CYBERSECURITY

Cyber Daily: Quantum Computing Could Wreck Encryption

WSJ Pro Cybersecurity Explainer: What Is Quantum-Safe Encryption?

IBM's 20-qubit machine quantum computer. PHOTO: IBM CORP.

By Catherine Stupp

Researchers warn that today's encryption is likely to be too weak to protect sensitive information when quantum computers become commercially available in the coming years.

Cryptographers are developing new algorithms that could resist the power of quantum computers, which are expected to be able to quickly solve mathematical problems that underpin common forms of encryption. While cyber experts with state-of-the-art tools can't break today's encryption, a quantum computer, scientists say, will be able to do it in minutes.

High hopes for quantum computing include smart digital assistants, systems to understand traffic patterns for self-driving cars, and speedy financial calculations, as WSJ CIO Journal has reported.

For cybersecurity professionals, the key question today is what will quantum do for and against encryption.

The U.S. and other countries are developing new types of encryption. In 2017, researchers used quantum-encryption to communicate between a satellite and stations based in China and Austria.

There's a time crunch: Commercial-grade quantum computers could be on the market within 20 years, according to a new working group led by**Princeton University** and the **Carnegie Endowment for International Peace**, a think tank.

The **National Institute of Standards and Technology** is playing a central role in deciding what encryption will be used in the coming years. In January, NIST chose 26 of 69 submitted algorithms designed to withstand

quantum computers for further evaluation. Researchers leading the initiative plan to approve standards for some of them by 2022.

That time frame poses a challenge for companies because they might need a decade or more to phase out old encryption systems, the Princeton and Carnegie Endowment research group said in an April report.

Some smart products secured by current encryption, such as cars, will need to be updated before quantum computers become available, even if they still function well. Car models require several years to develop, for example, said Thomas Pöppelmann, a senior staff engineer working on security architecture and cryptography research at German chip maker **Infineon Technologies AG**.

"It could mean that we replace a lot of devices or hardware that won't be secure in 10 years, even though the lifetime of those devices could be longer," Mr. Pöppelmann said. NIST is considering a proposal developed by Mr. Pöppelmann and a group of other researchers.

How will quantum-safe encryption be different from today's encryption? A common form of encryption protects messages with a public key, which a person can decrypt with a private key. In that interaction, a user doesn't share the private key. That method, known as public key encryption, was developed in the 1970s. Researchers say it will be vulnerable because it is based on mathematical problems that quantum computers easily solve.

Public key cryptography protects customers' information when they log into online banking applications, for example, said Dustin Moody, a mathematician who is leading NIST's initiative to approve post-quantum encryption standards.

Quantum computers won't be able to break all encryption, but they will weaken public key cryptography, said Mike Hamburg, a cryptographer who submitted a proposal for quantum-safe public key encryption to NIST.

While current encryption algorithms rely on prime numbers, new forms of post-quantum encryption will be based on different systems. The most well known type is lattice-based encryption that uses geometric structures to form complex mathematical problems.

"You can't solve them by factoring prime numbers so they're resistant to faster computing," said Roger Grimes, a security analyst at cybersecurity firm **KnowBe4 Inc.**

How do we know future forms of encryption will be safe from cyberattacks? Information about the proposals is public and NIST encourages outside researchers to study the proposals. Experts at the standards body test every algorithm for bugs. Researchers around the world are now scrutinizing the proposals and pointing out flaws.

Mr. Pöppelmann said debate among academics can be heated: He sometimes receives 10 to 20 emails a day through mailing lists where researchers discuss the algorithms and point out security problems.

In the past few weeks, one group of applicants told NIST that there were security problems in the algorithm they submitted, Mr. Moody said. He declined to name the algorithm those researchers developed and said they would publicly disclose the flaws soon.

"You can't completely prove a cryptography system can never be broken," Mr. Moody said. "The best we can do is say we've had a lot of smart people in industry, government and academia look at this."

What do companies need to know about using quantum-safe encryption? Experts recommend that corporate cybersecurity teams plan out what products and information they might need to protect with new encryption that could resist quantum computers.

In addition, quantum-safe algorithms could slow down some devices and companies might need to upgrade to more powerful computers to implement new forms of encryption. “Some low-cost or legacy devices will not provide a sufficient amount of resources for post quantum cryptography and investments in more powerful hardware will be required,” according to a 2017 report from the **Fraunhofer Institute for Secure Information Technology** in Germany.