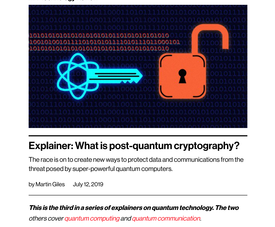


Explainer: What is post-quantum cryptography?

The race is on to create new ways to protect data and communications from the threat posed by super-powerful quantum computers.

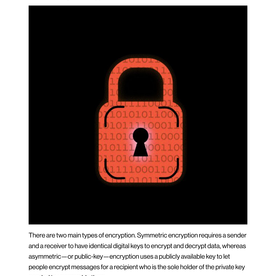
by Martin Giles July 12, 2019

This is the third in a series of explainers on quantum technology. The two others cover quantum computing and quantum communication.

Few of us give much thought to the tiny padlock symbol that appears in our web browsers every time we use an e-commerce site, send and receive emails, or check our bank or credit card accounts. But it's a signal that the online services are using HTTPS, a web protocol that encrypts the data we send across the internet and the responses we receive. This and other forms of encryption protect all kinds of electronic communications, as well as things like passwords, digital signatures, and health records.

Quantum computers could undermine these cryptographic defenses. The machines aren't powerful enough to do this today, but they are evolving fast. It's possible that in a little more than a decade—and perhaps even sooner—these machines could be a threat to widely used cryptography methods. That's why researchers and security firms are racing to develop new approaches to cryptography that will be able to withstand future quantum attacks mounted by hackers.

How does digital encryption work?



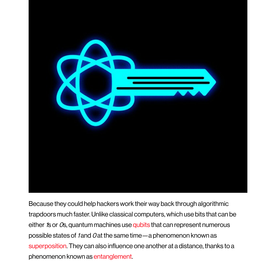
There are two main types of encryption. Symmetric encryption requires a sender and a receiver to have identical digital keys to encrypt and decrypt data, whereas asymmetric—or public-key—encryption uses a publicly available key to let people encrypt messages for a recipient who is the sole holder of the private key needed to unscramble them.

Sometimes these two approaches are used together. In the case of HTTPS, for instance, web browsers use public-key cryptography to check websites' validity and then establish a symmetric key to encrypt communications.

The goal is to stop hackers from using massive amounts of computing power to try to guess the keys being used. To do this, popular cryptography methods, including one known as RSA and another called elliptical curve cryptography, typically use so-called trapdoor functions—mathematical constructs that are relatively easy to compute in one direction to create keys, but are very hard for an adversary to reverse-engineer.

Hackers could try to break a code by trying all possible variations of a key until one works. But defenders make life really hard for them by using very long key pairs—like the RSA 2,048-bit implementation, which renders a key that is 617 decimal digits long. Running through all the possible permutations to derive the private keys could take many thousands—if not millions—of years on conventional computers.

Why are quantum computers a threat to encryption?



Because they could help hackers work their way back through algorithmic trapdoors much faster. Unlike classical computers, which use bits that can be either 1s or 0s, quantum machines use qubits that can represent numerous possible states of 1 and 0 at the same time—a phenomenon known as superposition. They can also influence one another at a distance, thanks to a phenomenon known as entanglement.

Thanks to these phenomena, adding just a few extra qubits can lead to exponential leaps in processing power. A quantum machine with 300 qubits could represent more values than there are atoms in the observable universe. Assuming quantum computers can overcome some inherent limitations to their performance, they could eventually be used to test all possible permutations of a cryptographic key in a relatively short time.

Hackers are also likely to exploit quantum algorithms that optimize certain tasks. One such algorithm, published by Lov Grover of AT&T's Bell Labs in 1996, helps quantum computers search possible permutations much faster. Another, published in 1994 by Peter Shor, who was then at Bell Labs and is now an MIT professor, helps quantum machines find the prime factors of integers incredibly fast.

Shor's algorithm poses a risk to public-key encryption systems such as RSA, whose mathematical defenses rely in part on how difficult it is to reverse-engineer the result of multiplying very large prime numbers together. A report on quantum computing published last year by the US National Academies of Sciences, Engineering, and Medicine predicted that a powerful quantum computer running Shor's algorithm would be capable of cracking a 1,024-bit implementation of RSA in less than a day.

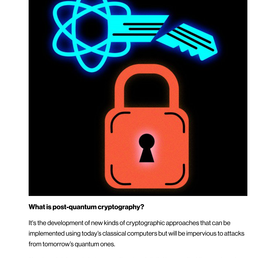
Will quantum computers breach cryptographic defenses soon?

That's highly unlikely. The National Academies study says that to pose a real threat, quantum machines will need far more processing power than today's best quantum machines have achieved.

Still, what some security researchers like to call "Y2Q"—the year in which quantum code-cracking becomes a major headache—may creep up surprisingly fast. In 2015, researchers concluded that a quantum computer would need a billion qubits to be able to crack the 2,048-bit RSA system pretty comfortably; more recent work suggests that a computer with 20 million qubits could do the job in just eight hours.

That's still way beyond the capabilities of today's most powerful quantum machine, with 128 qubits (see our qubit counter here). But advances in quantum computing are unpredictable. Without "quantum-safe" cryptographic defenses in place, all kinds of things, from autonomous vehicles to military hardware—not to mention online financial transactions and communications—could be targeted by hackers with access to quantum computers.

Any business or government planning to store data for decades should be thinking now about the risks the technology poses, because the encryption they use to protect it could later be compromised. It can take many years to go back and re-encode mountains of historical data with more robust defenses, so it would be better to apply these now. Hence a big push to develop post-quantum cryptography.



What is post-quantum cryptography?

It's the development of new kinds of cryptographic approaches that can be implemented using today's classical computers but will be impervious to attacks from tomorrow's quantum ones.

One line of defense is to increase the size of digital keys so that the number of permutations that need to be searched using brute computing power rises significantly. For instance, just doubling the size of a key from 128 bits to 256 bits effectively squares the number of possible permutations that a quantum machine using Grover's algorithm would have to search through.

Another approach involves coming up with more complex trapdoor functions that even a very powerful quantum machine running an algorithm like Shor's would struggle to crack. Researchers are working on a wide range of approaches, including exotic-sounding ones like lattice-based cryptography and supersingular isogeny key exchange.

The aim is to zero in on one or a few methods that can be widely adopted. The US National Institute of Standards and Technology launched a process in 2016 to develop standards for post-quantum encryption for government use. It's already narrowed down an initial set of 69 proposals to 26, but says it's likely to be around 2022 before draft standards start to emerge.

The pressure is on because encryption technologies are deeply embedded in many different systems, so unravelling them and implementing new ones can take a great deal of time. Last year's National Academies study noted that it took more than a decade to completely retire one widely deployed cryptographic approach that was shown to be flawed. Given the speed with which quantum computing is evolving, the world may not have that much time to tackle this new security threat.