QUANTUM INFORMATION FROM THE FOUNDATIONS TO A NEW TECHNOLOGY (HERZBERG MEMORIAL PUBLIC LECTURE 2012)

BY ANTON ZEILINGER

Anton Zeilinger
<anton.zeilinger@
univie.ac.at>,
University of Vienna,
Austrian Academy
of Sciences.

When I first learned quantum mechanics, I was immediately fascinated by the field. Most impressive was its immense mathematical beauty, which is particularly striking in the Dirac Formalism. Or, if one looks at the Schrödinger Equation: How is it possible that very few mathematical symbols comprise such a breadth of phenomena, all the way from subatomic particles via solid state systems to the physics of the early universe?

But I was also immediately attracted by the fact that apparently, there were problems in understanding what the theory means in a deep sense. Even well-known and famous textbooks somehow tried to avoid the subject of interpretation or analyzed it in a very formal manner. Very soon, I realized that there were actually discussions going on about the philosophical and conceptual consequences of quantum mechanics. But the positions often disagreed strongly.

INTRODUCTORY REMARKS

I am very grateful for the invitation to give the 2012 Herzberg Memorial Lecture at the occasion of the Annual Meeting of the Canadian Association of Physicists and I am glad to give the lecture in a country where my field of research – foundations of quantum mechanics and quantum information science – has developed very strongly in recent years. This has put Canada among the top countries in the world in the field. It is a particular pleasure to give the lecture here in Calgary. I had the opportunity to see the activities in quantum computing and quantum information science evolve here from the very beginning to the present status. Today the Institute for Quantum Information Science under the leadership of Barry Sanders boasts a unique combination of people with very diverse backgrounds, which is characteristic for the field of quantum information science and certainly important for its future development.

I was totally fascinated by the predictions of quantum mechanics in many ways, particularly by the predictions about the behavior of individual quantum particles. So very soon, already as a student, I became interested in the question whether it would be possible to perform such experiments some day in the laboratory.

So, having worked on my PhD thesis under Helmut Rauch in Vienna on investigations of magnetism using polarized neutron scattering, I was very happy when he invited me to join his pioneering work on neutron interferometry. My first contribution to the field was my participation in the experiment demonstrating that the state of a quantum system rotated by 360 degrees picks up a phase factor of -1. That experiment was done in parallel also by the group of Sam Werner in Missouri. This result is probably one of the first in the foundations of quantum mechanics which has later been applied in quantum information science. Today, the phase change of a quantum state upon a complete Rabi cycle is ubiquitous, for example in quantum computation. But I am jumping ahead.

The story is quickly told. When quantum mechanics was invented in the first quarter of the 20th century, it was immediately clear that it leads to new counter-intuitive predictions for the behavior of individual quantum systems. This was already realized by Max Planck himself. For many years, he searched unsuccessfully for another derivation of the black body radiation, which would not use the quantum concept with the built-in discontinuity that Planck disliked.

Likewise, Einstein – after he had introduced the concept of particles of light (later by Lewis called photons) – soon realized the tension between the particle concept and interference. In the 1909 meeting of the Gesellschaft Deutscher Naturforscher und Ärzte in Salzburg, he analyzed the question of whether a double-slit interference pattern would arise if single photons would pass one by one through the apparatus. His prediction was to the negative, as in his opinion, each particle has to go through either slit only. It therefore cannot carry information whether the other one is open or not. He expected interference to be due to many particles passing through the slits. When they meet at the observation screen, they jointly carry the information that both slits are open. Thus, the interference pattern can arise for high intensities only.

This is clearly one case where Einstein was wrong, as single-particle interference has today been demonstrated in many experiments, not only with photons, but also with systems such as fullerenes or even larger molecules. Quantum interference of states of individual systems is at the heart of many quantum computation protocols today.

Another point which had worried Einstein is the randomness of individual quantum events. It is remarkable that as early as 1917, he expressed his discomfort about the new role randomness plays in quantum physics. So he had realized already then that – while in classical physics randomness is a measure of ignorance – in quantum physics the randomness of the individual event is fundamental and irreducible. It is quite remarkable that he found this before the full theory had been developed by Heisenberg and Schrödinger, which came in 1925 and 1926. In a letter to Max Born of 4.12.1926, Albert Einstein explicitly said: "In any case, I am convinced that God does not play dice." Actually, he used the word "der Alte", the old guy, for God, expressing some special kind of familiarity.

Today, the randomness of individual quantum events is at the heart of quantum random number generators, which by all standards are the best available random number generators by any method, be it physical or mathematical. In my group, particularly with Thomas Jennewein, now at the Institute for Quantum Computing (IQC) at the University of Waterloo, we developed a random number generator which is based on a 50/50 beam splitter (see Figure 1). The random numbers generated that way pass all available tests, and a company to whom we had sent a couple of CDs full of these numbers told us that these were the best random numbers they had ever seen. So this is another case of a fundamental quantum phenomenon in an information context. Good random numbers are useful in many applications.

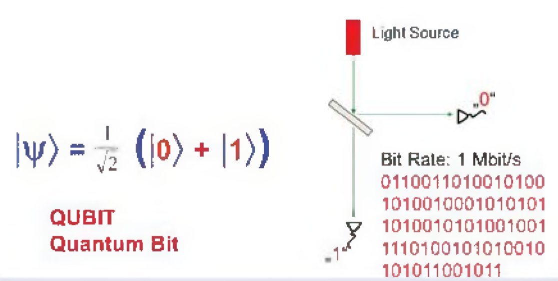

Fig. 1 Generation of random numbers using a 50/50 beam splitter [1]. An incoming light beam passes the half-silvered mirror. Half of the intensity is reflected, the other half is transmitted. Yet, any specific individual photon can only trigger either one of the two detectors. Which detector is triggered by a specific photon is completely random, thus giving randomly the bit value "0" or "1". Therefore, with many photons passing, one obtains a perfect sequence of random numbers. Actually, after the beam splitter, each individual photon is in a superposition of equal amplitudes "0" and "1". This is the simple case of a qubit (a quantum bit). Only upon detection, the quantum state collapses into either "0" or "1".

With the development of the full quantum theory in 1925 and 1926 by Heisenberg and Schrödinger, the debate about its meaning and its philosophical foundation gained significant momentum. Maybe best known is the debate between Bohr and Einstein which took place mainly at the occasion of conferences, for example the 1927 and 1930 Solvay Meetings in Brussels. The essence of these discussions was basically that Albert Einstein requested physics to describe a reality which exists independent of the observer and Niels Bohr held the position that physics primarily concerns what can be said about nature and that all conclusions about reality are indirect.

The workhorse tool of many of these discussions, including the Bohr-Einstein debate, were gedanken experiments which were invented to analyze very clearly the behavior of individual quantum systems in specific situations. It is part of the history of the field of quantum information that many of these gedanken experiments became possible in the 1970s due to technological progress. The main reasons were on the one hand the development of the laser, making possible experiments with photons, particularly on photonic entanglement, and on the other hand the construction of high-flux nuclear reactors, which provided neutron sources, making possible experiments in neutron interferometry.

The direct discussion between Einstein and Bohr was stopped by the tragic political developments in Germany. Einstein immediately decided to emigrate to the United States. But in 1935, a momentous indirect discussion happened. Einstein, together with Boris Podolsky and Nathan Rosen (EPR), published a paper [2] where they suggest that quantum mechanics is incomplete. This was the first paper where the fact that quantum correlations can be stronger than classical correlations was explicitly discussed. Erwin Schrödinger in the same year, in two papers, one in German and one in English, coined the notion of entanglement (in German "Verschränkung") to describe this new feature of quantum correlations.

Considering two systems which are entangled both in position and in momentum, EPR argued that quantum mechanics is incomplete because, based on the measurement of one of the two quantum systems, one can predict with certainty the corresponding value for the other one. So, if one measures the momentum of one system, one can predict the momentum of the other one with certainty. If one measures the position of the first system, one can predict with certainty the position of the other one. And, following EPR, since the two systems no longer interact, the real physical properties of the second system must be independent of the specific measurement done to the first.

But Heisenberg's uncertainty principle precludes both position and momentum for one system to be well defined together. Therefore, quantum mechanics must be incomplete, so EPR.

The impact of the EPR paper has a very interesting intellectual history (Figure 2). Immediately after it appeared, the paper received very few citations. The citations were not that bad. Two were those from Schrödinger already mentioned and one was from Bohr. Bohr's position is rather complex, and it is difficult to do it full justice. Basically, he said that measurement on one of the two particles immediately changes the possible predictions one can make for the other one. This may be seen as saying that the quantum state of an entangled system cannot be seen as describing the individual particles separately.

And then, the paper was basically ignored for a long time. So that paper would not have gotten Einstein tenure, according to today's procedures. But later, two remarkable things happened. Firstly, as one sees, the citations really picked up again in the 1960s. This was when John Bell found out that local realism, the philosophical conceptual position of the EPR paper, is in contradiction to quantum mechanics. And in the 1990s, it was discovered that entanglement plays a fundamental role in quantum information concepts.

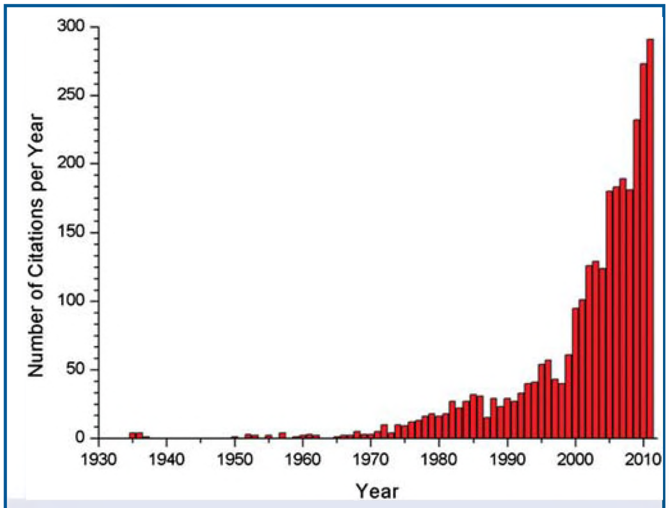

Fig. 2 Number of citations of the original Einstein-Podolsky-Rosen (EPR) paper of 1935. In the beginning, the paper had very few citations, and then it was essentially ignored for a long time. The first rise came after, in the 1960s, John Bell showed that the local realistic world view exposed in the EPR paper is in conflict with the predictions of quantum mechanics. The really big surge started around 2000. At that time, it turned out that quantum entanglement is a fundamental concept in many quantum information protocols, including quantum computation, quantum teleportation and some versions of quantum cryptography.

It is the position of local realism to assume (a) that systems carry real properties which then determine all measurement results (realism) and (b) that an observation here and now is independent of what somebody else does at the very same time at a distant location (locality). John Bell showed that one can very well explain the perfect correlations between two entangled systems using such local realistic properties. Surprisingly, he found that nonperfect correlations, *i.e.* superpositions for either particle, are such that the local realistic model is in conflict with quantum mechanics. The mathematical formulation of that fact is Bell's inequality. A way to also see the implications of Bell's inequality is that basically, there are situations where classical correlations cannot be as strong as those predicted by quantum mechanics. Today, many experiments have confirmed the predictions of quantum mechanics. Furthermore, as mentioned already, quantum entanglement has become a workhorse in many quantum information protocols.

I became interested in quantum entanglement in the early 1980s. At that time, I had been working at the neutron diffraction laboratory at MIT, doing neutron interferometry. At our lab, Mike Horne was a regular visitor who had contributed early to propose various possibilities to test Bell's inequalities in experiment. Together with him, we proposed the first interferometer-based realization of quantum entanglement. This was also the first proposal employing entanglement of momentum, *i.e.* an external variable. Up to that time, all entanglement experiments and proposals had been using internal variables, like spin for example.

Then, in 1987, Danny Greenberger, whom I also had known from my MIT days, visited me in Vienna as a Fulbright Professor. On the first day, we sat down together to decide what we wanted to do. It turned out that we both had been wondering whether anything new might happen if one studies entanglement beyond two particles. To our great surprise, we found cases of entanglement of three or more particles where something completely new and unexpected was predicted by quantum mechanics. These are situations where, based on measurements on two of the particles, one can predict with certainty what the respective property of the third is.

For example, in specific cases, when you know the measurement results of the spins of two spin ½ particles entangled with each other and with a third particle, a quantum physicist can predict with certainty what the spin of the third particle is. But remarkably, for the same experimental situation, a local realist would predict exactly the opposite. Both base their predictions on the same results of the first two particles. So this was very striking. There was a contradiction which was not statistical any more, between quantum mechanics and local realism. It was a definite prediction for each individual particle. We were very surprised by that discovery, because we would have expected, in hindsight naïvely, that quantum mechanics would agree with classical physics at least in those cases where one can make predictions with unit probability, that is, with certainty.

After we had discovered this, it became my scientific goal to realize such states in the laboratory, that is, to go beyond two-particle entanglement. It turned out that this was much more demanding and challenging than I had expected. We had to develop many new tools. For instance, nobody at that time had any realistic idea based on the experimental technology at that time, how to produce three-particle entanglement. What we came up with was to have two pairs of entangled particles and to subject one of the four particles to a measurement which erases any information to which of the two pairs it belonged. Then the other three are entangled! Finally, in 1998, we succeeded in performing the experiment (Figure 3), confirming perfectly the predictions of quantum mechanics.

Along the way, we developed many tools which today have become important in quantum information protocols. A characteristic example is quantum teleportation. When it was first suggested by Bennett, Brassard, Crépeau, Jozsa, Peres and Wootters in 1993 [4], our immediate reaction was that this is completely impossible to do. At that time, we were not aware of the fact yet that on the long road towards realizing three-particle entanglement, we already were working on developing the right tools to also do quantum teleportation. So in 1997, we finally succeeded.

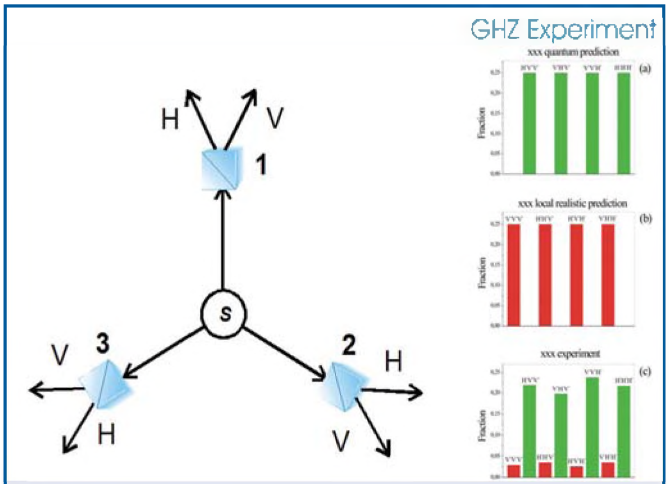

Fig. 3 Entanglement of three photons in a GHZ state. Each photon is subject to a measurement of horizontal (H) or vertical (V) polarization [3]. Each individual result is random. All combinations between results on two photons are also random. But the results of correlations between all three photons are not random for specific measurements. For example, if two photons are found to be differently polarized, one H and the other V, then quantum mechanics predicts the third photon to be definitely V polarized (a). In contrast, based on the first two results, a local realist predicts the third photon to be definitely horizontally polarized (b). Experiment (c) confirms the quantum prediction within experimental error.

Today, the multi-particle states which we found are called GHZ states, after the authors, where H refers to Horne. To our surprise, it turned out that GHZ states are not only of fundamental interest. They are today an essential workhorse in many quantum information and quantum computation paradigms, to the point that they are now a PACS entry.

If we talk a little bit about the present situation and the future development of quantum information, the application which is most advanced is quantum cryptography. This has been discussed in detail in the Herzberg Memorial Lecture by Raymond Laflamme in 2008 [5]. The present situation is such that distances of more than 100 km can be covered. Most interestingly, it turns out that entanglement-based quantum cryptography offers strong security in the following sense. Suppose you are a customer of a quantum cryptography provider. You want to be absolutely certain that nobody listens in. When a provider uses quantum entanglement to supply the secret key, which you use for encoding information, you can easily check whether he is playing fair or not. You simply check for a sub-set of the measurements on the two particles, whether they violate a Bell inequality. If this is the case with a sufficient safety margin, then you do not need to know which devices the provider is actually using. But ideally, this implies that the test of Bell's inequalities is loophole-free, which at present is not the case for long distances yet. A loophole-free experiment means that a sufficiently large subset of all particles is measured, typically about two thirds. Then, no local realistic explanation will be possible any more, and any action of an eavesdropper would lead to a breakdown of entanglement and therefore make the data look unentangled. Thus, the action of the eavesdropper can easily be discovered, making the communication secure. It is to be expected that such a loophole-free long-distance quantum experiment with photons will be performed within reasonable time.

A more futuristic application is quantum teleportation. It is generally understood that quantum teleportation and its generalization to quantum repeaters is an ideal way how future quantum computers could communicate with each other. It will allow teleportation of a quantum state from the output of one quantum computer to the input of another one. To demonstrate the feasibility of long-distance teleportation, recently experiments were performed in China by the group of Jian-Wei Pan [6] and by my group in Vienna.

The arrangement and the set-up of our teleportation experiment [7] between the Canary Islands of La Palma and Tenerife are shown in Figure 4. That experiment demonstrated that it is possible to teleport individual quantum states between these islands over distances of 143 km. Both the Chinese experiment and ours provide convincing proof that quantum communication with low-flying satellites is possible, even at the advanced level of teleporting a quantum state up to a satellite or down from a satellite. In the long run, we are working on doing quantum communication and quantum teleportation in space, this time in collaboration with the group of Jian-Wei Pan at the Chinese Academy of Sciences.

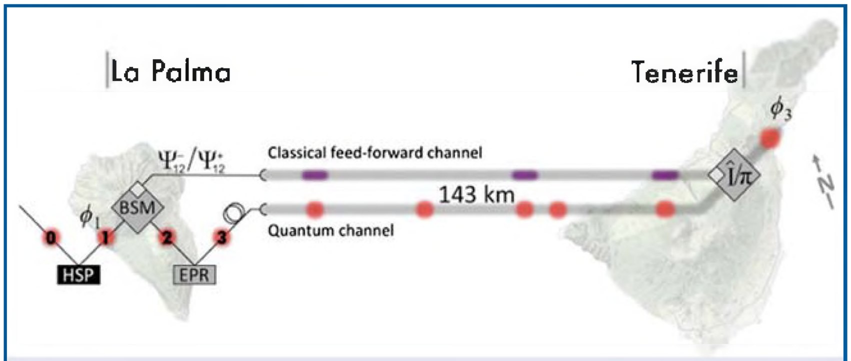

Fig. 4 Quantum teleportation experiment on the Canary Islands of an arbitrary quantum state ϕ_1. This is done by employing an auxiliary entangled EPR pair (photons 2 and 3). Photons 1 and 2 are then subjected to a Bell state measurement which projects them onto an entangled state. The random classical result of that measurement is transmitted through the classical feed-forward channel to Tenerife. Photon 3 passes via the quantum channel also to Tenerife, where the receiver, Bob, applies a unitary transformation. The result is that the output state ϕ_3 is identical with Alice's original input state ϕ_1. Furthermore, photon 1 is not in the state ϕ_1 anymore, but entangled with photon 2. So its quantum state has really been teleported rather than copied or faxed.

Figure 5 shows an artist's sketch of a futuristic experiment for the long-distance distribution of entanglement using the International Space Station ISS. It is evident that such an experiment is very challenging, as we have a moving source for the entangled state. But on the other hand, the big advantage of space-based quantum communication is that these photons only have to traverse a few kilometers of atmosphere, which leads to a much lower attenuation than on the ground over the same distance.

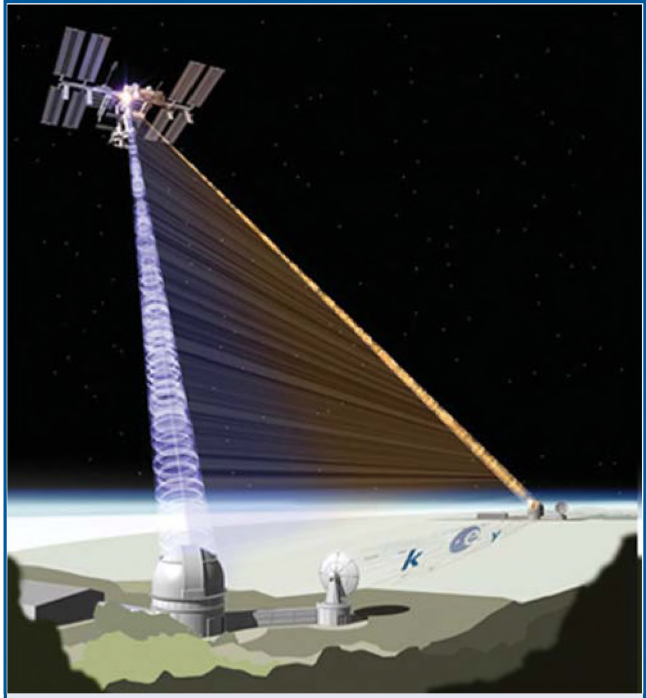

Fig. 5 Artist's sketch of a futuristic quantum entanglement experiment using the International Space Station ISS.

Experiments reflecting individual photons back from a satellite demonstrate that such a space-based quantum communication scenario is possible.

From today's point of view, the most advanced application of these fundamental quantum phenomena will be quantum computation. Again, I would like to refer to the presentation by Raymond Laflamme for the general concepts. A most interesting development happened since the time when he gave the Herzberg Lecture.

Imagine a future quantum internet with central servers, which have the full power of quantum computation. Then, if you are a client using these servers, you want to make absolutely sure that the operator of the central server has no idea which kind of problem you are working on. Are you calculating the development of some market prices, or are you just playing a quantum computer game? Also, you want to make sure that the server has no idea which data you are using.

Recently, it was shown by Broadbent, Fitzsimons and Kashefi that it is possible to operate a quantum server in a way which fulfills these demands. The client only has to be able to prepare individual quantum bits, individual qubits, in an arbitrary quantum state. He then sends these quantum bits to the quantum server who entangles them with each other. This highly entangled so-called cluster state is basically the central registry of the quantum computer. The calculation then proceeds as a sequence of measurements on this entangled state. Each sequence of measurements is characteristic for a specific algorithm. It is important that the operator of the server has no idea in which states the original qubits were, and he has no possibility to find out because of the theorem that arbitrary quantum states cannot be cloned. Therefore, the operator has no idea what the meaning of the instructions which you tell him in order to implement your computation is. He also has no idea what the meaning of the measurement results is. Only you as the client know how to interpret the measurement results such that they give you the final result of your computation.

Recently in my group with Stefanie Barz and Philip Walther and in collaboration with the original proposers of the concept [8], we demonstrated experimentally that such a scheme is possible in principle. This not only answers to the positive the old question whether blind computation can be realized. It also adds to the incentive of building a quantum internet in the future.

It may be safe to expect that quantum computation will become a reality on a time scale of the order of 15 to 20 years. This is also the time scale when, according to Moore's Law and as pointed out by Laflamme, present computer technology will be at a limit which is defined such that the carriers of information are so small that an individual system carries an individual bit. So, two independent developments have a tendency that they will meet in the future. The development of present computation from above and the development of quantum computation from below.

Which technology will eventually be realized in real-world quantum computers is completely open today. There are many concepts and ideas being tested. They use, for example, photons, ions, atoms, superconductors, semiconductors etc. etc. Maybe each of these technologies will have its own specific application. But if we have learned anything from the development of new technologies in history, then it is completely impossible to predict which way it will go and what a new technology will be used for. It is well known, for example, that the laser was seen for a long time as a great solution for problems which we don't know yet. To give another example, when Heinrich Hertz did his first experiment on the propagation of electromagnetic waves, the referees supported his proposal. They recommended that he should get his money because of the fundamental importance of his work even as, they said, "this will never lead to a practical application". I personally remember having heard similar comments in the 1970s about work on the foundations of quantum mechanics.

ACKNOWLEDGEMENTS

The results I have reported here would have been completely impossible without the many collaborators I had the privilege and pleasure to work with over my scientific life. Also, I appreciate the financial support from many sources, most notably the Austrian Science Fund, the Austrian Ministry of Science and the European Commission.

REFERENCES

1. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A Fast and Compact Quantum Random Number Generator", *Rev. Sci. Instr.* **71**, 1675–1680 (2000).
2. A. Einstein, B. Podolsky, and N. Rosen, "Can Quantum-Mechanical Description of Physical Reality be Considered Complete?", *Physical Review* **47**(10), 777–780 (1935).
3. D. M. Greenberger, M. A. Horne, and A. Zeilinger, "Going Beyond Bell's Theorem", in 'Bell's Theorem, Quantum Theory, and Conceptions of the Universe', M. Kafatos (Ed.), Kluwer, Dordrecht, 69–72 (1989).
4. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels", *Phys. Rev. Lett.* **70**, 1895–1899 (1993).
5. R. Laflamme and J. Chamilliard, "The 2008 CAP Herzberg Lecture: Harnessing the Quantum World", *Physics in Canada / La Physique au Canada* **65**(1), 23–28 (2009).
6. J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Quantum teleportation and entanglement distribution over 100-kilometre free-space channels", *Nature* **488**, 185–188 (2012).
7. X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward", *Nature* **489**, 269–273 (2012).
8. S. Barz, E. Kashefi, A. Broadbent, J. Fitzsimons, A. Zeilinger, and P. Walther, "Demonstration of Blind Quantum Computing", *Science* **335**(6066), 303–308 (2012).

Biography

Ever since Anton Zeilinger first learned about quantum mechanics as a student, he has been interested in its foundations. Then, already in the 1970s, he investigated quantum phenomena in neutron interferometry. In the 1980s he began to work on quantum entanglement and in the 1990s also on atom and molecule interferometry. All his work was initially motivated by the counter-intuitive predictions of quantum mechanics for individual systems. To his great surprise, the fundamental phenomena observed have become basic paradigms for a new field, the science and technology of quantum information, signified by concepts such as quantum communication, quantum cryptography and quantum computation. This earned him the inaugural Isaac Newton Medal of the Institute of Physics (UK) *"for his pioneering conceptual and experimental contributions to the foundations of quantum physics, which have become the cornerstone for the rapidly-evolving field of quantum information."* In his free time, Anton Zeilinger is interested in classical waves, for example those emanating from his cello, or the waves on water he observes from his sailboat.