cpl.thalesgroup.com

THALES

Quantum computing & quantum-safe security

White Paper

Contents

What's in this paper?

This paper looks at the implications of quantum computing on the cybersecurity landscape.

It explores what the technology is, alongside its benefits and threats. It also analyzes the need for quantum-safe cybersecurity measures; discussing solutions available today that can protect against quantum threats, alongside those that will be available in the near future.

Finally, this paper explains the need for organizations to embrace crypto-agility within their encryption solutions, so that they remain secure both today, and in the post-quantum era.

Quantum computing

Since work on quantum computing first began in the 1980s, when physicist Paul Benihoff proposed a quantum mechanical model of the Turing machine, the scientific and technological communities have touted it as 'the next big thing'.

Later, American theoretical physicist Richard Feynman and Russian mathematician Yuri Manin suggested that such a computer had the potential to do things a classical computer could not.

This claim was all-but proven in 1994, when MIT professor of applied mathematics Peter Shor developed a quantum algorithm for factoring integers (also known as prime factorization).

The now famous Shor's algorithm implies that public key cryptography, which uses this technique to generate keys, could be easily broken by a sufficiently powerful quantum computer running it.

The immense computing power of a quantum computer means that such encryption techniques could be broken in a matter of days, or even hours, while a 'classical' computer would take thousands of years to perform the equivalent task.

From theory to practice

Experimental quantum computers have been in the lab since the late 1990s, with progress being what could be described as steady at best for many years.

However, more recent times have seen great strides forward. Driven by Moore's Law, tech giants including IBM, Google, Microsoft and Amazon have entered the fray; either manufacturing their own quantum computers, or partnering with other manufacturers, in order to further R&D and open the technology to commercial markets.

Perhaps the most important announcement since Shor's algorithm was made in October 2019, when a paper published by Google and NASA claimed to have achieved 'quantum supremacy'; the point at which a quantum computer can solve problems that are practically unsolvable by classical computers.

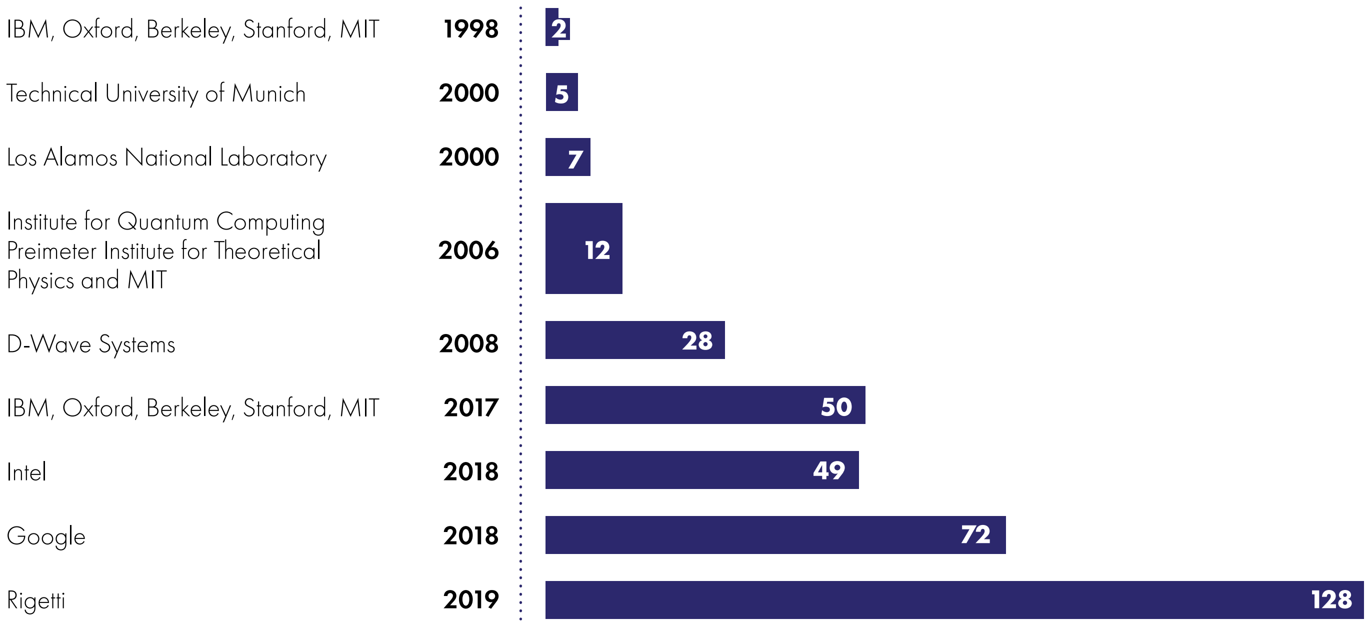
Growing awareness

In what used to be confined to scientific publications, news of quantum computing's development has become the focus of major media outlets.

Moreover, publications including the Cloud Security Alliance's 'Preparing Enterprises for the Quantum Computing Cybersecurity Threats' and Hudson Institute's 'Executive's Guide to Quantum Computing and Quantum-secure Cybersecurity' show an effort to raise the profile of the technology among IT and cybersecurity professionals, as well as in the C-suite.

20 Years of quantum computing growth

Quantum computing systems produced by organization(s) in qubits, between 1998 to 2019*



* Rigetti announced in August 2018 that it would release a 128-qubit quantum computer system within the next 12 months. 20 Years of Quantum Computing Growth, via https://www.statista.com/chart/17896/quantum-computing-developments/ Source: CB Insights

What is quantum computing?

While classical computers code information into bits, sending electrical or optical pulses representing 1s and 0s (a binary code) as first devised by Alan Turing in the 1930s, quantum computers use quantum bits (known as qubits).

These qubits, typically subatomic particles such as electrons or photons, can store information as 1s, 0s or anywhere between these values due to a principal called superposition.

In short, this means that qubits can store more information than bits, and therefore their computational power is exponentially greater.

Quantum computers in the real world

Rather than replacing classical computers, it seems that quantum computers will complement them.

Reasons behind this include, but are not limited to:

- The size and cost of manufacturing today's quantum computers
- The near-absolute zero conditions that many quantum computers must be housed in
- Their unsuitability to everyday tasks that classical computers perform

More likely, access to quantum computers will be provided 'as a service' in the cloud, as has already been indicated by the likes of Microsoft[1] and Amazon[2].

The quantum age

Fully-fledged, commercial quantum computers will have the power to change computing as we know it, but when this will happen is a subject of much debate.

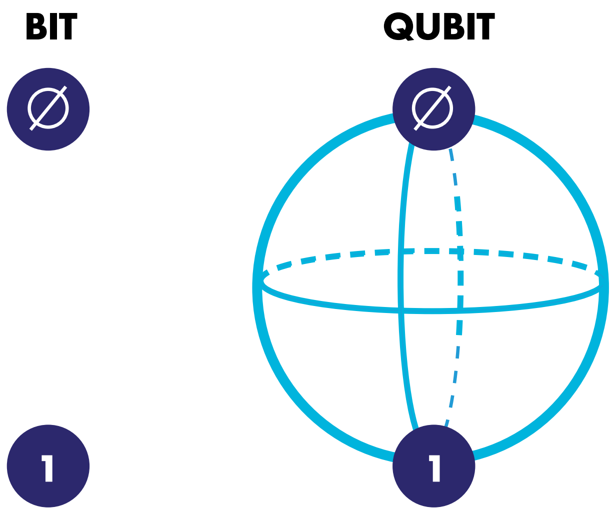
While some believe that the quantum age is a way off yet, others believe it is just around the corner. IBM, for instance, has stated that "in five years, the effects of quantum computing will reach beyond the research lab"[3].

These changes will have a transformative effect on areas including scientific and medical research, economic analysis, AI, Big Data, and many other disciplines which require large volumes of data and complex calculations.

The good, the bad and the ugly

Quantum computers will also have the ability to do harm. The very same computing power that allows complex problems to be solved can, in turn, be applied to undermine cybersecurity.

Of particular concern is the threat to public key cryptography which, if indeed is broken by Shor's algorithm, could leave critical infrastructure, banking systems and more vulnerable to attack.



1 https://azure.microsoft.com/en-gb/services/quantum/

2 https://aws.amazon.com/about-aws/whats-new/2019/12/introducing-amazon-braket/

3 https://www.research.ibm.com/5-in-5/quantum-computing/

The need for quantum-safe cybersecurity

With quantum computing set to render today's cryptographic primitives useless, there is an urgent need for organisations to implement cybersecurity measures that protect critical infrastructure and sensitive data from this new attack vector.

If predictions are correct, and quantum computers exist outside the lab in around five years' time, IT and cybersecurity professionals must act now to secure their systems and data against imminent quantum threats.

Thankfully, technologies that can mitigate the risks of quantum attacks are commercially available today, with further advances due in the near future.

Quantum Random Number Generation (QRNG)

When generating keys, it is crucial that numbers are seeded from a source that is not vulnerable to bias, or easy to predict.

This randomness is already key in today's cryptography, and will become even more so in the quantum era, when quantum computers will be able to ascertain patterns in the fraction of the time it takes their classical counterparts.

It is likely, therefore, that Pseudo Random Number Generators (PRNG) – which use inputs from the environment around them, such as a system clock or keyboard strokes – will simply not be random enough.

Quantum Random Number Generators (QRNGs) provide high entropy and generate a true source of randomness by leveraging principals from quantum physics.

They operate by firing photons (particles of light) at a semi-transparent mirror and assigning them a value of 0 or 1 depending on if they are absorbed or reflected.

Because these photons will behave completely randomly, there is no pattern to be observed as seeds are being generated.

Quantum Key Distribution (QKD)

Once keys are generated, they must be distributed in a way that guarantees forward secrecy, and thus data integrity.

QKD does just this by distributing keys via photons across an optical link. The technology uses another property of quantum physics, known as the 'observer effect', to verify the security and authenticity of these distributed keys.

This principle states that, in quantum physics, observation causes perturbation. In the event that a photon in transit was intercepted, the act of observing the particle would cause it to collapse into its final state.

In practical terms, this means that if a cyber criminal attempted to intercept a key being carried using QKD (via a wire tap for example) the intended recipient would be alerted that it had been observed or tampered with, and thus is not safe to use.

In turn, this will give the sender and recipient the chance to generate a new key before any sensitive data is transmitted using the compromised one.

The need for quantum-safe cybersecurity

Quantum Resistant Algorithms (QRA)

QRAs are algorithms which themselves are designed to remain secure in a post-quantum world.

In 2016, the National Institute of Science and Technology (NIST) acknowledged the importance of such algorithms and called for a public submission of post-quantum algorithms that could carry out this task.

In 2019, NIST revealed that 26 of the 69 submissions[4] "made the cut" and are undergoing further scrutiny. Draft standards are due as soon as 2022.

Once standardised, the current generation of encryption algorithms will need to be replaced with these new quantum-resistant algorithms.

This will ultimately require an update to all software and hardware devices that use Public Key encryption globally.

NIST guidelines recommend adopting a hybrid classic/quantum state in anticipation of the new standards.

Types of QRA

While the 26 algorithms NIST are evaluating come from a range of mathematical ideas and principals, they can broadly be fitted into three categories.

Lattice cryptosystems are built using geometric structures known as lattices and are represented using mathematical arrays known as matrices[5].

Code-based systems use error-correcting codes, which have been used in information security for decades[6], including public key encryption and digital signature schemes.

Multivariate systems depend on the difficulty of solving a system of quadratic polynomial nist-equations over a finite field[7].

A quantum-safe solution

Rather than looking at these elements in isolation, organisations should combine QRNG, QKD and (when available) QRAs to achieve a solution that secures against quantum and classical attacks.

4 https://www.nist.gov/news-events/news/2019/01 /nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

5 Ibid

6 Ibid

7 Ibid

The importance of crypto-agility

Organizations must remain agile in this changing threat landscape, especially when it comes to cryptography.

Combining high-assurance, end-to-end encryption with a true source of entropy and a method of key distribution that aids forward secrecy ensures your encryption solution is fit-for-purpose as the age of the quantum computer looms.

Using today's standards-based algorithms or providing your own and ensuring your encryption platform offers support for as many of these algorithms as possible, also allows for both security and flexibility.

When available, implementing quantum resistant algorithms will further mitigate the risk of a quantum attack.

Thales crypto-agility

Thales Luna Hardware Security Modules, and Thales High Speed Encryptors are crypto agile by design. They enable the most seamless, trustworthy and cost-effective method of transitioning to quantum-safe security while maintaining backward compatibility with existing systems.

This white paper focuses on Thales High Speed Encryptors, and how they provide long-term data protection in a post quantum computing world.

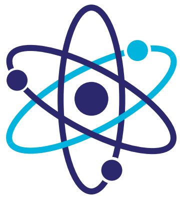
The future is coming

IT and cybersecurity professionals must begin to address the quantum computing threat today.

The scale of assessing threats, comparing vendors and implementing a solution is huge. Those that do not act risk finding themselves in a situation where they are unprepared for the quantum age, or worse-still, under attack with no method of defence.

So, in anticipation of this transformative technology, ask yourself: How much do you value your data?

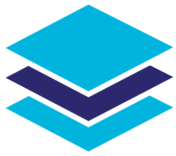
The components of crypto-agility



Quantum-ready

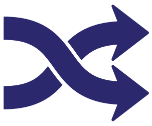
Custom curves
& algorithms

High entropy

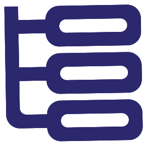


Network Independent
Encryption

Data sovereignty



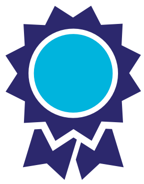
FPGA
programmable



Policy-based

Multiple encryption
modes

Key management



AES 128 & 256 bit

Quantum-ready

Any truly crypto-agile solution needs to be future-proof. Long-term data protection in a post-quantum computing world cannot be guaranteed without the incorporation of QKD and Quantum Safe Algorithms.

Custom curves & algorithms

Thales encryption solutions come with AES 128 and 256 bit standards-based algorithms by default. However, in some circumstances, customers may choose to customize their encryptors with user-defined (or alternative standards-based) algorithms or custom curves for elliptic curve cryptography.

External sources of entropy

It is often argued that a cryptographic system is only as strong as its weakest link. Entropy is a core component of cryptography as key generation is dependent upon randomness.

Random numbers can be generated from a variety of hardware and software sources. For secure operations, Thales encryptors use true hardware Random Number Generators (RNGs). Crypto-agile solutions also enable customers to incorporate external sources of entropy, such as Quantum Random Number Generators (QRNGs).

Data sovereignty

To remain compliant with country and region-specific data protection legislation, organizations may require an encryption solution that allows admins to customize and control where data and keys are stored.

FPGA flexibility

Flexibility is another key component of crypto-agility. Thales encryptors leverage FPGA versatility to both accelerate their time to market and enable simple after-market customization, without the need to update the hardware.

The use of FPGA technology provides, in-field flexibility, ease of management and reduces the TCO, improving the returns on any investment in hardware devices.

Policy-based

Flexible deployment is supported by the ability to set simple policies to manage encryption across the network. Truly agile solutions allow these policies to be set based on a variety of criteria, including VLAN ID or MAC address.

Multiple encryption modes

Crypto-agile solutions offer customers the ability to choose from a range of encryption (cipher) modes. For example, CFB and CTR encryption, or GCM for authenticated encryption.

Key management

Encryption key management sits at the heart of cryptography. Crypto-agile solutions include state-of-the-art, zero-touch key management and support both multiple key algorithms and multiple key systems.

For added security, the encryption keys are not visible to anyone but the customer, not even the vendor has visibility.

AES 128 & 256 bit

Crypto-agility is not just about future proofing, for customers using older applications, or those who prefer to use 128 bit encryption keys, having the flexibility to choose between 128 and 256 bit algorithms provides backwards compatibility and helps drive down the cost of ownership.

Network Independent Encryption

Today's Ethernet and Internet network infrastructure features multiple transport layers. To provide end-to-end network encryption, a crypto-agile solution should be able to deliver concurrent, policy-based multi-Layer encryption (e.g. Layers 2, 3 and 4).

Thales encryption solutions

If your data is worth anything, it's worth encrypting.

Thales is a global leader in the development of end-to-end encryption technologies. Our solutions protect sensitive data for a wide range of commercial, government, industrial and defence customers.

From certified high-assurance hardware and virtualised encryption to secure file-sharing; all Thales solutions share a common high-performance encryption platform and are used to protect sensitive network data around the world.

Thales encryption solutions have been trusted to protect much of the world's most sensitive information for more than 20 years.

They are used to protect everything from government and defense secrets to citizens' identity and intellectual property, financial transactions to real-time CCTV networks and critical national infrastructure control systems.

Hardware encryption

Thales Network Encryptors deliver high-assurance encryption for core network and IT infrastructure.

Certified by leading independent authorities (Common Criteria, FIPS and NATO), Thales CN Series encryptors provide maximum security and data protection for public and private networks.

Operating from ultra-fast 100 Gbps to modest 10 Mbps bandwidths, they feature near-zero latency and overhead.

Purpose built, secure and dedicated network encryption appliances; Thales CN encryptors provide maximum data protection and network security, without compromising network or application performance.

Virtual encryption

The Thales CV1000 Virtual Encryptor (CV1000) delivers strong and flexible encryption security for virtual customer premise equipment (VCPE) and wide area networks.

Scalable to thousands of endpoints, the CV1000 is a software application of the trusted Thales encryption platform. It delivers cost-effective, multi-Layer data protection at up to 5 Gbps (with DPDK) bandwidth for cloud, distributed and software-defined networks.

As a Virtual Network Function, the CV1000 is designed to meet the security and agility demands of virtualized data networks. It enables rapid encryption deployment to the virtual network edge.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

Americas
Arboretum Plaza II, 9442 Capital of Texas Highway North,
Suite 100, Austin, TX 78759 USA
Tel: +1 888 343 5773 or +1 512 257 3900
Fax: +1 954 888 6211 | E-mail: sales@thalesesec.com

Asia Pacific – Thales Transport & Security (HK) Ltd
Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East
Wanchai, Hong Kong | Tel: +852 2815 8633
Fax: +852 2815 8141 | E-mail: apacsales.cpl@thalesgroup.com

Europe, Middle East, Africa
350 Longwater Ave, Green Park,
Reading, Berkshire, UK RG2 6GF
Tel: +44 (0)1844 201800 | Fax: +44 (0)1844 208550
E-mail: emea.sales@thales-esecurity.com

> cpl.thalesgroup.com <