International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Future of Current Encryption Algorithm in Quantum Computing Age and their Future

Abhishek Shukla

Abstract: ***The advent of quantum computing poses a formidable challenge to the security landscape, particularly in the realm of encryption. Current encryption algorithms, which have safeguarded sensitive data for decades, face unprecedented threats from quantum computers capable of solving complex mathematical problems exponentially faster than classical computers. This essay explores the challenges that quantum computing presents to existing encryption methods, focusing on the vulnerabilities of widely-used schemes like RSA and AES. In response to this quantum threat, the concept of post-quantum cryptography is introduced, encompassing innovative encryption techniques resilient to quantum attacks. Additionally, the notion of quantum-safe encryption is examined, highlighting efforts to develop encryption methods that can withstand quantum adversaries. The essay also underscores the gradual nature of the transition to quantum-resistant encryption and emphasizes the importance of proactive measures for organizations and governments. As we stand on the cusp of the quantum computing age, the future of current encryption algorithms remains uncertain, but it also promises a new era of cryptographic innovation and resilience.***

Keywords: Quantum Computing, Encryption, Cryptography, Quantum-Safe Encryption

1. Introduction

The dawn of quantum computing marks a significant milestone in the ever-advancing realm of technology. They rely on mathematical problems that have proven computationally challenging for classical computers to solve efficiently. These algorithms have been the stalwarts of safeguarding sensitive information across various domains, from the intricacies of financial transactions to the confidentiality of healthcare records, and even in the realm of national security. However, the landscape transforms drastically when quantum computers enter the equation. Quantum computing, rooted in the enigmatic principles of quantum mechanics, possesses the remarkable ability to tackle specific mathematical problems at an exponential speed compared to classical counterparts. Among the myriad challenges posed by quantum computing, one critical threat looms over our current encryption methods: integer factorization [1].

Integer factorization serves as the bedrock of the security of widely-used encryption schemes such as RSA (Rivest–Shamir–Adleman). The RSA algorithm relies on the arduousness of factoring large numbers into their prime components. For classical computers, this process is painstaking and time-consuming. However, Shor's algorithm, a quantum marvel conceived by Peter Shor in 1994, promises to upend this delicate balance. Shor's algorithm showcases the potential to factor large numbers exponentially faster than the most potent classical algorithms. This quantum leap in computational capabilities directly threatens the security of RSA encryption and, by extension, the confidentiality of encrypted communications [2].

Another quantum algorithm, Grover's algorithm, presents a formidable challenge to symmetric key encryption schemes such as the widely adopted Advanced Encryption Standard (AES). Grover's algorithm showcases the power to search through unsorted databases with a quadratic time complexity, whereas classical computers require linear time. This substantial shift in computational efficiency shakes the very foundations of encryption methods that have been regarded as secure for decades [3].

The looming shadow of quantum computing has catalyzed a concerted effort in the domain of post-quantum cryptography. This emergent field seeks to develop encryption algorithms resilient to the disruptive capabilities of quantum computers. The crux of post-quantum cryptography lies in the exploration of mathematical problems that remain insurmountable not only for classical computers but also for quantum adversaries [4].

Various candidates for post-quantum encryption have surfaced, each grounded in distinct mathematical quandaries that quantum algorithms have thus far failed to crack. Lattice-based cryptography, code-based cryptography, and multivariate polynomial cryptography stand among these resilient contenders. Transitioning to post-quantum cryptography, however, necessitates a delicate balancing act between maintaining current security standards and preparing for the impending quantum threat [5].

In anticipation of the quantum computing age, organizations and governments have begun to earnestly consider quantum-safe encryption. Quantum-safe encryption signifies cryptographic methods meticulously designed to withstand the looming quantum threat. This proactive approach involves the deployment of encryption algorithms crafted to remain secure against both classical and quantum adversaries.

Yet, the future of our current encryption algorithms in the quantum computing age remains a complex terrain. While it is evident that these algorithms will face substantial challenges, they are unlikely to become obsolete overnight. Quantum computers capable of dismantling widely-used encryption methods remain in the experimental phase, confronting significant engineering and scalability hurdles. The proactive exploration of post-quantum cryptography and the pursuit of quantum-safe encryption initiatives herald a

Licensed Under Creative Commons Attribution CC BY

future where encryption remains steadfast in the face of quantum supremacy, fostering a new era of cryptographic innovation and resilience [5].

2. Objectives

1) To assess the vulnerabilities of widely-used encryption algorithms such as RSA and AES when faced with quantum computing threats.
2) To explore the landscape of post-quantum cryptography and its potential to provide robust encryption methods resilient to quantum attacks.
3) To analyze the practical challenges and strategies involved in transitioning from current encryption standards to quantum-safe encryption for organizations and governments.

Research Questions

- How do quantum computing capabilities, particularly quantum algorithms like Shor's and Grover's, challenge the security of current encryption algorithms such as RSA and AES?
- What are the key principles and mathematical foundations of post-quantum cryptography, and how do various encryption methods within this field differ in terms of quantum resistance?
- What are the specific challenges organizations and governments face when migrating from existing encryption practices to quantum-safe encryption, and what strategies can facilitate this transition effectively?

3. Literature Review

Challenges to Current Encryption Algorithms

Encryption algorithms, the silent sentinels of the digital world, have been our vanguards of secure communication and data protection for decades. They rely on mathematical problems that have defied efficient computation by classical computers. These algorithms have proven their mettle as they stood sentinel, guarding sensitive information across a myriad of domains. From the intricate web of financial transactions to the sanctity of healthcare records and the imperatives of national security, these algorithms have been unwavering in their commitment to safeguarding our data [3].

However, as quantum computers step into the spotlight, the equilibrium of this cryptographic fortress is poised to shift dramatically. Quantum computing, grounded in the enigmatic principles of quantum mechanics, wields an unprecedented ability to solve specific mathematical problems at an exponential pace compared to their classical counterparts. It is amidst this quantum renaissance that one critical threat emerges like a shadow cast upon our digital sanctuaries: integer factorization [6].

Integer factorization, the foundation of security for widely-used encryption schemes such as RSA (Rivest–Shamir–Adleman), may soon face a reckoning. The RSA algorithm, in all its cryptographic glory, relies on the intricate complexity of factoring large numbers into their prime components. For classical computers, this endeavor is akin to navigating a labyrinthine maze, demanding time and computational resources. Yet, in the quantum realm, a potent disruptor named Shor's algorithm has been unleashed. Conceived by the brilliant mind of Peter Shor in 1994, this quantum marvel promises to unravel the mathematical intricacies of factorization exponentially faster than the most formidable classical algorithms. With this quantum leap in computational prowess, Shor's algorithm casts a direct shadow over the robust security provided by RSA encryption, challenging the very essence of digital privacy and secure communications [2].

But Shor's algorithm is not the sole harbinger of change in this quantum symphony. Enter Grover's algorithm, another quantum virtuoso poised to shake the foundations of symmetric key encryption schemes. In the cryptographic realm, the Advanced Encryption Standard (AES) has long been the guardian of secrets, securing information through the manipulation of symmetric keys. For classical computers, searching through unsorted databases to discover the keys would be a laborious endeavor, demanding linear time and computational resources. Yet, Grover's algorithm, with its quantum prowess, dances through the digital labyrinth with unparalleled grace. It can search through these databases in quadratic time, a feat that classical computers can only dream of achieving. This quantum revolution disrupts the sanctuary of encryption methods that have been regarded as unassailable for decades [1].

The realm of cryptography, once marked by an equilibrium between security and computation, is now fraught with uncertainty. It is in the crucible of quantum supremacy that our trusted encryption algorithms face a daunting adversary. As we journey through this essay, we will delve deeper into these challenges, exploring the vulnerabilities and uncertainties that the quantum era presents [4].

Post-Quantum Cryptography

In the realm of cybersecurity, where the digital battleground is marked by an eternal struggle between attackers and defenders, a new epoch is dawning. This era is defined by the impending advent of quantum computing, a technological advancement that promises to redefine the rules of engagement. As the quantum horizon draws near, the very foundations of encryption, the guardians of our digital secrets, stand at a crossroads. The question that emerges from this shifting landscape is both profound and pressing: What will become of our trusted encryption algorithms in the face of quantum supremacy?

Encryption: The Shield of Digital Secrets

Encryption algorithms, the silent sentinels of the digital world, have been our vanguards of secure communication and data protection for decades. They are built upon mathematical problems so intricate and labyrinthine that classical computers can merely graze their surfaces, unable to penetrate the fortresses of encrypted data. These algorithms have proven their mettle time and again, standing sentinel over sensitive information across a myriad of domains. From the intricate web of financial transactions, where billions of dollars change hands daily, to the sanctity of healthcare records, safeguarding patients' privacy, and the imperatives of national security, where the integrity of

Licensed Under Creative Commons Attribution CC BY

classified information is paramount, encryption has held the line against the relentless tide of cyber threats [5].

The Quantum Revolution: Unveiling Quantum Computers

However, the advent of quantum computing heralds a tectonic shift in this equilibrium. Quantum computers, harnessed through the arcane principles of quantum mechanics, possess a computational prowess that transcends classical limitations. They have the potential to unravel certain mathematical problems at an exponential pace compared to their classical counterparts. In this quantum realm, one critical threat casts a looming shadow over our digital sanctuaries: integer factorization.

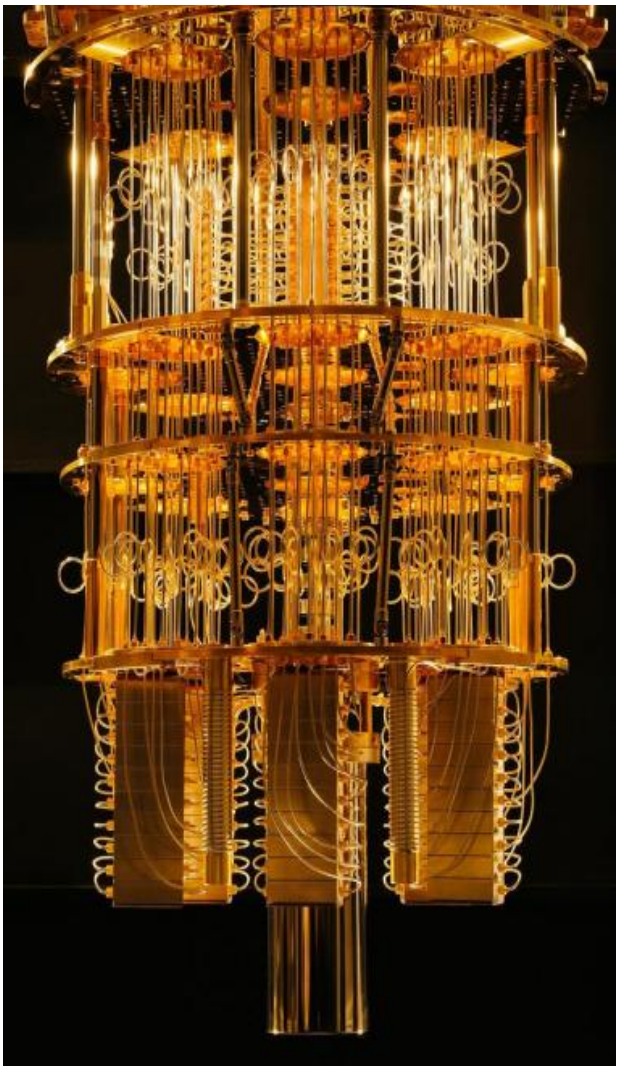

Figure 1: An image of IMB's quantum computer

Integer factorization is the cornerstone of security for widely-used encryption schemes such as RSA (Rivest–Shamir–Adleman). This method relies on the intricate complexity of breaking down large numbers into their prime components, a task that has eluded efficient classical computation for decades. Yet, quantum computing, with its potent disruptor known as Shor's algorithm, threatens to upend this cryptographic bedrock. Conceived by the brilliant mind of Peter Shor in 1994, this quantum marvel promises to untangle the mathematical intricacies of factorization exponentially faster than the most formidable classical algorithms. With this quantum leap in computational prowess, Shor's algorithm casts a direct shadow over the robust security provided by RSA encryption, challenging the very essence of digital privacy and secure communications.

But Shor's algorithm is not the sole harbinger of change in this quantum symphony. Enter Grover's algorithm, another quantum virtuoso poised to shake the foundations of symmetric key encryption schemes. In the cryptographic realm, the Advanced Encryption Standard (AES) has long been the guardian of secrets, securing information through the manipulation of symmetric keys. For classical computers, searching through unsorted databases to discover the keys would be a laborious endeavor, demanding linear time and computational resources. Yet, Grover's algorithm, with its quantum prowess, dances through the digital labyrinth with unparalleled grace. It can search through these databases in quadratic time, a feat that classical computers can only dream of achieving. This quantum revolution disrupts the sanctuary of encryption methods that have been regarded as unassailable for decades [5].

The Diverse Arsenal of Post-Quantum Cryptography

Within the arsenal of post-quantum cryptography lies a diverse array of cryptographic approaches, each fortified against the looming quantum threat. Among the candidates for post-quantum encryption, three stalwarts emerge as frontrunners: lattice-based cryptography, code-based cryptography, and multivariate polynomial cryptography.

Lattice-based cryptography finds its strength in the intricate complexities of lattice problems, mathematical conundrums that have thus far confounded all attempts at efficient classical and quantum solutions. This cryptographic approach leverages the inherent difficulty of lattice problems to create encryption methods that remain quantum-resistant.

Code-based cryptography, on the other hand, seeks refuge in the timeless realm of error-correcting codes. These codes, forged through decades of mathematical ingenuity, offer a fortress of security that quantum algorithms have yet to breach. This approach capitalizes on the formidable challenges posed by decoding these codes, ensuring the resilience of data protected by their embrace [5].

Multivariate polynomial cryptography stands as another bastion in the post-quantum cryptographic landscape. It harnesses the intricate dance of polynomials, transforming mathematical abstraction into robust encryption. The obfuscated relationship between variables in multivariate polynomials creates a cryptographic shield against quantum adversaries [3].

Quantum-Safe Encryption

In anticipation of the quantum computing age, organizations and governments are increasingly considering quantum-safe encryption. Quantum-safe encryption refers to cryptographic methods that are designed to withstand quantum attacks. It involves deploying encryption algorithms that are believed to be secure against both classical and quantum adversaries. The concept of quantum-safe encryption represents a proactive response to an existential threat in the digital realm. As we stand on the brink of the quantum computing age, the imperative to fortify our digital ramparts has never

Licensed Under Creative Commons Attribution CC BY

been clearer. Quantum-safe encryption is the clarion call of the cybersecurity community, a call to arms to ensure the continued sanctity of our digital secrets.

The NIST competition has catalyzed a crucible of innovation in the field of quantum-safe encryption. Cryptographers and mathematicians are engaged in a symphony of intellect, composing encryption algorithms that dance on the precipice of quantum possibility. The algorithms under development span a diverse array of mathematical approaches, each holding the promise of quantum resistance [4].

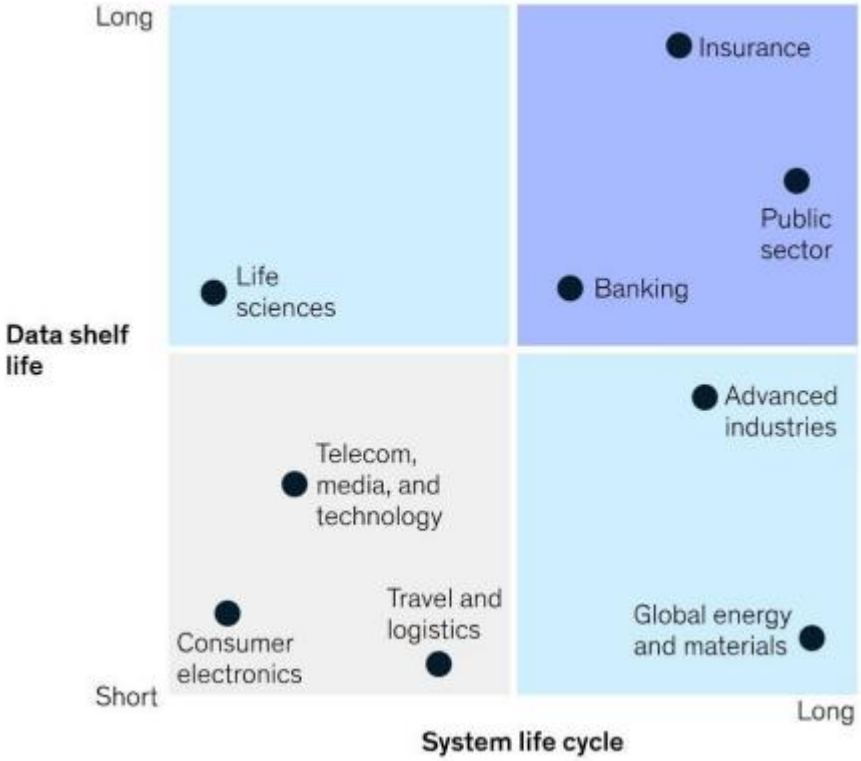

Figure 2: Relative risk from quantum powered attacks by industry

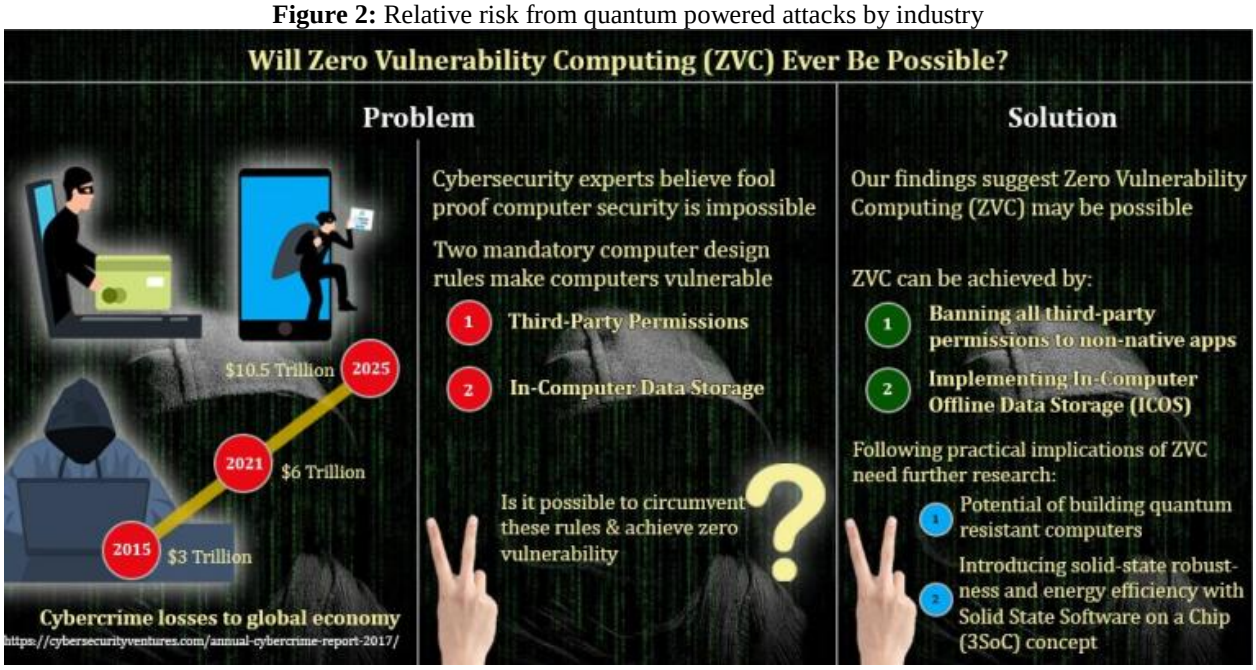

Figure 3: A graphical abstract of Zero Vulnerability Computing

A Delicate Balancing Act

As we navigate the transition to quantum-safe encryption, we find ourselves treading on a tightrope of delicate balance. The urgency of preparing for the quantum threat is palpable, yet the need to ensure a smooth transition for existing systems and infrastructure is equally imperative. Legacy systems, some deeply entrenched in critical operations and infrastructure, rely on existing encryption methods. A sudden shift to quantum-safe encryption is not always feasible, and thus, a phased approach is often necessary. Organizations and governments must meticulously assess their current encryption practices, identifying the systems and data that require immediate quantum-resistant protection [4].

4. Conclusion

Licensed Under Creative Commons Attribution CC BY

As we contemplate the future of our current encryption algorithms in the age of quantum computing, we find ourselves at a crossroads of both uncertainty and transformation. The advent of quantum computing has unveiled unprecedented challenges to the security of our well-established encryption methods. Yet, within this seemingly foreboding landscape, there emerges a glimmer of promise— a new era of quantum-safe encryption and cryptographic innovation. In the crucible of innovation, cryptographers, mathematicians, and computer scientists are forging new cryptographic techniques that defy the might of quantum adversaries. Lattice-based cryptography, code-based cryptography, multivariate polynomial cryptography— these are the building blocks of the quantum-safe encryption methods that promise to secure our digital future.

However, this transition to quantum-safe encryption is not a journey to be taken lightly or hastily. Legacy systems and infrastructure, deeply integrated into critical operations across industries, rely on our current encryption standards. A sudden shift to quantum-safe encryption is neither practical nor feasible in many cases. Hence, a measured and phased approach is imperative. Organizations, governments, and cybersecurity professionals must meticulously assess their current encryption practices, identifying the systems and data that require immediate quantum-resistant protection. In conclusion, the future of current encryption algorithms in the quantum computing age is a testament to the dynamic nature of cybersecurity. It is marked by uncertainty, yes, but it is also illuminated by the beacon of transformation. The age of quantum computing beckons, and the future of encryption hinges on our ability to proactively and thoughtfully navigate this computational revolution. As we do, we carry with us the promise of a digital world safeguarded by the resilience of human innovation.

References

[1] Z. Jin, “Design and Implementation of Full-stack Testing for Web SPA in JavaScript,” 2020, Accessed: Sep. 17, 2023. [Online]. Available: https://aaltodoc.aalto.fi/handle/123456789/46113.
[2] M. Koder, “Increasing Full Stack Development Productivity via Technology Selection,” 2021, Accessed: Sep. 17, 2023. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/509674/Masters_Thesis_Koder.pdf.
[3] S. Liao-Mäkinen, “Developing a full stack mobile application,” 2023, Accessed: Sep. 17, 2023. [Online]. Available: https://www.theseus.fi/handle/10024/795514.
[4] T. Huy, “Build and Deply a High-performance full stack JavaScript Web Application,” 2021, Accessed: Sep. 17, 2023. [Online]. Available: https://www.theseus.fi/handle/10024/400458.
[5] K. An and E. Tilevich, “Catch & release: An approach to debugging distributed full-stack javascript applications,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11496 LNCS, pp. 459–473, 2019, doi: 10.1007/978-3-030-19274-7_32.
[6] R. K. Soni, “The Big Picture of Full Stack Web Development,” *Full Stack AngularJS Java Dev.*, pp. 1–27, 2017, doi: 10.1007/978-1-4842-3198-2_1.
[7] M. Aedma, “Full-Stack Programming with React and ASP. NET: case study in technical knowledge from junior to medior developer,” 2023, Accessed: Sep. 17, 2023. [Online]. Available: https://www.theseus.fi/handle/10024/798042.

Licensed Under Creative Commons Attribution CC BY