WHITE PAPER

THE QUANTUM REVOLUTION

Security Implications and Considerations

THIS WHITE PAPER HAS BEEN CO-AUTHORED BY SECURE CHORUS & ISARA CORPORATION

August 2018
# Table Contents

1. List of Acronyms 3
2. About Secure Chorus 4
3. About ISARA Corporation 5
4. Executive Summary 7
5. Quantum computing: Benefits & Threats 9
   - The Power of a Quantum Computer 9
   - Threats Posed by Quantum Computing 9
6. Defensive technology against quantum attacks 11
   - Quantum-Safe Cryptography 11
   - Identity-Based Public Key Cryptography 11
   - Standardisation of Quantum-Safe Cryptography 12
   - Introducing MIKEY-SAKKE 13
   - Secure Chorus Interoperability Standards 14
7. Building the defence 17
   - What are the Risks? 17
   - When to Start? 18
   - Establishing Quantum-Safe Confidentiality 19
   - Establishing Quantum-Safe Authentication 20
   - Quantum-Safe Communications 20
8. Conclusion 22
9. References 23

This document is provided for information purposes only and should not be relied upon as giving advice or as a basis for making any decisions. We do not warrant that this document is error free and shall not be liable for any use of, or reliance upon, this document. No contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>3rd Generation Partnership Project</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>CESG</td>
<td>Communications-Electronics Security Group (predecessor to NCSC)</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DH</td>
<td>Diffie-Hellman</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital Signature Algorithm</td>
</tr>
<tr>
<td>ECDH</td>
<td>Elliptic Curve Diffie-Hellman</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>ETSI</td>
<td>European Telecommunication Standardisation Institute</td>
</tr>
<tr>
<td>GDPR</td>
<td>The General Data Protection Regulation</td>
</tr>
<tr>
<td>IBS</td>
<td>Identity-based Signature</td>
</tr>
<tr>
<td>IDE</td>
<td>Identity-based Encryption</td>
</tr>
<tr>
<td>IDPKC</td>
<td>Identity-Based Public Key Cryptography</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IPsec/IKE</td>
<td>Internet Protocol security/Internet Key Exchange</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>KMS</td>
<td>Key Management Server</td>
</tr>
<tr>
<td>LMS</td>
<td>Leighton Micali Signature</td>
</tr>
<tr>
<td>MIKEY</td>
<td>Multimedia Internet KEYing</td>
</tr>
<tr>
<td>NCSC</td>
<td>National Cyber Security Centre</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-the-Air</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>QSC</td>
<td>Quantum-safe cryptography</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest-Shamir-Adelman</td>
</tr>
<tr>
<td>SAKKE</td>
<td>Sakai-Kasahara Key Encryption</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SIKE</td>
<td>Singular Isogeny Key Encapsulation</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>XMSS</td>
<td>Extended Merkle Signature Scheme</td>
</tr>
</tbody>
</table>
Secure Chorus is a not-for-profit, membership organisation launched in 2016, serving as a global platform for public-private sector engagement, to support the development of forward looking strategies, common standards and tangible capabilities all aimed at building cyber resilience in the field of multimedia communication for government and enterprise.

We partner with governments, supranational organisations, corporates, technology innovators, academic institutions and regulators to rapidly scale our ecosystem of interoperable and secure information sharing technologies, driving wide-spread access and adoption across the global digital economy.

The requirement for secure multimedia communications exists across a variety of sectors including central government, public safety, banking, health, power and other critical national infrastructure. While each sector brings its own service requirements, every sector increasingly requires a secure mechanism for cross-sector collaboration.

Secure Chorus was originally formed in 2012 as an industry-led working group. It was focused on building secure multimedia services to address the UK Government’s requirement for protecting OFFICIAL and OFFICIAL SENSITIVE communications. The vision behind the initiative was that multimedia communication in UK Government should be appropriately protected, and that this protection should enhance, rather than hinder, collaboration.

At the time there were few usable, scalable, regulatory-compliant and, above all, affordable options that could make the global deployment of interoperable secure multimedia communication a reality for enterprise end users.

Creating a secure, highly-scalable interconnected network, where any user can securely communicate with another user required the development of appropriate common standards. In 2010, CESG (now the National Cyber Security Centre), in the UK, developed a standard that could meet the need. Using a cryptographic solution developed by two Japanese cryptographers, Sakai and Kasahara, CESG standardised MIKEY-SAKKE protocol in IETF RFCs 6507, 6508 and 6509.

The “early adopters” of MIKEY-SAKKE had all built technology securely connecting their users, in specific sectors. These “early adopters” joined forces and founded Secure Chorus with the vision of developing common interoperability standards to connect their user communities, allowing seamless secure cross-government and inter-industry communication.
About ISARA Corporation

ISARA Corporation is a cybersecurity company specializing in creating production-ready quantum-safe solutions for today’s computing ecosystems. We enable OEMs to achieve a seamless migration to next-generation security measures by embedding our optimized quantum-safe algorithms and unique crypto-agile technology.

One of the great accomplishments of the modern computing era is the ubiquity – and relative invisibility – of data security achieved using public key cryptography. Experts estimate that within the next eight to fifteen years, currently used public key cryptography will be broken by a large-scale quantum computer, forcing a complete migration to quantum-safe cryptography. The technology industry has never had to make this type of cryptographic change on such a large scale; governments and large organizations are not yet prepared and if action isn’t immediately taken they run the risk of exposing confidential data and compromising the integrity of critical, high-value assets. We believe that this migration should be cost effective, seamless and efficient.

The ISARA Radiate™ Security Solution Suite is the only complete solution on the market to offer a production-ready implementation of quantum-safe algorithms and integration tools built for developers. By embedding the ISARA Radiate cryptographic library, OEMs can create quantum-safe commercial products and systems today while maintaining performance and interoperability. Our unique crypto-agile technologies enable OEMs to seamlessly integrate our quantum-safe algorithms into their existing systems while maintaining backward compatibility.

ISARA Corp. was founded in 2015 and is headquartered in Waterloo, Ontario, Canada, with an office in Silicon Valley, California. Our team has grown to over 35 full-time employees, many with years of experience in technology companies, including BlackBerry, Certicom, Oracle, and McAfee, and academic and research institutions, including the Institute for Quantum Computing (IQC) and the Perimeter Institute. We actively collaborate with academic and standards institutions to conduct joint research and raise awareness of the quantum threat. We are a proud part of ‘Quantum Valley’ in Waterloo Region, a rich collaborative environment between academic and industry focused on accelerating the development of quantum computing and related technologies.
Executive Summary
Executive Summary

Powerful quantum computers have the potential to bring positive disruption and tremendous benefits to our society. However, they also pose a potential threat to the current security technology used to protect online transactions and digital information.

Modern-day encryption schemes, such as those used in public-key cryptography, are based on mathematical problems (e.g. the challenge of factoring large numbers) that are very difficult to solve using current/near-future computational power. However, these difficult problems will be easily solved by quantum computers. This fundamentally breaks the cryptographic foundations upon which the majority of our cyber security systems are based and threatens the security of our information in a number of ways.

Firstly, transmitted information will become vulnerable to eavesdropping and stored encrypted data will be able to be decrypted. Secondly, it will also no longer be possible to assure authenticity and integrity of information. Given the requirement for some kinds of information (e.g. health records) to remain secure for at least a lifetime, the need to develop solutions which are quantum-safe exists today, and not 10-20 years in the future, when the arrival of quantum computers is expected.

Secure Chorus, in collaboration with ISARA Corporation, instigated the writing of this paper to address the lack of simple, easy to understand and access information regarding the threats that quantum computing poses to secure data processing. The whitepaper also introduces technologies for enterprise and government to build defences against potential quantum attacks, provides analysis on the risks, and discusses strategies for migration and deployment.

As quantum computing capability becomes more accessible to potential attackers, the cryptography standards chosen by Secure Chorus will need to be updated to respond to the growing quantum computing threat. ISARA Corporation has joined Secure Chorus as a Partner Member to contribute their expertise to ensure Secure Chorus stays ahead of the curve in terms of its cryptography standard of choice. Secure Chorus intents to soon embrace a Post-Quantum Identity Based Crypto Scheme.

Secure Chorus and ISARA Corporation are also working together to educate Secure Chorus' members about post-quantum cryptography. This is to ensure Secure Chorus Compliant Products can provide the next generation of data protection capabilities.
Quantum Computing: Benefits & Threats
Quantum Computing: Benefits & Threats

The power of a quantum computer

In 2017, there were several significant and remarkable advancements in the development of quantum computers. Technology giants such as IBM, Microsoft, and Google are heavily involved in the implementation of quantum computing and its applications (see e.g. [1] [2] [3]). Demand for large-scale quantum computers is increasing due to the tremendous benefits they promise in many areas such as faster data analysis and unstructured data search. This is especially true for certain classes of problems, where traditional computers are now reaching their limits.

Quantum computers will provide us with tools to unravel problems that cannot be solved with traditional computers. For example, quantum computers are expected to drastically improve the drug design process to identify better chemical structures and to assist investigation in material science to find, for example, superior superconducting materials [4]. Also, their capability is expected to enhance big data mining, and thus can potentially provide considerable progress in machine learning and artificial intelligence technology [5].

Threats posed by quantum computing

Unfortunately, the powerful capabilities of quantum computers also introduce risks to our current security technology, namely public key cryptography.

It is worth highlighting that symmetric key cryptography such as Advanced Encryption Standard (AES) or Secure Hash Algorithm (SHA) -2 and -3 will not be completely compromised. The only known attack against these types of algorithms uses Grover’s algorithm, which achieves fast unstructured search for the key space for symmetric ciphers or the output space for cryptographic hash algorithms [6]. However, enhanced search by Grover’s algorithm has an upper limit. Furthermore, the attack requires a considerable amount of quantum resources. Therefore, these symmetric key algorithms can sustain their security in the face of quantum computing attacks by simply increasing the key sizes or output sizes to at most twice their current size [7].

However, it’s become apparent that, unlike symmetric key cryptography, traditional public key cryptosystems such as:

- the integer factorization-based cryptosystem, Rivest-Shamir-Adelman (RSA);
- the integer discrete log-based cryptosystems, Diffie-Hellman (DH) and Digital Signature Algorithm (DSA) and the
- elliptic curve discrete log-based cryptosystems, Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA)

are extremely vulnerable to Shor’s algorithm, which is designed to solve these hard-mathematical problems with extreme efficiency [8]. Since these algorithms, and the systems built upon them, such as Identity Based Cryptography, are used as the foundation of today’s network security, a quantum computer in the hands of an adversary would cause a total collapse of the security measures used for data processing today. It is necessary to replace these public key cryptosystems with quantum-safe equivalents as recommended by NIST [9].
Defensive technology against quantum attacks
Defensive technology against quantum attacks

Quantum-safe cryptography

One method to secure critical infrastructure and sensitive assets is the deployment of a new set of public key cryptosystems for traditional computers that resist attacks by quantum computers. The use of these new cryptosystems is referred to as “quantum-safe cryptography”, a.k.a. “post-quantum cryptography” [10].

Quantum-safe cryptography utilizes hard mathematical problems that are believed to be too difficult for quantum computers to solve. Currently, the industry recognizes the following five types of cryptosystems as promising replacement candidates for vulnerable cryptography [10] [11]:

- Hash-based cryptosystems
- Code-based cryptosystems
- Lattice-based cryptosystems
- Multivariate-based cryptosystems
- Supersingular isogeny-based cryptosystems

There have been several proposals of algorithms for these quantum-safe cryptosystems. However, it has been agreed that more research and analysis will be required by the National Institute of Standards and Technology (NIST) and other global standards bodies to determine which ones to deploy. Currently, there are a few accepted quantum-safe algorithms, including two hash-based digital signature algorithms: Leighton Micali Signature (LMS) and eXtended Merkle Signature Scheme (XMSS), which are soon expected to become standards. The standardisation of quantum-safe cryptography is an on-going process as described later in this paper.

Note that these algorithms vastly differ from traditional algorithms in key sizes, speed, and handshake steps. Therefore, the secure protocols such as Transport Layer Security (TLS) and Internet Protocol security/Internet Key Exchange (IPsec/IKE) must be adjusted to deploy quantum-safe algorithms. Again, standardisation activities are in progress.

Identity-based public key cryptography

Identity-Based Public Key Cryptography (IDPKC) is an advanced cryptography scheme whose quantum safety is just beginning to be explored. IDPKC is typically divided into two major areas: Identity-Based Encryption (IBE) for encryption, and Identity-Based Signature (IBS) for digital signature.

One of the main objectives of IDPKC is to avoid the use of digital certificates to build trust in public keys. When public key cryptography is used, it is critical to establish trust in the received public key. Unauthenticated public keys can easily compromise the system’s security. Traditionally, digital certificates with Public Key Infrastructure (PKI) have been used to build such trust. In PKI systems, a sender must obtain the recipient’s public key, which is contained in a digital certificate, from a trusted server or from the recipient via a secure communication.
channel. IDPKC’s advantage is that a digital certificate and its associated trust building process are no longer needed to obtain a trusted public key. It simply uses the known identity of the recipient to derive the public key.

An IDPKC approach can provide an effective solution to the challenges enterprises experience when endeavouring to communicate securely outside their perimeters. IDPKC can protect data by providing end-to-end encryption where encryption keys are directly associated with a user’s identity (e.g. an email address or phone number), while also providing authentication of those identities.

The most notable use case of IDPKC is Sakai-Kasahara Key Encryption in Multimedia Internet KEYing (MIKEY-SAKKE) [12] for Secure Chorus (discussed later in this paper). It uses a combination of Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption (ECCSI) [13] for digital signatures and Sakai-Kasahara Key Encryption (SAKKE) [14] for encryption.

Since these schemes are based on the ECDLP, alternatives are needed to achieve Quantum Safe Identity Based Cryptography. Lattice-based IBC is the only quantum-safe alternative that has been studied to date. The foundation of lattice-based IBE was established by Gentry, Peikert, and Vaikuntanathan in 2008.

Compared with elliptic curve paring-based IBE, lattice-based IBE has considerably larger public key sizes and is slower than schemes such as MIKEY-SAKKE. Further analysis is needed here on performance, while further security analysis may be needed to justify the assumptions and refine the parameters.

**Standardisation of quantum-safe cryptography**

In August 2015, the National Security Agency (NSA) announced a goal to move its Suite B cryptography to quantum-safe alternatives, referred to as quantum-safe cryptography (see e.g. [15]). This was followed by NIST publishing its Post-Quantum Cryptography algorithm selection process [9] in 2016. 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 [16].

In 2017, the European Telecommunication Standards Institute (ETSI) Industry Specification Group of Quantum-Safe Cryptography (ISG QCS) group was promoted to become the Working Group for Quantum-Safe Cryptography (WG QSC) of ETSI Technical Committee Cyber. This change provides the working group 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 [17].

The Internet Engineering Task Force (IETF) has also been active in quantum-safe cryptography standardization. Two proposals for hash-based signatures, LMS and XMSS, are in the final draft stage in the Crypto Forum Research Group (CFRC) [18] [19]. Also, there is a draft standard for hybrid key establishment, where shared secrets from classical and quantum-safe algorithms are combined in the TLS framework [20]. A similar approach to quantum safety has been discussed for Internet Key Exchange (IKE) 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 [17]. This extension lets Public Key Infrastructure (PKI) 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 following these developments closely and engaging with government, industry and academic organisations to assist these efforts and evaluate outcomes as they become available. Throughout 2018 we will continue to analyse the post-quantum challenges
in secure data processing and will work with our members and field experts alike to identify a long-term strategy for updating MIKEY-SAKKE to integrate cryptography that is quantum-safe.

**Introducing MIKEY-SAKKE**

MIKEY-SAKKE, Secure Chorus’ cryptography standard of choice, is an open cryptography standard that has broad appeal for inter-organisational secure communications. It has been standardised in the Internet Engineering Task Force (IETF) and has recently been approved by 3rd Generation Partnership Project (3GPP), the body responsible for standardising mobile communication, for use in mission-critical applications such as emergency services communications.

In 2012, the UK Government’s National Technical Authority for Information and Assurance (CESG) - now the National Cyber Security Centre (NCSC) - defined MIKEY-SAKKE as an open cryptography standard to answer the UK Government’s secure communication requirements at OFFICIAL and to have a cryptographic method for validating an identity for government communications.

As noted previously, this standard was based upon an existing standard for elliptic curve signatures, the Elliptic Curve Digital Signature Algorithm (ECDSA) and an identity-based cryptographic protocol developed by two Japanese researchers, SAKAI and KASAHARA. Combining these protocols for secure communications gave rise to MIKEY-SAKKE, defined by the IETF as RFC 6507 and RFC 6509.

MIKEY-SAKKE has been selected by Secure Chorus because it has a number of benefits that appeal to both government and enterprise users. It is highly scalable, requiring no prior setup between users or distribution of user certificates. It is highly flexible, supporting both real-time communications (such as voice), conference calls, and deferred delivery (such as messaging and voicemail). It is designed to be centrally managed, giving a domain manager full control of the security of the system. At the same time, it maintains high availability, as calling does not require interaction with centralised architecture.

As explained previously, Identity-based Public Key Cryptography (IDPKC) is a public-key cryptography method that allows for data to be encrypted for a user, based upon the knowledge of the identity of that user within a system. Users are identified by name, role, phone number or any other identifier.

End-to-end encryption of multimedia data can be done with wide-spread data encryption technologies, such as the Advanced Encryption Scheme (AES). In such an approach, all participating parties need to have access to the same AES keys, used for encrypting the data traffic between the parties (“traffic keys”).

The innovation in MIKEY-SAKKE is the idea that the initiator of communication may send a message, called a MIKEY message, to the recipient containing these traffic keys. The MIKEY message itself is encrypted using the recipient’s identity. Only a legitimate intended recipient can decrypt this message, recovering the traffic keys. As the message is also signed using an electronic signature, the recipient can also verify who sent it, all through a single message.

This idea extends to group calls by sending a separate message to each member of the group, encrypted to their identity. As before, only the intended recipients can recover the traffic key and verify that it was sent by the initiator – the group management server.

**Key Management Servers**

The architecture of MIKEY-SAKKE defines that each system in a network exchanging data is attached to a Key Management Server (KMS). The server distributes key information to the systems it manages on a regular (monthly or yearly) basis.
Any participant in a communication session can validate the origin of the messages it receives by validating the signature against the public key material of the KMS controlling that system.

This means communication between users controlled by different KMSs can be enabled. In this way, secure communication is enabled beyond the boundaries of a given agency or organisation.

The existence of the KMS means that an agency has access to its own encrypted data, without giving access to unauthorised third parties. This key management system can even be kept off-line if required, while allowing lawful interception of emergency communications, as required by all jurisdictions.

All MIKEY-SAKKE standards are publicly available, allowing the validity of the algorithms to be independently verified. These modern standards permit flexible and dynamic security associations to be made without the costs associated with public key infrastructure and online certificate authorities, such as those using X.509 certificates used in HTTPS communication.

With MIKEY-SAKKE, users’ identifiers (such as their phone number, name or role) are used as their public keys. MIKEY-SAKKE effectively addresses the security requirements of public safety multimedia communication by providing data confidentiality and authentication of participants, all while enabling efficient key management and responding to the requirements of inter-organisational communication and lawful interception.

Secure Chorus interoperability standards

Secure Chorus is producing, in collaboration with its vendor members, a full set of interoperability standards, using MIKEY-SAKKE as the underlying cryptographic protocol, to ensure that any vendor member’s Secure Chorus Compliant Product is able to share data with any other vendor member’s Secure Chorus Compliant Product in the ecosystem.

In addition to MIKEY-SAKKE, the interoperability standards are underpinned by widely accepted communication standards, developed by international standards bodies including the IETF and 3GPP.

Interoperability standards are absolutely necessary to enable widespread access to, and drive adoption of, secure data processing across the global digital economy. The vision is that every sensitive call, email or file transfer in government and industry should be appropriately protected, and furthermore that this protection should enhance, not hinder, collaboration.

The requirement for secure multimedia communications exists across a variety of sectors including central government, public safety, banking, health, power and other critical national infrastructure. In the UK, the cross-sector secure voice market is estimated at 2 million high-value subscribers, more than 3 percent of the subscriber base. While each sector brings its own service requirements, every sector increasingly requires secure cross-sector collaboration.

Historically, there have been some small-scale, isolated security solutions within each of these sectors. However, there are few usable, scalable, regulatory-compliant and, above all, affordable options that make enterprise deployment of multimedia security a reality for the end user. Without the scale of cross-sector interoperability, these security solutions will remain niche, or limited to a small number of endpoints. The wider need will remain unfulfilled.

The success of all communication solutions is intrinsically tied to scale: the more people that you are able to communicate with, the more valuable the offering, and the greater the demand for the communication solution. It is undeniable that a wide-scale demand exists. Secure Chorus Compliant Products aim to fill the gap of cross-sector interoperability. The products can provide a consistent, cross-platform security solution that supports secure messaging, voice, and video, alongside sector specific services and create a secure, highly-scalable interconnected network, where any user can securely communicate with another.
CESG developed, and NCSC owns, the intellectual property in the MIKEY-SAKKE protocol. MIKEY-SAKKE was produced as an unencumbered, free-to-use protocol, which has enabled a market of secure multimedia products to develop. As we contemplate a post-quantum world, it is necessary to identify a quantum-safe evolution of MIKEY-SAKKE; one that maintains the same security and operational characteristics and is equally proven, open and free-to-use.

Developing a quantum-safe evolution of MIKEY-SAKKE is, as described above, the work of a number of global standards bodies. Secure Chorus will monitor these activities and ensure it follows the evolution of MIKEY-SAKKE in the relevant forums through the work of our members. ISARA Corporation is a leading stakeholder in the ETSI group that is working on this. ISARA Corporation also works to help educate other Secure Chorus members on post-quantum cryptography, and together we will work to integrate the identified quantum-safe cryptographic protocols into the Secure Chorus interoperability standards. Ultimately, Secure Chorus vendor members will integrate quantum-safe technology into their solutions, contributing to a strengthened ecosystem of products that is usable, scalable, regulatory-compliant and affordable.
Building the defence
Building the defence

What are the risks?

When contemplating threats from quantum computers, one of the first questions to consider is: “When realistically will we see the launch of a commercially significant large-scale quantum computer?” Within the industry, there are many opinions with answers ranging from 2026 [21] to 2030 [22]. However, due to a variety of factors, such as length of secrecy obligations, complexity of migrating to new security and the lifetime of the product or service being protected, it is essential to ask: “What are the risks when a scalable quantum computer arrives, i.e., when an unprotected system comes to a complete cryptographic collapse?” Assessing the amount of potential damage caused by a successful quantum computer attack against currently used public key cryptography systems should be an essential consideration in determining when to start preparing and taking action.

As discussed in the previous sections, current public key cryptography is extremely vulnerable to quantum attacks. Public key cryptography is the foundation for establishing confidentiality and authentication in today’s telecommunication networks.

Confidentiality

Confidentiality ensures that sensitive information is kept secret, such that outsiders cannot obtain the information. In the Secure Chorus standards, the key establishment phase uses the SAKKE algorithm to establish a shared secret, which is then ultimately used to generate session keys. The subsequent data traffic is encrypted using the session keys.

Authentication

Authentication ensures that the source of data communication comes from the party that it claims to be. Without authentication, the received information may have been compromised by a malicious entity, such as an adversarial nation-state actor intent on causing damage, or the information may be sent to the wrong party resulting in the leak of secret information. Secure Chorus uses a Key Management Service (KMS) as a root of trust and distributor of key material, making use of ECCSI to do so. The KMS provides users with assurance of the authenticity of the peers with whom they communicate.

Public key cryptography systems are not only critical for secure multimedia communications in the form of calls and emails between individuals, but also when considering machine-to-machine communication. Authentication is especially critical in providing Over-the-Air (OTA) services. OTA software updates are very common because they reduce update costs, enable prompt action upon discovery of critical flaws, and provide convenience for the end user. However, if a server providing these OTA software updates is not authenticated, there is the possibility that the downloaded code has been compromised and sent by a malicious entity intent on causing serious damage.

A quantum computer in the hands of an attacker can considerably damage the security of today’s telecommunication networks. There is no confidentiality against such an attacker since the communicated data can easily be decrypted. The communicating parties cannot trust each other because there is no guarantee that the other party is indeed the intended party. It could be the attacker renders the OTA services untrustworthy since the software may be compromised and sent from a malicious source.
When to start?

Two significant factors to consider when determining when to take action are: the duration that the security is required, and the time it takes to upgrade the system to a quantum-safe state. If the duration has any intersection with the estimated ranges of when a large-scale quantum computer is available, preparation may be necessary. It is possible to determine when to start preparing and taking action by tracing back from the point of danger and including the time required to upgrade.

For example, consider that a vehicle model’s average lifespan on the road is 11.5 years [23] and the time to develop and produce the vehicle is approximately 6-8 years [24]. The total number of years from development to end of life is approximately 19.5 years. If a conservative date of 2033 is used to estimate the arrival of a quantum computer, vehicles with the model year of 2022 could potentially be vulnerable to a quantum-enabled attack via malicious OTA updates.

Another key example is secure communications systems. Secure communications systems gain their complexity through the long time frame required to properly design and implement them, combined with the long roll-out process. This is especially complicated by the fact that special hardware may be required in military or policing contexts. That process to selected quantum-safe algorithms, update protocols to utilize them, complete the software development and then perform all of the necessary quality assurance testing including forwards and backwards compatibility, can easily take 5-7 years. The deployment portion, both including the testing in corporate networks and then the long deprecation and swap out cycle, can easily take a similar amount of time. When you then consider this along with the fact that some nation states are already storing encrypted communications to decrypt later with a quantum computer, this implies that organizations need to begin planning now to protect their confidential information.

Typically, long-term confidential obligations are clear due to legal restrictions, etc. However, the realistic duration for migration to a quantum-safe environment may not be easily predicted. The following aspects must be taken into consideration:

1. Where does all the cryptography reside within an organization? Cryptography is ubiquitous and since IT leaders rarely have to consider altering cryptography, discovering every instance throughout systems and the technology stack can prove time-consuming and challenging.

2. How adept is your organization at dealing with even routine changes? Small organizations can oftentimes remain agile. However, as an organization grows larger, it becomes harder to make any change simply due to its size and complexity [25]. The sheer number of components makes it more cumbersome and time-consuming to make changes. For example, the United States Department of Defense (DoD) PKI interoperability structure allows those residing in DoD to interact with approved external PKIs through a federal bridge [26]. As a result, it can be assumed that it will be a significant logistical and costly challenge to transform the cryptography used throughout such a multi-actor system.
3. **Which partners and vendors do you rely on for systems or parts?** After understanding the vulnerability points, many organizations will have to work with their vendors and partners to ensure the components within the entire chain are quantum-safe, which requires a high level of coordination. Also, this may cause further complication due to points 1 and 2 above.

History has shown that it is an extremely time-consuming process to upgrade cryptography. More than ten years were required to replace Data Encryption Standard (DES) with Advanced Encryption Standard (AES) or to remove Message Digest 5 (MD5) from widespread use. The conversion to ECDH and ECDSA from RSA has still not been completed in many organizations. Therefore, immediate action may be needed to ensure protection of certain critical information and infrastructure. Regardless of the estimated time of arrival of large-scale quantum computers, it’s possible some organizations are already too late in starting preparations and migration.

**Establishing quantum-safe confidentiality**

There may be an immediate threat to data confidentiality. Encrypted data communicated today can be, and in some cases has been, harvested and saved in its encrypted form with the intention of decrypting the stolen data as soon as a large-scale quantum computer becomes available. If the communicated data has short-term confidentiality obligations, such as the financial information before a quarterly earnings announcement of a public company, there is no immediate need for quantum safety. This type of information will become public knowledge before a large-scale quantum computer arrives. In contrast, data such as trade secrets, patient records, and government communications may be at risk because they typically have confidentiality obligations longer than a decade. Furthermore, the General Data Protection Regulation (GDPR), which becomes effective in May 2018, mandates healthcare records of EU citizens be kept confidential for the life of the patient. In these scenarios, quantum-safe security is required today in order to maintain confidentiality of the information in the future.
To achieve quantum-safe key establishment, which builds confidentiality, a hybrid-algorithm approach is recommended. In this approach, one or more quantum-safe key establishment techniques such as Kyber and/or Super Singular Isogeny Key Encapsulation (SIKE) are used along with a traditional technique such as RSA encryption, DH, or ECDH. Each technique establishes shared secrets independently. Then they can be merged via various techniques to generate a shared secret. This hybrid approach, combined with a protocol designed to allow for cryptographic algorithm agility, provides the best approach to mitigate risks.

**Establishing quantum-safe authentication**

Unlike confidentiality, authentication is not vulnerable until a large-scale commercially significant quantum computer becomes available. This is because actually attacking authentication, such as impersonating a server, is an active attack and hence requires a quantum computer sufficiently large at the time of the attack. However, many systems rely upon roots of trust that are built into hardware. The design time required to prepare new hardware for quantum safe authentication, along with the sheer cost of updating the hardware on already deployed systems, indicates that action is needed soon. The complexity of changes required for hardware “roots of trust”, especially in long-life systems such as cars or the electrical grid, mean that planning is required today.

**Quantum-safe communications**

Secure communication requires both encryption (confidentiality) and authentication to build trust. As has been discussed, options to upgrade both functionalities to defend against quantum attacks exist and when combined with Quantum-Safe Identity Based solutions, we can be assured that communications, whether over voice, video or text, are protected from the quantum threat.
8 Conclusion
Conclusion

Large-scale quantum computers pose significant threats to our network security by defeating currently used public key cryptography. Our systems must be replaced with quantum-safe equivalents to protect critical infrastructure and confidential assets.

The time required to migrate large complex communications system in use today (e.g. the United States Department of Defense (DoD) PKI interoperability structure) to make them compatible with quantum-safe algorithms shouldn’t be underestimated. In collaboration with Secure Chorus, ISARA Corporation is taking the lead in developing Quantum-Safe Identity-based Public Key Cryptography communications solutions that government and large enterprise users can rely upon to protect them from the quantum threat.

Secure Chorus leverages the key innovations developed in MIKEY-SAKKE – Secure Chorus’ open cryptography standard of choice – to address modern needs for secure multimedia communications. Secure Chorus’ interoperability standards allow for the creation of a marketplace of compliant secure multimedia solutions with essential functionality that suit the requirements of the day-to-day activities of a wide range of users. ISARA, as a partner member of Secure Chorus, is working on the development of a Post-Quantum Identity Based Crypto Scheme to update Secure MIKEY-SAKKE. All Secure Chorus members need to work together to develop the quantum-safe versions of MIKEY-SAKKE and the necessary Secure Chorus interoperability standards.

Secure Chorus’ Members and Observers are working together to achieve a shared vision – to deliver a globally connected and safe digital environment through open standards and public private sector collaboration - now and in the future. Secure Chorus’ intention is to ensure post-quantum capability in its interoperability standards to ensure the longevity of its usable, scalable, regulatory-compliant and affordable ecosystem of products. Secure Chorus will be following the work of industry members, academia and government to identify the optimal solution to address this critical challenge. Secure Chorus’ business model, based on private-public sector collaboration and open industry standards can best address the challenges enterprises are facing with regard to the post-quantum future that awaits us.
References


CONTACT DETAILS:
One Canada Square,
Canary Wharf,
London E14 5AB

General Inquiries: info@securechorus.org
Membership Inquiries: membership@securechorus.org

www.securechorus.org

@SecureChorus

/company/secure-chorus-ltd/

Design
www.springboardmarketing.co.uk

Secure Chorus Ltd, a not-for-profit private company limited by guarantee, under The Companies Act 2006 and the situation of its registered office is in England and Wales.

Copyright © Secure Chorus Limited 2018 - Present. All Rights Reserved.