Quantum Computing and Encryption
What impact will quantum computing have on encryption?

Is there a problem looming?

The security of today's current range of cryptographic algorithms and encryption solutions relies on the difficulty conventional computers have with factoring large numbers. While quantum computers are still in their relative infancy, the underpinning technology and development is progressing rapidly. And a consequence of their different approach to processing is that they will be able to factor large numbers incredibly quickly. So, could quantum computing potentially threaten today's encryption techniques?

It has already been theoretically proven that a quantum computer running reliably at scale using algorithms such as Shor's or adiabatic factoring, will be able to crack asymmetric/public keys easily. Back in 2002, a group announced that it had successfully cracked a 64-bit encryption key in a brute force style attack. However, that attack involved over 330,000 volunteers and took 1,700 days or 4 ½ years.

However, it isn't clear how soon a viable quantum computer running at such scale will be a practical reality. Speaking in May 2018, Arvind Krishna of IBM Research warned: *"Quantum computers will be able to instantly break the encryption of sensitive data protected by today's strongest security… This could happen in a little more than five years because of the advances in quantum computer technologies."*

While the threat posed by quantum is clearly on the horizon, the general consensus seems to be that the likelihood of this technology being available within even five years is optimistic.

Several papers have been published on the subject in recent years, each recognising the severity of the threat to standard cryptographic encryption techniques. In a paper published in 2017, the European Telecommunications Standards Institute (ETSI) suggested that a viable quantum computer capable of running Shor's algorithm is likely to be available within 15 years. That is, some time after 2030.

The National Cyber Security Centre (NCSC) published a whitepaper[1] in 2016 which declared: *"…the NCSC recognises the need to end reliance upon asymmetric cryptography that will become vulnerable to quantum computation, and hence the need to transition to "quantum-safe cryptography": cryptographic primitives and protocols that cannot efficiently be broken using either a conventional or a quantum computer."*

Also in 2016, the National Security Agency (NSA) released a paper titled Commercial National Security Algorithm Suite and Quantum Computing FAQ[2] aimed at developers and operators of National Security Systems (NSS). Amongst the advisory guidance in this paper appeared a list of algorithms that: "…should not be used in National Security Systems".

This list of algorithms consisted of:

- ECDH and ECDSA with NIST P-256
- RSA with 2048-bit keys
- Diffie-Hellman with 2048-bit keys
- SHA-256
- AES-128

In its report published in 2017 titled Quantum-Safe Cryptography: Quantum-Safe Threat Assessment[3], ETSI also identified that solutions based upon Elliptic curve, RSA and Diffie-Hellman cryptography will no longer be secure against the threat of a quantum computing attack.

The alternative view

There is of course an alternative view which would seem to suggest that reliable quantum computing availability, capable of running the Shor's algorithm and breaking current day encryption solutions is still decades away. There are even some claiming that the encryption-breaking scare stories are simply a way of trying to attract funding to support generic quantum development.

But the potential applications and benefits derived from quantum computing are huge with promises of significant advances in areas beyond security, including pharmaceutical development, financial modelling and weather forecasting, to name just a few. And these advancements far outweigh the risks posed to encryption security.

So, how large is the risk?

Or maybe more to the point, how real is this risk? Clearly, there appears to be a credible threat that some asymmetric/public key encryption solutions could easily be broken by quantum computers. Data that has been stored or transmitted utilising such solutions will no longer be considered secure, and as such will be vulnerable to public disclosure.

The European Telecommunications Standards Institute (ETSI) has suggested a methodology for calculating this risk:

- **X** = the number of years the public-key cryptography needs to remain unbroken
- **Y** = the number of years it will take to replace the current system with one that is quantum-safe
- **Z** = the number of years it will take to break the current tools, using quantum computers or other means
- **T** = the number of years it will take to develop trust on quantum-safe algorithms

If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken.

[1] https://www.ncsc.gov.uk/whitepaper/quantum-safe-cryptography
[2] https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm
[3] https://www.etsi.org/deliver/etsi_gr/QSC/001_099/004/01.01.01_60/gr_QSC004v010101p.pdf

What's the answer?

Industry and academia have to develop and/or commercialise quantum-proof forms of encryption algorithms, ideally within the next five to ten years, or as a minimum within the next few decades, depending on your point of view. In the USA, the National Institute of Standards & Technology (NIST) is running a competition to identify the best quantum-proof means of encrypting data. The competition has identified three specific 'families' of quantum-proof solutions which it is continuing to evaluate:

- **Lattice** – using geometric structures represented as mathematical arrays
- **Code-based** – using error-correcting codes
- **Multivariate** – a system of quadratic polynomial equations

IBM is championing Lattice cryptography, which in their words *"...mathematically has been proven to be resistant to quantum computing attacks. So far, no known algorithms can break this method of encoding data."*

Cisco meanwhile is working on what it describes as next-generation encryption (NGE) solutions: *"NGE offers the best technologies for future-proof cryptography and it is setting the industry trend. These are the best standards that one can implement today to meet the security and scalability requirements for years to come and to interoperate with the cryptography that will be deployed in that time frame."*

Part of the work involved in developing 'post-quantum' solutions is how to handle the transition period between old and new algorithms. One area of development by Cisco is the creation of 'hybrid certificates'. These certificates would be able to support both traditional and quantum-resistant algorithms, dependent upon which algorithm a verifier supports.

Once these solutions are proven to be secure and capable of operating at the performance levels required, government and industry regulatory bodies have to write and approve new standards for their design and use. Businesses, governments and service providers then have to roll out these new solutions across their estates.

What's being done about it?

The UK Government Office for Science published a paper in 2016 titled The Quantum Age: Technological Opportunities[4] (Blackett Review) which contained a number of recommendations of areas of quantum the UK should pursue further investigation in. Amongst them was a specific recommendation for the National Quantum Technology Programme to fund collaborative work in the areas of post-quantum cryptography and quantum key distribution.

The UK National Quantum Technology Programme has since funded the establishment of a national network of four Quantum Technology Hubs with leading academic institutions, each focussing on differing areas of quantum technology. Two of the four hubs are engaged in activity relevant to the communications/computer security field:

- Networked Quantum Information Technologies (NQIT) is led by the University of Oxford and is the largest of the four hubs. It is working towards networked quantum information technologies *"...that will put today's supercomputers to shame"*.
- Meanwhile, the Quantum Communications Hub is led by the University of York and has a particular focus on developing quantum secure communications technologies, with the aim to advance proven concepts such as quantum key distribution (QKD) systems to a commercialisation-ready stage.

All of these hubs advertise differing levels of industry engagement. Notable amongst them are a number of organisations operating within the Defence & National Security sector including:

- NCSC
- IBM
- BT
- Leonardo
- BAE Systems
- Lockheed Martin
- Raytheon
- Thales
- DSTL
- Airbus Defence & Space
- L3-TR

The table below illustrates the impact NIST believes quantum will have on current cryptographic algorithms:

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key establishment	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key establishment	No longer secure

Table 1 – Impact of Quantum Computing on Common Cryptographic

In January 2019, NIST provided an update on their competition, reporting that 26 new algorithms have been selected to progress through to the next phase. These 26 are considered to be the strongest candidates for potential standardisation by NIST. They will now be subjected to a further 12 months of analysis and evaluation in a wide variety of systems and scenarios.

[4] https://www.gov.uk/government/publications/quantum-technologies-blackett-review

What is Fujitsu doing?

Fujitsu is leading the way in quantum-inspired computing having recently launched our Digital Annealer solution. This revolutionary technology can solve real-world combinatorial optimisation problems by harnessing the processing power of quantum to solve today's hugely complex business problems; problems which are otherwise unsolvable with existing computing methods.

However, the Annealer is not going to solve the encryption problem. We are working with our partners in industry and academia on the development of new security solutions, some of which are exploiting quantum technology to create completely new solutions, whilst others are enhancing existing technology to become quantum-proof. As the maturity of these new solutions develops, we will continue to engage with our customers, trade bodies and industry regulators as they work through the process of managing the impact of this rapidly advancing technology.

Fujitsu Digital Annealer at-a-glance

- The Digital Annealer solution can be miniaturised into a conventional datacentre environment, delivering much improved energy efficiency and much lower energy costs than true quantum computers.
- Unlike other quantum computers, Digital Annealer is able to operate at normal room temperatures and doesn't need advanced cooling solutions.
- Digital Annealer provides 8,192-bit full connectivity, allowing all bits to freely exchange signals, enabling the platform to deal with real-world, large-scale problems.
- Digital Annealer is 17,000 times faster than industry standard compute[5].
- The Digital Annealer solution supports a common tooling platform to that of quantum-annealing systems, making it easy for existing customers to qualify for quantum computing when this technology matures.

What should you be doing?

It is clear that the area of quantum computing is developing and evolving rapidly. So, it's simply imperative to keep abreast of these developments and of the associated technologies to inform future security and encryption-related decision-making. To do this, here are five areas for consideration:

- Consider advising against any future deployments of currently acknowledged vulnerable cryptographic keys.
- Investigate an analysis into the risk of data/communication compromise resulting from quantum computers decrypting historical and current data, and evaluate what the impact might be.
- Consider engaging with partners, academia and regulatory bodies that are currently investigating quantum-proof encryption solutions, with a view to formally participating in research activity.
- Take steps to enable the evaluation of quantum-proof encryption solutions.
- Establish and maintain contact with regulatory authorities in order to ensure you can react in a timely manner to future directives.

And right now...

Fujitsu is acutely aware of the potential security risks posed to asymmetric public key encryption solutions by the development of quantum computers. We are engaging with industry, academia and regulators as they continue to investigate and develop quantum- proof solutions. Like the technology, this is an area that is changing rapidly, and one that we are monitoring closely.

[5] Based on solving a typical combinatory optimisation problem in software using the algorithm implemented in the hardware running on a Zeon family processor.

About the Author

Mark Wixey has 30 years' experience in operating, supporting, and designing high security IT systems and services across the UK Public sector and UK and international commercial businesses. Since joining the Fujitsu Defence & National Security business unit. Mark has assumed responsibility for the department's strategy and portfolio in relation to cyber along with managing strategic technical security relationships with partners and UK government. In June 2019 Mark was awarded the status of Fujitsu Distinguished Engineer.

https://www.fujitsu.com/uk/innovation/fujitsu-distinguished-engineers/

Why Fujitsu?

For over 50 years we have innovated with the MOD, Government Departments and intelligence communities, co-creating new technologies and capabilities. As a result, Fujitsu has around 4,000 security cleared staff and the experience to deliver and manage both generic industry offerings and those tailored to specialist needs at all classifications.

Enabling Your Information Advantage

In today's complex, digital operational environment, never before has information been such a key asset in securing operational advantage. Fujitsu's vision is to provide customers with the means to translate complex data into useful information upon which to base critical decisions and actions. Transforming this ever-increasing pool of data into meaningful, useful information through analytics, automation and genuine Artificial Intelligence is critical to achieving this goal. Fujitsu is fully committed to working closely with our customers, and through the use of co-creation will seek to enhance capability both through the acceleration of existing processes, and also through the delivery of truly new capabilities and ways of working. Our approach is based upon maximising both existing investment and best-in-class innovation, delivering the full spectrum of capabilities needed to enable your information advantage.

FUJITSU
22 Baker Street, London W1U 3BW, United Kingdom
Tel: +44 (0) 1235 79 7711
Email: askfujitsu@uk.fujitsu.com
Ref: 3954
uk.fujitsu.com