THE WALL STREET JOURNAL.

https://www.wsj.com/articles/the-race-to-save-encryption-11559646737

BUSINESS | JOURNAL REPORTS: TECHNOLOGY

The Day When Computers Can Break All Encryption Is Coming

Quantum computers will be able to overpower current encryption within a decade. That has security experts scrambling to come up with new ways to protect our data before it is too late

ILLUSTRATION: JUSTIN METZ

By Christopher Mims
June 4, 2019 7:12 am ET

National-security experts and politicians have a message for America: A significant portion of the sensitive data we have today is going to be cracked by foreign powers in the not-too-distant future, and there is nothing anyone can do about it.

But we might be able to stop them from decoding the data we produce down the road, if we act quickly enough.

The danger comes from an ultrapowerful and still-experimental technology called quantum computing—which leverages the quantum properties of atoms to quickly compute problems that no conventional computer could crack. China has already launched the equivalent of a Manhattan Project in order to achieve this end, say experts, and companies like Google, Microsoft MSFT **-0.60%** ▼ and IBM IBM **0.53%** ▲ are all pushing ahead with their own efforts to create quantum computers.

Quantum computers, which are still in the very early stage, could revolutionize any number of real-world tasks, from researching new materials to picking the best route for delivery drivers. But right now, what many experts worry about is the problem of security.

“Whoever gets to true quantum computing first will be able to negate all the encryption that we’ve ever done to date,” Rep. Will Hurd, R-Texas, has said.

The critical race

This is why China and Russia are hacking every system they can get into, including banking, health care, military and intelligence, and downloading huge troves of data, added Rep. Hurd.

The information is currently indecipherable to them, but could become intelligible with quantum computers.

JOURNAL REPORT

- Read more at WSJ.com/journalreporttech

MORE IN CYBERSECURITY

- Our Emotional Attachment to Our Passwords
- Can the Sound of Your Typing Be Decoded?
- The Tussle Over Facial Recognition
- How Not to Be Hacked at an ATM

In the future, hackers could also intercept and decrypt new data as it is produced. If we don't act in time, it is possible that a foreign power with a sufficiently powerful quantum computer could hack into central nodes of the internet, capture the fire hose of traffic passing through them and start decoding much of what we now consider secure.

Researchers and security agencies are trying to beat foreign governments to the punch by coming up with quantum computers and new encryption methods as quickly as possible. But they face technical stumbling blocks, such as coming up with standards for researchers to use and then rolling out new measures in time. There are potential interim solutions, but some experts fear that even those can't be implemented quickly enough, as quantum projects ramp up overseas.

Quantum computers are so different from conventional computers that, arguably, the only thing the two have in common is that they both compute. Rather than circuits and processors, the new technology uses complex physics to cram large amounts of information into a single subatomic particle.

To completely mathematically describe a caffeine molecule, for example, would require a conventional supercomputer so big that it would occupy 1/10th the volume of the Earth, says Arvind Krishna, IBM's senior vice president of cloud and cognitive software. A quantum computer that could do the same would be the size of a coffee table.

Today's data are encrypted using systems that can only be cracked by software that can factor very large numbers, sometimes over 300 digits. This is an extremely difficult problem for a conventional computer but a relatively trivial problem for a quantum computer.

Currently, even if someone obtained a copy of everyone's bank record in the U.S., good cybersecurity practice means that the information is almost certainly encrypted in a way that has rendered it into incomprehensible gibberish. But once quantum computers can crack the encryption that is typically applied to data as it is transmitted and when it is at rest, all bets are off, says Dr. Krishna.

Thus, if a quantum computer of sufficient power could be built, passwords, financial transactions, emails, text messages, intellectual property, secret communiqués within and between the CIA, NSA, FBI, the rest of the federal government and all of our most important military assets—it would be as if all of it were suddenly being sent in the clear, unencrypted.

Experts at work

The good news is that many of the smartest mathematicians and cybersecurity experts in the world, employed by Google, Microsoft, IBM and the federal government, as well as many other tech giants, are well aware of the problem and have been cooking up solutions for years.

They're working on a completely different scheme of encryption, called quantum-safe encryption. This kind of encoding can be achieved by today's computers, in about the same amount of time that current encryption requires, but it can't be cracked by conventional or quantum computers, hence the moniker "quantum safe."

There are dozens of proposed algorithms for quantum-safe encryption, but the most popular approach, called lattice encryption, works by encoding information in a multidimensional "lattice" of data. Picture a three-dimensional grid of dots, add another hundred or so dimensions, and you get the idea.

But before quantum-safe encryption can get everywhere that it needs to be, it must first become an agreed-upon standard, and then developers, companies and government bodies must translate it into code and insert it into countless services and systems.

A project to create standards at the National Institute of Standards and Technology began in 2016, and probably won't be completed until around 2022, says Dustin Moody, a mathematician at the institute and the project lead for the institute's post-quantum cryptography standardization project.

If history is any guide, rolling out this quantum-safe standard will subsequently take five to 10 years, he adds. That transition could be sped up if there were a greater sense of urgency around this problem, and that is exactly what we need, says Dr. Krishna.

"Quantum computers will crack today's encryption within a decade," he adds.

SHARE YOUR THOUGHTS

What should the U.S. be doing to better prioritize cybersecurity? Join the conversation below.

IBM's researchers are working on lattice-encryption algorithms, and some of the ones they have created are under consideration by NIST, which is in the process of narrowing down a list of 26 possible quantum-safe algorithms.

It is important to note that 10 years is on the more aggressive end of predictions for when dangerous quantum computers will come online—"Q2K," as Rep. Hurd has called it. Others think it could take 15, 20, even 30 years, says Elsa Kania, an adjunct senior fellow at the Center for a New American Security who has interviewed dozens of experts on this topic and is a co-author of a report on the threat of quantum technologies.

In a way, it is the Y2K problem all over again, except this time it is about encryption instead of truncated dates. Of course, Y2K wasn't the disaster everyone thought it might be, in part because we updated critical systems in time; if we can do the same in anticipation of quantum computers, things could continue humming with the only inescapable outcome being a retroactive decoding of decades-old data by foreign governments.

A December 2018 report from the National Academy of Sciences cautions that there are many unknowns about how quickly physicists and engineers will be able to achieve quantum computers powerful enough to be a threat to current encryption schemes. Some of these schemes can be made quantum safe even without complex fixes like lattice encryption, simply by doubling the length of the "key," or the large numbers used to encipher data, a solution that would be easy to implement on current systems.

The report also allows, however, that the field of quantum-algorithm design is still in its earliest stages. It is possible that there are yet-to-be-discovered algorithms that are much more efficient than the ones that have been proposed, which could move up by years the date by which quantum computers will defeat classical encryption.

The incentive to do so is tremendous, which is why "I think it's widely believed that any government with a good amount of resources would be actively working on this," says Dr. Moody.

China's government is nearing completion on construction of an 880-acre national laboratory for quantum information science and technology in Hefei, and the country's scientists regularly set world records for the size and power of their quantum computers. China is spending tens of billions on researching quantum computing and related application in communication and sensing, says Ms. Kania, and U.S. spending is low by comparison, on the order of $1.2 billion at the federal level, through the National Quantum Initiative Act. If there is a modern-day equivalent of the Manhattan Project happening anywhere in the world in order to achieve a

quantum computer, it is happening in China and not the U.S., she adds.

Yet even if Google, Microsoft, IBM, the NSA or the labs provisioned by other governments revealed tomorrow a quantum computer of sufficient power, "the transition to quantum-safe algorithms won't happen instantaneously," Dr. Moody says. "Even when there are urgent threats, it doesn't happen as easily and quickly as people would like."

Mr. Mims writes The Wall Street Journal's Keywords column. He can be reached at christopher.mims@wsj.com.

GREAT MOMENTS IN ENCRYPTION

People have found all sorts of ways to encrypt their communications over the centuries. Here is a sampling.

Caesar's Cipher
Romans such as Julius Caesar encrypted sensitive and personal messages with a simple cipher that shifted letters in the alphabet a certain number of places— substituting D for A and E for B, for example. It was a relatively secure encryption method at a time when few people could even read.

World War II Breakthrough
In 1943, the U.S. deployed SIGSALY, a roomsized terminal that encrypted high-level conversations between people such as Franklin Roosevelt and Winston Churchill during World War II. SIGSALY converted their speech to a digital format, an innovation at the time, and scrambled it. The key in this system involved noise recorded onto identical records that were distributed to both parties and played on turntables at the same time, and then destroyed.

Modern Standards
In modern encryption, algorithms are used to encrypt and decrypt data, with the help of a secret key—often a randomly generated series of bits. In 1976, the Data Encryption Standard, an algorithm based on a design by IBM, became the federal standard for securing sensitive data. It has since been superseded by AES, which uses multiple, larger key sizes and is more secure

The Public Key
One weakness of DES and AES is that both parties need to have the same secret key— which means the key must be exchanged securely. RSA, introduced in 1977, was the first widely adopted encryption that uses both a public key and a private key that doesn't have to be shared. Keys are generated by mathematical problems that current computers can't easily crack, such as factoring the product of two large prime numbers

Sources: Joshua Holden, author of "The Mathematics of Secrets"; University of Virginia professor David Evans; NIST, NSA

—Compiled by Chris Kornelis

Appeared in the June 5, 2019, print edition as 'The Race to Save Encrypt1on.'

- **Leadership**
- **Retirement**
- **Small Business**
- **Technology**
- **Wealth Management**