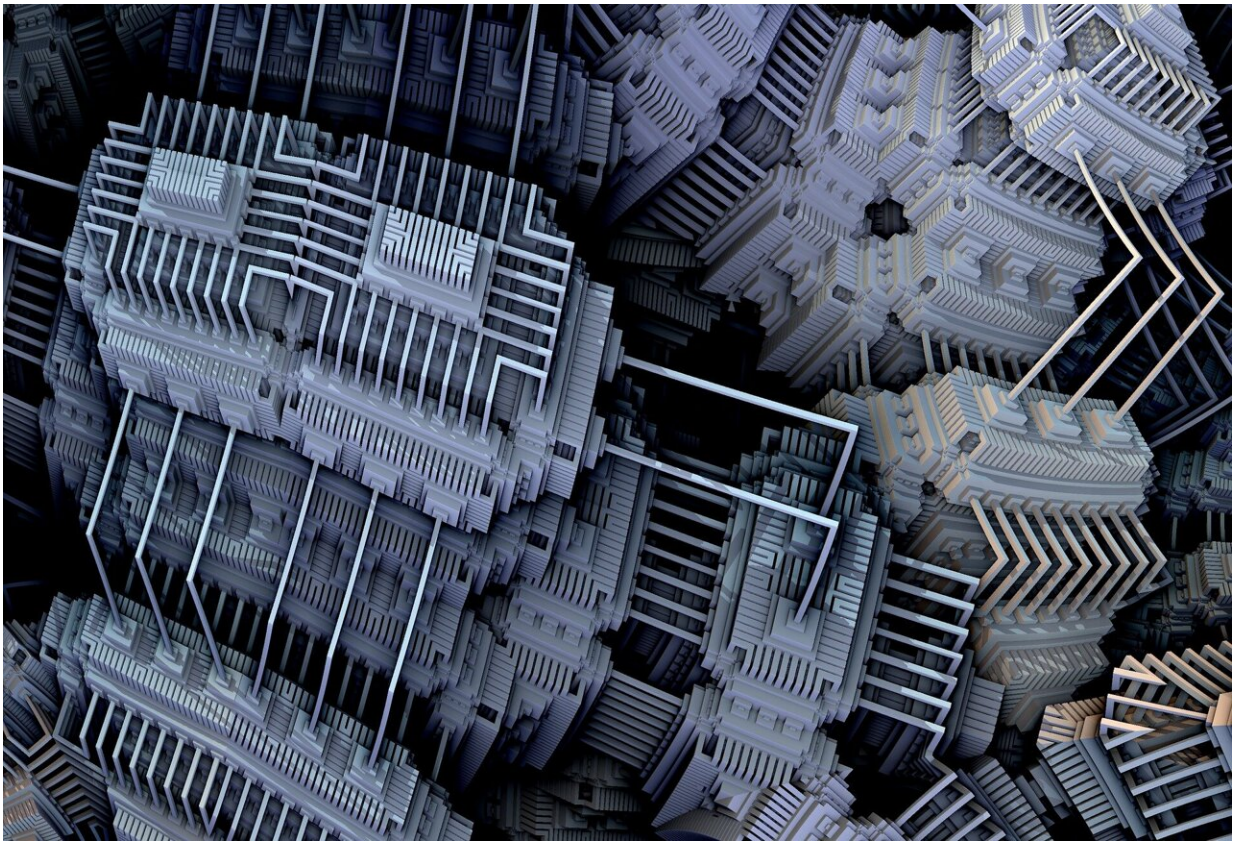
As quantum computers advance, encryption methods will need to keep up

April 29 2024, by Nalini Joshi



Credit: Pixabay/CC0 Public Domain

Imagine the tap of a card that bought you a cup of coffee this morning also let a hacker halfway across the world access your bank account and buy themselves whatever they liked. Now imagine it wasn't a one-off

glitch, but it happened all the time: imagine the locks that secure our electronic data suddenly stopped working.

This is not a science fiction scenario. It may well become a reality when sufficiently powerful quantum computers come online. These devices will use the strange properties of the quantum world to untangle secrets that would take ordinary computers more than a lifetime to decipher.

We don't know when this will happen. However, many people and organizations are already concerned about so-called "harvest now, decrypt later" attacks, in which cybercriminals or other adversaries steal encrypted data now and store it away for the day when they can decrypt it with a quantum computer.

As the advent of quantum computers grows closer, cryptographers are trying to devise new mathematical schemes to secure data against their hypothetical attacks. The mathematics involved is highly complex—but the survival of our digital world may depend on it.

'Quantum-proof' encryption

The task of cracking much current online security boils down to the mathematical problem of finding two numbers that, when multiplied together, produce a third number. You can think of this third number as a key that unlocks the secret information. As this number gets bigger, the amount of time it takes an ordinary computer to solve the problem becomes longer than our lifetimes.

Future quantum computers, however, should be able to crack these codes much more quickly. So the race is on to find new encryption algorithms that can stand up to a quantum attack.

The US National Institute of Standards and Technology has been calling

for proposed "quantum-proof" encryption algorithms for years, but so far few have withstood scrutiny. (One proposed algorithm, called Supersingular Isogeny Key Encapsulation, was dramatically broken in 2022 with the aid of Australian mathematical software called Magma, developed at the University of Sydney.)

The race has been hotting up this year. In February, Apple updated the security system for the iMessage platform to protect data that may be harvested for a post-quantum future.

Two weeks ago, scientists in China announced they had installed a new "encryption shield" to protect the Origin Wukong quantum computer from quantum attacks.

Around the same time, cryptographer Yilei Chen announced he had found a way quantum computers could attack an important class of algorithms based on the mathematics of lattices, which were considered some of the hardest to break. Lattice-based methods are part of Apple's new iMessage security, as well as two of the three frontrunners for a standard post-quantum encryption algorithm.

What is a lattice-based algorithm?

A lattice is an arrangement of points in a repeating structure, like the corners of tiles in a bathroom or the atoms in a diamond crystal. The tiles are two dimensional and the atoms in diamond are three dimensional, but mathematically we can make lattices with many more dimensions.

Most lattice-based cryptography is based on a seemingly simple question: if you hide a secret point in such a lattice, how long will it take someone else to find the secret location starting from some other point? This game of hide and seek can underpin many ways to make data more

secure.

A variant of the lattice problem called "learning with errors" is considered to be too hard to break even on a quantum computer. As the size of the lattice grows, the amount of time it takes to solve is believed to increase exponentially, even for a quantum computer.

The lattice problem—like the problem of finding the factors of a large number on which so much current encryption depends— is closely related to a deep open problem in mathematics called the "hidden subgroup problem".

Yilei Chen's approach suggested quantum computers may be able to solve lattice-based problems more quickly under certain conditions. Experts scrambled to check his results—and rapidly found an error. After the error was discovered, Chen published an updated version of his paper describing the flaw.

Despite this discovery, Chen's paper has made many cryptographers less confident in the security of lattice-based methods. Some are still assessing whether Chen's ideas can be extended to new pathways for attacking these methods.

More mathematics required

Chen's paper set off a storm in the small community of cryptographers who are equipped to understand it. However, it received almost no attention in the wider world—perhaps because so few people understand this kind of work or its implications.

Last year, when the Australian government published a national quantum strategy to make the country "a leader of the global quantum industry" where "quantum technologies are integral to a prosperous, fair and

inclusive Australia," there was an important omission: it didn't mention mathematics at all.

Australia does have many leading experts in quantum computing and quantum information science. However, making the most of quantum computers—and defending against them—will require deep mathematical training to produce new knowledge and research.

Provided by The Conversation

Citation: As quantum computers advance, encryption methods will need to keep up (2024, April 29) retrieved 17 May 2024 from https://techxplore.com/news/2024-04-quantum-advance-encryption-methods.html