chapter 3

Advanced Quantum Communications Experiments with Entangled Photons

M. Aspelmeyer and A. Zeilinger
University of Vienna and
Austrian Academy of Sciences

H. R. Böhm, A. Fedrizzi, S. Gasparoni,*
*M. Lindenthal, G. Molina-Terriza**, A. Poppe,*
*K. Resch***, R. Ursin and P. Walther*
University of Vienna

T.D. Jennewein
Austrian Academy of Sciences

Contents

*Present address: Center for Biomedical Engineering and Physics, Medical University of Vienna, Austria

**Present address: ICFO — Institut de Ciències Fotòniques, Barcelona, Spain

***Present address: Department of Physics, University of Queensland, Brisbane, Australia

3.1 Introduction

Quantum communication and quantum computation are novel methods of information transfer and information processing, all fundamentally based on the principles of quantum physics. The performances outdo their classical counterparts in many aspects [1,2]. In almost all quantum communication and quantum computation schemes, quantum entanglement [3] plays a decisive role. In essence, an entangled system can carry all information (e.g., on their polarization properties) only in their correlations, while no individual subsystem carries any information. This leads to correlations that are much stronger than classically allowed [89, 100], which is a powerful resource for information processing. It is therefore important to be able to generate, manipulate, and distribute entanglement as accurately and as efficiently as possible.

Successful demonstrations of quantum communication protocols started with photon experiments in 1992 and include quantum cryptography [4,5], the simultaneous distribution of a cryptographic key that is ultimately secured by the laws of quantum physics; later followed quantum dense coding [6,7], a protocol to double the classically allowed capacity of a communication channel by encoding two bits of information per bit sent, and finally quantum teleportation [8,9], the remote transfer of an arbitrary quantum state between distant locations.

Since these early achievements, the field of quantum communication, or more generally quantum information processing, has very much advanced. New schemes and techniques allow the generation and manipulation of entangled photon pairs and even of four-photon states with much higher efficiency and precision [10,11]. Also, the distances over which entanglement can be distributed are regularly pushed further. Owing to new protocols one can now achieve the successive use of teleported states and also the teleportation of entanglement via entanglement swapping (see Section 3.2.1). An important method for distributing pure entangled states even over noisy channels is entanglement purification (see Section 3.2.2), which is one ingredient for a quantum repeater and is also based on the application of elementary quantum gates such as a controlled NOT (CNOT) gate (see Section 3.2.3). Another promising line of development involves entanglement in higher dimensions, which might allow further advances such as quantum communication with a higher resistance against noise (see Section 3.2.4). A very recent development is the real-world application of entanglement-based quantum cryptography (see Section 3.2.5). This is linked to the research on distributing entanglement over long distances, which aims at the establishment of a quantum communication network (see Section 3.2.6), eventually on a global scale by using satellites.

3.2 *Advanced Quantum Communication Schemes*

3.2.1 *Scalable Teleportation and Entanglement Swapping*

Teleportation of quantum states [12] is an intriguing concept within quantum physics and a striking application of quantum entanglement. Besides its importance for quantum computation [13,14], teleportation is at the heart of the quantum repeater [15], a concept eventually allowing the distribution of quantum entanglement over arbitrary distances and thus enabling quantum communication over large distances and even networking on a global scale.

The purpose of quantum teleportation is to transfer an arbitrary quantum state to a distant location, e.g., from Alice to Bob, without transmitting the actual physical object carrying the state. Classically this is an impossible task, since Alice cannot obtain the full information of the state to be teleported without previous knowledge about its preparation. Quantum physics, however, provides a working strategy. Suppose, Alice and Bob share an ancilla entangled pair in advance. Alice then performs a Bell state measurement between the teleportee particle and her shared ancilla, i.e., she projects the two particles into the basis of Bell states. The four possible outcomes of this measurement provide her with two bits of classical information, which is sufficient to reconstruct the initial quantum state at Bob's side. After communicating the classical result to Bob, he can perform one out of four unitary operations to obtain the original state to be teleported. In detail: suppose photon 1, which Alice wants to teleport to Bob, is in a general polarization state $|\chi\rangle_1 = \alpha|H\rangle_1 + \beta|V\rangle_1$ (unknown to Alice), and the pair of photons 2 and 3 shared by Alice and Bob is in the polarization-entangled state $|\Psi^-\rangle_{23}$. This state is one of the four maximally entangled Bell states $|\Psi^\pm\rangle_{ij} = \frac{1}{\sqrt{2}}(|HV\rangle_{ij} \pm |VH\rangle_{ij})$ and $|\Phi^\pm\rangle_{ij} = \frac{1}{\sqrt{2}}(|HH\rangle_{ij} \pm |VV\rangle_{ij})$, where H and V denote horizontal and vertical linear polarizations, and i and j index the spatial modes of the photons. The overall state of photons 1, 2, and 3 can be rewritten as

$$
\begin{aligned}
|\Psi\rangle_{123} = |\Psi\rangle_1 |\Psi^-\rangle_{23} = \frac{1}{2}[& -|\Psi^-\rangle_{12}\,(\alpha\,|\mathrm{H}\rangle_3 + \beta\,|\mathrm{V}\rangle_3) \\
& -|\Psi^+\rangle_{12}\,(\alpha\,|\mathrm{H}\rangle_3 - \beta\,|\mathrm{V}\rangle_3) \\
& +|\Phi^-\rangle_{12}\,(\alpha\,|\mathrm{V}\rangle_3 + \beta\,|\mathrm{H}\rangle_3) \\
& +|\Phi^+\rangle_{12}\,(\alpha\,|\mathrm{V}\rangle_3 - \beta\,|\mathrm{H}\rangle_3)].
\end{aligned} \tag{3.1}
$$

It can thus be seen that a joint Bell measurement on photons 1 and 2 at Alice's side, i.e., a projection of particles 1 and 2 onto one of the four Bell states, projects the state of photon 3 at Bob's side into one of the four corresponding states, as shown in Equation (3.1). The outcome of the Bell measurement is totally random (otherwise Alice and Bob could communicate faster than light). However, when knowing Alice's measurement results, Bob can perform a unitary transformation, independent of $|\chi\rangle_1$, on photon 3 and convert its state into the initial state of photon 1.

3.2.1.1 *Entanglement Swapping*

An important feature of teleportation (also of relevance for long-distance quantum communication) is that it provides no information whatsoever about the state being teleported. This means that an arbitrary unknown quantum state can be teleported. In fact, the quantum state of a teleportee particle does not have to be well defined, and it could thus even be entangled with another photon. A Bell state measurement of two of the photons — one each from two pairs of entangled photons — results in the remaining two photons becoming entangled, even though they have never interacted in the past (see Figure 3.1(a)). This was demonstrated recently by violating a Bell inequality between particles that never interacted with each other [16] (see Figure 3.1(b)). A chain of several entanglement swapping systems [17] can in principle be used to transfer quantum entanglement between distant sites.

3.2.1.2 *Scalable Teleportation*

A recent result also of relevance for long-distance quantum communication is the first realization of freely propagating teleported qubits [18], which will eventually allow the subsequent use of teleported states. In previous experimental realizations of teleportation with photons, the teleported qubit had to be detected (and thus destroyed) to verify the success of the procedure. This can be avoided by providing, on average, more entangled ancilla pairs than states to be teleported. In the modified teleportation scheme (Figure 3.2), a successful Bell state analysis results in freely propagating individual qubits, which can be used for further cascaded teleportation. In many of our experiments, two independent polarization entangled photon pairs, produced by spontaneous parametric down-conversion (SPDC) with a probability p, are used both for the preparation of the entangled pair $|\Psi^-\rangle_{23}$ (photons 2 and 3) and for the preparation of the initial state to be teleported (photons 1 and 4).

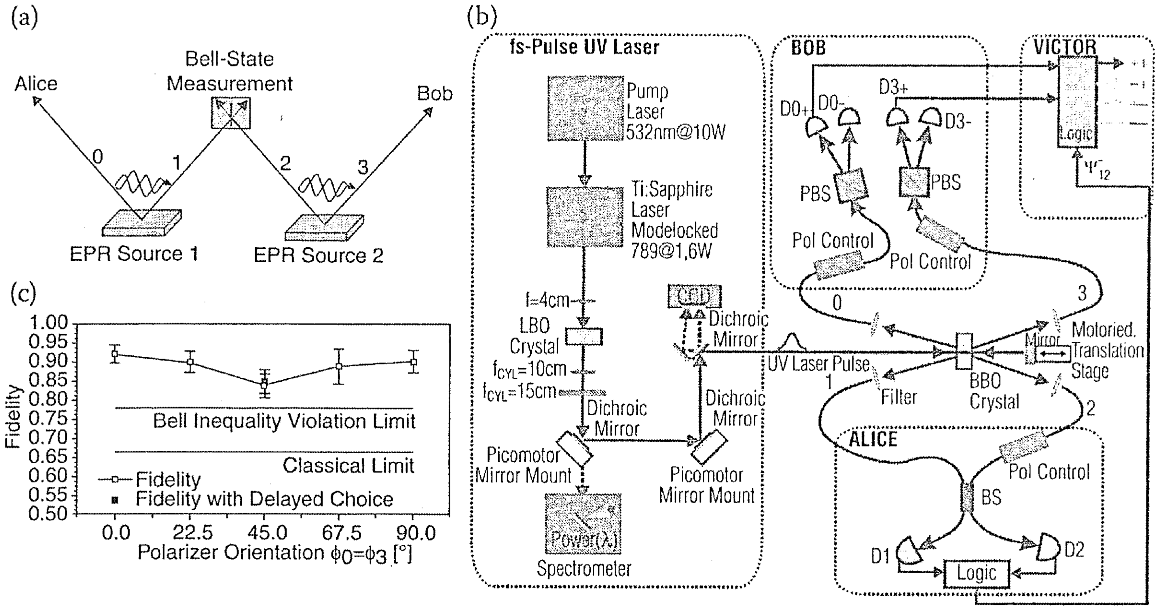

Figure 3.1 (a) Scheme for entanglement swapping, i.e., the teleportation of entanglement. Two entangled pairs 0, 1 and 2, 3 are produced by two entangled photon sources (EPR). One particle from each of the pairs is sent to two separated observers; say 0 is sent to Alice and 3 to Bob. 1 and 2 become entangled through a Bell state measurement, by which 0 and 3 also become entangled. This requires the entangled qubits 0 and 3 neither to come from a common source nor to have interacted in the past. (b) Experimental setup for the demonstration of teleportation and entanglement swapping using pairs of polarization entangled photons. The two entangled photon pairs were produced by down-conversion in barium borate (BBO), pumped by femtosecond UV laser pulses traveling through the crystal in opposite directions. After spectral filtering, all photons were collected in single-mode optical fibers for further analysis and detection. Single-mode fibers offer the benefit that the photons remain in a perfectly defined spatial mode allowing high-fidelity interference. In order to optimize the temporal overlap between photon 1 and 2 in the beam splitter, the UV mirror was mounted on a motorized translation stage. Photons 0 and 3 were sent to Bob's two-channel polarizing beamsplitters for analysis, and the required orientation of the analyzers was set with polarization controllers in each arm. All photons were detected with silicon avalanche photodiodes, with a detection efficiency of about 40%. Alice's logic circuit detected coincidences between detectors D1 and D2. (c) Experimental violation of Bell's inequalities from particles that never interacted with each other obtained through correlation measurements between photons 0 and 3, which is a lower bound for the fidelity of the teleportation procedure (from [16]). ϕ_0 (ϕ_3) is the setting of the polarization analyzer for photon 0 (photon 3) and $\phi_0 = \phi_3$. The minimum fidelity of 0.84 is well above the classical limit of 2/3 and also above the limit of 0.79 necessary for violating Bell's inequality.

Photon 4 acts as a trigger to indicate the presence of photon 1. If one pair of photons is emitted in each of the pairs of modes 1-4 and 2-3, a threefold coincidence of T-D1-D2 is sufficient to guarantee a successful teleportation.

However, owing to the probabilistic nature of SPDC, two photon pairs are both emitted into modes 1-4 with the same probability p^2 as for a

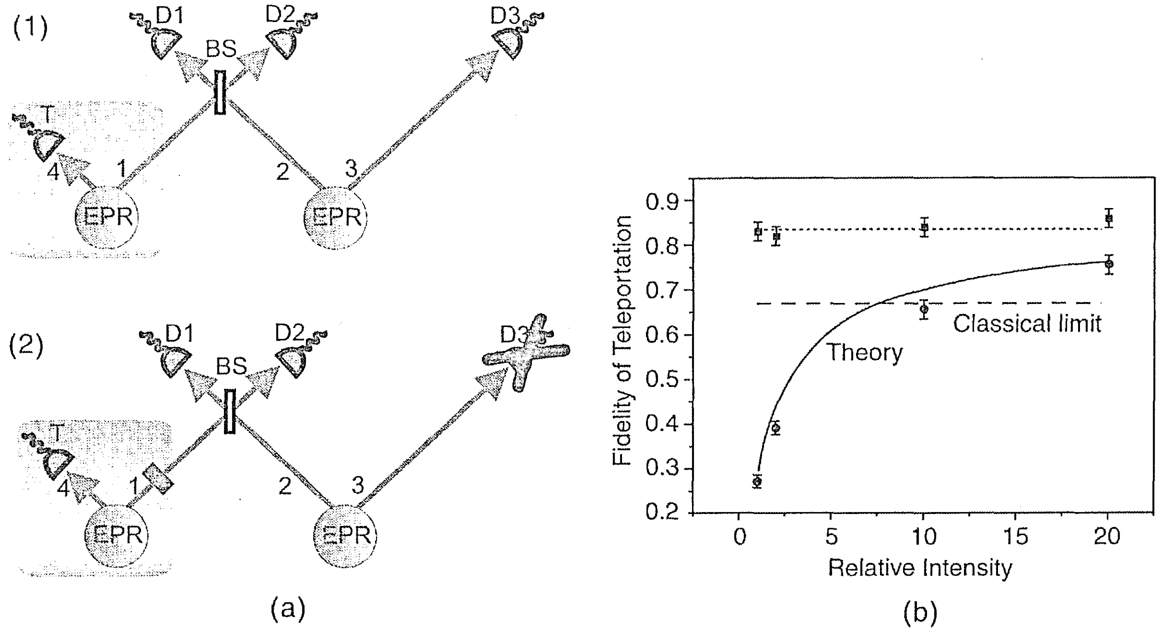

Figure 3.2 (a) (1) Original qubit teleportation scheme using polarization-entangled photon pairs based on spontaneous parametric down-conversion (EPR sources); (2) Freely propagating teleported qubits. (b) Conditional fidelities (squares) and nonconditional fidelities (circles) obtained in 45° teleportation for different attenuation $1/\gamma$. With increasing attenuation of mode 1, an increase of nonconditional fidelities is observed while the conditional ones remain constant. For $\gamma = 0.05$, the classical limit 2/3 is clearly overcome.

successful teleportation. This will also lead to threefold coincidences of T-D1-D2, but in this case no teleportation occurs, as mode 3 is simply empty. To ensure a successful teleportation, it has been necessary to confirm the presence of photon 3 by actually detecting it (Figure 3.2). For this reason, the original Innsbruck experiment [9], the first experimental demonstration of quantum teleportation, has been called a "postselected" one, while probably the word "conditional" would be more appropriate, as detection of photon 3 does not depend on its state. In the new protocol, an unbalanced two-photon interferometer is used to make a detection at Bob's side obsolete and therefore allow for a free propagation of the teleported qubits. The number of unwanted D1-D2 coincidence counts is reduced by attenuating beam 1 by a factor of γ while leaving the modes 2-3 unchanged. Then a threefold coincidence D1-D2-T will occur with probability p^2 owing to successful teleportation, and with significantly lower probability γp^2 there will be a spurious coincidence. Thus the probabilty for a successful teleportation event (conditioned on D1-D2-T) will scale with $1/(1+\gamma)$, and for sufficiently low γ it will not be necessary anymore to detect the teleported photon 3; a freely propagating teleported beam of qubits emerges.

To demonstrate experimentally nonconditional teleportation, we inserted a series of neutral density filters in mode 1 and showed that the probability of having a successful teleportation conditioned on a threefold coincidence

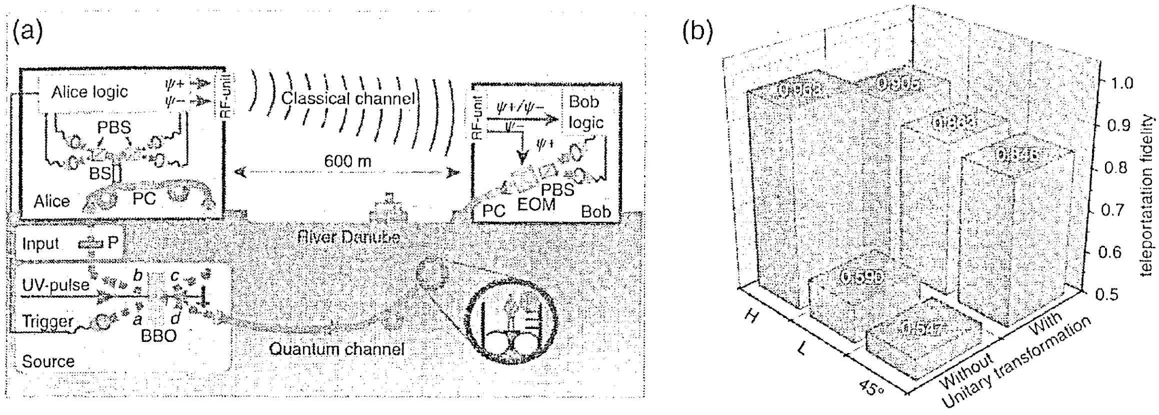

Figure 3.3 (a) Sketch of the two laboratories located on either side of the Danube River (from [23]). The laboratories were located in two sewage water system buildings owned by the city of Vienna. The faster classical channel (microwave) and the slower quantum channel (fiber) are shown above and underneath the Danube. The vertical separation of the two channels is about 40 m. (b) Fidelity of the teleported states with and without active switching.

of D1, D2, and T increases with decreasing γ. The corresponding fidelities for conditional (fourfold detection) and nonconditional (threefold detection D1-D2-T) teleportation are shown in Figure 3.2b. We were able to demonstrate the preparation of a freely propagating teleported quantum state with high (nonconditional) fidelity of 0.85 ± 0.02, i.e., well above the classical limit.* The possibility of letting the teleported qubit travel freely in space, together with the high experimental visibility obtained, is a fundamental step in the direction of the realization of long-distance quantum communication. Further protocols, such as entanglement purification, are then needed to overcome decoherence in long-distance quantum channels (see Section 3.2.2).

3.2.1.3 Long-Distance Quantum Teleportation

Teleportation is the basis for the quantum repeater [15], which allows distributing quantum entanglement over long distances. Also, quantum teleportation over longer distances will be needed for realizing quantum network schemes involving several parties [22] and naturally for interconnecting devices utilizing quantum computational algorithms. As a next step toward a full-scale implementation of a quantum repeater, we have realized a large-scale implementation of teleportation [23] of photon qubits in an outdoor environment. The two laboratories involved, Alice and Bob, are separated by 600 m across the Danube River in Vienna (see Figure 3.3). Additionally, while it has been shown that systems based on linear optical elements can only determine two of the four Bell states perfectly [24,7,25], our system achieves the

*Other nonconditional quantum teleportation experiments have been performed with continuous variables [19] and, only recently, with ions [20,21]. However, the most suitable systems for long-distance transmission are currently photons.

optimal teleportation efficiency of 50% when using linear optics alone. This is realized by an active feed-forward technique, namely by detecting two of the four Bell states on the transmitter site, Alice, and correspondingly switching the unitary transformation for the receiver photon at the receiver site, Bob, with a fast electro optic modulator (EOM).

An important feature of our experiment was the implementation of an optimized Bell state analyzer (BSA) capable of detecting two of the four Bell states on Alice's side, and the implementation of an "actively switched" unitary transformation on Bob's side triggered by the outcome of Alice's Bell state measurement (BSM). Alice's BSM result was sent to Bob via a microwave link (2.4 GHz) above the Danube River. The classical channel transmitted one bit of information about Alice's BSM outcome (Ψ^- or Ψ^+). This signal traveled the distance of 600 m almost at the vacuum speed of light, which took about 2 μs. Additionally, delays in the detectors and in several signal stages of the transceivers introduced an extra delay of 0.6 μs. However, since the speed of light in a fiber is approximately 2/3 of the vacuum speed of light, the entangled photon d traveled the 800 m fiber from Alice to Bob in about 4 μs. Therefore, the information on Alice's BSA outcome arrived at Bob's laboratory approximately 1.4 μs before the arrival of photon d. This provided Bob with sufficient time to set an EOM to apply the birefringent phase shift of 0 or π between the $|H\rangle$ and $|V\rangle$ optical light modes on the received photon d. When Alice's BSM result was a Ψ^-, then Bob left the EOM at the idle voltage (i.e., the EOM introduces no phase shift and the teleported state remains unchanged), and when it was a Ψ^+, then Bob applied the activation voltage (i.e., the EOM introduced a π phase shift between the horizontal and vertical polarization) just before the photon passed through the EOM. In both cases, Bob eventually obtains an exact replica of the initial teleportee state (see Equation (3.1)).

The EOM was a KDP Pockels cell, which achieved the phase shift of π with an accuracy of 1:200 at a voltage of 3.4 kV. The timing information of the received classical signal was delayed with a digital delay generator, and when a Ψ^+ was received, then the EOM was triggered with a 100 ns pulse with a rise time of 20 ns. Additionally, Bob used a logic circuit to count only those detections of his photons that arrived at the expected times within a coincidence window of ±10 ns. Note that without operation of the EOM, Bob observes only a completely mixed polarization for a $|45°\rangle$ and a circular polarization input state. When teleporting polarizations along H or V, the transformation is irrelevant, since the EOM phase shift does not affect these states. The full teleportation protocol was demonstrated by teleporting distinct linear polarization states and circular polarization states (see Figure 3.4b). The classical fidelity limit of 2/3 [26] is clearly surpassed by our observed fidelities of around 0.85. This is a step toward a full-scale implementation of a quantum repeater to achieve shared pure entanglement between arbitrarily separated quantum communication partners. Such a quantum repeater requires quantum teleportation, purification of entanglement, and quantum memories. Recent results [27,28] indicate the advance of quantum memory, which might be suitable for future quantum communication networks.

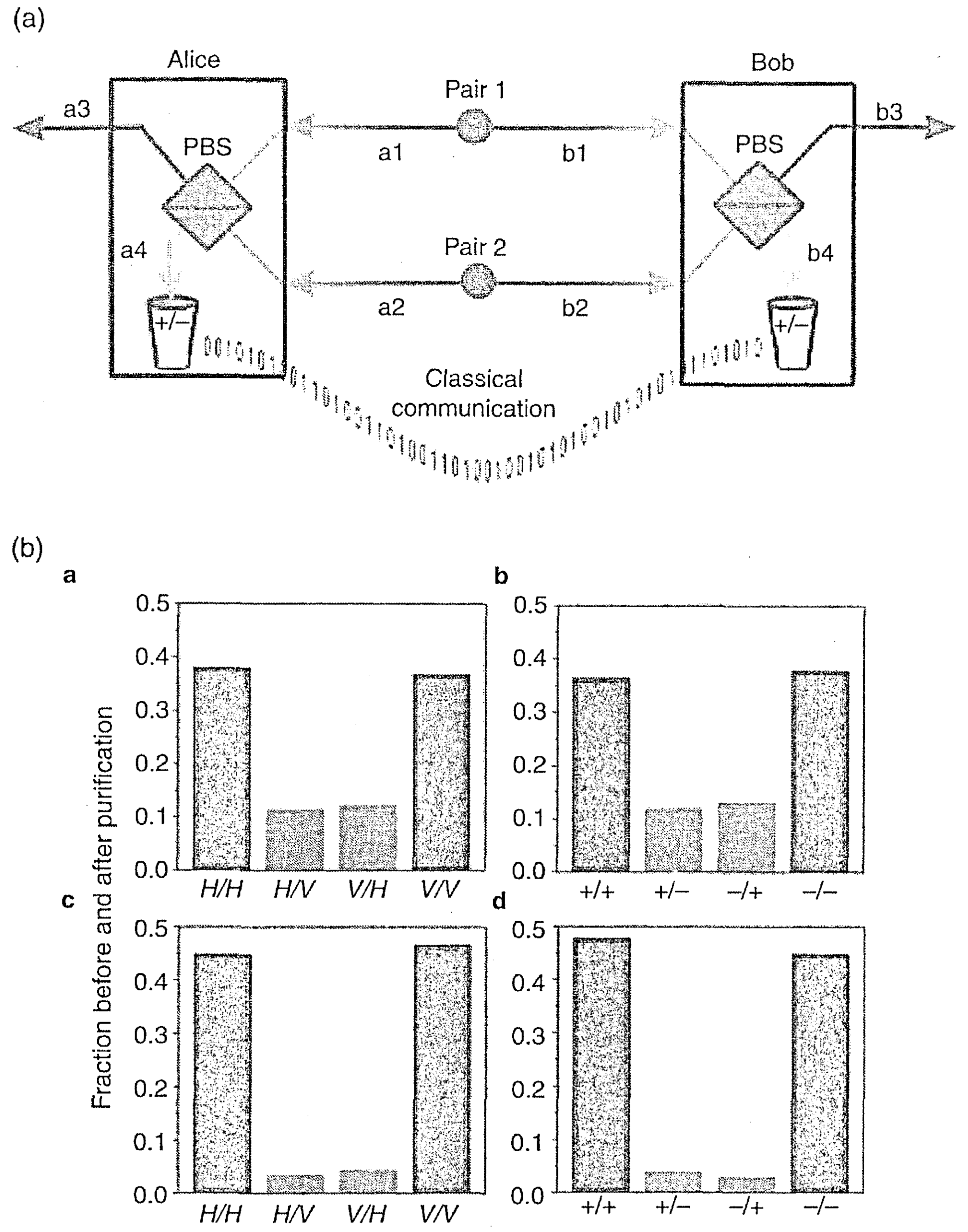

Figure 3.4 (a) Scheme for entanglement purification of polarization-entangled qubits [30]. Two shared pairs of an ensemble of equally mixed entangled states ρ_{AB} are fed into the input ports of polarizing beam splitters that substitute the bilateral CNOT operation necessary for a successful purification step. Alice and Bob keep only those cases where there is exactly one photon in each output mode. This can happen only 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 a_4 and b_4. Depending on the results, Alice performs a specific operation on the photon in mode a_3. After this procedure, the remaining pair in modes a_3 and b_3 will have a higher degree of entanglement than the two original pairs. (b) Experimental results. **a** and **b** show the experimentally measured fractions both in the H/V and in the $+/-$ bases for the original mixed state. **c** and **d** show the measured fractions of the purified state in the modes a_3 and b_3 both in the H/V and in the $+/-$ bases. Compared with the fractions in **a** and **b**, the experimental results shown in **c** and **d** both together confirm the success of entanglement purification.

3.2.2 Purifying Quantum Entanglement

Owing to unavoidable decoherence in the quantum communication channel, the quality of entangled states generally decreases with the channel length. Entanglement purification schemes [29] allow two spatially separated parties to convert an ensemble of partially entangled states (which result from transmission through noisy channels) to a set of almost perfectly entangled states by performing local unitary operations and measurements on the shared pairs, and coordinating their actions with a classical channel. One thus simulates a noiseless quantum channel by a noisy one, supplemented by local actions and classical communication. In a recent experiment, entanglement purification could be demonstrated for the first time experimentally for mixed *polarization-entangled two-particle states* [30].

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 (see Section 3.2.3) 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 leads to a less noisy quantum channel [29]. For the case of polarization entanglement, such a parity check on the correlations can be performed in a straightforward way by using polarizing beamsplitters (PBS) [31] that transmit horizontally polarized photons and reflect vertically polarized ones.

Consider the situation in which Alice and Bob have established a noisy 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 3.2). Only if the entangled input states have the same correlations, i.e., they have the same parity with respect to their polarization correlations, will the four photons 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 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 one of the four maximally entangled Bell states. 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 $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$ will create the pure states $|\Phi^+\rangle_{a_3,b_3}$ with probability $F' = F^2/[F^2 + (1 - F)^2]$ and $|\Psi^+\rangle_{a_3,b_3}$ with probability $1 - F'$, respectively. The fraction F' of the desired state $|\Phi^+\rangle$ becomes larger for each purification step if $F > \frac{1}{2}$. 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. In these experiments, decoherence is overcome to the extent that the technique would achieve tolerable error rates for quantum repeaters in long-distance quantum communication based only on linear optics and polarization entanglement.

Purification not only provides a way to implement long-distance quantum communication but also plays an important role in fault-tolerant quantum computation. Quantum error correction [32,33] allows a universal quantum computer to be operated in a fault tolerant way [34,35]. However, in order for quantum repeaters and quantum error correction schemes to work, there are stringent requirements on the precision of logic operations between two qubits. While the tolerable error rate of logic gates in quantum repeaters is of the order of several percent [15], that in quantum error correction is of the order of 10^{-4} to 10^{-5}, still far beyond experimental feasibility. Fortunately, a recent study shows that entanglement purification can also be used to increase the quality of logic operations between two qubits by several orders of magnitude [36]. In essence, this implies that the threshold for tolerable error in quantum computation is within reach using entanglement purification and linear optics. Our experiments achieved an accuracy of local operations at the PBS of about 98%, or equivalently an error probability of 2%. Together with the high fidelity achieved in the latest photon teleportation experiments, the present purification experiment implies that the threshold of tolerable error rates in quantum repeaters can be well fulfilled. This opens the door to realistic long-distance quantum communication. On the other hand, with the help of entanglement purification the strict accuracy requirements of the gate operations for fault-tolerant quantum computation are also reachable, for example, within the frame of linear optics quantum computation [37].

3.2.3 A Photonic Controlled NOT Gate

As can be seen above, advanced quantum communication protocols such as entanglement purification may require nontrivial manipulation of qubits, e.g., bilateral parity checks on pairs of photons (see Section 3.2.2). The underlying operations are typically elementary quantum gates, which are also used for universal quantum computation. Well-known examples of such gates are the controlled NOT (CNOT) and controlled phase (CPhase) operations. The crucial trait of these gates is that they can change the entanglement between qubits. A CNOT gate flips the value of the target bit if and only if the control bit has the logical value 1 (see below). Entanglement can now be created between two independent input qubits if the control bit is in a superposition of 0 and 1. On the other hand, any Bell state that is fed into a CNOT gate will result in distinct separable output states that make it possible to distinguish all four Bell states deterministically.

In previous experiments [38,39,40] destructive linear optical gate operations have been realized. However, such schemes necessarily destroy the output state and are hence not classically feed-forwardable, i.e., they do not

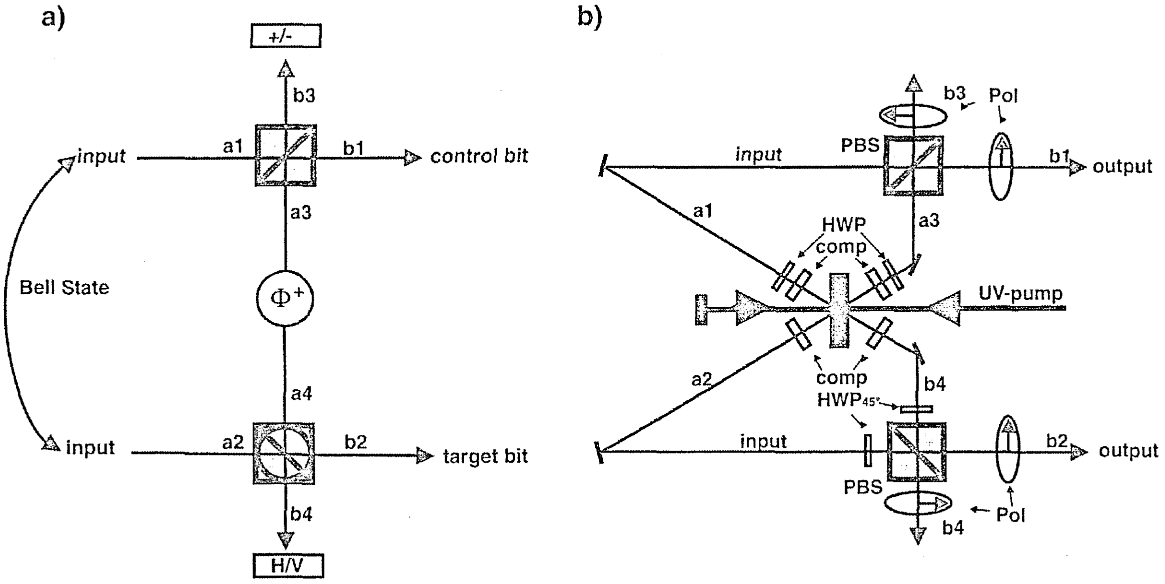

Figure 3.5 (a) The scheme to obtain a photonic realization of a CNOT gate with two independent qubits. The qubits are encoded in the polarization of the photons. The scheme makes use of linear optical components, polarization entanglement, and postselection. When one and only one photon is detected at the polarization sensitive detectors in the spatial modes b_3 and b_4, the scheme works as a CNOT gate. (b) The experimental setup. A type II spontaneous parametric down-conversion is used both to produce the ancilla pair (in the spatial modes a_3 and a_4) and to produce the two input qubits (in the spatial modes a_1 and a_2). In this case, initial entanglement polarization is not desired, and it is destroyed by making the photons go through polarization filters, which prepare the required input state. Half-wave plates (HWP) have been placed in the photon paths in order to rotate the polarization; compensators (comp) are able to nullify the birefringence effects of the nonlinear crystal. Overlap of the wavepackets at the PBSs is assured through spatial and spectral filtering.

allow scalable quantum computation. This section will discuss the realization of a CNOT gate, which operates on two polarization qubits carried by independent photons and which satisfies the feed-forwardability criterion [41]. The scheme, shown in Figure 3.5, was first proposed by Franson et al. [42]. It performs a CNOT operation on the input photons in spatial modes a_1 and a_2; the output qubits are contained in spatial modes b_1 and b_2. The ancilla photons in the spatial modes a_3 and a_4 are in the maximally entangled Bell state $|\phi^+\rangle_{a_3,a_4} = \frac{1}{\sqrt{2}}(|H\rangle_{a_3}|H\rangle_{a_4} + |V\rangle_{a_3}|V\rangle_{a_4})$.

In the following, $|H\rangle$ (a horizontally polarized photon) and $|V\rangle$ (a vertically polarized photon) will denote our logical "0" and "1". The CNOT operation for qubits encoded in polarization can be written as $|H\rangle_c|H\rangle_t \rightarrow |H\rangle_c|H\rangle_t$, $|H\rangle_c|V\rangle_t \rightarrow |H\rangle_c|V\rangle_t$, $|V\rangle_c|H\rangle_t \rightarrow |V\rangle_c|V\rangle_t$, $|V\rangle_c|V\rangle_t \rightarrow |V\rangle_c|H\rangle_t$, where the indices c and t denote the control and target qubit.

The scheme works in those cases where one and only one photon is found in each of the modes b_3 and b_4. It combines two simpler gates, namely the destructive CNOT and the quantum encoder. The first gate can be seen in the lower part of Figure 3.5 and comprises a polarizing beam splitter (PBS2) rotated by 45° (the rotation is represented by the circle drawn inside the symbol of the PBS), which works as a destructive CNOT gate on the polarization qubits, as was experimentally demonstrated in [42]. The upper part, comprising the entangled state and the PBS1, is meant to encode the control bit in the two channels a_4 and b_1.

Owing to the PBS operation, which transmits horizontally polarized photons and reflects vertically polarized ones, the successful detection of the state $|+\rangle$ at the port b_3 postselects the following transformation of the arbitrary input state in a_1: $\alpha|H\rangle_{a_1} + \beta|V\rangle_{a_1} \rightarrow \alpha|H\rangle_{a_4}|H\rangle_{b_1} + \beta|V\rangle_{a_4}|V\rangle_{b_1}$. The control bit is thus encoded in a_4 and in b_1. The photon in a_4 serves as the control input to the destructive CNOT gate and will be destroyed, while the second photon in b_1 serves as the output control qubit.

For the gate to work properly, one has to demonstrate that the most general input state,

$$|\Psi\rangle^{in}_{a_1,a_2} = |H\rangle_{a_1}(\alpha_1|H\rangle_{a_2} + \alpha_2|V\rangle_{a_2}) + |V\rangle_{a_1}(\alpha_3|H\rangle_{a_2} + \alpha_4|V\rangle_{a_2}),$$

can be converted to the output state,

$$|\Psi\rangle^{out}_{b_1,b_2} = |H\rangle_{b_1}(\alpha_1|H\rangle_{b_2} + \alpha_2|V\rangle_{b_2}) + |V\rangle_{b_1}(\alpha_3|V\rangle_{b_2} + \alpha_4|H\rangle_{b_2}).$$

Let us consider first the case where the control photon is in the logical zero or horizontally polarized. The control photon will then travel undisturbed through the PBS, arriving in the spatial mode b_1. As required, the output photon is $|H\rangle$. In order for the scheme to work, a photon needs to arrive also in mode b_3: given that the input photon is already in mode b_1, the additional photon will necessarily be provided by the EPR pair and is $|H\rangle$ after transmission through PBS1. We know that the photons in a_3 and a_4 are entangled, so the photon in a_4 is also in the horizontal polarization state. For a $|H\rangle$ ($|V\rangle$) target photon, taking into account the 45° rotation of the polarization on the paths a_2, a_4 due to the half-wave plates, the input at PBS2 will then be in the state $|+\rangle_{a_2}|+\rangle_{a_4}(|+\rangle_{a_2}|-\rangle_{a_4})$. This state will give rise, with a probability of 50%, to the state where two photons go through the PBS2, namely $|\phi^{\pm}\rangle_{b_2,b_4} = \frac{1}{\sqrt{2}}(|H\rangle_{b_2}|H\rangle_{b_4} \pm |V\rangle_{b_2}|V\rangle_{b_4})$. After the additional rotation of the polarization and after the subsequent change to the H/V basis (where the measurement will be performed), this state acquires the form $|\phi^{+}\rangle_{b_2,b_4} = \frac{1}{\sqrt{2}}(|H\rangle_{b_2}|H\rangle_{b_4} + |V\rangle_{b_2}|V\rangle_{b_4})$ $(|\psi^{+}\rangle_{b_2,b_4} = \frac{1}{\sqrt{2}}(|H\rangle_{b_2}|V\rangle_{b_4} + |V\rangle_{b_2}|H\rangle_{b_4}))$.

The expected result, $|H\rangle(|V\rangle)$, in the mode b_2 is found for the case where the photon in b_4 is horizontally polarized. We can see in a similar way that the gate works also for the cases where the control photon is vertically polarized or is polarized at 45°.

The experimental setup for the CNOT gate is shown in Figure 3.5. An ultraviolet pulsed laser, centered at a wavelength of 398 nm, with pulse duration 200 fs and a repetition rate of 76 MHz, impinges on a nonlinear BBO crystal [43], in which it produces probabilistically the first photon pair in the spatial modes a_1 and a_2. They serve as input qubits to the gate. The UV laser is reflected back by the mirror M1 and, on passing through the crystal a second time, produces the entangled ancilla pair in spatial modes a_3 and a_4.

Half-wave plates and nonlinear crystals in the paths provide the necessary birefringence compensation, while the same half-wave plates are used to adjust the phase between the down-converted photons (i.e., to produce the state ϕ^+) *and to implement the* CNOT gate.

We then superpose the two photons at Alice's (Bob's) side in the modes a_1, a_3 (a_2, a_4) at a polarizing beam splitter PBS1 (PBS2). The indistinguishability between the overlapping photons is improved by introducing narrow bandwidth (3 nm) spectral filters at the outputs of the PBSs and monitoring the outgoing photons by fiber-coupled detectors. The single-mode fiber couplers guarantee good spatial overlap of the detected photons; the narrow bandwidth filters stretch the coherence time to about 700 fs, substantially larger than the pump pulse duration [44]. The temporal and spatial filtering process effectively erases any possibility of distinguishing the photon pairs and therefore allows two-photon quantum interference.

The described CNOT scheme is nondestructive, i.e., the output photons can travel freely in space and may be further used in quantum communication protocols. This is achieved by detecting one and only one photon in modes b_3 and b_4. Since photon-number resolving detectors are not yet readily available at this wavelength, we implement a fourfold coincidence detection to confirm that photons actually arrive in the output modes b_1 and b_2.

To demonstrate experimentally the working operation of the CNOT gate, we first verify the CNOT truth table for input qubits in the computational basis states $|H\rangle|H\rangle$, $|H\rangle|V\rangle$, $|V\rangle|H\rangle$, and $|V\rangle|V\rangle$. Figure 3.6(b) compares the count rates for all 16 possible combinations. We then show that the gate also works for a superposition of input states. The special case in which the control input is a 45° polarized photon and the target qubit is an $|H\rangle$ photon is particularly interesting: we expect that the state $|+\rangle_{a_1}|H\rangle_{a_2}$ evolves into the maximally entangled state $|\phi^+ b_1, b_2 = \frac{1}{\sqrt{2}}(|H\rangle_{b_1}|H\rangle_{b_2} + |V\rangle_{b_1}|V\rangle_{b_2})$. We prepare $|+\rangle_{a_1}|H\rangle_{a_2}$ as the input state; first we measure the count rates of the four combinations of the output polarization $(|H\rangle|H\rangle, \ldots, |V\rangle|V\rangle)$ and then after going to the $|\pm\rangle$ linear polarization basis an Ou–Hong–Mandel interference measurement is possible; this is shown in Figure 3.6.

On the other hand, the same CNOT operation can be used to identify Bell states when they are used as input states [45]. For this procedure, the gate performs an operation that transforms each of the entangled Bell states into well-defined but different separable states, which are simple to distinguish. When a Bell state enters a CNOT gate in modes a_1 and a_2, the gate operation can be described by

$$|\phi^{\pm}\rangle_{a_1,a_2} \to |\pm\rangle_{b_1}|H\rangle_{b_2}$$

$$|\psi^{\pm}\rangle_{a_1,a_2} \to |\pm\rangle_{b_1}|V\rangle_{b_2}.$$

Figure 3.6 shows the count rates of all 16 possible combinations (four different inputs and four different outputs). They clearly confirm the successful implementation of the Bell state analyzer. The fidelity of each Bell state analysis is $F_{\phi^+} = (0.75 \pm 0.05)$, $F_{\phi^-} = (0.79 \pm 0.05)$, $F_{\psi^+} = (0.79 \pm 0.05)$,

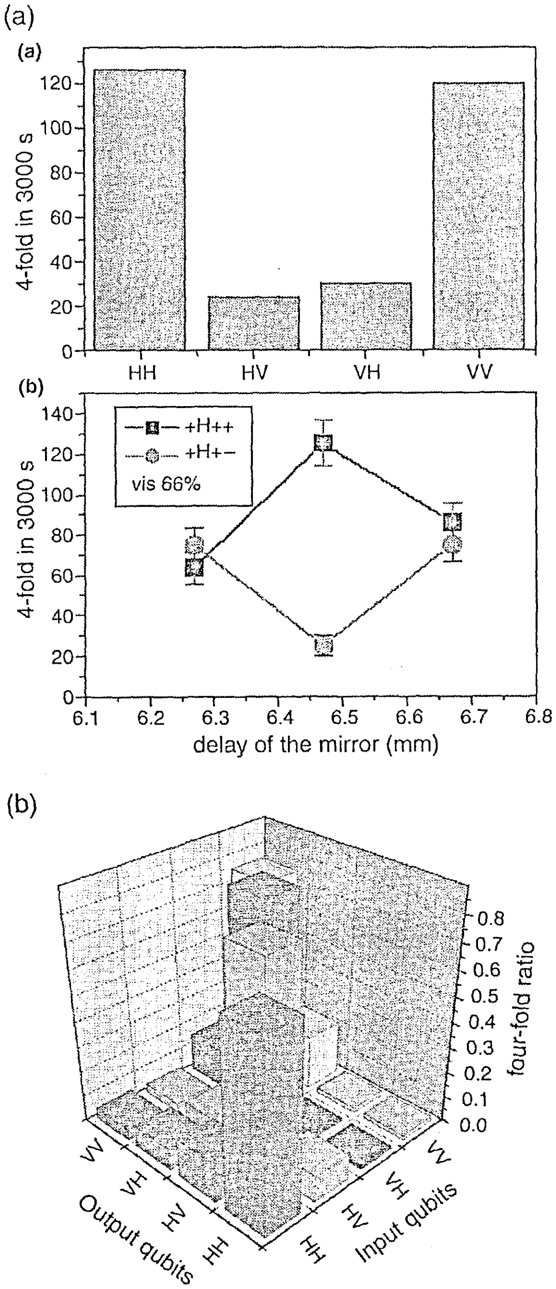

Figure 3.6 (a) Demonstration of the ability of the CNOT gate to transform a separable state into an entangled state. In (a), the coincidence ratio between the different terms $|H\rangle|H\rangle, \ldots, |V\rangle|V\rangle$ is measured, proving that the birefringence of the PBS has been sufficiently compensated; in (b) the superposition between $|H\rangle|H\rangle$ and $|V\rangle|V\rangle$ is proved to be coherent, by showing via the Ou–Hong–Mandel dip at 45° that the desired $|+\rangle$ state of the target bit emerges much more often than the spurious state $|-\rangle$. The fidelity is of $(81 \pm 2)\%$ in the first case and $(77 \pm 3)\%$ for the second. (b) Experimental demonstration of the optical Bell state analyzer. Fourfold coincidences for all possible 16 combinations of the inputs and outputs are shown. Each of the four different polarization-encoded Bell states is transformed into a distinguishable separable state $|\phi^{\pm}\rangle_{a_1,a_2} \to |\pm\rangle_{b_1}|H\rangle_{b_2}$ and $|\psi^{\pm}\rangle_{a_1,a_2} \to |\pm\rangle_{b_1}|V\rangle_{b_2}$. Each input state was measured for 1800 seconds at each of the four different polarizer settings. The fidelity is, on average, 77%.

$F_{\psi^-} = (0.75 \pm 0.05)$, without subtracting background of any kind. The incorrect outcomes originate mainly from incomplete suppression of the double pair emission and imperfections in the PBS operation.

3.2.4 *Higher Dimensional Entanglement for Quantum Communications*

In classical communication protocols it is not unusual to send the information encoded not only in 0's and 1's but also in a higher number of levels. For example, when the information is encoded in phase-modulated electrical signals, coding two bits per phase change doubles the number of bits per second. This is called two-level coding. This method is suitable, for example, for 2400 bps modems (CCITT V.26). Encoding more bits per phase change increases the number of bits per second but, assuming a constant noise, decreases the signal-to-noise ratio (SNR). The right choice of level coding per physical information carrier is a complicated engineering problem which, besides the speed and the SNR, includes the elaboration of new and efficient communication protocols for higher level encoding.

As we have already reviewed in previous chapters, quantum communication and quantum computation protocols usually encode the information in two-dimensional quantum systems, better known as qubits. Nevertheless, there are ways of enlarging the available dimension of the quantum information carrier. A system that is completely described by n different orthogonal vectors is called a qunit. In the same way as in their classical counterpart, the use of qunits increases the information rate, but surprisingly enough the system is also more resistant to noise. For example, entangled qunits can violate Bell's inequalities more than their two-dimensional counterpart, protecting in this way the nonlocal quantum correlations against noise. Also, a quantum cryptography protocol using qunits is usually more secure against noise than those protocols based on qubits [46,47,48]. On the other hand, there are a series of protocols in quantum communication that are designed specifically for being implemented in higher dimensional spaces [49,50,51]. On a more fundamental level, higher dimensional Hilbert spaces provide novel counterintuitive examples of the relationship between quantum information and classical information, which cannot be found in two-dimensional systems [52,53,54].

Encoding qunits with photons has been experimentally demonstrated using interferometric techniques such as time-bin schemes [55] and superpositions of spatial modes [56]. Up to now, the only noninterferometric technique of encoding qunits in photons is using their orbital angular momentum or, equivalently, their transversal modes [57,58]. Orbital angular momentum modes usually contain dark spots that regularly exhibit phase singularities.

The orbital angular momentum of light has already been used to entangle and to concentrate entanglement of two photons [57,59]. This entanglement has also been shown to violate a two particle three-dimensional Bell inequality [60]. There have been proposals of some experimental techniques to engineer entangled qunits in photons [58,61,62]. Here we will discuss a general scheme for a quantum communication protocol based on the orbital angular momentum of light [63]. This scheme has already been succesfully used for the experimental realization of a quantum coin tossing protocol [64].

In a general communication scheme, prior to the sharing of information, the two parties, say Alice and Bob, have to define a procedure that will assure that the signal sent by one party is properly received by the other. Usually, this scheme works as follows. First, Alice prepares a signal state she wants to send. Bob will measure it and communicate the result to Alice, who will correct the parameters of her sending device following Bob's indications. This process will be repeated until the two parties adjust the corresponding devices. After this step is completed, Alice can safely assume that any subsequent signal which is sent is properly received by Bob.

Using pairs of photons entangled in orbital angular momentum, we can prepare any qutrit state, transmit it, and measure it. The preparation is done by projecting one of the two photons onto some desired state. This projects the second photon nonlocally onto a corresponding state. This state may be transmitted to Bob and finally measured by him. The measurement employs tomographic reconstruction. This last step is usually a technically demanding problem, inasmuch as it needs the implementation and control of arbitrary transformations in the quantum system's Hilbert space.

The experimental setup we used is shown in Figure 3.7. A 351 nm wavelength argon-ion laser pumps a 1.5-mm-thick BBO (β-barium-borate) crystal cut for Type I phase matching conditions. The crystal is positioned so as to produce down-converted pairs of equally polarized photons at a wavelength of 702 nm emitted at an angle of 4° off the pump direction. These photons are directly entangled in the orbital angular momentum degree of freedom. Alice can manipulate one of the down-converted photons while the other is sent to Bob. Before being detected, Bob's photon traverses two sets of holograms.

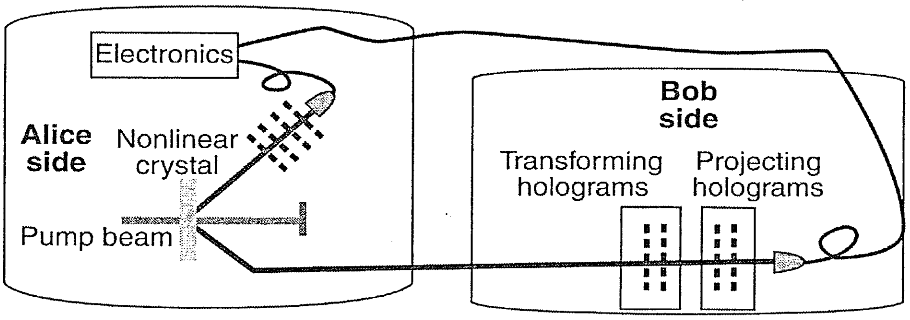

Figure 3.7 Experimental setup from [63]. A 351 nm wavelength laser pumps a BBO crystal. The two generated 702 nm down-converted photons are sent to Alice's and Bob's detectors, respectively. Before being detected, each photon propagates through a set of holograms. Each photon was coupled into single-mode fibers and directed to detectors based on avalanche photodiodes operating in the photon counting regime.

Each set consists of one hologram with charge $m = 1$ and another with charge $m = -1$. The first set of holograms provides the means of a transformation in the three-dimensional space expanded by the states $|-1\rangle$, $|0\rangle$, and $|1\rangle$. The second set, together with a single-mode fiber and a detector, acts as a projector onto the three different basis states. All these elements are Bob's receiving device. Alice's photon also traverses a set of holograms, which, together with the source and the detector on Alice's side, act as Alice's sending device. Whenever Alice detects one photon, the transmission of a photon to Bob is initiated. Due to the quantum correlations between the entangled photons, Alice can radically control the state of the photon sent to Bob. In order to adjust their respective devices properly, Bob has to perform a tomographic measurement of the received state and classically to communicate his result to Alice.

In Figure 3.8 we present three examples of qutrits that were received by Bob and remotely prepared by Alice. All of them were found to be very nearly pure states, their largest eigenvalues and corresponding eigenvectors being (a) $\lambda_{max} = 0.99$, $|e_{max}\rangle = 0.68|0\rangle + 0.71|1\rangle - 0.14|-1\rangle$; (b) $\lambda_{max} = 0.99$, $|e_{max}\rangle = 0.65|0\rangle + 0.53\exp(-i0.26\pi)|1\rangle + 0.55\exp(-i0.6\pi)|-1\rangle$; (c) $\lambda_{max} = 0.99$, $|e_{max}\rangle = 0.58|0\rangle + 0.58\exp(-i0.05\pi)|1\rangle + 0.58\exp(-i0.89\pi)|-1\rangle$. From these examples it is shown that besides the relative intensities, Alice could also control the relative phases of the states sent. Other reconstructed qutrits (not presented in Figure 3.8) showed an effective suppression of the $|0\rangle$ mode through destructive interference from the two holograms. The result was $\lambda_{max} = 0.97$, $|e_{max}\rangle = 0.26|0\rangle + 0.68\exp(i0.11\pi)|1\rangle + 0.68\exp(-i0.21\pi)|-1\rangle$. As can be deduced from the maximum eigenvalue of all the data, the purity of the reconstructed states was larger than 97%. By direct comparison of the measured data and the data estimated by the reconstructed matrix, the error was comparable to the statistical Poissonian noise, which demonstrates the reliability of the tomography.

The method presented establishes a point-to-point communication protocol in a three-dimensional alphabet. Using the orbital angular momentum of photons, we can implement the three basic tasks inherent in any communication or computing protocol: preparation, transmission, and reconstruction of a qutrit. This communication scheme has already been experimentally implemented in a quantum coin tossing experiment [64], which is an original cryptographic protocol using qutrits.

3.2.5 Entanglement-Based Quantum Cryptography

Quantum cryptography is the first technology in the area of quantum information that is in the process of making the transition from purely fundamental scientific research to an industrial application. In the last three years, several companies have started developing quantum cryptography prototypes, and the first products have hit the market. Up to now, these commercial products were all based on various faint-pulse implementations of the BB84 protocol [5,65,66].

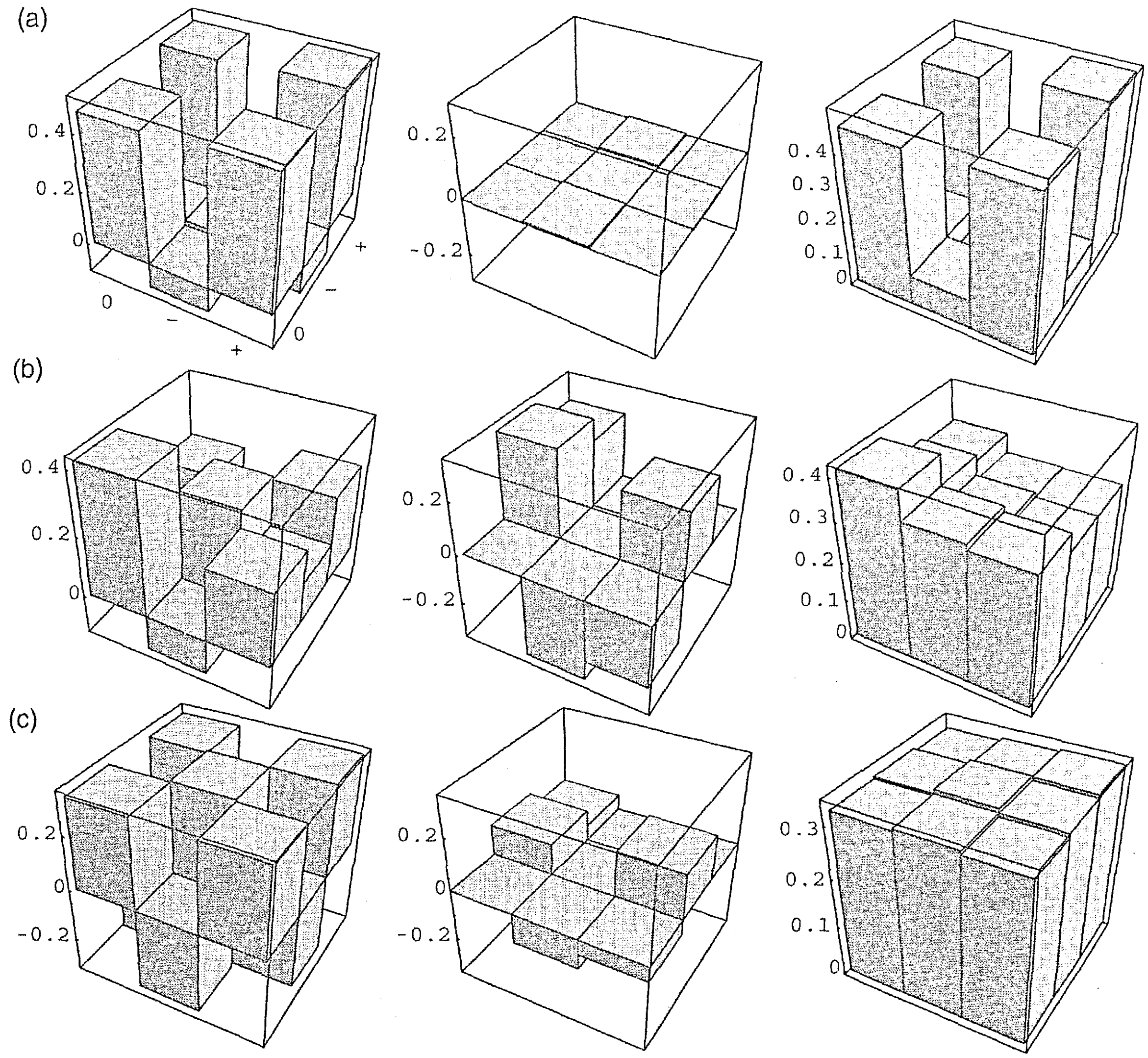

Figure 3.8 Results of quantum state tomography applied to three different remotely prepared states of Bob's qutrits: (a) $0.68|0\rangle + 0.71|1\rangle - 0.14|-1\rangle$; (b) $0.65|0\rangle + 0.53\exp(-i0.26\pi)|1\rangle + 0.55\exp(-i0.6\pi)|-1\rangle$; (c) $0.58|0\rangle + 0.58\exp(-i0.05\pi)|1\rangle + 0.58\exp(-i0.89\pi)|-1\rangle$. Left and middle panels show real and imaginary parts of the reconstructed density matrices; right panels show the absolute values of those elements for better comparison of how large are the contributions of the three basic states. From the results it is shown that Alice can control both the relative amplitudes and the phases of the sent states.

The use of entanglement provides a superior approach to quantum cryptography and was first proposed by Ekert [67]. One of the main conceptional advantages over single-photon quantum cryptography is the inherent randomness in the results of a quantum-mechanical measurement on an entangled system leading to purely random keys. Furthermore, the use of entangled pairs eliminates the need for a deterministic single photon source, because a pure entangled photon state consists, by definition, of exactly two photons that are sent to different recipients. Multiple-pair emissions are inherently rejected by the protocol, in contrast to the faint-pulse case, where a beam-splitting attack might be successful.* Additionally, high-intensity sources would allow longer transmission paths compared to single-photon based systems [69,70]. Another important advantage over single-photon systems is that the photon pair source is immune to tampering by an illegitimate party. Any manipulation at the photon source can be detected by the communicating parties and communication can be stopped.

3.2.5.1 *Adopted BB84 Scheme*

A very elegant implementation of the BB84 scheme utilizes polarization-entangled photon pairs instead of the polarized single photons originally used. This is very similar to the Ekert scheme [67] when Alice and Bob chose different settings of their analyzers for their measurements of the entangled photons. As opposed to the Ekert scheme, in which both Alice and Bob randomly vary their analyzers between three settings, the adopted BB84 scheme uses only two analyzer states, namely 0° and 45°. If they share, for example, the entangled Bell singlet state $|\Psi^-\rangle$, Alice's and Bob's polarization measurements will always give perfect anticorrelations if they measure with the same settings, *no matter whether the analyzers are both at* 0° or at 45°. A way to view this is to assume that Alice's measurement on her particle of the entangled pair projects the photon traveling to Bob onto the orthogonal state of the one observed by Alice. So the photons transmitted to Bob are polarized in one of the four polarizations 0°, 45°, 90° and 135°, as with the BB84 scheme.

After a measurement run, when Alice and Bob independently collect photons for a certain time, they communicate over an open classical channel. By comparing a list of all detection times of photons registered by Alice and Bob, they find out which detection events correspond to entangled photon pairs. From these events they extract those cases in which they both had used the same basis setting of the analyzers. Owing to the perfect anticorrelations in these cases, Alice and Bob can build a string of bits (the sifted key) by assigning a "0" to the $+1$ results and a "1" to the -1 result of the individual polarization measurements. In order to obtain identical sets of a random bit sequence, one of them finally has to invert the bits.

3.2.5.2 *An Entanglement-Based Quantum Cryptography Prototype System*

We have recently developed a quantum cryptography prototype system in cooperation with the Austrian Research Centers Seibersdorf (ARCS). It was

*This is due to the nonvanishing probability of producing more than two photons per faint pulse. One possible attack on the security would then simply involve a beamsplitter, which distributes one photon of a pulse to Eve and one to Bob. This would allow Eve to gain sufficient information to reconstruct the distributed key. True single-photon sources are needed to overcome this sufficiency [68].

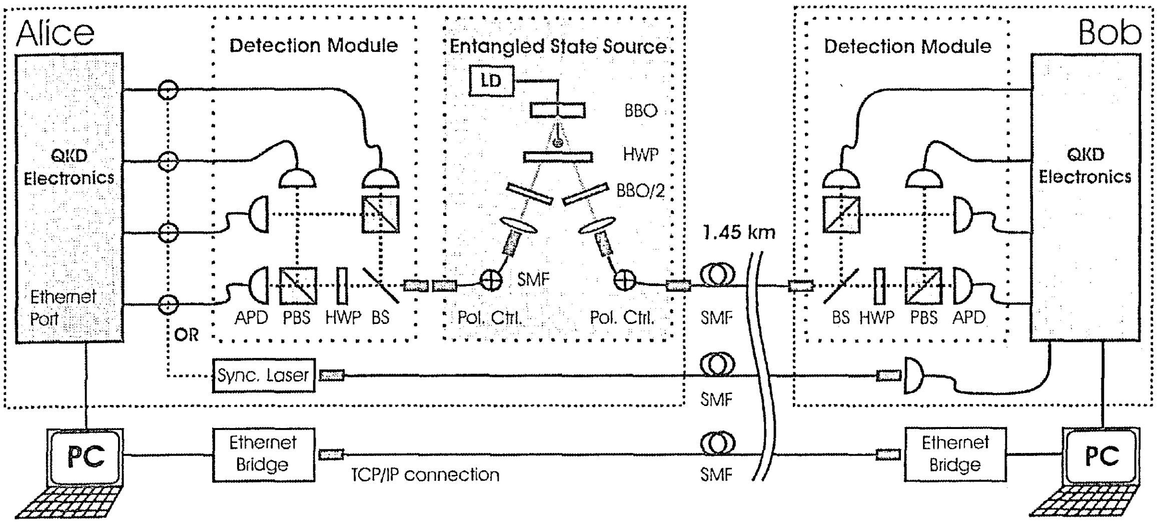

Figure 3.9 Sketch of the experimental setup from [71]. Our entangled state source produces polarization-entangled photon pairs. One of the photons is locally analyzed in Alice's detection module, while the other is sent over a 1.45 km long single-mode optical fiber (SMF) to the remote site (Bob). Polarization measurement is done in one of two bases (0° and 45°) by using a beam splitter (BS) that randomly sends incident photons to one of two polarizing beamsplitters (PBS). One of the PBS is defined for measurement in the 0 basis, and the other in the 45 basis as the half-wave plate (HWP) rotates the polarization by 45°. 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 APDs, an optical trigger pulse is created (sync. laser) and sent over a second fiber to Bob to establish a common time basis. At both sites, this trigger pulses and the detection events from the APDs are fed into a dedicated quantum key generation (QKG) device for further processing.

applied in a real-world scenario in April 2004. This was the first time that a quantum cryptography system was used for the encryption of an Internet bank transfer [71]. The system was installed at the headquarters of a large bank (Alice) and at the Vienna City Hall (Bob), and a key was distributed over the 1.45 km optical single-mode fiber connecting the parties.

The quantum cryptography system (Figure 3.9) consists of a portable source for polarization-entangled photons (Figure 3.10) and two sets of fourfold single-photon detection modules with integrated polarization analyzers and embedded hardware devices that are capable of handling the complete software protocol needed to extract a secure and private key out of raw detection events. The quantum channel between Alice and Bob consisted of an optical fiber that has been installed between the two experimental sites in the Vienna sewage system. The classical protocol in that experiment is performed via a standard TCP/IP connection. The exposure of the fibers to realistic environmental conditions, such as stress and strain during installation as well as temperature changes, was an important feature of this experiment; the successful operation of the system shows that laboratory conditions are not necessary for its operation.

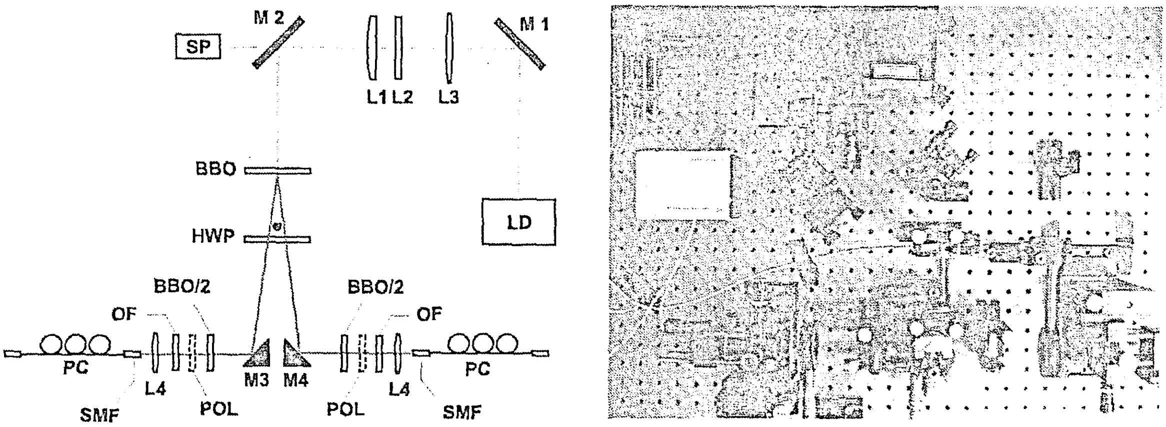

Figure 3.10 Sketch of the experimental implementation. The beam of a laser diode (LD) is focused by a telescope (lenses L1, L2, and L3) onto the nonlinear crystal (BBO). The photon pairs created by SPDC leave the crystal with an opening angle of 6°, passing a half-wave plate (HWP); the polarization of the photons is flipped before they pass the two compensation crystals (BBO/2). Before they are coupled into a single-mode optical fiber (SMF) by the coupling lens L4, they pass an optional polarizer (POL) and an orange glass filter (OF) that blocks scattered UV light. To compensate for arbitrary polarization rotation within the fiber, a polarization control module (PC) is connected to the end of the SMF.

3.2.5.2.1 The Photon Source. The entangled-photon source has been inspired by the design of several previous experiments [72,73] (see Figure 3.10). There, the entangled photons are created by spontaneous parametric down-conversion in a nonlinear crystal. In our setup, a continuous wave (CW) violet GaN laser diode was used to pump a nonlinear β-barium borate (BBO) crystal with 18.6 mW optical power at 405 nm. To achieve a narrow line width, the laser diode was mounted in Littrow configuration.

The pump beam was focused to a round waist of approximately 100 μm at the BBO crystal using a telescope lens system. Three lenses form an imaging system in which an achromatic lens creates a distortion-free elliptical focus that could then be imaged, astigmatically corrected, into the crystal. The Rayleigh range of the pump beam is much longer than the length of the BBO crystal used (4 mm long). We used a half-wave plate and a 2 mm long BBO crystal for compensating for the transversal and longitudinal walkoff effects [72] (see Figure 3.10). We assumed a gaussian distribution of angles and rotational symmetry around the intersection lines for the emission of entangled photons [73]. The collection efficiency was optimized by matching the emission modes of the entangled photons with the modes accepted by the fiber coupler.

The setup is aligned to produce the maximally entangled Bell singlet state

$$|\psi^-\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|V\rangle_2 - |V\rangle_1|H\rangle_2\right). \tag{3.2}$$

To characterize realistically the quality of our source without completely reconstructing the density matrix, we make an assumption on the noise present in our produced output state. Assuming random (white) noise, our produced state becomes

$$\rho_{12} = v|\psi^-\rangle\langle\psi^-|_{12} + \frac{(1-v)}{4}\mathcal{I}_{12}. \tag{3.3}$$

In this model, the quality of our source is entirely described by the two-photon visibility v and the pair production rate per second. The overall number of detected photon pairs was approximately 25,000 pairs per second, and the average visibility was better than $v = 0.95$.

3.2.5.2.2 QKD Electronics. The prototype of the dedicated quantum key distribution (QKD) hardware currently under development consists of three main computational components: acquisition of the raw key, generation of synchronization pulses, and QKD protocol tasks. All three units are situated on a single printed circuit board. The developed detection logic is implemented in a FPGA and runs at a sampling frequency of 800 MHz, while employing a time window of 10 ns for matching the detection events and synchronization signals.

The board handles the synchronization channel and generates a strong laser pulse whenever a photon counting event is detected at Alice's site. This is ensured by a logical OR connection of the detector channels. The synchronization laser pulse at the wavelength of 1550 nm was sent over a separate single-mode fiber.

A full scale QKD protocol was implemented very recently including data acquisition, error estimation, error correction, implementing the algorithm CASCADE [74], privacy amplification, and a protocol authentication algorithm that ensures the integrity of the quantum channel by using a Töplitz matrix approach. Furthermore, the encryption library modules applied include one-time pad and AES encryption schemes, the latter allowing key exchange on a scale determined by the user.

3.2.5.2.3 Results. The average total quantum bit error rate (QBER) of the raw key was found to be less than 8% for more than the entire run time of the experiment. An analysis of the different contributions to the QBER showed that about 2.6% originate in imperfections of the detection modules and 1.2% are due to reduced visibility of the entangled state. The rest of the QBER was attributed to the error produced by the quantum channel. The average raw key bit rate in our system was found to be about 80 bits/s after error correction and privacy amplification. This value is mainly limited by the attenuation on the quantum channel, by the detection efficiency of the avalanche photodiodes, and by the electronics.

To conclude, polarization-entangled photon systems provide an excellent alternative for systems based on weak coherent pulses. Our results suggest that the development of a commercial entanglement based quantum cryptography system is not far away.

3.2.6 Toward a Global Quantum Communication Network

3.2.6.1 Free-Space Distribution of Quantum Entanglement

In more recent years, work has begun on extending the reach of quantum communication to longer and longer distances — after all, what good is a quantum phone if you can only call across the room? Clearly, optical photons are the ideal system for quantum communication over distances, owing to their weak interaction with the environment (i.e., long decoherence times) and high speed. The two methods for sharing photons over long distances are through optical fibers or via free-space optical links. Previously, entangled photons have been shared over long distances only in optical fiber up to 50 km [75]. Similar systems were used to perform a Bell inequality experiment that closed the locality loophole [76]. Free-space optical links provide an exciting alternative quantum channel when there is a direct line of sight between two communicating parties. They consist of at least two telescopes — a transmitter and a receiver — which are used to send light over large distances through the air. Free-space links have been used in conjunction with faint laser pulses to implement the BB84 quantum cryptography protocol up to a distance of 23.4 km [77] and even at daylight [78,79,80]. Theoretical studies have shown that quantum communication in optical fiber can be extended to approximately 100 km before attenuation overwhelms the signal [81]. Recent fiber-based experiments already reach this limit. Similar limitations are valid for optical free-space links, which suffer from attenuation in the atmosphere due to aerosols [82] and from atmospheric turbulences, which are eventually limited by the Earth's curvature. Why is this distance of some hundred kilometers not a limit in our optical networks of today? Quantum information suffers from a fragility that is not present in its classical counterpart. For example, classical optical pulses that encode 0's and 1's in an optical network can be detected and regenerated or amplified every so often in repeater stations, effectively extending the range of optical communication indefinitely. However, the polarization state of a single photon cannot be faithfully amplified — this can be seen as a consequence of the no-cloning theorem [83]. This makes the quantum analogue of repeaters much more complicated than their classical counterparts. A quantum repeater [15] is in principle possible with the use of quantum memories, entanglement purification [29,18], and entanglement swapping [84,85]. In addition, free-space optical links may be the way to increase significantly the present quantum communication distance limit: while earthbound free-space links are just as limited as fiber, they have the advantage in that they can be combined with satellites. The atmosphere is relatively thin, and most of the absorption takes place near the Earth's surface. The attenuation experienced on a clear day at the Earth's surface over approximately 4 km is roughly equivalent to that experienced vertically through the atmosphere [86]. Transmitting entangled photons from space to Earth will definitely allow us to overcome the current distance limits and bridge distances much larger than those achievable with purely ground-based laboratories.

3.2.6.1.1 Free-Space Optical Links with Entangled Photons. Our group recently demonstrated how combine free-space optical technology with entangled photon pairs. The first experiment took place over the Danube in Vienna, where we could demonstrate the distribution of entangled photon pairs over 600 m [87]. The second experiment [88] was set up over the city of Vienna and achieved a distance of approximately 8 km, which exceeds the atmospheric attenuation for satellite communication.

The schematic setup of the Danube experiment is shown in Figure 3.11. The compact, portable down-conversion source (see Section 2.5) was placed

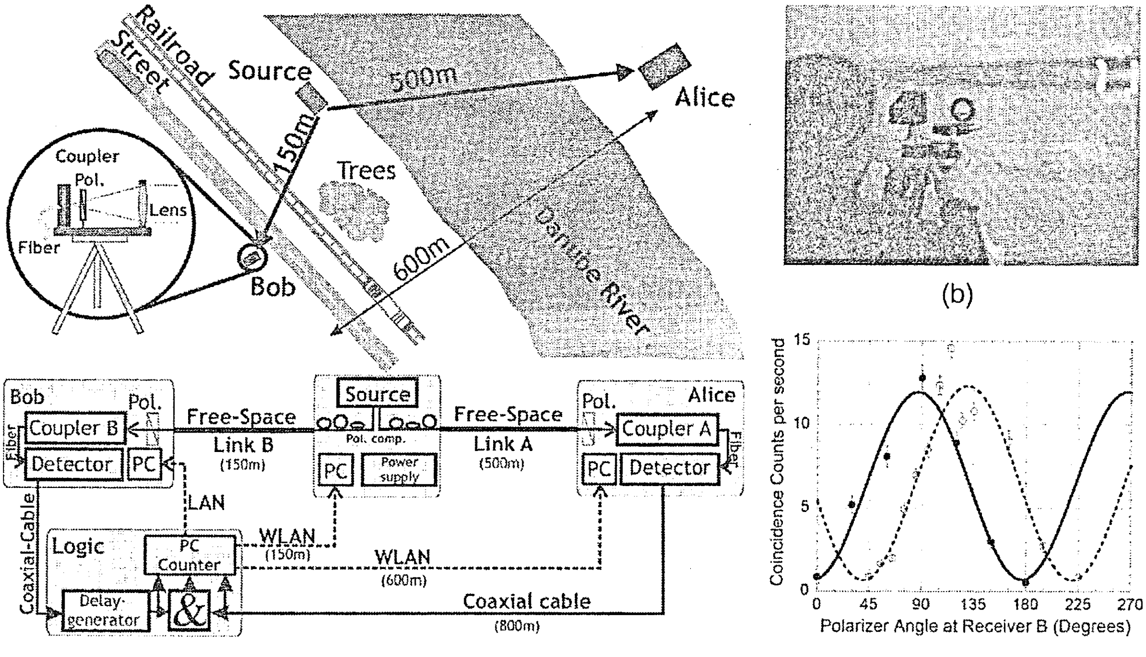

Figure 3.11 (a) Experimental schematic and communication diagram from [87]. The upper figure shows the positioning of the source and receiver stations for the experiment. The down-conversion source was positioned on the southwest bank of the Danube River. One receiver station, named Alice, was located 500 m away on a rooftop on the northeast side of the river, while the second receiver, Bob, was located on a second rooftop 150 m away across a railroad and a highway. The inset shows a schematic of the receiver telescope (the sender is the same with no polarizer). The lower figure shows how data were communicated and shared for the experiment (see text). (b) One of the transmitter telescopes during alignment. (c) Measured polarization correlations between receivers. The data show the measured coincidence rate (per second) between the two receivers as a function of the angle of the polarizer at receiver B when the polarizer at receiver A was set to 0° (solid circles, solid line) and to 45° (open circles, dotted line), respectively. The obviously noisy part in the data coincides with the passing of a freight train underneath the link to receiver B. The visibilities of the best fit curves are 88.2 ± 5.7% and 89.0 ± 3.3%.

on one bank of the Danube and stored in a shipping crate. One receiver station, Alice, was on the far bank of the Danube and located on a rooftop approximately 500 m away. The second receiver, Bob, was located about 150 m from the source location on a second rooftop. Although both receiver stations were located above ground level, the Alice link was periodically blocked by passing ships, and the Bob link, while not completely blocked, experienced extra beam fluctuations from passing freight trains on the railroad. Our diode-laser-pumped down-conversion source requires a fraction of the electrical power and none of the water cooling of an argon-ion- or titanium-sapphire-pumped system. For this experiment, all electrical power for the source was supplied from a gas-powered 2 kW generator. This demonstrates that down-conversion sources are no longer tied to the laboratory environment and can be taken virtually anywhere; they can function in real-world applications. In addition to using the diode-pumped system, we took advantage of a second recent advance in entangled photon-pair generation — high efficiency coupling of the down-conversion light into single-mode optical fiber [73]. Transmission from and collection into nighttime ambient background sources without resorting to high-loss band-pass filters. The transmitting telescopes for the experiment were simply single-mode fiber couplers and a 5-cm achromatic lens with a 150 mm focal length. The receiver telescopes were identical except for a polarizer placed in front of the coupler that could be rotated for polarization measurements. Our singles rate background level was limited to about 600–700 Hz, which was essentially due only to the dark counting rates of the detectors. The communication schematic for the experiment is shown in Figure 3.11. Alice's detection signals were sent directly to Bob via a long coaxial cable that connected the two labs. At the Bob station, a delay generator was used to account for the extra propagation time of the Alice signal and synchronize the coincident pulses, which were measured using standard NIM electronics. While the singles rates and coincidence rates were measured only at the Bob station, the results were distributed via local area network (LAN) connections to the Bob rooftop and Wave-LAN to the source and Alice station. This allowed for remote polarization compensation, telescope adjustments, and data accumulation using only a single measurement configuration. The source parameters have already been described in detail in Section 3.2.5. In short, the polarization-entangled singlet Bell state $|\Psi^-\rangle_{12} = \frac{1}{\sqrt{2}}(|HV\rangle_{12} - |VH\rangle_{12})$ could be generated with a two-photon visibility of approximately $v = 0.95$ with singles rates and coincidence rates of approximately 120,000 Hz and 20,000 Hz, respectively, at a UV pumping power of 18 mW. The light was coupled through the optical telescope links, each of which had an attenuation of 12 dB (or about 6% transmission). This was sufficient to yield singles count rates at the receivers of about 4000 s^{-1} (including background) and a maximum coincidence rate of 15 s^{-1}.

In order to support our claim that the shared photons were entangled, we measured a set of polarization correlations designed to violate maximally a CHSH Bell inequality [89,90] for the singlet. We define a polarization correlation as

$$E(\phi_A, \phi_B) = \frac{N^{++} + N^{--} - N^{+-} - N^{-+}}{N^{++} + N^{--} + N^{+-} + N^{-+}}, \tag{3.4}$$

where N is the number of coincidence counts when the polarizer is set to the angle ϕ_A ("+") or $\phi_A^{\perp}$ ("−") at Alice and when the polarizer is set to the angle ϕ_B ("+") or $\phi_B^{\perp}$ ("−") at Bob. The CHSH Bell inequality, which holds for any local realistic description of the photon pair's polarization states, is then written as a combination of such polarization correlations for a set of angles; this inequality is

$$S = |E(\phi_A, \phi_B) - E(\phi_A, \widetilde{\phi}_B) + E(\widetilde{\phi}_A, \phi_B) + E(\widetilde{\phi}_A, \widetilde{\phi}_B)| \leq 2, \tag{3.5}$$

where S is the so-called Bell parameter and $\phi_{A(B)}$ and $\widetilde{\phi}_{A(B)}$ represent different polarization settings for Alice (Bob). For a pure singlet state, quantum mechanics predicts a maximal violation of this inequality of $S = 2\sqrt{2}$, for the set of angles $\{\phi_A, \widetilde{\phi}_A, \phi_B, \widetilde{\phi}_B\} = \{0°, 45°, 22.5°, 67.5°\}$.

The experimentally obtained polarization correlations are $E(0°, 22.5°) = -0.509 \pm 0.057$, $E(0°, 67.5°) = +0.643 \pm 0.042$, $E(45°, 22.5°) = -0.558 \pm 0.055$, and $E(45°, 67.5°) = -0.702 \pm 0.046$. Using these results, we calculate $S_{EXP} = 2.41 \pm 0.10$, which is a sufficient violation of the Bell inequality by over four standard deviations. It is also the experimental signature of shared entangled states between the two receiver stations. This work was the first demonstration of the distribution of entangled photon pairs over free-space optical links. A cryptographic system based on our setup would have shown a total raw key generation rate of a few tens of bits per second and an estimated quantum bit error rate (QBER) of 8.4%. It is interesting to note that our link attenuation of 12 dB corresponds to a value that might be achievable with state-of-the-art space technology when establishing a free-space optical link between an Earth-based receiver telescope of 100-cm diameter and a satellite-based transmitter telescope of 20-cm diameter orbiting Earth at a distance of 600 km [91]. Typical losses in an actual satellite experiment might vary, depending on the link optics and on the performance of satellite pointing and tracking [92,93].

In an extended experiment, we could significantly increase the distance between the stations. We have distributed entangled photons between an old observatory and a modern office skyscraper in Vienna, that are 7.8 km apart [88]; see Figure 3.12. The source of the entangled photons is placed at the observatory. The reason for choosing such a distance is that in a 4.5-km link along the ground, one expects the same level of attenuation from scattering with airborne particles as in going through the whole atmosphere vertically.* In order to have a reasonable signal at this distance, we have built redesigned

*The transmission of 800 nm light from the whole vertical atmosphere is about 80% under good weather conditions [94,93]. The horizontal attenuation coefficient measured in Vienna was approximately $\alpha = 0.05$ km^{-1}. The horizontal distance with the same attenuation as the whole atmosphere vertically is $L = -ln(0.8)/\alpha = 4.5$ km [82].

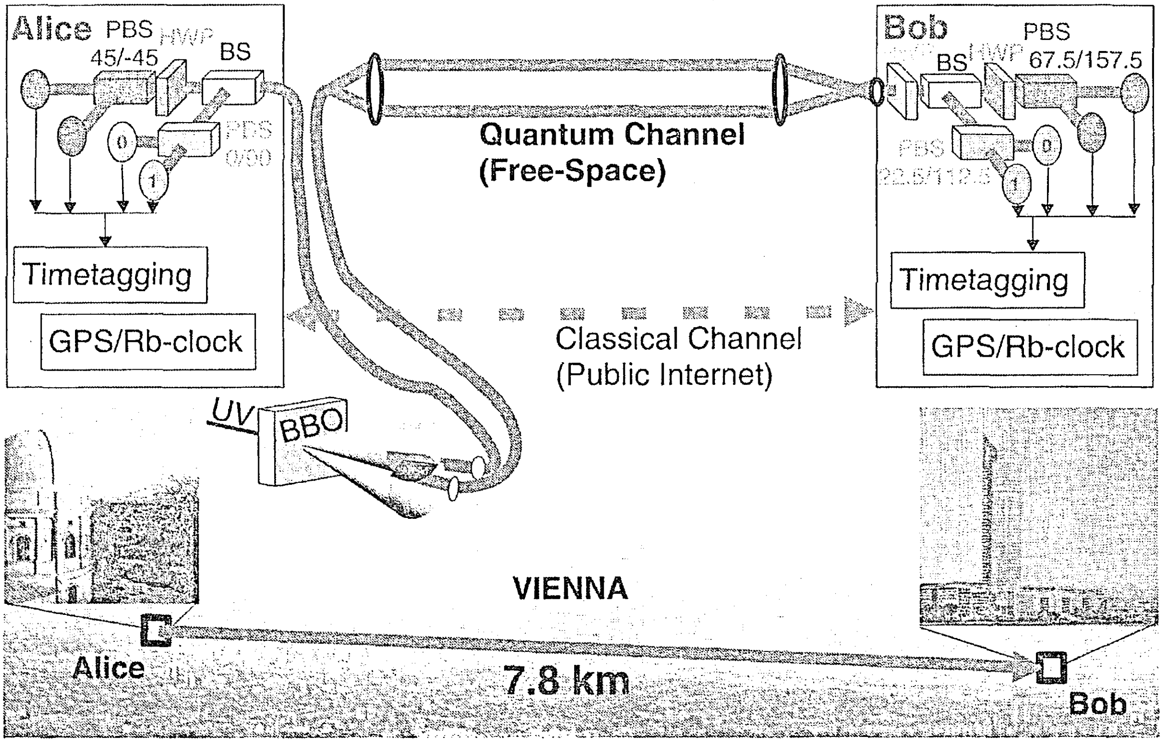

Figure 3.12 Scheme of the free-space quantum communication experiment over Vienna. The transmitter Alice, comprising the single-mode fiber coupled polarization-entangled photon source (DC) and sending telescope, is located in the 19th-century observatory Kuffner Sternwarte. Bob has a receiver telescope and is located on the 46th floor of the Millennium Tower skyscraper 7.8 km away. Alice measures the photons in mode A from each entangled pair using a four-channel detector made of a 50/50 beam splitter (BS), a half-wave plate (HWP), and polarizing beam splitters (PBS), which measures the photon polarization on either the H/V or +/− basis, where $\pm = \frac{1}{\sqrt{2}}(H \pm V)$. She sends the other photon in mode B, after polarization compensation (Pol.), via her telescope and free-space link to Bob. Bob's receiver telescope is equipped with a similar four-channel detector and can measure the polarizations in the same bases as Alice or, by rotating an extra HWP, measure another pair of complementary linear polarization bases. Alice and Bob are both equipped with time-tagging cards, which record the times at which each detection event occurs. Rubidium atomic clocks provide good relative timing stability between the local measurements. Both stations also embed a 1 pps signal from the global positioning system (GPS) into their time-tag data stream to give a well-defined zero time offset. During accumulation, Bob transmits his time tags in blocks over a public Internet channel to Alice. She finds the coincident photon pairs in real time by maximizing the cross-correlation of these time tags. Which of the four detector channels fired is also part of each time tag and allows Alice and Bob to determine the polarization correlations between their coincident pairs. Alice uses her polarization compensators to establish singlet-like anticorrelations between her measurements and Bob's.

refractor telescopes. Our new designs are based on larger and higher quality optical elements. We also relaxed our spatial filtering requirement to reduce sensitivity to beam wander and fluctuations. Using locally recorded time stamps and a public Internet channel, coincident counts from correlated photons are demonstrated to violate a Bell inequality by 14 standard deviations. This confirms the high quality of the shared entanglement and it is an encouraging step toward satellite-based distribution of quantum entanglement and future intracity quantum networks.

3.2.6.2 *Quantum Communications in Space*

Although free-space optical links are in general superior to optical fibers with respect to photon absorption, terrestrial free-space links will eventually suffer from obstruction of objects in the line of sight, from possible severe attenuation due to weather conditions and aerosols [82] from atmospheric turbulence, and from the Earth's curvature. They are thus limited to rather short distances. To exploit fully the advantages of free-space links, it will 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 and thus would allow quantum communication applications on a global scale. Such a scenario looks unrealistic at first sight, but we have recently shown that demonstrations of quantum communication protocols using satellites are already feasible today [91, 96, 101].

Based on present-day technology and assuming reasonable link parameters, one can achieve enough entangled photons per receiver pair to demonstrate several quantum communication protocols. For example, a single optical link between a satellite based transmitter terminal and an optical ground station would suffice to establish a (single-photon) quantum cryptography protocol such as BB84 and hence to generate a secure key between the satellite and the ground station. If the same terminal generates another key with another ground station (at an arbitrary distance from the first one), classical communication between the two ground stations suffices to establish a secret key between them. In other words, satellite-based single-photon links already allow quantum key distribution on a global scale. Note, however, that in this scenario the security requirements on the satellite are as high as for standard cryptography schemes. In contrast, these requirements are relaxed if one can fully exploit an entangled source that distributes pairs of entangled photons to two ground stations. For example, assuming a LEO based transmitter terminal, a simultaneous link to two separate receiving ground stations (see Figure 3.13) and a (conservatively estimated) total link attenuation of approximately 51 dB, one can expect a local count rate of approximately 2600 per second in total at each of the receiver terminals. The number of shared entangled photon pairs is then expected to be approximately 4 per second. For a link duration of 300 seconds, this accumulates to a net reception of 1200 entangled qubits. One can expect erroneous detection events on the order of 7 per 100 seconds, which yields a bit error of approximately 2%. This would already allow a quantum key distribution protocol between the two receiver stations. It is thus clear that a demonstration of basic quantum communication protocols based on quantum entanglement can already be achieved today. Furthermore, the possibility of distributing entangled particles over

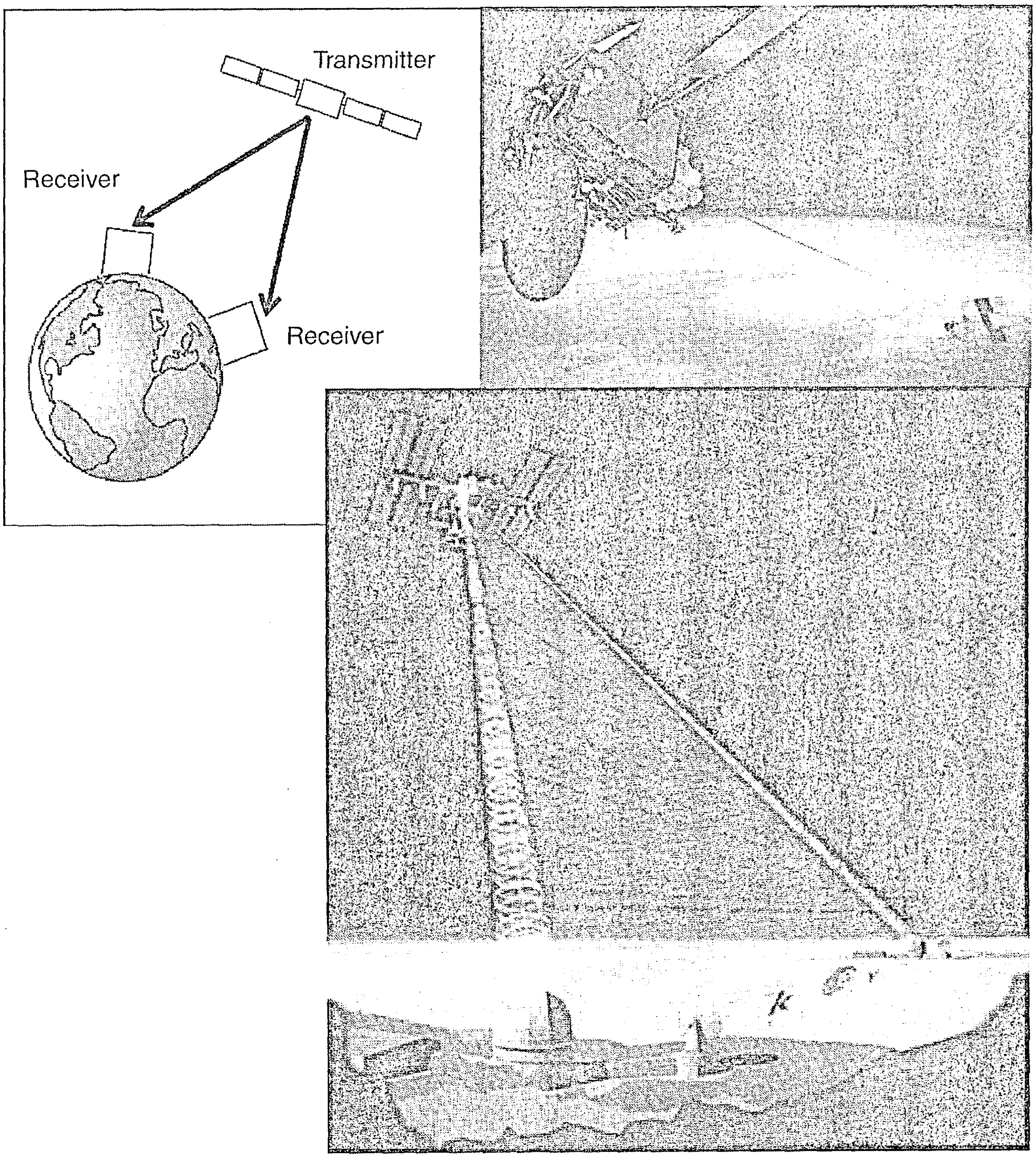

Figure 3.13 Quantum entanglement for space experiments (space-QUEST). Scheme for satellite-based distribution of entangled photons (left: schematic (from [96]); lower right: simulation for source on ISS and two specific ground stations (courtesy of ESA General Studies, Copyright ESA-Autigravite)). Laser comunication satellite terminals such as SILEX (upper right; courtesy of ESA) might provide the technology necessary to establish the optical links between satellites or between satellite and ground stations.

distances beyond the capabilities of earthbound laboratories provides novel opportunities for fundamental tests of quantum physics [95, 101].

Although one must not underestimate the demanding technological challenges associated with bringing quantum entanglement into space, the next steps are both clear and feasible. They include the development of a next generation of space-proof sources for entangled photons as well as the development of space-based and ground-based transmitter and receiver concepts for quantum communication hardware. On the space-terminal side, we have started to investigate the possibility of incorporating an entangled photon source onboard (existing) laser communication satellite terminals [96]. On the ground station side, we have performed the first proof-of-concept tests to demonstrate the feasibility of adapting existing optical ground stations for satellite-ground quantum communication [97]. It may not be too long until the first space-based quantum communication experiment with entangled photons will take off.

3.3 Conclusion and Outlook

Quantum communication has come the long way from purely fundamental considerations on the nature of quantum physics to the implementation of novel concepts and technologies of information processing. Somewhat as a surprise, the role of quantum entanglement has also become more and more important for the applications. It is now a relevant resource for most advanced quantum communication schemes and even for novel quantum computing architectures such as the one-way quantum computer [98,99]. Main future experimental challenges in the field of quantum communication and quantum computation certainly include the development of more reliable and more efficient sources for entanglement. For example, space-based experiments will require a compact, robust, and efficient source for entangled pairs, while quantum computing schemes and multiparty quantum communication schemes will benefit from high-fidelity sources of multiparticle entangled states. Also, improving the interface between photonic qubits and stationary systems such as atoms or solids will eventually allow the realization of quantum memories, which are the major building blocks in any quantum communication network.

We have presented a collection of recent advances in the field of entanglement-based quantum communication. It is fascinating to observe how the last years have paved the way for key quantum technologies such as a quantum repeater and even the realization of a satellite-based global quantum communication network. The quantum physics community is about to reach a stage in which the developed concepts and techniques of quantum communication, which started from curiosity about fundamental aspects of the nature of quantum physics, will evolve into technologies and commercial products on an industrial level. Quantum cryptography has already reached this stage. We are confident that other technologies will soon follow.

Acknowledgments

We acknowledge discussions and collaborations with our scientific colleagues and friends. Our work was supported by the Austrian Science Foundation under Project SFB1506; the European Commission under projects IST-QuComm, RamboQ and SECOQC; the Austrian Research Center Seibersdorf; the

Austrian and European Space Agencies ASA and ESA; and the city of Vienna. We also acknowledge support from Wien Kanal AG, the Austrian BA-CA Bank, Energie AG Oberosterreich, Stumpf AG, Wienerberger AG, the Alexander von Humboldt Foundation (M.A.), the NSERC (K.R.), and the Marie-Curie Program of the EC (G.M.-T.).

References

1. D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer-Verlag, Berlin, 2000.
2. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, U.K., 2000.
3. E. Schrödinger, Die gegenwärtige Situation in der Quantenmechanik, *Naturwissenschaften*, 23, 807–812; 823–828; 844–849, 1935.
4. C.H. Bennett and G. Brassard, Quantum cryptography: public key distribution and coin-tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, pp. 175–179.
5. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *J. Crypt.*, 5, 3–28, 1992.
6. C.H. Bennett, G. Brassard, and N.D. Mermin, Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.*, 68, 557–559, 1992.
7. K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, Dense coding in experimental quantum communication, *Phys. Rev. Lett.*, 76(25), 4656–4659, 1996.
8. C.H. Bennett, G. Brassard, C. Crépeau, 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.
9. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Experimental quantum teleportation, *Nature*, 390, 575, 1997.
10. N.A. Peters, J.B. Altepeter, D. Branning, E.R. Jeffrey, T.-C. Wei, and P.G. Kwiat, Maximally entangled mixed states: creation and concentration, *Phys. Rev. Lett.*, 92, 133601, 2004.
11. P. Walther, J.-W. Pan, M. Aspelmeyer, R. Ursin, S. Gasparoni, and A. Zeilinger, De Broglie wave of a nonlocal 4-photon, *Nature*, 429, 158–161, 2004.
12. C.H. Bennett, G. Brassard, C. Crépeau, 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.
13. D. Gottesman and I.L. Chuang, Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations, *Nature*, 402, 390–393, 1999.
14. E. Knill, R. Laflamme, and G. Milburn, A scheme for efficient quantum computation with linear optics, *Nature*, 409, 46–52, 2000.
15. H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Quantum repeaters: the role of imperfect local operations in quantum communication, *Phys. Rev. Lett.*, 81, 5932–5935, 1998.
16. T. Jennewein, G. Weihs, J.-W. Pan, and A. Zeilinger, Experimental nonlocality proof of quantum teleportation and entanglement swapping, *Phys. Rev. Lett.*, 88, 17903, 2002.

17. M. Żukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, "Event-ready-detectors." Bell experiment via entanglement swapping, *Phys. Rev. Lett.*, 71(26), 4287–4290, 1993.
18. J.-W. Pan, S. Gasparoni, M. Aspelmeyer, T. Jennewein, and A. Zeilinger, Freely propagating teleported qubits, *Nature*, 421, 721, 2003.
19. A. Furusawa, J.L. Sorensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, and E.S. Polzik, Unconditional quantum teleportation, *Science*, 282, 706–709, 1998.
20. M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri, and D.J. Wineland, Quantum teleportation with atomic qubits, *Nature*, 429, 737–739, 2004.
21. M. Riebe, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G. P. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, Quantum teleportation with atoms, *Nature*, 429, 734–737, 2004.
22. S. Bose, V. Vedral, and P.L. Knight, Multiparticle generalization of entanglement swapping, *Phys. Rev. A*, 57, 822–829, 1998.
23. R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, Quantum teleportation across the Danube, *Nature*, 430, 849, 2004.
24. N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Bell measurements for teleportation, *Phys. Rev. A*, 59, 3295–3300, 1999.
25. M. Michler, K. Mattle, H. Weinfurter, and A. Zeilinger, Interferometric Bell-state analysis, *Phys. Rev. A*, 53, R1209–R1212, 1996.
26. S. Popescu, Bell's inequalities and density matrices, revealing "hidden" nonlocality, *Phys. Rev. Lett.*, 74, 2619–2622, 1995.
27. C.H. van der Wal, M.D. Eisaman, A. Andre, R.L. Walsworth, D.F. Phillips, A.S. Zibrov, and M.D. Lukin, Atomic memory for correlated photon states, *Science*, 301, 196, 2003.
28. A, Kuzmich, W.P. Bowen, A.D. Boozer, A. Boca, C.W. Chou, L.-M. Duan, and J.H. Kimble, Generation of nonclassical photon pairs for scalable quantum communication with atomic ensembles, *Nature*, 423, 731, 2003.
29. C.H. Bennett, C.A. Fuchs, and J.A. Smolin, Entanglement-enhanced classical communication on a noisy quantum channel, in *Proc. 3d Int. Conf. on Quantum Communication and Measurement*, C.M. Caves, O. Hirota, and A.S. Holevo, eds., Plenum, New York, 1997.
30. J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, Experimental entanglement purification, *Nature*, 423, 417–422, 2003.
31. J.-W. Pan, C. Simon, C. Brukner, and A. Zeilinger, Entanglement purification for quantum communication, *Nature*, 410, 1067, 2001.
32. P.W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A*, 52, R2493–R2496, 1995.
33. A. Steane, Multiple particle interference and quantum error correction, *Proc. R. Soc. Lond. A*, 452, 2551, 1995.
34. E. Knill and R. Laflamme, A theory of quantum error correcting codes, *Phys. Rev. A*, 55, 500, 1997.
35. A. Steane, The ion trap quantum information processor, *Appl. Phys. B*, 64, 623–642, 1997.
36. H.J. Briegel, R. Raussendorf, and A. Schenzle, Optical lattices as a playground for studying multiparticle entanglement, in *Laserphysics at the Limit*, H. Figger, D. Meschede, and C. Zimmerman, eds., Springer, Heidelberg, 2002, pp. 433–477.

37. E. Knill, R. Laflamme, and G. Milburn, A scheme for efficient quantum computation with linear optics, *Nature*, 409, 46–52, 2000.
38. T.B. Pittman, M. Fitch, B. Jacobs, and J. Franson, Experimental controlled-NOT logic gate for single photons in the coincidence basis, *Phys. Rev. A*, 68, 032316, 2003.
39. J.L. O'Brien, G.J. Pryde, A.G. White, T.C. Ralph, and D. Branning, Demonstration of an all-optical quantum controlled-NOT gate, *Nature*, 426, 264, 2003.
40. K. Sanaka, T. Jennewein, J.-W. Pan, K. Resch, and A. Zeilinger, Experimental nonlinear sign shift for linear optics quantum computation, *Phys. Rev. Lett.*, 92(1), 017902, 2004.
41. S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, Realization of a photonic controlled-NOT gate sufficient for quantum computation, *Phys. Rev. Lett.*, 93(2), 020504, 2004.
42. T.B. Pittman, B. Jacobs, and J. Franson, Demonstration of nondeterministic quantum logic operations using linear optical elements, *Phys. Rev. Lett.*, 88, 257902, 2002.
43. P.G. Kwiat, H. Weinfurter, T. Herzog, A. Zeilinger, and M. Kasevich, Experimental realization of interaction-free measurements, *Ann. N.Y. Acad. Sci.*, 755, 383–393, 1995.
44. M. Zukowski, A. Zeilinger, and H. Weinfurter, Entangling photons radiated by independent pulsed sources, *Ann. N.Y. Acad. Sci.*, 755, 91–102, 1995.
45. P. Walther and A. Zeilinger, Experimental realization of a photonic Bell-state analyzer, *quant-ph/0410244*.
46. H. Bechmann-Pasquinucci and A. Peres, Quantum cryptography with 3-state systems, *Phys. Rev. Lett.*, 85, 3313, 2000.
47. H. Bechmann-Pasquinucci and W. Tittel, Quantum cryptography using larger alphabets, *Phys. Rev. A*, 61, 62308–62313, 2000.
48. N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, *Phys. Rev. Lett.*, 88, 0127902, 2002.
49. D. Kaszlikowski, P. Gnacinski, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Violations of local realism by two entangled n-dimensional systems are stronger than for two qubits, *Phys. Rev. Lett.*, 85, 4418, 2000.
50. T. Durt, D. Kaszlikowski, and M. Zukowski, Security of quantum key distributions with entangled qudits, *Phys. Rev. A*, 64, 024101, 2001.
51. D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Bell inequalities for arbitrarily high-dimensional systems, *Phys. Rev. Lett.*, 88, 040404, 2002.
52. P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, 233, 233, 1997.
53. C.H. Bennett, D.P. DiVincenzo, T. Mor, P.W. Shor, J.A. Smolin, and B.M. Terhal, Unextendible product bases and bound entanglement, *Phys. Rev. Lett.*, 82, 5385–5388, 1999.
54. R. Jozsa and J. Schlienz, Distinguishability of states and Von Neumann entropy, *Phys. Rev. A*, 62, 012301, 2000.
55. R.T. Thew, A. Acin, H. Zbinden, and N. Gisin, Experimental realization of entangled qutrits for quantum communication, *quant-ph/0307122*.
56. M. Zukowski, A. Zeilinger, and M.A. Horne, Realizable higher-dimensional two-particle entanglements via multiport beam splitters, *Phys. Rev. A*, 55, 2564, 1997.
57. A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Entanglement of the orbital angular momentum states of photons, *Nature*, 412, 313, 2001.

58. G. Molina-Terriza, J.P. Torres, and L. Torner, Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum, *Phys. Rev. Lett.*, 88, 013601, 2002.
59. A. Vaziri, J. Pan, T. Jennewein, G. Weihs, and A. Zeilinger, Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum, *Phys. Rev. Lett.*, 91, 227902, 2003.
60. A. Vaziri, G. Weihs, and A. Zeilinger, Experimental two-photon, three-dimensional entanglement for quantum communication, *Phys. Rev. Lett.*, 89, 240401, 2002.
61. J.P. Torres, Y. Deyanova, L. Torner, and G. Molina-Terriza, Preparation of engineered two-photon entangled states for multidimensional quantum information, *Phys. Rev. A*, 67, 052313, 2003.
62. A. Vaziri, G. Weihs, and A. Zeilinger, Superpositions of the orbital angular momentum for applications in quantum experiments, *J. Opt. B*, 4, S47–S50, 2002.
63. G. Molina-Terriza, A. Vaziri, J. Rehacek, Z. Hradil, and A. Zeilinger, Triggered qutrits for quantum communication protocols, *quant-ph/0401183 (2004).*
64. G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Experimental quantum coin tossing, *Phys. Rev. Lett.*, 94, 040501, 2005.
65. C.H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computer Systems and Signal Processing*, Bangalore, 1984, p. 715.
66. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.*, 74, 145–195, 2002.
67. A.K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.*, 67(6), 661, 1991.
68. P. Grangier, B. Sanders, and J. Vuckovic, (Eds.), Focus issue: Single photons on demand, *N. J. Phys.*, Vol. 6, 2004.
69. G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.*, 85, 1330–1333, 2000.
70. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Long-distance teleportation of qubits at telecommunication wavelengths, *Nature*, 421, 509, 2003.
71. A. Poppe, A. Fedrizzi, T. Lörunser, O. Maurhardt, R. Ursin, H.R. Böhm, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger, Practical quantum key distribution with polarization entangled photons, *Optics Express*, 12, 3865–3871, 2004.
72. P.G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, New high-intensity source of polarization-entangled photons, *Phys. Rev. Lett.*, 75, 4337, 1995.
73. C. Kurtsiefer, M. Oberparleiter, and H. Weinfurter, High-efficiency entangled photon pair collection in type-II parametric fluorescence, *Phys. Rev. A*, 64, 23802, 2001.
74. G. Brassard and L. Salvail, Secret-key reconciliation by public discussion, in *EUROCRYPT*, T. Helleseth, ed., Vol. 765, Springer, New York, 1993, p. 410.
75. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legr, and N. Gisin, Distribution of time-bin entangled qubits over 50 km of optical fiber, *Phys. Rev. Lett.*, 93, 180502, 2004.
76. G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Violation of Bell's inequality under strict Einstein locality conditions, *Phys. Rev. Lett.*, 81, 5039–5043, 1998.
77. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. Gorman, P. Tapster, and J. Rarity, A step towards global key distribution, *Nature*, 419, 450, 2002.

78. W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, and C.M. Simmons, *Phys. Rev. Lett.*, 81, 3283–3286, 1998.
79. W.T. Buttler, R.J. Hughes, S.K. Lamoreaux, G.L. Morgan, J.E. Nordholt, and C.G. Peterson, Daylight quantum key distribution over 1.6 km, *Phys. Rev. Lett.*, 84, 5652–5655, 2000.
80. R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, Practical free-space quantum key distribution over 10 km in daylight and at night, *New J. Phys.*, 4, 43.1–43.14, 2002.
81. E. Waks, A. Zeevi, and Y. Yamamoto, Security of quantum key distribution with entangled photons against individual attacks, *Phys. Rev. A*, 65, 052310, 2002.
82. H. Horvath, L.A. Arboledas, F.J. Olmo, O. Jovanović, N. Gangl, W. Kaller, C. Sánchez, H. Sauerzopf, and S. Seidl, Optical characteristics of the aerosol in Spain and Austria and its effect on radiative forcing, *J. Geophys. Res.*, 107(D19), 4386, 2002.
83. W.K. Wootters and W.H. Zurek, A single quantum cannot be cloned, *Nature*, 229, 802–803, 1982.
84. M. Zukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, event-ready-detectors" Bell experiment via entanglement swapping, *Phys. Rev. Lett.*, 71, 4287–4290, 1993.
85. J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental entanglement swapping: entangling photons that never interacted," *Phys. Rev. Lett.*, 80, 3891, 1998.
86. H. Horwath, L.A. Arboledas, F. Olmo, O. Jovanovic, M. Gangl, W. Kaller, C. Sanchez, H. Sauerzopf, and S. Seidl, Optical characteristics of the aerosol in Spain and Austria and its effect on radiative forcing. *J. Geophys. Res. (Atmospheres)*, 107, No. D19, AAC 9, 2002.
87. M. Aspelmeyer, H.R. Böhm, 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*, 301, 621–623, 2003.
88. K.J. Resch, M. Lindenthal, B. Blauensteiner, H.R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, Distributing entanglement and single photons through an intra-city, free-space quantum channel, *Opt. Express*, 13, 202, 2005.
89. J.S. Bell, On the Einstein Podolsky Rosen paradox, *Physics*, 1, 195–200, 1964.
90. J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Proposed experiment to test local hidden-variable theories, *Phys. Rev. Lett.*, 23, 880, 1969.
91. M. Aspelmeyer, T. Jennewein, M. Pfenningbauer, W. Leeb, and A. Zeilinger, Long-distance quantum communication with entangled photons using satellites, *IEEE J. Selected Top. Quantum Electron.*, 9, 1541–1551, 2003.
92. R. Hughes, W. Buttler, P. Kwiat, S. Lamoreaux, G. Morgan, J. Nordholt, and C. Peterson, Free-space quantum key distribution in daylight, *J. Mod. Opt.*, 47, 549–562, 2000.
93. J.G. Rarity, P.R. Tapster, P.M. Gorman, and P. Knight, Ground to satellite secure key exchange using quantum cryptography, *New J. Phy.*, 4, 82, 2002.
94. J.E. Nordholt, R. Hughes, G.L. Morgan, C.G. Peterson, and C.C. Wipf, Present and future free-space quantum key distribution, in *Free-Space Laser Communication Technologies XIV, Proc. SPIE*, 4635. SPIE, 2002, p. 116.

95. R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, M. Pfennigbauer, W. Leeb, and A. Zeilinger, Proof-of-concept experiments for quantum physics in space, Proc. of SPIE, *Quantum Communications and Quantum Imaging*, 5161, 252–268, 2003.
96. M. Pfennigbauer, W. Leeb, G. Neckamm, M. Aspelmeyer, T. Jennewein, F. Tiefenbacher, A. Zeilinger, G. Baister, K. Kudielka, T. Dreischer, and H. Weinfurter, Accommodation of a quantum communication transceiver in an optical terminal (ACCOM), Report prepared for the European Space Agency (ESA) under ESTEC/Contract No. 17766/03/NL/PM, 2005.
97. P. Villoresi, F. Tamburini, M. Aspelmeyer, T. Jennewein, R. Ursin, C. Pernechele, G. Bianco, A. Zeilinger, and C. Barbieri, Space-to-ground quantum-communication using an optical ground station: a feasibility study, in *Quantum Communications and Quantum Imaging II*, R. Meyers and V. Shih (eds.), Proc. of SPIE, Vol. 5551, 113–120, 2004.
98. R. Raussendorf and H.J. Briegel, A one-way quantum computer, *Phys. Rev. Lett.*, 86(22), 5188–5191, 2001.
99. P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, Experimental one-way quantum computing, *Nature*, 434, 169, 2005.
100. D.M. Greenberger, M.A. Horne and A. Zeilinger, Going beyond Bell's theorem, in M. Kafatos (ed.), *Bell's theorem, quantum theory, and conceptions of the universe*, Kluwer, Dordrecht, 1989.
101. M. Aspelmeyer, T. Jennewein, H.R. Böhm, C. Brukner, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, J. Petschinka, R. Ursin, P. Walther, A. Zeilinger, M. Pfennigbauer and W. Leeb, QSpace — Quantum communications in space, Report prepared for the European Space Agency (ESA) under ESTEC/Contract No. 16358/02/NL/SFe, 2003.

Quantum Communications and Cryptography

edited by

Alexander V. Sergienko

Taylor & Francis
Taylor & Francis Group
Boca Raton London New York

A CRC title, part of the Taylor & Francis imprint, a member of the Taylor & Francis Group, the academic division of T&F Informa plc.

Published in 2006 by
CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-3684-8 (Hardcover)
International Standard Book Number-13: 978-0-8493-3684-3 (Hardcover)
Library of Congress Card Number 2005050636

Library of Congress Cataloging-in-Publication Data

Quantum communications and cryptography / Alexander V. Sergienko, editor.
p. cm.
Includes bibliographical references and index.
ISBN 0-8493-3684-8
1. Quantum communication--Security measures. 2. Cryptography. 3. Coding theory. 4. Data encryption (Computer science) I. Sergienko, Alexander V.

TK5102.94.Q36 2005
005.8--dc22 2005050636

T&F informa

Taylor & Francis Group
is the Academic Division of T&F Informa plc.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com