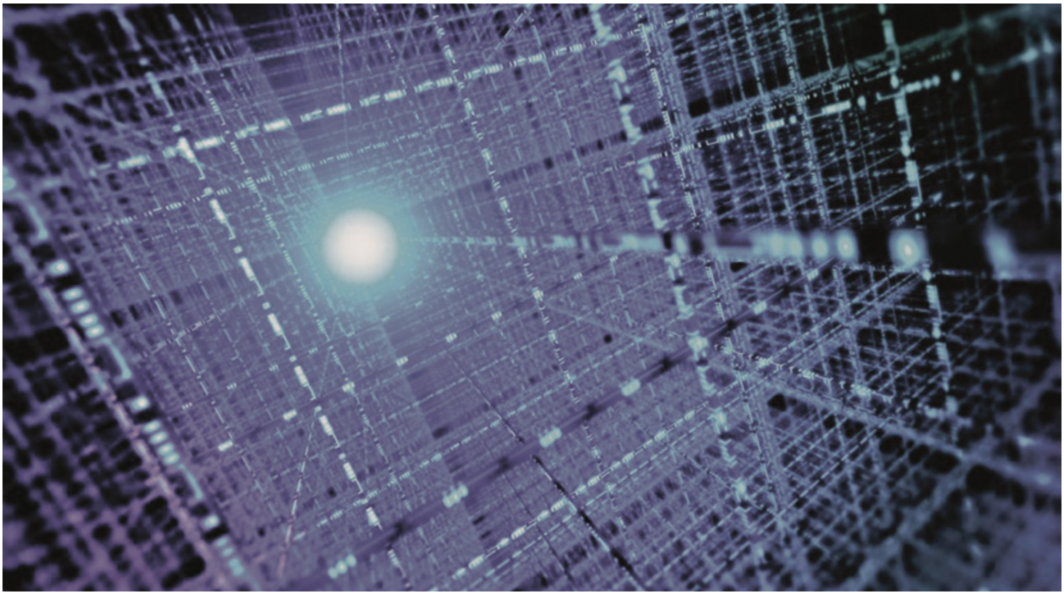


QUANTUM COMPUTERS: CYBER SECURITY THREATS FOR CRITICAL INFRASTRUCTURE

By Roderick Hodgson, Director Secure Chorus

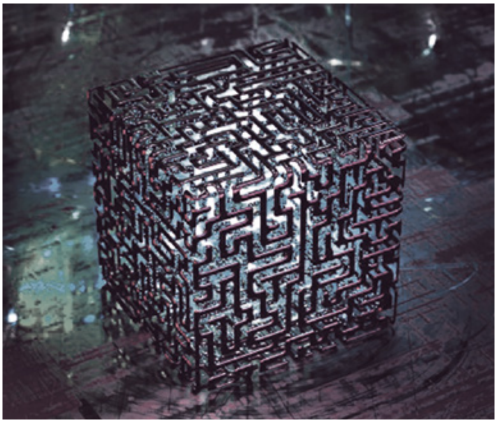
Secure Chorus Director Roderick Hodgson discusses the risk posed by quantum computers to critical infrastructure data security and explains the increasing need for current encryption methods to be upgraded with ‘quantum-safe’ equivalents.

Quantum computing has the potential to massively disrupt critical infrastructure, in terms of its much-improved capabilities in timing, imaging, communications, sensing and measurement, computing and simulation. It is expected to bring innovation in many major sectors including healthcare, defence, aerospace, transport, civil engineering, telecommunications, finance and information technology. But, at the same time, quantum computers create a problem in the field of data security due to their ability to solve complex mathematical problems better and faster than the computers we use today, including those used at the core of public key cryptography methods currently used by governments, public and private sectors to protect sensitive data.

Quantum computers are based on the principles of quantum physics, which is a mathematical description of how elementary particles move and interact in nature. In classical physics, particles have a precise position and move along well-defined paths. The more recent quantum physics is based on the wave-particle dual description that evolved through the work of such as eminent scientists as Bohr, Einstein, Heisenberg, Schrödinger and others. In quantum, the basic units of the natural world are still particles, but the description of their motion differs in that it brings in wave mechanics, which defines the probability of finding specific particles in specific places.

The first difference between currently deployed (so-called ‘classic’) computers and quantum computers is the advantage of ‘superposition’, which means a particle can be in two or more states at once, only settling into one of the possible states once it is measured. While classic computers operate on ‘Bits’ (zero or one), quantum computers make use of a quantum-mechanical phenomenon that represents data as ‘Qubits’ (zero, one, or a little bit of both). The superposition effect means that, instead of being constrained to one of two possible values (i.e. 1 or 0), Qubits can exist as a mixture of both.

The second difference is ‘entanglement’, a quantum phenomenon where pairs or groups of particles have an extremely strong correlation so that what happens to one will affect the others, even if the particles are physically separated by great distances. For example, while it may be known that two entangled particles are spinning in opposite directions, it may not yet be known which particle is spinning in which direction. However, if the measurement of one particle shows that it is spinning clockwise, there is no need to measure the other to know that that it is spinning anti-clockwise. This is true even if the particles are far apart in time or space. When applied to quantum computers, this means all Qubits can have their value changed at the same time, and so do not need to perform a set of sequential operations. They can do them simultaneously.



Due to ‘superposition’ and ‘entanglement’, there are two main tasks that quantum computers are expected to perform more efficiently than conventional computers. They will be able to factorise large numbers as well as being able to search through large volumes of unstructured data. The security of public key cryptography fundamentally relies on the difficulty of factorising large numbers or on the difficulty of calculating discrete logarithms: both are problems that classic computers cannot readily solve. Quantum computers have the capacity to solve such complex mathematical problems better and faster, which means they can break the cryptographic keys quickly by calculating or searching exhaustively all possible secret keys for a given public key.

Public key cryptography refers to any system that employs pairs of keys: one is used to encrypt data (the public key), and the other is used to decrypt data (the private key). Because the public key can be shared without restriction, the paired key approach is the solution to an important problem in establishing secure communications. It allows two parties to protect the data they exchange without requiring both parties to have a pre-agreed shared secret. This type of cryptography plays an important role in many information security systems used in critical infrastructure today, as it ensures confidentiality, integrity, authenticity and non-repudiation in data transmission and data storage.

While it is expected that quantum computers won’t become mainstream until at least 2025, critical infrastructure organisations that process sensitive data need to start planning for a post-quantum computing world. When considering the replacement of current cryptography with quantum-resistant solutions, three main considerations should be taken into account.

First is the amount of time it may take to build a given information security system for a new critical infrastructure project. Such a project may have long development cycles with the result that, by the time it is completed, the information security landscape may have changed substantially in terms of threat profile. This means it is important to consider quantum-resistant approaches to security as part of the design of a new critical infrastructure project or, at the very least, consider the time involved to undertake an upgrade to make the security implemented at the outset quantum-resistant. For example, if a new nuclear power station is expected to take a decade to build, quantum-safe information security systems should be considered as part of the design phase of the project. If not, consideration should be given to how and when an upgrade to quantum safe solutions will need to be started.

Second, there is the issue of the lifespan of an existing information security system, device or piece of equipment that will be used in a critical infrastructure environment. For example, connected vehicles may be expected to operate on the roads for more than a decade. High-speed smart rail even longer. A manufacturer designing vehicles to be built in the next few years will need to consider quantum computing risks as part of their design process today: namely making decisions that account for the emergence of quantum computers during the lifespan of the vehicle.

Third, there is the question of the length of time a given information security system may need to secure sensitive data in a critical infrastructure environment. For example, financial institutions may need to secure historical financial transaction for decades to come. The question then becomes one of determining what approach must be taken to ensure the data generated today can be protected well into the future when the threat from quantum computers materialises.

> ... THE QUESTION THEN BECOMES ONE OF DETERMINING WHAT APPROACH MUST BE TAKEN TO ENSURE THE DATA GENERATED TODAY CAN BE PROTECTED WELL INTO THE FUTURE WHEN THE THREAT FROM QUANTUM COMPUTERS MATERIALISES …

These considerations are time critical, as once the process to select quantum-safe algorithms has started, it can take in the region of five to seven years to undertake the following activities: update protocols to utilise these algorithms, complete the software development and perform all of the necessary quality assurance testing including forward and backward compatibility. It is also important to note that the deployment phase of such quantum safe algorithms – including testing in critical infrastructure networks, the long deprecation and swap out cycle – can take a similar amount of time.

One method of developing quantum-safe cryptography is the deployment of a new set of public key cryptosystems for classic computers capable of resisting quantum computer attack. These cryptosystems are called 'quantum-safe' or 'post-quantum cryptography'. The principle behind them is the use of mathematical problems of complexity beyond quantum computing's ability to solve them. The information security industry currently recognises five types of cryptosystems as promising replacement candidates for current cryptography. These are: hash-based, code-based, lattice-based, multivariate-based and supersingular isogeny-based. International standards bodies, including the National Institute of Standards and Technology (NIST) in the USA, are currently in the process of conducting more analysis and research before they can go forward on determining which of these to adopt.

The candidate submission period for NIST Post-Quantum Cryptography algorithms ended in November 2017, with 69 candidates proposed. The selection process is currently in the first round of evaluation. At the same time, several other standards bodies are also conducting work to address this challenge, including the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF) and the International Telecommunication Union (ITU).

In 2017, the European Telecommunications Standards Institute (ETSI) Industry Specification Group of Quantum-Safe Cryptography (ISG QCS) was promoted to become the Working Group for Quantum-Safe Cryptography (WG QSC) of ETSI Technical Committee Cyber. This change provides the working group with a broader scope of normative specification activities. The primary focus of ISG QSC is the implementation, architecture and any other practical aspects of building and deploying quantum-safe cryptographic services.

The Internet Engineering Task Force (IETF) has been active in quantum-safe cryptography standardisation, as several proposed replacement algorithms are in the final draft stage in the Crypto Forum Research Group (CFRC). The IETF has also produced a draft standard for so-called 'hybrid key establishment', which sees the protocol for securing communications over the internet, Transport Layer Security (TLS), combining public keys from classic and quantum-safe algorithms. A similar approach to quantum safety has been discussed for Internet Key Exchange (IKE) protocol as well.

The International Telecommunication Union (ITU) has begun work on deployment specifications for quantum-safe cryptography. The ITU Telecom (ITU-T) sector Study Group 17 (SG17) introduced an optional extension to the next version of the ITU-T Rec. X.509 digital certificate standard. This extension allows Public Key Infrastructure (PKI) to seamlessly migrate current traditional cryptographic algorithms to new quantum-safe equivalents, while maintaining the ability to use legacy certificates as upgrades occur over time.

Secure Chorus is a not-for-profit membership organisation providing thought leadership, common interoperability standards and tangible capabilities for the information security industry. We are following the development of quantum-safe cryptography closely and engaging with governments, industry and academic institutions globally to evaluate outcomes as they become available so that we can identify a long-term strategy for adopting quantum-safe cryptography into the Secure Chorus cryptography standard of choice – MIKEY-SAKKE.

MIKEY-SAKKE is a method of key exchange that uses Identity-based Public Key Cryptography (IDPKC) to establish a shared secret value and certificateless signatures to provide source authentication. It has been developed by the UK government's National Technical Authority for Information Assurance (CESG), which advises on how to protect information and information systems against today's threats. CESG is now part of the National Cyber Security Centre (NCSC) which is a government member of Secure Chorus. MIKEY-SAKKE was standardised by the Internet Engineering Task Force (IEFT). It has also recently been approved by the 3rd Generation Partnership Project (3GPP), the body responsible for standardising mobile communications for use in mission-critical applications, hence receiving endorsement at a global level for its innovative approach to public key cryptography.

MIKEY-SAKKE has a number of desirable features for the IT systems of critical infrastructure organisations, including end-to-end encryption and can be used in a variety of environments, both at rest (e.g. storage) and in transmission (e.g. network systems), centralised management, giving organisations full control of IT system's security, as well as the ability to comply with any data auditing requirements, through a managed and logged process. Additional benefits include scale and flexibility.

Secure Chorus' members develop interoperability standards for MIKEY-SAKKE-based information security products. The traditional approach that focused on protecting the security perimeter of a critical infrastructure organisation doesn't fully address the issues arising from the interconnection and hyper-digitalisation, which pushes the security perimeter beyond organisational network boundaries through a global network of interconnected technologies.

Interoperability it therefore also a very important feature for the IT systems of critical infrastructure.

Secure Chorus recently collaborated with one of its partner member, ISARA Corporation, to produce a white paper about post-quantum cryptography. ISARA Corporation, a leader in post-quantum cryptography, is committed to the collaborative development of quantum-safe standards at the European Telecommunications Standards Institute (ETSI). ISARA is also working with Secure Chorus, to evolve MIKEY-SAKKE to become quantum-safe.

Entitled 'The Quantum Revolution: Security Implications and Considerations', the paper provides a framework for assessing if and when organisations need to start working on protecting themselves against the threat posed by quantum computers. It also addresses the key considerations an organisation needs to take into account when migrating to a new cryptography standard. The paper introduces the MIKEY-SAKKE identity-based public key open cryptography standard and explains that this cryptography standard, if made quantum safe, would offer a unique combination of benefits to the critical infrastructure sector.

While it is likely to be a decade before quantum computing has any significant effect on critical infrastructure, its potential impact on its information security means that critical infrastructure organisations must begin to prepare for its arrival now. In security terms, this should be done through quantum risk assessments as well as investment in well-recognised and endorsed quantum-safe public key cryptography. ■

END-NOTE

This article is based on a new white paper entitled 'The Quantum Revolution: Security Implications and Considerations' co-authored by Secure Chorus and the ISARA Corporation. To download your free copy go to the Secure Chorus website www.securechorus.org

ABOUT THE AUTHOR

Roderick Hodgson is a technologist and innovation strategist with oversight of all technology aspects of Secure Chorus, including technical management, setting technical strategy and representing the technology externally. Throughout his career, he has defined, developed and delivered disruptive products in video streaming, telecoms, cyber-security, IoT and Big Data for different companies.

ABOUT SECURE CHORUS

Secure Chorus is a not-for-profit membership organisation serving as a platform for multi-stakeholder cooperation, for the development of forward-looking strategies, common technology standards and tangible capabilities in the field of information security. For more information visit www.securechorus.org and follow the company on LinkedIn and Twitter.

For further information, please contact:
Secure Chorus Ltd via PRPR
Elisabetta Zaccaria, Chairman
Roderick Hodgson, Director

PRPR
Peter Rennison
Email: pr@prpr.co.uk
Phone number: +44 (0) 7831 208109