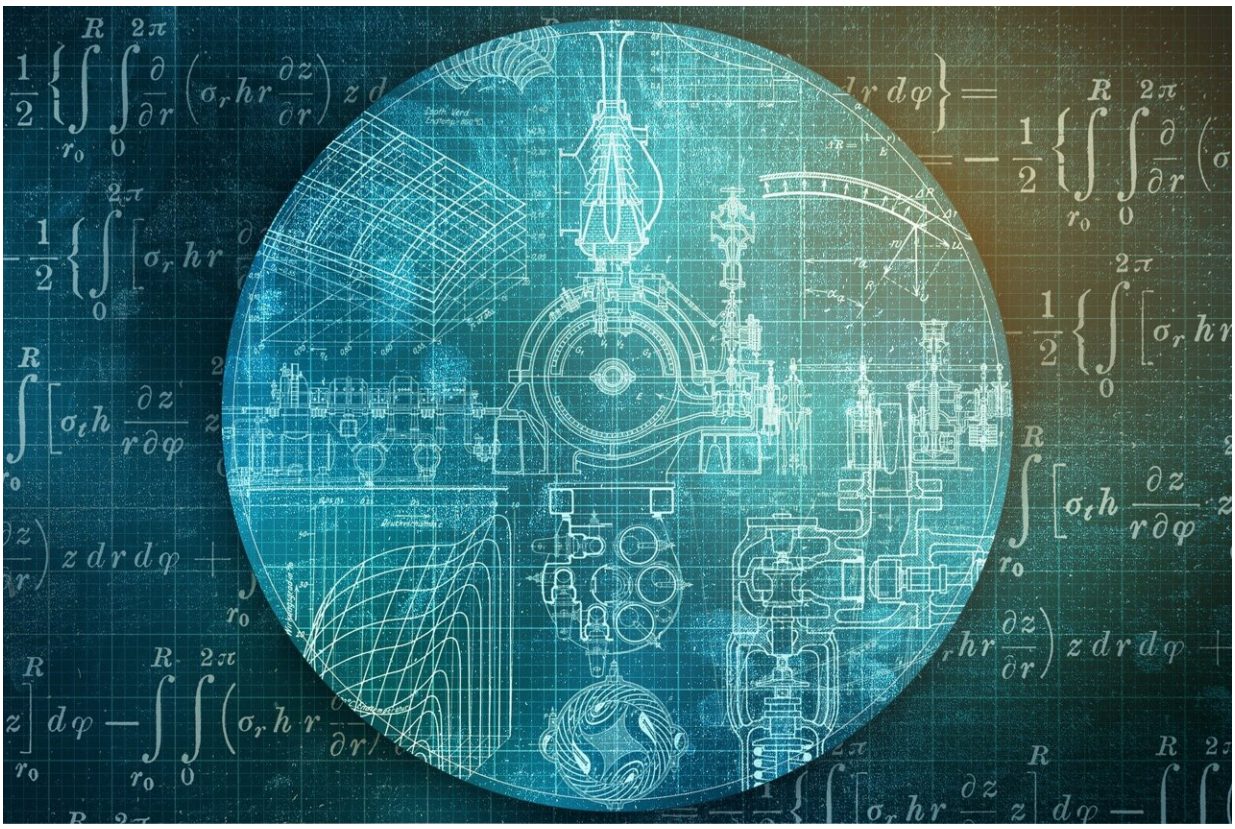
Researchers propose a smaller, more noise-tolerant quantum factoring circuit for cryptography

August 23 2024, by Adam Zewe



Credit: Pixabay/CC0 Public Domain

The most recent email you sent was likely encrypted using a tried-and-true method that relies on the idea that even the fastest computer would

be unable to efficiently break a gigantic number into factors.

Quantum computers, on the other hand, promise to rapidly crack complex cryptographic systems that a classical computer might never be able to unravel. This promise is based on a quantum factoring algorithm proposed in 1994 by Peter Shor, who is now a professor at MIT.

But while researchers have taken great strides in the last 30 years, scientists have yet to build a quantum computer powerful enough to run Shor's algorithm.

As some researchers work to build larger quantum computers, others have been trying to improve Shor's algorithm so it could run on a smaller quantum circuit. About a year ago, New York University computer scientist Oded Regev proposed a major theoretical improvement. His algorithm could run faster, but the circuit would require more memory.

Building off those results, MIT researchers have proposed a best-of-both-worlds approach that combines the speed of Regev's algorithm with the memory-efficiency of Shor's. This new algorithm is as fast as Regev's, requires fewer quantum building blocks known as qubits, and has a higher tolerance to quantum noise, which could make it more feasible to implement in practice.

In the long run, this new algorithm could inform the development of novel encryption methods that can withstand the code-breaking power of quantum computers.

"If large-scale quantum computers ever get built, then factoring is toast and we have to find something else to use for cryptography. But how real is this threat? Can we make quantum factoring practical?

"Our work could potentially bring us one step closer to a practical

implementation," says Vinod Vaikuntanathan, the Ford Foundation Professor of Engineering, a member of the Computer Science and Artificial Intelligence Laboratory (CSAIL), and senior author of a paper describing the algorithm.

The paper's lead author is Seyoon Ragavan, a graduate student in the MIT Department of Electrical Engineering and Computer Science. The research was presented at the 2024 International Cryptology Conference (Crypto 2024).

Cracking cryptography

To securely transmit messages over the internet, service providers like email clients and messaging apps typically rely on RSA, an encryption scheme invented by MIT researchers Ron Rivest, Adi Shamir, and Leonard Adleman in the 1970s (hence the name "RSA"). The system is based on the idea that factoring a 2,048-bit integer (a number with 617 digits) is too hard for a computer to do in a reasonable amount of time.

That idea was flipped on its head in 1994 when Shor, then working at Bell Labs, introduced an algorithm which proved that a quantum computer could factor quickly enough to break RSA cryptography.

"That was a turning point. But in 1994, nobody knew how to build a large enough quantum computer. And we're still pretty far from there. Some people wonder if they will ever be built," says Vaikuntanathan.

It is estimated that a quantum computer would need about 20 million qubits to run Shor's algorithm. Right now, the largest quantum computers have around 1,100 qubits.

A quantum computer performs computations using quantum circuits, just like a classical computer uses classical circuits. Each quantum

circuit is composed of a series of operations known as quantum gates. These quantum gates utilize qubits, which are the smallest building blocks of a quantum computer, to perform calculations.

But quantum gates introduce noise, so having fewer gates would improve a machine's performance. Researchers have been striving to enhance Shor's algorithm so it could be run on a smaller circuit with fewer quantum gates.

That is precisely what Regev did with the circuit he proposed a year ago.

"That was big news because it was the first real improvement to Shor's circuit from 1994," Vaikuntanathan says.

The quantum circuit Shor proposed has a size proportional to the square of the number being factored. That means if one were to factor a 2,048-bit integer, the circuit would need millions of gates.

Regev's circuit requires significantly fewer quantum gates, but it needs many more qubits to provide enough memory. This presents a new problem.

"In a sense, some types of qubits are like apples or oranges. If you keep them around, they decay over time. You want to minimize the number of qubits you need to keep around," explains Vaikuntanathan.

He heard Regev speak about his results at a workshop last August. At the end of his talk, Regev posed a question: Could someone improve his circuit so it needs fewer qubits? Vaikuntanathan and Ragavan took up that question.

Quantum ping-pong

To factor a very large number, a quantum circuit would need to run many times, performing operations that involve computing powers, like 2 to the power of 100.

But computing such large powers is costly and difficult to perform on a quantum computer, since quantum computers can only perform reversible operations. Squaring a number is not a reversible operation, so each time a number is squared, more quantum memory must be added to compute the next square.

The MIT researchers found a clever way to compute exponents using a series of Fibonacci numbers that requires simple multiplication, which is reversible, rather than squaring. Their method needs just two quantum memory units to compute any exponent.

"It is kind of like a ping-pong game, where we start with a number and then bounce back and forth, multiplying between two quantum memory registers," Vaikuntanathan adds.

They also tackled the challenge of error correction. The circuits proposed by Shor and Regev require every quantum operation to be correct for their algorithm to work, Vaikuntanathan says. But error-free quantum gates would be infeasible on a real machine.

They overcame this problem using a technique to filter out corrupt results and only process the right ones.

The end-result is a circuit that is significantly more memory-efficient. Plus, their error correction technique would make the algorithm more practical to deploy.

"The authors resolve the two most important bottlenecks in the earlier quantum factoring algorithm. Although still not immediately practical,

their work brings quantum factoring algorithms closer to reality," adds Regev.

In the future, the researchers hope to make their algorithm even more efficient and, someday, use it to test factoring on a real quantum circuit.

"The elephant-in-the-room question after this work is: Does it actually bring us closer to breaking RSA cryptography? That is not clear just yet; these improvements currently only kick in when the integers are much larger than 2,048 bits. Can we push this algorithm and make it more feasible than Shor's even for 2,048-bit integers?" says Ragavan.

More information: Space-Efficient and Noise-Robust Quantum Factoring: eprint.iacr.org/2023/1501.pdf

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: Researchers propose a smaller, more noise-tolerant quantum factoring circuit for cryptography (2024, August 23) retrieved 23 August 2024 from https://techxplore.com/news/2024-08-smaller-noise-tolerant-quantum-factoring.html