Why our data might need protection from the future: Apple's 'Post-Quantum' security move

March 27 2024, by Shaun Chornobroff

Credit: Unsplash/CC0 Public Domain

Computing giant Apple recently announced it was taking steps to protect

the more than 1 billion people worldwide who use its iMessage app—from a threat that doesn't yet exist.

Hackers today might be able to steal your password, but they can't crack the "cryptographic keys" that lock down messages, at least not using the current generation of so-called classical computers, said University of Maryland computer science Professor Jonathan Katz.

But powerful quantum computers—machines that operate on completely different principles that allow them to do some operations exponentially more quickly—widely expected to become available in coming years, could make such security measures vulnerable.

Katz, an expert in quantum-secure cryptography who is a fellow in the Joint Center for Quantum Information and Computer Science, explained in an interview why these new quantum security measures are needed now, and what we may see in the future.

Why is Apple already talking 'post-quantum' when quantum computing is only in its infancy and no powerful, fully programmable quantum computers yet exist?

One thing is the possibility of quantum computers being built in the next decade or so, in which case we need to start being prepared now. But it's even more than that, because there's this issue that can happen where, if I encrypt a message to you today, or governments encrypt messages to each other today, an attacker could theoretically take that communication and just store it on their hard drive.

Then 10 years from now, if quantum computers come out, they can then use a quantum computer to decrypt that message. So that's why you need protection against quantum computers now, even though they may not exist for another decade.

Do hackers really want to dig through our texts? Most of them are pretty trivial.

If we're talking about the average user on the street sending a message to their friend, it's not important that the message remain secret for a decade. But if you have government-level communications, many times those need to remain classified for several decades. Then there's a concern about state-sponsored agencies going after those communications.

It seems likely that the first people who will develop quantum computers will be state-sponsored agencies because of the resources needed to develop them. Once developed, they're likely to remain classified, so that people won't know about them right away.

Is Apple protecting our texts with quantum computing, as some outlets have reported or implied?

No. The new protocol they deployed is entirely classical; it runs on classical computers like current iPhones and iPads. However, even though they are entirely classical, they are intended to provided security against adversaries who might use quantum computers to attack them.

How can classical computers of the present fight off futuristic quantum computers?

You must get a little bit into the math, but the point is that there are a couple of examples of classical mathematical problems, where we believe that they're hard, even for quantum computers.

What is the difference between traditional cryptography and quantum cryptography?

At a high level, it comes down to the mathematical problems that they're based on. Classical cryptography algorithms are primarily based on number theoretic-type problems, which involve the relationship between prime numbers, rational numbers and algebraic integers.

Now people are looking at new classes of mathematical problems that are believed to be hard even for quantum computers. One of the leading candidates for those problems is related to something called lattices. This is another mathematical object, but a little bit different from traditional number theory.

What can the public do now to better protect their iMessage communications?

The nice thing about it is that the new protocol will be available by default. Apple rolled out this new protocol and people are going to be using it, and they're protected automatically by using it.

The main thing is, if you care about the privacy of your messages, you need to make sure to use a protocol—a method or technique used to protect networks, systems and data from unauthorized access—that offers you encrypted messaging; not every protocol offers the same level of security. You need to choose one that offers a level of security you're comfortable with.

Provided by University of Maryland