The Complex Path to Quantum Resistance

**IS YOUR
ORGANIZATION
PREPARED?**

ATEFEH MASHATAN AND DOUGLAS HEINTZMAN

There is a new technology on the horizon that will forever change the information security and privacy industry landscape. Quantum computing, together with quantum communication, will have many beneficial applications but will also be capable of breaking many of today's most popular cryptographic techniques that help ensure data protection—in particular, confidentiality and integrity of sensitive information. These techniques are ubiquitously embedded in today's digital fabric and implemented by many industries such as finance, health care, utilities, and the broader information communication technology (ICT) community. It is therefore imperative for ICT executives to prepare for the transition from quantum-vulnerable to quantum-resistant technologies.

This transition will be particularly complex, time-

consuming, and expensive for larger organizations with vendor dependencies and/or legacy infrastructure. Hence, it is critical that ICT leaders spend adequate time—now, while they have the luxury to do so—on planning the transition and determining their next steps. Otherwise, they may find their organizations in a chaotic state, scrambling to meet a compliance deadline or to prevent an actual loss of confidentiality or integrity of their, their customer's, or their partner's sensitive information. The absence of a well-thought-out plan could result in further delays and security vulnerabilities. Ultimately, it could have drastic implications for their core businesses and bottom lines.

The good news is that security systems not susceptible to quantum attacks (i.e., those that are *quantum-resistant*), can be implemented using today's classical computers. Organizations will not need quantum computers to resist attacks by another party's quantum computer. Several algorithms that are mathematically shown to be quantum-resistant already exist.

Standardization bodies such as the National Institute of Standards and Technology (NIST) in the U.S. and the European Telecommunications Standards Institute (ETSI) in Europe have been working on the standardization of quantum-resistant primitives since 2015,^{12,23} promising a final set of alternatives by 2025. In many cases, however, these algorithms may not be compatible with current hardware or software. For example, when existing algorithms are hardcoded in a piece of hardware, replacing the quantum-vulnerable algorithm with a quantum-resistant alternative involves swapping out the hardware.

Given the serious nature of the threat, the question organizations should be asking is how can the process of transitioning to quantum-resistant systems be accomplished in a timely and cost-effective manner, even as the solutions have yet to be standardized?

The industry's challenge is in migrating to compatible hardware platforms and ensuring the software running on those platforms is upgraded to use quantum-resistant protocols. Depending on the needs of an organization and its approach to cryptography management, modifications to digital information security systems can range from relatively straightforward, quick, and inexpensive; to massively complex, drawn-out, and costly. The transition to a quantum-resistant state is no exception.

Competing quantum-resistant proposals are currently going through academic due diligence and scrutiny by industry leaders. Until the newly minted quantum-resistant standards are finalized, ICT leaders should do their best to plan for a smooth transition. This article provides a series of recommendations for these decision-makers, including what they need to know and do today. It will help them in devising an effective quantum transition plan with a holistic lens that considers the affected assets in *people*, *process*, and *technology*. To do so, the decision-makers first need to comprehend the nature of quantum computing in order to grasp the impact of the impending quantum threat and appreciate its magnitude.

QUANTUM COMPUTING

A quantum computer uses qubits (quantum bits), as opposed to classical bits, to process information. Qubits

are two-state quantum systems. While a classical bit can be either a one or a zero, a qubit can be in any *quantum superposition* of zero and one. Measuring the state of a qubit causes it to collapse into one of the two states. With classical computing, four bits can have 2^4 (16) possible states but can be in only one state at a time. Superposition allows quantum computing to process all 2^4 possible states with four qubits at the same time.

Indeed, superposition paves the way for massive parallelization when searching for an answer to an equation. As the number of qubits scale so do the number of states, but with an exponential rate. For example, with 30 qubits, you can represent and process more than a billion values at once. The use of qubits in a superposition state allows quantum computers to solve some problems significantly faster than classical computers. This speedup is the reason why quantum computing is a threat to information systems' security and privacy.

THREAT TO CYBERSECURITY

Quantum computing's main potential threat to information security is in the area of cryptography. Cryptography runs behind the scenes, out of the user's view, to keep information and communications secure. Two broad types of cryptography exist: symmetric/secret key and asymmetric/public key. Understanding the difference between the two is critical, as quantum computing impacts each differently.

Let's look at an example that illustrates the impact of a scalable quantum computer on the security of sensitive data. Many of the world's data-security practices rely on the RSA (Rivest-Shamir-Adleman) cryptosystem, which

uses a product of two large prime numbers and assumes it is hard for an adversary to factor the resulting product to find the initial prime numbers. This is known as an integer factorization problem (IFP), the intractability of which is a cornerstone in ensuring online security.

There is a good reason for this: If you choose the numbers carefully, factoring the resulting large product is indeed very difficult. A classical 2.2-GHz Opteron CPU (a standard benchmark) would take about 10^{145} years to factor a 1,024-bit number, or about 7.25×10^{135} times the age of the universe. If a quantum computer is developed that can execute 100 million instructions per second (not unheard of in a desktop computer today), it could factor that number in a matter of seconds.²⁶ The main alternative cryptographic system—ECC (elliptic curve cryptography)—is not spared either. Although it is based on a different mathematical problem—namely, the discrete logarithm problem (DLP)—it too can be efficiently broken by a scalable quantum computer. At this point, the question isn't about whether quantum computers break today's encryption standards but *when* will they reach the performance level to do so.

This presents a significant challenge because the standardized RSA and ECC cryptosystems serve as the foundation of many of the cybersecurity tools and techniques that protect the world's economy. The advent of the age of quantum computers will be massively disruptive. It is safe to assume that in the next decade or two, malicious actors (individuals or organizations) will be able to circumvent today's commonly used and trusted means of securing confidential information.

Organizations should be asking themselves now to what extent this will impact them and what they need to do to mitigate the risk.

It is not unreasonable for organizations to wonder why they should worry about the quantum threat if it is many years away. This is partially warranted. It is true that attackers cannot truly attack today's cybersecurity ecosystem until they have a scalable quantum computer, but their awareness of the inevitable availability of scalable quantum computers in the future may incentivize data harvesting breach attacks in the present. Furthermore, even if the threat is not imminent, major security changes, especially those that involve asymmetric cryptography, will take time to implement.⁵ Careful analysis, planning, and action need to be performed immediately.

When planning a response strategy, security professionals need to be concerned about two forms of attacks: *realtime* and *harvest-then-decrypt*.²⁹

Realtime attacks occur when a quantum computer is actually in the hands of an adversary. As already mentioned, asymmetric cryptography relying on IFP or DLP is catastrophically vulnerable to a scalable quantum computer attack. Symmetric cryptography is vulnerable, at least with its current key sizes, for slightly different reasons. Organizations or individuals whose communications, transactions, and authentications are still using current asymmetric or symmetric algorithms could be attacked when a scalable quantum computer is realized.¹² These realtime attacks are not currently possible, because a scaled-quantum computer is not yet available.

The harvest-then-decrypt attack happens when an adversary captures and stores encrypted data and sits on it until a quantum computer becomes available to provide a means for decryption.²⁹ Depending on the sensitivity or the shelf life of the data, this type of attack can be a serious current threat. Malicious actors could harvest encrypted data today, put it aside for a few years, and wait for the availability of an affordable quantum computer so they can decrypt that data. Considering the many well-publicized large-scale security breaches of companies such as Yahoo in 2013 and 2014, Marriott Starwood Hotels in 2018, and Capital One in 2019, this threat is very real. (Note that in 2019 alone, four billion records were breached.²⁷) In the meantime, a constant game of cat and mouse is being played out between the attackers who seek to cause harm and the security professionals who are tasked with stopping them.

IMPACT ON SYMMETRIC CRYPTOGRAPHY

Symmetric-key cryptography uses a secret key shared between two users. Party A can encrypt the data using the secret key and send the result to Party B, who uses the same key to decrypt and read the data. The secure exchange of the secret key between users, also known as key management, forms the security basis for symmetric cryptography. The vulnerability of this system is twofold: the need to transmit the key introduces the possibility that the key can be intercepted in transmission, and that quantum computers can use Grover's algorithm¹⁶ to improve the efficiency of a brute-force attack.

A secret key is generated using a source of randomness

and is of a predetermined size. Thus, because of the creation process, and since there is only one key, there is no mathematical relationship to crack. The only two ways to attack symmetric algorithms are cryptanalysis and brute force. A brute-force attack involves trying every possible key to decrypt the ciphertext and obtain the plaintext. On average, an attacker would have to try half of all possible keys to obtain the correct one. Therefore, a secret key with enough entropy and length can sufficiently protect encrypted information. Grover's algorithm, however, can make use of superposition of qubits to speed up the brute-force attack by roughly a quadratic factor (i.e., proportional to the square of the speed in which classical computing can make a brute-force attack on the keyspace^{6,22}). This reduces the strength of symmetric algorithms by approximately 50 percent. For example, 256-bit Advanced Encryption Standard (AES 256) would be able to provide only 128-bit security.²⁹

Fortunately, doubling the symmetric key sizes, when the algorithm specification can accommodate it, allows this form of cryptography to remain safe.¹² Doubling the key size is not a trivial task, however. It is reasonably straightforward when the cryptography is implemented in software, because an update may allow for an efficient key-size change. But in situations where the cryptography is implemented in hardware, changing the size is more challenging and expensive. For example, some types of routers and all hardware security modules (HSMs) will need to be replaced with hardware capable of accommodating larger key sizes. Depending on the size of the organization and the extent of its symmetric

cryptography use, this could be an extremely time-consuming and costly undertaking. Regardless, it will be a massive industry-wide transition, especially from a change management perspective.

IMPACT ON ASYMMETRIC CRYPTOGRAPHY

Asymmetric cryptography uses two keys: public (anyone can see it) and private (only authorized people can see it). The two keys are mathematically bound, which forms the basis of asymmetric cryptography's security. One of several computationally difficult mathematical problems can be used to bind the two keys and act as the basis for security. IFP and DLP are two of the more commonly used problems. Integer factorization derives its security from the difficulty of factoring the product of two large prime numbers. Discrete logarithms involve finding an unknown integer K , from $g=b^K$, where g and b are known elements with certain mathematical attributes.

Other mathematical problems have been proposed as ways to bind the public and private pair, resulting in a variety of different asymmetric cryptosystems. Among all such cryptosystems, RSA (based on IFP) and ECC (based on DLP) have been standardized and are widely used. Indeed, they strike a nice balance between simplicity, efficiency, and security—that is, until now. When the underlying computationally difficult problems can be efficiently solved by a scalable quantum computer, an attacker can go back in time and decrypt already harvested encrypted data through the application of Shor's algorithm.³⁰ This algorithm takes advantage of the fact that with enough qubits in superposition, a quantum computer can

simultaneously examine countless combinations of zeros and ones in parallel and, as research has demonstrated, solve the computationally difficult mathematical problems that form the basis of the public-key algorithm's security.

The number of combinations that can be explored simultaneously is dependent on the number of qubits available to a quantum computer. With enough qubits, a quantum computer can quickly reverse calculate the computationally difficult problem and obtain the private key.¹² In other words, the private key can be recovered from the public key, and the information being secured can be decrypted.

Other algorithms that are similarly vulnerable to quantum-enabled attacks include the Digital Signature Algorithm, Diffie-Hellman, Elliptic-Curve Diffie-Hellman, and Elliptic-Curve Digital Signature Algorithm.¹² Together with RSA and ECC, these algorithms are staples of security for the Internet, email, virtual private networks, and the Internet of things (IoT), making the quantum threat very serious and potentially broadly impactful. If the vulnerabilities of asymmetric cryptography were all to occur at the same time, they could lead to the deterioration of the security fabric that protects the digital society.

No matter how much the size of the initial parameters is increased, resulting in a larger key, the mathematical problems that asymmetric cryptosystems rely on can be solved in polynomial time on a scalable quantum computer. Hence, standardized and widely used asymmetric cryptographic systems will be severely impacted by a sufficiently capable quantum computer.

UNDERSTANDING TERMINOLOGY

Quantum information computing and cybersecurity mitigation against it are being researched heavily in academia and industry. With so much research and development, varying approaches, and the inherent complexity of the topic, different terminologies are used to describe different aspects of these related fields. As the language of the vendors is added on top of this, the various terminologies inevitably get muddled. So before proceeding, it is useful to clarify some of the often-used terminology.

QUANTUM CRYPTOGRAPHY

Quantum cryptography leverages the properties of quantum mechanics, as opposed to mathematics, to carry out cryptographic objectives such as key distribution. Quantum key distribution (QKD) is a method of transmitting a secret key over distance. It allows two parties to produce a shared random secret key known only to them, which can then be used to encrypt and decrypt messages and cannot be intercepted without the parties noticing, nor can it be reproduced by a third party. It is an *information-theoretically secure* solution to the key-management problem, which means its security is not based on any computational hardness assumption. It is the use of a quantum technology, and the need for physical infrastructure capable of transmitting quantum states, that gives rise to the label of quantum cryptography (which is not the focus of this article).

POST-QUANTUM CRYPTOGRAPHY

Post-quantum cryptography, also known as quantum-

resistant or quantum-safe cryptography, is a subset of classical cryptography which can be deployed on existing classical devices and is currently believed to be safe against the threat of a scalable quantum computer.

Quantum computers are not good at efficiently solving every kind of mathematical problem. In fact, there are some encryption schemes that can be run on classical devices and are based on mathematical techniques that are *quantum-resistant*. The benefit of quantum-resistant cryptography is that it does not require a new physical infrastructure to deploy. The disadvantage is that it still relies on computational security (a hard-to-solve mathematical problem).

Cryptographers have been proposing such cryptosystems since as early as 1978 when the McEliece cryptosystem was developed at NASA's Jet Propulsion Laboratory.²⁰ The reason these quantum-resistant cryptosystems have not as yet been adopted is that standardized non-quantum-resistant cryptosystems were simpler, less resource intensive (and thus less expensive to implement), and "good enough." So there seemed to be no need for the quantum-resistant systems which, after all, only protected against a theoretical future threat. These systems were viewed more as theoretical contributions within the cryptographic community.

Moreover, such cryptosystems were not as closely examined as current widely used systems and they were not standardized—yet. As part of any standardization process, the algorithms typically go through years of due diligence and scrutiny conducted by academics and standardization bodies such as NIST and ETSI. Anticipating

that quantum development was accelerating, NIST announced a competition in 2015 for proposals for standards candidates for its quantum-resistant algorithm transition. It plans to evaluate the proposals through 2021 or 2022 and then formalize those selected into draft standards by 2024.²³

QUANTUM DEVELOPMENT

Many organizations are working toward developing scalable “universal gate” quantum computers (or simply universal quantum computers), including the Institute for Quantum Computing (IQC) at the University of Waterloo, QuTech at the University of Delft, the Yale Quantum Institute at Yale University, the Centre for Quantum Technologies in Singapore, and the Joint Quantum Institute in Maryland. Well-known companies such as Microsoft, Intel, IBM, and Google are in the race for quantum supremacy as well.⁸ There are some companies, such as D-Wave,¹¹ which build systems with thousands of qubits but use quantum annealing as opposed to universal gate architectures. These systems are very good at finding “good enough” or “local minima” solutions but not specific solutions. Quantum annealing computers cannot efficiently run Shor’s algorithm and thus do not represent the same threat to cryptography that the universal quantum gate computers do. Predictions about when one of these organizations will produce a quantum computer capable of breaking much of the world’s encryption vary greatly, but most estimates range between 6 and 11 years with a non-negligible success probability.²²

An important measure of quantum computing

development is its ability to execute Shor’s algorithm or perform a Grover’s search. This depends on the number of qubits, among other factors. The current estimates of the number of qubits in a universal quantum computer needed to break RSA 2048 (asymmetric cryptography) and AES 256 (symmetric cryptography) are 4,098 and 6,681, respectively.^{15,28} This number depends on several factors, such as the efficiency of fault-tolerant error-correcting codes, physical error models, error degrees of the physical quantum computer, optimizations in quantum factoring, and the efficiency of factoring algorithms into quantum gates.²² The number of qubits that predominant companies have been able to use is summarized in Figure 1.

At first glance, it may seem that a scalable quantum

FIGURE 1: **QUBIT COUNT BY COMPANY**

COMPANY	# OF QUBITS	NOTES
Google	53-72	Sycamore (Universal 54 qubit non-linear superconducting resonator); Bristlecone (Universal 72 qubit superconducting)
IBM	53	IBM Q-system53 (Universal 53 qubit superconducting). Announced plans for 127 qubits in 2021, 433 qubits in 2022, and 1000 qubits in 2023.
Intel	49	TangleLake (Universal 49 qubit superconducting universal test chip)
Rigetti	28	Aspen-7 (Universal 28 qubit superconducting)
Xanadu	24	X24 (Universal 24 qubit photonics)
D-Wave	5000	D-Wave Advantage (Annealing 5000 qubit superconducting). Designed for optimization problems. Not a threat to cryptography.

computer is still a long way off and, if history is a guide, current estimates of when a quantum computer at scale will be available may be overly optimistic (or pessimistic from a cryptography point of view). In 2009, Cisco predicted the first commercial quantum computer would be available by mid-2020.¹³ In 2016, other experts predicted a quantum computer within a decade.³ Over the years, much has been learned and significant improvements have been made, which may make more recent estimations more realistic. Mosca estimates a 20 percent chance of a universal quantum computer, with the ability to break RSA 2048, within 10 years.²² Mosca also states that “the likelihood of a scaled quantum computer in the next 20 years is an order of magnitude higher than it was 10 years ago.” With the increased global interest in quantum computing and increased resources dedicated to its development, these estimates may need to be revisited.

STRATEGIC IMPLICATIONS OF QUANTUM-RESISTANT SECURITY

The nature and capabilities of quantum computing and the complexities and tradeoffs of quantum-resistant primitives are well-documented in the physics, computer science, and engineering literature. This body of knowledge is kept current by several established research labs as quantum computing and quantum-resistant technologies advance. A large gap exists, however, between the theoretical and technical understanding of these technologies on the one hand and practical implications for businesses on the other. These businesses will need to spend time and money to

study the problem and adopt new technology to protect themselves.

As quantum computers are developed at a rapid pace, and with early models already on the market, the overall perception of the ICT community toward a quantum reality is slowly changing. Awareness of the issue has dramatically improved thanks in large part to the efforts of NIST¹⁰ and ETSI¹, organizations providing quantum and quantum-resistant solutions, not-for-profit groups,^{14,17,32} and most importantly, recent academic work that bridges the technical and managerial aspects of the quantum threat and its implications.¹⁹

There are some keystone works, such as the books by Bernstein et al.⁴ and Yan,³⁵ a white paper by Accenture Labs,²⁴ as well as the article by Mosca that examines the issue comprehensively.²² These works succinctly explain which types of cryptographic algorithms are susceptible to quantum attacks and why, and they provide possible solutions that existed at the time of publication. While academic and standardization bodies such as NIST and ETSI have been considering the steps that organizations should take against the threat of quantum computers to cryptography for many years, the issue did not gain popular media, and presumably public, attention until the National Security Agency began issuing warnings in mid-2015.^{10,12} This was also around the time when news of the first functioning quantum computers, produced by D-Wave Systems and vetted by Google and NASA, first showed up in popular media.³¹

Around the same time, the literature—both academic and popular—began to suggest business implications

for organizations needing to implement quantum-resistant security measures. Some of the literature, and related research and experimentation, was measured and pragmatic, while some was more sensational.^{9,18,32} Google announced in mid-2016 it was experimenting with quantum-resistant security in its Chrome browser using the algorithm code-named “New Hope.”⁷ The company stated that this was not intended to be a new standard; rather, it was explicitly an experiment. Around the same time, Microsoft made the “LatticeCrypto” library, which developers can use to experiment with quantum-resistant key exchange.²¹ The NIST Report on Post-Quantum Cryptography in April 2016 identified the impact of quantum computing on cryptographic algorithms and the families of quantum-resistant primitives.¹⁰

More recently, targeted vendor articles have been written for trade websites.^{22,33} These cover the issue in more practical terms but do not consider variances among industries in terms of their information security requirements or cryptography management structures. Notably, only one example could be found involving a survey of ICT managers, and this was in a nonacademic article in an online cybersecurity magazine.²⁵

While there is more awareness of the potential threat of quantum computing, this progress may not be enough. As a quantum reality gets closer and closer, the available time in which currently standardized cryptographic primitives can be relied upon is getting narrower and narrower. Organizations must get to work and move on to the next step. There needs to be more traction in response to calls for devising a plan ahead of the massive industry-

wide adoption from quantum-vulnerable to quantum-resistant technologies.

ICT leaders must devise concrete plans and dedicate adequate resources in their 5- to 10-year budget allocations. To do this, they need to fully understand the threat to valuable information assets and the related business implications.

RECOMMENDATIONS

Organizations in large, regulated sectors tend to be more aware of the threat of quantum attacks and their implications than their counterparts in smaller and unregulated sectors. Even among those aware of the threat, few are planning for mitigation steps in advance of formal recommendations from the standardization bodies. Most organizations do not have the in-house expertise needed to know what to do or when to do it. This can pose a significant threat to those industries handling sensitive data with a long expiry date, such as Social Security numbers and financial or health records.

The recommendations provided here, illustrated in Figure 2, focus on the *process* by which organizations can effectively assess and mitigate their exposure to quantum attacks. These recommendations are based on the existing literature, combined with empirical information gathered by an investigative study in which 23 ICT managers were asked about their companies' level of quantum threat awareness and plans for the transition to quantum resistance. The range of business scenarios is far broader than the current literature indicates, and the flexible recommendations presented here are intended to be more

2

FIGURE 2: QUANTUM READINESS ROADMAP

relevant to business managers than those previously proposed.

The steps detailed below are intended to aid technology executives and be applicable to organizations of various sizes and regulatory structures, and with diverse information security needs ranging from minimal to highly complex and integrated. By following these recommendations, business and technology managers can effectively size the risk of this threat to their respective organization, and then establish and execute the appropriate mitigation strategies (Scenarios A-C, described in the sidebar).

In all cases, establishing/empowering a governance model and body is a prerequisite to following these recommendations. The next step is to conduct a thorough quantum risk assessment that determines the scope of the risk to the organization, its potential magnitude, and the likelihood of a system being compromised. The output of this assessment is specific to each organization and largely depends on the sensitivity of its assets and its current approach to safeguarding them.

The next common step is to assess the organization's current cryptographic footprint to establish which cryptographic methods are being used and exactly where (software, hardware, or network) they are being employed. Where quantum vulnerabilities are found, quantum-resistant alternatives should be selected and implemented at the appropriate time (Scenarios A-C), based on technical and organizational requirements and feasibility. By taking the appropriate recommended steps, technology managers can ensure that they are effectively minimizing

Planning for Quantum Readiness

Determine Transition Path. Large and complex organizations tend to rely on established legislation and industry standards to inform their decisions in adopting, maintaining, and sunseting technology. These decisions are typically part of a 5- to 10-year planning and capital expense budget cycle.¹² At the same time, there is a good chance that commercial-scale quantum technology will become part of mainstream computing during the next 5-10 years.³⁴ As such, some of these organizations are already late in starting to plan for the transition to “quantum readiness,” and will be left scrambling to protect what data they can before time runs out.²² Having allocated appropriate resources, performed a risk assessment, and determined which systems may be at risk of quantum attacks in the future, organizations reach a critical decision point as follows:

- ➔ **Wait for Standardization.** In some cases, organizations may choose not to act until standardization bodies announce formal recommendations for quantum-resistant security, estimated to be available from NIST by 2024. This could be an appropriate business strategy decision for ICT managers when their organization’s confidential information is perceived to be of very low value to malicious attackers, has a very short shelf life, or is transient in nature. It may also be reasonable when they rely primarily or exclusively on external vendors for security and are confident those vendors will transition to quantum-resistant security quickly.
- ➔ **Invest in Crypto-agility.** Crypto-agility is the ease with which an organization is able to implement cryptographic changes. Where significant risk is present, and strategic mandate permits, organizations should invest in crypto-agility. This step is not unique to the threat of quantum attacks, but it is a prerequisite to reacting effectively once standards have been finalized.

➡ ***Establish and Maintain a Quantum-Resistance Roadmap.*** Before the certification of quantum-resistance standards, the projected timelines for an attack-capable quantum computer will be refined, as will the options for mitigating the risk. Organizations should establish a roadmap that tracks these developments as they pertain to their own specific context, and they should maintain it for the coming years until quantum-resistant security has been standardized, adopted, and implemented.

➡ ***Implement Hybrid Cryptography.*** For organizations with high risk, sufficient resources, and end-to-end control over their cryptographic ecosystems, overlaying a quantum-resistant security layer on top of existing pre-quantum security can be advantageous. It retains the standardized and mandated level of mitigation against attacks by today's classical computers, while mitigating the risk of harvest-then-decrypt attacks. Despite the additional cost, some organizations will have sufficient incentive and resources to pursue a hybrid strategy.

Remediation Projects. Regardless of which alternative is chosen, once the standards are published, organizations should move quickly to implement them in accordance with the ensuing compliance mandates. Organizations that adopt the wait-and-see approach (Scenario A) will need to research their path to quantum resistance based on their respective position at that time. Organizations that maintain a roadmap but do not implement a hybrid solution (Scenario B) will execute their roadmap. Those that implement a hybrid solution (Scenario C) will simply need to make (relatively minor) adjustments to what they already have in place. All organizations will also need to determine the deprecation path for their pre-quantum cryptographic implementations (e.g., RSA and ECC), as will likely be mandated in the standardization body recommendations.

the threat of quantum attacks on their respective organization.

Acknowledgments

This research was funded, in part, through a generous contribution from The Burnie Group, a Toronto-based management consulting firm with extensive practical experience rolling out large-scale technology transformations, and the Natural Sciences and Engineering Research Council of Canada (NSERC) under Engage Grant [EGP 543598 – 19, PI: Atefeh Mashatan]. The authors would like to acknowledge the efforts of Robert Fullerton and Ryan Kennedy for their assistance in conducting the preliminary stages of this research.

References

1. Alléaume, R., et al. 2018. Implementation security of quantum cryptography: introduction, challenges, solutions. ETSI White Paper No. 27. European Telecommunications Standards Institute; https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp27_qkd_imp_sec_FINAL.pdf.
2. Barker, W., Polk, W., Souppaya, M. 2020. Getting ready for post-quantum cryptography: explore challenges associated with adoption and use of post-quantum cryptographic algorithms. Cybersecurity White Paper. U.S. Department of Commerce, National Institute of Standards and Technology; <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.05262020-draft.pdf>
3. Bauer, B., Wecker, D., Millis, A., Hastings, B., Troyer, M. 2016. Hybrid quantum-classical approach to correlated

- materials. *Physical Review X* 6[3]; <https://journals.aps.org/prx/pdf/10.1103/PhysRevX.6.031045>.
4. Bernstein, D. J. 2009. Introduction to post-quantum cryptography. In *Post-Quantum Cryptography*, eds. D.J. Bernstein, J. Buchmann, and E. Dahmen, 1-14. Springer.
 5. Bindel, N., Herath, U., McKague, M., Stebila, D. 2017. Transitioning to a quantum-resistant public-key infrastructure. In *Post-Quantum Cryptography, Proceedings of PQCrypto 2017* eds. T. Lange and T. Takagi, 384-405. Springer; https://link.springer.com/chapter/10.1007/978-3-319-59879-6_22.
 6. Boyer, M., Brassard, G., Hoeyer, P., Tapp, A. 1998. Tight bounds on quantum searching. *Fortschritte der Physik*, 46(4-5), 493-505; <https://arxiv.org/abs/quant-ph/9605034>.
 7. Braithwaite, M. 2016. Experimenting with post-quantum cryptography. Google Security Blog; <https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html>.
 8. Buchmann, J., Lauter, K., Mosca, M. 2018. Postquantum cryptography, part 2. *IEEE Security & Privacy* 16(5), 12-13; <https://ieeexplore.ieee.org/document/8490197>.
 9. Campagna, M., Chen, L., Dagdelen, Ö., Ding, J., Fernick, J. K., Gisin, N., Hayford, D., Jennewein, T., Lütkenhaus, N., Mosca, M., et al. 2018. Quantum-safe cryptography and security. ETSI White Paper No. 8; <https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>.
 10. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D. 2016. Report on post-quantum cryptography. U.S. Department of Commerce,

- National Institute of Standards and Technology; <https://nvlpubs.nist.gov/nistpubs/lir/2016/NIST.IR.8105.pdf>.
11. D-Wave. Processing with D-Wave; <https://www.dwavesys.com/>.
 12. European Telecommunications Standards Institute (ETSI). 2015. Quantum-safe cryptography and security; <https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf>.
 13. Evans, D. 2009. Top 25 technology predictions. CISCO Internet Business Solutions Group; https://www.cisco.com/c/dam/en_us/about/ac79/docs/Top_25_Predictions_121409rev.pdf.
 14. evolutionQ; <https://evolutionq.com/news.html>.
 15. Grassl, M., Langenberg, B., Roetteler, M., Steinwandt, R. 2015. Applying Grover's algorithm to AES: quantum resource estimates. arXiv preprint arXiv:1512.04965; <https://arxiv.org/abs/1512.04965>.
 16. Grover, L. 1996. A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212-219; <https://dl.acm.org/doi/10.1145/237814.237866>.
 17. Isara. Isara's quantum-safe readiness program for enterprise. Isara; <https://www.isara.com/services/quantum-readiness-enterprise.html>.
 18. Majot, A., Yampolskiy, R. 2016. Global catastrophic risk and security implications of quantum computers. *Futures* 72, 17-26; <https://www.sciencedirect.com/science/article/abs/pii/S0016328715000294?via%3Dihub>.
 19. Mashatan, A., Turetken, O. 2020. Preparing for the information security threat from quantum computers.

- MIS Quarterly Executive* 19(2); <https://aisel.aisnet.org/misq/vol19/iss2/17>.
20. McEliece, R. 1978. A public-key cryptosystem based on algebraic coding theory. *DSN (Deep Space Network) Progress Report 42-44*; https://tmo.jpl.nasa.gov/progress_report/42-44/44N.PDF.
21. Microsoft. 2016. Lattice cryptography library. Microsoft; <https://www.microsoft.com/en-us/research/project/lattice-cryptography-library/>.
22. Mosca, M. 2018. Cybersecurity in an era with quantum computers: will we be ready? *IEEE Security & Privacy* 16(5), 38-41; <https://www.computer.org/csdl/magazine/sp/2018/05/msp2018050038/17D45W9KVFr>.
23. National Institute of Standards and Technology. 2020. Post-quantum cryptography round 3 finalists: public-key encryption and key-establishment algorithms. NIST; <https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions>.
24. O'Connor, L., Dukatz, C., DiValentin, L., Farhady, N. 2018. Cryptography in a post-quantum world: preparing intelligent enterprises now for a secure future. Accenture Labs; https://www.accenture.com/_acnmedia/pdf-87/accenture-809668-quantum-cryptography-whitepaper-v05.pdf.
25. Olenick, D. 2015. Quantum leap? *SC Magazine* 26(12), 16-17; <https://www.scmagazine.com/home/security-news/quantum-leap-the-impact-of-quantum-computing-on-encryption/>.
26. Phillips, T., The mathematics behind quantum computing. <https://www.math.stonybrook.edu/~tonyl/whatsnew/may07/quantum1.html>

27. Rafter, D. 2019. 2019 data breaches: 4 billion records breached so far. Norton; <https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html>.
28. Roetteler, M., Naehrig, M., Svore, K. M., Lauter, K. 2017. Quantum resource estimates for computing elliptic curve discrete logarithms. arXiv 1706.06752; <https://arxiv.org/abs/1706.06752>.
29. Schanck, J., Whyte, W., Zhang, Z. 2016. Criteria for selection of public-key cryptographic algorithms for quantum-safe hybrid cryptography. Internet draft. IETF; <https://tools.ietf.org/html/draft-whyte-select-pkc-qsh-02>.
30. Shor, P. 1997. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing* 26(5), 1484-1509; <https://epubs.siam.org/doi/10.1137/S0097539795293172>.
31. Simonite, T. 2015. Google says it has proved its controversial quantum computer really works. *MIT Technology Review*; <https://www.technologyreview.com/s/544276/google-says-it-has-proved-its-controversial-quantum-computer-really-works/>.
32. Soukharev, V. 2020. InfoSec Global's roadmap to migrate to NIST's new standards. InfoSec Global; <https://www.infosecglobal.com/post/infosec-globals-roadmap-to-migrate-to-nists-new-standards>.
33. Totzke, S. 2017. Top five questions about using quantum-safe security in financial transactions. *FinTech Futures*; <https://www.fintechfutures.com/2017/07/top-five-questions-about-using-quantum-safe-security-in-financial-transactions>.

34. Wallden, P., Kashefi, E. 2019. Cyber security in the quantum era. *Communications of the ACM* 62(4), 120; <https://cacm.acm.org/magazines/2019/4/235578-cyber-security-in-the-quantum-era/fulltext>.
35. Yan, S. Y. 2013. Quantum-resistant cryptosystems. In *Quantum Attacks on Public-Key Cryptosystems*, 189-203. Boston: Springer; https://doi.org/10.1007/978-1-4419-7722-9_5.

Dr. Atefeh Mashatan is an Associate Professor at the Ted Rogers School of Information Technology Management and the founder and director of the Cybersecurity Research Lab at Ryerson University. Mashatan's expertise at the frontlines of the global cybersecurity field was recognized by SC Magazine in 2019, when she was named one of the top five Women of Influence in Security.

Doug Heintzman is a technology strategist with 30 years of experience in enterprise software. He consults with companies around the world on innovation and technology disruption.

Copyright © 2021 held by owner/author. Publication rights licensed to ACM.