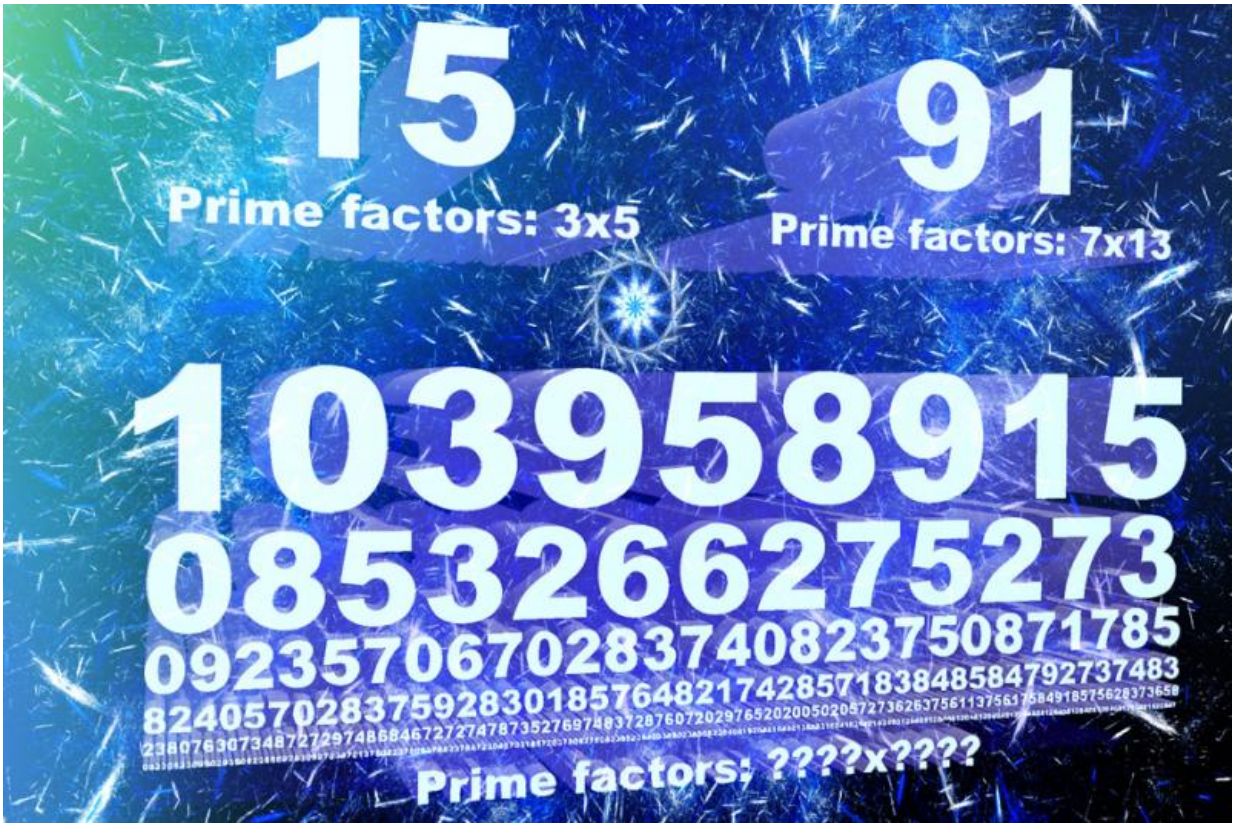
Quantum computer factors numbers, could be scaled up

March 3 2016, by Jennifer Chu



Researchers have designed and built a quantum computer from five atoms in an ion trap. The computer uses laser pulses to carry out Shor's algorithm on each atom, to correctly factor the number 15. Credit: Jose-Luis Olivares/MIT

What are the prime factors, or multipliers, for the number 15? Most

grade school students know the answer—3 and 5—by memory. A larger number, such as 91, may take some pen and paper. An even larger number, say with 232 digits, can (and has) taken scientists two years to factor, using hundreds of classical computers operating in parallel.

Because factoring large numbers is so devilishly hard, this "factoring problem" is the basis for many encryption schemes for protecting credit cards, state secrets, and other confidential data. It's thought that a single quantum computer may easily crack this problem, by using hundreds of atoms, essentially in parallel, to quickly factor huge numbers.

In 1994, Peter Shor, the Morss Professor of Applied Mathematics at MIT, came up with a quantum algorithm that calculates the prime factors of a large number, vastly more efficiently than a classical computer. However, the algorithm's success depends on a computer with a large number of quantum bits. While others have attempted to implement Shor's algorithm in various quantum systems, none have been able to do so with more than a few quantum bits, in a scalable way.

Now, in a paper published today in the journal *Science*, researchers from MIT and the University of Innsbruck in Austria report that they have designed and built a quantum computer from five atoms in an ion trap. The computer uses laser pulses to carry out Shor's algorithm on each atom, to correctly factor the number 15. The system is designed in such a way that more atoms and lasers can be added to build a bigger and faster quantum computer, able to factor much larger numbers. The results, they say, represent the first scalable implementation of Shor's algorithm.

"We show that Shor's algorithm, the most complex quantum algorithm known to date, is realizable in a way where, yes, all you have to do is go in the lab, apply more technology, and you should be able to make a bigger quantum computer," says Isaac Chuang, professor of physics and

professor of electrical engineering and computer science at MIT. "It might still cost an enormous amount of money to build—you won't be building a quantum computer and putting it on your desktop anytime soon—but now it's much more an engineering effort, and not a basic physics question."

Seeing through the quantum forest

In classical computing, numbers are represented by either 0s or 1s, and calculations are carried out according to an algorithm's "instructions," which manipulate these 0s and 1s to transform an input to an output. In contrast, quantum computing relies on atomic-scale units, or "qubits," that can be simultaneously 0 and 1—a state known as a superposition. In this state, a single qubit can essentially carry out two separate streams of calculations in parallel, making computations far more efficient than a classical computer.

In 2001, Chuang, a pioneer in the field of quantum computing, designed a quantum computer based on one molecule that could be held in superposition and manipulated with nuclear magnetic resonance to factor the number 15. The results, which were published in *Nature*, represented the first experimental realization of Shor's algorithm. But the system wasn't scalable; it became more difficult to control the system as more atoms were added.

"Once you had too many atoms, it was like a big forest—it was very hard to control one atom from the next one," Chuang says. "The difficulty is to implement [the algorithm] in a system that's sufficiently isolated that it can stay quantum mechanical for long enough that you can actually have a chance to do the whole algorithm."

"Straightforwardly scalable"

Chuang and his colleagues have now come up with a new, scalable quantum system for factoring numbers efficiently. While it typically takes about 12 qubits to factor the number 15, they found a way to shave the system down to five qubits, each represented by a single atom. Each atom can be held in a superposition of two different energy states simultaneously. The researchers use laser pulses to perform "logic gates," or components of Shor's algorithm, on four of the five atoms. The results are then stored, forwarded, extracted, and recycled via the fifth atom, thereby carrying out Shor's algorithm in parallel, with fewer qubits than is typically required.

The team was able to keep the quantum system stable by holding the atoms in an ion trap, where they removed an electron from each atom, thereby charging it. They then held each atom in place with an electric field.

"That way, we know exactly where that atom is in space," Chuang explains. "Then we do that with another atom, a few microns away—[a distance] about 100th the width of a human hair. By having a number of these atoms together, they can still interact with each other, because they're charged. That interaction lets us perform logic gates, which allow us to realize the primitives of the Shor factoring algorithm. The gates we perform can work on any of these kinds of atoms, no matter how large we make the system."

Chuang's team first worked out the quantum design in principle. His colleagues at the University of Innsbruck then built an experimental apparatus based on his methodology. They directed the quantum system to factor the number 15—the smallest number that can meaningfully demonstrate Shor's algorithm. Without any prior knowledge of the answers, the system returned the correct factors, with a confidence exceeding 99 percent.

"In future generations, we foresee it being straightforwardly scalable, once the apparatus can trap more atoms and more laser beams can control the pulses," Chuang says. "We see no physical reason why that is not going to be in the cards."

What will all this eventually mean for encryption schemes of the future?

"Well, one thing is that if you are a nation state, you probably don't want to publicly store your secrets using encryption that relies on factoring as a hard-to-invert problem," Chuang says. "Because when these quantum computers start coming out, you'll be able to go back and unencrypt all those old secrets."

More information: "Realization of a scalable Shor algorithm," *Science* (2016). DOI: 10.1126/science.aad9480

Provided by Massachusetts Institute of Technology