Keeping secrets in the age of quantum computing

By Aline Gouge

19 Nov 2018

The dramatically enhanced computing power offered by quantum technology could compromise traditional cryptography - but the industry is working hard to come up with solutions.

With the advent of quantum computing, technological capabilities are set to take a substantial leap forward. But at the same time, quantum computing may also present new security challenges owing to the sheer processing power it offers.

This new computing paradigm could be used crack cryptographic codes that have until now been regarded as unbreakable: codes like the public key infrastructures (PKIs) around which most secure communications are currently built.

Aline Gouge is technical advisor and security researcher, Gemalto

This is a potentially ominous development, but leading industry players have already recognised the issue and are taking steps to address it. And that makes quantum computing something to be welcomed, rather than feared.

Quantum computing performs data calculations in a radically new way, superseding the transistors upon which computing has relied since the 1960s (and which are reaching the very limits of their potential).

Instead, quantum computing encodes data differently by exploiting the ability of sub-atomic particles to exist in more than one state at a time. Because these particles on an order of magnitude smaller than transistors could ever possibly be, far

more data can be stored and manipulated far faster.

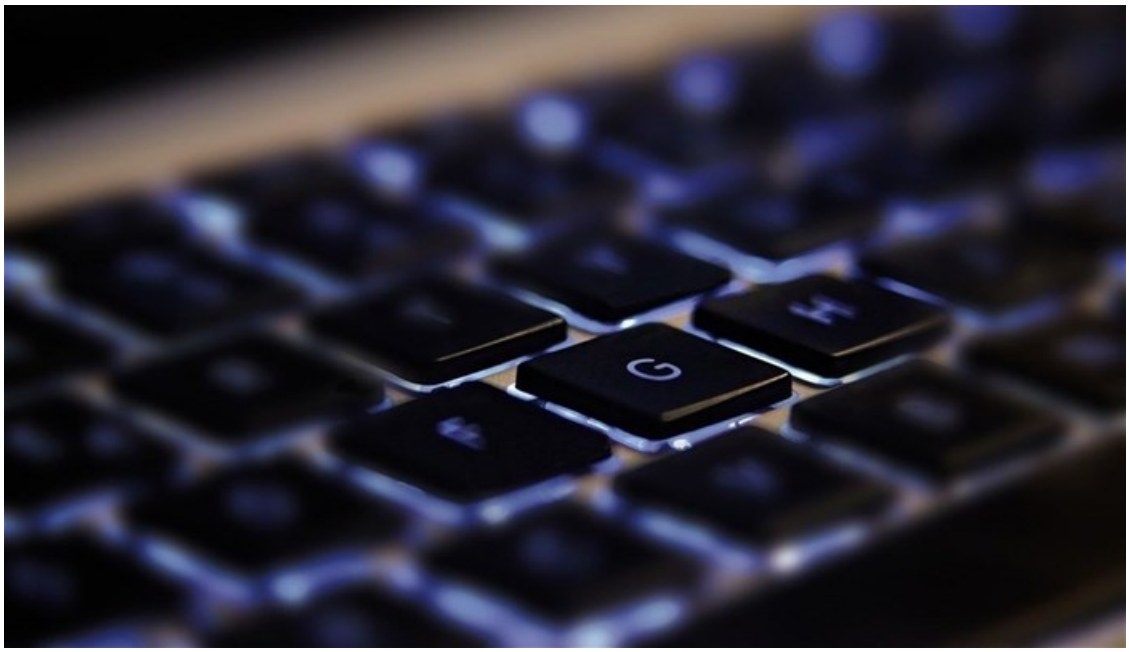
It's time to take note of quantum computing

17 Oct 2018

In other words, problems which cannot be tackled by traditional machines aren't an issue for quantum computers.

Breaking the unbreakable

Among those problems is the breaking of formerly unassailable cryptography used for securing data and communications. Cryptographic algorithms that may be weakened by the deployment of quantum computing include public key-based methodologies such as RSA and elliptic-curve cryptography for PKI applications, and applications for exchanging cryptographic keys over a public channel (such as the Diffie-Hellman key exchange).



Source: pixabay.com

What these algorithms have in common is that they were previously thought impossible to break given that the number of calculations required to test every possible combination of keys was just too great for any computer to tackle - even a supercomputer. Quantum computing's enormous power changes the picture.

And it could happen soon. Michele Mosca, from the Institute for Quantum Computing, said there is "...a one-in-seven chance that some fundamental public key crypto will be broken by quantum by 2026, and a one in two chance of the same by 2031".

If that happened, a lot of what we take for granted on the internet simply wouldn't be safe to use. Among these would be things like paying with credit cards, exchanging sensitive information, or accessing applications for business.

On the ball

Companies like Gemalto are already working on products which embed "crypto-agility". This involves developing software which could replace keys and algorithms if they were to be compromised or become obsolete. This mechanism enables the maintenance of a fleet of resistant products, even if algorithms were exposed as vulnerable.

> *Choosing an algorithm which is more resistant to quantum computing is an additional measure which can be taken. Resistant products use symmetric key algorithms with larger keys, ones which are proven quantum-safe (such as hash-based signatures) and those which combine pre- and post-quantum algorithms.*
>
> This last option allows computing to approach the future without abandoning today's effective cryptography, which the security industry has well and truly mastered.

Multiple industry players are actively involved in the search for answers to the new challenges which come with the imminent introduction of quantum computing. Protecting the future of public key encryption depends on creating algorithms resistant to quantum computing while also capable of working with "classic" computers.

New public key cryptographic systems that meet the criteria are currently under development and evaluation. NIST (the US National Institute for Standards and Technology) recently received over 80 submissions in response to a call out to research teams. After vetting these proposals, standardisation work will start, with deliverables expected in 2019.

7 digital disruptions CIOs may not see coming
23 Oct 2018

As quantum computing begins to mature and become commercially used, both companies and state entities will need to have plans in place to protect their networks, and the data on them, from the threat this new technology could pose. If, as anticipated, Africa exploits the potential of digital technologies to power its economic growth, care must be taken to stay abreast of developments in quantum computing per se, and in the development of quantum cryptography as well.

A lesson from history

Back in the 1940s, Allied codebreakers successfully unlocked Germany's "unbreakable" Enigma machine ciphers using a landmark electro-mechanical device called the "bombe". Quantum computing today is the equivalent new generation of technology poised to undermine supposedly infallible cryptographic techniques.

However, quantum computing is simultaneously opening the door to completely new data security approaches. While it is still very early days, these are exciting times and it is well worth staying abreast of developments. In other words, don't just keep calm and carry on. Stay tuned, too.

ABOUT THE AUTHOR

Aline Gouge is technical advisor and security researcher, Gemalto