# Photonic entanglement as a resource in quantum computation and quantum communication

**Robert Prevedel**

*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria*

**Markus Aspelmeyer, Caslav Brukner, and Anton Zeilinger**

*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, 1090 Wien, Austria, and*
*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften,*
*Boltzmanngasse 3, 1090 Wien, Austria*

**Thomas D. Jennewein**

*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften,*
*Boltzmanngasse 3, 1090 Wien, Austria*

Received July 18, 2006; revised September 10, 2006; accepted September 19, 2006;
posted October 16, 2006 (Doc. ID 73141); published January 26, 2007

Entanglement is an essential resource in current experimental implementations for quantum information processing. We review a class of experiments exploiting *photonic* entanglement, ranging from one-way quantum computing over quantum communication complexity to long-distance quantum communication. We then propose a set of feasible experiments, that will exploit the advantages of photonic entanglement for quantum information processing. © 2007 Optical Society of America

*OCIS codes:* 200.0200, 200.3050, 270.0270.

## 1. INTRODUCTION

Quantum entanglement[1] has become an important resource for many practical tasks in quantum information processing such as quantum computing, quantum communication, or quantum metrology. From an early stage on, entanglement proved to be an essential tool for quantum physics, both in theory and experiment: Early experimental realizations of entangled photon pairs were used to demonstrate the quantum nature of polarization correlations that can occur in decay processes,[2,3] to confirm quantum predictions of radiation theory and falsify semiclassical models,[4,5] or to test Bell's theorem and exclude local realistic descriptions of the observed quantum phenomena.[6–9] It led to the development of quantum information science, partly triggered by the introduction of quantum cryptography,[10–12] which has evolved to a strongly expanding branch of science. There, entanglement is a fundamental resource, as a quantum channel in quantum communication (e.g., for quantum state teleportation[13,14] or quantum dense coding[15,16]) or as a computational resource. Quantum computing with photons has recently experienced a new boom by discovering the possibility of universal computing with linear optics and measurements alone.[17] Although it is still unclear what the minimal resource requirements for optical quantum computing are, the number of required optical elements per universal gate is constantly decreasing. Another appealing feature of photonic quantum computing is the possibility of gate times much faster than in any other physical implementation to date.

In the following, we will discuss new examples involving experiments on entangled photons that underline the importance of entanglement for quantum information processing. Section 2 starts with an introduction to photonic one-way quantum computing, a new approach that makes optimal use of entanglement as a resource. We lay out an experiment to achieve deterministic quantum computing, a unique feature of the one-way quantum computer, by introducing active corrections during the computation. Section 3 describes experimental challenges and perspectives when exploiting distributed entanglement for quantum networking tasks, in particular, long-distance quantum communication, higher-dimensional quantum cryptography, and quantum communication complexity.

## 2. TOWARD DETERMINISTIC ONE-WAY QUANTUM COMPUTING WITH ACTIVE FEEDFORWARD

Linear optical quantum computing (LOQC) is one of the promising candidates for the physical realization of quantum computers. LOQC employs photonic qubits as information carriers, which have the immense advantage of suffering negligible decoherence and providing high-speed gate operations. It was shown that linear optics and projective measurements allow for essential nonlinear interactions and eventually for scalable quantum computing.[17] This has led to a flurry of research in both theory and experiments. A recent and comprehensive overview can be found in Ref. 18. The intrinsic randomness of the projective measurements in linear optics, however, only allows for probabilistic gate operations, i.e., the gate operations are successful only in a small fraction of the time. The other times the outcomes need to be discarded. Although the gate success probability increases with additional resources (optical elements and/or ancilla photons), such schemes achieve nearly deterministic gate operations only in the asymptotic regime of infinite resources, which is experimentally infeasible.

In contrast, the one-way quantum computer model,[19,20] an exciting alternative approach in LOQC, allows the resource for the quantum computation to be prepared *off-line* prior to any logical operations. The computational resource is a highly entangled state (the so-called cluster state). Once the cluster state is prepared, the computation proceeds deterministically, i.e., *every* measurement produces a meaningful result, requiring only single-qubit measurements and feedforward of the measurement result. Feedforward is the essential feature that makes one-way quantum computing deterministic and can be seen as an active correction of errors introduced by the randomness of measurement outcomes. We will argue in the following that present state-of-the-art technology allows for a demonstration of deterministic one-way quantum computing by implementing this active feedforward technique.

A cluster state is a network of entangled qubits and represents a universal state for quantum computing. Universal means that any quantum logic operation can be carried out on a sufficiently large and appropriately structured cluster state. These states arise when individual qubits are prepared in the superposition state $|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$, where $|0\rangle$, $|1\rangle$ denote the computational basis states, and connected by applying a controlled-PHASE operation $|j\rangle|k\rangle\rightarrow(-1)^{jk}|j\rangle|k\rangle$ with $(j,k\in 0,1)$ between neighboring qubits, effectively generating entanglement. Recent experiments succeeded in creating cluster states with various methods,[21–23] including linear optical realizations of simple controlled-PHASE gates.[24–26]

Single-qubit measurements are essential in cluster state quantum computing. The shape of the cluster state and the nature of these measurements, i.e., the order of measurements and the individual measurement bases are determined by the desired algorithm. The input state $|\psi_{in}\rangle$ is always initialized as $|+\rangle$. It is important to note that the entire information of the input state is initially stored in the multiparticle correlations of the cluster, with the individual physical qubits being completely undefined and therefore not carrying any information about the input state. In this sense, namely that properties of individual subsystems are completely undefined, the cluster state is a maximally entangled state. Well-known examples include two-qubit Bell states and three-qubit GHZ states. Single-qubit measurements on the cluster process the encoded input from one qubit to another analogous to remote state preparation. In principle, two basic types of single-particle measurements suffice to operate the one-way quantum computer. Measurements in the computational basis $\{|0\rangle_j,|1\rangle_j\}$ have the effect of disentangling, i.e., removing the physical qubit $j$ from the cluster. This leaves a smaller cluster state and thus gives the ability to shape the cluster in the specific algorithm. The measurements that perform the actual quantum information processing are made on the basis $B(\alpha)=\{|\alpha_+\rangle,|\alpha_-\rangle\}$, where $|\alpha_\pm\rangle=(|0\rangle\pm e^{-i\alpha}|1\rangle)/\sqrt{2}$ with $\alpha\in[0,2\pi]$. For simplicity, we will restrict our discussion to single-qubit gate operations, i.e., measurements on linear cluster states.[21] The argument can be generalized in a straightforward manner. The choice of measurement basis determines the single-qubit rotation, $R_z(\alpha)=\exp(-i\alpha\sigma_z/2)$, followed by a Hadamard operation, $H=(\sigma_x+\sigma_z)/\sqrt{2}$, on the input state ($\sigma_x$, $\sigma_y$, $\sigma_z$, being the Pauli matrices).

$$R_z(\alpha)H|\psi_{in}\rangle \quad\Rightarrow\quad |\psi_{in}\rangle - \boxed{R_{\mathrm{z}}^{(\alpha)}} - \boxed{H} - |\psi_{out}\rangle. \tag{1}$$

The order and choices of these measurements determine the unitary gates that are implemented and therefore the algorithm that is computed. Rotations around the $z$ axis can be implemented through the identity $HR_z(\alpha)H=R_x(\alpha)$ so that two consecutive measurements on a linear three-qubit cluster can rotate the input state to any arbitrary output state on the Poincare sphere:

$$\begin{aligned} &R_z(\alpha)HR_z(\beta)H|\psi_{in}\rangle \\ &\quad = R_z(\alpha)R_x(\beta)|\psi_{in} \quad\Rightarrow\quad |\psi_{in}\rangle - \boxed{R_{\mathrm{z}}^{(\alpha)}} - \boxed{R_{\mathrm{x}}^{(\beta)}} - |\psi_{out}\rangle. \end{aligned} \tag{2}$$

Until now, we have not incorporated the actual measurement result in our analysis. Equation (1) only holds if the outcome of the measurement $s$ is as desired, say $s=0$. Due to the intrinsic randomness of the quantum measurement, it happens with equal probability that the measurement yields the unwanted result $s=1$. In that case, a well-known Pauli error ( $\sigma_x = -\boxed{X}-$) is introduced in the computation, so that the single measurement in basis $B_j(\alpha)$ rotates the qubit to

$$R_z(\beta)H\sigma_x|\psi_{in}\rangle \quad\Rightarrow\quad |\psi_{in}\rangle - \boxed{R_{\mathrm{z}}^{(\alpha)}} - \boxed{H} - \boxed{X} - |\psi_{out}\rangle. \tag{3}$$

Obviously, by adapting the measurement bases of subsequent measurements, these errors can be eliminated. In the following, let us consider the general case of a single-qubit operation by taking into account the feedforward rules. If we choose consecutive measurements in bases $B_1(\alpha)$ and $B_2(\beta)$ on physical qubits 1 and 2 of a three-qubit cluster, then we rotate the encoded input qubit $|\psi_{in}\rangle$ to the output state

$$\begin{aligned} |\psi_{out}\rangle &= \sigma_x^{s_2}HR_z((-1)^{s_1}\beta)\sigma_x^{s_1}HR_z(\alpha)|\psi_{in}\rangle \\ &= \sigma_x^{s_2}\sigma_x^{s_1}R_x((-1)^{s_1}\beta)R_z(\alpha)|\psi_{in}\rangle, \end{aligned} \tag{4}$$

which is stored on qubit 3. The measurement outcome, $s_i=\{0,1\}$, on the physical qubit $i$ determines the measurement basis for the next qubit and indicates any introduced Pauli errors that have to be compensated for. This idea can schematically be depicted as a circuit diagram, as shown in Fig. 1. Single wires represent quantum channels, while double lines denote classical communication. The ellipses in front of the measurement meters show the measurement basis. No error correction is required for the specific case where the outcomes of the first and second qubit are $s_1=s_2=0$ and hence, as expected, $|\psi_{out}\rangle=R_x(\beta)R_z(\alpha)|\psi_{in}\rangle$. However, if the outcome of the second

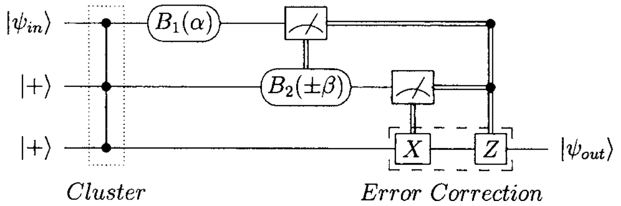

Fig. 1. Circuit diagram showing the principle idea of error correction via feed forward for one-way quantum computing.

**Table 1. Compensation for Two Pauli Errors on Qubit 3**

| Outcome Qubit 1 | Outcome Qubit 2 | Basis Adaptation | Error Correction |
|---|---|---|---|
| $s_1=0$ | $s_2=0$ | No: $B_2(\beta)$ | No |
| $s_1=0$ | $s_2=1$ | No: $B_2(\beta)$ | $\sigma_z$ |
| $s_1=1$ | $s_2=0$ | Yes: $B_2(-\beta)$ | $\sigma_x$ |
| $s_1=1$ | $s_2=1$ | Yes: $B_2(-\beta)$ | $\sigma_x\sigma_z$ |

qubit is $s_1=1$ ($s_2=0$), the measurement basis of the third qubit has to be changed from $B_2(\beta)$ to $B_2(-\beta)$ and finalized by a Pauli-error correction, i.e., $\sigma_z$ on the output qubit, to get the desired output of the computation. This yields $|\psi_{out}\rangle=\sigma_z R_x(-\beta)R_z(\alpha)|\psi_{in}\rangle$. A similar correction is required in the cases when the third qubit's outcome is $s_2=1$ ($s_1=0$) and hence $|\psi_{out}\rangle=\sigma_z R_x(\beta)R_z(\alpha)|\psi_{in}\rangle$. Finally, if an unwanted projection occurs to both qubits, ($s_1=s_2=1$), two Pauli errors, $\sigma_z$ and $\sigma_x$, have to be compensated for on qubit 3 yielding $|\psi_{out}\rangle=\sigma_x\sigma_z R_x(-\beta)R_z(\alpha)|\psi_{in}\rangle$. This is summarized in Table 1.

Experimentally, feedforward can only be achieved by recording both measurement outcomes, $s_i=\{0,1\}$. The recent photonic realization of a one-way quantum computer[21] employed single-port polarizers, which are, although sufficient to demonstrate the working principle, not suited for this purpose. Simultaneous recording of the measurement results can be achieved with polarizing beam splitters (PBSs), preceded by half- and quarter-wave plates to choose arbitrary measurement bases. The basis of the measurements can be adapted by employing fast-switching and low-loss electro-optical modulators (EOMs), which, depending on the applied voltage, change the photon's state of polarization. Analogously, error correction can be performed on the output qubit if the EOMs are aligned to apply $\sigma_x$ and $\sigma_z$ rotations, respectively.

In an experimental implementation of this scheme, the individual photonic qubits must be delayed just long enough so that the classical feedforward process can be carried out, i.e., that an individual outcome can adapt the measurement basis for the next measurement. The most rudimentary "quantum memory" that can be used for such a purpose is a single-mode fiber of a specific length, which has negligible photon loss over moderate distances. Every single feedforward process includes detection of the photon, processing of the measurement result, and finally switching of the modulator to adapt the measurement basis in real time and/or performing error correction on the output qubit. A major advantage of optical quantum computation is the unprecedented high speed of the gate operation. Various types of EOMs achieve low-loss and high contrast switching with fidelities above 99%. Switching times are well below 100 ns when combined with custom-built drivers, and such devices have successfully been implemented in early demonstrations of feedforward control.[27–29] Currently available logic boards and single-photon detectors have response times of approximately 10 and 30 ns, respectively, so that feedforward cycles of less than 150 ns seem experimentally feasible. This time scale corresponds to a single-mode fiber delay line of approximately 30 m. A gate time of 150–300 ns for one computational step is, to the best of our knowledge, approximately 3 orders of magnitude faster than the speeds achievable in other physical realizations of quantum computers such as in ion traps[30,31] or in NMR.[32]

Based on our recent successful demonstration of one-way quantum computing,[21] we have recently performed a proof-of-concept demonstration of *deterministic* quantum computing, i.e., implementation of active feedforward and error correction in real time, on a four-photon cluster state.[33] Conceptually, this presents a crucial step toward realizing scalable optical quantum computing, showing that it is indeed possible to build a deterministic quantum computer, which uses both entanglement and the intrinsically random measurement outcomes as an essential feature.

## 3. ENTANGLEMENT AS COMMUNICATION CHANNEL—QUANTUM COMMUNICATION

### A. Distributed Computing: Entanglement for Quantum Communication Complexity

Although entanglement on its own cannot be used for communication, it surprisingly can produce effects as if information had been transferred. In a communication complexity problem, separated parties performing *local* computations exchange information in order to accomplish a *globally* defined task, which is impossible to solve single-handedly.[34,35] Remarkably, if the parties share entanglement, the required information exchange in the communication complexity problem can be reduced[36] or even eliminated.[37] Such a reduction of communication complexity might be important in the future for speeding up distributed computations, e.g., within very large-scale integration circuits.

Here, we will determine the experimental requirements for quantum communication complexity protocols to outperform their classical counterparts in solving certain types of problems. This will include determination of the required minimal visibility $V$ and the detection efficiency $\eta$ for the advantage. The type of problems considered here is as follows. There are $n$ separated partners who receive local input data $x_i$ such that they know only their own data and not those of the partners. The goal is for all of them to determine the value of a function $f(x_1,\ldots,x_n)$. Before they start the protocol, they are allowed to share classically correlated random strings or quantum entanglement. If only a *restricted* amount of communication is allowed, we ask the question: What is the highest possible probability for the parties to arrive at the correct value of the function? We refer to this probability as the "success rate" of the protocol.

Recently, it has been realized that communication complexity problems are tightly linked to Bell's theorem.[6] On the basis of this insight, quantum protocols are developed that exploit entanglement between qubits,[38] qutrits,[39] and higher-dimensional states.[40] The crucial idea is that every classical protocol can be simulated by a local realistic model, and thus, its success rate is limited by the Bell-type inequalities.[38] In contrast, the success rate of quantum protocols—which make use of entangled states—can exceed these limits, since entangled states are at variance with local realism. More precisely, for every Bell inequality—even those, which are not yet known—there exists a communication complexity problem, for which a protocol assisted by states, which violate the inequality has a higher success rate than any classical protocol. Violation of Bell inequalities is thus the necessary and sufficient condition for quantum protocols to beat the classical ones.

Consider the general Bell inequality for correlation functions:

$$\sum_{x_1,\ldots,x_n=0}^{1} g(x_1,\ldots,x_n)E(x_1,\ldots,x_n) \leq B(n). \qquad (5)$$

Here $g$ is a real function, $B(n)$ is a bound imposed by local realism, and $E(x_1,\ldots,x_n)$ is the correlation function for measurements on $n$ particles, which involve, at each local measurement station $i$, two alternative dichotomic observables, parameterized here by $x_i=0$ and 1. In Ref. 38, it was shown that this Bell's inequality puts limits on the success rate in computation of certain two-valued functions $f(x_1,\ldots,x_n)$ with the inputs $x_i=0$ or 1.[41] The execution of the protocol is successful when *all* parties arrive at the correct value of $f$.

The most interesting case found is for $g=\sqrt{2^{n+1}}\cos[(\pi/2)(x_1+\cdots+x_n)]$, $n$ odd, and $B(n)=2^n$ for which the success probability of classical solutions cannot be larger than

$$P_{\text{class}}=\frac{1}{2}\left(1+\frac{1}{\sqrt{2^{n-1}}}\right), \qquad (6)$$

whereas a quantum protocol solves the problem with certainty, i.e., $P_{\text{quant}}=1$.[41] This implies that in the limit of very large $n$ one has $P_{\text{class}}\rightarrow\frac{1}{2}$ which is not better than if the partners simply agree beforehand to choose all the same (random) value for the value of the function.

Without going into the details of the protocols, we mention here that both in the classical and quantum cases, the partners give all the *same* value for their guess of the value of the function $f$. (This value is obtained as a product of $n$ locally produced values $e_i$, where $e_i$ is broadcast by party $i$. See Refs. 38 and 41 for details.) The important difference is that in a quantum protocol, this value is obtained from local results of the Bell experiment for $n$ parties, whereas in a classical protocol, it is obtained from the results of local (classical) operations assisted by classical correlations. The maximal success rate of $P_{\text{quant}}=1$ of the quantum protocol is obtained using the Greenberger–Horne–Zeilinger state $|GHZ\rangle=(|0\rangle_1\cdots|0\rangle_n+|1\rangle_1\cdots|1\rangle_n)/\sqrt{2}$.[42]

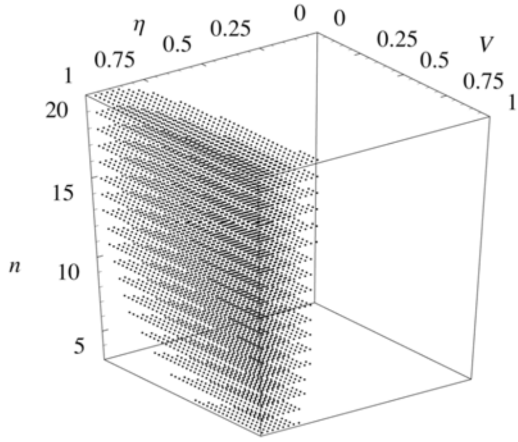

Fig. 2. Dotted volume indicates the region where the visibility $V$, detection efficiency $\eta$, and the number of partners $n$ allow for a multiparty quantum communication complexity protocol, which is more efficient than any classical one for the same task. The volume corresponds to that given by inequality (7).

For the quantum protocol to beat the best classical one, we need a success higher than $P_{\text{class}}$. We now analyze detectors with finite detection efficiency $\eta$ and nonmaximal visibility $V$ due to experimental imperfections as modeled by an admixture of white noise to the perfect state: $\rho=V|GHZ\rangle\langle GHZ|+(1-V)I/2^n$.

With a finite detector efficiency $\eta\leq 1$, the partners obtain perfect quantum correlations in $\eta^n V$ of the cases and proceed with the quantum protocol with the success rate $P_{\text{quant}}=1$. The partners must agree beforehand on a procedure for the case that their detectors fail. They are not allowed to communicate the failure, as this would consist of further bits of communication between the parties, but the allowed communication is restricted. The most effective way for a partner is to proceed with the best classical protocol in case her/his detector fails. It is assumed that there are no experimental constraints for classical protocols as they are based on manipulating and detecting classical systems (e.g., balls or pencils), which could be done with very high efficiency.

Whenever all detectors fail, which happens in $(1-\eta)^n$ of the cases, the partners will obtain the best classical success rate $P_{\text{class}}$. In the cases when some of the detectors fail and the rest fire, the partners whose detectors fail would start the best classical protocols, whereas those whose detectors fire proceed with the quantum protocol. Since the two protocols are completely independent, the success rate is not better than the probability that all partners give the same but random guess for the value of the function. In the rest of the cases, all detectors fire measuring white noise. Thus, in $1-\eta^n V-(1-\eta)^n$ of the cases, the success rate is $P_{\text{rand}}=\frac{1}{2}$.

Taking all this into account, the condition for a higher-than-classical success rate is

$$\eta^n V+(1-\eta)^n P_{\text{class}}+(1-\eta^n V-(1-\eta)^n)\tfrac{1}{2}>P_{\text{class}}. \qquad (7)$$

A similar analysis for the special case of $n=3$ and special function $f$ was given by Galvao in Ref. 43. In Fig. 2, we show the region in the parameter space of $V$, $\eta$ and $n$ that guarantees a higher-than-classical success rate. Taking $\eta = 0.8$ for the detector efficiency and visibility $V = 0.9$, one obtains $n = 4$ for the minimal number of photons in the entangled state, which is well within the scope of current technology. Recently, a quantum communication complexity protocol based on the sequential transfer of a *single* qubit[43] was experimentally implemented, and its advantage over the classical counterpart was shown in the presence of the imperfections of a state-of-the-art setup.[44] It can therefore be expected in the near future that entanglement-based quantum communication complexity protocols will become comparable to quantum key distribution, the only commercial application of quantum information science so far.

### B. Distributed Entanglement in Higher Dimension: Entangled Qutrit Quantum Cryptography

All quantum cryptography experiments performed so far were based on two-dimensional quantum systems (qubits). However, the use of higher-dimensional systems offers advantages such as an increased level of tolerance to noise at a given level of security and a higher flux of information compared to the qubit cryptography schemes.

In a recent experiment, we produced two identical keys using, for the first time to the best of our knowledge, entangled trinary quantum systems (qutrits) for quantum key distribution.[45] The advantage of qutrits over the normally used binary quantum systems is an increased coding density and a higher security margin of 22% (instead of ~15%). The qutrits are encoded into the orbital angular momentum of photons, namely, Laguerre–Gaussian modes with azimuthal index $l$ of +1, 0, or −1, respectively. The orbital angular momentum is controlled by static phase holograms. In an Ekert-type protocol, the violation of a three-dimensional Bell inequality verifies the security of the generated keys. A key is obtained with a qutrit error rate of approximately 10%. The security of this key is ascertained by the violation of the generalized Bell inequality, with $S = 2.688 \pm 0.171$. In contrast to the polarization degree of freedom, in principle, there is no limitation on the dimension of the two-photon entanglement with orbital angular momentum, and therefore, an extension of the qutrit to a more general qudit case is feasible. This opens up a new class of experiments with higher-dimensional entanglement.

Spatial light modulators (SLM) promise a fascinating new experimental approach for working with the orbital angular momentum of photons. The main idea is to use the SLM for applying computer calculated holograms to the entangled photons (see Fig. 3) instead of static phase plates. Thereby, we gain huge experimental flexibility, since we are now able to superimpose several optical elements such as lens configurations, mirrors, and phase singularity onto one active phase element, and fine-tune the holograms simply by adjusting the parameters in the calculation. This will open up possibilities of further study of three-dimensional entanglement (or more dimensions), which is an area with many unknown features. A first successful demonstration of this method is shown in Fig. 3 where we analyzed the correlation of entangled photons, while the orbital angular momentum of one of the photons is transformed via the SLM.

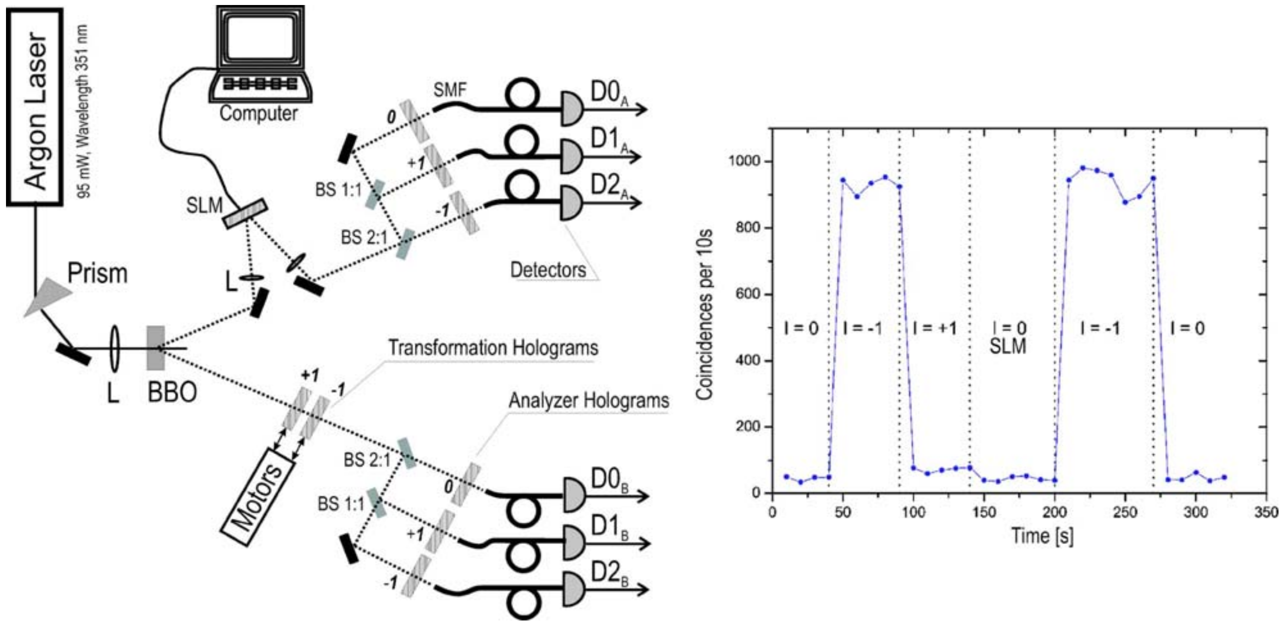

Fig. 3. (Color online) (Left) Setup demonstrating the photon manipulation by a spatial light modulator (SLM) (Ref. 46). The photon pairs produced by downconversion in a $\beta$-barium borate (BBO crystal; L, focusing lens) are entangled in their orbital angular momentum, represented by the Laguerre–Gaussian mode functions. The mode index corresponds to the orbital angular momentum of each photon. The transformation between different modes is performed by passing the photons through phase diffraction gratings containing a phase singularity, which is generated by the SLM. Analyzer holograms in different modes behind beamsplitters (BS) are used to confirm the mode index. (Right) Demonstrating the transformation of the photon by the computer-calculated hologram on the SLM. The coincidence between the detectors $D0_A$ and $D1_B$ is shown. Due to the initial correlation between the photons, there are little coincidence counts, unless the SLM performs a −1 transformation. This clearly demonstrates that we are able to manipulate the orbital angular momentum of the entangled photon by means of the computer-generated hologram.

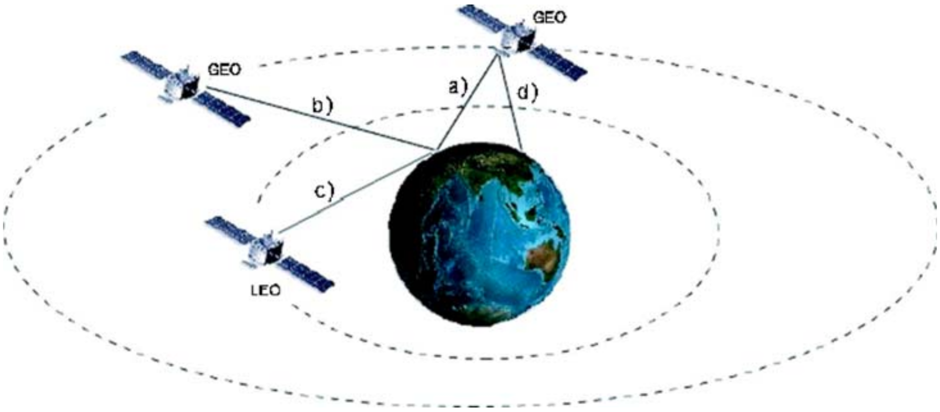

Fig. 4. (Color online) Quantum communication links realized as uplinks from ground to space. Entangled photons or single photons are generated on the ground and sent toward one or more space-based receivers. If only one receiver is available, link (a) will allow single quantum communication. If this were a geostationary Earth orbit (GEO) satellite, several ground stations could see the very same receiver, for successive quantum key exchanges [link (d)]. If a second receiver were available, e.g., also in GEO [link (b)] or in low-Earth orbit (LEO) [link (c)], also the study of fundamental aspects of quantum entanglement over large distances may be accomplished.

### C. Distributed Entanglement: Long-Distance Quantum Communication and Quantum Networking

Subsections 3.A and 3.B illustrate some of a range of unique applications that emerge when entanglement is shared between several users. Other examples include quantum cryptography,[11,12,47–49] quantum teleportation,[13,14] or quantum dense coding.[15,16] Clearly, there are important prerequisites to establishing networks of quantum communication, similar to classical communication networks. It is particularly desirable to establish entanglement between several users, with a very flexible network hierarchy. For example, two users who wish to share entangled particles might just call their network operator, who performs the necessary settings to accomplish this task. Likewise, if three users wish to share GHZ states, again the network operator performs the required operations for this task.

Fortunately, quantum physics allows us to perform these tasks, if several users initially share entangled particles with a central network operator. Utilizing the procedure known as entanglement swapping,[50,51] the generalization of quantum teleportation, the operator may simply swap the entanglement between the particles entangled with two different users, such that finally the particles of the two users get entangled. The operations that the central node (operator) must perform are projection measurements onto the desired entangled state. Since the particles originally have no relation, the projective measurement will give a random result, which must be communicated to the users, so they can use the entangled particles. Entanglement swapping can, in principle, be generalized to arbitrary quantum network sizes if the network operator performs the swapping operations (e.g., projections onto Bell states, GHZ states), depending on which users wish to communicate. This is at the heart of a quantum repeater,[52] which additionally makes use of entanglement purification[53,54] and quantum memories to faithfully transmit entanglement over arbitrary distances. Important experimental progress has been made along this line, for example, by demonstrating quantum teleportation over long distances[27] or by realizing nonclassical interference of photons from completely independent photon sources.[55]

In the future, the use of satellite-based technology could provide the means for distribution of quantum signals even on a global scale.[56–58] These schemes will involve sources for entangled photons onboard satellites, with optical receiver stations on other satellites as well as on optical Earth-based ground stations. The principles of this concept, free-space quantum communication, have been demonstrated in various experiments both for faint-pulse systems[59–62] and for entangled photons.[63–66] The current distance record has been only recently achieved in a 144 km interisland link using entangled photons.[65] These results are very promising for entanglement-based free-space quantum communication in high-density urban areas and also for optical quantum communication between ground stations and satellites, since the length of our free-space link exceeds the atmospheric equivalent.

The clear aim in this research program of extending quantum communication to space is to place an entangled photon source onboard a low earth orbit (LEO) satellite or the International Space Station (ISS) and to send the photons toward two receiving ground stations.[67] The entangled photons can thus be separated by distances up to 1500 km in a single shot, which is well above distances that are possible with a ground-based architecture. This will allow unique long-distance quantum physics experiments,[68] and it will also provide a test bed for demonstrations of quantum communication applications on a global scale.

A very interesting approach, alternative to the ISS system, is to implement quantum communication uplinks from ground to satellites (see Fig. 4). This scheme is particularly interesting, as the technical complexity of a space-based receiver is significantly simpler than for the full quantum communication transmitter.

## 4. CONCLUSION

In summary, we have introduced and reviewed some recent experimental progress in the understanding of photonic quantum entanglement as a resource for quantum information processing. We have also provided an outlook into future experiments that should be feasible with current technology and that will further highlight the distinctive role of entanglement. Besides the impressive achievements in laboratories all over the world, there remain fascinating challenges for the future ranging from the interfacing of photons to scalable and durable architectures, i.e., including quantum memories, over the faithful production and characterization of multipartite entangled states of significant particle number to the realization of a full-scale quantum repeater.

## ACKNOWLEDGMENTS

We thank J. Kofler for valuable discussions. We acknowledge financial support by the Austrian Science Fund FWF, the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST Directorate as contract 015846, the ARO-funded U.S. Army Research Office contract W911NF-05-0397 and the City of Vienna.

A. Zeilinger is the corresponding author and can be reached via e-mail at zeilinger-office@univie.ac.at.

## REFERENCES AND NOTES

1. E. Schrödinger, "Die gegenwärtige situation in der quantenmechanik," Naturwiss. **23**, 807–812; 823–828; 844–849 (1935).
2. C. S. Wu and I. Shaknov, "The angular correlation of annihilation radiation," Phys. Rev. **77**, 136–136 (1950).
3. C. A. Kocher and E. D. Commins, "Polarization correlation of photons emitted in an atomic cascade," Phys. Rev. Lett. **18**, 575–577 (1967).
4. J. F. Clauser, "Experimental limitations to the validity of semiclassical radiation theories," Phys. Rev. A **6**, 49–54 (1972).
5. J. F. Clauser, "Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect," Phys. Rev. D **9**, 853–860 (1974).
6. J. S. Bell, "On the Einstein–Podolsky–Rosen paradox," Physics (N.Y.) **1**, 195–200 (1964).
7. S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," Phys. Rev. Lett. **28**, 938–941 (1972).
8. A. Aspect, J. Dalibard, and G. Roger, "Experimental test of Bell's inequalities using time-varying analyzers," Phys. Rev. Lett. **49**, 1804–1807 (1982).
9. 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).
10. S. Wiesner, "Conjugate coding," SIGACT News **15**, 78–88 (1983).
11. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin-tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signa Processing* (IEEE, 1984), pp. 175–179.
12. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
13. 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**, 1895–1899 (1993).
14. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurte, and A. Zeilinger, "Experimental quantum teleportation," Nature **390**, 575–579 (1997).
15. C. H. Bennett and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states," Phys. Rev. Lett. **69**, 2881–2884 (1992).
16. K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," Phys. Rev. Lett. **76**, 4656–4659 (1996).
17. E. Knill, R. Laflamme, and G. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46–52 (2000).
18. P. Kok, W. Munro, K. Nemoto, T. Ralph, J. P. Dowling, and G. Milburn, "Review article: linear optical quantum computing," arxiv.org e-print archive, quant-ph/0512071, March 14, 2005, http://arxiv.org/abs/quant-ph/0512071.
19. R. Raussendorf and H. J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188–5191 (2001).
20. M. A. Nielsen, "Optical quantum computation using cluster states," Phys. Rev. Lett. **93**, 040503 (2004).
21. 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**, 169–176 (2005).
22. N. Kiesel, C. Schmid, U. Weber, G. Toth, O. Gühne, R. Ursin, and H. Weinfurter, "Experimental analysis of a four-qubit photon cluster state," Phys. Rev. Lett. **95**, 210502 (2005).
23. A.-N. Zhang, C.-Y. Lu, X.-Q. Zhou, Y.-A. Chen, Z. Zhao, T. Yang, and J.-W. Pan, "Experimental construction of optical multiqubit cluster states from Bell states," Phys. Rev. A **73**, 022330 (2006).
24. N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White, "Demonstration of a simple entangling optical gate and its use in Bell-state analysis," Phys. Rev. Lett. **95**, 210504 (2005).
25. N. Kiesel, C. Schmid, U. Weber, R. Ursin, and H. Weinfurter, "Linear optics controlled-phase gate made simple," Phys. Rev. Lett. **95**, 210505 (2005).
26. R. Okamoto, H. F. Hofmann, S. Takeuchi, and K. Sasaki, "Demonstration of an optical quantum controlled-NOT gate without path interference," Phys. Rev. Lett. **95**, 210506 (2005).
27. R. Ursin, T. Jennewein, M. Aspelmeyer, R. Kaltenbaek, M. Lindenthal, P. Walther, and A. Zeilinger, "Quantum teleportation across the Danube," Nature **430**, 849–849 (2004).
28. S. Giacomini, F. Sciarrino, E. Lombardi, and F. D. Martini, "Active teleportation of a quantum bit," Phys. Rev. A **66**, 030302(R) (2002).
29. T. B. Pittman, B. C. Jacobs, and J. D. Franson, "Demonstration of feed-forward control for linear optics quantum computation," Phys. Rev. A **66**, 052305 (2002).
30. M. Riebe, H. Häffner, C. F. Roos, W. Hänsel, J. Benhelm, G. P. T. Lancaster, T. W. Körber, C. Becher, F. Schmidt-Kaler, D. F. V. James, and R. Blatt, "Deterministic quantum teleportation with atoms," Nature **429**, 734–737 (2004).
31. 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).
32. L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance," Nature **414**, 883–887 (2001).
33. R. Prevedel, P. Walther, F. Tiefenbacher, P. Böhl, R. Kaltenbaek, T. Jennewein, and A. Zeilinger, "High-speed linear-optics quantum computing using active feed-forward," Nature (to be published).
34. A. C.-C. Yao, "Some complelxity questions related to distributed computing," in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (Association for Computing Machinery, 1979), pp. 209–213.
35. A. C.-C. Yao, "Quantum circuit complexity," in *Proceedings of the 34th Annual IEEE Symposium in Foundations of Computer Science* (IEEE, 1993), pp. 352–361.
36. R. Cleve and H. Buhrman, "Substituting quantum entanglement for communication," Phys. Rev. A **56**, 1201–1204 (1997).
37. H. Buhrman, R. Cleve, and W. van Dam, "Quantum entanglement and communication complexity," arxiv.org

e-print archive, quant-ph/9705033, May 18, 1997, http://arxiv.org/abs/quant-ph/9705033.

38. C. Brukner, M. Zukowski, J.-W. Pan, and A. Zeilinger, "Bell's equalities and quantum communication complexity," Phys. Rev. Lett. **92**, 127901 (2004).

39. C. Brukner, M. Zukowski, and A. Zeilinger, "Quantum communication complexity protocol with two entangled qutrits," Phys. Rev. Lett. **89**, 197901 (2002).

40. C. Brukner, T. Paterek, and M. Zukowski, "Quantum communication complexity protocols based on higher-dimensional entangled systems," Int. J. Quantum Inf. **1**, 519–525 (2003).

41. Strictly speaking, in communication complexity problems of Ref. 38 each party $i$ receives *two* one-bit inputs $(x_i,y_i)$, and their goal is to compute a function of the form $F(x_1,y_1,\ldots,x_n,y_n)=y_1\cdot\cdots\cdot y_n\cdot f(x_1,\ldots,x_n)$. The values of the function $f$ and the $y_i$ are ±1. Each party is allowed to broadcast only *one bit* of information (denoted as $e_i$). For the present analysis, the existence of inputs $y_i$ is not of importance and is ommitted here. See Ref. 38 for details.

42. D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going beyond Bell's theorem," in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, M. Kafatos, ed. (Kluwer, 1989), p. 69.

43. E. F. Galvao, "Feasible quantum communication complexity protocol," Phys. Rev. A **65**, 012318 (2002).

44. P. Trojek, C. Schmid, M. Bourennane, Č. Brukner, M. Zukowski, and H. Weinfurter, "Experimental quantum communication complexity," Phys. Rev. A **72**, 050305(R) (2005).

45. S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. **8**, 75 (2006).

46. M. Stütz, "Qutrit-manipulation mit aktiven Phasenhbologrammen," Master's thesis (University of Vienna, 2006).

47. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, "Quantum cryptography with entangled photons," Phys. Rev. Lett. **84**, 4729–4732 (2000).

48. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol," Phys. Rev. Lett. **84**, 4733–4736 (2000).

49. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy-time Bell states," Phys. Rev. Lett. **84**, 4737–4740 (2000).

50. M. Zukowski, A. Zeilinger, and H. Weinfurter, "Entangling photons radiated by independent pulsed sources," Ann. N.Y. Acad. Sci. **755**, 91–102 (1995).

51. T. Jennewein, G. Weihs, J.-W. Pan, and A. Zeilinger, "Experimental nonlocality proof of quantum teleportation and entanglement + swapping," Phys. Rev. Lett. **88**, 017903 (2002).

52. 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).

53. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noise channels," Phys. Rev. Lett. **76**, 722–725 (1996).

54. J.-W. Pan, S. Gasparoni, R. Ursin, G. Weihs, and A. Zeilinger, "Experimental entanglement purification," Nature **423**, 417–422 (2003).

55. R. Kaltenbaek, B. Blauensteiner, M. Zukowski, M. Aspelmeyer, and A. Zeilinger, "Experimental interference of independent photons," Phys. Rev. Lett. **96**, 240502 (2006).

56. 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**, 116–126 (2002).

57. J. G. Rarity, P. R. Tapster, P. M. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," New J. Phys. **4**, 82 (2002).

58. M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Long-distance quantum communication with entangled photons using satellites," IEEE J. Sel. Top. Quantum Electron. **9**, 1541–1551 (2003).

59. 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 (2002).

60. J. Rarity, P. Tapster, and P. Gorman, "Secure free-space key exchange to 1.9 km and beyond," J. Mod. Opt. **48**, 1887–1901 (2001).

61. B. Jacobs and J. Franson, "Quantum cryptography in free space," Opt. Lett. **21**, 1854–1856 (1996)

62. C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, and J. G. Rarity, "A step towards global key distribution," Nature **419**, 450–450 (2002).

63. M. Aspelmeyer, H. R. Böhm, T. Gyatso, T. Jennewein, R. Kaltenbae, 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).

64. K. Resch, M. Lindenthal, B. Blauensteiner, H. 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**, 202–209 (2005).

65. C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication," Phys. Rev. Lett. **94**, 150501 (2005).

66. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Free-space distribution of entanglement and single photons over 144 km," arxiv.org e-print archive, quant-ph/0607182, July 27, 2006, http://arxiv.org/abs/quant-ph/0607182.

67. 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)," Technical Rep. ESTEC/Contract 17766/03/NL/PM (European Space Agency, 2005).

68. R. Kaltenbaek, M. Aspelmeyer, T. Jennewein, C. Brukner, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger, "Proof-of-concept experiments for quantum physics in space," in *Quantum Communications and Quantum Imaging*, R. Meyers and Y. Shih, eds. (SPIE, 2003), Vol. 5161, pp. 252–268.