EPiC Series in Computing
Volume 84, 2022, Pages 61–71
Proceedings of the Society 5.0 Conference 2022
- Integrating Digital World and Real World
to Resolve Challenges in Business and Society

Post-Quantum Cryptography: An Introductory Overview and Implementation Challenges of Quantum-Resistant Algorithms

Sherdel A. Käppler[1] and Bettina Schneider[1]
[1] University of Applied Sciences and Arts Northwestern Switzerland FHNW
sherdel.kaeppler@students.fhnw.ch, bettina.schneider@fhnw.ch

Abstract

Cryptographic algorithms are an essential measure to ensure confidentiality and integrity of internet communication. The development of quantum computers (QCs) and their potential to utilize Shor's Law, is increasingly recognized as a threat to asymmetric cryptography. In response, post-quantum cryptography (PQC) is gaining prominence as a notable field of research aiming to standardize quantum resistant algorithms before the operational usage of QCs. This paper is addressed to people with preliminary knowledge in the field of cryptography and QC. Based on a literature review, the authors provide an overview of challenges faced by the research community and elaborate the advancements in addressing post-quantum threats. A migration strategy from classical cryptosystems to PQC systems is in development, but obstacles such as time constraints and improper implementation complicate the process. Full implementation could take a decade or more. Until then, our paper aims to create awareness for potential challenges when transitioning towards PQC. As categorization scheme for these potential obstacles, we refer to a well-established model in cybersecurity – the McCumber Cube. Conclusions embrace preparing for risks of improper implementation and deriving a multi-step migration. Special attention is expected to be needed for data migration of existing data sets. As a request for future research in PQC, the authors identified the process of implementing post-cryptography standards, e.g., from the National Institute of Standards and Technology (NIST), and an assessment of the perceived readiness of industry to adapt.

Keywords: Post-Quantum Cryptography, Quantum Computing, Implementation Challenges.

1 Introduction

As digital communication has become the backbone of our business collaboration, secure transmission of data is essential. Cryptographic algorithms employ generated and deciphered codes to

conceal private information from unauthorized access when shared over the internet. Most of these algorithms are based on the difficulty of solving mathematical computations within a limited timeframe (Kumar & Pattnaik, 2020, p. 1). This difficulty varies depending on whether classical computers or Quantum Computers (QCs) are used. In the 1990s, QCs gained public interest through Shor's algorithm (Nannicini, 2020). If executed on a QC, the algorithm could potentially enhance the encryption of cryptographic methods used for communication systems. For instance, algorithms such as RSA, Diffie-Hellman, and Elliptical Curve, take a classical computer hundreds of years to compute but could be solved by a QC in seconds (Mailloux et al., 2016, p.1). With new opportunities in QC on the horizon, researchers recognize that these systems can decipher some of our most used algorithms with ease.

An emerging field of research known as post-quantum cryptography (PQC) is developing new cryptographic systems able to withstand the threat of QCs. In 2015, the National Institute of Standards and Technology (NIST), launched their PQC standardization process to address the issues. It aims to create quantum-resistant public key algorithms (Moody et al., 2020, p. 8). As researchers work to standardize new post-quantum algorithms, the development of QCs is also progressing.

In this paper, the authors review the current state of research in the field of PQC and advocate for increased research into how to accomplish the implementation of algorithms by businesses and industries. We aim to contribute to the elaborating the topic of PQC for an IT management target group. Our work provides insight into the challenges of implementing PQC in business IT.

In doing so, the following research questions are answered:

- Why are our current methods of cryptography vulnerable in a post-quantum world?
- What is the current state of research into ways to alleviate the threats related to PQC?
- What obstacles stand in the way of implementing PQC-related standards?

The remainder of this paper is structured as follows. Section 2 explains the process of the literature review, in particular the key terms used, the inclusion and exclusion criteria, a categorization, and an overview of the review results. Section 3 gives a background of cryptography, QC, and selected cryptographic algorithms. It also brings to light security dilemmas that the public may not be aware of. Next, PQC and related developments in the field are introduced, as well as research involved in addressing post-quantum threats. Shown here is an acknowledgement that teams of researchers are taking the threats related to PQC seriously and are developing solutions. Section 4 discusses implementation and obstacles of post-quantum standardization. This section shows how difficult it will be to accomplish this task, by considering constraints to progress due to limited resources and time. The findings of this section are structured referring to the McCumber Cube. Section 5 provides a synopsis of the results of the research question and lastly, section 6 proposes further research.

2 Literature Research Methodology

2.1 Search Approach

A structured literature search on the topic was conducted using mainly the following databases: IEEE, Elsevier, and Google Scholar. IEEE contains a significant repository of high-quality scientific papers. It also mandates that all papers are peer reviewed before publication and does not seek money from the author to do so. Elsevier was chosen because it is a respected journal with a large database. Google Scholar was chosen for its search engine capabilities. It provided links to full-text pdfs and books, and generated citations based on user preference. Additionally, the reference lists of related papers contributed to finding more credible resources.

The following keywords were used to acquire the relevant knowledge:

'post-quantum cryptography', 'standards', 'migration', 'implementation', 'threat'. These search terms were produced directly from the research questions. Special attention was given to include synonyms, associated words, and Boolean queries within a search.

To establish how best to answer the research questions, criteria for inclusion and exclusion of publications were determined. Article language was restricted to English, and the publication year was limited to 2016 or newer. Dates prior to 2016 were excluded as the information may no longer be relevant. Excluding articles not published in English prevented translation errors, while excluding articles that had not undergone peer review was done to maintain accuracy. Some books and articles not related to the theme of PQC were also used. These resources were needed to develop a research methodology and used in reference to implementations of other technologies.

Identifying relevant literature consisted of multiple searches by topic and keywords on the mentioned search engines. Major contributions to data collection involved peer reviewed articles, published by industry professionals, academics, and government agencies from leading journals. The validity and reliability of the sources found was deferred to the publishers of the articles, who performed peer review. Although many research papers were found, the most relevant to this research were published by the professional association IEEE. The literature search was started 30.09.2021 and last updated 28.02.2022.

Exceptions for the peer-review requirement were made for one report published as draft from the NIST (Barker et al., 2020), and for a blog entry (Schechter 2018) used for the conclusions whose credibility was determined by the author's professional experience.

2.2 Result Categorization

While laying the groundwork for this paper, existing research was divided into two categories. The first category was comprised of articles concentrating on algorithm analysis and testing, with further concentration on the math behind post-quantum algorithms. These papers highlight the current algorithms competing in the NIST Post-Quantum Competition then dissected the robustness of the chosen algorithm or its proof system. The resulting articles involved high levels of linear algebra and were not targeted for novice readers or people from a non-technical background.

The second category grouped articles, which were more descriptive and explanatory. They gave a basic overview of algorithms, then called attention to gathered data, such as the development and timeline of QCs, threats to current algorithms, explanations of adverse effects to today's way of life, and best practices for the implementation of standardization.

What both categories had in common was a desire to appeal to their audiences for further research, while stressing the importance of remedial action. This research benefitted most from utilizing the articles from the second category for answering the research questions.

2.3 Result Overview

One of the most relevant sources for this current research was published by NIST in 2020. It explores the challenges associated with the adoption and use of PQC algorithms and aims to inform of the impact of QC on classical cryptography (Barker et al., 2020, p. 1). The following table provides an overview of the articles taken into consideration for more detailed analysis clustered according to their topic focus.

Topic	Authors
Cryptography	Barker et al., 2020 ; Bobrysheva & Zapechnikov, 2019 ; Kumar & Pattnaik, 2020 ; Mailloux et al., 2016 ; Mavroeidis et al. 2018, Zhang et al., 2019
Quantum computing	Angara et al., 2020 ; Borges et al., 2020 ; Fernández-Carames & Fraga-Lamas, 2020 ; Kumar & Pattnaik, 2020 ; Mailloux et al., 2016 ; Mavroeidis et al. 2018 ; Nannicini, 2020
Post-quantum cryptography	Barker et al., 2020 ; Mailloux et al., 2016 ; Mavroeidis et al. 2018 ; Moody et al., 2020
Post-quantum algorithms	Barker et al., 2020 ; Mailloux et al., 2016 ; Mavroeidis et al. 2018
Post-quantum implementation	Barker et al., 2020 ; Barker et al., 2021 ; Easttom & Butler, 2019 ; Maconachy et al., 2001 ; McCumber, 1991 ; McCumber, 2004 ; Ott & Peikert, 2019 ; Schechter, 2018

Table 1: Article Selection

3 Towards Post-Quantum Cryptography

The purpose of this section is to establish some of the key components of PQC. Section 3 is divided into two parts. First, sub-section 3.1 will provide examples of classical algorithms to demonstrate their relation to Shor's algorithm, while also highlighting the differences between classical computers, classical algorithms, and QCs. Second, sub-section 3.2 discusses the field of PQC and the development of PQ algorithms.

3.1 Cryptography and Quantum Computers

Cryptography can be defined as, "the theoretical basis and core technology of information security, which includes various technologies of encryption and decryption, entity authentication, message authentication, etc." (Zhang et al., 2019, p. 1). Features such as digital signatures, identity authentication, key transport, and privilege authorization processes are commonplace in many industries (Barker et al., 2020, p. 4).

A digital signature, such as the Digital Signature Algorithm (DSA) is an encryption algorithm used in identification and authorization. For instance, when an email is sent from one party to another, a digital signature guarantees that the sender is who they claim to be. Hidden from the user's view, a mathematical function is matching each unique input to an already established stored value. This is referred to as a hash. Hash-based schemes quickly match one-way digital signatures however, if reused they lower security through key exhaustion (Mailloux et al., 2016, p. 5).

Symmetric algorithms, such as the Advanced Encryption Standard (AES), use shared keys and the same algorithm for both encryption and decryption, unlike asymmetric keys, which differ depending on the process (Zhang et al., 2019, p. 1). Two popular asymmetric algorithms are Diffie-Hellman and

RSA. Diffie-Hellman, which is primarily used in key exchange, uses the primitive Discrete Logarithm Problem (DLP), while RSA creates digital signatures through the Integer Factorization Problem (IFP).

In 1994 Peter Shor devised an algorithm that could solve both DLP and IFP efficiently using QCs (Borges et al., 2020, pp. 1-2). He demonstrated that it was possible to break asymmetric algorithms, if a computer was capable of factoring prime numbers quickly. This became known as Shor's algorithm. Given that some of our most utilized algorithms are derived from this design, they are susceptible to breaking from a computer with greater computational ability (Mailloux et al., 2016, p. 1).

To understand the novelty of **QCs**, it is worth understanding the key distinction between classical and QCs. Classical computers operate on binary bits. Each bit holds a unit of information represented by a position of 0 or 1. Therefore, the bits are considered deterministic. (Mailloux et al., 2016, p. 2). Although classical computers can break some public key algorithms, for example Diffie-Hellman and RSA, they need an unreasonable amount of time to do so.

The field of quantum computing, which is responsible for the threat to classical cryptographic algorithms addressed in this paper "[…] was born in the 1980s with seminal contributions from the likes of Richard Feynman, David Deutsch, and many others" (Mailloux et al., 2016, p. 2). Feynman championed the development of the field, which according to Angara (2020) began, "[…] with quantum information theory, computing models, and algorithms" (p. 1).

A QC may perform basic functions comparable to that of a classical computer, such as storing information, data manipulation, interpretation, and retrieval, but with increased speed and precision (Mailloux et al., 2016, p.2). Such that, the technology can fundamentally change how computations are solved and benefit the fields of mathematics, medicine, and science (Angara et al., 2020, p. 1).

QCs are based on the principles of quantum mechanics (Angara et al., 2020, p. 1). More specifically, on the fact that, in quantum mechanics, a unit of information can exist in multiple states simultaneously (Mailloux et al., 2016, p. 3; Mavroeidis et al. 2018). This idea is represented by the qubit or quantum bit, which represents a unit of quantum information. A visual example could be the idea of a coin spinning in motion. At rest, the coin has one of two states, that of heads or tails, but in quantum mechanics the spinning coin may represent two states simultaneously, a so-called superposition (Mailloux et al., 2016, p. 3).

Executing multiple computations simultaneously, on successive stored values, requires an unspecified amount of time for a classical computer (Mailloux et al., 2016, p. 2). In contrast, superposition provides QCs with the ability to complete computations for a multitude of scenarios simultaneously. this enables them to solve complex algorithms within seconds (Mailloux et al., 2016, p. 1).

Considering that classical computers do not possess the computational ability to break algorithms within a reasonable timeframe, it is helpful to understanding how QCs differ. In a QC, thousands of qubits can be held together in a bound state. Thus, performing complex simultaneous calculation on an asymmetric algorithm such as Diffie-Hellman, one can uncover private keys from public keys in a negligible timeframe (Bobrysheva & Zapechnikov, 2019, p. 1).

In hopes of gaining a competitive edge, industries are investing in the technology needed to create QCs. Angara (2020) states, "[…] companies engineered the first real QCs and developed quantum development kits (QDK) such as IBM Qiskit, D-Wave Leap, Microsoft QDK, Google Cirq, Rigetti Forest, or Strawberry Fields" (p.1).

There are no QCs on the market capable of running Shor's algorithm. Instead, specific frameworks with limited processing powers have been tested. Mailloux (2016) states, "[single-purpose quantum mechanical information processors] are designed to execute a single subroutine such as Shor's factoring algorithm or Grover's search algorithm and require extensive classical computing integration to precisely control the quantum phenomena" (p. 2).

By adapting a processor to compute calculations, Google achieved quantum states on 53 qubits. This achievement resulted in the company declaring Quantum Supremacy in 2019 (Mailloux et al.,

2016, p. 1). The experiment demonstrated the capability of an experimental system to solve a problem similarly to that of a fully-fledged QC. In other words, when calculations cannot be easily solved by a classical computer, the technological advantage is called Quantum Supremacy (Borges et al., 2020, p. 1).

There has been no consensus on the completion date of a working QC. Estimates vary considerably between a few decades to non-development (Mailloux et al., 2016, p. 1). Nevertheless, the 2018 Accenture Report postulates a QC capable of running Shor's algorithm by 2028 (Kumar & Pattnaik, 2020, p. 1).

3.2 Post-Quantum Cryptography and Post-Quantum Algorithms

In response to the potential capabilities of QCs, and the danger they could inflict upon established encryption techniques, members of the cryptographic community, along with governmental bodies and industry professionals, are in the process of developing asymmetric algorithms capable of producing, encoding, and decrypting keys.

PQC is a field of research specializing in the creation of cryptographic algorithms robust enough to withstand attacks by a QC (Mailloux et al., 2016, p. 3; Mavroeidis et al. 2018). Once standardized, quantum resistant algorithms will need to replace the currently used public key cryptosystems (Mailloux et al., 2016, p. 3).

In 2016, NIST launched an open competition to the public. The competition entitled "NIST Post-Quantum Cryptography Standardization Process" was created to develop public key post-quantum algorithms resistant to QCs. The chosen algorithms will be used to create cryptographic standards for digital signatures, public key encryptions, and key establishment algorithms (Moody et al., 2020, p. 2).

So-called quantum resistant algorithms include Lattice, Hash and Code based cryptography along with Multivariate, Isogeny, and Symmetric key algorithms. The latter form the basis of the newly developed algorithms in the NIST competition.

Algorithms within the field can be split into two branches, quantum proof systems and PQC. Since not all algorithms are at risk, the first step of incorporation will be to assess which standards are susceptible to attack. Barker (2020) suggests outlining plans for data transfer through, "the identification of critical applications and protocols on both an enterprise and sector-wide basis" (p. 4).

Sixty-nine qualifying algorithms were chosen for the first round of the competition. After undergoing extensive assessment, which included security tests, experiments, cryptanalysis, and performance benchmarks, twenty-six algorithms were chosen for the second round of competition (Moody et al., 2020, pp. 4, 32). The third-round finalists who will be considered for standardization (see table 2), include four public-key encryption and key-establishment algorithms and three digital signature algorithms. Eight alternative algorithms are also being considered for standardization (Moody et al., 2020, pp. 2-7).

The public-key encryption and key-establishment algorithm, "Classic McEliece" and the digital signature, "Rainbow" are the only two of the seven algorithms not based on a structured lattice scheme. NIST will limit its final choice for standardization to only two of the remaining five algorithms and begin the standardization process in the beginning of 2022 (Moody et al., 2020, pp. 25-26).

Public-key Encryption and Key Establishment Algorithms	Digital Signatures	Alternate Candidate Algorithms
Classic McEliece	CRYSTALS-DILITHIUM	BIKE
CRYSTALS-KYBER	FALCON	FrodoKEM,
NTRU	Rainbow	HQC
SABER		NTRU
		Prime
		SIKE
		GeMSS
		Picnic

Table 2: NIST PQC Standardization Process 3rd Round Candidates (Moody et al. 2020)

4 Implementation of Post-Quantum Cryptography

In this section three challenges to the implementation of PQC will be discussed: the difficulty of data migration, the risk of improper implementation and the lengthy timeframe needed for it. As structuring element, we will refer to the McCumber Cube, which will be introduced as prerequisite in the following section.

4.1 Background on McCumber Cube

The McCumber Cube is a model for assessing and managing risks in IT systems created by John McCumber in 1991 (McCumber, 1991). Until 2004, it has been enhanced to a comprehensive, risk-driven methodology (McCumber, 2004), and has since then evolved into one of the best-known approaches in information systems security. The model starts out from the traditional CIA triangle (**c**onfidentiality, **i**ntegrity, and **a**vailability) and expands it by two more dimensions. One of these additional perspectives is the state of data – in transit, in use, or at rest. The other perspective concerns the areas of security controls – by policies, by technology, or by education. Figure 1 shows a visualization of the described approach. By creating a multi-dimensional model, the McCumber cube facilitates a holistic view of security in IT systems (Easttom & Butler, 2019). It has been applied to various contexts (e.g., software development, product assessment, security program building), and due to its popularity, the model has undergone several adaptations and enhancements in academia (e.g., Maconachy et al., 2001; Easttom & Butler, 2019).

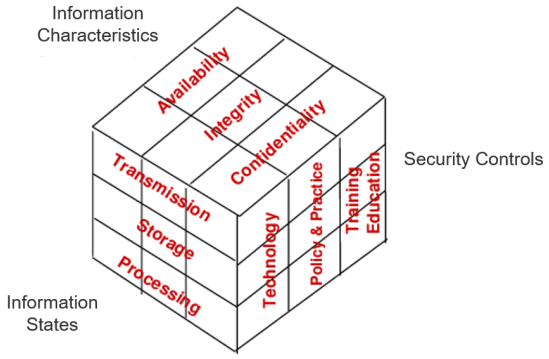

Figure 1: McCumber Cube (adapted from Maconachy et al., 2001)

For the introductory level of this study, the authors stick to the original McCumber Cube model to reflect on the challenges of transitioning IT systems to PQC.

4.2 Problems to the Implementation of Post-Quantum Cryptography

Referring to the previous section, cryptography is one baseline mechanism of cybersecurity and supports multiple **information characteristics** – it enables first confidentiality by transforming data into ciphertext; second, it supports integrity mechanisms by services such as digital signature schemes. However, these properties can only be ensured if the cryptographic schemes are properly implemented. Improper implementation is an obstacle that challenges the adoption as "many information systems lack crypto agility - that is, they are not designed to encourage support of rapid adaptations of new cryptographic primitives and algorithms without making significant changes to the system's infrastructure" (Barker et al., 2020, p. 1). In other words, some industries may not have access to the knowledge needed in support of the change.

When changing the perspective to the **information states**, it then becomes apparent that PQCs are not only to be considered for securing data transfers via the internet (data in transfer) but are equally important in processing digital information in main memory (data in use). Moreover, any organization needs to have transparency of its sensitive data on storage devices (data at rest). NIST acknowledges that migrating existing data (data at rest) is a multifaceted challenge that will require the knowledge and involvement of multiple members of the cryptographic community. To prepare for this challenge, virtual workshops have been held to discuss the development of an implementation strategy. In partnership with the National Cybersecurity Center of Excellence (NCCoE), a data migration playbook will be deployed. In addition, reports, such as white papers will provide continued information. Active participation is encouraged and can be obtained by joining the Applied Cryptography Community of Interest[*] (Barker et al., 2020, p. 6).

If PQC standards are not implemented before the onset of QCs, not only will current information be at risk of exposure, but all recorded and stored data will similarly be threatened. For example, most industries must abide by legal archiving requirements for multiple years. Another compounding factor involves the need of technology to be readily shared within industries, such as the use of email. Both archiving requirements and technological interoperability create weak points in data systems (Barker et al., 2020, p. 2).

Looking at the third perspective, there are different areas of **security controls**. Technology, and hence IT products incorporating PQC algorithms, are only one aspect. A broader view shows additional aspects such as appropriate organizational policies guiding decisions on IT product or service purchases. In addition, IT personnel in organizations need to be appropriately trained on the technology change.

On a general view, implementation of PQC might also be hindered by the lengthy timeframe needed to migrate multiple legacy algorithms to new post-quantum algorithms, and the financial cost of such a disruption. Each cryptographic system serves a specific set of functions. Once standardization is finalized, new algorithms will be used for public-key encryptions, key-establishments, and digital signatures. Since it is not possible to predict all the changes QCs will bring about, additional resources may be used to accommodate differing and new application standards (Barker et al., 2020, p. 3). Barker (2020) advises that, "[…] in the best case, 5 to 15 or more years will elapse after the publication of cryptographic standards before a full implementation of those standards is completed" (p. 2). However, due to the complexity of post-quantum standardization, it is presumably the case that implementation will differ from the initial rollout of classical cryptography. Barker emphasizes that without proper planning implementation could last decades (Barker et al., 2020, p. 3). While proper implementation may help to mitigate risks, unforeseen defects in newly standardized PQC algorithms may be difficult to assess without large scale testing in real-world scenarios.

[*] https://www.nccoe.nist.gov/events/virtual-workshop-considerations-migrating-post-quantum-cryptographic-algorithms

Lastly, Ott (2019) brings forward the notion that some systems will have to, "[...] remain interoperable with other systems during the period of massive industry migration" (p. 8). This further complicates the migration process but may be addressed by creating multiple migration schemes. The first with hybrid classical and post-quantum algorithms before the complete migration to full PQC (Ott & Peikert, 2019, p. 8).

5 Conclusions

In line with the research questions the authors have shown, why current methods of cryptography are vulnerable in a PQ world, have summarized the current state of research into ways to alleviate the threats related to PQC, and have given an outlook on the obstacles standing in the way of implementing PQC-related standards.

Why are our current methods of cryptography vulnerable in a post-quantum world? While dependence on public key algorithms keep data safe, the development of quantum computers and their potential to utilize Shor's Law, is increasingly recognized as a threat in the field of information security (Fernández-Carames & Fraga-Lamas, 2020, p. 1). QC – even though offering immense opportunity – poses significant new hazards to business entities. To meet this threat, both quantum resistant algorithms and the corresponding implementation strategies must be developed simultaneously. The authors argue that, while the former has garnered sufficient attention in the cryptographic community, the latter has not.

What is the current state of research into ways to alleviate the threats related to PQC? Various members of the cryptographic community are currently working on or researching ways to alleviate the threats related to PQC, such as NIST and other affiliated organizations. Most researchers have contributed through the creation and assessment of post-quantum algorithms, while research in furthering the rollout of standardization implementation has received less attention.

What obstacles stand in the way of implementing PQC-related standards? The risk of improper implementation, limited time, financial costs, and the lack of an equivalent undertaking are thus some of the challenges to implementing PQC standards.

Research within the field of PQC is progressing. Seven public key and digital signature algorithms are being considered for industry standardization. However, due to the complexity of algorithm migration, these post-quantum cryptosystems will take decades to implement. According to Barker (2020), "[…] the identification of affected standards by standards developing organizations (SDOs) and consortia, and the identification of critical applications and protocols on both an enterprise and sector-wide basis", are the initial steps of assessing "[…] where migration to post-quantum cryptography will be required." (p. 4). Standards organizations such as the Internet Engineering Task Force [IETF] should identify insecure standards then develop a rollout strategy based on priority. Another suggestion is a pre-emptive critical protocol guideline based on the algorithm classes of the NIST candidate algorithms.

For example, a lattice-based guideline would represent five of the current candidate algorithms. The development of QCs before wide-scale PQC implementation, as demonstrated by Shor's law, is of increasing concern to data security. Thus, this level of threat calls for Immediate action (Barker et al., 2021, pp. 4 - 6).

6 Outlook

The results of this paper are intended to serve as a guideline for investigation and should be used as a basis for further research. This study follows a qualitative literature review approach to elaborate the current developments in PQC. The quantity of research papers used was constrained by facets of

language, publication year and relevancy to the research questions. It resulted in an overview of recently published works which pertains to an emergent and specialized segment of research.

Although creating an implementation strategy should ideally be prepared along-side the development of quantum resistant algorithms, the cryptographic community has contributed limited research into the process of standardization implementation. NIST plans to begin standardization in 2022 yet predicts the arrival of the first fully fledged QC in the 2030s. This leaves less than a decade to develop a proper rollout strategy. An enhancement to this paper would be to further address the challenges of standardization implementation in future research. The following question can be a benefit to further research:

How can previous experience with the introduction of new security standards inform the strategy of implementing PQC standards?

For instance, when secure transmission was introduced to webservers implementation was slow to be achieved. With the release of Google's web browser, Chrome 68, a feature was added to mark all HTTP sites as "not secure" (Schechter, 2018). At that time HTTPS had been formally specified for 18 years, yet website owners had not taken the initiative to transition from HTTP to HTTPS, despite its security advantages. This gap in introduction to implementation is emblematic of the challenges faced when adapting to a new security risk. Studying processes like these will help to improve implementation strategies in the future.

To achieve an understanding of how the public will react to the changes brought on by post-quantum implementation, we believe that answering why some people are slow to adapt to new technologies, would be a helpful strategy to further the research needed on standardization implementation. To do so, an experimental study could be created that incorporated randomly assigned participants into groups were their behaviors could be monitored. Identifying how the groups respond to learning about the threats of PQC and their subsequent willingness to protect their data could be observed. Next an analysis of what obstacles would prevent them from moving forward could be studied. The aim of this research would be to estimate the likelihood of PQC implementation in the public. It could also reveal which strategies are the most effective in informing the public about PQC implementation.

References

Angara, P. P., Stege, U., & MacLean, A. (2020, October). Quantum Computing for High-School Students An Experience Report. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE) (pp. 323-329). IEEE.

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. The Publications of NIST Cyber Security White Paper (DRAFT), CSRC, NIST, GOV, 26.

Barker, W., Souppaya, M., & Newhouse, W. (2021). Migration to Post-Quantum Cryptography. NIST National Institute of, Standards and Technology and National Cybersecurity, Center of Excellence, 1-15.

Bobrysheva, J., & Zapechnikov, S. (2019, January). Post-quantum security of communication and messaging protocols: achievements, challenges and new perspectives. In 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus) (pp. 1803-1806). IEEE.

Borges, F., Reis, P. R., & Pereira, D. (2020). A comparison of security and its performance for key agreements in post-quantum cryptography. IEEE Access, 8, 142413-142422.

Easttom, C., & Butler, W. (2019, January). A modified McCumber cube as a basis for a taxonomy of cyber attacks. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0943-0949). IEEE.

Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE access, 8, 21091-21116.

Kumar, M., & Pattnaik, P. (2020, September). Post Quantum Cryptography (PQC)-An overview. In 2020 IEEE High Performance Extreme Computing Conference (HPEC) (pp. 1-9). IEEE.

Maconachy, W. V., Schou, C. D., Ragsdale, D., & Welch, D. (2001, June). A model for information assurance: An integrated approach. In Proceedings of the 2001 IEEE workshop on information assurance and security (Vol. 310, pp. 5-6). United States Military Academy, West Point. IEEE.

Mailloux, L. O., Lewis II, C. D., Riggs, C., & Grimaila, M. R. (2016). Post-quantum cryptography: what advancements in quantum computing mean for it professionals. IT Professional, 18(5), 42-47.

Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.

McCumber, J. (1991, October). Information systems security: A comprehensive model. In Proceedings of the 14th National Computer Security Conference (pp. 328-337). Baltimore, Maryland, USA: National Institute of Standards and Technology.

McCumber, J. (2004). Assessing and managing security risk in IT systems: A structured methodology. Auerbach Publications.

Moody, D., Alagic, G., Apon, D. C., Cooper, D. A., Dang, Q. H., Kelsey, J. M., ... & Alperin-Sheriff, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process.

Nannicini, G. (2020). An introduction to quantum computing, without the physics. SIAM Review, 62(4), 936-981.

Ott, D., & Peikert, C. (2019). Identifying research challenges in post quantum cryptography migration and cryptographic agility. arXiv preprint arXiv:1909.07353.

Schechter, E. (2018, February 8). A secure web is here to stay. Chromium Blog. https://blog.chromium.org/2018/02/a-secure-web-is-here-to-, last accessed 2022/12/29.

Zhang, H., Ji, Z., Wang, H., & Wu, W. (2019). Survey on quantum information security. China Communications, 16(10), 1-36.