Quantum Computers Could Crack Encryption Sooner Than Expected With New Algorithm

One of the most well-established and disruptive uses for a future quantum computer is the ability to crack encryption. A new algorithm could significantly lower the barrier to achieving this.

Despite all the hype around quantum computing, there are still significant question marks around what quantum computers will actually be useful for. There are hopes they could accelerate everything from optimization processes to machine learning, but how much easier and faster they'll be remains unclear in many cases.

One thing is pretty certain though: A sufficiently powerful quantum computer could render our leading cryptographic schemes worthless. While the mathematical puzzles underpinning them are virtually unsolvable by classical computers, they would be entirely tractable for a large enough quantum computer. That's a problem because these schemes secure most of our information online.

The saving grace has been that today's quantum processors are a long way from the kind of scale required. But according to a report in Science, New York University computer scientist Oded Regev has discovered a new algorithm that could reduce the number of qubits required substantially.

The approach essentially reworks one of the most successful quantum algorithms to date. In 1994, Peter Shor at MIT devised a way to work out which prime numbers need to be multiplied together to give a particular number—a problem known as prime factoring.

For large numbers, this is an incredibly difficult problem that quickly becomes intractable on conventional computers, which is why it was used as the basis for the popular RSA encryption scheme. But by

taking advantage of quantum phenomena like superposition and entanglement, Shor's algorithm can solve these problems even for incredibly large numbers.

That fact has led to no small amount of panic among security experts, not least because hackers and spies can hoover up encrypted data today and then simply wait for the development of sufficiently powerful quantum computers to crack it. And although post-quantum encryption standards have been developed, implementing them across the web could take many years.

It is likely to be quite a long wait though. Most implementations of RSA rely on at least 2048-bit keys, which is equivalent to a number 617 digits long. Fujitsu researchers recently calculated that it would take a completely fault-tolerant quantum computer with 10,000 qubits 104 days to crack a number that large.

However, Regev's new algorithm, described in a pre-print published on arXiv, could potentially reduce those requirements substantially. Regev has essentially reworked Shor's algorithm such that it's possible to find a number's prime factors using far fewer logical steps. Carrying out operations in a quantum computer involves creating small circuits from a few qubits, known as gates, that perform simple logical operations.

In Shor's original algorithm, the number of gates required to factor a number is the square of the number of bits used to represent it, which is denoted as n^2. Regev's approach would only require $n^{1.5}$ gates because it searches for prime factors by carrying out smaller multiplications of many numbers rather than very large multiplications of a single number. It also reduces the number of gates required by using a classical algorithm to further process the outputs.

In the paper, Regev estimates that for a 2048-bit number this could reduce the number of gates required by two to three orders of magnitude. If true, that could enable much smaller quantum computers to crack RSA encryption.

However, there are practical limitations. For a start, Regev notes that Shor's algorithm benefits from a host of optimizations developed over the years that reduce the number of qubits required to run it. It's unclear yet whether these optimizations would work on the new approach.

Martin Ekerå, a quantum computing researcher with the Swedish government, also told Science that Regev's algorithm appears to need quantum memory to store intermediate values. Providing that memory will require extra qubits and eat into any computational advantage it has.

Nonetheless, the new research is a timely reminder that, when it comes to quantum computing's threat to encryption, the goal posts are constantly moving, and shifting to post-quantum schemes can't happen fast enough.

what quantum computers will actually be useful for

Quantum computing is expected to revolutionize a broad swathe of industries. But as the technology edges closer to commercialization, what will the earliest use cases be?

Quantum computing is still a long way from going mainstream. The industry had some significant breakthroughs in 2021 though, not least IBM's unveiling of the first processor to cross the 100-qubit mark. But the technology is still experimental, and has yet to demonstrate its usefulness for solving real-world problems.

That milestone might not be so far off, though. Most quantum computing companies are aiming to produce fault-tolerant devices by 2030, which many see as the inflection point that will usher in the era of practical quantum computing.

Quantum computers will not be general-purpose machines, though. They will be able to solve some calculations that are completely

intractable for current computers and dramatically speed up processing for others. But many of the things they excel at are niche problems, and they will not replace conventional computers for the vast majority of tasks.

That means the ability to benefit from this revolution will be highly uneven, which prompted analysts at McKinsey to investigate who the early winners could be in a new report. They identified the pharmaceutical, chemical, automotive, and financial industries as those with the most promising near-term use cases.

The authors take care to point out that making predictions about quantum computing is hard because many fundamental questions remain unanswered; for instance, the relative importance of the quantity and quality of qubits or whether there can be practical uses for early devices before they achieve fault tolerance.

It's also important to note that there are currently fewer than 100 quantum algorithms that exhibit a quantum speed-up, the extent of which can vary considerably. That means the first and foremost question for business leaders is whether a quantum solution even exists for their problem.

But for some industries the benefits look clearer than others. For drug makers, the technology holds the promise of streamlining the industry's long and incredibly expensive research and development process; the average drug takes 10 years and $2 billion to develop.

Quantum simulations could predict how proteins fold and tease out the properties of small molecules that could help produce new treatments. Once promising candidates have been found, quantum computers could also help optimize critical attributes like absorption and solubility.

Beyond research and development, quantum computers could also help companies optimize the clinical trials used to validate new

drugs, for instance by helping identify and group participants or selecting trial sites.

Quantum simulation could also prove a powerful tool in the chemical industry, according to the report. Today's chemists use computer-aided design tools that rely on approximations of molecular behavior and properties, but enabling full quantum mechanical simulations of molecules will dramatically expand their capabilities.

This could cut out the many rounds of trial-and-error lab experiments normally required to develop new products, instead relying on simulations to do the heavy lifting, with limited lab-based validation to confirm the results.

Quantum computers could also help to optimize the formulations used in all kinds of products—from detergents to paints—by modeling the complex molecular-level processes that govern their action.

For both the pharmaceutical and chemical industries, it's not just the design of new products that could be impacted. Quantum computers could also help improve their production processes by helping researchers better understand the reaction mechanisms used to create drugs and chemicals, design new catalysts, or fine-tune conditions to optimize yields.

In the automotive industry, the technology could significantly boost prototyping and testing capabilities. Better simulation of everything from aerodynamic properties to thermodynamic behavior will reduce the cost of prototyping and lead to better designs. It could even make virtual testing possible, reducing the number of test vehicles required.

As carmakers look for greener ways to fuel their vehicles, quantum simulations could also contribute to finding new materials and better designs for hydrogen fuel cells and batteries. But the biggest impact

could be on the day-to-day logistics involved in running a major automotive company.

Supply chain disruptions cost the industry about $15 billion a year, but quantum computers could simulate and optimize the sprawling global networks companies rely on to significantly reduce these headaches. They could also help fine-tune assembly line schedules to reduce inefficiencies and even optimize the movements of multi-robot teams as they put cars together.

Quantum computing's impact on the financial industry will take longer to be felt, according to the report's authors, but with the huge sums at stake it's worth taking seriously. The technology could prove invaluable in modeling the behavior of large and complex portfolios to come up with better investment strategies. Similar approaches could also help optimize loan portfolios to reduce risk, which could allow lenders lower interest rates or free up capital.

How much of this comes to pass depends heavily on the future trajectory of quantum technology.

Despite significant progress, there are still many unknowns, and plenty of scope for timelines to slip. Nonetheless, the potential of this new technology is starting to come into focus, and it seems that business leaders in those industries most susceptible to disruption would do well to start making plans.

As concerns mount surrounding the potential threat posed by quantum computing to existing cryptographic methods, Fujitsu today revealed that it conducted successful trials to evaluate the widely-used RSA cryptosystem (1) for possible vulnerability to code-cracking by quantum computers.

Fujitsu conducted the trials in January 2023 using its 39-qubit quantum simulator to assess how difficult it would be for quantum computers to crack

existing RSA cryptography, using a Shor's algorithm (2) to determine the resources necessary to perform such a task. Fujitsu researchers discovered that a fault-tolerant quantum computer (3) with a scale of approximately 10,000 qubits and 2.23 trillion quantum gates would be required to crack RSA —well beyond the capabilities of even the most advanced quantum computers in the world today. Researchers further estimated that it would be necessary to conduct fault-tolerant quantum computation for about 104 days to successfully crack RSA .

While the research reveals that the limitations of present quantum computing technology preclude the possibility of this threat in the short term, Fujitsu will continue to proactively evaluate the potential impact of increasingly powerful quantum computers on cryptography security, as well as the eventual need for quantum-resistant cryptography. Dr. Tetsuya Izu, Senior Director of Data & Security Research at Fujitsu Limited and Global Fujitsu Distinguished Engineer, commented: "Our research demonstrates that quantum computing doesn't pose an immediate threat to existing cryptographic methods. We cannot be complacent either, however. The world needs to begin preparing now for the possibility that one day quantum computers could fundamentally transform the way we think about security."

With plans to boost performance of its quantum simulator to 40 qubits by the first quarter of fiscal 2023, and recently revealed plans to build a 64 qubit superconducting quantum computer within fiscal 2023 with the cooperation of RIKEN, Fujitsu remains at the vanguard of research and development in this critical field.

Fujitsu will present parts of the results at the 2023 Symposium on Cryptography and Information Security (SCIS 2023) to be held from Tuesday, January 24 to Friday, January 27, 2023, in Kitakyushu City, Fukuoka Prefecture, Japan and online.

Background
RSA, a widely used standard cryptographic algorithm, represents a secure method to guarantee the confidentiality and integrity of data for digital

interactions including the transmission and reception of credit card information in online shopping and the exchange of messages in SNS.

The RSA cryptosystem is based on the fact that factoring a large integer is difficult. As current computers can factor composite numbers up to 829 bits (4), experts believe that an RSA cryptosystem with 2,048-bit key length (5) will remain secure with regard to future improvements in computing capabilities.

Despite this, concerns remain that once available, fault-tolerant quantum computers will be able to factor even huge composite numbers, and thus pose a potential threat to RSA cryptography. This means that one day, it will become necessary to shift from the RSA cryptosystem to alternative technologies such as post-quantum cryptography. Due to a lack of respective trials, estimating the computational resources necessary for quantum computers to actually perform integer factorization of 2,048 bits composite numbers remains a difficult task, and the timing of transition to alternative technologies remains unclear.

About the evaluation of the safety of RSA encryption using a quantum simulator

To address these issues, Fujitsu conducted factorization trials to confirm the safety of the RSA cryptosystem using Fujitsu's 39 qubit quantum simulator developed in September 2022.

Within the trials, Fujitsu implemented a general-purpose program using Shor's algorithm on a quantum simulator to generate a quantum circuit that factors the input composite number into prime factors. As a result, Fujitsu succeeded in factoring 96 RSA-type integers (a product of two different odd primes) from N = 15 to N = 511, and confirmed that the general-purpose program can generate correct quantum circuits.
By using the above general purpose program, Fujitsu further generated quantum circuits that factor several composite numbers from 10 bits to 25 bits, and estimated the required resources of the quantum circuits necessary for factoring 2,048 bits composite numbers from the calculated resources. As

a result, Fujitsu found that approximately 10,000 qubits, 2.23 trillion quantum gates, and a quantum circuit with a depth (6) of 1.80 trillion were required to factor a composite number of 2,048 bits. This equates to a 104-day long calculation using a fault-tolerant quantum computer. As a quantum computer that can operate stably and at such a large scale will not be realized in the short term, Fujitsu's tests quantitatively proved that the RSA cryptosystem is safe against the Shor's algorithm for the time being.

Within the trials, Fujitsu utilized its quantum simulator leveraging the high speed computing power of the CPU "A64FX" of the supercomputer "Fugaku" (7) and Fujitsu's massively parallel computing technology. Using a cluster system based on Fujitsu's 512 node supercomputer "FUJITSU Supercomputer PRIMEHPC FX700" hardware, which features the A64FX CPU, and a newly developed technology that automatically and efficiently rearranges the state information of quantum bits, Fujitsu achieved a speed increase of more than 100 times that of a system without rearrangement in 64 nodes, and was able to perform factoring of N = 253 in 463 seconds, which previously took 16 hours.

---

[1]
RSA cryptosystem :
Cryptographic system named for its developers Rivest, Shamir, and Adleman, that uses a private key for decryption and a public key for encryption. Even if the encryption key is made public, only those with the private key can correctly receive the information due to the difficulty of factoring.
[2]
Shor's algorithm :
A quantum algorithm developed in 1994 by Peter Shore, a theoretical computer scientist and mathematician in the United States, that can perform integer factorization at high speed.
[3]
fault-tolerant quantum computer :

A *quantum computer that is not limited by quantum bit noise or the upper limit of the number of quantum gates. It is used in conducting theoretical analysis.*
[4]
Current computers can factor composite numbers up to 829 bit :
Source: [Cado-nfs-discuss] Factorization of RSA-250 (archive.org)
[5]
Key length :
Length of a key in the cryptosystem. In RSA cryptosystem, the key length is the bit length of the composite number used as the decryption key and the encryption key. When using RSA cryptosystem, it is recommended to set the key length to 2,048 bits or more.
[6]
Depth :
The number of steps required to perform quantum computation in a quantum circuit.
[7]
Supercomputer "Fugaku" :
A computer jointly developed by RIKEN and Fujitsu as a successor to the K computer. Full operation started on March, 2021. From June 2020 to November 2021, it ranked first in 4 categories in the supercomputer rankings for 4 consecutive terms.