PERSPECTIVE • OPEN ACCESS

Light for the quantum. Entangled photons and their applications: a very personal perspective

To cite this article: Anton Zeilinger 2017 *Phys. Scr.* **92** 072501

OPEN ACCESS
IOP Publishing | Royal Swedish Academy of Sciences Physica Scripta
Phys. Scr. 92 (2017) 072501 (33pp) https://doi.org/10.1088/1402-4896/aa736d

Perspective

Light for the quantum. Entangled photons and their applications: a very personal perspective

Anton Zeilinger
Vienna Center for Quantum Science and Technology, University of Vienna & Austrian Academy of Sciences, Austria
E-mail: anton.zeilinger@univie.ac.at

Abstract
The quantum physics of light is a most fascinating field. Here I present a very personal viewpoint, focusing on my own path to quantum entanglement and then on to applications. I have been fascinated by quantum physics ever since I heard about it for the first time in school. The theory struck me immediately for two reasons: (1) its immense mathematical beauty, and (2) the unparalleled precision to which its predictions have been verified again and again. Particularly fascinating for me were the predictions of quantum mechanics for individual particles, individual quantum systems. Surprisingly, the experimental realization of many of these fundamental phenomena has led to novel ideas for applications. Starting from my early experiments with neutrons, I later became interested in quantum entanglement, initially focusing on multi-particle entanglement like GHZ states. This work opened the experimental possibility to do quantum teleportation and quantum hyper-dense coding. The latter became the first entanglement-based quantum experiment breaking a classical limitation. One of the most fascinating phenomena is entanglement swapping, the teleportation of an entangled state. This phenomenon is fundamentally interesting because it can entangle two pairs of particles which do not share any common past. Surprisingly, it also became an important ingredient in a number of applications, including quantum repeaters which will connect future quantum computers with each other. Another application is entanglement-based quantum cryptography where I present some recent long-distance experiments. Entanglement swapping has also been applied in very recent so-called loophole-free tests of Bell's theorem. Within the physics community such loophole-free experiments are perceived as providing nearly definitive proof that local realism is untenable. While, out of principle, local realism can never be excluded entirely, the 2015 achievements narrow down the remaining possibilities for local realistic explanations of the quantum phenomenon of entanglement in a significant way. These experiments may go down in the history books of science. Future experiments will address particularly the freedom-of-choice loophole using cosmic sources of randomness. Such experiments confirm that unconditionally secure quantum cryptography is possible, since quantum cryptography based on Bell's theorem can provide unconditional security. The fact that the experiments were loophole-free proves that an eavesdropper cannot avoid detection in an experiment that correctly follows the protocol. I finally discuss some recent experiments with single- and entangled-photon states in higher dimensions. Such experiments realized quantum entanglement between two photons, each with quantum numbers beyond 10 000 and also simultaneous entanglement of two photons where each carries more than 100 dimensions. Thus they offer the possibility of quantum communication with more than one bit or qubit per photon. The paper concludes discussing Einstein's contributions and viewpoints of quantum mechanics. Even if some of his positions are not supported by recent experiments, he has to be given credit for the fact that his analysis of fundamental issues gave rise to developments which led to a new information technology. Finally, I reflect on some of the lessons learned by the fact that

nature cannot be local, that objective randomness exists and about the emergence of a classical world. It is suggestive that information plays a fundamental role also in the foundations of quantum physics.

Keywords: quantum mechanics, quantum entanglement, teleportation, entanglement swapping, Greenberger–Horne–Zeilinger states, Bell tests, quantum cryptography

(Some figures may appear in colour only in the online journal)

Introduction

The International Year of Light 2015 [1] gave us the opportunity to celebrate a number of important anniversaries. Among these are the publication in 1015 of a seven-volume treatise on optics by Ibn Al-Haytham [2], the 200th anniversary of the Wave Theory of Light as proposed by Fresnel in 1815 [3] and the 150th anniversary of the Electromagnetic Theory of Light Propagation by Maxwell [4]. For quantum optics particularly relevant is the 110th anniversary of Albert Einstein's 1905 proposal of particles of light [5], the 80th anniversary of the 1935 publication of both the Einstein–Podolsky–Rosen (EPR) paper [6], opening up the issue of quantum entanglement, and Schrödinger's paper of the same year containing the Schrödinger cat paradox [7] which raises the question of the quantum–classical transition.

In the present paper, I will discuss some of these issues from a rather personal perspective, focusing on my own development and experience. This will begin with my early interest in quantum mechanics and end with some of the most recent developments. It came as a surprise to us early explorers of the then still largely uncharted quantum territory when, over the years, applications arose which none of us had expected when we set out. These new technologies are known under names like quantum communication, quantum teleportation, quantum cryptography and quantum computation. As has happened before in the history of physics, a completely new technology emerged, kindled by initial fundamental curiosity—in this case, about the nature of light.

From my fascination with quantum physics to first experiments

My interest in science was probably sparked by my father, who was a biochemist. Having thus become curious about how the world works, I was put on the track towards mathematics and physics by an exciting teacher in high school. He was able to give us the feeling that we understood the basics of relativity theory or quantum mechanics. While in hindsight, this feeling was not really justified, it was crucially motivating. Then, when I started to study physics and mathematics at the University of Vienna in 1963, there was no fixed curriculum at all. One was essentially free to choose the topics according to one's liking. Only at the end, one had to pass a rigorous examination and present a PhD thesis. This resulted in me taking not even a single hour of quantum mechanics, but I learned it all from textbooks for the final exam. Reading these textbooks, I was immediately struck by the immense mathematical beauty of quantum theory. But I got the feeling that the really fundamental questions were not addressed, a fact which just increased my curiosity.

Then, something serendipitous happened. While I was working with my PhD supervisor, Helmut Rauch, on neutron scattering investigations of magnetism, he developed a fantastic neutron interferometer together with Treimer and Bonse [8]. Since I knew about neutron polarization, I worked out what would happen if the neutron spin were utilized in an interference experiment. The resulting experiment became my first involvement in the foundations of quantum mechanics. It was the

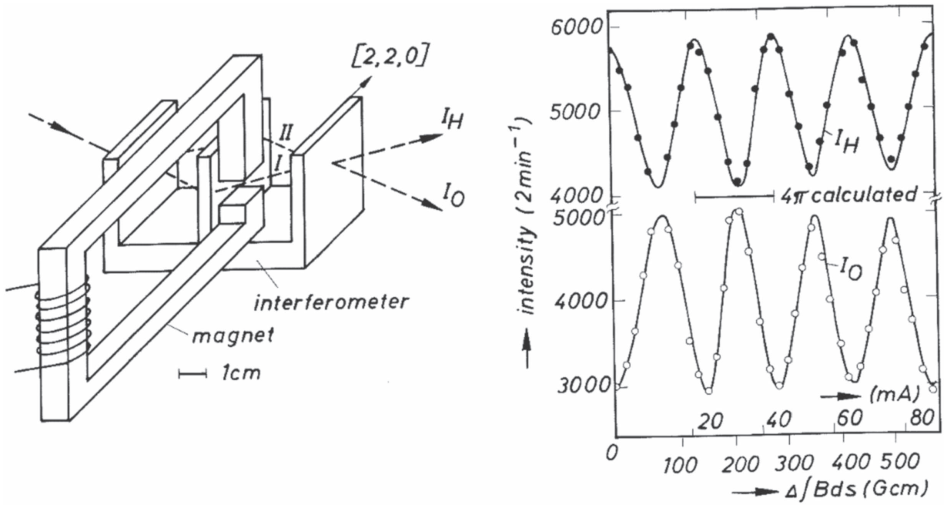

Figure 1. Rotational symmetry of a two-state system. The neutron interferometer (left), which is made out of a single piece of a dislocation-free silicon crystal, splits an incoming neutron beam into beams I and II. One of the two beams is then subjected to a varying magnetic field. The two outgoing beams thus observe intensity oscillations (right) with a period of 4π, thus confirming the fact that a spinor wave function changes sign upon one single full rotation. Reprinted from [9], Copyright (1975), with permission from Elsevier.

confirmation that a spinor wave function changes sign upon 2π rotation (figure 1) [9]. Only after a double rotation is the original state recovered. This is also the first case in my personal history of a fundamental quantum result which has found its applications today. The fact that a two-state wave function changes sign upon a full Rabi flop is central to many quantum computation schemes. I will be forever grateful to Helmut Rauch for allowing me to participate in his neutron interferometry project. From him, I also learned that it is important to trust one's own inspiration. Sometimes, one should follow one's own ideas, even if, or maybe particularly when, one does not really understand them.

The phenomenon that spinor wave functions are not symmetric under a 2π rotation, but only a 4π one, follows from the Schrödinger equation for a two-state system. In that sense, it is a mathematical phenomenon, but it also has a deeper implication because objects with an unbreakable connection to the outside resemble such a 4π symmetry as well. The 4π spin rotation just mentioned also opened up new possibilities for my career. In 1976, John Bell and Bernard d'Espagnat organized a meeting in Erice entitled 'Thinkshop in Physics'. The meeting was focused on new fundamental experiments in quantum mechanics. There, I heard for the first time about EPR correlations, Bell's inequalities and entanglement. There, I met some of the people who later became very famous in the field, as for example John Clauser, Ed Fry, Alain Aspect and Abner Shimony. Frankly, I did not really understand what was going on. But some comfort was provided in the talk given by Michael Horne, of later Clauser–Horne [10] and Clauser–Horne–Shimony–Holt [11] fame. He basically said that he also did not know what is really going on. This meeting was very important for me, because Valentin Telegdi, who also participated, opened up for me the possibility to go to MIT. There, I joined the group of Cliff Shull, who was interested in working on neutron interferometry and also later received the Nobel Prize for his development of neutron diffraction [12].

From neutron interferometry to Bell's inequalities

At MIT, I built new neutron interferometers and performed fundamental experiments which are beyond the scope of the present paper. Most importantly, I met

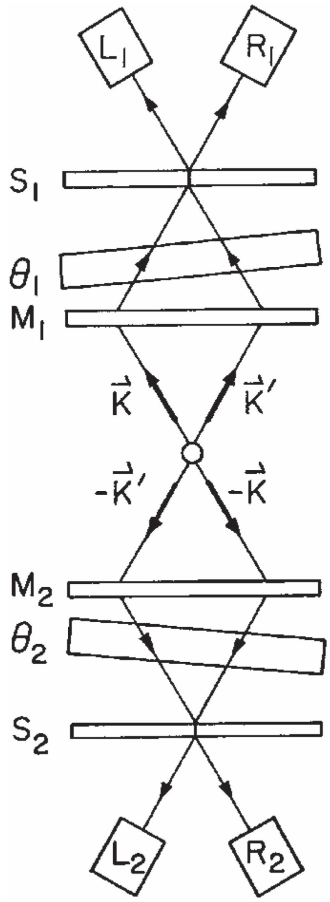

Figure 2. Two-particle interferometry. A source emits momentum-entangled pairs of particles, say photons. Each one is submitted to an interferometer. For a maximally entangled state in momentum, Einstein–Podolsky–Rosen correlations result between the detectors for the two particles. Also, upon variation of the phases θ_1 and θ_2, a violation of Bell's inequality can be observed. This idea was triggered by the announcement of the conference '50 Years of the Einstein–Podolsky–Rosen Gedankenexperiment', which took place in Joensuu, Finland, in 1985. Reused from [13] © 1985 by World Scientific Publishing Co.

Mike Horne again when I arrived, and a lifelong fruitful collaboration and friendship ensued. This close collaboration was later joined by Danny Greenberger. Slowly, I made my way into the fascinating field of entanglement. The crucial trigger was the organization of the conference '50 Years of the EPR Gedankenexperiment' in 1985 by Laurikainen in Joensuu, Finland. Mike Horne and I were interested in going there. Having worked on neutron interferometry for a long time, we were looking for a connection between interferometry and EPR correlations. That way, we developed the idea of a Bell-type EPR experiment using linear momenta, which was the first ever proposal for a violation of Bell's inequality using external variables instead of internal variables such as spin (figure 2) [13]. In a subsequent paper with Abner Shimony [14], we proposed an explicit Bell experiment with photons from down-conversion [15]. This experiment was later performed by Rarity and Tapster [16]. Today, momentum entanglement or its generalization, multi-mode entanglement, is at the basis of many experiments in quantum computation.

From entanglement of two particles to three particles, another surprise

In 1987, Daniel Greenberger visited me in Vienna as a Fulbright fellow. On the first day, we sat together and found out that both of us had been wondering what

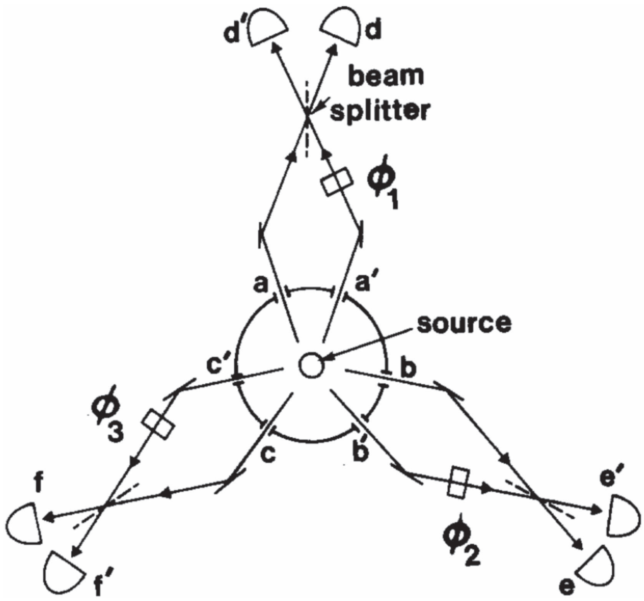

Figure 3. The three-particle GHZ interferometer. The source emits three particles, 1, 2, and 3, in six beams in a GHZ state. A phase shift ϕ_1 is imparted to beam a' of particle 1, and beams a and a' are brought together on a beam splitter before illuminating detectors d and d'. Likewise for particles 2 and 3. The contradiction between quantum mechanics and local realism arises for the perfect correlations between the detectors for the three particles. From [18] ©1990 American Association of Physics Teachers (http://aapt.scitation.org/doi/abs/10.1119/1.16243).

would happen with Bell's theorem if more than two particles were entangled with each other. Danny Greenberger did all the calculations. We also had long-distance support from Mike Horne back in Boston. I still remember how messy the results of the calculations were for our specific case: we studied one spin-zero particle decaying into two spin-one particles and each one again into two spin-one-half particles. So we decided to reduce the complexity and look at perfect correlations only. Such correlations are important for two-state systems, for example spin. There, John Bell had found for the case of just two entangled particles that the perfect correlations can be explained from a local realistic viewpoint. For two spin one-half systems, these are for example spin measurements along the same direction. Only correlations at oblique measurement angles would contradict quantum mechanics. To our surprise, we found that for three or more entangled particles, not even the perfect correlations can be explained in a local realistic way. That is, a contradiction arises between quantum mechanics and local realism, Einstein's EPR view, already for individual quantum events and not just for statistical ensembles, as was the case of Bell's inequality [17]. A generalization of two-particle interferometry explicitly proposed for a three-particle interferometry case (figure 3) [18] would show exactly the kind of contradiction just mentioned.

Ever since our surprising discovery of the curious properties of multi-particle entangled states, it had been my goal to realize such states in the laboratory. In the late 1980s, this was a huge challenge. No sufficiently good sources for entangled states existed, the procedures to entangle more than two particles were completely unknown, the coincidence and detection criteria in that situation had to be found etc—in short, none of the tools for the creation of multi-particle entangled states existed, and we basically had to invent them from scratch in our labs. The first important step was to switch from neutrons to atom optics on the one hand and to photonic entanglement on the other, because neutrons were not suitable to realize entangled states.

For example, at the time of the proposal [18], it was evident that the existing sources of entangled photons based on the procedure of type I down-conversion [15] did not produce beams of entangled pairs with sufficient intensity. Thus, the

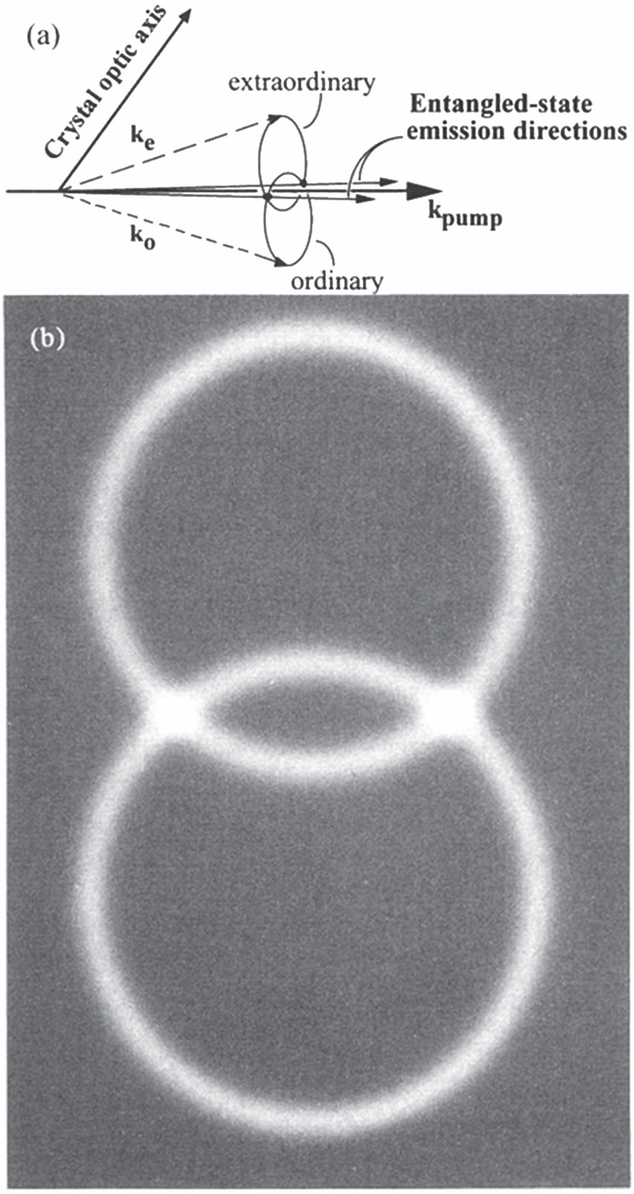

Figure 4. (a) Spontaneous down-conversion cones present with type-II phase matching. Correlated photons lie on opposite sides of the pump beam. (b) A photograph of the down-conversion photons, through an interference filter at 702 nm (5 nm full width at half maximum (FWHM)). Polarization-entangled pairs emerge at the intersections of the rings. This source became central to many experiments performed in my group. Reprinted figure with permission from [19], Copyright (1995) by the American Physical Society.

development by Paul Kwiat and others in my group of a new high-intensity source for polarization-entangled photon pairs (figures 4 and 5) [19] also became crucial for many of our subsequent experiments.

Equipped with this new source, we were finally in a position to realize a number of basic concepts in quantum information science. One of them was the first experimental realization of GHZ states (figure 6) [20] and they were also used in tests of quantum nonlocality in three-particle entanglement [21].

The first application of photon entanglement in quantum information

As I mentioned above, in our work towards realizing multi-photon entangled GHZ states in the laboratory, we developed many toys which over time became

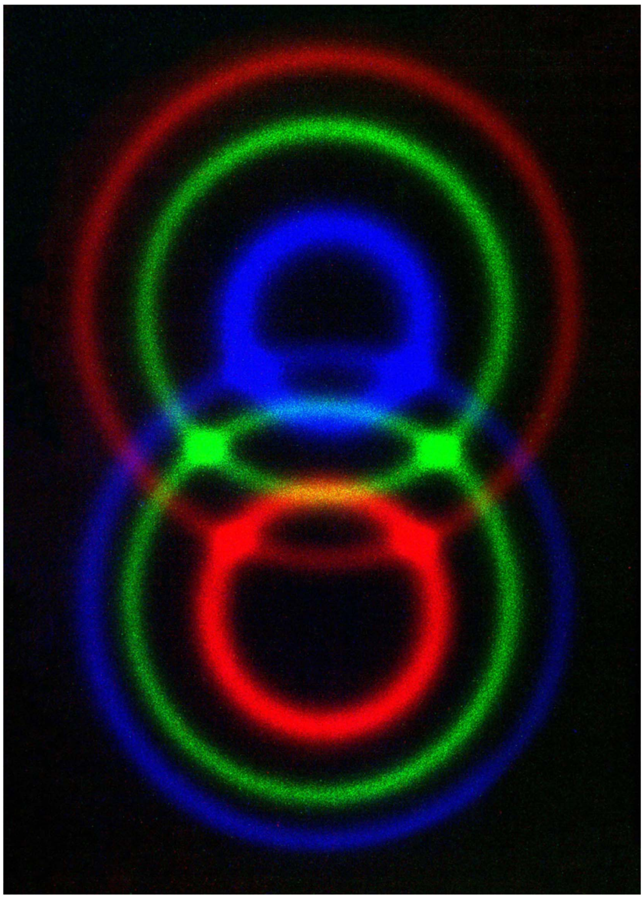

Figure 5. A photograph of the down-conversion photons, taken with different interference filters. Photo: Michael Reck and Paul Kwiat.

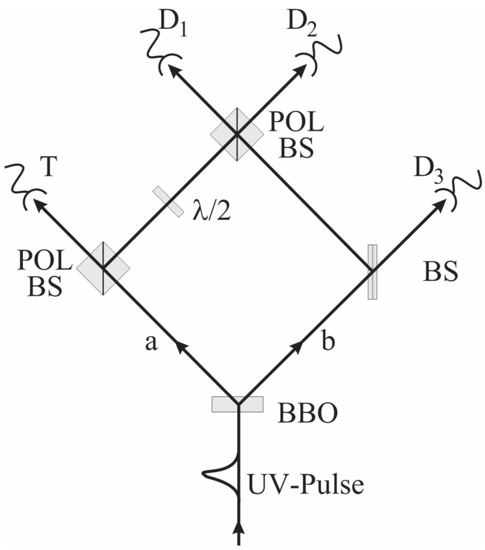

Figure 6. Experimental realization of GHZ states. The drawing shows the setup used in the first demonstration of GHZ entanglement. The BBO crystal creates probabilistically two pairs of entangled photons at the same time. The timing of the experiment and the geometry were arranged such that when the trigger detector T registers a photon, the information from which of the two pairs it comes is erased. Then, when three photons are registered at D_1, D_2 and D_3, they exhibit the desired GHZ correlations. Reprinted figure with permission from [20], Copyright (1999) by the American Physical Society.

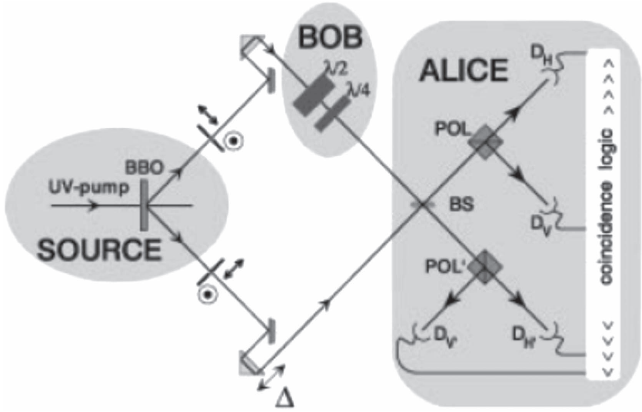

Figure 7. Experimental setup for quantum dense coding. The source produces a pair of polarization-entangled photons in one of the Bell states. Bob then, by modifying only one of the two photons, can switch around between four orthogonal possibilities for the two-photon state, thus sending two bits of information. In a classical setting, he would only be able to send one bit, if he has access to the polarization of one photon only. Alice then, having access to both photons, can identify the full message. In our experiment, it was possible to resolve three possibilities, that is, send 1.76 bits of information, which still results in more than one bit of information per photon handled by Bob. Reprinted figure with permission from [22], Copyright (1996) by the American Physical Society.

useful in numerous quantum information applications. Along the road, our—and probably anyone's—first application of quantum entanglement in an information theoretic protocol was the experimental realization [22, 23] of hyper-dense coding. The basic concept had been proposed by Bennett and Wiesner in 1992 [24]. To realize this idea, consider first just a single photon's polarization. For example, one can encode into it one bit of classical information by choosing horizontal or vertical polarization at the basis. I should remark that there is full isomorphism with the physics of spin ½ particles. A vertically polarized photon may for example be considered to be equivalent to a particle with spin up and a horizontally polarized photon may be equivalent to one with spin down.

The idea of hyper-dense coding is based on an interesting feature of entanglement. When one looks at the maximally entangled states of two photons, the four orthogonal Bell states result. These four orthogonal states represent two independent bits of classical information. The only question is how to produce these states in order to encode the information and how to measure the states in order to decode it. The basic point of hyper-dense coding is that in order to switch around among all four two-photon Bell states, one needs to have access to just one photon (figure 7). It suffices to manipulate the polarization and the phase of one photon only. Suppose one starts with one Bell state, then, to switch to another one, one just has to change the phase of a single photon photon, for example by inserting a $\lambda/4$ plate, as shown in figure 7. To switch to another state, one swaps horizontal and vertical polarization with the $\lambda/2$ plate, as shown. To switch to the fourth, one applies both the $\lambda/2$ and the $\lambda/4$ plates. Note that operating on a single non-entangled beam, only one bit of information could be encoded. But because the photon is entangled with another, proper identification of the entangled states results in four possibilities, i.e. two bits of information which can be encoded and decoded.

In the experiment itself, we were able to discriminate between three possibilities by measuring the correlations for the two photons in the beam splitter and polarizer setup shown in (figure 7). Thus, 1.76 bits of information could be encoded and decoded by just accessing a single photon. This clearly surpasses the classical limit of one bit per photon.

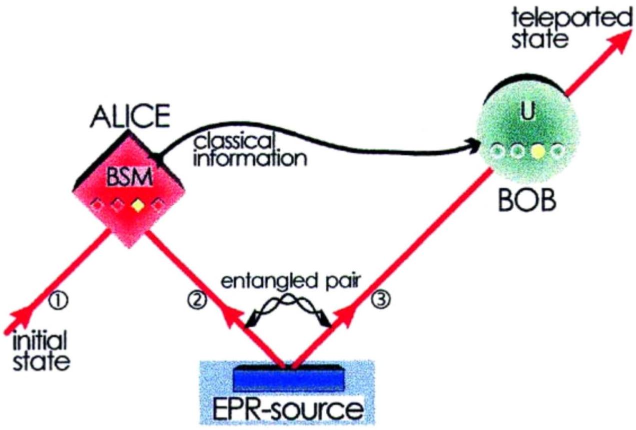

Figure 8. Quantum teleportation. Alice has a quantum system, particle 1, in an unknown initial state which she wants to teleport to Bob. Alice and Bob share an ancillary entangled pair of particles 2 and 3 emitted by an EPR source. Alice then performs a joint Bell state measurement (BSM) on the initial particle and one of the ancillaries, projecting them, too, onto an entangled state. After she has sent the result of her measurement as classical information to Bob, he can perform a unitary transformation (U) on the other ancillary particle resulting in it being in the state of the original particle. Reprinted by permission from Macmillan Publishers Ltd: Nature [26], Copyright 1997.

Experimental quantum teleportation

As I mentioned above, my goal had been to realize GHZ states ever since Greenberger, Horne and I had proposed them. Along the road, again something unexpected happened. In 1992, Bennett, Brassard, Crépeau, Jozsa, Peres and Wootters proposed the concept of quantum teleportation [25]. When this paper came out, my immediate reaction was that it is impossible to do the experiment within the foreseeable future. I was not aware of the fact that in my lab, we were developing all the necessary tools to perform it. The reason is that the requirements for quantum teleportation are very similar to the requirements to establish multi-particle entanglement.

We realized that such an experiment is similar to the GHZ experiment because in teleportation, too, one creates two entangled pairs, and then, one has to perform a measurement which erases the source information (figure 8). The most challenging requirement in the development of the technology was to meet the precise timing requirements for creating and measuring the two photon pairs. Otherwise, precise time measurements could reveal source information and thus prohibit projection onto a joint state. In the first experiment [26], we were able to teleport over a distance of about one meter in the laboratory. Quantum teleportation allows one to teleport the quantum state of an unknown system over an arbitrary distance without Alice having to send the state itself to the receiver Bob [26]. We therefore also performed the quantum teleportation experiment over 143 km (figure 9) [27] in a series of quantum communication experiments on the Canary Islands (figure 12).

Most remarkably, at the same time, a similar long-distance teleportation experiment was realized by the group of Jian-Wei Pan across Qinghai Lake in China [28].

Entanglement swapping—a blockbuster application

A crucial step forward already used in teleportation which then became important in many future protocols was the realization that a simple beam splitter can be used to entangle independent photons. This idea found immediate application in the realization of the proposal together with Żukowski *et al* [29] of entanglement swapping. In entanglement swapping, two photons which have never interacted with each other become entangled.

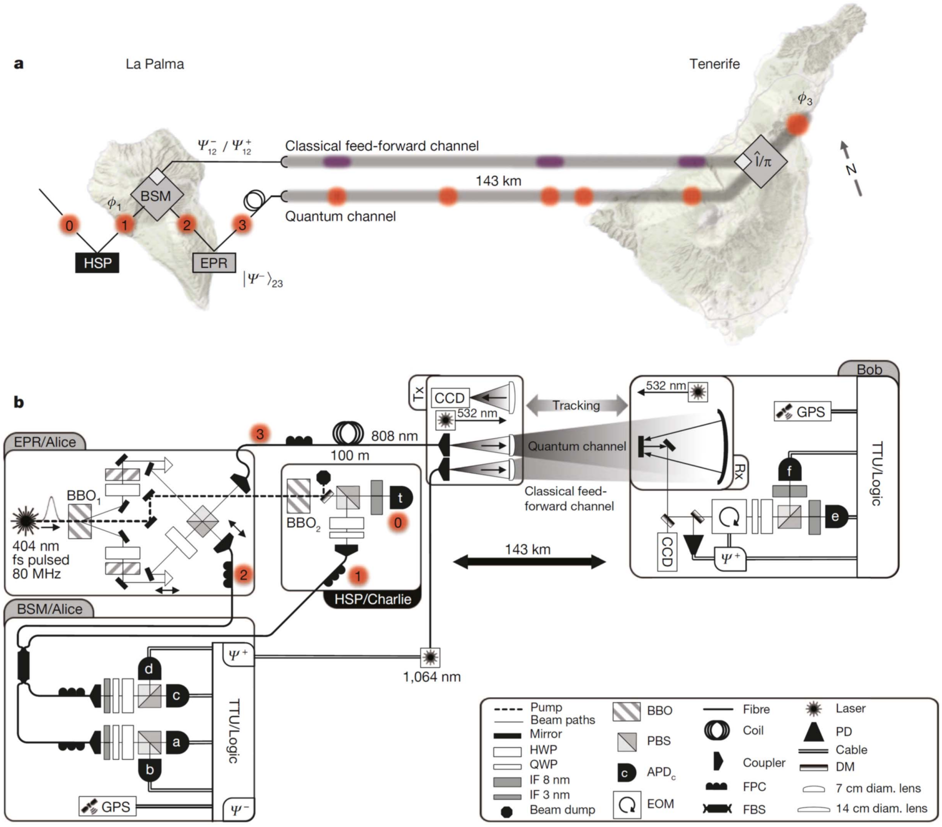

Figure 9. Quantum teleportation between the Canary Islands La Palma and Tenerife over both quantum and classical 143 km free-space channels. (a) Experimental scheme. Alice and Charlie are situated in La Palma and Bob in Tenerife. Charlie prepares the teleportation input photon 1 in $|\phi\rangle_1$, using a heralded single-photon (HSP) source with a trigger photon 0 (photons are indicated by black numerals on red circles). An EPR source generates an entangled pair of photons 2 and 3 in the state $|\psi^-\rangle_{23}$. Alice then performs a Bell state measurement (BSM) on photons 1 and 2, projects them onto two of the four Bell states ($|\psi^-\rangle_{12}|\psi^+\rangle_{12}$), and sends the result via the classical feed-forward channel to Bob, who applies a unitary transformation (identity operation or π phase shift) on photon 3 depending on the BSM result and thus turns its state $|\phi\rangle_3$ into a replica of the initial quantum state $|\phi\rangle_1$. (b) Setup. In La Palma, a frequency-uncorrelated polarization-entangled photon pair source generated photons 2 and 3 in BBO_1 (EPR/Alice) and a collinear photon pair source generated photons 0 and 1 in BBO_2 (HSP/Charlie). All single photons were coupled into single-mode fibers. For implementing the BSM, photons 1 and 2 interfered in a fiber beam splitter (FBS) followed by polarization-resolving single-photon detection (BSM/Alice). Photon 3 was guided to the transmitter telescope via a 100 m single-mode fiber and sent to Bob in Tenerife, where the unitary transformation was implemented using an electro-optical modulator (EOM) and photon 3's polarization was measured. A real-time feed-forward operation was implemented by encoding the $|\psi^+\rangle_{12}$ BSM result in 1.064 nm laser pulses, which were then sent to Bob via the feed-forward channel. On Bob's side, they were separated by a dichroic mirror (DM), detected with a photodetector (PD) and used to trigger the EOM to perform the required π phase shift operation. Reprinted by permission from Macmillan Publishers Ltd: Nature [27], Copyright 2012. See there for details.

Entanglement swapping is a most curious situation. In essence, it is the teleportation of an entangled state [25]. When we proposed the method in 1993 [29], the motivation was to realize the so-called 'event-ready situation' in a test of Bell's inequality as it had been proposed by John Bell [30]. In essence, one takes two entangled pairs and projects one photon from each pair onto an entangled state, with the result that one knows that the other two photons, one from each pair, which can be at distant locations, have now become entangled. In consequence, one has an entangled state for these two distant photons at hand. This evidently holds for any kind of entangled particles. It became important for example in a recent loophole-free Bell experiment, as will be discussed below.

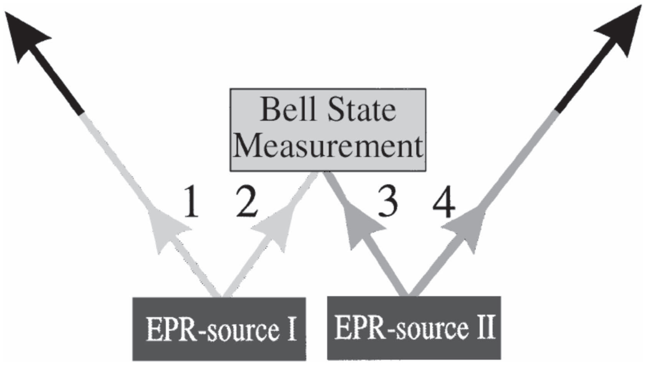

Figure 10. Principle of entanglement swapping. Two EPR sources produce two pairs of entangled photons, pair 1–2 and pair 3–4. One photon from each pair (photons 2 and 3) is subject to a Bell state measurement, which entangles them. This results in projecting the other two outgoing photons 1 and 4 onto an entangled state. This resulting state can be used, for example in a quantum repeater, to connect quantum computers with each other. Evidently, the scheme can be repeated to provide—via chained entanglement swapping—long-distance connections. Reprinted by permission from Macmillan Publishers Ltd: Nature [27], Copyright 2012.

One can also see why this procedure is called entanglement swapping (figure 10). The entanglement is swapped from the original two pairs, 1–2 and 3–4, which can be created independently, to the two photons 2–3 and 1–4.

Conceptually most interesting, these two photons have never interacted in the past. Thus, and this is what caught my personal fancy at that time, entanglement is not restricted to situations where the two particles are coming from the same source or where something like an interaction exists between the particles, or where a conservation law is responsible for the entanglement. In the experiment itself, one produces two entangled pairs and overlaps one photon from each pair at the Bell state analyzer. Again, rather strict timing coincidence conditions have to be obeyed [31].

It is interesting to note that the proposal to use entanglement swapping in a Bell test has recently been implemented in two experiments closing many loopholes at once. In that case, it was the creation of entanglement between two spins [32] or between two atoms [33]. They became entangled with each other by entangling one photon each emitted from each spin or atom.

Entanglement swapping can now cover distances of the order of 150 km, as recently also demonstrated between the islands of La Palma and Tenerife (figure 11) [34].

As I mentioned, I was mainly interested in entanglement swapping because of the curious feature that one can use this to entangle two completely independent photons with each other. This is fundamentally quite interesting. But, once more, I was surprised by an important application that emerged. Entanglement swapping will be essential for connecting future quantum computers with each other over large distances in a quantum internet. Entanglement swapping turns out to be an important ingredient in a quantum repeater [35], which is basically a combination of entanglement swapping and tiny quantum computer nodes which provide entanglement purification (figure 19) [36] and enhancement of a quantum signal [35].

Quantum cryptography and Bell tests: fundamentals and early applications in parallel

As I mentioned above, I became interested in the late 1980s in quantum entanglement just out of fundamental curiosity. Like everyone else in the field at that time, I imagine, I was not aware of any possible applications. Even more, I was

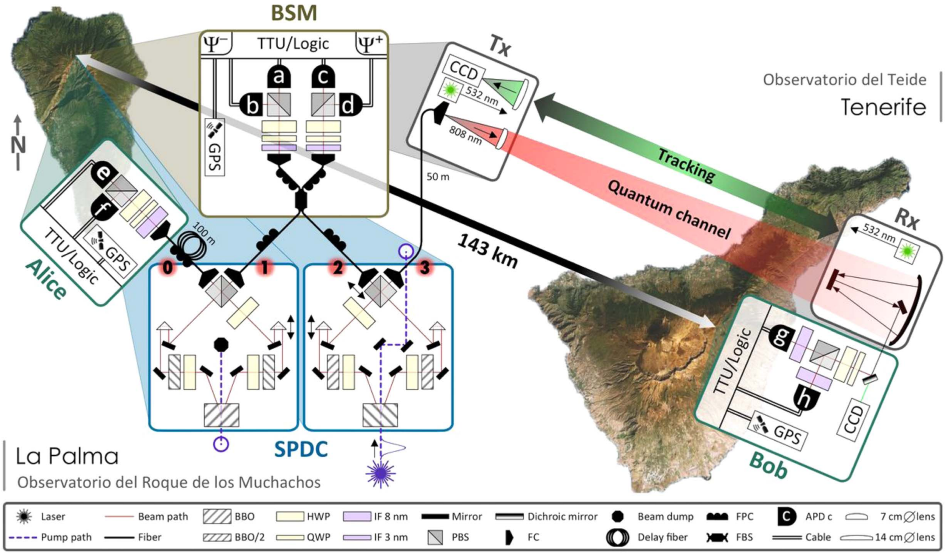

Figure 11. Entanglement swapping over a 143 km free-space channel between the Canary Islands of La Palma and Tenerife. Both spontaneous parametric down-conversion (SPDC) sources, the Bell state measurement (BSM) module and Alice, were situated on La Palma. Bob was located on Tenerife. The two SPDC sources generated the polarization-entangled photon pairs 0–1 and 2–3. Photons 1 and 2 (photons are indicated by black numbers on red circles) were subjected to a Bell state measurement which entangled them. A 100 m fiber delayed photon 0 with respect to photon 3, such that Alice's and Bob's measurements were space-like separated, because no signal from Alice's measurement could have arrived in time to influence Bob's measurement. Revealing entanglement of photons 0 and 3 between Alice and Bob verified successful entanglement swapping. All detection events were time stamped by time-tagging units (TTU) with a resolution of 156 ps and stored for subsequent analysis. Reproduced with permission from [34]. See there for details.

Figure 12. The OGS (Optical Ground Station) established on the island of Tenerife by the European Space Agency ESA. This telescope is used in our tests of long-distance quantum communication between the Canary Islands of Tenerife and La Palma which are separated by about 150 km. The laser beam shown is an alignment laser going over to La Palma. At the end of the laser line, one sees a bright spot, which is another alignment laser pointing from La Palma to Tenerife. Photo: Daniel Padrón.

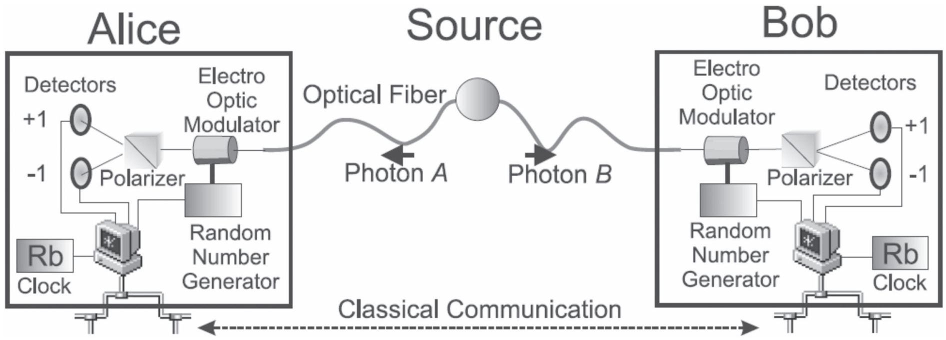

Figure 13. Entanglement-based quantum cryptography and Bell test with polarizer settings varied by a quantum random number generator. Polarization-entangled photons are created in the source and transmitted via optical fibers to Alice and Bob, who are separated by 360 m, and both photons are analyzed, detected and registered independently. The Rubidium clocks serve to identify correctly the photons belonging to a pair. After a measurement run, the keys are established by Alice and Bob through classical communication over a standard computer network. Reprinted figure with permission from [40], Copyright (2000) by the American Physical Society.

probably—but it is hard to tell in hindsight—convinced that there never would be any applications, that pursuing such issues was simply part of the joy of physics. All this changed.

I still remember my sheer delight when at a conference in Italy in 1990 or 1991 I discovered a poster presented by Artur Ekert where he suggests exploiting quantum entanglement for quantum cryptography. For me, this proposal was of an enjoyable intellectual clarity and simplicity. But still, even at that time, I did not really think that it could be more than an intellectual game. A real-world technical large-scale application sounded too far away for me. But then, I underestimated the creativity of my colleagues world-wide and, I have to admit, also of my own group to come up with the possibilities for realizing such 'toy applications' of quantum entanglement. I certainly did not expect that such 'toy applications' would lead to useful technology. And in hindsight even more surprisingly, I underestimated my own group's creativity and determination to realize such schemes experimentally. Since then, this field has seen an enormous explosion, first of experiments realizing the basic ideas and subsequently with an emerging wave of technological applications.

Quantum cryptography is the application which has become most mature today. In a broad sense, there are two types of quantum cryptography, one based on individual quantum systems and the other one on quantum entanglement. A forerunner is the proposal of unforgeable quantum money by Wiesner [37]. Apparently, it is well known in the community that Wiesner had these ideas already in the early 1970s, communicating them verbally at least to Charles Bennett, but being unable to get a paper published. That early proposal already contains some important features of quantum information, such as the randomness of the individual measurement events encoding in conjugate bases and, implicitly, the no-cloning-theorem which was later formalized most elegantly by Wooters and Zurek [38]. These concepts also play a central role in the first proposal of quantum cryptography by Bennett and Brassard [39]. Interestingly, entanglement was the main fundamental quantum concept that was not yet contained in the Wiesner idea.

In the entanglement-based version of quantum cryptography, one uses the perfect correlations in entangled systems to establish a secure key at two locations at the same time (figure 13). Due to entanglement, the key comes into existence at both separations because of the correlation between the measurement results on the two entangled photons. Or, more precisely, the two measurements can be so far removed from each other that no communication between them can establish

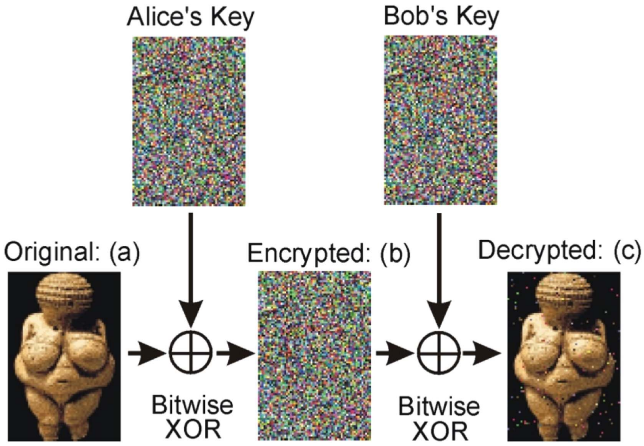

Figure 14. In the entanglement-based quantum cryptography experiment [40], the image of the 'Venus von Willendorf' effigy, an Austrian prehistoric carving and a well-known icon of prehistoric art, was transmitted—encrypted and decrypted. Reprinted figure with permission from [40], Copyright (2000) by the American Physical Society.

the key. After our realization (figure 14) [40], we learned that the groups of Paul Kwiat [41] and Nicolas Gisin [42] also were very close to publishing similar results, so we held off our publication such that the three could be published together.

Our quantum cryptography experiment owes its existence to a test of Bell's inequalities which we performed in Innsbruck. The idea of that experiment came about in a very simple way. The first experiment testing Bell's inequality [43] used a static setup. That implied the communication loophole to be wide open. Since the measurement settings were decided a long time before the measurement, there remained the in principle possibility of communication between measurement stations, for instance about the measurement settings opening up a possibility for local realism to explain the results. The first experiment closing that loophole was performed by Aspect, Dalibard and Roger [44] with periodically switched polarization measurements. I became fascinated by the idea to use randomly switched polarizers, which are switched just immediately before the photon arrives at the respective measurement station. Because random switching takes more time, this required experimental separations of a few hundred meters. Luckily, I had an outstanding young experimentalist, Gregor Weihs, who wanted to work with me on a PhD thesis, and I gave him that project. Even more luckily, Alain Aspect was visiting us in Innsbruck at that time, and in discussions with Gregor, he provided a lot of motivation for the experiment. The result [45] beautifully violated a Bell-type inequality (figure 15). In the realization, the source of the entangled photons was located in the basement underneath one of the libraries of the University of Innsbruck. The fiber-optic cables of the two photons ran through underground paths to different locations, one to the physics building and the other one to a building where colleagues at the Technical Department tested the effect of large amounts of water running down artificial ravines and rivers. The intellectual tension between our small experiment exploring the quantum world and the huge experiments exploring flooding and dams was quite fascinating.

Another surprise

One of the biggest surprises of my life was that one day, I was invited to participate in dOCUMENTA (13). The dOCUMENTA is one of the biggest exhibitions of contemporary art. It takes place every five years in Kassel. dOCUMENTA (13) happened from 6 June to 16 November 2012.

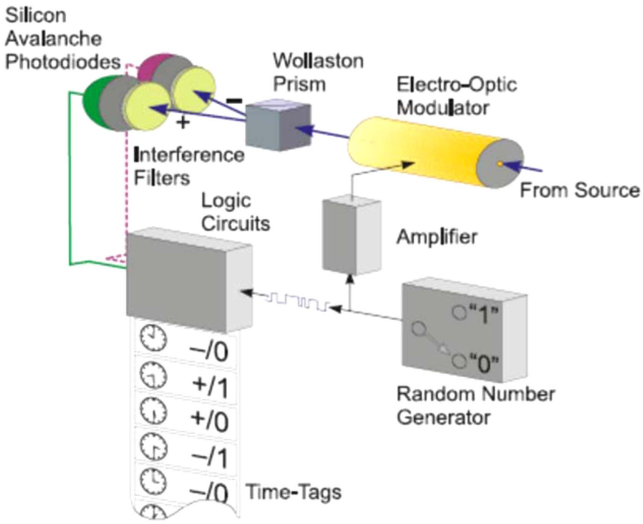

Figure 15. One of the two observer stations used both in the quantum cryptography experiment and in the Bell test that closed the communication loophole. A fast quantum random number generator is driving the electro-optic modulator and thus changing the polarization measurement. Silicon avalanche photodiodes are used as detectors. A 'time tag' is stored for each detected photon together with the corresponding random number '0' or '1' and the code for the detector '+' or '–' corresponding to the two outputs of the Wollaston prism polarizer. All alignments and adjustments were purely local operations that did not rely on a common source or on communication between the observers. Reprinted figure with permission from [45], Copyright (1998) by the American Physical Society.

The invitation came from Carolyn Christov-Bakargiev, the curator of dOCUMENTA (13). Actually, she and her associate Chus Martínez visited me in the summer of 2011 during my vacation at Lake Traunsee in Austria. The three of us spent a whole day discussing the foundations of quantum mechanics, the role of the observer, the quantum–classical transition, quantum entanglement etc etc. My immediate reaction to the invitation was that we could not do this, basically because I did not want to take away the time of my young collaborators from their research. But actually, three of my team members volunteered, Robert Fickler, Christoph Schäff and Bernhard Wittmann. So we decided to design five experiments altogether for installation in the Fridericianum (figure 16).

The idea was to show fundamental phenomena which are important for understanding the nature of light and in particular its quantum features. The five experiments shown were:

1. wave interference in a glass fiber interferometer,
2. quantum randomness at a beam splitter,
3. the double-slit experiment,
4. the change of state by a polarizer,
5. quantum entanglement and Bell's inequality.

The construction of these experiments was actually very interesting and taught us an important lesson. We decided from the very beginning to perform absolutely real experiments, and not just mock-ups or simulations. Also, we built them as simply as possible, that is, with few components, just enough to show the real phenomenon. We later learned that it is also an objective in art to express as much as possible with the smallest effort which is necessary. An extreme example is Malevich's Black Square [46].

We also decided to operate the experiments such that at least two members of my group were present at all times, to make sure that everything was running smoothly, to talk to the visitors, to give explanations, answer questions, etc etc. This was actually quite unusual for an art exhibition, since artists generally are not

Figure 16. dOCUMENTA (13) in the Fridericianum in Kassel. The quantum experiments were located in the rooms on the upper floor, just to the right of the central portico. Because of the central location, our experiments were seen by a large fraction of the 860 000 visitors of dOCUMENTA.

present all the time. When I talked to Carolyn Christov-Bakargiev about that, she simply declared us physicists to be part of the presentation. Altogether, dOCUMENTA (13) had 860 000 visitors. We guessed that a very significant fraction of them passed by our experiments simply because of the central location of our setup—and it also felt that way!

In the double-slit experiment, the intensity of the laser light passing the two slits was reduced such that every observer could see on the screen that the photons arrived individually. In this way, the buildup of the interference pattern could be followed in real-time (figure 17). The experiment showed clearly that such an interference phenomenon can only be understood by accepting that the photon propagation through the two slits is governed by a probability wave and that the photons arrive individually on the screen. In other words, this experiment shows that light traverses the slits in a superposition of passing through the right slit and passing through the left slit, but it is detected as individual quanta.

The most difficult and challenging experiment was a real-life test of Bell's inequality during dOCUMENTA (13). Figure 18 shows the source. Blue pump light enters a crystal in the center of the picture, where entangled pairs of red photons (simulated) are generated. Each photon is then fed into a glass fiber. One of them can be seen at the center right of the figure. These glass fibers pass the photons to two independent detector stations which are spatially separated and located a few meters away. The photons created in the source were entangled in polarization. Therefore, polarization measurements of the two photons by Alice and Bob were able to verify their entanglement. The experiment was set up in such a stable way that we were indeed able to obtain a violation of Bell's inequality while literally scores of visitors were passing by. This was a major achievement by my colleagues Robert Fickler, Christoph Schäff and Bernhard Wittmann. The Bell inequality experiment had significant theoretical help from Bill Plick in my group. One of the experiments performed there live was actually a first direct test of Wigner's version of Bell's inequality [47]. This result, not published thus far, is probably the first real physics experiment performed in an art exhibition, which provides a novel result not achieved before.

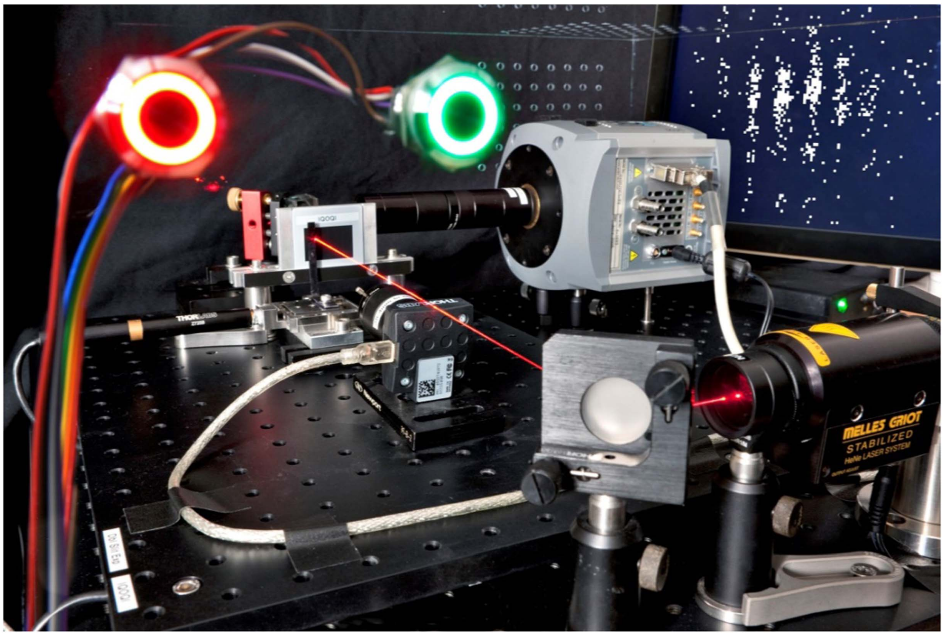

Figure 17. The double-slit experiment, as shown at dOCUMENTA (13): probability wave and particle detection. Light coming from a laser (lower right) was reflected by a mirror towards a slide. That slide contained two parallel slit openings. Behind the slide, the light was reflected to the right into a camera (large gray-black block). This camera was capable of single-photon detection and registered the patterns of the photons passing through. By hitting a green or a red button, visitors could open or close one of the two slits. It was obvious to the visitors that the photons arrived individually at the camera and that each photon makes a spot. For any observer, the arrival of an individual photon appears random. In the end, they form a pattern with stripes (top right, showing the pattern when both slits are open). Photo: Lois Lammerhuber.

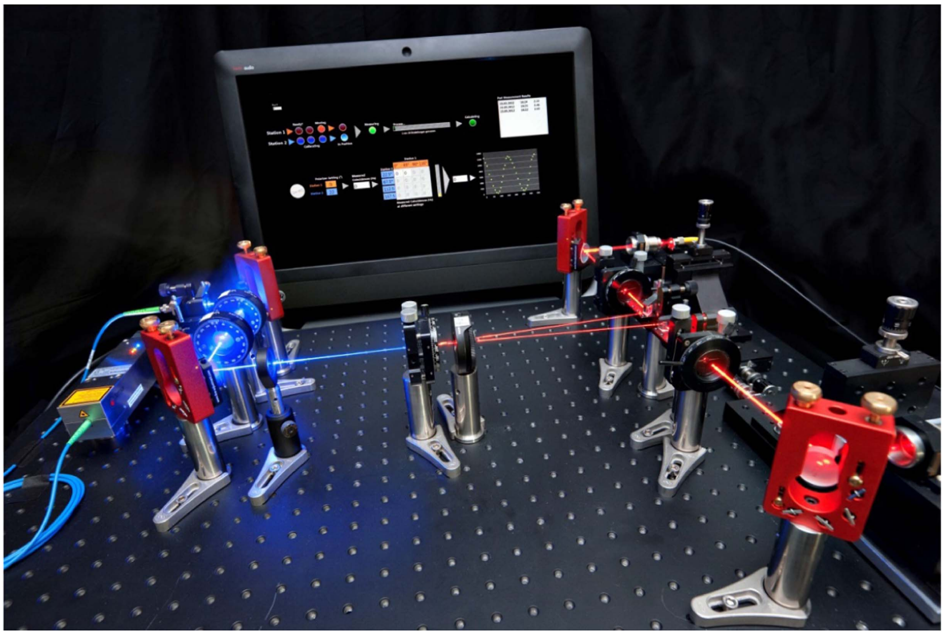

Figure 18. The source of entangled photon pairs used in the test of Bell's inequality at dOCUMENTA (13). Photo: Lois Lammerhuber.

Einstein and quantum light

At dOCUMENTA, a number of visitors asked about Einstein's role in quantum physics. For me personally, Einstein's contributions to and his criticisms and

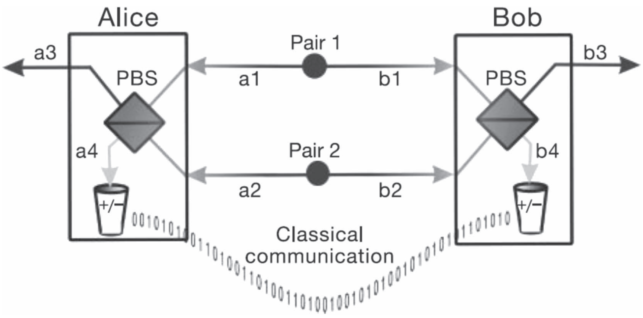

Figure 19. Schematic drawing showing the principle of entanglement purification using linear optics. We start with two less entangled pairs shared by Alice and Bob who superpose their photons on a polarizing beam splitter (PBS). Alice and Bob keep only those cases where there is exactly one photon in each output mode. Then, certain polarization measurements on the photons in *a*4 and *b*4 result in an entangled state emerging into two modes *a*3 and *b*3 in higher purity than the original entangled states. The procedure of entanglement purification is essential for future quantum repeaters. Reprinted by permission from Macmillan Publishers Ltd: Nature [36], Copyright 2003. See there for details.

analyses of the quantum physics of light were always fascinating. While I certainly do not agree with all his conclusions, his considerations provided very significant stimulations along my intellectual path.

When Einstein proposed in 1905 the concept of particles of light [5] later called photons [48], he was rather cautious, talking in the title about a 'heuristic point of view' and evidently aware of its potential conceptual impact. His language in the paper implies that he viewed particles of light to be real objects. And in a letter to his friend Habicht, he called this paper 'very revolutionary'[1]. Apparently, he also was aware of the fact that the particle idea is in conflict with quantum interference at low intensities. Einstein himself considered fundamental questions about the nature of light as not settled, as witnessed by his famous quote of 1917:

> *For the rest of my life I want to reflect on what light is.*

This was at the same time as he was laying the foundations for the theory of the laser [49] and the general concepts of stimulated and spontaneous emission [50].

I should mention that Einstein's 1905 paper, which is usually represented just as explaining the photoelectric effect, is actually much more elegant. His argument primarily rests on entropy considerations. In particular, he observes that the entropy of a light field in a cavity varies in the same way as a function of volume, like that of an ideal gas in a container. Therefore, he argued, since the entropy of a gas can be understood using particles, the radiation field must also consist of particles.

Einstein's paper of 1935, where, together with Boris Podolsky and Nathan Rosen he introduces the concept of entanglement into the discussions on the foundations of quantum mechanics, had a very interesting reception. In the beginning, it received a few citations, but then it was essentially ignored until John Bell discovered that the predictions of quantum mechanics are in conflict with the local realistic theory. This was the viewpoint presented in the EPR paper. The position is very clearly defined by Albert Einstein in 1947 [51], where he said about quantum theory:

> *The reason I cannot seriously believe in it is that the theory cannot be reconciled with the principle that physics has to describe a reality in space and time without spooky action at a distance*[2].

It is not the purpose of the present paper to discuss the subtleties of the EPR argument, but suffice it to say that in the same year, Erwin Schrödinger picked up

[1] Apparently, this was the only of his papers he ever called 'revolutionary' himself, but that question might need further clarification by historians.
[2] The translation is mine.

the EPR reasoning twice, firstly in his paper in *Naturwissenschaften* [7] introducing *Verschränkung*, where he also proposes the Schrödinger cat paradox, and secondly in a paper for the Cambridge Philosophical Society introducing *entanglement* [52], a notion coined by him, of which he says:

> *I would not call that* ***one*** *but rather* ***the*** *characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.*

A most modern position which leads directly to today's applications of entanglement is Schrödinger's analysis of entanglement in terms of 'expectation catalogues' [7]. He remarks that when two systems are entangled, we only have a joint expectation catalogue, but never expectation catalogues for the individual systems. Today, one would say that when a maximally entangled system is in a pure state, the individual particles are in mixed states.

For Schrödinger, the quantum state, or the wave function, are just representations of expectation catalogues of future experimental results. In modern language, one can say that an entangled state expresses well defined information about joint measurement results on the entangled systems, but the information for the individual systems is completely undefined [53]. This definition can be seen to directly lead to modern applications.

Another surprise: quantum computation and entangled photons

Around the same time when I began to work on quantum entanglement and did my own first fundamental experiments just out of curiosity, an interesting development began in parallel. First, proposals appeared that a new field would open up for computation when the computer itself would operate according to quantum rules [54–57]. Again, it is amazing to me that the methods we developed to entangle more than two photons became important to demonstrate some basic procedures in quantum computation. This was made possible by a very interesting development. Quantum computation has to utilize the interaction between two quantum bits (qubits). Thus, it has to employ some nonlinear element. This is in practice not possible for individual photons, because the nonlinear effects introduced by a single photon in any medium are too small to significantly modify the quantum state of another photon.

The important idea was [58] that measurement itself can provide the necessary nonlinear element. This is because a projective measurement breaks the unitarity of quantum evolution. A most important concept here is the one-way quantum computer [59]. This is a device which operates with a combination of unitary operations and measurements. The proper sequence of unitary operations and measurements implements the algorithm in a multi-qubit entangled system. The interesting point now is that such a quantum computer can implement any algorithm, so it is general. In a sense, it is an implementation of the 'Infinite Library' invented by the medieval philosopher Raimundus Lullus[3]. The Argentinian writer Jorge Luis Borges wrote a beautiful short story, where he explains that the Infinite Library contains all books which have ever been written and all books which will ever be written, because it contains books with all possible combinations of letters [60]. Clearly, such a library is useless, because finding the one and only one single copy of for example Shakespeare's 'Hamlet' without any misprints is a task of the same complexity as writing the book from the beginning. But the quantum state of the one-way quantum computer can be seen to do just that because it represents all possible solutions. Having demonstrated entanglement purification [36, 61] and some basic quantum gates using entangled photons [62, 63], we were also able to implement one-way quantum computation [64].

[3] Known as Raimundus or Raymundus Lullus or Lullius or, in anglicized versions, as Raymond Lully or Lull or as Ramon Llull.

A most interesting idea along that line of research is the concept of blind quantum computation. The challenge is that in a future quantum information network, a client wants to use a quantum server—that is, a centrally located quantum computer—in an absolutely secure way. The condition is that the operator of the server not only has no possibility to know which data the operator is using, but also that the operator has no clue about which program the client is running—whether the client is just playing a game or analyzing stock market data. An answer to the first challenge is provided by quantum cryptography. A solution to the second challenge was discovered by Broadbent *et al* [65]. The advantage is that the client needs only very limited quantum computational power. Basically, he needs only to be able to produce quantum bits in an arbitrary state and to send them to the quantum server. The quantum server commands the full power of quantum computation, that is, implementing any unitary state and creating any entangled state out of the qubits, which the client sends to it. The client sends a series of qubits in arbitrarily changing states. Only he knows which state they are in. The quantum server then entangles these qubits, producing a highly entangled, so-called cluster state. This is the essential operating state of a one-way quantum computer. Then, the client also tells the quantum server what the sequence of measurements is that he has to perform on the cluster state in order to carry out the computation. Finally, the server reports to the client the measurement result. Only the client understands what the result of the measurement means, because only he knows what the quantum state was on which the server was operating. In a very simple first demonstration, we were able to show that the basic principle can be implemented already with four photons [66, 67].

It is evident that for real-world large-scale applications, one has to be able to create entangled states out of more photons. It is understood in the quantum community that a quantum computer made of more than 40 qubits would be too complex for simulation on classical computers. Then, something really interesting and new begins.

In that sense, it is exciting that more recently, the group of Jian-Wei Pan in China has succeeded in entangling up to eight photons with each other, in two different independent experiments [68, 69]. Most recently, the same group was also able to demonstrate ten-photon entanglement [70]. A development which promises to be able to carry forward to more photons and higher dimensions was recently realized in the group of Mohamed Bourennane [71]. For a review of multi-photon entanglement and interferometry, see [72].

Closing loopholes, making quantum communication secure

Many quantum communication protocols, like the entanglement-based version of quantum cryptography, quantum teleportation, and entanglement swapping, are based on the quantum correlations between distant entangled states. Given the importance of the role of quantum mechanics in these procedures, an important question remains: Can the correlations observed in a real experiment with certainty not be explained classically? No experiment is perfect, and measurement flaws may present possibilities for classical interpretation alternatives. It is the issue of loopholes in existing experiments. Closing such loopholes is not only relevant from a fundamental point of view, because it excludes a classical local realistic world-view, but it is also relevant for the security of various quantum communication protocols. The reason is that for example in quantum cryptography, if the correlations are not perfect, one cannot be sure whether an eavesdropper, a spy, is taking advantage of such a situation, because the influence of the eavesdropper would also be to make the correlations weaker. For a completely loophole-free experiment, even the most critical skeptic has to admit that the experiment is secure. This is because there is no room for even a presently unknown mechanism to explain the results in a local realistic way. Such a way might provide an inroad for an attacker on the cryptography link.

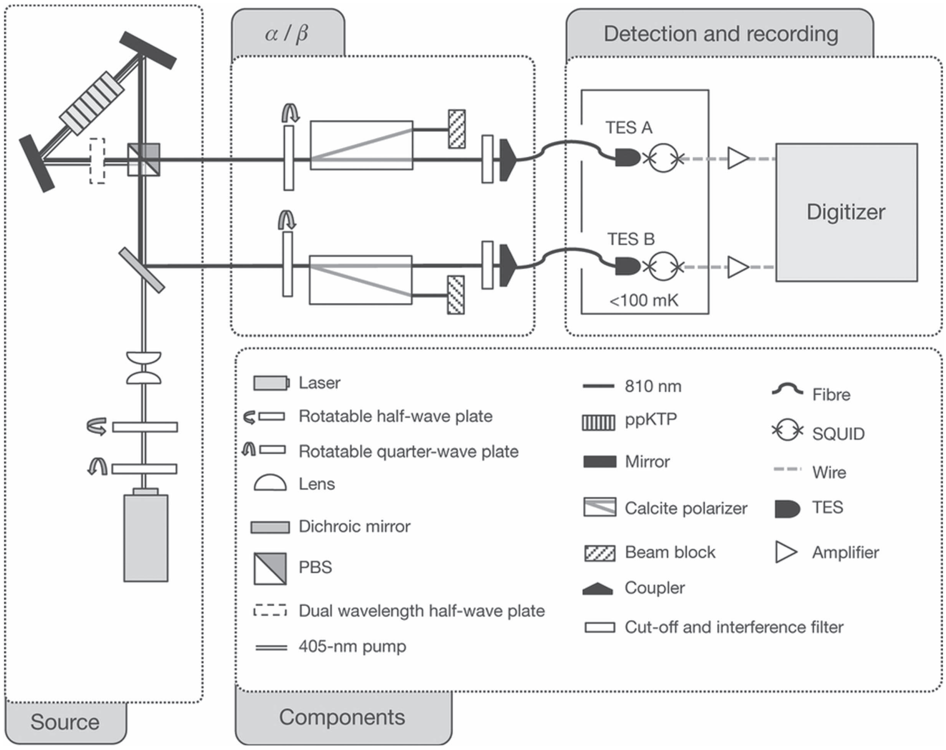

Figure 20. Experiment closing the fair-sampling loophole for photon pairs. The source, based on spontaneous parametric down-conversion in ppKTP (periodically poled potassium titanyl phosphate) in a Sagnac configuration, produces polarization-entangled photons with a wavelength of 810 nm. A measurement setting is implemented in each arm by rotating a half-wave plate to the desired angle α (β) in front of a calcite polarizer. Photons transmitted through the calcite polarizer (ordinary output beam) are spectrally filtered and coupled into an optical fiber (SMF-28), which leads them to transition-edge superconducting detectors (TES) for detection. The output signals from the detectors are amplified by SQUIDs and further electronics before being digitized and processed by an algorithm that identifies photons and time-correlated photon pairs. Reprinted by permission from Macmillan Publishers Ltd: Nature [75], Copyright 2013.

There are a number of different loopholes, but three of them are considered to be more significant than the others. One is the communication loophole. It is based on the assumption that some unknown communication between both sides measuring the entangled state could establish the observed correlations in the measurement results. As mentioned above, that loophole can be excluded by fast switching, because any classical signal is limited by the speed of light.

The loophole to be mentioned second is the fair-sampling loophole, sometimes also called detection efficiency loophole, which was suggested by Pearle [73]. There, one assumes that nature is really vicious. No experiment detects all particles emitted from a source. The assumption of that loophole is that there is an unknown mechanism in such experiments which is responsible for the fact that the fraction of the events which are detected obeys quantum mechanics. The assumption is also that if one were to be able to detect all events, then a classical picture would result. It is known that this loophole can be closed if more than about two-thirds of all events are detected. The exact value varies and depends on the protocol chosen. Two-thirds just gives an indication of the order of magnitude for two-particle two-bit correlations. If a higher fraction is detected and observed to violate the Bell-type inequality, the results cannot be explained classically anymore. This loophole was closed for the first time by the Wineland group using atoms sitting close together in a trap [74]. For photons, Marissa Giustina and colleagues in my group closed this loophole using transition-edge superconductors with high detection efficiency (figure 20) [75]. At the same time, Paul Kwiat with his group [76] performed an analogous experiment.

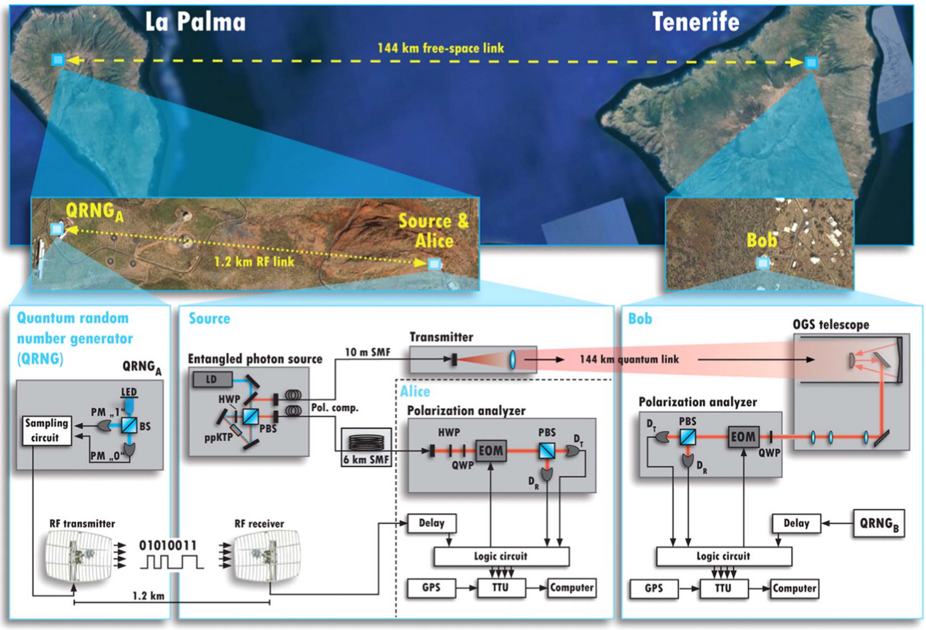

Figure 21. Violation of local realism with freedom of choice. Experimental setup. The Bell experiment was carried out between the islands of La Palma and Tenerife at an altitude of 2400 m. (La Palma). A 405 nm laser diode (LD) pumped a periodically poled potassium titanyl phosphate (ppKTP) crystal in a polarization-based Sagnac interferometer, to generate entangled photon pairs in the ψ_- singlet state. One photon per pair was sent through a 6 km long, coiled optical single-mode fiber (SMF) to Alice (located next to the source). Alice's polarization analyzer consisted of half- and quarter-wave plates (HWP, QWP), an electro-optical modulator (EOM), a polarizing beam splitter (PBS) and two photodetectors (D_T, D_R). A quantum random number generator ($QRNG_A$) located at a distance of 1.2 km, consisting of a light-emitting diode (LED), a 50/50 beam splitter (BS), and two photomultipliers (PMs), generated random bits which were sent to Alice via a 2.4 GHz radio link. The random bits were used to switch the EOM, determining if the incoming photon was measured in the 22.5°/112.5° or the 67.5°/157.5° linear polarization basis. A time-tagging unit (TTU), which was locked to the global positioning system (GPS) time standard, compensated for small drifts up to 10 ns. It recorded every detection event (arrival time, detector channel, and setting information) onto a local hard disk. The other photon was guided to a transmitter telescope and sent through a 144 km optical free-space link to Bob on Tenerife. (Tenerife) The incoming photon was received by the 1 m optical ground station (OGS) telescope of the European Space Agency. At Bob's polarization analyzer (triggered by an equal but independent quantum random number generator $QRNG_B$), the photons were measured in the horizontal (0°)/vertical (90°), or the 45°/135° linear polarization basis. Bob's data acquisition was equivalent to Alice's. (Geographic pictures taken from Google Earth, ©2008 Google, Map Data ©2008 Tele Atlas.) Reproduced with permission from [77].

In my opinion, the conceptually most interesting loophole is the freedom-of-choice one. It is connected to fundamental considerations of possible influences in space-time. The freedom-of-choice assumption states that it is important for the settings of the polarizers on both sides not to be influenced by some unknown common event in their joint past, that is, in the overlap of the backward light cones of the measurement events. The first experiment closing that loophole was performed by Scheidl *et al* (figure 21) [77]. The experiment excluded a specific class of such models, namely that the source, when emitting the entangled pair, also influences the measurements. In that experiment, the communication loophole was also closed.

There have been other experiments closing various loopholes, but given the limited space and the fact that this is a personal account, I am taking the liberty of focusing on works directly related to my group. The year 2015 saw a wave of loophole-free experiments. This seems like a coincidence, but actually, all four groups knew of each other's activities. The first experiment published, which closed the communication and the fair-sampling loophole, was the one by the Hanson group at TU Delft [32]. They, in an experimental tour de force, used

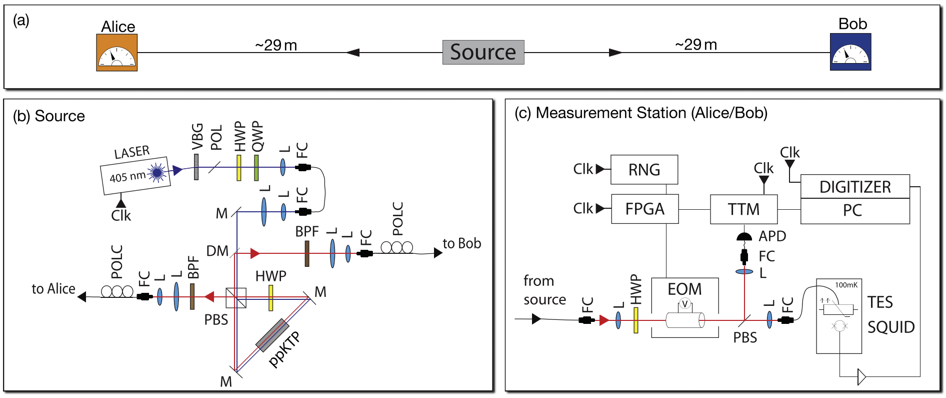

Figure 22. The Vienna loophole-free experiment. (a) Schematic of the setup. (b) Source: the source distributed two polarization-entangled photons between the two identically constructed and spatially separated measurement stations Alice and Bob (distance ≈58 m), where the polarization was analyzed. It employed type-II spontaneous parametric down-conversion in a periodically poled crystal (ppKTP), pumped with a 405 nm pulsed diode laser (pulse length: 12 ns FWHM) at 1 MHz repetition rate. (c) Measurement stations: in each measurement station, one of two linear polarization directions was selected for measurement, as controlled by an electro-optical modulator (EOM), which acted as a switchable polarization rotator in front of a PBS (polarizing beam splitter). Customized electronics (FPGA) sampled the output of a random number generator (RNG) to trigger the switching of the EOM. The transmitted output of the PBS was coupled into a fiber and delivered to the transition-edge sensor TES. The signal of the TES was amplified by a SQUID and additional electronics, digitized, and recorded together with the setting choices on a local hard drive. The laser and all electronics related to switching or recording were synchronized with clock inputs (Clk). Reprinted with permission from [79], Copyright (2015) by the American Physical Society.

entanglement swapping to entangle two spins in diamond, which were separated by a distance of 1280 m. The spins were entangled each with a different photon, and the two photons were brought to a joint measurement station, where they were projected onto an entangled state. Thus, the two spins were also projected onto an entangled state. This is a direct application of entanglement swapping as introduced above. The advantage is that the states of the spins were then observed with high efficiency. In their experiment, they observed a violation of Bell's inequality with more than two standard deviations.

A similar strategy was followed by the group of Weinfurter at the University of Munich [33]. They entangled two atoms sitting in traps separated by 396 m, again by entanglement swapping. Each atom emitted a photon, and they were subject to a Bell state measurement entangling them and therefore entangling the distant atoms. This group also observed a violation of more than two standard deviations.

In December 2015, two experiments were reported simultaneously using down-conversion photon pairs emitted in the process of parametric down-conversion. In the experiment at NIST [78], the photons had the telecom wavelength of 1550 nm and they were detected with fast nanowire detectors. The separation between the measurement stations was 185 m. In that experiment, a p-value of 5.9×10^{-9} was obtained. This is the statistical probability that a local realistic theory could have obtained the data. That experiment was published in the same issue of Physical Review Letters as our experiment, because the NIST group and our group agreed to submit at the same time and have our papers published jointly. Our experiment (figure 22) [79] used 810 nm wavelength photons. It was set up on the second basement level of the Imperial Castle of Vienna, because there, we found the quiet and stable environment necessary to do the experiment. The measurement stations of Alice and Bob were separated by nearly 60 m. In our case, we used transition-edge superconducting detectors, which have nearly 100% intrinsic detection efficiency. Finally, this resulted in a total collection efficiency of the photons arriving in a total photon collection efficiency of 78.6% and 76.2% for

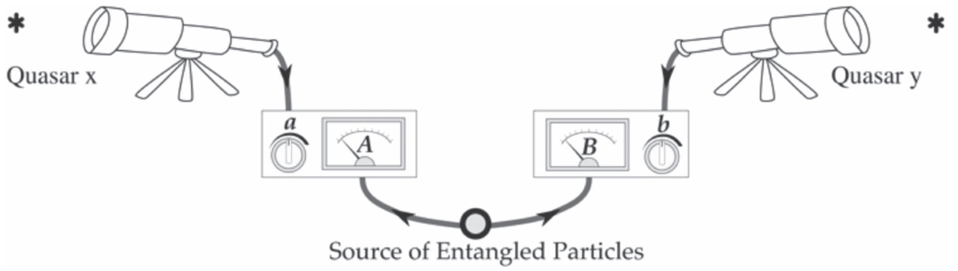

Figure 23. Proposal for a Cosmic Bell experiment. Two telescopes observe distant objects, for example, two quasars. The random fluctuations in the light obtained from the quasars are used to set the polarizers in a Bell inequality experiment. These quasars are probably the most independent sources of randomness one can have in the Universe. Reprinted with permission from [82], Copyright (2014) by the American Physical Society.

Alice and Bob, respectively. The visibility for the entangled states was 99%. The observed violation of a Bell inequality was 11.5 standard deviations, which resulted in a p-value of 3.7×10^{-31}. It is clear that for such a small p-value, any other possible systematic errors would probably be more significant than statistical ones.

All these experiments are relevant from a fundamental point of view. They are also important because they prove that unconditionally secure quantum cryptography is possible. Furthermore, and this is another interesting result of the development in recent years, an additional application emerges. This is based on the fact that in a maximally entangled state, the measurements on one member of the pair are completely random. That again is a consequence of, as mentioned above, Schrödinger's dictum that the individual expectation catalogues are not well defined or, in modern language, the states of the individual entangled particles are maximally mixed. This can be seen by tracing out one of the two photons from a maximally entangled state. This will now be used and applied to create a 'randomness beacon', a project at the National Institute of Standards and Technology NIST [80, 81]. The idea is to create pairs of entangled photons. One of them is just measured to serve as a trigger. So, that way, one knows that the other photon has been created. Polarization measurement or another suitable measurement of a sequence of these photons produces a sequence of random numbers. Such numbers have important applications in many algorithms. They could for example also be used to digitally sign documents. NIST intends to publish these continuous sequences on the internet.

A loophole which would benefit from more tests in the future is the freedom-of-choice loophole. It has thus far only been tested for rather limited causes in the common past of both detectors. One might therefore ask what the most independent possible sources for randomness could be which had no chance at all to interact or communicate with each other. One therefore has to look for cosmic sources, which are widely separated from each other. A specific possibility is quasars located at opposite extremes in the Universe (figure 23) [82]. It turns out that if the sources are far enough away, their backward light cones have no causal overlap after the end of cosmic inflation [83]. The inflation itself dilutes any initial information from the period of the Big Bang by a factor of the order of at least 10^{-40}. Such sources of randomness would be rather independent.

A first Cosmic Bell test experiment was performed recently [84]. That experiment in the city of Vienna used two telescopes pointing to stars in our Milky Way galaxy. The entangled photon source was separated from one measurement station by 557 m and from the other by 1149 m. Fluctuations in the color spectrum received from the two stars served to set the respective polarization measurement. That experiment allowed to push back by ~600 years the most recent time by which any local realistic effect could have influenced the observed Bell violation.

This experiment sets the stage for further experiments performed with larger telescopes pointed towards quasars. For conceptual discussions relating to these kinds of experiments, see [84] and references therein.

Communication with higher alphabets, entanglement in new dimensions

Thus far, we have discussed quantum communication and correlation experiments where the photons are only defined as two-state systems. An important challenge is to go beyond that limitation. This can be done utilizing systems of states with higher dimensions for single photons. There are essentially two possibilities. One of these possibilities is to use multi-mode communication, that is, many spatial single-mode states, or many frequency modes, in an analogous way, as is done in classical communication. In one such example [85], we used in-fiber and on-chip integrated technologies, as is standard in today's telecommunication industry. Using these methods, we explicitly realized all possible unitary operations for two entangled qutrits, which form a nine-dimensional quantum system.

Another distinct possibility takes advantage of orbital angular momentum states [86], which provide a discrete Hilbert space of in-principle infinite dimension. Once the paper by Allen *et al* came out, there arose a discussion whether the orbital angular momentum states thus created could be entangled. Particularly, there was even an experiment suggesting that orbital angular momentum is not conserved in the down-conversion process [87]. As always, this triggered my curiosity, and we were able to show that not only is orbital angular momentum conserved in the process, but that the emerging states are indeed entangled [88]. The result opened up new avenues for the study of entanglement in very high dimensions. For that experiment, again, we had to invent the tools necessary. In particular, no one knew how to identify arbitrary OAM states of individual light quanta including their superpositions. The solutions we found, as always, were rather simple, just a suitable combination of phase modulators and mono-mode fibers which support the propagation of a single Gaussian mode [88].

I would like to mention another pleasant surprise: the paper demonstrating entanglement of orbital angular momentum modes has become one of my most cited papers [88]. Once more, very curiously, something interesting happened. I gave up working with OAM states because of limited resources in my group and even stopped following the literature in the field. Some time later, I was invited to a conference on OAM states and to my big surprise, I saw there that a very active field had emerged. Thus with my group I became interested in taking up these topics once more, specifically focusing on higher dimensions. In the course of this renewed research, we were able to demonstrate some very interesting features. In one experiment, we demonstrated that very high quantum numbers can be entangled with each other. In our first experiment of that kind (figure 24) [89] we were able to demonstrate entanglement of photons carrying $+300\hbar$ and $-300\hbar$ units of angular momentum. In a more recent experiment, we extended this to quantum numbers higher than 10 000 [90].

The question of how large the quantum numbers can be that are entangled with each other is sometimes seen as related to the quantum–classical transition. Our experiments show that even for very large quantum numbers, one can still have a qubit, and the limitation is more a practical one than a limitation in principle.

Another somewhat similar, but independent, question is also interesting. How many quantum states can be entangled at the same time between two particles? For example, in the usual Bell experiment with only two states, both photons are qubits, i.e. defined in a two-dimensional Hilbert space, likewise in the original GHZ state, the photons are also qubits. In our experiment to show entanglement

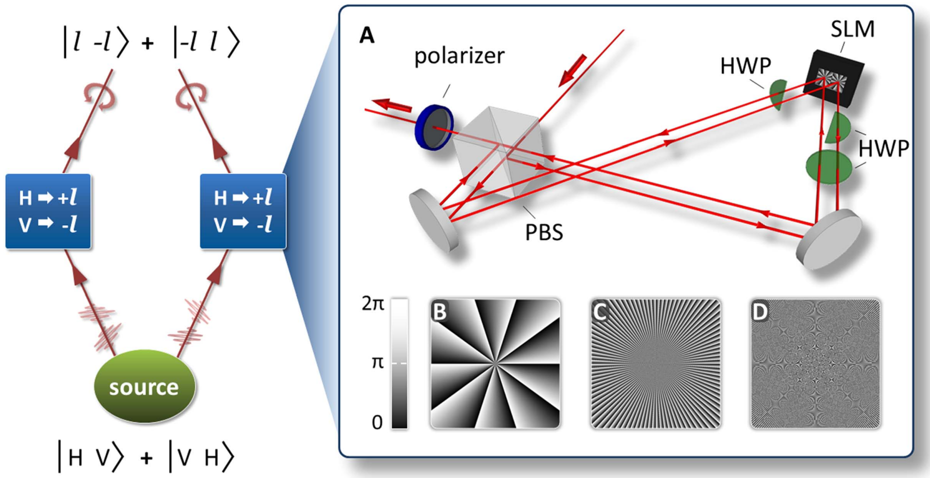

Figure 24. Observation of entanglement of very high angular momenta. Left: schematic sketch of the setup. Polarization entanglement is created in a parametric down-conversion process (source—oval green box) and afterwards transferred to modes with high quanta of OAM (transfer setup—rectangular blue boxes). The inset (A) shows the experimental layout for one of the two identical transfer setups where the photon is split by polarization (PBS) and its spatial mode is transformed to a higher order Laguerre–Gauss mode by a spatial light modulator (SLM). Half-wave plates (HWP) in the paths ensure that the SLM works optimally and the output is separated from the input. A polarizer (blue) projects the photon to diagonal polarization and completes the transfer. Three phase patterns, $l = 10$ (B), $l = 100$ (C) and $l = 300$ (D), visualize the increasing complexity of the structure and the limitations because of emergence of a Moiré pattern due to the finite resolution of the SLM. From [89]. Reprinted with permission from AAAS.

between many dimensions [91], we again used orbital angular momentum states, where each photon was defined in a Hilbert space with dimensions much larger than 100. Each photon was not just a qubit, but had amplitudes in more than 160 discrete dimensions. For details, see [91]. Having developed a novel entanglement witness, we were able to confirm that at least 100 dimensions of each photon were entangled with at least 100 dimensions of the other photon. It is apparent that this experiment, and the one just mentioned before, open up applications using high dimensions for photons to carry more than one bit of information. This might be important in future quantum communication networks.

Another question is whether such orbital angular momentum states in higher dimensions can indeed be used for long-distance communication. Again, there were arguments in the literature that this would not be possible (see references in [92]). The standard argument was that fluctuations in the atmosphere would disturb the wave-fronts of these states in such a way that they cannot be identified anymore at distances beyond about 1 km. This again challenged us, and we came up with a method using superpositions of angular momentum states which carry characteristics particularly related to the singularities of the modes. Contrary to immediate intuition, there are properties of superpositions which are more stable against atmospheric fluctuations than the states themselves. Recently we were able to demonstrate that such a classical communication is indeed possible over a distance of 3 km (figure 25) [92].

While the experiment just mentioned is confirming that classical communication is possible using these doughnut modes, most recently, we were able to demonstrate that even entangled states of such photons survive the transmission over a free-space channel across a heavily populated area of the city of Vienna [93]. It is obvious that such experiments open up novel communication ideas, particularly when combined with entanglement swapping and employed in quantum repeaters. Even more recently in a proof-of-principle experiment we

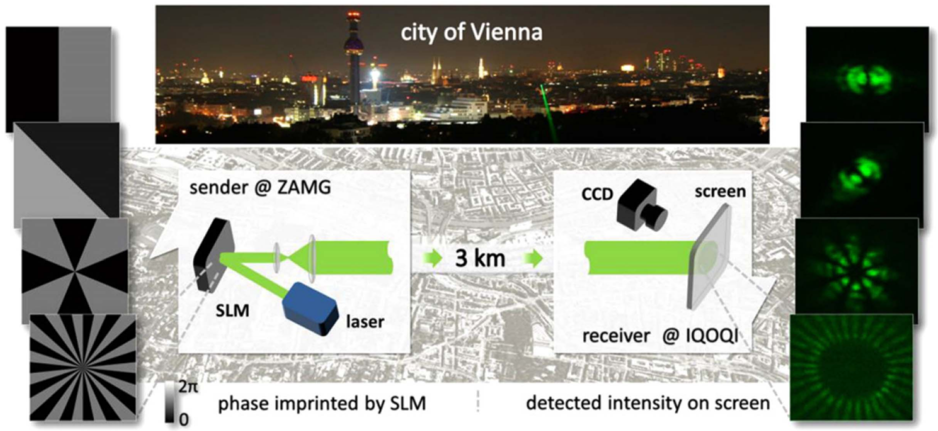

Figure 25. Long-distance free-space communication with orbital angular momentum states of light. The three kilometer free-space link was established in the city of Vienna, from ZAMG (Zentralanstalt für Meteorologie und Geodynamik, Central Institute for Meteorology and Geodynamics) to our institute IQOQI. Top: picture of an alignment laser from IQOQI to ZAMG, captured at ZAMG. Left: the sender modulates a 532 nm laser with an SLM. The different phase holograms that modulate the beam are shown. Right: at the receiver, we observe the transmitted modes and record them with a CCD camera. The images correspond to the modulated phases on the left. By analyzing the observed images, we characterize the atmospheric stability of the OAM modes and use them for transmitting real information. (Geographic pictures taken from Google Earth, ©2014 Google, Cnes/Spot Image, DigitalGlobe.) Reproduced from [92] CC BY 3.0. See there for details.

demonstrated classical communication with OAM states over 143 km between La Palma and Tenerife [94]. For a view of the telescope, see figure 26.

Concluding comments and conceptual considerations

We might now come back to Albert Einstein and his question mentioned above: What is light? Late in his life, Einstein gave his own summary [95].

> *All the fifty years of conscious brooding have brought me no closer to answer the question, 'What are light quanta?' Of course today every rascal thinks he knows the answer, but he is deluding himself*[4].

Naturally, one could today say that light quanta are the quantized excitations of the electromagnetic field, but obviously, Einstein was after a deeper explanation. Coming back to the beginnings of quantum physics, it is an interesting lesson to learn that new ideas obviously often have difficulty being accepted. A striking point in case is the proposal written by Planck, Nernst, Rubens and Warburg for Einstein's membership in the Prussian Academy of Sciences. After giving the arguments why Einstein should be appointed to the Prussian Academy, it says:

> *The fact, that in his speculations he occasionally went too far, for example, in is hypothesis of light quanta, should not too heavily be held against him, because without occasionally taking a risk, even in the most exact natural sciences, no real innovation can be introduced*[5].

Besides maybe causing us to smile today, this also contains a message of great hope for the sciences. That letter was written in 1913, and in 1922, Albert Einstein received his Nobel Prize for exactly that idea. This fact—namely, that scientists are able to abandon fundamental strongly held positions in the face of evidence—

[4] Translation public domain.
[5] Translation AZ. I thank Issachar Unna for making excerpts of the original German version of the document from the Einstein Archives available to me.

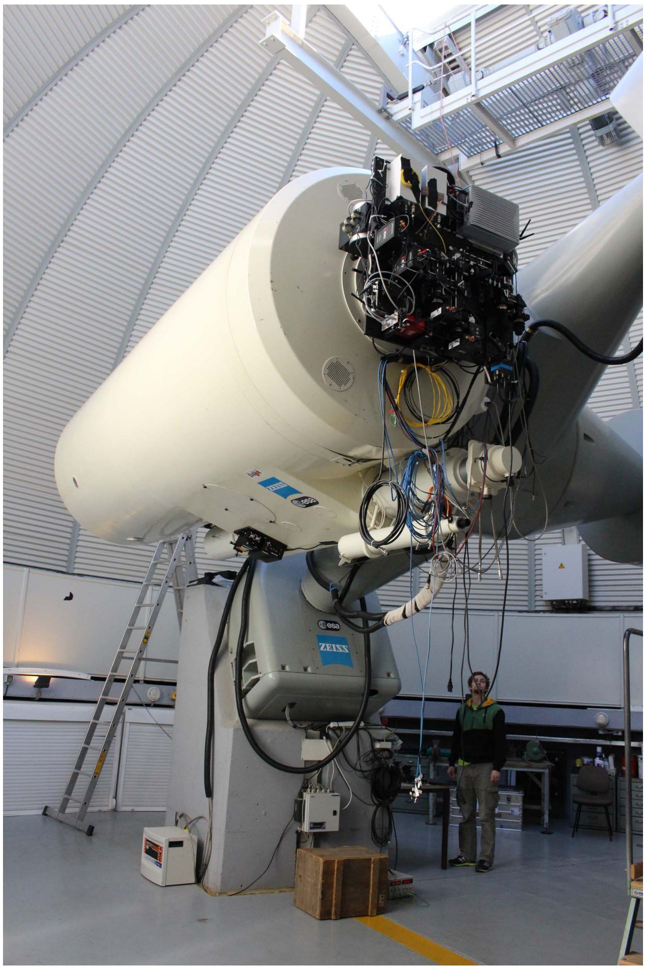

Figure 26. The telescope at OGS (Optical Ground Station) established on Tenerife. At the back of the telescope, one sees the receiver station for the entangled photons to be used in the experiment to test intercontinental quantum communication in cooperation with the Chinese Academy of Sciences. The incoming photons from the Chinese QUESS satellite MICIUS are received by the telescope and then coupled through glass fibers into the detection setup. The picture also shows Johnny Handsteiner, the PhD student working on the project. Photo: Thomas Herbst. Copyright Austrian Academy of Sciences.

is one of the big strengths of doing scientific research, and it is one of its most rewarding and enjoyable features.

While Einstein's critique of quantum mechanics turned out to be incorrect in various cases, particularly in his criticisms of randomness and of entanglement, he should be given credit for having *emphasized* these interesting features of quantum mechanics. I trust that he would have enjoyed the fact that these concepts, which he disliked, have now led to interesting applications. After all, his first position was at the Swiss Patent Office and there, he even patented some inventions of his own.

As I mentioned in the beginning, I was very surprised when these applications emerged as a result of such fundamental questions. Developments such as this have continued to amaze us throughout the history of physics.

One might ask in general what we have learned from these many experiments and whether there is a joint 'morale' to be found in the very personal story which I present in this paper. When I, more than 40 years ago, had the privilege to start working on the foundations of quantum mechanics, this was just out of curiosity. I had learned quantum mechanics from some very good and interesting textbooks available at that time. This study was delightful because the incredible mathematical beauty of quantum theory had a deep impact on me. In parallel, I was also impressed by the incredible mathematical accuracy with which the theory was confirmed in a multitude of experiments. But there were two points which caught my fancy and aroused my interest even more.

Firstly, there was the observation that there did not seem to be a consensus about the interpretation of quantum theory. By this, I do not mean interpretation in the sense of the Born Interpretation, which connects the theoretical predictions with experimental observations, but rather the interpretation of what this might mean for our view of the world (Weltanschauung) or maybe even for our position in the world (for a discussion, see [96]). Secondly, there was very little experimental evidence for confirming the predictions of quantum mechanics for individual particles or individual quantum systems, like superposition for individual particles or quantum entanglement etc.

This way, I drifted into studying predictions for individual systems in detail, and I consider myself very lucky that, because I worked in the group of Helmut Rauch in Vienna, I was encouraged to pursue these ideas and was able to slowly move into experiments on the foundations of quantum mechanics. Back then, there were rather diffuse views around about the interpretation and meaning of quantum physics for individual systems. I still remember that when I gave talks about some of the neutron experiments (which were initiated by Helmut Rauch), even famous senior members of the community came up to us and expressed their amusement: 'superposition really works out that way, particle per particle?' My answer was: 'What else did you expect?'

At that time, there was significant disagreement, for example about whether quantum mechanics describes individual systems or only statistical ensembles, what the role of the environment is, or what quantum nonlocality really implies. The experience of many groups world-wide with a multitude of quantum phenomena for individual systems has also led to a much better understanding of fundamental issues of quantum mechanics. It is now commonly accepted and understood that nature cannot be described in a local way, that entanglement is a fundamental part of our description of the world, that objective randomness exists, and many more. The viewpoint that quantum physics describes the behavior of individual quantum systems if seen in the right way has become broadly accepted. We also have a much better understanding of the role of the environment and of decoherence, and many new phenomena were discovered on a fundamental level. For many, the emerging viewpoint now is that information plays a very fundamental role in the understanding of quantum mechanics. I personally see this as a confirmation and further development of the Copenhagen Interpretation of quantum mechanics as expressed for example by Werner Heisenberg, who said that the quantum state is a representation of our knowledge, and Erwin Schrödinger, who in his famous 1935 paper on the present situation in quantum mechanics [7] talked about the quantum state representing expectation catalogues. For a discussion of some of the issues, see [97, 98]. But evidently, the discussion has not been settled yet, as evidenced for example by [99].

As mentioned already above, to the great surprise of everyone who had the luck to come early into the field, applications arose which go beyond any of our wildest dreams at the time. I personally feel there is a very good chance that someday, quantum information technologies will replace traditional information technologies, if not completely, then in significant ways.

A typical most interesting recent example is the emergence of quantum experiments at space scale [100]. In 2016, the first quantum satellite was launched by the Chinese Academy of Sciences [101]. A specific vision for the future is a world-wide quantum internet, where ground stations are directly connected to quantum communication links using glass fibers, and over long distances and intercontinentally via quantum satellite networks.

Certainly, nobody in the early days of experiments on individual systems to test the foundations of quantum mechanics had even the faintest idea that today there are huge groups world-wide with altogether probably thousands of scientists working on possible applications. This once more is a confirmation of a pattern observed very often in the history of physics or science in general for that matter. The deepest and most important applications are not found by searching for applications but by doing fundamental research and thus opening completely new doors.

In conclusion, I would like to stress that I consider myself extremely privileged to have been able to work on such questions. The results which I achieved with my group would not have been possible without the many young and spirited minds (PhD and diploma students as well as young Postdocs) I was able to work with over many years. To all of them goes the credit for these achievements.

As I mentioned at the beginning, this paper represents an account of my personal path. I ask for understanding that because of this focus of the paper and certainly also for limitations of space, it is not possible to include even just the most beautiful and important achievements of many groups and colleagues world-wide. Having become part of such a stimulating international community is another privilege of my life.

Acknowledgments

This work has been supported over the years by many institutions, most importantly, the Austrian Science Fund, the European Commission, the European Space Agency, the Austrian Research Promotion Agency, the US National Science Foundation and many others.

References

[1] Wikipedia article on the International Year of Light 2015 https://en.wikipedia.org/wiki/International_Year_of_Light
[2] Wikipedia article on Ibn Al-Haytham https://en.wikipedia.org/wiki/Alhazen
[3] Fresnel A 1900 Memoir on the diffraction of light *The Wave Theory of Light—Memoirs by Huygens, Young and Fresnel* (New York: American Book Company) pp 79–145
[4] Maxwell J C 1865 A dynamical theory of the electromagnetic field *Phil. Trans. R. Soc.* **155** 459–512
[5] Einstein A 1905 Über einen die Erzeugung und Verwandlung des Lichtes betreffenden heuristischen Gesichtspunkt *Ann. Phys.* **322** 132–48
Arons A B and Peppard M B 1965 *Am. J. Phys.* **33** 367 (transl.)
[6] Einstein A, Podolsky B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777
[7] Schrödinger E 1935 Die gegenwärtige Situation in der Quantenmechanik *Naturwissenschaften* **23** 823–8
Schrödinger E 1980 The present situation in quantum mechanics *Proc. Am. Phil. Soc.* **124** 323–38 (transl.)
[8] Rauch H, Treimer W and Bonse U 1974 Test of a single crystal neutron interferometer *Phys. Lett.* **47A** 369
[9] Bauspiess U *et al* 1975 Verification of coherent spinor rotation of fermions *Phys. Lett.* A **54** 425–7
[10] Clauser J F and Horne M A 1974 Experimental consequences of objective local theories *Phys. Rev.* D **10** 526–35
[11] Clauser J F *et al* 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880
[12] Wikipedia article on Clifford Shull https://en.wikipedia.org/wiki/Clifford_Shull
[13] Horne M A and Zeilinger A 1985 A Bell-type EPR experiment using linear momenta *Symp. on the Foundations of Modern Physics* (Joensuu: World Scientific) pp 435–9
[14] Horne M A, Shimony A and Zeilinger A 1989 Two-particle interferometry *Phys. Rev. Lett.* **62** 2209–12

[15] Burnham D C and Weinberg D L 1970 Observation of simultaneity in parametric production of optical photon pairs *Phys. Rev. Lett.* **25** 84
[16] Rarity J G and Tapster P R 1990 Experimental violation of Bell's inequality based on phase and momentum *Phys. Rev. Lett.* **64** 2495
[17] Greenberger D M, Horne M A and Zeilinger A 1989 Going beyond Bell's theorem *Bell's Theorem, Quantum Theory, and Conceptions of the Universe* (Dordrecht: Kluwer) pp 69–72
[18] Greenberger D *et al* 1990 Bell's theorem without inequalities *Am. J. Phys.* **58** 1131
[19] Kwiat P *et al* 1995 New high-intensity source of polarization-entangled photon pairs *Phys. Rev. Lett.* **75** 4337–41
[20] Bouwmeester D *et al* 1999 Observation of three-photon Greenberger–Horne–Zeilinger entanglement *Phys. Rev. Lett.* **82** 1345
[21] Pan J-W *et al* 2000 Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement *Nature* **403** 515–9
[22] Mattle K *et al* 1996 Dense coding in experimental quantum communication *Phys. Rev. Lett.* **76** 4656–9
[23] Kwiat P *et al* 1996 Polarization-entangled photons and quantum dense coding *Opt. Photon. News* **7** 14–5
[24] Bennett C H and Wiesner S J 1992 Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states *Phys. Rev. Lett.* **69** 2881
[25] Bennett C *et al* 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[26] Bouwmeester D *et al* 1997 Experimental quantum teleportation *Nature* **390** 575–9
[27] Ma X-S *et al* 2012 Quantum teleportation over 143 kilometres using active feed-forward *Nature* **489** 269–73
[28] Yin J *et al* 2012 Quantum teleportation and entanglement distribution over 100-kilometre free-space channels *Nature* **488** 185–8
[29] Żukowski M *et al* 1993 'Event-ready-detectors' Bell experiment via entanglement swapping *Phys. Rev. Lett.* **71** 4287–90
[30] Bell J S 1987 *Speakable and Unspeakable in Quantum Mechanics* (Cambridge: Cambridge University Press)
[31] Pan J-W *et al* 1998 Experimental entanglement swapping: entangling photons that never interacted *Phys. Rev. Lett.* **80** 3891–4
[32] Hensen B *et al* 2015 Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres *Nature* **526** 682–6
[33] Rosenfeld W *et al* 2016 *Presentation at the 46th Winter Colloquium on the Physics of Quantum Electronics (PQE) (Snowbird, UT)* arXiv:1611.04604 [quant-ph]
[34] Herbst T *et al* 2015 Teleportation of entanglement over 143 km *Proc. Natl Acad. Sci.* **112** 14202–5
[35] Duan L M *et al* 2001 Long-distance quantum communication with atomic ensembles and linear optics *Nature* **414** 413–8
[36] Pan J-W *et al* 2003 Experimental entanglement purification of arbitrary unknown states *Nature* **423** 417–22
[37] Wiesner S 1983 Conjugate coding *Sigact News* **15** 78
[38] Wooters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3
[39] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Piscataway, NJ: IEEE) pp 175–9
Bennett C H and Brassard G 2014 Quantum cryptography: public key distribution and coin tossing *Theor. Comput. Sci.* **560** 7–11 (reprinted)
[40] Jennewein T *et al* 2000 Quantum cryptography with entangled photons *Phys. Rev. Lett.* **84** 4729–32
[41] Naik D S *et al* 2000 Entangled state quantum cryptography: eavesdropping on the Ekert protocol *Phys. Rev. Lett.* **84** 4733–6
[42] Tittel W *et al* 2000 Quantum cryptography using entangled photons in energy-time Bell states *Phys. Rev. Lett.* **84** 4737–40
[43] Freedman S J and Clauser J F 1972 Experimental test of local hidden-variable theories *Phys. Rev. Lett.* **28** 938
[44] Aspect A, Dalibard J and Roger G 1982 Experimental test of Bell's inequalities using time-varying analyzers *Phys. Rev. Lett.* **49** 1804
[45] Weihs G *et al* 1998 Violation of Bell's inequality under strict Einstein locality conditions *Phys. Rev. Lett.* **81** 5039–43
[46] Wikipedia article on Malevich's Black Square https://en.wikipedia.org/wiki/Black_Square_%28painting%29
[47] Wigner E P 1963 The problem of measurement *Am. J. Phys.* **31** 6–15
[48] Lewis G N 1926 The conservation of photons *Nature* **118** 874–5
[49] Einstein A 1917 Zur Quantentheorie der Strahlung *Phys. Z.* **18** 121–8
[50] Einstein A 1916 Strahlungs-Emission und -Absorption nach der Quantentheorie *Verh. Dtsch. Phys. Ges.* **18** 318–23

[51] Born M 1983 Letter from Albert Einstein to Max Born *Physik im Wandel meiner Zeit* (Berlin: Springer) p 228
[52] Schrödinger E 1935 Discussion of probability relations between separated systems *Math. Proc. Camb. Phil. Soc.* **31** 555–63
[53] Zeilinger A 1999 A foundational principle for quantum mechanics *Found. Phys.* **29** 631–43
[54] Benioff P 1980 The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines *J. Stat. Phys.* **22** 563–91
[55] Deutsch D 1985 Quantum theory, the Church–Turing principle and the universal quantum computer *Proc. R. Soc.* A **400** 97–117
[56] Feynman R P 1982 Simulating physics with computers *Int. J. Theor. Phys.* **21** 467–88
[57] Shor P 1997 Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer *SIAM J. Sci. Stat. Comput.* **26** 1484–509
[58] Knill E, Laflamme R and Milburn G J 2001 A scheme for efficient quantum computation with linear optics *Nature* **409** 46–52
[59] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
[60] Borges J L 1941 La biblioteca de Babel *El Jardín de senderos que se bifurcan* (Buenos Aires: Sur)
[61] Pan J-W *et al* 2001 Entanglement purification for quantum communication *Nature* **410** 1067–70
[62] Sanaka K, Resch K J and Zeilinger A 2006 Filtering out photonic fock states *Phys. Rev. Lett.* **96** 083601
[63] Gasparoni S *et al* 2004 Realization of a photonic controlled-NOT gate sufficient for quantum computation *Phys. Rev. Lett.* **93** 020504
[64] Walther R *et al* 2005 Experimental one-way quantum computing *Nature* **434** 169–76
[65] Broadbent A, Fitzsimons J and Kashefi E 2009 Universal blind quantum computation *Proc. 50th Annual IEEE Symp. on Foundations of Computer Science* (Piscataway, NJ: IEEE) pp 517–26
[66] Barz S *et al* 2013 Experimental verification of quantum computation *Nat. Phys.* **9** 727–31
[67] Barz S *et al* 2012 Demonstration of blind quantum computing *Science* **335** 303–8
[68] Yao X-C *et al* 2012 Observation of eight-photon entanglement *Nat. Photon.* **6** 225–8
[69] Huang Y-F *et al* 2011 Experimental generation of an eight-photon Greenberger–Horne–Zeilinger state *Nat. Commun.* **2** 546
[70] Wang *et al* 2016 Experimental ten-photon entanglement *Phys. Rev. Lett.* **117** 210502
[71] Bourennane M 2016 private communication
[72] Pan J-W *et al* 2012 Multiphoton entanglement and interferometry *Rev. Mod. Phys.* **84** 777
[73] Pearle P M 1970 Hidden-variable example based upon data rejection *Phys. Rev.* D **2** 1418–25
[74] Rowe M A *et al* 2001 Experimental violation of a Bell's inequality with efficient detection *Nature* **409** 791–4
[75] Giustina M *et al* 2013 Bell violation using entangled photons without the fair-sampling assumption *Nature* **497** 227–30
[76] Christensen B G *et al* 2013 Detection-loophole-free test of quantum nonlocality, and applications *Phys. Rev. Lett.* **111** 130406
[77] Scheidl T *et al* 2010 Violation of local realism with freedom of choice *Proc. Natl Acad. Sci.* **107** 19708–13
[78] Shalm L K *et al* 2015 Strong loophole-free test of local realism *Phys. Rev. Lett.* **115** 250402
[79] Giustina M *et al* 2015 Significant-loophole-free test of Bell's theorem with entangled photons *Phys. Rev. Lett.* **115** 250401
[80] Homepage of the NIST Randomness Beacon https://beacon.nist.gov
[81] Nam S W 2016 *Presentation at the 46th Winter Colloquium on the Physics of Quantum Electronics (PQE) (Snowbird, UT)*
[82] Gallicchio J, Friedman A S and Kaiser D I 2014 Testing Bell's inequality with cosmic photons: closing the setting-independence loophole *Phys. Rev. Lett.* **112** 110405
[83] Guth A 2015 private communication
[84] Handsteiner J *et al* 2017 Cosmic Bell test: measurement settings from milky way stars *Phys. Rev. Lett.* **118** 060401
[85] Schaeff C *et al* 2015 Experimental access to higher-dimensional entangled quantum systems using integrated optics *Optica* **2** 523–9
[86] Allen L *et al* 1992 Orbital angular momentum of light and the transformation of Laguerre–Gaussian laser modes *Phys. Rev.* A **45** 8185–9
[87] Arlt J *et al* 1999 Parametric down-conversion for light beams possessing orbital angular momentum *Phys. Rev.* A **59** 3950–2
[88] Mair A *et al* 2001 Entanglement of the orbital angular momentum states of photons *Nature* **412** 313–6
[89] Fickler R *et al* 2012 Quantum entanglement of high angular momenta *Science* **338** 640–3
[90] Fickler R *et al* 2016 Quantum entanglement of angular momentum states with quantum numbers up to 10010 *Proc. Natl Acad. Sci.* **113** 13642–7
[91] Krenn M *et al* 2014 Generation and confirmation of a (100 $\times$ 100) dimensional entangled quantum system *Proc. Natl Acad. Sci.* **111** 6243–7

[92] Krenn M *et al* 2014 Communication with spatially modulated light through turbulent air across Vienna *New J. Phys.* **16** 113028
[93] Krenn M *et al* 2015 Twisted photon entanglement through turbulent air across Vienna *Proc. Natl Acad. Sci.* **112** 14197–201
[94] Krenn M *et al* 2016 Twisted light transmission over 143 kilometers *Proc. Natl Acad. Sci.* **113** 13648–53
[95] Klein M J 1970 The first phase of the Bohr-Einstein dialogue *Hist. Stud. Phys. Sci.* **2** iv–9 (*Letter to M Besso*, by A Einstein)
[96] Zeilinger A 1996 On the interpretation and philosophical foundation of quantum mechanics *Vastakohtien todellisuus, Festschrift for K V Laurikainen* (Helsinki: Helsinki University Press) pp 167–78
[97] Zeilinger A 2005 Happy centenary, photon *Nature* **433** 230–8
[98] Zeilinger A 2005 The message of the quantum *Nature* **438** 743
[99] Schlosshauer M, Kofler J and Zeilinger A 2013 A snapshot of foundational attitudes toward quantum mechanics *Stud. Hist. Phil. Mod. Phys.* **44** 222–30
[100] Wikipedia article on quantum experiments at space scale https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale
[101] News article 'China Focus: China's space satellites make quantum leap' on Xinhuanet http://news.xinhuanet.com/english/2016-08/16/c_135604287.htm