February 23, 2018

The Quantum Revolution:

Security Implications and Considerations

Atsushi Yamada, VP of Research & Development
ISARA Corporation

Table of Contents

Abstract

Powerful quantum computers have the potential to bring positive disruption and tremendous benefits to our society. However, they also pose a potential threat to our current security technology used to protect online transactions and digital information. This whitepaper introduces technologies to build defence against potential quantum attacks, provides analysis on the risks, and discusses strategies for migration and deployment.

1 Quantum Computing: Benefits & Threats

1.1. 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].

1.2. Threats Posed by Quantum Computing

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

Symmetric key cryptography such as Advanced Encryption Scheme (AES) or Secure Hash Algorithm (SHA) -2 and -3 will not be completely compromised. The only known attack 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 by simply increasing the key sizes or output sizes to at most twice their current size [7].

However, it's become apparent that 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)
- elliptic curve discrete log-based cryptosystems, Elliptic Curve Diffie-Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA)

are extremely vulnerable by using Shor's algorithm, which is designed to solve these hard-mathematical problems with extreme efficiency [8]. Since these algorithms 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 today. It is necessary to replace these public key cryptosystems with quantum-safe equivalents as recommended by NIST [9].

2 Defensive Technology Against Quantum Attacks

2.1. Quantum-Safe Cryptography

As discussed in Section 1.2, 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 [10] [11]:

- Hash-based cryptosystems
- Code-based cryptosystems
- Lattice-based cryptosystems
- Multivariate cryptosystems
- Supersingular isogeny 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 standardization of quantum-safe cryptography is an on-going process as described in Section 2.2.

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, standardization activities are in progress as described in Section 2.2.

2.2. Standardization 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. [12]). 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 [13].

In 2017, the European Telecommunication Standardization 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 [14].

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) [15] [16]. 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 [17]. 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 (SC17) introduced an optional extension to the next version of the ITU-T Rec. X.509 digital certificate standard [14]. 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.

3 Building the Defence

3.1. What are the Risks?

When contemplating threats by 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 [18] to 2030 [19]. 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 damages 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 Section 1.2, 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 ensures that sensitive information is kept secret, such that outsiders cannot obtain the information. In secure communication protocols

such as TLS and IPsec/IKE, key establishment phase uses Rivest Shamir Adelman (RSA) encryption, Diffie-Hellman (DH), or Elliptic Curve Diffie-Hellman (ECDH) algorithms to establish a shared secret, which is then used to generate session keys. The subsequent data traffic is encrypted using the session keys.

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 communication protocols such as TLS and IPsec/IKE use digital signatures and digital certificates to authenticate one another at the initial connection establishment period. A digital certificate binds the identity of the entity and its public key by a digital signature of a third-party authority referred to as a Certificate Authority (CA). Thus, the trust of the signature within a certificate is established by the Public Key Infrastructure (PKI) system.

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 provides convenience for the end users. However, if such a server 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, rendering the OTA services untrustworthy since the software may be compromised and sent from a malicious source. Section 3.3 provides the strategy to achieve quantum-safe confidentiality, and Section 3.4 discusses migration to quantum-safe authentication.

3.2. When to Start?

Two significant factors to consider when determining when to take action include: 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's average lifespan on the road is 11.5 years [20] and the time to develop and produce the vehicle is approximately 6-8 years [21]. 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.

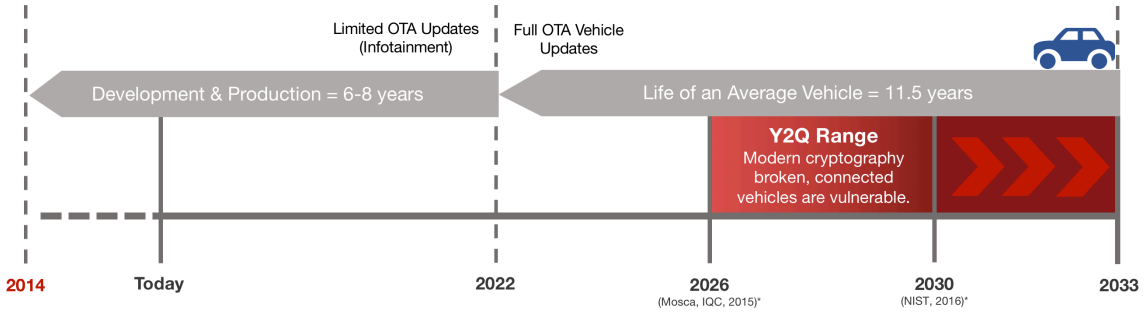

Figure 1: When vehicles may be impacted by quantum-enabled attacks on OTA updates

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 straightforward. 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 each and 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 [22]. 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 [23]. As a result, one can

assume that it will be a significant logistical and costly challenge to transform the cryptography.

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 the first and second point 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), and 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.

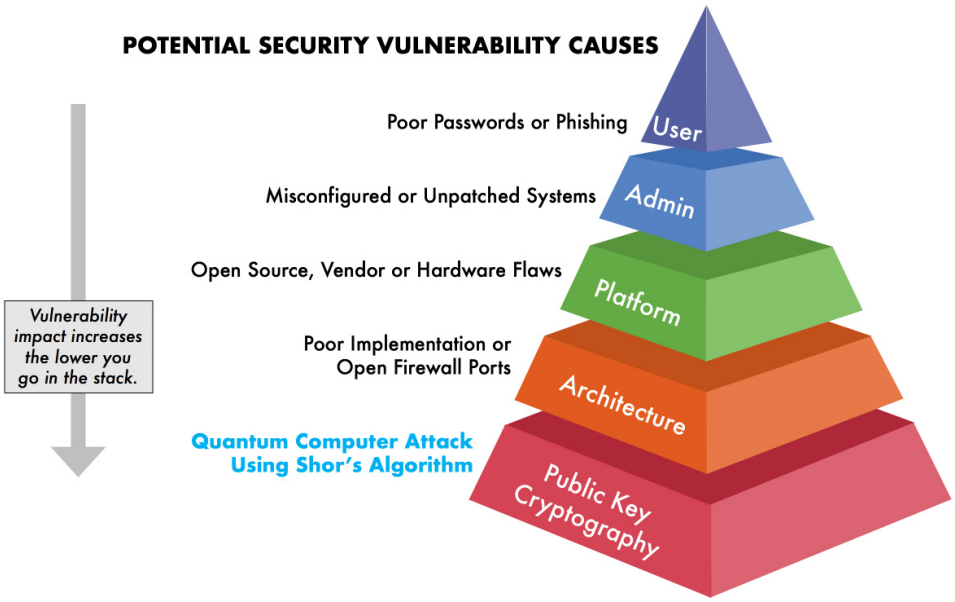

Figure 2: Demonstrating the various potential security vulnerability causes, and the foundation of security relying upon cryptography.

3.3. 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 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. The information will become public knowledge before a large-scale quantum computer arrives. In comparison, 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 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 by an exclusive or cryptographic hash to generate a shared secret. It is recommended to use at least two quantum-safe algorithms from different cryptosystems in case one may be broken in the near future.

3.4. Establishing Quantum-Safe Authentication

Unlike confidentiality, authentication is not vulnerable until a large-scale commercially significant quantum computer becomes available. However, action will need to be taken soon due to the sheer scope of the work required to update current PKI systems to quantum-safe security. It is extremely time-consuming due to the size and complexities of the infrastructure and it's many forward and backward dependencies. This is especially true for large government organizations, such as the United States Department of Defense's incredibly intricate PKI system [23]. When migrating critical components within a PKI, the root of trust is examined first. This is followed by a discussion to determine how to seamlessly migrate the PKI system while maintaining forward and backward capability.

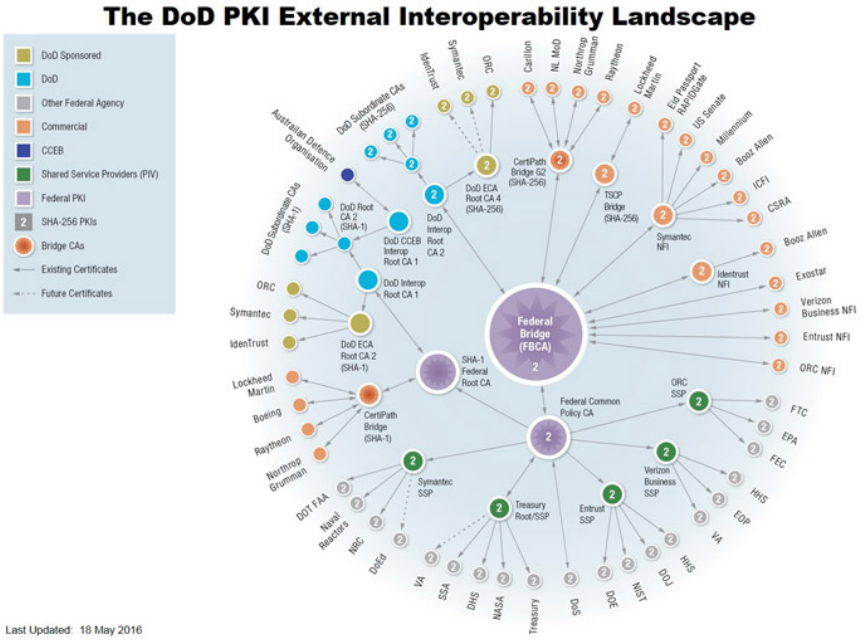

Figure 3: Demonstrating the complexity of the United States Department of Defense PKI [23].

3.4.1 Securing the Root of Trust

The Root of trust in the PKI system is a single point of failure. Therefore, it is exposed to a significant amount of risks. The most trusted, reliable, and stable digital signature algorithm must be used to secure roots of trust against quantum-enabled attacks. LMS and XMSS may be the most trusted and stable quantum-safe digital signature algorithms suited to deploy for root CAs.

These algorithms are derivatives of a Merkle Tree Signature, which was first published in 1979 and has been well studied [10] [24]. The security of the algorithms is based on second pre-image resistance of cryptographic functions, which is believed to be quantum-safe. In fact, these algorithms are expected to soon become a part of an approved standard at IETF [15, 17, 25] [16].

The drawback of these algorithms is that they have states that need to be managed securely. Thus, they must be implemented carefully in a way where the state information is secured with safeguards against accidents (such as physical system failures). Furthermore, they have limits in the number of signatures that can be produced for a single public key. Once the signatures are exhausted, a new key pair must be generated. These algorithms are suitable for CAs and code signing servers, where the systems are heavily secured, and do not require excessive amounts of signature generations.

3.4.2 Migrating to Quantum-Safe PKI

Corporate and government identity management systems rely on PKI for authentication. Current PKI systems rely on X.509 certificates, which allow only a single algorithm to be used at a time [26]. Migration of a PKI system today is typically performed by creating a complete duplicate of the infrastructure, where a new system with a new digital signature algorithm is built for the entire network and used simultaneously during the transition. This is a very slow, logistically complex and cost prohibitive migration process.

A new innovative approach that introduces an optional extension that allows an additional public key of a different signature algorithm to be added to a single X.509 certificate was proposed and has been approved by the ITU [27]. This new version is expected to be added to "Recommendation ITU-T X509 | ISO/IEC 9594-8" [28]. This certificate preserves the X.509 structure, while adding a quantum-safe subject public key and an issuer signature in the optional extension. Therefore, PKI infrastructure that combines an unmodified legacy system using RSA or ECDSA with one that contains quantum-safe upgraded elements can validate either type of certificate. Elements of the infrastructure already upgraded can use the quantum-safe algorithm to ensure quantum-safe communications. This type of hybrid transition provides true backwards compatibility during migration.

This new digital certificate technology allows the mixture of entities with old and new digital signature algorithms simultaneously, while enabling the seamless migration to a new cryptosystem without service stoppage. Also, it uses the existing PKI system and does not require duplication of the system, which minimizes migration costs. In fact, it achieves cryptographic agility in a true sense [29].

4 Conclusions

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 PKI systems in use today to make them compatible with quantum-safe algorithms cannot be underestimated. While the NIST standardization process for quantum-safe algorithms is underway (taking several years to select the final algorithms), achieving cryptographic agility is critical to the future of security.

ISARA has been working tirelessly to enable a seamless migration to quantum-safe world. We have been contributing to quantum-safe algorithms development, implementation, standardization, and deployments since 2015. We have also achieved the world's first Hardware Security Module (HSM) quantum-safe code signing proof of concept. In addition, ISARA has developed a new technology that extends X.509 certificate to achieve cryptographic agility.

5 About ISARA Corporation

ISARA Corporation is a security solutions leader specializing in creating **class-defining quantum-safe cryptography** (QSC) for today's computing ecosystems.

Experts estimate that within a decade, a large-scale quantum computer will be able to break public-key cryptography, the universal foundation of digital trust. Migrating to QSC is a long-term project, therefore NIST advises starting early. The ISARA Radiate™ Security Solution Suite is a high-quality implementation of recognized quantum-safe algorithms and integration tools. Embedding ISARA Radiate™ into ICT products secures data with long-term protection requirements while maintaining current encryption standards.

ISARA, headquartered in Waterloo, Ontario with an office in Silicon Valley, includes 9 PhDs in quantum physics and math, numerous Master's graduates and several ex-BlackBerry executives from the product security team and sales.

6 Bibliography

[1] E. Pednault, "Quantum Computing: Breaking Through the 49 Qubit Simulation Barrier," 17 October 2017. [Online]. Available: https://www.ibm.com/blogs/research/2017/10/quantum-computing-barrier/.

[2] M. Locklear, "Microsoft offers developers a preview of its quantum computing kit," 12 November 2017. [Online]. Available: https://www.engadget.com/2017/12/11/microsoft-developers-preview-quantum-computing-kit/.

[3] MIT Technology Review, "Google Reveals Blueprint for Quantum Supremacy," 4 October 2017. [Online]. Available: https://www.technologyreview.com/s/609035/google-reveals-blueprint-for-quantum-supremacy/.

[4] MIT Technology Review, "IBM Has Used Its Quantum Computer to Simulate a Molecule—Here's Why That's Big News," 13 September 2017. [Online]. Available: https://www.technologyreview.com/the-download/608866/ibm-has-used-its-quantum-computer-to-simulate-a-molecule-heres-why-thats-big/.

[5] HuffPost, "How Quantum Computers Will Revolutionize Artificial Intelligence, Machine Learning And Big Data," 12 October 2017. [Online]. Available: https://www.huffingtonpost.com/entry/how-quantum-computers-will-revolutionize-artificial_us_59ca1ab6e4b0b7022a646d84.

[6] Wikipedia, "Grover's algorithm," 9 January 2017. [Online]. Available: https://en.wikipedia.org/wiki/Grover's_algorithm . [Accessed 12 January 2018].

[7] ETSI, "Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges," June 2015. [Online]. Available: http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[8] Wikipedia, "Shor's algorithm," 12 January 2017. [Online]. Available: https://en.wikipedia.org/wiki/Shor's_algorithm .

[9] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography," 3 January 2017. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[10] D. J. Bernstein, J. Buchmann and E. Dahmen, Post-Quantum Cryptography, Springer, 2009.

[11] C. Costello, P. Longa and M. Naehrig, "Efficient algorithms for supersingular isogeny Diffie-Hellman," Microsoft Research, USA, 26 April 2016. [Online]. Available: https://eprint.iacr.org/2016/413.pdf.

[12] B. Schneier, "Schneier on Security," 21 August 2015. [Online]. Available: https://www.schneier.com/blog/archives/2015/08/nsa_plans_for_a.html. [Accessed 22 February 2018].

[13] National Institute of Standards and Technology (NIST), "Post-Quantum Cryptography Round 1 Submissions," 3 January 2017. [Online]. Available: https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[14] M. Pecen, "Why technology standards are critical to Quantum-Safe Security," SAFEGUARD Blog Post, 26 October 2017. [Online]. Available: https://www.safeguard.com/2017/10/26/technology-standards-critical-quantum-safe-security/.

[15] D. McGrew, M. Curcio and S. Fluhrer, "Hash-Based Signatures," IETF CFRG, 6 October 2017. [Online]. Available: https://datatracker.ietf.org/doc/draft-mcgrew-hash-sigs/.

[16] A. Huelsing, D. Butin, S. Gazdag, J. Rijneveld and A. Mohaisen, "XMSS: Extended Hash-Based Signatures," IETF CFRG, 13 December 2017. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/.

[17] W. Whyte, Z. Zhang, S. Fluhrer and O. Garcia-Morchon, "Quantum-Safe Hybrid (QSH) Key Exchange for Transport Layer Security (TLS) version 1.3," IETF, 3 October 2017. [Online]. Available: https://tools.ietf.org/html/draft-whyte-qsh-tls13-06.

[18] M. Mosca, "Cybersecurity in an era with quantum computers: will we be ready?," Institute for Quantum Computing and Department of Combinatorics and Optimization, University of Waterloo, 5 November 2015. [Online]. Available: https://eprint.iacr.org/2015/1075.pdf.

[19] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner and D. Smith-Tone, "Report on Post-Quantum Cryptography," NIST, April 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[20] IHS Markit, "Average Age of Light Vehicles in the U.S. Rises Slightly in 2015 to 11.5 years, IHS Reports," 29 July 2015. [Online].

Available: http://news.ihsmarkit.com/press-release/automotive/average-age-light-vehicles-us-rises-slightly-2015-115-years-ihs-reports.

[21] R. Schmidgall, "Automotive Embedded Systems Software Reprogramming Thesis," May 2012. [Online]. Available: http://bura.brunel.ac.uk/bitstream/2438/7070/1/FulltextThesis.pdf.

[22] A. Crowther, "The unfair advantage," 13 October 2015. [Online]. Available: https://www.linkedin.com/pulse/wining-all-matters-adrian-crowther/.

[23] I. A. S. E. (IASE), "External and Federal PKI Interoperability," May 2016. [Online]. Available: https://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx.

[24] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[25] P. Kampanakis, P. Panburana, E. Daw and D. Van Geest, "The Viability of Post-Quantum X.509 Certificates," 11 January 2018. [Online]. Available: https://eprint.iacr.org/2018/063.pdf.

[26] "X.509," Wikipedia, 22 February 2018. [Online]. Available: https://en.wikipedia.org/wiki/X.509.

[27] ISARA Corporation, "ISARA sets new international standard for quantum-safe security," 7 September 2017. [Online]. Available: https://www.prnewswire.com/news-releases/isara-sets-new-international-standard-for-quantum-safe-security-300515858.html?tc=eml_cleartime .

[28] "ITU-T X.509 (10/2016)," ITU, October 2016. [Online]. Available: http://www.itu.int/itu-t/recommendations/rec.aspx?rec=X.509.

[29] B. Sullivan, "Cryptographic Agility," 2010. [Online]. Available: https://media.blackhat.com/bh-us-10/whitepapers/Sullivan/BlackHat-USA-2010-Sullivan-Cryptographic-Agility-wp.pdf.