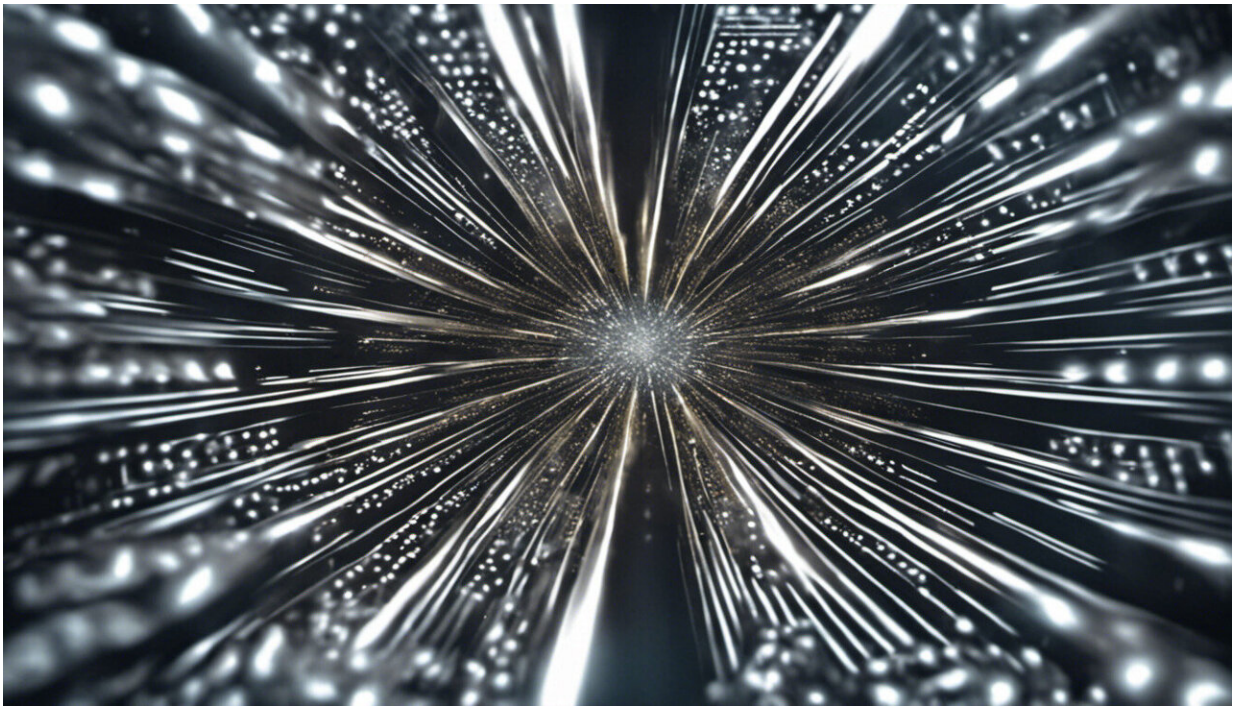
Will superfast 'quantum' computers mean the end of unbreakable encryption?

August 25 2016, by Keith Martin



Credit: AI-generated image (disclaimer)

There is a computing revolution coming, although nobody knows exactly when. What are known as "quantum computers" will be substantially more powerful than the devices we use today, capable of performing many types of computation that are impossible on modern machines. But while faster computers are usually welcome, there are some computing

operations that we currently rely on being hard (or slow) to perform.

Specifically, we rely on the fact that there are some codes that computers can't break – or at least it would take them too long to break to be practical. Encryption algorithms scramble data into a form that renders it unintelligible to anyone that does not possess the necessary decryption key (normally a long string of random numbers). This is what lets us send information securely over the internet. But will quantum computers mean we can no longer create encryption techniques that can't be broken?

For one system, known as symmetric encryption, quantum computing doesn't pose much of a threat. To break symmetric encryption you need to work out which (of many) possible keys has been used, and trying all possible combinations would take an unimaginable amount of time. It turns out that a quantum computer can test all these keys out in one square root of the time it would take existing computers – in other words, slightly less time but not so dramatically that we need to worry.

But for another type of encryption system, known as asymmetric or public-key encryption, it doesn't look so good. Public-key systems are used for things like securing the data that comes through your web browser. They encrypt data using a key that is available to anyone but need another private key for decryption.

The private key is related to the public key, so to break the encryption you would need to perform a very difficult calculation that would give you the private key. This would take a conventional computer an impractical amount of time. But when it comes to the two most common types of public-key encryption in use today, a quantum computer would be able to perform the calculations quickly enough to render them practically insecure.

Fortunately, we have already foreseen this pending disaster. Researchers across academia, government and industry are currently working hard to develop new public-key encryption techniques that rely on different, harder calculations that will be immune to the powers of a quantum computer. I am confident that these efforts will be successful, particularly since we already know some techniques that appear to work. By the time that quantum computers arrive, we will be ready.

Quantum computing represents a new type of computing environment where many amazing things will be possible. But when it comes to encryption, nothing much will change. Developing new encryption techniques won't require any special quantum trickery, just an awareness of what a quantum computer can do. And we'll probably see a long transition period where quantum computers are only available to some specialist organisations. This means that quantum-safe encryption techniques will need to work on the contemporary computers that the rest of us will still be using.

New lock, new house

My guess is that in a future world of quantum computers we will certainly have new encryption techniques, but the security of these techniques will be broadly comparable to those of today. The main reason I am confident of this is because the sources of weaknesses associated with encryption are likely to be just the same as they are today. Here's why.

Encryption is essentially a locking mechanism. A lock needs a key. If you put the best lock money can buy on the door of a house then you can be confident that the lock itself will not be broken. Quantum computing represents a new type of house, quantum-safe encryption a new type of lock that is fit for that house.

But if someone wants to break into that house, and they know the lock is good, then they won't try to bust the lock at all. Instead, they will look for other options. For example, they could try to steal the key or they could chuck a brick through the window. Broadly speaking, this is exactly what happens in most cyber security incidents today. Modern encryption is excellent, but we are less competent at protecting decryption keys and even worse at properly integrating encryption into wider systems. And I don't see this changing in a world of quantum computers, no matter how wonderful, whenever that will be.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation