IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207117 |

The Effects of Quantum Computing on Cryptography

Gaurav Shankaram[1], Prashanth K[2]

P.G. Student, Department of Master of Computer Applications, R V College of Engineering, Bangalore, India[1]

Assistant Professor, Department of Master of Computer Applications, R V College of Engineering, Bangalore, India[2]

ABSTRACT: Understanding the influence of quantum computing on current cryptographic systems is crucial due to the potential threat it poses to data security. By examining the distinctions between quantum and classical computation, we gain insights into the unique computational properties of quantum systems. By examining key quantum algorithms like Shor's and Grover's, we can assess the specific encryption schemes that are susceptible to attacks and explore alternative post-quantum methods that can provide secure solutions in the age of quantum computing. Overall, the purpose of this paper is to raise awareness about the implications of quantum computing on cryptography and provide essential knowledge.

KEYWORDS: Quantum computers, Shor's algorithm, Grover's algorithm, cryptography, Hash Functions.

I. INTRODUCTION

The field of cryptography holds significant importance in the realm of information technology as it is essential for ensuring the confidentiality, integrity, authenticity, and non-repudiation of data during its transmission and storage. The technique of protecting data from third party adversaries while it is in transit or being stored is known as cryptography, which derives its name from the Greek words for concealed and writing. Asymmetric and symmetric cryptosystems are the two main types of cryptosystems.

In 1982, Richard Feynman initially introduced the concept of quantum computing theory. Since then, extensive research has been conducted on it, and it is now widely believed to pose a significant threat to current Public-key encryption methods. Moreover, it is indeed accurate that specific quantum algorithms can potentially influence secret key cryptography. However, the security of this encryption method can be enhanced by employing larger key spaces, thereby reducing its vulnerability to quantum attacks. In addition, approaches that potentially defeat the current Public-key cryptography techniques have been developed. These schemes security relies on the discrete logarithm problem and the difficulty of factoring big prime numbers. Even elliptic curve cryptography, which is currently thought to be the most effective and safe method, seems to be vulnerable to quantum computers.

The demand for cryptographic methods that are resistant to quantum computing has led to the need for advanced solutions. The subsequent sections of the paper delve into the analysis of hash functions, secret key cryptography, and Public-key cryptography. Particularly, the focus lies on techniques that capitalize on the discrete log problem and the difficulties involved in factoring large prime numbers. Next, the paper provides a brief overview of quantum mechanics and the difficulty of creating a genuine quantum computer. Furthermore, the document presents Shor's algorithm and Grover's algorithm as noteworthy quantum algorithms that can potentially exert a substantial influence on Public-key cryptography and to a lesser extent on symmetric encryption.

II. CURRENT STATE OF CRYPTOGRAPHY

In this chapter, a concise overview is presented to elucidate the roles performed by hash functions, symmetric algorithms, and asymmetric techniques in modern cryptography. We examine the difficulties associated with factorizing large numbers and delve into the discrete logarithm problem, which serves as the fundamental basis for efficient asymmetric ciphers.

A. Secret key cryptography

In secret key cryptography, information is encoded and decoded by both the sender and the recipient utilizing an identical secret key and cryptographic algorithm. Mary has the option to utilize the shared secret key for encrypting a plaintext message, while Harry can employ the same cryptographic method and shared secret key to decrypt the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207117 |

message. Due to the importance of maintaining the key's privacy, a dependable approach for exchanging secret keys over public networks is necessary to ensure that only Mary and Harry are aware of it. To address the issue of key distribution in secret key encryption, Public-key cryptography was developed. The data encryption standard and the advanced encryption standard (AES) are two common examples of symmetric algorithms.

B. Public-key cryptography

Asymmetric cryptography, often known as public key cryptography (PKC), is a type of encryption in which the keys are dispersed in pairs. Each side should have their own set of private and public keys. For example, Harry would require Mary's public key to encrypt a message, and Mary would provide Harry that key. After that, Harry would encrypt the message using Mary's public key. After Harry sends the message to Mary, she can use her private key to decrypt it. Consequently, the message is encrypted using a public key, and decoding it necessitates the possession of the corresponding private key.

Digital signatures also make use of Public-key cryptography. For instance, after Mary has digitally signed a document using her private key, Harry can use Mary's public key to verify Harry's signature on the document. The discrete logarithm problem and difficulties with large prime number factoring are two examples of the computational problems that underlie PKC's security. One-way functions are a class of algorithms whose inversion is challenging but whose execution is simple in one direction [1].

1) Factorization Problem

Factoring bi-prime numbers, which are utilized in RSA, presents significant challenges. Given their computationally intensive nature, RSA and other asymmetric algorithms are generally not intended to replace symmetric methods [2]. The primary application of RSA is secure key exchange between end nodes. As highlighted by Kirsch [3], RSA is potentially vulnerable if a rapid factorization method is developed or if there is a substantial increase in computing power.

2) Discrete Logarithm Problem (DLP)

DLP is the foundation of Public-key cryptographic systems like Diffie-Hellman. The challenge of finding the integer "r" such that "gr ≡ x (mod p)" is what determines the level of difficulty in breaking various cryptosystems. The discrete logarithm problem of "x" to the base "g" as an integer can be expressed using the formula "r = logg(x) (mod p) ". Elliptic curve cryptography (ECC) employs a pair (x, y) that can be represented by the equation "y2 = x3 + ax + b (mod p)," along with an imaginary point Θ (theta) at infinity. The parameters "a" and "b" belong to the set of residues modulo "p," and it is essential that the condition "4a3 + 27b2 ≠ 0 (mod p)" is satisfied, as mentioned in the referenced source [2]. In (ECC), it is imperative that the primitive or pair elements employed are both of order G and cyclic in Group G. As subsequent sections will elucidate, ECC is widely regarded as the most efficient and secure public key cryptosystem.

III. COMPARISON OF QUANTUM COMPUTING AND CLASSICAL COMPUTING

The fundamental building blocks of a classical computer are called bits and are observable in states of 0 and 1. In contrast, quantum computers utilize quantum bits, commonly referred to as qubits [4]. Qubits are particles that possess the unique ability, known as superposition, to exist in both the 0 and 1 states simultaneously. However, when observed, a qubit collapses into one of these states. Quantum computers leverage this characteristic to address complex problems, utilizing the potential of qubits in their computations. An action performed on a qubit in superposition simultaneously affects both of its values. Quantum entanglement is another physical phenomenon utilized in quantum computing. When two qubits become entangled, they can no longer be considered as separate entities with distinct states; instead, they form a unified system with four composite states. Additionally, irrespective of the physical distance between the two entangled qubits, any change in the state of one qubit will correspondingly impact the other qubit. This property allows for true parallel computing power to be achieved [5].

A classical computer, which utilizes conventional transistors and diodes, is fundamentally distinct in design from a quantum computer [8]. Researchers have explored numerous designs for quantum computers, including quantum dots, which involve electrons in a superposition state, and computing liquids. These examples represent a small fraction of the diverse range of designs that have been investigated.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207117 |

IV. CRYPTOSYSTEMS EXPOSED TO QUANTUM ALGORITHM

Cryptosystems exposed to quantum algorithms face vulnerabilities that pose significant challenges to their security. Among the vulnerable cryptosystems, RSA encryption, based on the difficulty of factoring large numbers, can be efficiently broken by Shor's algorithm. The Diffie-Hellman key exchange, relied upon for secure communication, becomes compromised as quantum algorithms solve the discrete logarithm problem effectively. Even elliptic curve cryptography (ECC), known for its security, can be broken by quantum computers' ability to compute discrete logarithms efficiently. While symmetric key cryptography is not directly vulnerable to quantum algorithms, the security of symmetric encryption can be compromised if an adversary gains access to the secret key through quantum attacks on key exchange protocols. As a result, it is crucial to develop post-quantum cryptographic algorithms to ensure the security of these vulnerable cryptosystems in the quantum computing era.
Table 1, provides an overview of the impact that quantum computing will have on existing cryptographic techniques [14].

A. Shor's Algorithm for public-key cryptography

Shor's algorithm utilizes the discrete logarithm problem or the factorization of large prime integers as its foundation, can lead to the failure of modern public-key cryptography. The following example demonstrates the process of Shor's algorithm in factoring large prime numbers. Specifically, we aim to determine the prime factors of 15. To achieve this, a 4-qubit register is required. By utilizing a 4-qubit register, it becomes feasible to store and compute the prime factorization of the number 15, which in binary representation is represented as 1111. The computation performed on the register can be envisioned as simultaneous calculations for every possible value that the register can hold (ranging from 0 to 15). The algorithm does the following:

- The number to be factorized is represented as n = 18.
- A random number x is chosen, where 1 < x < n - 1.
- x is raised to the power of each state in the register, and the result is divided by n.
- The resulting information is stored in a second 4-qubit register, containing the outcomes of the superposition. Let's assume x = 2, which falls between 1 and 17.
- By dividing x by 18 and raising it to the powers of the 4-qubit register (up to a maximum of 18), the results are recorded.
- The outcomes will reveal a pattern that can be analyzed to determine any potential factors and their corresponding values.

Shor's algorithm can also be utilized to solve discrete logarithm problems. Vazirani [12] extensively studied the methodology of the Shor algorithm and demonstrated how, starting from a random superposition of two numbers, it is possible to construct a new superposition that, with a high probability, yields two integers satisfying a specific equation.

B. Grover algorithm for secret key cryptography

The Grover's algorithm, primarily known for its application in quantum database search, can also be used in secret key cryptography. It provides a way to perform an unstructured search through a large solution space with a significant speedup compared to classical algorithms. In secret key cryptography, Grover's algorithm can be utilized to enhance the brute-force search process. For example, if a secret key is represented by N bits, a classical computer would require an average of 2(N-1) attempts to find the correct key through exhaustive search. In contrast, Grover's algorithm can accomplish the same task with approximately $\sqrt{}(2N)$ operations, offering a quadratic speedup.
However, it is important to note that Grover's algorithm does not break the fundamental security of secret key cryptography. It only provides a computational advantage over classical brute-force search algorithms. Hence, secret key cryptography algorithms can still maintain their security by using longer key lengths to withstand the potential impact of quantum algorithms such as Grover's algorithm.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207117 |

Algorithm	Type	Purpose	Effect from Quantum Computer
AES-256	Symmetric Key	Encryption	Safe
SHA-256, SHA-3	-	Hash functions	Safe
RSA	Public Key	Signatures, Key establishment	Unsafe
ECDSA, ECDH	Public Key	Signatures, Key swap	Unsafe
DSA	Public Key	Signatures, Key swap	Unsafe

Table 1. Quantum Computing impact analysis on encryption schemes (from [14])

C. Public-key Encryption Schemes Affected

Public-key encryption schemes face significant vulnerabilities when exposed to quantum algorithms. RSA encryption, relying on the factorization problem, is highly susceptible to Shor's algorithm, which efficiently factors large numbers. The Diffie-Hellman key exchange protocol, used for secure communication, is compromised as quantum algorithms can efficiently solve the discrete logarithm problem. Elliptic Curve Cryptography (ECC), known for its security and efficiency, can be broken by quantum computers' ability to compute discrete logarithms effectively. Additionally, lattice-based cryptography, a potential post-quantum solution, may also be vulnerable to quantum attacks if more efficient lattice-based quantum algorithms are developed. The emergence of these vulnerabilities highlights the need for post-quantum cryptographic schemes to ensure the security of public-key encryption in the era of quantum computing.

In Table 2, a comparison of classical and quantum security levels for the most used cryptographic schemes are presented.

D. Secret key Encryption Schemes Affected

While secret key encryption schemes are not directly vulnerable to quantum attacks in the same way as public-key encryption, certain aspects of these schemes can still be impacted. The security of secret key encryption relies on the confidentiality and integrity of the shared secret key. Quantum algorithms, such as those capable of efficient key search or exhaustive key space exploration, can potentially undermine the security of secret key encryption by compromising the confidentiality of the key. Therefore, secret key encryption schemes may need to adapt to the quantum computing era by employing larger key spaces or implementing quantum-resistant key exchange mechanisms to ensure continued security in the face of evolving threats.

Crypto Scheme	Key Size	Effective Key Strength	
		Classical Computer	Quantum Computer
RSA-1024	1024	80	0
RSA-2048	2048	112	0
ECC-256	256	128	0
ECC-384	384	256	0
AES-128	**128**	**128**	**64**
AES-256	**256**	**256**	**128**

Table 2. Comparison of security levels for the common Cipher system

E. Hash Functions

Since the security of the hash function family depends on a set output length, they share the same issue as secret key ciphers. With Grover's approach, a collision in a hash function can be located in square roots of the length of the function. Additionally, it has been demonstrated that the birthday paradox and Grover's technique can be combined. Brassard and associates [16] introduced a quantum birthday assault. An assault is said to be successful if a table of size $3\sqrt{N}$ is produced and Grover's technique is used to locate a collision. This indicates that a hash function needs to output at least 3b bits in order to give a b bit security level against Grover's quantum method. Since they cannot be used in the quantum era, many of the hash methods in use today. Despite having longer outputs, SHA-2 and SHA-3 are nonetheless quantum resistant.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207117 |

V. CONCLUSION

In our data-centric society, ensuring secure data transmission and storage is crucial. However, both traditional public key methods (3DES, AES) and secret key algorithms (3DES, ElGamal, ECC, DSA) face substantial risks from the emergence of quantum computers. Protecting sensitive information demands the development of quantum-resistant encryption techniques. The ongoing progress towards developing a fully functional universal quantum computer capable of utilizing powerful quantum algorithms, such as Grover's and Shor's, brings the imminent downfall of existing secure public key techniques like RSA and Elliptic Curve Cryptosystems. To address this challenge, new cryptographic techniques immune to quantum computing must be developed. These include lattice-based cryptography, hash-based signatures, code-based encryption, and quantum key distribution methods.

REFERENCES

[1] M. Dusek, N. L ˇ utkenhaus, and M. Hendrych, “Quantum cryptography,” Progress in Optics, vol. 49, pp. 381–454, 2006.
[2] C. Paar and J. Pelzl, “Introduction to Public-Key Cryptography,” in Understanding Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 149–171.
[3] Z. Kirsch, “Quantum Computing: The Risk to Existing Encryption Methods,” Ph.D. dissertation, Tufts University, Massachusetts, 2015.
[4] 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.
[5] 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.
[6] W. Tichy, “Is quantum computing for real?: An interview with catherine mcgeoch of d-wave systems,” Ubiquity, vol. 2017, no. July, pp. 2:1–2:20, Jul.2017. [Online]. Doi: http://doi.acm.org/10.1145/3084688
[7] M. Soeken, T. Haner, and M. Roetteler, “Programming quantum computers using design automation,” arXiv preprint arXiv:1803.01022, 2018.
[8] 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/surprise97/journal/vol4/spb3/.
[9] M. Campagna and C. Xing, “Quantum Safe Cryptography and Security: An Introduction, Benefits, Enablers and Challenges,” ETSI, Tech. Rep. 8, 2015.
[10] 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.
[11] 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.
[12] U. Vazirani, “On the Power of Quantum Computation,” Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, vol. 356, no. 1743, pp. 1759–1768, 1998.
[13] L. Grover, “A Fast Quantum Mechanical Algorithm for Database Search,” Bell Labs, New Jersey, Tech. Rep., 1996.
[14] J. Proos and C. Zalka, “Shor’s Discrete Logarithm Quantum Algorithm for Elliptic Curves,” Quantum Info. Comput., vol. 3, no. 4, pp. 317–344, 2003
[15] National Security Agency, “National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information,” NSA, Tech. Rep., 2003.
[16] G. Brassard, P. Høyer, and A. Tapp, Quantum Cryptanalysis of Hash and Claw-Free Functions. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 163–169.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details