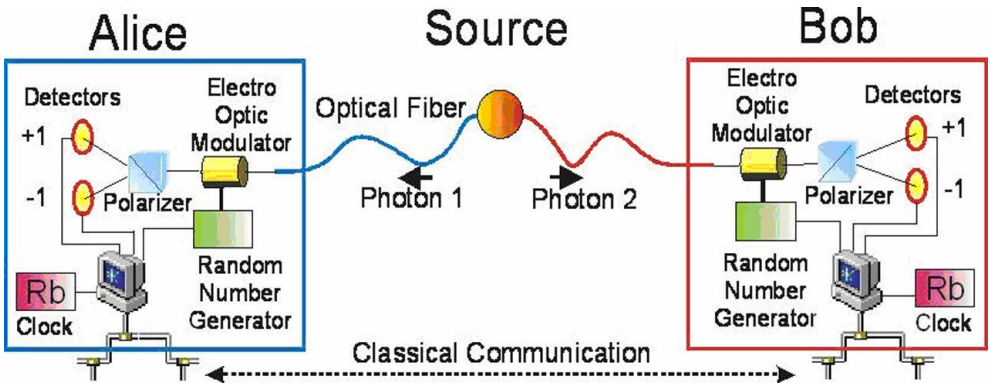

Fig. 1. Experimental set-up of the Innsbruck entanglement-based quantum cryptography experiment. The polarization-entangled photons are sent to Alice and Bob via glass fibers. There, the specific measurement basis is decided in the last instant using fast-forward random number generators. The secure keys are then extracted using classical communication via the Innsbruck University computer network.

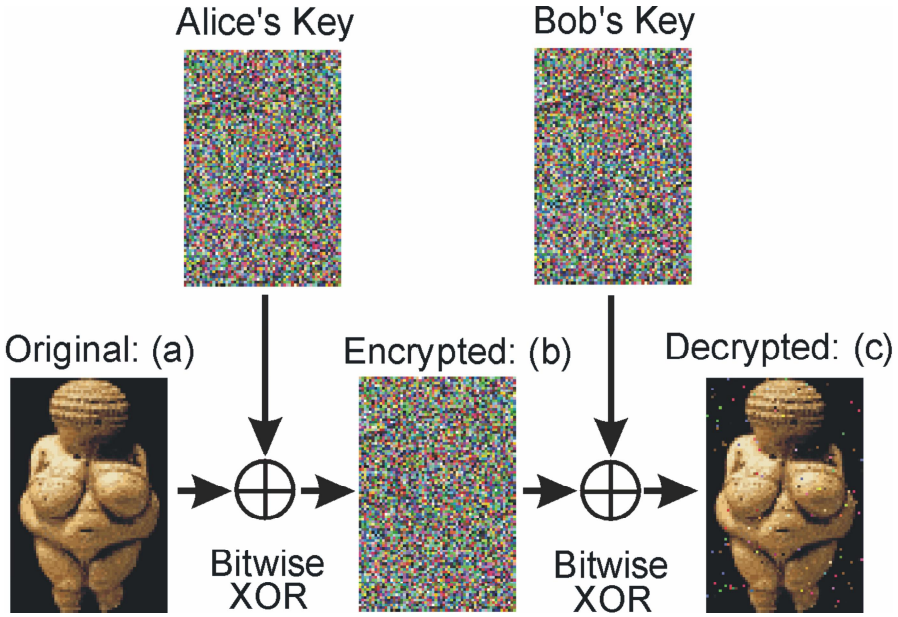

Fig. 2. In the first entanglement-based quantum cryptography experiment [4], an image of the "Venus von Willendorf" effigy was transmitted. Alice and Bob initially generated a raw key of ~ 80.000 bits of length with a quantum bit error rate of 2,5%. This was distilled to ca. 50.000 bits of error corrected key with a bit error rate of 0,4%. The transmitted image itself was 43.200 bits large.

When compared to other quantum cryptography schemes [10, 11, 12, 13], entanglement-based quantum cryptography has a distinct advantage. This is because, being based on entanglement, its security is easily understandable on an intuitive basis even by non-physicists. This intuitive position has recently been corroborated [14] by the observation that entanglement-based quantum cryptography testing for security by utilizing a Bell inequality may have distinct advantages concerning side channel attacks.

2. FREE-SPACE ENTANGLEMENT-BASED QUANTUM CRYPTOGRAPHY OVER 144 KM AND BEYOND

An interesting challenge and goal for quantum cryptography is to cover distances on a global scale. In the absence of sufficiently good quantum repeaters, this can only be achieved using satellites. It is imperative to test free-space quantum cryptography over distances beyond 100 km, because the most likely implementation of quantum cryptography with satellites will employ Low-Earth-Orbit (LEO) satellites at heights between 300 km and 500 km. With larger distances, the limits of diffraction optics become very severe. This feature makes quantum communication with Geo-Stationary (GEO) satellites very challenging, as appealing such a communication link might be.

In order to demonstrate entanglement-based quantum cryptography over such distances, we recently [15] performed an experiment between the Canary Islands of La Palma and Tenerife, which are separated by 144 km. In that experiment, polarization-entangled photon pairs were generated using a picosecond-pulsed Nd:vanadate laser emitting light at 355 nm wavelengths. The repetition rate of the laser was 249 MHz. It pumped a beta-barium-borate crystal in the process of spontaneous parametric down-conversion. Of the two photons, each with a wavelength of 710 nm and a bandwidth of 3 nm, one was detected locally at Alice's transmitter station and the other one was sent over 144 km of free space to Bob on Tenerife (Fig. 3).

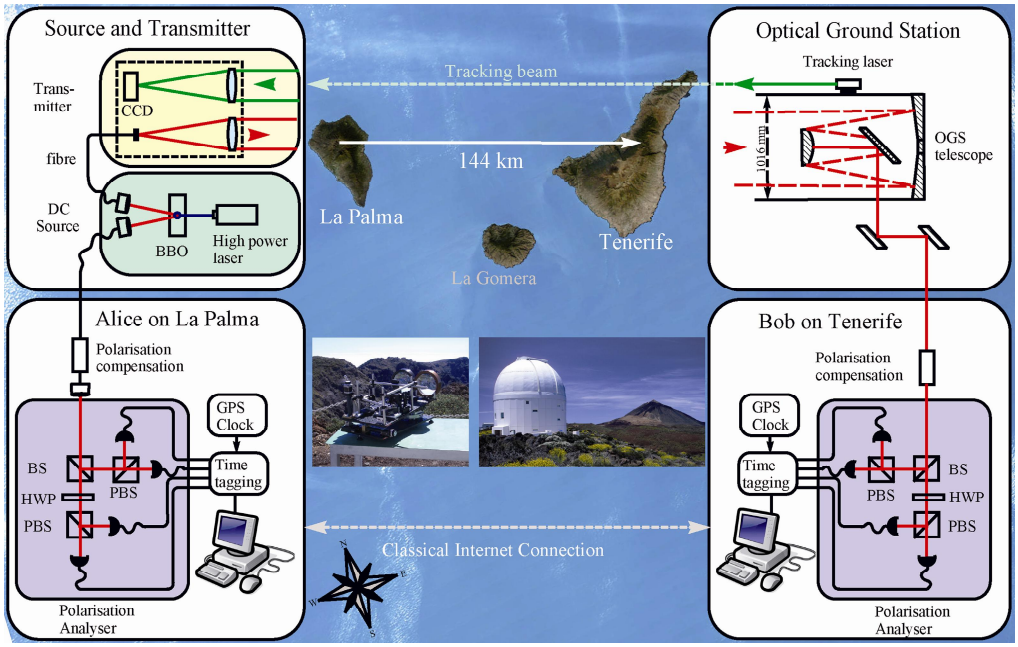

Fig. 3. Quantum communication link between the islands of La Palma and Tenerife. Entangled photons are created using pulsed type-II parametric Down-conversion. They are then coupled into glass fibers. One of the fibers leads one photon over a short distance to Alice on La Palma, the other photon is guided through the long-distance link over to the Canary Island of Tenerife. The long-distance link consists of two telescopes whose lenses are shown in the center of the figure. One of the lenses transmits the single photon, the other one receives a tracking laser beam originating from Tenerife. On Tenerife, the photon is received by the Optical Ground Station (OGS) telescope of the European Space Agency (ESA) with a diameter of 1.016 mm. Finally, on both sides, each photon is transmitted to a polarization analyzer. The classical communication between both sides which is necessary to establish the secure key goes via a standard internet connection.

The optical link consisted of a 140 mm diameter lens on the sending station and on the receiving station we utilized the telescope of the Optical Ground Station (OGS) of the European Space Agency (ESA). The OGS has a 1 m mirror with an effective focal length of 39 m. Over such distances, atmospheric turbulence becomes significant, causing the beam to blur and wander around. For the beam wandering, a tracking laser was installed on OGS. The tracking beam was received at Alice's sending station on La Palma using another independent lens which was connected through a common basis with the single-photon transmitting lens. Thus, by optimizing the throughput of the tracking laser link, the problems of beam wandering could be corrected to a significant extent. Finally, on both Alice's and Bob's side, the photons encountered a four-channel polarization analyzer employing a beam splitter which randomly sent the photon to either one of two polarizing beam splitters, one oriented at 45° with respect to the other.

The active tracking was instrumental to limit beam attenuation (Fig. 4). With the tracking system on, it was possible to limit the beam attenuation to -25 dB under best conditions and typically better than -30 dB. Evidently, the blurring of the beam caused by inhomogeneities of the atmosphere could not be corrected that way. We found that the quality of our transmission was limited by a Fried parameter of 1 cm under poor conditions and 6 cm under best conditions. The Fried parameter describes the effective size of an aperture over which photon transmission can be described by a coherent wave front. The quality of our quantum communication link was finally established by violating a Clauser-Horne-Shimony-Holt inequality. We found that the usual S-parameter was S=2,508±0,037, which violates the local realistic limit by more than 13 standard deviations without any background correction. Thus, our experiment clearly demonstrates entanglement between these two photons, which were separated by 144 km.

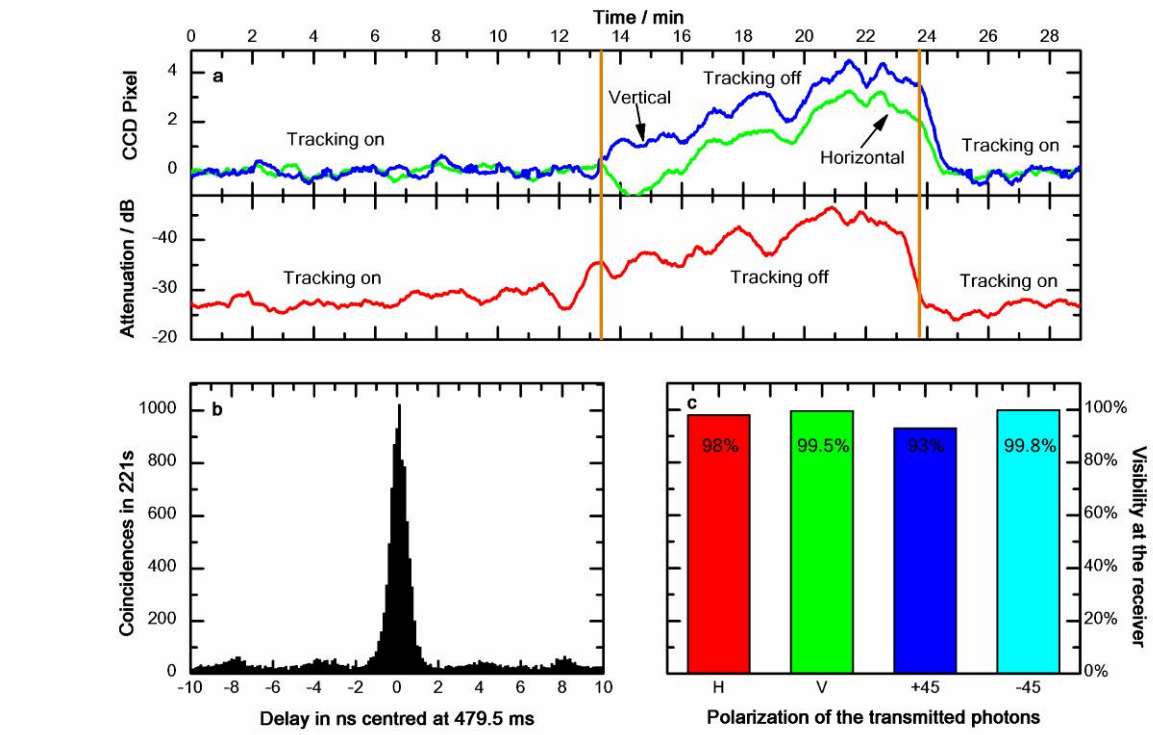

Fig. 4. The quantum communication link between La Palma and Tenerife. The position of the image of the tracking laser (a) on a CCD camera shows very clearly the difference between "tracking on" and "tracking off". Actually, beam wander is stronger in the vertical direction than in the horizontal one. This is due to the layered structure of Earth's atmosphere. The beam wandering observed is clearly correlated with the link attenuation (red curve). The temporal distribution of the observed coincidences (b) shows the pulsed character of our source. Finally, using a polarized test laser beam at 808 nm, we could demonstrate (c) that the polarization of the beams for the four cases H, V, +45°, -45°, was highly preserved.

Evidently, our results cannot be used to test against local realism. This is because Alice's photon was measured locally immediately after the transmission. Therefore the two measurements were not space-like separated. Nevertheless, the claim that we observed entanglement is supported by the fact that the quantum correlations observed in any measurement on entangled systems are independent of the relative space-time ordering of the individual measurements. Measurements in the H/V basis and in the +/- basis, which is rotated by 45° with respect to H/V, then were used to establish a quantum key. Within a measurement period of 75 seconds, in total 789 coincidences were obtained.

In future experiments using satellites, one would like to increase the collection efficiency. A big advantage in satellite-based experiments will be that the beam would only have to pass through a few km of air, resulting in significantly reduced wave-front distortion as compared to our experiment. Finally, one might want to contemplate future experiments with fully active, adaptive optics at the receiving station.

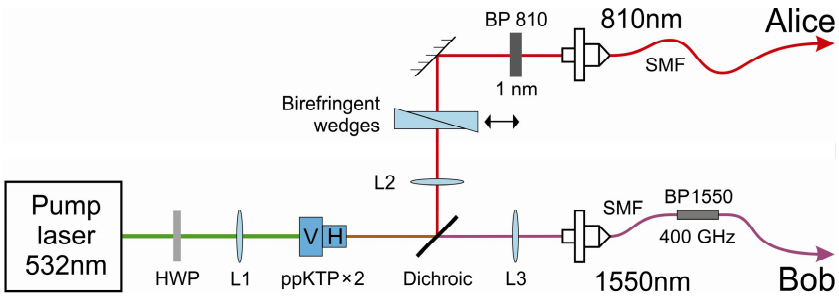

Fig. 5. Arrangement of the source for asymmetric generation of an 810 nm photon and a 1550 nm photon entangled in polarization. Using the half-wave plate HWP, the polarization of the pump photon is arranged such that the vertical (V) and the horizontal (H) crystals are excited equally. This results in a polarization-entangled state between the 810 nm and the 1550 nm photons.

3. TRANSMISSION OF POLARIZATION-ENTANGLED QUBITS THROUGH FIBERS OVER 101 KM

Clearly, over earthbound communication links, fibers carry distinct advantages, as at first sight they are independent of external influences such as depolarization or polarization mode dispersion. Yet, when using polarization as the carrier of entanglement, it remained an open question whether birefringent effects might seriously limit the use of optical fibers in such experiments. Recently, it was successfully demonstrated that time-bin entanglement can be transmitted over distances of the order of 50 km of optical fiber [16, 17]. In a related experiment [18], polarization entanglement could only be observed after background subtraction, which might be a significant problem in implementing practical quantum key distribution.

In our experiment [19], we created polarization-entangled photons by pumping a periodically-poled KTP nonlinear crystal. The down-conversion was degenerate in direction, but non-degenerate in energy. The two photons created had wavelengths of 810 nm and 1.550 nm respectively and were separated from each other using a dichroic mirror (Fig. 5). Again, the 810 nm photon was measured locally by Alice using a silicone avalanche photodetector (APD) while the 1.550 nm photon was sent over distances of up to 101 km to Bob, who used a gated InGaAs-APD. This detector was triggered using the signal from Alice's APD. The glass fibers leading from the source to Bob were locally coiled up within the laboratory (Fig. 6).

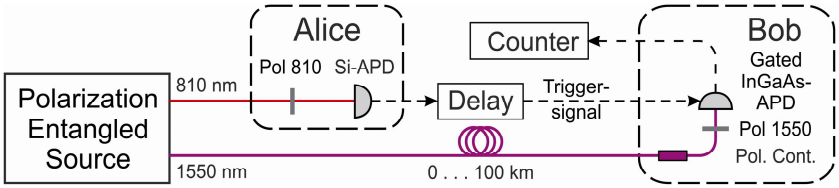

Fig. 6. Experimental set-up for measuring the transmission of polarization-entangled photons over large distances. The 810 nm photon emerging from the polarization-entangled source (Fig. 5) is measured locally by Alice. That way, a trigger signal is generated. The 1.550 nm photon is sent over to Bob, where it is registered by an InGaAs-APD triggered by Alice's signal. An electronic delay generator serves to adjust carefully the timing necessary.

In the experiment, fibers of different lengths were used. In the large distance experiment, we used two spools of non-zero dispersion shifted (NZD) fibers, each with a fiber of 50,4 km length resulting in a total length of 100,8 km. This results in a broadening of the total wave packet to 1,5 ns, the size of the gate window.

For the 101 km fiber, the observed two-photon visibility was 88,6%. A detailed model shows that this reduction of visibility is predominantly due to detector dark counts and chromatic dispersion effects. After a distance of 101 km, a coincidence rate of 104 counts/s could still be observed. From the raw visibility, we estimate a qubit error rate of 5,7%. Estimating the effects of realistic error correction, privacy amplification, we expect a secure key rate of 35 bit/s to be extracted after 101 km of fiber. Thus again, these experiments demonstrate the feasibility of entanglement distribution over distances of the order of 100 km.

4. CONCLUDING COMMENTS

Based on the free-space experiment and on the experiment using glass fibers, it has been demonstrated that entanglement can certainly survive distances of the order of 100 km. Nevertheless, the obtained data rate is rather low. Yet, possible applications of such experiments are not limited to quantum cryptography. Interesting future experiments might include quantum teleportation over these large distances and other fundamental questions.

This work was supported by the Austrian Science Fund FWF, the Austrian Research Promotion Agency FFG, the European Commission, the European Space Agency, and DTO, U.S. ARO.

REFERENCES

1. A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Phys. Rev. Lett.* 67, 661 (1991).
2. C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in *Proceedings of the International Conference on Computer Systems and Signal Processing*, Bangalore, pp. 175 – 179, 1984.
3. S. Wiesner, “Conjugate Coding,” SIGACT News 15 (1), 78 (1983).
4. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter and A. Zeilinger, “Quantum Cryptography with Entangled Photons,” *Phys. Rev. Lett.* 84, 4729-4732 (2000).
5. P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A.V. Sergienko and Y. H. Shih, “New High-Intensity Source of Polarization-Entangled Photon Pairs,” *Phys. Rev. Lett.* 75, 4337 (1995).
6. E. P. Wigner, “On Hidden Variables and Quantum Mechanical Probabilities,” *Am. J. Phys*. 38, 1005 (1970).
7. J. S. Bell, *Physics* 1, 195, Long Island City, N.Y., 1965.
8. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund and P. G. Kwiat, “Entangled State Quantum Cryptography: Eavesdropping on the Ekert Protocol,” *Phys. Rev. Lett.* 84, 4733 - 4736 (2000).
9. W. Tittel, J. Brendel, H. Zbinden and N. Gisin, “Quantum Cryptography Using Entangled Photons in Energy-Time Bell States,” *Phys. Rev. Lett.* 84, 4737 - 4740 (2000).
10. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.* 74, 145–195 (2002).

11. M. Dusek, N. Lutkenhaus and M. Hendrych, “Quantum Cryptography,” in: *Progress in Optics*, vol. 49, Ed. E. Wolf, Elsevier, pp. 381-454, 2006.

12. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, “Quantum key distribution using Gaussian-modulated coherent states,” *Nature* 421, 238-241 (2003).

13. S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus and G. Leuchs, „Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection,“ *Phys. Rev. A* 74, 042326 (2006).

14. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” *Phys. Rev. Lett.* 98, 230501 (2007).

15. 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, “Entanglement-based quantum communication over 144 km,” Nature Physics 3, 481 - 486 (2007).

16. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legre and N. Gisin, “Distribution of time-bin entangled qubits over 50 km of optical fiber,” *Phys. Rev. Lett*. 93, 180502 (2004).

17. H. Takesue, “Long-distance distribution of time-bin entanglement generated in a cooled fiber,” *Opt. Express* 14, 3453-3460 (2006).

18. C. Liang, K. F. Lee, J. Chena and P. Kumar, “Distribution of fiber-generated polarization entangled photon-pairs over 100 km of standard fiber in OC-192WDMenvironment,” postdeadline paper, *Optical Fiber Communications Conference*, paper PDP35, 2006.

19. H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe and A. Zeilinger, “High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber,” *Opt. Express* 15, 7853-7862 (2007).