PHYSICS

Where Is My Quantum Computer?

With applications in quantum cryptography, rudimentary quantum computers already exist.

P. Hemmer[1] and J. Wrachtrup[2]

The title question is echoed by electrical engineers and consumers alike. It has now been 15 years since quantum computing came to the forefront of popular science with its promise of superpowered computers for the future, so it is natural to be wondering when the first commercial products will appear on the market.

Actually, the answer may seem somewhat surprising: The quantum computer is already here. Demonstration versions are available from several companies (*1*, *2*), and high-performance versions have been (*3*) and are currently being (*4*) constructed. Although these devices are referred to as quantum cryptography or quantum key distribution systems (*5*), they operate on similar principles as does a quantum computer. Individual quantum bits (qubits) in the form of photons are sent out one at a time in one of four polarizations that redundantly encode 0s and 1s. When a qubit is received, an attempt is made to perform a single qubit operation, called the Hadamard transformation (see the figure); this operation is one of the most elemental quantum computing operations, from which more complex codes can be constructed. Whenever this operation succeeds, the data are discarded; what is left behind is a random one-time code that can be used as an unbreakable cipher.

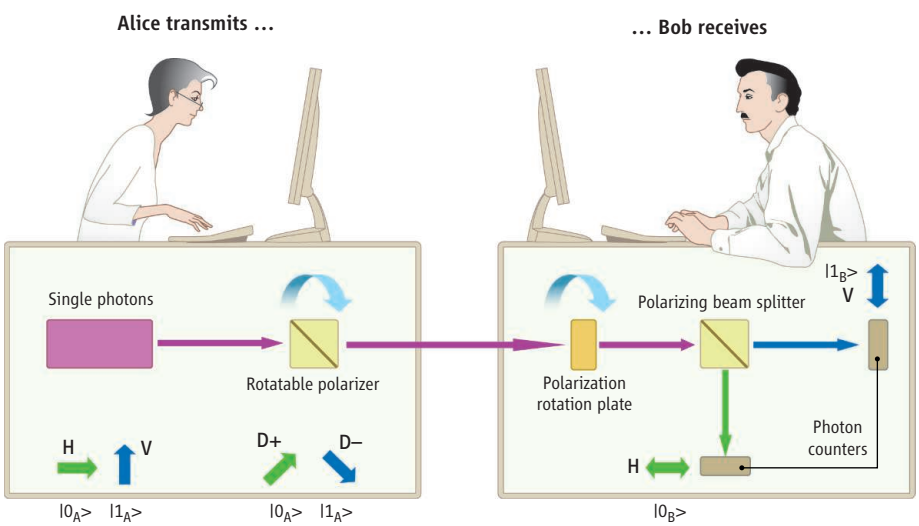
This seems a long way from what we would consider to be a superpowered quantum computer capable of doing sophisticated calculations using quantum entanglement, but consider the next generation of quantum secure communication systems, currently under development, that are based on the theoretical concept of quantum teleportation (*6*). Here, the information itself is never even transmitted but appears at the receiver as a result of the peculiar properties of quantum mechanics. What could be more secure than that? A quantum teleporter additionally requires two qubit operations to be performed to create entangled states. Measurements determine what kind of entangled state dominates, and this is much like reading out the answer from a quantum computation. Photons were teleported long ago, but it is generally accepted that qubits in material systems are needed to store entanglement long enough to ensure its presence before attempting teleportation. This was recently shown using atomic vapors as a qubit storage medium. Long-distance matter qubit teleportation has also been accomplished with individual trapped ions (*7*), opening the door to error-correction protocols needed to make teleportation practical.

Single-qubit and two-qubit gates like those used in teleportation are sufficient to construct even the most complex quantum computer (*8*). A quantum teleporter will be the first to incorporate all the key elements of a general purpose quantum computer.

Also under development are quantum repeaters that are needed to make secure quantum communication work over long distances, such as over Internet optical fibers (*9*). These repeaters perform even more complex quantum computation operations such as entanglement purification, and it is expected that nontrivial quantum computers will be needed at the repeater nodes to accomplish these tasks. For example, the purification protocol (*10*) that can be implemented on a few-qubit quantum computer for a diamond-based system (*11*) holds the promise to do these operations in a scalable microchip system. Some key components have already been demonstrated at room temperature (*12*).

So quantum computers are now a reality and will continue to be developed. However, the long-term emphasis will shift from factoring large numbers to break classical codes, to applications that emphasize the unbreakable nature of quantum codes.

What will be the first consumer product? Every time we search the Internet, information is collected about us and our personal habits, whether we like it or not. A quantum computer could prevent this from happening. For example, a recently proposed quantum algorithm uses the highly fragile nature of quantum entanglement to let us know whether the search engine we queried peeked at our search terms or not (*13*). The implementation of this is not unlike the quantum key distribution



Quantum key distribution. The transmitter, Alice, sends single photons with linear polarization oriented in one of four possible directions, chosen at random. Orthogonal polarization directions encode logical 0s and 1s. For example, a photon in the horizontal-vertical (HV) basis H can represent logical 0 and V a logical 1. In the diagonal (DI) basis D+ can represent logical 0 and D– a logical 1. If the receiver, Bob, selects the same basis as Alice, then he can determine with 100% accuracy whether a 0 or 1 was transmitted. If the bases are different then there is a 50% chance of getting the wrong answer. Discarding this data leaves behind a random shared code that can give absolute security when used as a one-time cypher. However, if we look more closely at the polarizing beam splitter Bob uses to distinguish polarization states, we find that it can actually create well-defined mixed polarization states. For example, if Alice transmits the D+ state and Bob receives in the HV basis, there is equal amplitude in H and V states. In essence, the input state D+ = $|0_A\rangle$ is converted to the output state H + V = $|0_B\rangle + |1_B\rangle$. Similarly the input state D– = $|1_A\rangle$ is converted to H – V = $|0_B\rangle - |1_B\rangle$. But this is exactly the action of a single qubit Hadamard gate.

[1]Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843, USA. [2]Institute of Physics, University of Stuttgart, 70550 Stuttgart, Germany. E-mail: prhemmer@ece.tamu.edu; wrachtrup@physik.unistuttgart.de

CREDIT: P. HUEY/SCIENCE

Published by AAAS

systems that allow us to detect the presence of an eavesdropper by an unexplained increase in error rate. There may well be a valuable consumer product in a few years.

Other possible applications include implementing quantum games (*14*). Again, security is the key consideration. If you are playing a big-stakes game—such as sealed-bid auctions, digital rights management, or looking for alternatives to taxation for public goods allocation—you want to be sure that the other gamers, or even the system administrator, are not cheating. You may also want to ensure that your move is anonymous, so that it is more difficult for other players to guess your strategy. Quantum computers may offer a way to provide these functions, and, additionally, the inherent randomness of some quantum measurements may be able to enhance fairness.

Whether or not we eventually have quantum security chips in our laptops, the spin-offs from quantum computing research are likely to be at least as exciting. Consider, for example, that single-spin qubits in diamond might be used as ultrasensitive magnetometers operating as nanoscale probes in living cells (*15*). Other applications include quantum imaging for superresolution and lensless ghost imaging (*16*), as well as ultraprecise atomic clocks (*17*) that can measure general relativistic effects in the universe or at least give us a more accurate global positioning system. Quantum computers are here and are likely to become an important part of our everyday lives in the not-so-distant future.

References

1. MagiQ, www.magiqtech.com.
2. ID Quantique, www.idquantique.com/company/overview.htm.
3. C. Elliott, *New J. Phys.* **4**, 46 (2002).
4. R. Ursin *et al.*, *Proceedings of the 2008 Microgravity Sciences and Process Symposium*, Glasgow, Scotland, 29 September to 3 October 2008.
5. C. H. Bennett, G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 9 to 12 December 1984, p. 175.
6. C. H. Bennett *et al.*, *Phys. Rev. Lett.* **70**, 1895 (1993).
7. S. Olmschenk *et al.*, *Science* **323**, 486 (2009).
8. S. Lloyd, *Phys. Lett. A* **167**, 255 (1992).
9. Z.-S. Yuan *et al.*, *Nature* **454**, 1098 (2008).
10. L. Childress, J. M. Taylor, A. S. Sørensen, M. D. Lukin, *Phys. Rev. A* **72**, 052330 (2005).
11. J. Wrachtrup, F. Jelezko, *J. Phys. Condens. Matt.* **18**, S807 (2006).
12. M. V. G. Dutt *et al.*, *Science* **316**, 1312 (2007).
13. V. Giovannetti, S. Lloyd, L. Maccone, arXiv:0708.2992v2 [quant-ph] (2007).
14. H. Guo, J. Zhang, G. J. Koehler, *Decis. Support Syst.* **46**, 318 (2008).
15. G. Balasubramanian *et al.*, *Nature* **455**, 648 (2008).
16. R. Meyers, K. S. Deacon, Y. Shih, *Phys. Rev. A* **77**, 041801R (2008).
17. A. Andre, A. S. Sorensen, M. D. Lukin, arXiv:quant-ph/0401130 (2006).

10.1126/science.1170912

GEOPHYSICS

The Thickness of Tectonic Plates

Seismic studies continue to refine the elusive boundary that defines the depth at which the lithosphere ends.

Barbara Romanowicz

A fundamental premise of plate tectonics on Earth is that rigid lithospheric plates, formed at mid-ocean ridges, float above a more deformable substratum, the asthenosphere (*1*). The precise nature of the asthenosphere is still debated. Mechanical models predict a well-defined, sharp lithosphere-asthenosphere boundary (LAB), but evidence for such a boundary from conventional seismic measurements is ambiguous. On pages 499 and 495 of this issue, Kawakatsu *et al*. (*2*) and Rychert and Shearer (*3*) present analyses of more sophisticated seismic studies that help refine the LAB and hence the thickness of the lithosphere and tectonic plates, although challenges still remain in picking out this boundary versus other structures within the lithosphere.

Observations of seismic surface waves reveal a well-developed zone where seismic wave velocities are low under the ocean basins, at depths of about 80 to 200 km. This low-velocity zone (LVZ), which also causes strong losses of seismic energy, likely corresponds to the low-viscosity asthenosphere. The thickness of the overlying high-velocity lithospheric "lid" increases with age, which would be expected as the plates cool after formation. The lithosphere is thickest under the oldest, most stable part of continents, the cratons, and here the asthenosphere is poorly developed. Recent estimates that combine seismic tomography, heat flow, and geochemical data from kimberlites (rocks that originate from the mantle) constrain the lithospheric thickness to about 200 to 250 km under the cratons (*4*–*6*).

Other major boundaries in the earth, such as the core-mantle boundary, are more readily observed by seismic body waves that travel through the planet and encounter compositional discontinuities or phase changes. In contrast, detection of the LAB has been elusive, and it has been difficult to determine whether the seismic properties of the LVZ arise from partial melting of rocks (*7*), from increased water content (*8*, *9*), or simply from the competing effects of increasing temperature and pressure with depth (*10*).

One approach that has been successful for detecting and characterizing fainter mantle discontinuities is that of "receiver functions" (*11*), in which conversions of elastic energy from compressional to shear (Ps) or from shear to compressional (Sp) waves are identified on broadband seismic records. This approach constrains the depth, sign, and amplitude of velocity jumps across discontinuities. Receiver function studies have identified drops in velocity at candidate LABs at depths of about 70 to 80 km under ocean islands (*12*) and from 80 to 110 km under relatively young parts of continents (*13*).

Ocean islands, however, generally sit on "anomalous" mantle, such as regions of hotspot plumes. The observation of the LAB under the more representative ocean basins has been hampered by the lack of seismic stations on the ocean floor. The high-quality observations of both Ps and Sp conversions at LAB depths made by Kawakatsu *et al*. were enabled by the long-term operation of several low-noise seismic borehole observatories on the ocean floor in the western Pacific Ocean (*14*). The sharpness of the LAB boundary rules out a purely thermal origin or one arising only from increased water content. The authors convincingly argue that partially melted rock must be present. This melting process is enhanced by the presence of increased amounts of water at this depth, as was predicted experimentally (*15*).

The LAB has also been difficult to detect at the expected depths under the cratonic parts of continents (*16*). Numerous other discontinuities, with either positive or negative jumps in seismic velocity, have been observed at shallower depths and are often referred to as the Hales discontinuity (*17*). Rychert and Shearer present the results of a global study of Ps receiver functions in vari-

Berkeley Seismological Laboratory and Department of Earth and Planetary Science, University of California at Berkeley, Berkeley, CA 94720, USA. E-mail: barbara@seismo.berkeley.edu