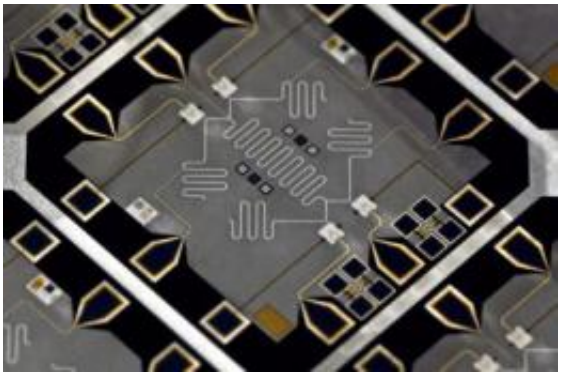
Physicists demonstrate that 15=3x5 about half of the time

August 19 2012



The device in the photomicrograph was used to run the first solid-state demonstration of Shor's algorithm. It is made up of four phase qubits and five superconducting resonators, for a total of nine engineered quantum elements. The quantum processor measures one-quarter inch square. Credit: UCSB

Computing prime factors may sound like an elementary math problem, but try it with a large number, say one that contains more than 600 digits, and the task becomes enormously challenging and impossibly time-consuming. Now, a group of researchers at UC Santa Barbara has designed and fabricated a quantum processor capable of factoring a composite number — in this case the number 15 — into its constituent prime factors, 3 and 5.

Although modest compared to a 600-digit number, the achievement represents a milestone on the road map to building a quantum computer

capable of factoring much larger numbers, with significant implications for cryptography and cybersecurity. The results are published in the advance online issue of the journal *Nature Physics*.

"Fifteen is a small number, but what's important is we've shown that we can run a version of Peter Shor's prime factoring algorithm on a solid state quantum processor. This is really exciting and has never been done before," said Erik Lucero, the paper's lead author. Now a postdoctoral researcher in experimental quantum computing at IBM, Lucero was a doctoral student in physics at UCSB when the research was conducted and the paper was written.

"What is important is that the concepts used in factoring this small number remain the same when factoring much larger numbers," said Andrew Cleland, a professor of physics at UCSB and a collaborator on the experiment. "We just need to scale up the size of this processor to something much larger. This won't be easy, but the path forward is clear."

Practical applications motivated the research, according to Lucero, who explained that factoring very large numbers is at the heart of cybersecurity protocols, such as the most common form of encoding, known as RSA encryption. "Anytime you send a secure transmission — like your credit card information — you are relying on security that is based on the fact that it's really hard to find the prime factors of large numbers," he said. Using a classical computer and the best-known classical algorithm, factoring something like RSA Laboratory's largest published number — which contains over 600 decimal digits — would take longer than the age of the universe, he continued.

A quantum computer could reduce this wait time to a few tens of minutes. "A quantum computer can solve this problem faster than a classical computer by about 15 orders of magnitude," said Lucero. "This

has widespread effect. A quantum computer will be a game changer in a lot of ways, and certainly with respect to computer security."

So, if quantum computing makes RSA encryption no longer secure, what will replace it? The answer, Lucero said, is quantum cryptography. "It's not only harder to break, but it allows you to know if someone has been eavesdropping, or listening in on your transmission. Imagine someone wiretapping your phone, but now, every time that person tries to listen in on your conversation, the audio gets jumbled. With quantum cryptography, if someone tries to extract information, it changes the system, and both the transmitter and the receiver are aware of it."

To conduct the research, Lucero and his colleagues designed and fabricated a quantum processor to map the problem of factoring the number 15 onto a purpose-built superconducting quantum circuit. "We chose the number 15 because it is the smallest composite number that satisfies the conditions appropriate to test Shor's algorithm — it is a product of two prime numbers, and it's not even," he explained.

The quantum processor was implemented using a quantum circuit composed of four superconducting phase qubits — the quantum equivalents of transistors — and five microwave resonators. The complexity of operating these nine quantum elements required building a control system that allows for precise operation and a significant degree of automation — a prototype that will facilitate scaling up to larger and more complex circuits. The research represents a significant step toward a scalable quantum architecture while meeting a benchmark for quantum computation, as well as having historical relevance for quantum information and cryptography.

"After repeating the experiment 150,000 times, we showed that our quantum processor got the right answer just under half the time" Lucero said. "The best we can expect from Shor's algorithm is to get the right

answer exactly 50 percent of the time, so our results were essentially what we'd expect theoretically."

The next step, according to Lucero, is to increase the quantum coherence times and go from nine quantum elements to hundreds, then thousands, and on to millions. "Now that we know 15=3x5, we can start thinking about how to factor larger — dare I say — more practical numbers," he said.

Provided by University of California - Santa Barbara

Citation: Physicists demonstrate that 15=3x5 about half of the time (2012, August 19) retrieved 24 April 2024 from https://phys.org/news/2012-08-ucsb-153x5.html