Revolutionizing Computing

In about 20 years, computer chips will be so small that the effects of quantum mechanics will replace the physical laws we take for granted. While today's computing is based on bits that are either 0 or 1, the basic unit in quantum computing is the quantum bit—the qubit—which can be 0 and 1 simultaneously (with a probability associated with each). In the strange world of quantum computing, complicated procedures such as factoring large numbers are done much faster because the many steps involved can be done concurrently. The ultimate goal of mathematicians, physicists, computer scientists, and engineers in the field is to create a quantum computer that could solve in seconds some problems that would take today's most powerful computers billions of years to solve.

Among the capabilities of a quantum computer would be the ability to do the calculations necessary to break today's electronic encryption methods. This is not as alarming as it may sound, because cryptographers have already designed algorithms to take advantage of the quantum mechanics principle that observing a system's state changes it. Thus, users of a quantum communications network could detect any attempt to intercept their communication. It is somehow ironic that the laws that govern the barrier to the miniaturization of today's computers may provide a boon to future computing.

For more information: "Rules for a Complex Quantum World," *Scientific American,* November 2002, Michael A. Nielsen.

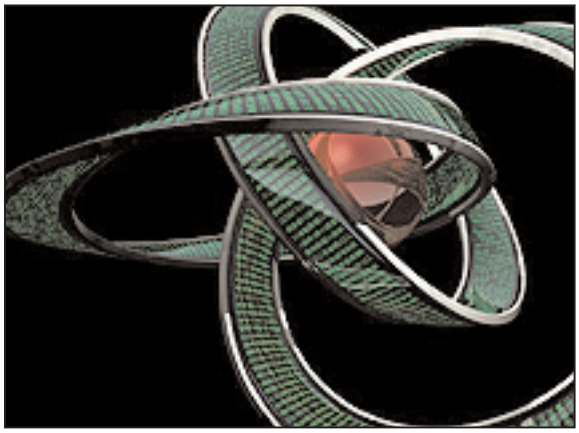

Image courtesy of the MITRE Corporation.

AMS
American Mathematical Society

*The **Mathematical Moments** program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.*

www.ams.org/mathmoments

MM/26