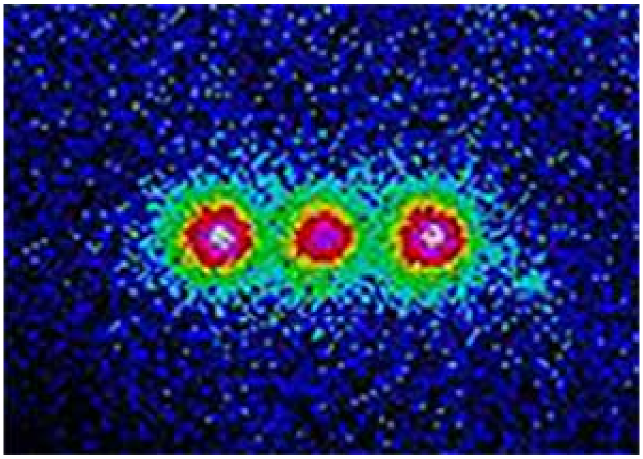
PHYS.ORG

NIST Demonstrates Key Step in Use of Quantum Computers for Code-Breaking

May 12 2005



A crucial step in a procedure that could enable future quantum computers to break todayâ€™s most commonly used encryption codes has been demonstrated by physicists at the U.S. Commerce Departmentâ€™s National Institute of Standards and Technology (NIST).

Image: This colorized image shows the fluorescence from three trapped beryllium ions illuminated with an ultraviolet laser beam. Black and blue areas indicate lower intensity, and red and white higher intensity.

Credit: NIST

As reported in the May 13 issue of the journal Science,* the NIST team showed that it is possible to identify repeating patterns in quantum information stored in ions (charged atoms). The NIST work used three ions as quantum bits (qubits) to represent 1s or 0sâ€”or, under the unusual rules of quantum physics, both 1 and 0 at the same time. Scientists believe that much larger arrays of such ions could process data in a powerful quantum computer. Previous demonstrations of similar processes were performed with qubits made of molecules in a liquid, a system that cannot be expanded to large numbers of qubits.

â€œOur demonstration is important, because it helps pave the way toward building a large-scale quantum computer,â€? says John Chiaverini, lead author of the paper. â€œOur approach also requires fewer steps and is more efficient than those demonstrated previously.â€?

The NIST team used electromagnetically trapped beryllium ions as qubits to demonstrate a quantum version of the â€œFourier transformâ€? process, a widely used method for finding repeating patterns in data. The quantum version is the crucial final step in Shorâ€™s algorithm, a series of steps for finding the â€œprime factorsâ€? of large numbersâ€”the prime numbers that when multiplied together produce a given number.

Developed by Peter Shor of Bell Labs in 1994, the factoring algorithm sparked burgeoning interest in quantum computing. Modern cryptography techniques, which rely on the fact that even the fastest supercomputers require very long times to factor large numbers, are used to encode everything from military communications to bank transactions. But a quantum computer using Shorâ€™s algorithm could factor a number several hundred digits long in a reasonably short time. This algorithm made code breaking the most important application for quantum computing.

Quantum computing, which harnesses the unusual behavior of quantum systems, offers the possibility of parallel processing on a grand scale. Unlike switches that are either fully on or fully off in todayâ€™s computer chips, quantum bits can be on, off, or on and off at the same time. The availability of such â€œsuperpositions,â€? in addition to other strange quantum properties, means that a quantum computer could solve certain problems in an exponentially shorter time than a conventional computer with the same number of bits. Researchers often point out that, for specific classes of problems, a quantum computer with 300 qubits has potentially more processing power than a classical computer containing as many bits as there are particles in the universe.

Harnessing all this potential for practical use is extremely difficult. One problem is that measuring a qubit causes its delicate quantum state to collapse, producing an output of an ordinary 1 or 0, without a record of what happened during the computation. Nevertheless, Shorâ€™s algorithm uses these properties to perform a useful task. It enables scientists to analyze the final quantum state after the computation to find repeating patterns in the original input, and to use this information to determine the prime factors of a number.

The work described in the Science paper demonstrated the pattern-finding step of Shorâ€™s algorithm. This demonstration involves fewer and simpler operations than those previously implemented, a significant benefit in designing practical quantum computers.

In the experiments, NIST researchers performed the same series of operations on a set of three beryllium qubits thousands of times. Each set of operations lasted less than 4 milliseconds, and consisted of using ultraviolet laser pulses to manipulate individual ions in sequence, based on measurements of the other ions. Each run produced an output consisting of measurements of each of the three ions. The NIST team has the capability to measure ionsâ€™ quantum states precisely and use the results to manipulate other ions in a controlled way, before the delicate quantum information is lost.

The same NIST team has previously demonstrated all the basic components for a quantum computer using ions as qubits, arguably a leading candidate for a large-scale quantum processor. About a dozen different types of quantum systems are under investigation around the world for use in quantum processing, including the approach of using ions as qubits.

The new work was supported in part by the Advanced Research and Development Activity/National Security Agency.

As a non-regulatory agency, NIST develops and promotes measurement, standards and technology to enhance productivity, facilitate trade and improve the quality of life.

Citation: NIST Demonstrates Key Step in Use of Quantum Computers for Code-Breaking (2005, May 12) retrieved 24 April 2024 from https://phys.org/news/2005-05-nist-key-quantum-code-breaking.html