Impact of Quantum Computing on Cybersecurity: A Literature Survey

Krishna Saharsh Mamidipalli
Department of Electrical and Computer Engineering
Boston University
Boston, USA
mkrishna@bu.edu

***Abstract*—The aim of this paper is to understand the rapidly-growing technology, Quantum Computing and its impact on Cybersecurity, the base on which secure communications take place. Quantum Computing algorithms, like Shor's and Grover's algorithms that can pose a threat to currently used encryption algorithms are discussed and their effects are understood. In addition, various types of cryptographic techniques, like symmetric and asymmetric, and hash functions are explained. The solution to tackle quantum algorithms, known as "post-quantum cryptography" techniques, like Lattice-based cryptography, code-based cryptography are discussed. This paper is inspired from another paper posted on International Journal of Advanced Computer Science and Applications (IJACSA) on the same topic [1].**

***Index Terms*—Quantum Computing, Cryptography, Lattice-based Cryptography, RSA, AES, Shor's algorithm and Grover's algorithm, Post-quantum cryptography.**

I. Introduction

Quantum Computing was a concept introduced in 1982 as theory by Richard Feynmann. It is defined, by Amazon Web services, as "a multidisciplinary field comprising aspects of computer science, physics, and mathematics that utilizes quantum mechanics to solve complex problems faster than on classical computers" [2]. These computers use the natural properties and behaviours of sub-atomic particles to execute complex calculations in contrast to classical computers that use electrical signals.

Cybersecurity, on the other hand, is defined as "the practice of protecting critical systems and sensitive information from digital attacks" by IBM. This area protects multiple domains from people with evil intentions and those who pose a threat to any organization(s) [3].

"Cryptography is a technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information" as defined in Geeksforgeeks [4]. This process plays a pivotal role in most communication networks and satisfies the three major pillars of security, i.e., Confidentiality, Integrity and Availability, popularly knows as the CIA Triad [**?**]. There are two types of encryption techniques: Symmetric and asymmetric, each of them having their advantages and disadvantages.

With the advent of quantum computers, reliability on current encryption algorithms is found to be at stake because the duration of time required to break an encryption algorithm can be reduced to minutes. Symmetric encryption technique like Advanced Encryption Standard (AES) is the most secured algorithm till date. However, if only 128 bits are used as a key, it is vulnerable to be broken by quantum algorithms. Similarly, in asymmetric techniques, RSA algorithm is the most secure but it is also susceptible to be broken using quantum computers.

We analyse and discuss about the post algorithms that have the potential to deem current cryptography techniques not secure, namely, Shor's algorithm and Grover's algorithm for asymmetric and symmetric encryption techniques respectively.

Finally, we understand the concepts of encryption standards that are quantum resistant.

II. Quantum vs Classical Computing

Quantum Computers are looked at as the new-age computers to solve complex problems instead of the classic super computers. They use the properties of sub-atomic particles to solve complex problems. They use 'Quibits' instead of binary digits [5]. Quibits may be electrons, nucleus or protons. The binary digits have two discrete outputs, 0 or 1. However, in the case of quibits, they can hold both states simultaneously. This property of quibits is known as superposition. However, when a quibit's state is measured, only one among the two states is served as the output. Another concept that makes quantum computing dynamic is a phenomenon called Entanglement [6]. It can vaguely be defined as a close connection that make each of the quibits react to a change in other's state instantaneously no matter how far apart they are. Therefore, when two quibits are taken, their state is not described individually, rather as a single object projecting four various states. These concepts put together make quantum computers powerful to solve complex mathematical problems quickly and efficiently by parallel computation [**?**]. To compare between the two computers, n-qubit quantum computer can process 2^n operations in parallel. The design and architecture of quantum computers differ from classical ones. The normal computers are made up of transistors and diodes while quantum ones generally use electrons as quibits in computing liquids [7].

Although a lot of praise is dedicated to these super fast quantum computers, their performance for regular day usage is rather disappointing. They do not show any improvement or difference in speed with respect to classical computers. Their usage is currently only effective to solve large complex problems quickly.

III. Cryptography Today

This section aims to build an understanding on the various types of encryption standards that are in practice today. We also look at how these standards are difficult to break even using super computers.

A. *Symmetric Cryptography*

Symmetric Cryptography is a technique where the sender and receiver use the same key to encrypt and decrypt. To understand it better, let two people, John and Jacob, communicate sensitive information between each other. To encrypt the data, John uses a special key along with an algorithm and sends the message to Jacob. During the transit, outsider cannot interpret the message without knowing the algorithm and the key used. Jacob also must use the same key to decrypt the message to read it. Although this method is fast, it is not secure enough because only a single key is used. Hence it is used along with Asymmetric algorithms.

Advanced Encryption Standard (AES) is the most popular and secure encryption technique available today. It uses a key size of either 128/192/256 bits. It is known as a block cipher because it encrypts the plain text in blocks [8]. Each block undergoes 10/12/14 rounds of substitutions depending on the length of the key respectively. Similarly, for decryption the inverse of the same operation is carried out. It is widely used in Data storage, wireless security, password storage, etc. Triple Data Encryption Standard (3DES) is another famous technique.

B. *Asymmetric Cryptography*

Asymmetric Cryptography is an upgrade of symmetric encryption in terms of security but at the expense of time lag. In contrast to symmetric, this technique uses two separate keys, one for encryption and another for decryption. To explain with an explain, let John and Jacob communicate with each other. Both have two keys with them, a private key and a public key. Public key, as the name suggests, is available to everyone but the private key is only available to the owner of the key. To send a message, John may use the public key of Jacob to encrypt the message and send it to Jacob. Only Jacob can decrypt the message using his private key. This provides more security to the message. However this technique cannot be used alone because anyone can send a message to Jacob as John because his public key is accessible. Hence, authenticity is lost. If private key is used to encrypt the message, confidentiality is lost because any person who has the public key of the sender can intercept the message, decrypt and read it.

Rivest-Shamir-Adleman encryption (RSA) is the most famous algorithm in asymmetric techniques, also known as public-key cryptography (PKC) [?]. The idea behind this technique is based on large numbers prime factorization. The keys are generated using multiplication of two really large prime numbers of roughly same length and Euler's totient function. Currently, classic super computers cannot break this algorithm but it is vulnerable to quantum computer's speed. Apart from RSA, Diffie-Helman and Elliptical Curve Cryptography (ECC) are also widely accepted and used techniques. These techniques are secure but they use shorter keys and hence can be broken easily using quantum computers.

IV. Effect of Quantum Computing on Encryption Standards

The current encryption standards are safe from the quantum computers but are vulnerable when the number of quibits used inside the quantum computers increase. This section introduces the algorithms built that have the ability to deem these encryption standards useless. They are Shor's algorithm and Grover's algorithm. The encryption standards that rely on large prime factorization problem difficulty are vulnerable. Most of these cryptographic algorithms are secure presently because the time required to find the prime factors using classical computers is not computationally feasible. They will take a lifetime to find the prime factors and eventually the private key. This is because these computers conduct iterations sequentially and end up taking a long time. In contrast, quantum computers conduct exhaustive key searches parallelly reducing time required to find the key.

National Institute of Standards and Technology (NIST) has reported its finding on reliability on cryptographic algorithms post-quantum phase. It is noteworthy that public key exchange algorithms are prone to quantum algorithms than symmetric encryption. Table I describes the findings from NIST on current cryptographic standards [?].

A. *Shor's Algorithm*

Shor's algorithm was first introduced in 1994 by Peter Shor, an American Mathematician. In his paper "Algorithms for Quantum Computation: Discrete Logarithms and Factoring", he mentioned that cryptographic standards that function using factorization problem or discrete logarithmic problem are prone to be vulnerable his algorithm [?]. An example is used to explain the working of Shor's algorithm. Let N be a product of two prime numbers, p and q. [?]

- Let N be 77 for this example.
- Let us pick a number g, such that it satisfies the condition, 1 ¡ g ¡ N-1. For this example, let g be 8.

TABLE I. IMPACT ANALYSIS OF QUANTUM COMPUTING ON ENCRYPTION SCHEMES

Cryptographic Algorithm	**Type**	**Purpose**	**Impact From Quantum Computer**
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

r in g^r:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Remainders:	1	2	4	8	1	2	4	8	1	2	4	8	1	2	4	8

TABLE II. REMAINDERS

- When g is multiplied by itself over and over, it always reaches a multiple of N + 1. i.e., mN + 1.
- This means you can always find an exponent r for which g to the power r is a multiple of N plus 1

$$g^r = mN + 1 \tag{1}$$

- Table II shows the remainders when g^r is divided by N. It is to be noted that the remainders repeat themselves once the remainder is 1.
- If r is even, in this case 10, we found an equation that is similar to the product of two prime numbers:

$$(g^{r/2} + 1)(g^{r/2} - 1) = mN \tag{2}$$

- Now we have r = 10 and g = 8. Using the Euclid's algorithm, we find the factors, p and q.
- Equation (2) signify the **possible factors** of the chosen number N.

The same procedure is followed with different r and g values until the result is obtained.

Shor's algorithm can also be used to compute problems related to discrete logarithms. It involves using Fourier Transformations and superpositions of integers.

B. Grover's Algorithm

Grover's algorithm came into existence in 1996 when Lov Grover proposed the idea. It is also known as the "quantum search algorithm". The algorithm can is used for unsorted databases of N entries [**?**]. It can find the required entry in $\sqrt{N}$ searches. A conventional computer would need N/2 searches to find the same entry. A famous standard DES was cracked using this algorithm easily because it uses only 56-bit key. However, if the key size is increased, the time required to crack the key also increases exponentially. Therefore, it is not as fast and effective as Shor's algorithm. This algorithm is only used for symmetric encryption. But its threat is not pronounced because the algorithm starts to be ineffective when the key size is increased.

The Advanced Encryption Standard (AES) is one of the cryptographic standards that proves to be in quantum secure, but under the constraint that the key size must be 192 or 256 bits.

C. Hash Functions

Hash functions in cryptography are used to maintain the integrity of the message. It takes as input, a variable length message and yields an output of field length irrespective of the input length. Unlike other functions, the output of this function cannot be reversed. Whenever a message is received along with its hash value, the receiver also generates a hash of the received message. If the incoming hash value is the same as the value generated by the receiver, it implies that the message has retained its integrity and was not tampered by anyone.

The effect of quantum algorithms on hash functions is similar to that of symmetric encryption. Only Grover's algorithm, when integrated with birthday paradox, is capable of collapsing hash functions. However, if the hash key value's length is increased, even the quantum algorithms will not be computationally feasible [**?**]. Algorithms like SHA-3 are currently quantum resilient.

V. QUANTUM RESILIENT CRYPTOGRAPHY

The agenda of quantum resilient cryptography or post-quantum cryptography is to provide encryption solutions that are not susceptible to quantum computing algorithms while being able to operate with the current network and communication protocols [**?**]. The research for post-quantum algorithms started as early as 2016 and NIST had released a deadline, November 2017 to release the first set of proposals. Around 82 proposal were released. All the algorithms under consideration do no relate to complex problems like prime factorization or discrete logarithms but on other complex mathematical problems.

A. Mathematics-based Quantum Cryptography

There are many mathematical-based cryptography techniques being researched. Amongst them, the most researched are as follows:

- Lattice-based Cryptography [?]
- Code-based Cryptography [?]
- Multivariate-based Cryptography [?]
- Hash-based Cryptography [?]

Not all of the current options and novel schemes that are being developed in these mathematical fields necessarily meet the criteria for the ideal scheme. We will present a summary of these cryptographic techniques in the subsections that follow.

*1) **Lattice-based Cryptography**:* Lattice-based is the most researched and highly looked into concept because it checks most of the boxes required to be quantum safe. Also, Lattices as a subject is well studied as a mathematical subject and they are extremely versatile when it comes to the blueprint for crypto-systems that are allowed to be built. Further, the ability to perform computation on encrypted data is one of the many use cases for lattice-based cryptographic primitives and protocols, which offer strong foundations for protocols based on asymmetric key cryptography against strong attackers.
To understand the technique better, we shall first discuss the basics. Lattices are grids that have regularly spaced points in n-dimensions formed by vectors dependent on basis. Basis is a collection of vectors to represent any point in the grid that forms the lattice [?].

The shortest vector problem (SVP), which is the most fundamental of the lattice problems, is the basis for lattice-based cryptography constructs. The idea is to find the closest point in a lattice in a given long basis that is as close to the origin as possible and this problem deals with as many as 10000 dimensions [?].

Initially, two scientists Ajtai and Dwork [?], in 1997, gave their first solution to the shortest vector problem and claimed that their idea can be proved to be secure. But in Nguyen and Ster disproved it because their public key was big and makes their message look unrealistic. Damien Stehle and Ron Steinfeld [?], in 2013, developed a version of NTRU (relies on factorizing a polynomial problem) to be provably secure. Another revision was made in 2016 by Bernstein et al. and he coined it ”NTRU Prime” [?].

Therefore, NTRU is a potential choice for the post-quantum future since it is the most effective and secure algorithm among all the lattice-based candidates that were previously stated.

*2) **Code-based Cryptography**:* This comprises error-correcting code-based cryptographic methods like the Courtois, Finiasz, and Sendrier Signature scheme and the McEliece and Niederreiter encryption algorithms. When the key sizes are multiplied by a factor of 4, the algorithms—which are predicated on how difficult it is to decode linear codes—are thought to be resistant to quantum attacks. The ideal solution to solve the decoding problem, according to Buchmann et al. [?], is to convert it into a Low-Weight-CodeWorld Problem (LWCWP), however doing so in huge dimensions is thought to be impossible. It would be simpler to understand this scheme's workings if Buchmann's succinct analysis of McEliece's original code-based public-key encryption method was used.

The application of code-based cryptography involves a trade-off between efficiency and security, just like any other type of cryptosystems. McEliece's cryptosystem uses big public keys (between 100 kilobytes and several gigabytes), however the encryption and decryption processes are quick and extremely simple.

*3) **Multivariate-based Cryptography**:* This public key scheme's security depends on how challenging it is to solve systems of multivariate polynomials over finite fields. The creation of a multivariate equation-based encryption method is challenging, according to research [?]. Multivariate cryptosystems can be used for both digital signatures and encryption.

There have been various attempts to create asymmetric public key encryption methods based on multivariate polynomials, according to Tao et al. [?], however the majority of them are insecure because some quadratic forms connected to their central maps have low rank. The authors developed a new effective multivariate approach based on matrix multiplication called Simple Matrix (ABC), which fixes the aforementioned flaw. Additionally, digital signatures can be created using multivariate cryptosystems.

Rainbow and Unbalanced Oil and Vinegar (multivariate quadratic equations) are two of the most potential signature schemes. The signatures are three times longer than the values of the hash in UOV because there are more variables and equations than there are variables (3:1). The sizes of the public keys are also substantial. However, Rainbow is more effective since it employs smaller ratios, which lead to reduced digital signature and key sizes.

*4) **Hash-based Signatures**:* In this type, first invention took place in 1979 by Lesie Lamport [?]. It was called the Lamport signature scheme. The appropriate level of security of the system is defined by a parameter *b*. If b is 128-bit, we need a hash that can generate a 256-bit output for any variable length input. Hence SHA-256 is the ideal solution for the message *m*. We need to have two keys, public and private key. we generate a private key of 256 pairs of random numbers so that private key contains a total of $8b^2$ bits. Similarly, public key also contains equal number of bits.

To sign the message, we take the message that is hashed and for every bit of the message digest, we chose a number from each pair of private key so that we have 256 number sequence. This is the digital signature published in addition to the plaint text. After this signature, the rest of the numbers must be deleted from the pairs and the private key must not be used again.

Two hash-based signature techniques are being assessed for standardization right now. In particular, the Stateless Practical Hash-based Incredibly Nice Collision-resilient Signatures (SPHINCS) and the Extended Merkle Signature Scheme (XMSS), both of which are stateful signature schemes.

VI. Limitations of Quantum Computing

A lot of businesses could be completely transformed by quantum computing, a topic that is currently undergoing tremendous development. However, it also has a few drawbacks, like [**?**]:

- **Hardware complexity and cost:** These computers are extremely complex in structure and hence expensive to construct. The hardware required to build is not easy to maintain and manufacture.
- **High error rates:** The quibits are sensitive to environmental changes, in other words, very delicate. Since all the results collapse while measuring any output, it is difficult to detect errors and correct.
- **Output is probabilistic, not deterministic:** When the computer provides an output, multiple solutions are returned but out of which only one is right. Finding the right answer by running the algorithm multiple times reduces the speed of the computer.
- **Limited applications:** These computers are not designed to solve all type of problems. They are used only for specific set of complex algorithms that classical super computers cannot solve.
- **Scalability:** The current technology does not have enough quibits to develop a quantum super computer. It is because these quibits are delicate and they need to be isolated carefully to prevent interference.
- **Coherence:** The output retention time for quibits is short, holding the superposition state for a total of 35 seconds. This is currently a world record. To hold the information for longer, the external conditions must be carefully handled and quibits must be isolated properly.

In behalf of all this challenges, quantum computing proves to be a promising technology and has the capability to revolutionize many fields. There is consistent research taking place to overcome these challenges and it is certain that breakthroughs are just a couple of years away.

VII. Conclusion

The importance of secure communication has grown in priority in the recent years due to increasing cyber attacks. The need for secure encryption standards is of high importance. The arrival of quantum computers and their algorithms posed an immediate threat to cryptography because the complex algorithms these computers were able to solve serve as the basis for encryption algorithms. With time, the algorithms like Shor's and Grover's are getting stronger and the number of quibits used in a quantum computer are also increasing. Multiple techniques of cryptography are already broken and many are vulnerable. The solution for this to switch to quantum resistant cryptographic techniques like mathematical based solutions that include lattice-based, hash-based, code-based cryptography and other concepts like quantum key distribution, etc. The world of communication hangs in balance without these solutions. However, the same quantum computers can be used to derive a solution.

References

[1] arXiv:1804.00200v1, "The impact of quantum computing on present cryptography," 2018.

[2] "What is Quantum Computing (1978)", Amazon. Available at: https://aws.amazon.com/what-is/quantum-computing/.

[3] "What is cybersecurity?" (no date) IBM. Available at: https://www.ibm.com/topics/cybersecurity.

[4] "Cryptography and its types (2023)", GeeksforGeeks. Available at: https://www.geeksforgeeks.org/cryptography-and-its-types/.

[5] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information: 10th Anniversary Edition, 10th ed. New York, NY, USA: Cambridge University Press, 2011.

[6] R. Jozsa, "Entanglement and Quantum Computation," in Geometric Issues in the Foundations of Science, S. Huggett, L. Mason, K. Tod, S. Tsou, and N. Woodhouse, Eds. Oxford University Press, July 1997.

[7] S. Bone and M. Castro, "A Brief History of Quantum Computing," Surveys and Presentations in Information Systems Engineering (SURPRISE), vol. 4, no. 3, pp. 20–45, 1997, http://www.doc.ic.ac.uk/nd/surprise 97/journal/vol4/spb3/

[8] "Advanced encryption standard (AES)," GeeksforGeeks, https://www.geeksforgeeks.org/advanced-encryption-standard-aes/.

[9] "RSA algorithm in cryptography," GeeksforGeeks, https://www.geeksforgeeks.org/rsa-algorithm-cryptography/.

[10] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NIST: Report on Post-Quantum Cryptography," NIST, Tech. Rep., 2016.

[11] W. Buchanan and A. Woodward, "Will Quantum Computers be the End of Public Key Encryption?" Journal of Cyber Security Technology, vol. 1, no. 1, pp. 1–22, 2016.

[12] R. Jozsa, "Entanglement and Quantum Computation," in Geometric Issues in the Foundations of Science, S. Huggett, L. Mason, K. Tod, S. Tsou, and N. Woodhouse, Eds. Oxford University Press, July 1997

[13] M. Campagna and C. Xing, "Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges," ETSI, Tech. Rep. 8, 2015.

[14] Wikipedia, ”Shor’s algorithm,” https://en.wikipedia.org/wiki/Shor27salgorithm/

[15] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” in Proceedings of the 35th Annual Symposium on Foundations of Computer Science, ser. SFCS ’94. Washington, DC, USA: IEEE Computer Society, 1994, pp. 124–134.

[16] Wikipedia, ”Grover’s algorithm,” https://en.wikipedia.org/wiki/Grover27salgorithm/

[17] D. Micciancio, “Lattice-Based Cryptography,” in Post-Quantum Cryptography, 2009, no. 015848, pp. 147–192.

[18] R. Overbeck and N. Sendrier, “Code-based Cryptography,” in PostQuantum Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 95–145.

[19] J. Ding and B.-Y. Yang, “Multivariate Public Key Cryptography,” PostQuantum Cryptography, pp. 193–241, 2009.

[20] C. Dods, N. P. Smart, and M. Stam, “Hash Based Digital Signature Schemes,” Cryptography and Coding, vol. 3796, pp. 96–115, 2005.

[21] W. Wickr, ”What is lattice-based cryptography why should you care?” Medium, CryptoBlog [Online]. Available: https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717

[22] D. Micciancio, “Lattice-Based Cryptography,” in Post-Quantum Cryptography, 2009, no. 015848, pp. 147–192.

[23] M. Ajtai and C. Dwork, “A Public-Key Cryptosystem With WorstCase/Average-Case Equivalence,” Proceedings of The 29th Annual ACM Symposium on Theory of Computing - STOC ’97, pp. 284–293., 1997.

[24] D. Stehle and R. Steinfeld, “Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices,” Cryptology ePrint Archive, Report 2013/004, 2013.

[25] D. J. Bernstein, C. Chuengsatiansup, T. Lange, and C. van Vredendaal, “NTRU Prime,” IACR Cryptology ePrint Archive, vol. 2016, p. 461, 2016.

[26] D. Bernstein, E. Dahmen, and Buch, Introduction to Post-Quantum Cryptography. Springer-Verlag Berlin Heidelberg, 2010.

[27] W. Buchanan and A. Woodward, “Will Quantum Computers be the End of Public Key Encryption?” Journal of Cyber Security Technology, vol. 1, no. 1, pp. 1–22, 2016.

[28] C. Tao, A. Diene, S. Tang, and J. Ding, “Simple Matrix Scheme for Encryption,” in International Workshop on Post-Quantum Cryptography. Springer, 2013, pp. 231–242.

[29] E. Bernstein and U. Vazirani, ”Limitations of quantum computation,” in Proceedings of the 25th Annual ACM Symposium on Theory of Computing, 1993, pp. 111-117.