International Journal of Research in Engineering, Science and Management
Volume 6, Issue 1, January 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Quantum Computing Posing a Challenge to the Businesses

Vikalp Nagori[1*], Vijayakumar Varadarajan[2]
[1]DBA Student, Swiss School of Business Management, Bangalore, India
[2]Adjunct Professor, University of New South Wales, Sydney, Australia

***Abstract*: With the development in Quantum Computing, the current strength of public key cryptography is challenged. Large-scale Quantum computers will be able to break many of the public-key cryptosystems currently in use and it would threaten the confidentiality and integrity of digital communications on the public networks. The literature review studies the hypothesis based on which it is predicted that Quantum Computing will challenge current use of public key cryptography. The review also analyzes research by NIST, and several other researchers to analyze the impact of Quantum Computing to cryptography in use by businesses, time it may take to break the current strength of cryptography and what business should do to protect data. The literature review concludes with recommendations for the businesses on approach and transition from current cryptography to Quantum safe cryptography.**

***Keywords*: Cryptography, Quantum, Quantum safe.**

1. Introduction

Cryptography is the most important element leveraged by all the security systems to protect confidentiality and integrity of data.

The transmission of data and key exchanges relies on public key cryptography that is expected to break as Quantum computing scales. We are in a race against time to deploy Quantum resistant cryptography before Quantum computers are in the hands of adversaries. Communications over public network including the communication by IoT devices uses PKI for security. Quantum computing may break the cryptographic methods used in securing the communication. With quantum-safe cryptography, the IoT devices and communications can be made resilient to the attacks leveraging Quantum computing.

This literature review article reviews Shor's algorithm and hypothesis that suggests Quantum computers will break cryptography based on finding prime factors of an integer. The review includes current state of NIST (National Institute of Standards and Technology) project on likely availability of the Quantum resistant algorithms

The paper reviews the current state of maturity in the businesses on deployment and implementation of cryptography especially the small and medium sized businesses. With the current state of maturity in cryptography deployment and crypto agility being a relatively new subject for the businesses, the transition from classic cryptography to the Quantum safe cryptography would be humongous challenge and businesses should start preparing for this transition.

2. Literature Review

A. Demystifying Shore's Algorithm

RSA algorithm assumes that factoring large integers is computationally intractable. As far as it is known, this assumption is valid for classical (non-Quantum) computers; no classical algorithm is known that can factor integers in polynomial time. However, Shor's algorithm shows that factoring integers is efficient on an ideal Quantum computer, so it may be feasible to defeat RSA by constructing a large Quantum computer. It was also a powerful motivator for the design and construction of Quantum computers, and for the study of new Quantum-computer algorithms. It has also facilitated research on new cryptosystems that are secure from Quantum computers, collectively called post-Quantum cryptography [1]. In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3x5, using an NMR implementation of a Quantum computer with 7 qubits. In 2012, the factorization of 21 was achieved, setting the record for the largest integer factored with Shor's algorithm.

If a Quantum computer with a sufficient number of qubits could operate without succumbing to Quantum noise and other Quantum-decoherence phenomena, then Shor's algorithm could be used to break public-key cryptography schemes, such as:

- The RSA scheme
- The Finite Field Diffie-Hellman key exchange
- The Elliptic Curve Diffie-Hellman key exchange

After referring Shor's algorithm and research by IBM and others, the direction of the literature review is to evaluate strength of Quantum Computing and timeline it may take to break current popularly used cryptography schemes.

Quantum mechanics, describes the behavior of very small particles, provides the basis for a new paradigm of computing called Quantum Computing (QC). It was proposed to improve computational modeling of the behavior of very small ("quantum") physical systems [2].

A classical computer uses bits to represent the values it is operating on, but a quantum computer uses quantum bits, or qubits. A bit can either be 0 or 1, while a qubit can represent the

*Corresponding author: vikalp@2pqc.tech

values 0 or 1, or some combination of both at the same time (known as a "superposition"). When qubits are linked, the interference between their wave-like quantum states to perform calculations can be exploited that might otherwise take millions of years.

B. Why Building and Using Quantum Computer is a Challenge?

Creating and making use of quantum computers (QCs) brings a new set of challenges. They use a different set of operations than those of classical computers, requiring new algorithms, software, control technologies, and hardware abstractions. Developing a Quantum ecosystem requires new kinds of algorithm design principles and also debugging as current methods of debugging are based on memory or machine state that would not help.

Developing a Quantum computer that executes Shor's algorithm to find the private key in RSA encrypted message requires building a machine that is multiple orders of magnitude larger and with capability to handle error rate better than currently available. The software development environment on the Quantum computers is still developing. There is significant progress required from current capability to break the currently used reasonable strength of public key cryptography.

At the current state of quantum computing and looking at the progress, it is highly unexpected that a quantum computer can compromise RSA 2048 bits which is popularly used, in couple of years as of 2022.

C. What is Post Quantum Cryptography? What Could be the Impact to Businesses in Protecting Confidentiality and Integrity of Data?

Post-Quantum cryptography is an area of cryptography in which systems are studied under the security assumption that the attacker has a Quantum computer. This attack model is interesting because Shor has shown a Quantum algorithm that breaks RSA, ECC, and finite field discrete logarithms in polynomial time. This means that in this model all commonly used public-key systems are no longer secure. Symmetric cryptography is also affected but significantly less [3]. At this moment the Quantum computers that exist are not large enough to pose a threat against current cryptography. However, rolling out new cryptographic systems takes a lot of time and effort, and it is thus important to have replacements in place well before large, powerful Quantum computers exist. What makes matters worse is that any ciphertext intercepted by an attacker today can be decrypted by the attacker as soon as they have access to a large Quantum computer. This means that any data encrypted using any of the standard public-key systems today will need to be considered compromised once a Quantum computer exists and there is no way to protect it retroactively, because a copy of the ciphertext is in the hands of the attacker. This means that data that needs to remain confidential after the arrival of Quantum computers need to be encrypted with alternative means. Signatures can be updated, and old keys can be revoked when a signature system is broken. On top of that, one important use case for signatures is operating-system upgrades. If a post-Quantum signature system is not in place by the time an attacker has a Quantum computer, then the attacker can take control of the operating system through a fake upgrade and prevent any future upgrades from fixing the problem [3].

This research suggests that post Quantum signature system should be in place before the large Quantum computer is released and gets to the hands of adversaries. With this, we infer that business shouldn't wait for Quantum computer to mature for commercial usage as by then Quantum computer will pose risk to the current encrypted data and operating system and software updates.

Present cryptographic algorithms and protocols such as RSA, DSA, DH, ECDSA, ECDH are under threat of Quantum computing. To protect the collapse of present cryptographic systems, there is a need to develop Quantum resistant cryptographic algorithms, protocols and signatures such as BB84 key distribution protocol, E91 key distribution protocol, lattice based signature, Multivariate Quadratic signature, Hash-based signature etc. The major challenge in Post-Quantum cryptography is the practical implementation of Quantum protocols and Quantum signatures algorithms [4].

In agreement to the researchers, further explored the status of development of Quantum resistant public-key algorithms at NIST [5]. NIST has initiated a process to solicit, evaluate, and standardize one or more Quantum-resistant public-key cryptographic algorithms. The most up to date status on the project is available [5].

Most algorithms on which we depend are used worldwide in components of many different communications, processing, and storage systems. 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. As a result, an organization may not possess complete control over its cryptographic mechanisms and processes so that it can make accurate alterations to them without involving intense manual effort. As a general rule, cryptographic algorithms cannot be replaced until all components of a system are prepared to process the replacement. Updates to protocols, schemes, and infrastructures often must be implemented when introducing new cryptographic algorithms. Consequently, algorithm replacement can be extremely disruptive and often takes decades to complete.

Continued progress in the development of Quantum computing foreshadows a particularly disruptive cryptographic transition. The implementation of post-Quantum public-key standards is likely to be more problematic than the introduction of new classical cryptographic algorithms. In the absence of significant implementation planning, it may be decades before the community replaces most of the vulnerable public-key systems currently in use [6].

In absolute agreement with the research, the transition to Quantum resistant algorithms will be long and challenging as it would require replacing cryptographic libraries, implementation tools, hardware that accelerates cryptographic performance, application and communication devices etc. It would require significant planning, effort in transitioning from

the current landscape to the future ready cryptographic ecosystem. The effort is so significant that businesses would require investment in preparation for the transition and technology refresh. It gets complicated with the interdependencies with 3rd party provided products and services.

D. Current status of Post Quantum Cryptography Standardization

Considering the use cases and evaluation criteria including security, performance and cost, NIST has selected four of the third-round candidates for standardization [7]. Refer Table 1.

Table 1
List of shortlisted algorithms

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS+

This announcement is major step towards standardization, evaluation and development of migration/implementation approach towards Post Quantum Cryptography.

E. State of Cryptographic Maturity at Present

A02:2021 – Cryptographic Failures [8], is the 2nd most severe vulnerability due to the failures related to cryptography (or lack thereof). Which often lead to exposure of sensitive data. OWASP collects data from organizations that are testing vendors by trade, bug bounty vendors, and organizations that contribute internal testing data. Once OWASP has the data, it performs a fundamental analysis of what Common Weakness Enumeration (CWEs) map to risk categories. On selection of top ten vulnerabilities, OWASP applies generalized factors for exploitability and impact to help rank in a risk based order.

The cryptographic failures appearing as the top 2 vulnerability shows the maturity (or immaturity) of the businesses in cryptography to protect sensitive data. Some of the current problems identified as per OWASP are following:

- Old or weak cryptographic algorithms or protocols are used either by default or in older code.
- Default crypto keys are in use, weak crypto keys are generated or re-used. A proper key management solution is not used that leads no rotation of keys.
- Crypto keys added into source code.
- Appropriate randomness is not used for cryptographic purposes.
- Passwords are used as cryptographic keys.
- Deprecated hash functions such as MD5 or SHA1 are in use, or are non-cryptographic hash functions used when cryptographic hash functions are needed.
- Deprecated cryptographic padding methods such as PKCS number 1 v1.5 are in use.

The business has seen several challenges when Heartbleed bug was disclosed in OpenSSL cryptographic software library. Reasonably mature businesses took few months based on rigorous program to remediate the risk however, smaller businesses had taken a long time to fix the bug or remediate the risk.

The businesses have these challenges due lack of understanding on cryptographic usage by the developers and implementors of servers, network and applications. This is evident from the OWASP vulnerability ranking and the typical cryptographic issues observed.

With the current state of maturity in cryptography deployment and configuration, talent shortage, the transition from classic cryptography to the Quantum safe cryptography would be humongous challenge and businesses should start preparing for this transition.

3. Discussion

As NIST has communicated timeline to release standards on Quantum resistant cryptographic algorithms by 2024 and Open Quantum Safe project already started benchmarking the algorithms in OpenSSL, it's time for businesses to plan and prepare for the transition.

Referencing the research papers and updates at the NIST website on the progress in selecting and standardizing Quantum resistant algorithms, its going to be a large engagement in the business to plan and prepare for the transition from current cryptographic ecosystem to the Quantum resistant ecosystem that includes applications, libraries, hardware, networks and 3rd party products and services. Though importance of transition and challenge in transition is highlighted on the research papers however, researchers have not researched and recommended what may be a potential approach for a business to start planning and start a program on the transition. Though it may take few years (by 2024) for availability of standardized Quantum resistant cryptographic algorithms, businesses shall start planning by inventorying their current cryptographic usage, applications and priority for the transition. Business shall also identify with their transition what may be the impact on their B2B, B2C and C2C ecosystem. In absence of such planning and preparation, businesses may feel like Y2K (Year 2000) kind of situation where businesses may be disrupted one day.

4. Conclusions

Its not all doom and gloom or a situation. For business to avoid getting overwhelmed by the release of Quantum resistant cryptography and development of powerful Quantum computers, businesses shall start planning for the cryptographic transition that is coming in few years. If businesses do not start now, their supplier and customer would start asking for it as public key cryptography is leveraged between B2B, B2C and C2C.

Several researchers have highlighted the importance of transition to Quantum resistant cryptography and evaluating the progress made by the NIST Post Quantum Cryptography (PQC). Research and recommendations are required for an approach on transition planning that will be different for each organization based on business, complexity and reliance on 3rd parties for technology. Research shall be performed on understanding what is the awareness on post Quantum Era in

the businesses and are the businesses aware of the transition coming in few years. Also, what may be the transition approach for a business to prepare and prioritize for the upcoming large transition and start a program to deploy post Quantum cryptography in the ecosystem.

Data Availability Statement: Data reviewed is available at NIST

https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4#:~:text=PQC%20Standardization,-After%20careful%20consideration&text=NIST%20will%20recommend%20two%20primary,SPHINCS%2B%20will%20also%20be%20standardized (Accessed on 13th January 2023)

References

[1] Wikipedia on Shor's Algorithm. Available online: https://en.wikipedia.org/wiki/Shor%27s_algorithm (accessed on 6th November 2022).

[2] National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press.

[3] Bernstein DJ, Lange T. Post-quantum cryptography. Nature. 2017;549(7671):188-194.

[4] Pal, O., Jain, M., Murthy, B. and Thakur, V. (2022). Quantum and Post-Quantum Cryptography. *In Cyber Security and Digital Forensics* (eds M.M. Ghonge, S. Pramanik, R. Mangrulkar and D. N. Le).

[5] Post Quantum Cryptography. Available online: https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022 (accessed on 6th November 2022).

[6] William Barker.; William Polk.; Murugiah Souppaya. Getting Ready for Post-Quantum Cryptography. *NIST Cybersecurity White Paper* 2021, pp. 1-4.

[7] PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates. Available online: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4 (accessed on 6th November 2022).

[8] OWASP Top 10. Available online: https://owasp.org/Top10/ (accessed on 6th November 2022).