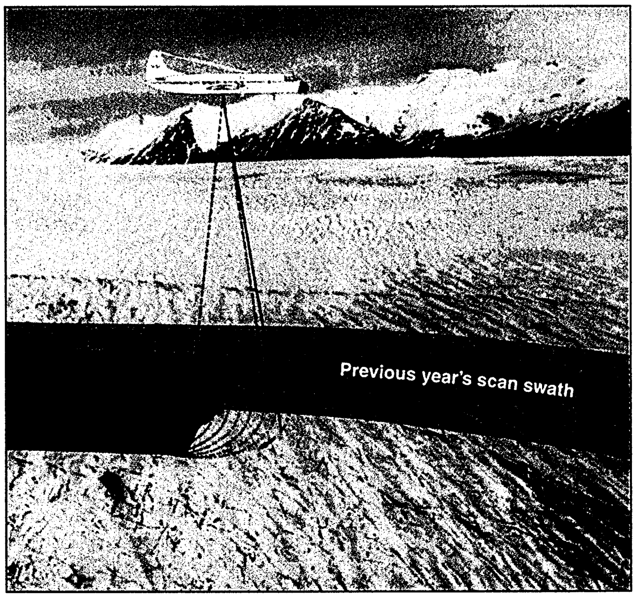
fluctuations are connected with present climate changes. General circulation models can be used to estimate temperature and precipitation variations and thus the sensitivity of ice sheet mass balance to these climate changes. Model results have indicated that in Greenland, climate warming would result in increased melt rates along the margin of the ice sheet but that this would be counteracted at least in part by increased precipitation rates in the high-elevation areas (*1*). A series of a few warm years is expected to produce a sea level rise. This is most likely what is being observed; the years from 1993 to 1999 have been warm years, although the long-term component is also present.

The mass balance budget considerations presented by Thomas *et al.* (*3*) are based on measurements of the amount of mass deposited on the high-elevation area and the amount of ice that flows out of this region. Surface velocities have been measured at stations 30-km apart along the 2000-m contour line by repeated measurements with the Global Positioning System (GPS). On the basis of these velocities, the discharge of mass is estimated. The measured discharge represents the response to the mass budget over a time scale of a century to a millennium. The total precipitation was estimated from a compilation of all available data (*10*) on time scales ranging from a few years to centuries. The authors conclude that there has been no substantial ice volume change over several decades in the high-elevation area of the Greenland Ice Sheet. The difficulty is that the imbalance is determined by subtracting two large figures: the total precipitation and the total discharge by flow across the 2000-m contour line. The uncertainty of the estimate is an ice thickness change of 7 mm/year, the same order of magnitude as the expected long-term trend from climate and dynamic history.

It is not surprising that slightly different results are reached in the two reports: They represent mass balances over different time scales. What is perhaps surprising is that they agree on the balance of the high-elevation regions.



Airborne measurements of ice sheet elevation changes. Surface elevation changes of the Greenland Ice Sheet are detected by repeated laser altimeter surveys. The entire region above 2000 m is in balance within ±5 mm/year, whereas thinning predominates along 70% of the region below 2000 m. The net loss over the Greenland Ice Sheet leads to a sea level rise of 0.13 mm/year (*2*).

How can we predict sea level changes from ice volume changes in the Greenland Ice Sheet in the future? In my opinion, we need to be able to detect both the long-term trend and the short-term signal. The ability to detect annual to decadal surface elevation changes by airborne and satellite observations (*2*, *9*) will be refined. Future satellites will provide additional information and hopefully decrease the uncertainty of the observations. But the records need to be extended to several decades before the long-term trend can be estimated. The "waiting time" can be reduced by using general circulation models to calculate the long-term impact of past climate change on the Greenland Ice Sheet and estimate the size of the fluctuations. The mass budget approach (*3*) may be able to provide a more reliable long-term trend if internal radio echo layers in the ice can be used to reconstruct the spatial and temporal distribution of ice deposition over a longer time period (*4*).

It should be noted that the Greenland Ice Sheet contains only 10% of the ice bound globally in ice sheets. The Antarctic Ice Sheet contains almost all of the remainder. Its area is an order of magnitude larger, accumulation is a factor of 10 less, and ice shelves and ice grounded below present sea level further complicate the picture. The balance of the Antarctic Ice Sheet thus represents another extremely important challenge for the coming generations of air- and spaceborne remote sensing methods.

References

1. R. Warrick *et al.*, in *Climate Change, 1995: The Science of Climate Change*, J. T. Houghton *et al.*, Eds. (Cambridge Univ. Press, Cambridge, 1996), pp. 359–405.
2. W. Krabill *et al.*, *Science* **289**, 428 (2000).
3. R. Thomas *et al.*, *Science* **289**, 426 (2000).
4. N. Reeh, *Geograf. Ann.* **81A**, 735 (1999).
5. K. M. Cuffey and S. J. Marshall, *Nature* **404**, 591 (2000).
6. P. Huybrechts, *Global Planet. Change* **9**, 39 (1994).
7. D. Dahl-Jensen *et al.*, *Science* **282**, 268 (1998).
8. N. Reeh, *Nature* **317**, 797 (1985).
9. C. H. Davis, C. A. Kluever, B. J. Haines, *Science* **279**, 2086 (1998).
10. A. Ohmura and N. Reeh, *J. Glaciol.* **37**, 140 (1991).

PERSPECTIVES: QUANTUM COMPUTING

Quantum Entangled Bits Step Closer to IT

Anton Zeilinger

Today's computers and methods of communication are based on digital technology, where information is represented in bits that either take the value "0" or "1." From a fundamental point of view, these machines and procedures are equivalent to the glass beads and smoke signals of the past. But as elements in computers become smaller and smaller and communication technologies try to use less and less energy to send the same information, individual bits will ultimately be represented by individual quantum systems. Fundamentally new phenomena such as quantum superposition and quantum entanglement will result, bringing with them novel ways of communication and computation with no analog in today's information technology. Recent research provides a glimpse into the future by realizing entanglement-based quantum cryptography and by demonstrating entanglement of more than two quantum systems with methods that may allow scaling up to even more particles.

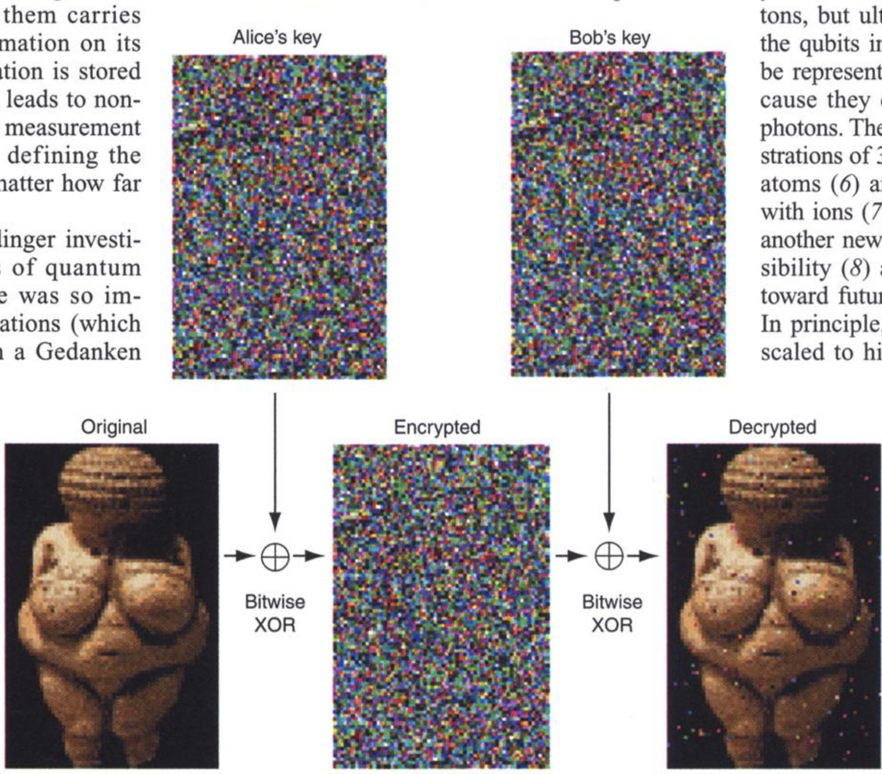
A quantum bit, or qubit, can not only

The author is at the Institute of Experimental Physics, University of Vienna, Boltzmanngasse 5, Vienna 1090, Austria. E-mail: Anton.Zeilinger@univie.ac.at

be in the state "0" or "1," it may also be in a superposition of the two, just as a photon or an electron in a two-slit experiment can be in a superposition of passing through one slit or the other. In a sense, a qubit carries both values at the same time. Even more counterintuitive, two or more qubits can be entangled, which means that neither of them carries any well-defined information on its own; rather, all information is stored in joint properties. This leads to nonlocal correlations, with measurement on one qubit instantly defining the state of the others, no matter how far they are apart.

When Erwin Schrödinger investigated the foundations of quantum mechanics in 1935, he was so impressed by these correlations (which had been introduced in a Gedanken experiment designed by Albert Einstein, Boris Podolsky, and Nathan Rosen in the same year) that he coined a special term for it, entanglement ("Verschränkung" in the German original), and called it the essence of quantum physics.

Recently, entanglement-based quantum cryptography as suggested by Ekert (*1*) was demonstrated in three independent experiments (*2–4*). In these experiments, our quantum cryptographers Alice and Bob exploit the perfect correlations between two entangled photons (see the figure). They obtain the same random sequence of bits, which they can then use as a key to encrypt a secret message. The essential point here is that the key is created spontaneously on both sides by Alice's and Bob's measurement and does not need to be transmitted. An eavesdropper therefore has no chance to catch the key in flight. To make sure that the eavesdropper cannot tap into the quantum entanglement line by measuring one of the particles, Alice and Bob each randomly and independently switch between two different measurements. Alice and Bob can then readily identify the presence of the eavesdropper, who invariably disturbs the perfect correlations between their measurements. The present status of quantum cryptography is such that it can be used to generate a key at the rate of 1 kilobit per second over distances of 10 kilometers or so. High data rates will only become possible after further substantial technological development, but quantum cryptography can already be useful today to exchange extremely sensitive information, over distances spanning a business or banking district in a big city.



Transmission of secret information with quantum cryptography. A picture of the Venus of Willendorf effigy (22,000 B.C., found near Vienna, Austria) is encoded into an 8-bit deep color map. The two random keys obtained by Alice and Bob, through independent measurements on the photons in an entangled pair, are also represented as color maps. Alice encodes the original picture by bit-wise XOR addition. The transmitted image is completely random and has no structure at all, making any eavesdropping futile. Bob finally recovers the original message again by bit-wise XOR addition of his key. The few errors left are due to occasional imperfect correlations between the two measurements. Adapted from (*2*).

Quantum computation aims to use the property that an entangled state can be viewed as a superposition of different bitwise representations of information. The quantum computer then acts on the whole superposition of all individual pieces of information at the same time. This results in what is called massive parallel computation. For the realization of future quantum computers, it will be essential that entangled states of many qubits can be produced in the laboratory. Recently, first steps in this direction have been made for photons (*5*) and atoms and ions (*6–8*). It had been predicted earlier that entanglement of three qubits leads to a striking contradiction between quantum mechanics and classical theory (*9*).

In the photon experiments, entangled pairs are used as building blocks for higher order entanglement. Such entangled photon pairs can be created with very high purity, recently enabling verification of the Greenberger-Horne-Zeilinger (GHZ) prediction mentioned above (*10*). The experiments can readily be scaled to more than three photons, but ultimately one would want the qubits in a quantum computer to be represented by atoms or ions, because they do not buzz around like photons. Therefore, the recent demonstrations of 3-qubit entanglement with atoms (*6*) and 4-qubit entanglement with ions (*7*) and the development of another new scheme having that possibility (*8*) are very important steps toward future quantum computation. In principle, these ideas can also be scaled to higher numbers of qubits.

These experiments with atoms and ions show that entanglement of a higher number of atoms might be possible—which would be important for the development of future quantum computers—but they also demonstrate that the quality of the entanglement needs to be substantially improved both for testing the fundamental physics and for developing a useful quantum computation procedure. This represents an enormous challenge for further technological progress.

The philosophical conundrum alluded to by Schrödinger when he coined the notion of entanglement is still not sufficiently resolved, but investigation of these fundamental issues is already giving birth to a new technology. The fact that as little as 10 years ago, virtually none of this existed gives reason to be very optimistic for the future.

References

1. A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
2. T. Jennewein *et al.*, *Phys. Rev. Lett.* **84**, 4729 (2000).
3. D. S. Naik *et al.*, *Phys. Rev. Lett.* **84**, 4733 (2000).
4. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).
5. D. Bouwmeester *et al.*, *Phys. Rev. Lett.* **82**, 1345 (1999).
6. A. Rauschenbeutel *et al.*, *Science* **288**, 2024 (2000).
7. C. A. Sackett *et al.*, *Nature* **404**, 256 (2000).
8. B. T. H. Varcoe, S. Brattke, M. Weidinger, H. Walther, *Nature* **403**, 743 (2000).
9. D. M. Greenberger, M. A. Horne, A. Shimony, A. Zeilinger, *Am. J. Phys.* **58**, 1131 (1990).
10. J.-W. Pan *et al.*, *Nature* **403**, 515 (2000).

CREDIT: ADAPTED FROM (2)