Post-Quantum Cryptography

Author

Abdullah Alomari – Haitham Alghamdi

# Introduction

Technological advancement, though, has led to the rapid development and transformation of our lives. It does bring about significant challenges specifically related to security that increase the overall threat. One of these technologies that is said to pose a critical challenge for the future is quantum computing, which provides hackers with a lot of processing power that would allow them to decrypt messages, hack bank accounts, transfer money at will, and spy on corporate networks which would all have a negative impact on trust in digital platforms [1], [2]. Thus, there is a need to ensure safety and security, and the tool that is used for securing communication and data is cryptography, which makes use of codes or algorithms that ensure that only those who have the right key to decrypt the message have access to the final message and this ensures unwanted access [3], [4]. The approach's importance is its advantages, like data integrity achieved through confirming that the data has not been altered in the process, which is crucial if trust is to be maintained. It also develops a mechanism that prevents an entity from denying the authenticity of its messages or documents and provides a secure channel for communication. Considering the complexity and advancement quantum technology provides to possible threat actors, cryptography also needs to evolve to meet these threats, and post-quantum cryptography is an algorithm that is designed in a way to secure the system against any quantum computer-based attack [1]. We first look at how quantum computing works before looking at the workings and capabilities of post-quantum cryptography.

# Quantum computing synopsis

Quantum mechanics are considered critical in governing the behavior of all physical phenomena, and even computers operate under this theory, but they are not quantum computers. A quantum computer would be one that is capable of exploiting a certain special transformation of its internal states. The laws of quantum mechanics allow this peculiar transformation to happen to understand carefully controlled conditions [5], [6]. Within the physical system, it is required to encode the individual logical bits such that there are no physical interactions that are not under the control of the program. All the interactions, even if they are considered irrelevant for classical systems, could have catastrophic disruption capability in quantum computers. This is due to the fundamental basis of the technology, which built on Landauer's observation that all information is, in the end, physical, and the information could be binary 1s and 0s as in classical computers, or it could be recorded through a physical system [7], [8].

This leads to the concept of quantum bit or qubit and the ability, as mentioned, to exist in the state of superposition, which plays a critical role in improving the processing power for specific tasks. Another critical principle in computing technology is entanglement, which is required to enable the qubits to be interconnected to allow one qubit to impact the other regardless of the distance between them [9], [10]. This is critical in improving the computational power and the error connection mechanism. The interference that is developed from the mechanism allows for amplifying the correct computational paths and deleting the incorrect ones, which improves the overall efficiency of the operation. From start to end, these computers are known to manipulate the qubits to perform computation, allowing leveraging the unique properties to process information in ways that traditional computers cannot [11], [12]. These systems need extremely low temperatures and isolation from all external environments to ensure there is no loss of quantum behavior or decoherence, which is extremely difficult. Resolving these issues would allow quantum computing to transform industries like cryptography, drug development, and optimization challenges, and over the years, studies and research have been focused on tackling and looking into different solutions while research also has been increased on the possible impact the quantum computing could have on cybersecurity specifically the cryptography.

# The threat of quantum computing

One of the most popular and widely used encryption algorithms currently is Rivest, Shamir, Adleman (RSA). It is the backbone of the most well-known security infrastructure provided by companies like Nokia and Microsoft [13]. Advanced Encryption Standard, or AES, is employed to provide encryption on the client/server side, similar to web traffic [14], [15]. These algorithms are mathematically based and extremely complex, and the longer the key, the more challenging or difficult it becomes to crack the key and hence make the network more secure. The time taken to crack these algorithms is a lot, which makes them secure with current technologies. The most commonly used cryptography is 256-bit, which means it contains 256 1s and 02, and the quantum technology with its qubits would be capable of cracking an RSA algorithm that is 2048-bit encryption is just eight hours, which highlights the challenge and impact that quantum computer would have [16]. This is enabled by the difference in the use of qubits, which can exist in multiple stages at a given time, as mentioned before, which is also referred to as quantum parallelism, and this increases the speed with which the encryption can be decoded [17].

Most digital infrastructure uses the Secure Sockets Layer (SSL)/ Transport Level Security (TLS) protocol to provide security services that ensure authentication, integrity, and overall confidentiality of the service. The stack is said to be formed using a complex symmetric algorithm that undertakes encryption and generation of MAC codes . Quantum algorithms like Shor’s algorithm would be able to efficiently consider large integers and break the encryption as seen with RSA, which is often used in the key exchange under the protocol. The advancement observed with other algorithms like Grover is said to reduce the theoretical effectiveness of the keys by half, meaning that a 256-bit key would have the security of a 128-bit key. These highlight the critical challenge and why there is increasing research in the field to ensure better protection.

# The Shor’s Algorithm

Shor’s algorithm is said to be one of the most popular in quantum computing and was developed as early as 1994 by Peter Shor. The popularity of the model has been due to the ability of the algorithm to factor numbers exponentially faster than other algorithms while also being able to be used in different applications. Shor’s algorithm would work on factoring numbers where a random integer is selected, provided the integer is smaller than the number to be factored [18], [19], [20]. Let us consider a to be the number and N to be the co-prime. The next stage would be the heart of the algorithm, which focuses on finding the quantum period and is represented using the function [21]:

$f\left(x\right)= a^{x}$ mod N

The above equation uses the quantum Fourier transform, and period r is the smallest positive integer such that the ar =1 mod N. The number or period achieved is used in a way to figure out the factors of the target number, and the pattern found is said to focus on the special property of the numbers that you would be dealing with [21]. In a simple way, instead of using a single key to open a door, the algorithm allows us to quickly narrow down the possible keys that would work even without trying one by one. This algorithm is said to have three major components. The first of these is the classical computation followed by quantum, and in the end, there is classical computation against. In addition, the algorithm is said to have at least four subcomponents, and each of them is critical, with one being the phase estimation as it performs modular arithmetic and is responsible for finding the period of the number to be factored. The other critical subcomponent is the inverse QFT, which would take the quantum result from the modular arithmetic that would precede it and then transform it into classical information that could be retrieved from the quantum circuit by measurement. The capability provided and the working is a threat to existing RSA and other cryptosystems due to the powerful capability in reducing the time and exponential speed of decrypting, which leads to switching towards quantum-resistant algorithms.



Figure 1 Shorr's algorithm process [22]

# Countering quantum threats

Over the years, many techniques under Post Quantum Cryptography (PQC) and Quantum cryptography have developed different cryptography techniques or algorithms that have improved the resistance to quantum threats. PQC, unlike quantum cryptography, does not use any quantum properties based simply on mathematical problems. It focused on avoiding the use of integer factorization and discrete log problems for data encryption. One technique that has been used to counter the threats using PQC is the development of new algorithms using different approaches [23]. The code-based cryptography, for example, makes use of the theory of error-correcting codes and relies on the difficulty of decoding linear codes that would be randomly generated. McEliece's cryptosystem, developed in 1978, is said to be one of the first of this algorithm to be able to withstand cryptanalytic attacks, including quantum attacks [24]. The issue here, though, is that the key size is too large, which makes it hard for regular computing often.



Figure 2 NIST Round 3 Candidates [23]

An isogeny-based code, which is a non-constant map between the elliptic curves, could be represented in the form of polynomials, and this would be compatible with the addition of both curves such that images of the total of the two points from the first curve would equal to the sum of the entire image when it Is computed within the second curve [23]. The Advantage of this system is the smaller key size compared to the other methods, and its variation, like SIIDH, is a key exchange algorithm that improves quantum resistance [25], [26]. The work is based on each party receiving a private key, a secret integer, and the public key being computed based on their private key. The public key would be an elliptical curve developed based on the isogenies. The two parties would exchange their public keys, and then each would use their public keys together along with private keys, which would compute an isogeny to develop a new curve. The issue, thus, is that it is critical for both parties to follow the protocol correctly.

Hash-based cryptography is another approach that uses functions that are mathematical algorithms that convert the input data into a fixed-size string of bytes. This would be primarily used in the creation of digital signatures [23]. The main security fundamental or principle relies on the collision resistance property of the hash function, which is said not to be weakened even under quantum computing. These keys, though, are said to have a larger signature size than their traditional counterparts. Of all the techniques, the most prominent and reliable has been identified is lattice-based cryptography, which is based on mathematical structures that would girds of points that extend infinitely in all directions. There could be a lot of points in the n-dimensional space that are developed using a linear combination of integer coefficients and have n linearly independent vectors [27], [28]. The vectors would be the base of the lattice, and the problem would require finding the point that has specific properties within the structure, like using a short vector problem or a closed vector problem. In the shortest vector problem, the goal would be identifying the non-zero vector in the lattice, which is not simple when the dimensions increase, and the possibility of identifying the shortest vector becomes increasingly challenging. Quantum computers are capable of solving problems that can be broken down into parallel computations as they are capable of processing multiple possibilities at the same time [29]. Lattice problems are high-dimensional spaces that have no simple path that can be identified using parallelism, and no algorithm has been found to reduce the complexity of this approach. Figure 2 provides a list of different algorithms that have been developed under the different schemes.

# Role of NSIT in Quantum-Resistant Cryptography

The National Institute of Standards and Technology (NIST) plays a critical role in developing and standardizing algorithms or technologies to improve quantum-resistance encryption, as they aim to protect digital infrastructure from the complexities and challenges presented by quantum technology. As the agency responsible for governing and guiding the best practices for cybersecurity, NIST is responsible for identifying future risks that could impact the people or corporation and taking measures to counter or mitigate the risks as it deems fit. Understanding the capabilities of the quantum protocols, the NIST initiated a project focused on developing PQC algorithms that would be immune to attacks from quantum computing threats. The goal was to develop different technologies or approaches that would help in improving and preserving the safety and integrity of digital infrastructure while ensuring smooth communication regardless of quantum technology development. In Figure 2, we have listed different approaches that have been developed, which are said to be a result of a multi-year global competition undertaken by NIST to find and standardize the quantum-resistant algorithms. In 2023, it was reported that of all the algorithms, four of them, each having different security protocols, had been chosen for standardization, and this was considered to be the first step towards ensuring safety from quantum threats. One of them was a public-key encapsulation technique, while the other three were digital signature schemes.

## CRYSTAL-Kyber

Key Encapsulation Mechanism (KEM) is said to be a three-algorithm mechanism where there is an algorithm for generating the key pair, an encapsulation algorithm that takes the public key to help with computing a session key and ciphertext, while the decapsulation algorithm takes the ciphertext and private key to develop a session key. Cryptographic Suite for Algebraic Lattices (CRYSTAL)- Kyber is based on lattice-based principles and also involves the hardness of the Learning with Errors (LWE) problem that helps to improve the security of key exchanges. The process would involve generating a pair of keys, with the private being held or remaining secret while the public key is shared. The keys are developed by manipulating the lattices in a way that would make them intertwined with the LWE problem. When the sender wants to establish a secure connection, they would use the public key and create a secret key or encapsulated key, which would allow them to use their private key in decapsulating it and recovering the secret key that would allow both parties to encrypt and decrypt messages which ensure security. Kyber is considered efficient as it does not use too many resources or bandwidth, and the key sizes are often optimized for performance, making it more suitable for many applications.

## CRYSTALS-Dilithium

This is another lattice-based approach, but it focuses on the digital signature, which is required for providing authenticity, integrity verification, and non-repudiation. This, too, works with LWE and its variants and would develop a pair of keys with private keys for signing documents and a public key to verify the signature. Due to the complexity of the lattice problem, it is not traceable, and it improves signature verification as well as flexibility in implementation. In addition, the Dilithium samples often have uniform distribution, and this would avoid the over-complex and inefficient sampling from the Gaussian distribution. The modular structure is also said to help with polynomial multiplication, which is performed in a similar way regardless of the level of security that ensures easy switching between the levels [23].

## FALCON

This is also a signature scheme that is based on the Gentry-Peikert0Vaikuntanathna (GPV) blueprint and makes use of lattice-based signature along with trapdoor functions. For one example, there are instances of developing NTRU lattices with an efficient Gaussian sampler that would develop a secure system when it is assumed that the SIS would be hard in the lattice sued. Falcon is developed in a way that all the calculations can be computed only using efficient Fourier-transform techniques [23]. This algorithm is said to be compact and efficient, and the chosen ring structure, as well as error distribution, helps in the process and partially cancels the negatives from the Gaussian error distortion, which is the reason for the improved performance. One of the drawbacks is the overall complexity involved in understanding the details of construction and implementation.

## SPHINCS+

This is the only hash-based algorithm that has been selected, and it integrated the techniques with other layers of cryptographic techniques that improve security and efficiency. A pair of keys would be generated using the algorithm, and the private key is considered to be the random seed from which the other components of the signature scheme would be derived using a secure hash function [23]. This ensures that backward calculation is not possible. When signing a message, the private key is used to create a unique signature for the message, and it involves creating a one-time signature and then linking it back to the public key through various trees and intermediate keys, which would show that the individual has the key without revealing it. To verify the signature, the verified would send the public key, and the signature would confirm that the message was signed with the corresponding private key. One of the main disadvantages of this would be the size of the signatures and computational overhead, which is common for hash-based methods.

The four chosen algorithms highlight the groundwork done by NIST in promoting PQC and working towards shifting from existing algorithms to systems resistant to quantum computing and its capabilities. To ensure security and advancement, NIST needs to keep emphasizing and working on developing more measures and technological advancements that improve the capabilities and simplify the complexities of the four solutions that were designed.

# Digital Safety in Quantum World

With the growing complexity and challenges presented by quantum computing, the increased focus has led to radical changes in digital security. We have explored the need for new encryption techniques as a result of the complications presented by quantum computing to existing methods, and PQC is just one of the available techniques. Quantum computing-based activities like Quantum Key Distribution (QKD) are considered novel and cutting-edge technologies that would help improve resilience. The QKD based on quantum mechanics can provide a level of security that is theoretically invulnerable to computational and technological advancements, including the advancements in quantum computing [30]. The core principle includes superposition, entanglement, and no-cloning theorem. The theorem is said to state that it would be impossible to create an identical copy of a quantum state that is unknown. These three principles have led to the development of different security protocols like BB84 and E91. Due to its capabilities, the technology has been found to be used more in governmental communication and banking transactions, but the technology still has its limitations due to the photon loss observed in optical fiber.

While the advancements have been rapid, there is an increasing focus on research on developing more quantum-safe encryption techniques, all of which focus on ensuring their ability to withstand the computational power of quantum machines. The PQC-based algorithms are the most promising, but there is also the use of mathematical puzzles that are unsolvable by quantum computers, which allows different ways of data security. The development, though, is not just limited to software or algorithms, as hardware-based solutions like quantum random number generators have been explored to increase the unpredictability of the system. They are based on fundamental indeterministic quantum events that would help ensure unpredictability and use measurement of the system in superposition, entanglement, and photon arrival time to generate the random number.

The technologies are still relatively new, and many challenges hinder the shift to quantum-resistant technologies. These challenges would include the lack of integration with current infrastructure, the lack of standardization, and the algorithmic deployment design. Often, there is a trade-off between performance and security, which needs to be carefully considered, and the new techniques must be effective with minimal negative impact that could impact the system's performance and ensure its security against quantum assaults.

# Advancements in Quantum-safe Encryption

The idea is developed based on the current or recent methods that have been developed to create a safe information flow that does not require the trust of a third party like that seen with quantum concurrent signatures. Even in situations where the participants are known to show a great level of mistrust, the novel procedures are capable of ensuring that communication is secure and fair. Thanks to technological advancement, digital signatures are now able to be exchanged in such a way that they maintain their provisional character until important details regarding the transaction are revealed. This is said to provide evidence of the capability and impartial intent of the technology. Quantum-safe encryption or security is a type of approach that is able to withstand all challenges posed by quantum computing, and at the same time, it does provide a model that shows how digital safety will be transformed in the future.



Figure 3 Quantum Computing Security Opportunities

# Practical Use

PQC has made significant progress in securing digital communication, data storage, and online transactions from possible quantum attacks due to the existing systems' inability to protect against computing capabilities under quantum mechanisms. Moving away from the existing tactics or mathematical approaches and taking a more sophisticated mathematical approach, the PQC is able to fortify digital security and also ensure that the encrypted information remains confidential and tamper-proof. While quantum technology is still in its development phase, the threat of the possibility of the technology being used for attacks has led to the need to develop technologies that could counter quantum computing capabilities, and NIST has led this transition, which has allowed for developing critical communication networks that are safe from eavesdropping and interception. This is critical for diplomatic exchange, corporate communication, and the military, where sensitive information needs to remain secure. PQC-based digital signatures could help ensure the documents remain verifiable, tamper-proof, and authentic. The Finance sector would significantly benefit from the technology as it would improve the security of online transactions and can even be used in the voting process. The advancement in the field would lead to additional applications and capabilities that would help challenge the threats posed by the traditional and quantum computing environment in the future.

# The role of various companies in quantum research

## IBM

Over the years, IBM has been a leader in the field of research in quantum computing and has a critical role to play in advancing both quantum computing and PQC. Their contribution, though, is not limited to just theoretical research but is focused on the development of practical tools and platforms that would help with PQC development. Over the years, IBM has been responsible for developing many algorithms, such as CRYSTALS-Kyber, one of the finalists in the NIST campaign to develop PQC algorithms [31]. In fact, all four finalists discussed in the paper have been developed by IBM researchers or have made significant contributions to the development of the technology [32]. IBM understands the threats posed by quantum computing and has been at the forefront of global efforts in standardizing cryptography and working with industry leaders for standard development.

Another major contribution is the Qiskit SDK, an open-source platform made available by IBM that focuses on developing quantum algorithms, research, and execution. The tool comes with a set of basic primitives and additional functionalities, such as similar applications that allow for using different tests to develop algorithms based on new standards [33], [34]. In PQC, the SDK could help simulate quantum attacks on cryptographic protocols, which would help test the resilience of the developed algorithm and explore the integration of different methods. Technology and IBM have ensured democratization and access to all through developing and keeping the technology open source, which has been critical in advancing our preparedness for changes or transformation.

## Google

Google, too, has been focused on quantum computing and, over the years, has developed and invested considerably in technology, including partnerships with universities and corporations, to advance the technology [35], [36]. Google is said to have achieved the milestone of Quantum Supremacy in 2019, which indicated that quantum computers are able to perform tasks faster than existing supercomputers [37]. The company also played a critical role in exploring Shorr’s algorithm for factoring large numbers that were able to highlight the vulnerabilities of the existing methods.

One tool that Google is famous for is the open-source library known as Cirq, which allows for designing, simulating, and running quantum circuits on simulators and quantum computers. It was developed to allow researchers and developers to work with quantum processors and provide them with the tools that would allow for easy design and simulation and test the capability of new algorithms under quantum swarm attacks under real-world scenarios that ensure their ability and use in the applications. Studies have used Cirq and Qiskit to develop new algorithms and test them under PQC requirements, highlighting the importance of the two tools. [38].

Another tool is Tensor Flow Quantum, which was built in collaboration with Tensor Flow, with the aim of bridging the gap between machine learning and quantum computing. Using this tool provides a researcher with sufficient tools that would help to construct, train, and simulate quantum machine learning models, and it also helps in testing their capability for different applications and possibilities [39]. The system is critical as it helps manipulate the quantum data under different scenarios, which highlights how machine learning models could act in different situations and thus develop new algorithms under PQC to ensure better safety and protection.

## Microsoft

Microsoft has been a pioneer in data security from the beginning due to its operating systems and cloud servers, and the company, with advancements in technology, also played a critical role in making significant contributions towards the growth of PQC. The company focused its work on ensuring that the protocols that exist are in line with the requirements of the changing landscape and work efficiently together, which led to the development of tools like PQC VPN, which is said to be an adaptation of traditional VPN technologies that encrypt and secure data transmission over the network which has been one of the many tools that are quantum-safe under VPNs. Another tool would be the modification of the Transport Layer Security (TLS) protocol to accommodate the PQC requirements with the help of the OpenSSL development platform, which allows for smoother integration of the algorithms into the existing infrastructure. Last but not least is the Post-quantum SSH, which is a secure shell that is a network protocol for operating the network services more securely across unsecured networks. The development of the SSH based on PQC would involve using the integration of the algorithm into the protocol as a way of protecting the threats.

## Juniper

Often, work has been done to integrate PQC with QKD, which would ensure the best of the two worlds. One such work is that of the Juniper Network solution, which has led to the development of Quantum-safe IPsec VPNs that work on both PQC and QKD in which the former provides the algorithms that are resistant to the computing attacks, which is critical for the integrity and safety of the data. On the other hand, the latter is said to provide a secure method for exchanging cryptographic keys, which can use quantum mechanics to detect any attempt of possible interception. The main reason for the capability of using QKD with PQC is because, unlike other quantum computing, QKD does not require high process capability as required for quantum computing cryptography, but it does use the principles of quantum mechanics. The security of QKD is based on the fundamental principles of quantum physics, and these principles are critical in providing the required security that is immune to computation hacking. That said, to use the system, modification would be needed at the endpoints of existing optical fiber communication [40].



Figure 4 Safe IPsec VPNs [41]

# Future innovation and critical investments

The majority of the tech leaders understand that PQC is critical to answering the quantity challenge of quantum computing that might cause significant disruption similar to Y2K with its introduction. The capabilities presented by PQC have been critical in ensuring the safety of data before the onset of quantum computing, which would be able to crack the current cryptographic methods [42]. The increasing concerns about security have also led to an increase in investment by different countries. Some countries like the US and China are focused on preparing themselves to protect the data [43]. This has made significant investments in the field and the development of a new set of protocols and algorithms using the PQC concept. The interest and potential have also led to increased investment from countries across the world, including the Middle East. KAUST and Zapata Computing Inc., which is a leading software company that allows NISQ-based quantum applications, are focused on working together to examine how quantum computing can simulate and optimize the aerodynamic design process of automobiles [44]. This is said to help save time in the process, enable better design, and provide more applications for quantum computing. In addition, it was observed that Saudi Aramco Wa’ed ventures had invested around $100 million in PASQAL, which is a quantum computer start-up company. These showcase the growing interest and growing investment in the field that would certainly accelerate the development and growth of the technology.

# Conclusion

The emergence and continuous advancements of quantum computing are said to be critical catalysts for the accelerated development and implementation of PQC. As investment in the field grows, as well as research, it highlights the pressing need to develop more quantum-resilient systems to ensure that the technology would not disrupt or cause havoc. The current algorithm or cryptographic techniques, which are based on mathematical problems, are said to be simple for quantum computers to decipher, reducing their capability, and this has led to the development which NIST has spearheaded in developing new PQC algorithms that rethink the security and encryption focused on a complex mathematical problem that quantum computers cannot solve by exploiting the existing flaws or it quantum principles which is a double-edged sword. The new algorithms based on lattice-based coding have allowed significant safety and contributed to new applications. The research also saw that IBM, Google, and other companies are working effectively in developing the technologies for quantum computing and PQC. Often, companies like Juniper look to integrate the PQC with Quantum solutions like QKD to develop safe and secure solutions for current use. Overall, we can say PQC would help mitigate the threat posed by quantum computing, but the disruption caused by the change might not be minimal.

# References

[1] L. O. Mailloux, C. D. Lewis, C. Riggs, and M. R. Grimaila, “Post-Quantum Cryptography: What Advancements in Quantum Computing Mean for IT Professionals,” *IT Prof*, vol. 18, no. 5, 2016, doi: 10.1109/MITP.2016.77.

[2] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-Quantum Cryptography*, 2009. doi: 10.1007/978-3-540-88702-7\_1.

[3] M. T. Gençoğlu and M. T. Gençoğlu, “Importance of Cryptography in Information Security,” *Iosr-Jce*, vol. 21, no. 1, 2019.

[4] L. G. De Lazo and Dr. P. V. S. Kumar, “Role and Importance of Cryptography Techniques in Cloud Computing,” *Technoarete Transactions on Internet of Things and Cloud Computing Research*, vol. 2, no. 2, 2022, doi: 10.36647/ttitccr/02.02.art005.

[5] A. Glassner, “An Introduction to Quantum Computing,” in *Proceedings - SIGGRAPH 2023 Courses*, 2023. doi: 10.1145/3587423.3595538.

[6] J. D. Prince, “Quantum Computing: An Introduction,” *Journal of Electronic Resources in Medical Libraries*, vol. 11, no. 3, 2014, doi: 10.1080/15424065.2014.939462.

[7] R. Landauer, “Information is inevitably physical,” in *Feynman and Computation*, 2018. doi: 10.1201/9780429500459.

[8] J. A. Wheeler, “Information, physics, quantum: The search for links,” in *Feynman and Computation*, 2018. doi: 10.1201/9780429500459.

[9] M. A. Nielsen, I. Chuang, and L. K. Grover, “ Quantum Computation and Quantum Information,” *Am J Phys*, vol. 70, no. 5, 2002, doi: 10.1119/1.1463744.

[10] Y. Wang, “Quantum computation and quantum information,” *Statistical Science*, vol. 27, no. 3, 2012, doi: 10.1214/11-STS378.

[11] F. J. Furrer, “Quantum Computing for Everyone,” *Informatik-Spektrum*, vol. 42, no. 5. 2019. doi: 10.1007/s00287-019-01229-3.

[12] C. Bernhardt, *Quantum Computing for Everyone*. 2019. doi: 10.7551/mitpress/11860.001.0001.

[13] M. S. A. Mohamad, R. Din, and J. I. Ahmad, “Research trends review on RSA scheme of asymmetric cryptography techniques,” *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, 2021, doi: 10.11591/eei.v10i1.2493.

[14] M. Nabil, A. A. M. Khalaf, and S. M. Hassan, “Design and implementation of pipelined and parallel AES encryption systems using FPGA,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 20, no. 1, 2020, doi: 10.11591/ijeecs.v20.i1.pp287-299.

[15] N. Aleisa, “A comparison of the 3DES and AES encryption standards,” *International Journal of Security and its Applications*, vol. 9, no. 7, 2015, doi: 10.14257/ijsia.2015.9.7.21.

[16] ULTRA, “Quantum Computing Cyber Threats: Resistant Algorithms Help Prevent the Most Advanced Attacks,” 2021.

[17] A. Vaishnavi and S. Pillai, “Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods,” in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1964/4/042002.

[18] A. G. Fowler, S. J. Devitt, and L. C. L. Hollenberg, “Implementation of shor’s algorithm on a linear nearest neighbour qubit array,” *Quantum Inf Comput*, vol. 4, no. 4, 2004, doi: 10.26421/qic4.4-1.

[19] M. Rossi *et al.*, “Using Shor’s algorithm on near term Quantum computers: a reduced version,” *Quantum Mach Intell*, vol. 4, no. 2, 2022, doi: 10.1007/s42484-022-00072-2.

[20] J. Barzen and F. Leymann, “Continued Fractions and Probability Estimations in Shor’s Algorithm: A Detailed and Self-Contained Treatise,” *AppliedMath*, vol. 2, no. 3, 2022, doi: 10.3390/appliedmath2030023.

[21] T. Moore, “Quantum Computing and Shor’s Algorithm,” 2016.

[22] S. Nagaich and Y. C. Goswami, “Shor’s algorithm for quantum numbers using MATLAB simulator,” in *International Conference on Advanced Computing and Communication Technologies, ACCT*, 2015. doi: 10.1109/ACCT.2015.16.

[23] W. Beullens, J.-P. D’Anvers, A. Hulsing, T. Lange, L. Panny, and N. P. Smart, “POST-QUANTUM CRYPTOGRAPHY Current state and quantum mitigation,” 2021.

[24] H. Gray, C. Battarbee, S. F. Shahandashti, and D. Kahrobaei, “A novel attack on McEliece’s cryptosystem,” *International Journal of Computer Mathematics: Computer Systems Theory*, vol. 8, no. 3, 2023, doi: 10.1080/23799927.2023.2229278.

[25] C. Costello, “B-SIDH: Supersingular Isogeny Diffie-Hellman Using Twisted Torsion,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2020. doi: 10.1007/978-3-030-64834-3\_15.

[26] R. Azarderakhsh *et al.*, “SIKE: Supersingular Isogeny Key Encapsulation,” *NIST proposal*, 2020.

[27] A. Aikata, A. Basso, G. Cassiers, A. C. Mert, and S. S. Roy, “Kavach: Lightweight masking techniques for polynomial arithmetic in lattice-based cryptography,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2023, no. 3, 2023, doi: 10.46586/tches.v2023.i3.366-390.

[28] J. Huang *et al.*, “Improved Plantard Arithmetic for Lattice-based Cryptography,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2022, no. 4, 2022, doi: 10.46586/tches.v2022.i4.614-636.

[29] C. Peikert, “Lattice cryptography for the internet,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 8772, 2014, doi: 10.1007/978-3-319-11659-4\_12.

[30] M. Mehic *et al.*, “Quantum Key Distribution: A Networking Perspective,” *ACM Comput Surv*, vol. 53, no. 5, 2020, doi: 10.1145/3402192.

[31] IBM, “Quantum-safe Cryptography Algorithms,” IBM. Accessed: Apr. 02, 2024. [Online]. Available: https://research.ibm.com/projects/quantum-safe-cryptography

[32] IBM, “Embracing Our Quantum Future,” IBM. Accessed: Apr. 02, 2024. [Online]. Available: https://www.ibm.com/policy/quantum-future/

[33] K. Das and A. Sadhu, “Experimental study on the quantum search algorithm over structured datasets using IBMQ experience,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, 2022, doi: 10.1016/j.jksuci.2022.01.012.

[34] Pennylane, “What is Qiskit? ,” Pennylane.ai. Accessed: Apr. 02, 2024. [Online]. Available: https://pennylane.ai/qml/glossary/what-is-qiskit/

[35] Google, “Building scalable quantum systems,” Google Quantum AI. Accessed: Apr. 02, 2024. [Online]. Available: https://quantumai.google/quantumcomputer#:~:text=We%20develop%20the%20necessary%20calibration,for%20near-term%20quantum%20computers.

[36] C. Chou and H. Neven, “A quantum computing partnership with the University of Chicago and the University of Tokyo,” Google Keyword. Accessed: Apr. 02, 2024. [Online]. Available: https://blog.google/technology/ai/quantum-computing-partnership-chicago-tokyo-universities/

[37] E. Gibney, “Hello quantum world! Google publishes landmark quantum supremacy claim,” *Nature*, vol. 574, no. 7779. 2019. doi: 10.1038/d41586-019-03213-z.

[38] S. Pattanayak, *Quantum Machine Learning with Python: Using Cirq from Google Research and IBM Qiskit*. 2021. doi: 10.1007/978-1-4842-6522-2.

[39] Tensor Flow, “TensorFlow Quantum,” Tensor Flow. Accessed: Apr. 02, 2024. [Online]. Available: https://www.tensorflow.org/quantum/overview

[40] J. Lai *et al.*, “Application and Development of QKD-Based Quantum Secure Communication,” *Entropy*, vol. 25, no. 4. 2023. doi: 10.3390/e25040627.

[41] M. Aelmans *et al.*, “DAY ONE: QUANTUM-SAFE IPSEC VPNs,” 2023. [Online]. Available: www.juniper.net/dayone.

[42] B. K. Williams, “Preparing for Y2Q and Post-Quantum Disruption,” Wilson Center. Accessed: Apr. 02, 2024. [Online]. Available: https://www.wilsoncenter.org/blog-post/preparing-y2q-and-post-quantum-disruption

[43] D. Lague, “U.S. and China race to shield secrets from quantum computers,” Reuters. Accessed: Apr. 02, 2024. [Online]. Available: https://www.reuters.com/investigates/special-report/us-china-tech-quantum/

[44] KAUST innovation, “Partnering with KAUST to Bring Quantum Computing to the Middle East,” KAUST Innovation. Accessed: Apr. 02, 2024. [Online]. Available: https://innovation.kaust.edu.sa/zapata-kaust-quantum-computing-research-collaboration/