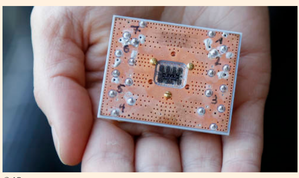
Quantum technologies

Why you need to quantum-proof your cyber security now

The quantum threat comes just as the internet of things and 5G mobile connectivity are arriving, with higher security requirements



© AP

October 17, 2018 4:01 am by Ilyas Khan

For close to 40 years, quantum computing has been seen as a curious but exciting mix of science fiction and hard computer science somewhere in the distant future.

In the past 10 years, however, large organisations such as Microsoft, Google and IBM have invested more heavily in quantum computing, which uses quantum mechanics rather than binary digital transistors for its calculations. Tools that had previously been theoretical have materialised. Quantum computing is no longer "decades away".

IBM started giving the public access to a basic quantum computer in the cloud in 2016 and, so far, more than 100,000 people have run more than 6.7m experiments on it. This year, the first quantum computers came into use. These noisy intermediate-scale quantum, or NISQ, computers are not error-corrected and therefore only able to accomplish part of what full quantum computers will be able to do, but people are now able to move beyond theory.

Not surprisingly, the main area of concern emerging for governments and large corporations is security and encryption. Quantum technologies dramatically move the boundaries of what can be computed. Calculations that would take advanced supercomputers thousands of years to perform will eventually be done in less than a minute by quantum computers. At some point this will render whole swaths of current encryption technologies obsolete.

Governments are aware of the security threat. The US House of Representatives recently passed the Quantum Computing Research Act, which aims to establish a new federal programme to advance quantum technologies. Tellingly, the bill is being managed through the US Senate by the armed services committee.

The US National Institute of Standards and Technology, meanwhile, recently unveiled a consortium to support the quantum industry. A new cohort of companies such as Intel, Hitachi and Huawei are also entering the fray alongside more established players. It is critical that companies and governments adopt quantum-secure methods sooner rather than later to replace existing methods of encryption.

I often use the analogy of a child in a room to highlight the difference between "secure" encryption and "unhackable" methods of securing data. Imagine a three-month-old infant in a room with an unlocked door. The baby is incapable of escaping; it is secure. A toddler in that same room simply walks up to the door, turns the handle, and walks out. Secure suddenly becomes vulnerable.

The quantum threat comes just as the internet of things and 5G mobile connectivity are arriving, with higher security requirements than we have had before. There are broadly two ways to create a quantum secure future. One is to create new algorithms that, in the view of many mathematicians and computer scientists, not even the most powerful quantum computers will be able to breach. Organisations such as NIST have a list of such "quantum-proof" constructs with names such as "lattice-based" or "hash-based" protocols, and some organisations may decide this is the way to become quantum-proof.

However, being reliant on algorithms is risky. As man-made constructs, these will always have patterns that are capable of being unpicked. The history of the past 25 years shows just how quickly today's secure algorithm is tomorrow's vulnerability. AES-256 encryption, for example, which secures much of the internet backbone and which has been widely touted as "uncrackable", was hacked by Dutch security researchers last year.

The second alternative is building a physical solution based on quantum mechanics. Unlike algorithms, quantum computers can produce truly random numbers with no patterns. Only these can withstand hacking attempts by other quantum computers. The first commercially available quantum security solutions will start to be deployed in 2019.

The commercialisation of quantum technologies will continue as we move into 2019. According to Gartner, the US research group, within five years more than 20 per cent of all companies will be investing in quantum computing products, including quantum secure encryption, to ensure their safety from cyber attacks.

The writer is chief executive of Cambridge Quantum Computing

View comments

Latest on

Technology sector

SoftBank voices doubts over second Vision Fund
October 17, 2018 11:31 am

Fun facts about quantum computing
October 17, 2018 10:32 am

Netflix subscriber growth shoots past estimates
October 17, 2018 9:47 am

Samsung buys Spanish networks analysis firm in 5G push
October 17, 2018 9:06 am

Cyber Security — Internet of Things
October 17, 2018 4:02 am