International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Study of Post Quantum Cryptographic Security Model Using Symmetric Key Algorithm

Sonali Sharma[1], Shilpi Sharma[2,*], Tanupriya Choudhury [3]

Submitted: 30/01/2023 **Accepted:** 03/04/2023

Abstract: The advancement in the field of technology and science has rendered the classical algorithms used for securing data vulnerable to attacks by quantum computers. Post quantum cryptography aims at establishing quantum safe algorithms so that data can be secured. Advanced Encryption Standard (AES) is a symmetric key block cipher which provides security against known quantum attacks. The Shor's and Grover's algorithms are the quantum algorithms which have proved to break encryption provided by security mechanisms like RSA and even have the potential to break AES-128 in future. However, if key size of symmetric key security mechanisms is increased then security provided by them cannot be broken by both classical and quantum computers in near future. Quantum computers are becoming more and more prevalent, but there is still some concern about their security. In this paper, we will show that the current quantum computers in use cannot break AES-256 encryption with Grover's algorithm. We have implemented AES-256 for encryption of files in our system and proposed a proof that the qubits used by quantum computers are not enough to break AES-256 with Grover's algorithm. We believe that this provides strong evidence that current quantum computers are not a threat to encrypted data using AES-256. We hope this will ease concerns about using quantum computing for secure applications and encourage further development of these powerful machines.

Keywords- *Post-Quantum Cryptography, Grover's algorithm, AES-256, Quantum attacks.*

1. Introduction

Digitization in recent years has resulted in development of technology and security schemes which are capable of doing computations at an exponential speed. The advancements in the field of quantum computing has led to the advent of quantum computers [30]. Organizations like IBM, Google and many others are rigorously dedicated in developing quantum computers with a large number of qubits. Recently in December, 2020 a quantum computer named Jiuzhang has been developed by a team of researchers in China which is considered to be do computations 10 billion times faster as compared to Sycamore (quantum computer developed by Google in 2019). The ideology of developing a quantum computer and achieve quantum supremacy is leading to the development of post cryptographic algorithms so as to safeguard the systems which use the classical security mechanisms. An initiative has been taken by NIST (National Institute of Standards and Technology) in 2017 for testing of potential algorithms which can be resistant to quantum attacks.

Currently, submissions for round-3 have been received by the organization for review in June 2020. According to the submissions received in round-2 the public key security systems have been implemented majorly in FIPS 186-4 and digital signature standard which are considered to be vulnerable to the quantum computers having large number of qubits [1]. In this paper, we have discussed the working and capability of a computer which has the ability to use quantum theory along with the properties like entanglement and superposition. The qubits used in quantum computers can be superimposed to do computations

[1] *Department of Computer Science and Engineering, Amity University, Uttar Pradesh, India*
[2] *Department of Computer Science and Engineering, Amity University, Uttar Pradesh, India*
[3] *Department of Computer Science and Engineering, UPES, Dehradun, India*
Corresponding author: - ssharma22@amity.edu

having exponential or quadratic speedup. This property has been used by Grover's algorithm which works on unstructured data to perform search which is comparatively very less time as compared to the algorithms used by classical computers, this method is used to find the key combinations in the field of cryptographic systems [26]. The proposed solution to this problem is increasing the key size of the symmetric key algorithms so that they cannot be broken, the Asymmetric key security systems however are susceptible to be decrypted by Shor's algorithm which possesses the capability of finding the prime factors at a exponentially high speed. Advanced encryption standard (AES), is the best known block cipher developed by NIST in 2001, uses key sizes of 128, 192 and 256. Although the traditional computer systems can break AES-128 in 5x1021 years [2], but with the advancements in quantum computing the post-quantum era has the capability of breaking down AES-128 in fairly less time. Therefore, we have implemented AES-256 to encrypt the files in the system so that they are safe from both classical and quantum computers. One of the known quantum attacks includes Demirci- Selçuk meet-in-the-middle attack [3], which is unable to break the encryption standards used by AES-256.

2. Related Work

The literature review shows that the studies derived aim at providing an insight of the advancements which have been made in the field of quantum safe algorithms and the research gaps which need to be reviewed so as to propose a framework for building systems which are quantum safe.

Brandon Rodenburg and Stephen P. Pappas [4] published a research on vulnerabilities which need to be addressed by blockchain architecture as the world advances to a new technology known as quantum computers. The second threat to blockchain which uses the asymmetric key security model at any point is by Shor's Algorithm which can factorize prime numbers by exponentially increasing the computations. To counter the threats posed by these quantum algorithms, post quantum cryptographic methods along with some secure algorithms and security models and have been discussed. The development of Quantum Key distribution (QKD) protocol in which a randomly generated random bit stream is used to encrypt a secret message, also known as OTP or One time password is recommended by the authors. This generation of random key needs to establish by the sender and receiver and once that is achieved then the message is considered to be unconditionally secured [4]. It has been stated in the paper that NIST has been working towards building stronger quantum resistant algorithms which work on some promising areas like- Hash-based cryptography, Code-based cryptography, Lattice- based cryptography and multivariate quadratic based cryptography. Therefore, either QKD can secure this computational data structure from a quantum attack or post quantum cryptographic algorithms. It has also been stated that a proposal of Quantum bitcoin has been put forward which will work on the classical computers but will use the albitites of Quantum computing to mine and verify the block.

Sandeep Kumar Rao et al. [2] published about post quantum cryptography, QKD (Quantum key distribution) and have done a comparison analysis of security provided by various popular cryptographic algorithms. According to their research, the Public key cryptographic security models like RSA, ECC can be broken down by attacks carried out by an quantum computer by using Shor's algorithm. They have also discussed about Grover's algorithm and it's capability to break down some of the symmetric key cryptographic algorithms like DES, AES-128 and IDEA [2]. After the comparison analysis and examining the capabilities of Grover's algorithm it has been concluded in their paper that AES-256 is quantum safe and can be used to provide better security and strong encryption standards to the confidential data.

Awadesh Kumar and R.R Tewari [5] extended a framework which implements AES-256 and AES-512 key generation algorithm. The model discussed in the paper is based on AES-512. The sub key generation model discussed for 512 bit key constitutes of 16 rounds and17 sub key. Although this model is not implemented yet because larger key size provides more security and takes more time in encryption and decryption process to take place but the computation becomes complex. AES-256 is being used currently and is considered to be secure for providing security as compared to other key lengths in AES. They have also discussed about the time required for encryption and decryption during pre-computation and fly key generation. In their paper they have proved that fly key generation method takes very less time as compared to the pre computation method [5]. The encryption decryption carried out using the operation modes like CBC take large time and if OFB and CFB are used for decryption mechanism.

Deepraj Soni et al. [6] discussed about the post-quantum cryptographic security scheme and the hardware required to implement them. As stated in the paper the lattice based security systems are built on shortest vector problem and are hard to break even with a quantum computer. Their study has improved the latency by using optimization techniques such as loop unrolling and loop pipelining for enhancing PQC. For the signature algorithms they have performed the key generation procedure along with signature verification. Since NIST is rigorously working towards finding algorithms which are quantum safe the studies in this paper have helped enhance the hardware implementation of two algorithms so that in future they can be implemented with wase and provide the security which the other classical algorithms fail at. The key takeaways from their findings is that as the security is improved the latency also increases at a significant rate but the overhead of area does not. Also they concluded that qTESLA has more requirement of area as compared to CRYSTALS-Dilithium for 1-3 level security in the case of key generation and verification of signatures. These findings can be used for development of more such secure algorithms which can safeguard the data against the quantum attacks.

Stephen Clarke [7] published a research based on Shor's algorithm along with the detailed explanation of its capabilities to factorize prime numbers has been discussed. An experiment has been carried out to compare the functionalities and workability of classical computers as compared to simulated and physical quantum computers. In the first segment of the paper the basics of quantum computing along with some important terms like the Bloch Sphere, Qubit, Hadamard gate, superposition and entanglement have been explained. Later, the discussion and implementation of Shor's algorithm to find the prime factors has concluded the research that the traditional computers cannot exceed their computations greater than 2^n but Shor's algorithm can complete the task in n^3 computations. This makes the public key cryptographic security model RSA vulnerable to the quantum attacks as the time for calculation of prime factors has been fairly reduced. By increasing the key size also RSA cannot be secured as it will make the transmission of the key a very difficult task. The research paper also depicts that major companies are working to build strong quantum computers in the future but regardless of the portability of these computers have to offer they can still be accessed through cloud platforms.

Xavier Bonnetain, María Naya-Plasencia and André Schrottenloher [3] suggested a framework based on post quantum cryptography and security analysis of AES. The framework proposed by them focuses on the classical and Quantum attacks. They have used a Q1 model wherein it has been pre assumed that the attacker has an access to the quantum computer but can encrypt and decrypt the data by using only classical algorithms. In the other segment of their research they have applied the square attacks on 6 round AES-128, 7 round AES-192 and 7 round AES-256. DS-MITM attack has been applied to 8 rounds of AES-256 [3]. Detailed explanation on the cost effectiveness of Grover exhaustive search is also discussed along with some quantum tools which can efficiently be applied to differential properties of AES S-box with a small memory usage. The quantum attacks that they have used to target AES-256 only reach till 8 rounds, thus it gives a good security margin for its usage. After evaluating the results obtained for the attacks which are carried out against AES in classical as well as quantum world it is termed that AES-256 is safe to be used to encrypt data and files.

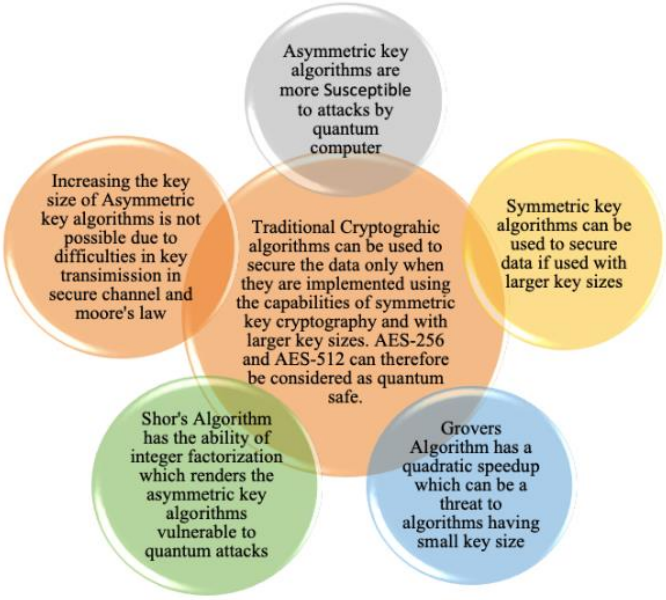

Fig. 1 Conclusion of the literature review

Table 1 shows a comparative analysis of various cryptographic algorithms which are reviewed for building a strong security model resistant against the quantum attacks [37,39]. In Fig. 1 it has been depicted that the post quantum cryptographic algorithms which are considered to be secure are based on symmetric key algorithms with larger key sizes [38]. Although many researches and advancements are being done by NIST in the this field to review new and secure algorithms which are quantum safe [34] but the switch from traditionally used algorithms to new upcoming algorithms remains a challenge and as a solution we propose to improve the traditionally used algorithm AES by increasing their key size because AES-256 and AES-512 are still quantum safe against the known quantum attacks and algorithms.

Table 1 Analysis of cryptographic algorithms

Technique	Category	Gaps identified
Quantum key distribution (QKD)	Encryption by using random bit stream or one time password	QKD, can be used to generate strong OTP, but cannot be used to transmit the data through secured channel
RSA	Public key encryption	Susceptible to attacks by Shor's algorithm and therefore even the larger key sizes are considered to be insecure.
MARS	Symmetric key-Block Cipher	MARS as compared to AES has low performance on the basis of speed and diffusion
RC-6	Symmetric key-Block Cipher	This block cipher uses block size of 128 bits.
IDEA	Symmetric key-Block Cipher	Uses block size of 64 bit and 128 bit key, therefore less secure as compared to other block ciphers.
AES	Symmetric key-Block Cipher	It is considered to be quantum safe only if larger key sizes are used to encrypt the block of size128 bits.
qtesla	Lattice based Digital signature scheme	It is inefficient for software implementation

3. Overview of Grover's Algorithm

In 1996, Lov Grover Implemented the Grover's algorithm which works as an quantum search algorithm [4]. Grover's algorithm can be applied on unstructured data to search the components by using qubits in superposition to make the computations [8].To understand this algorithm let's consider an Oracle function.

$$f(p) \rightarrow 0$$
$$f(q) \rightarrow 1$$

f(p) signifies all the values which don't lead to the significant search result which is required, whereas f(q) signifies the value which is required as a search result [29].

Step 1: Put Qubits in super position through Hadamard Gate, it's a quantum gate which is responsible for superposition of the qubits with a 0.5 probability of the qubit to be 0 or 1.
This can be done with the following equation:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{p=0}^{N-1} |p\rangle \quad (1)$$

The above equation helps the qubits in having uniform amplitude.

Step 2: The Equation to be implemented in this step is as follows:

$$U_f\ |p\rangle = (-1)^{f(p)}\ |p\rangle \quad (2)$$

f(p) gives the value 1 when the required value is found, else it will give a value something other than 1. So, in this equation if the eigen value comes out to be negative for the value which we are looking for then the amplitude of the required value will be flipped to the negative side of the axis other values which are not required will remain as they are.

Step 3: This step is again performed on the Hadamard gate.

$$U_s = 2|s\rangle\langle s| - I$$

And the probability of finding the correct value at time t+1 is given by the following:

$$|\psi_{t+1}\rangle = U_s U_f |\psi_t\rangle$$

U_f stands for oracle matrix and U_s stands for Hadamard gate.
This step increases the expectation value and amplifies the value which we required to search.
The probability and the expectation value is amplified to a greater extend [8].

Final Step: After the amplitudes are increased, we need to take square root of those values to check the highest value and that will be the desired output.

$$|\psi_t\rangle = \left(U_s U_f\right)^t |\psi_0\rangle$$

The above equation gives us the final output after the steps 2 and 3 are repeated t number of times.
Therefore, the time required for Grover's algorithm to perform a search on unstructured data is $\sqrt{n}$ as compared to n in the traditional systems.

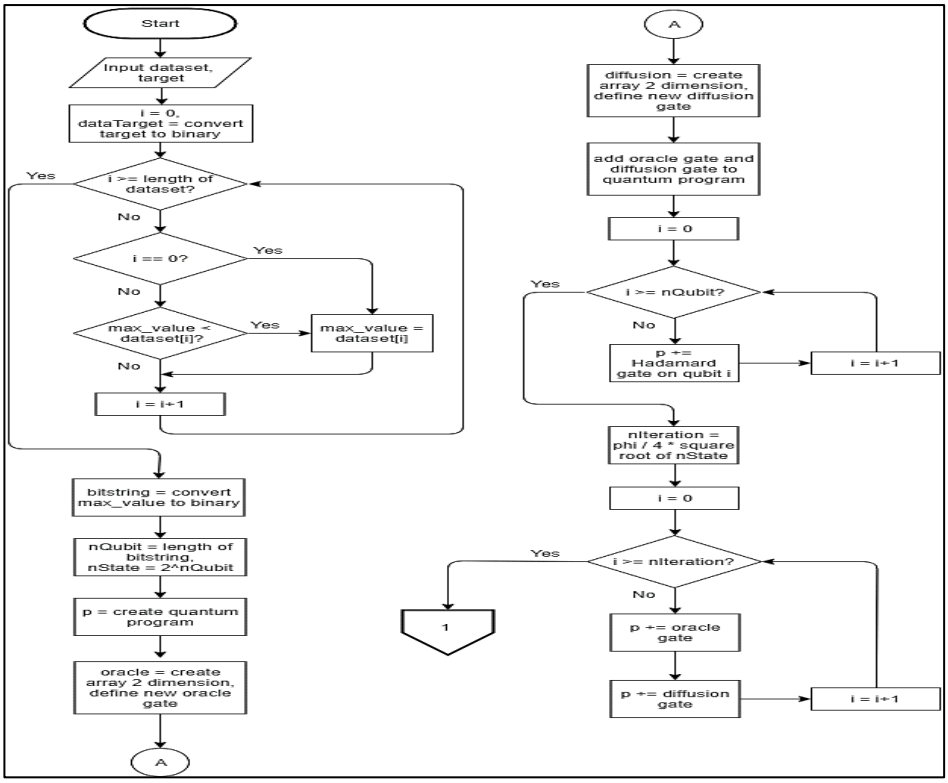

Fig. 2 Flow chart of working of Grover's Algorithm [18]

In Fig. 2 the working of Grover's algorithm is depicted based on the equations discussed. The Grover's algorithm can be applied using a simulator and the results can be obtained in time comparatively less than the traditional search algorithms.

Algorithm 1: Grover's Algorithm

Input: $f:\{1,2,\ldots..,N\} \rightarrow \{0,1\}$

Output:

Index which satisfies $f(p)= 1$ denoted as ω

Initialization:

1. Uniform superposition applied to system over all states

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{p=0}^{N-1} |p\rangle$$

Repeat the process $r(N) \sim \frac{\pi}{4}\sqrt{N}$ ***times where*** $N=2^n$

2. Define Oracle operator U_ω

U_ω is U_f when ancillary qubit is in the state

$|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$

Where,

$$U_f |p\rangle = (-1)^{f(p)} |p\rangle$$

3. Apply U_ω to qubit states

4. Define Operator U_s
5. Apply Grover's diffusion operator to qubit state

$$U_s = 2|s\rangle\langle s| - I$$

6. Measure resulting quantum state
7. End

4. Quantum Safe Algorithms

The various cryptographic algorithms which are available for providing security to confidential data work on either Symmetric key or Public key cryptography. All algorithms which fall under these categories are not susceptible to quantum attacks, some algorithms are considered to be quantum safe. By the term quantum safe we refer to the segment of those algorithms which can resist attacks that can be performed by all types of known quantum algorithms [9]. The algorithms which can easily be targeted and broken down by a quantum computer have the following characteristics:

1. Security protocols or algorithms working on the theories of Integer factorization and discrete logarithms.
2. Any algorithm or protocol which derives the security from the public key ciphers which use the complexities of the above stated theories.
3. Security systems or products which are in use by adapting to the security standards of above protocols.

It is important to note that RSA, Diffie Helman, ECDH, ECDSA, Digital signature Algorithm and other variants of these ciphers are not considered to be quantum safe [28]. Almost all public key ciphers use the theories of the above mentioned algorithms for providing security [9]. The algorithms that are considered to be vulnerable to quantum attacks but still can be rectified by certain way is the AES (Advanced Encryption Standard) algorithm. Table 2 shows the report released by NIST in 2016 on post quantum cryptography and effect of quantum computers on popular cryptographic algorithms [2]. In the quantum era the public key security models will stand insecure due to the issues of integer factorization and discrete log [10]. Whereas, in the case of symmetric key cryptographic methods Grover's algorithm as a quadratic speedup and it is relevant from the researches that exponential speedup for search algorithms is not possible [10].

Table 2 Impact of Quantum Computers on Classical and Common Cryptographic Algorithms

Algorithm	Encryption Type	Purpose	Impact Of Quantum Computer
AES	Symmetric Key	Encryption	Larger key sizes needed
SHA-2, SHA-3	Hash Function	Larger output needed	
RSA	Public key	Digital signatures, establishment of key	Not secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public Key	Digital signatures, establishment of key	Not secure
DSA (Finite Field Cryptography)	Public Key	Digital signatures, establishment of key	Not secure

Other public key security controls like RSA and ECC cannot resist the power of algorithms used by quantum computers because they cannot adapt to the security which can be ensured by increasing the key size of these security controls. If the key size of these algorithms is doubled then the run time capacity

of these public ciphers will increase by a factor of 8. This chain continues every time the key size is doubled due to the advancements the quantum computers will have in the coming future [38]. Rapid advancement in the run time of public ciphers by doubling the key size will transcend Moore's law and will soon become non-viable in terms of speed and channel size which is required to maintain the required bandwidth to transfer the key information over any electronic channel [19]. By increasing the key size used in AES encryption it can be ensured that AES can resist the quantum attacks. In the further sections of this paper this has been explained that AES-256 is considered to be quantum safe. Quantum resistant cryptography or post quantum cryptography aims at designing or identifying algorithms which are capable of securing the data even if a quantum computer is used to decrypt the data encrypted using those algorithms. The most popular communication channels encrypt the data by using public key encryption, digital signatures and algorithms which use the concept of key exchange. These techniques are primarily implemented using Diffie- Helman key exchange algorithm, Elliptic curve cryptography and Rivest-Shamir-Adleman (RSA) cryptography [31,20]. Symmetric key cryptography also termed as secret key cryptography is a method wherein a single key is used to encrypt and decrypt the data, therefore the sender and receiver should be aware of this key which is transmitted using a secure channel [21].

4.1 Quantum attacks

Quantum attack is a phenomena which aims at recovering the key faster than the classical search [40]. As in the case of classical search the key is recovered and calculated after searching all the possibilities but a Grover's algorithm working on the process of function inversion has to work only till $\sqrt{n}$ times where n is the possible number of outcomes [32]. IBM uses a quantum computer with 65 qubits and recently it has announced that by 2023 it will be successful in building a 1000 qubit quantum computer. Microsoft and Amazon have also announced their plan to accelerate their technology of cloud quantum computing. While the industry giants are working towards quantum computing it is believed that in next 20 years significantly large quantum computers using thousands of qubits will be able to break all public key cryptography algorithms currently in use [33]. Therefore we need to closely look at the algorithms which are quantum resistant regardless of the fact that we still cannot estimate the time by which quantum supremacy can actually be achieved [35][41].

4.2 Quantum Resistant Cryptography- Comparison Analysis

In Fig. 3 a comparison analysis has been done on the basis of qubits required to break the encryption provided by various symmetric and asymmetric key cryptographic methods [9]. It is stated that public key ciphers are not quantum secured but by using AES with a larger key size it becomes difficult for a quantum attack to break this algorithm. Therefore, it is considered that in applications where public key cryptography is favoured as compared to Symmetric key cryptography to outstrip the difficulty of key distribution and management, quantum resistant algorithms should be used as an substitute to safeguard the data and other confidential information which is transmitted over the electronic media. IBM has promised a quantum computer of 1000 qubits by the year 2023 and thus many other leading companies are also working towards achieving the quantum computer of a greater capabilities [12]. The cryptographic algorithms which are popularly used to build secure channels and provide security are vulnerable to quantum attacks. However, some algorithms can still be trusted for providing security based on their increased key size [11] [42][43].

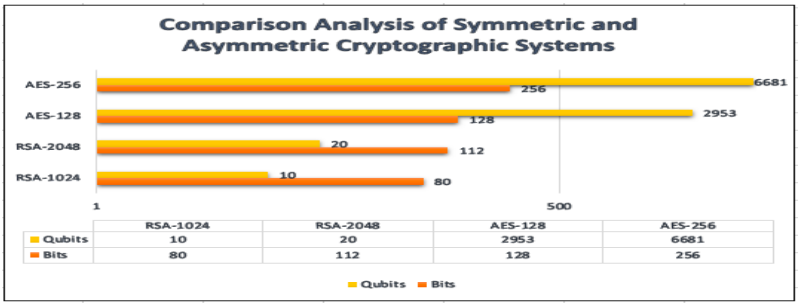

Fig. 3 Comparison analysis of Asymmetric vs Symmetric key cryptographic systems

5. Advanced Encryption Standard

Advanced Encryption standard (AES) was introduced in 2001 by NIST as a substitute to the Data Encryption standard (DES) as it was more susceptible to brute force attacks. AES is a symmetric block cipher encryption mechanism which is used to encrypt the sensitive and confidential data by implementing the encryption algorithm in hardware as well as in software across the world [44] [45].

5.1 Structure of AES

There are three block ciphers associated with the AES algorithm depending on the key length which is used by them: 128, 192 and 256. Each of these block ciphers use a single key of respective length to encrypt and decrypt the data [6]. AES has two version implementation [50][51][52].

1. Plain text block of 128 bit and 128 bit key size.
2. Plain text block of 128 bit and 256 bit key size.

In this paper we will be implementing AES-256 as it is considered to be more secured due to its large key size. It is important to note here that AES uses Galvois Field (2^8) to perform the arithmetic operations like addition, subtraction and multiplication. In case of AES encryption or decryption input size of 128-bit is used as a single block. A 4x4 square matrix of bytes is used for representation of this block. The block is then copied to the state array with modification which is performed at each step of AES encryption and decryption. The state is copied to the output matrix after the completion of last stage. In the similar manner the key is also represented as a square matrix of bytes and is further expanded. For key generation 15 subkeys are required for key length of 256 and are arranged in matrix of 4x8. Therefore, 60 word length key schedule is developed after the expansion of the key length of 256, while ordering of bytes in the matrices is by column.

Table 3 Key schedule for AES

Key Length	No. of Rounds	No. of sub keys	Required Iteration	Key length after expansion
128	10	11	10	44 words
192	12	13	8	52 words
256	14	15	7	60 words
512	16	17	4	68 words

In Table 3 it is important to note that as the key size increases the iterations required to generate the sub keys in AES decreases, this depends on the size of keys and the size of fixed block size. These keys are computed recursively [6]. The key schedule depicted in the table is represented in the word format where each word is 32 bit or 4 bytes and these sub keys are stored in an expansion array in the word format. As depicted in Table 3 there are 15 sub keys which are used for maintaining 14 rounds with 7 iterations required all sub keys are stored in key expansion array from W[0],W[1],….W[59]. To transform plain text into cipher text using AES encryption algorithm a series of steps which are constituted in a round are performed. These steps include Substitution using S-box, transposition and mix column operation to finally obtain the cipher text. In total the above steps are performed 10 times in case of key size 128 bit, 12 times when the key size is 192 bit and 14 times for 256 bit key size [46][47].

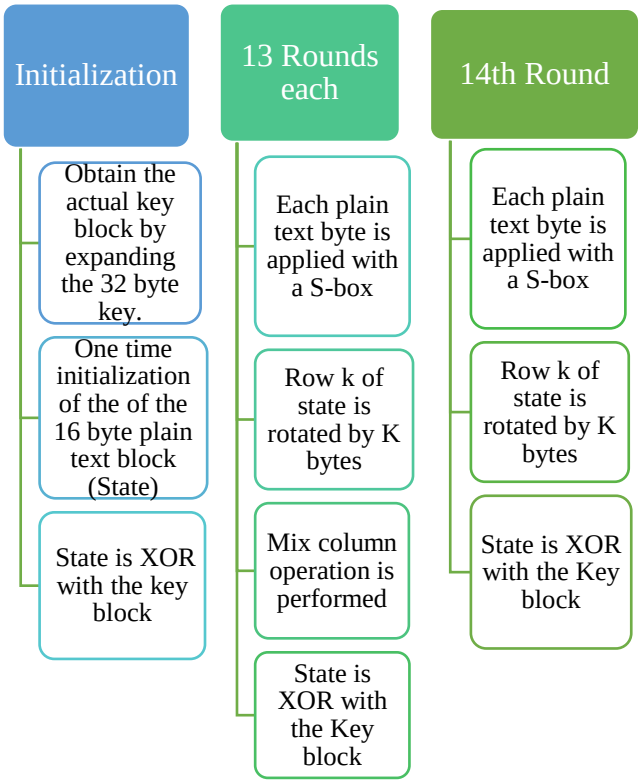

Fig. 4 AES-256 Description Flowchart

As the key size increases the number rounds increase which ensure more security to the data encrypted using this security mechanism. Fig. 4 shows the flowchart description of the various steps involved in implementing AES-256 [6]. To transform plain text into cipher text using AES encryption algorithm a series of steps which are constituted in a round are performed. These steps include Substitution using S-box, transposition and mix column operation to finally obtain the cipher text. In total the above steps are performed 10 times in case of key size 128 bit, 12 times when the key size is 192 bit and 14 times for 256 bit key size. As the key size increases the number rounds increase which ensure more security to the data encrypted using this security mechanism [48] [49].

6. AES-256: Quantum Safe Cryptographic Algorithm

The search which is performed by Grover's algorithm is much faster as compared to the classical computers. AES-256 is quantum resistant which can be proved by looking closely at the logic implemented by Grover's algorithm. As stated by Bennett, Bernstein, Brassard, and Vazirani, the proof that Grover's algorithm is asymptotically optimal is that there is no quantum solution available to a problem which can evaluate the problem in less than $O(\sqrt{n})$ time order [2]. The algorithm is considered as an quantum search algorithm which has a quadratic speed up factor of $2^{k/2}$, where k is the length of key or hash value in any cryptographic algorithm, which can be very efficient. Therefore, if the key size is doubled then the security of the various cryptographic algorithms can be secured. Grover's algorithm is used to implement function inversion by finding pre-image value of a function which is difficult to invert [53].

Let's consider a digital signature calculated by applying hash function on some data P = H(X), provided the hash function H(X) is implemented on a quantum computer, then by using Grover's algorithm we will be able to find X in time order $O(\sqrt{n})$ where n is the number of valid hashes calculated. Whereas, in classical computations brute force search is implemented which calculates the valid hashes in time order $O(n)$. This implies that if Grover's algorithm is used for finding all possible solutions to a 128 bit symmetric cryptographic key then 2^{64} computations will be required and for a cryptographic key algorithm which uses 256 bit then 2^{128} computations will be required [2]. Therefore, it can be stated that AES-256 is an quantum safe algorithm and can resist the quantum attacks till date.

7. Implementation Of AES-256

AES-256 is implemented using ASP.net in this paper. Visual studio 2019 has been used for the implementation and execution of code on a computer system of 4GB RAM and 64 bit Windows 10 operating system. ASP.net supports AES with key size of 128,192 and 256 [13]. By default the key size used in this case is AES-256.

1. Key Generation process- ASP.net supports AES with key size 128,192 and 256. 256 is the default key size which is implemented. While the key is transmitted, hash of the key needs to be generated since it's an symmetric key algorithm. For hash SHA-512 is used which increases the security of the key. A Pseudo code generation of describes the implementation of this process.
2. File Encryption- For encrypting the files using ASP.net RijndaelManaged class is used which cannot be inherited. In this step itself we will also consider the length of entire file which needs to be encrypted using the method *fsInput.Length*.
3. Scanning the entire file to be encrypted- The entire file will be scanned using the method declared in the previous step and the length of the file will be stored in a variable.
4. Deletion of Original file - Once the file has been encrypted then the unencrypted file will be deleted.
5. Update the user that the encryption has been done- For this step a message box is used which gives the message to the user about the encryption process completed.

Fig. 5 shows the pseudo flow chart for the procedure to be followed in ASP.net framework for completion of the above mentioned steps. The decryption process is only possible if the user has the key for decrypting the file. The time taken for this process to complete depends on some parameters like- system configuration, size of file to be encrypted and the RAM of the system. This can usually differ when the algorithm is executed on different platforms operating on different configurations and operating systems. The cryptographic algorithms which work on the theories of integer factorization and discrete logarithmic logic have more probability of being attacked by a quantum computer because the algorithms used by the quantum computers having large number of qubits have the capability of breaking down the cryptographic keys these popular algorithms use. Some of the algorithms which are more susceptible to such attacks are as follows: Digital signature Algorithm (DSA), Diffie Helman key exchange algorithm, RSA, Elliptic curve Diffie Helman and Elliptic curve Digital Signature Algorithm [25]. Advanced Encryption standard works on the capabilities of securing the key with a hash and then encrypting the files, therefore the security provided increases with the increase in key size. The cryptographic algorithms which are popularly used to build secure channels and provide security are vulnerable to quantum attacks. However, some algorithms can still be trusted for providing security based on their increased key size [11].

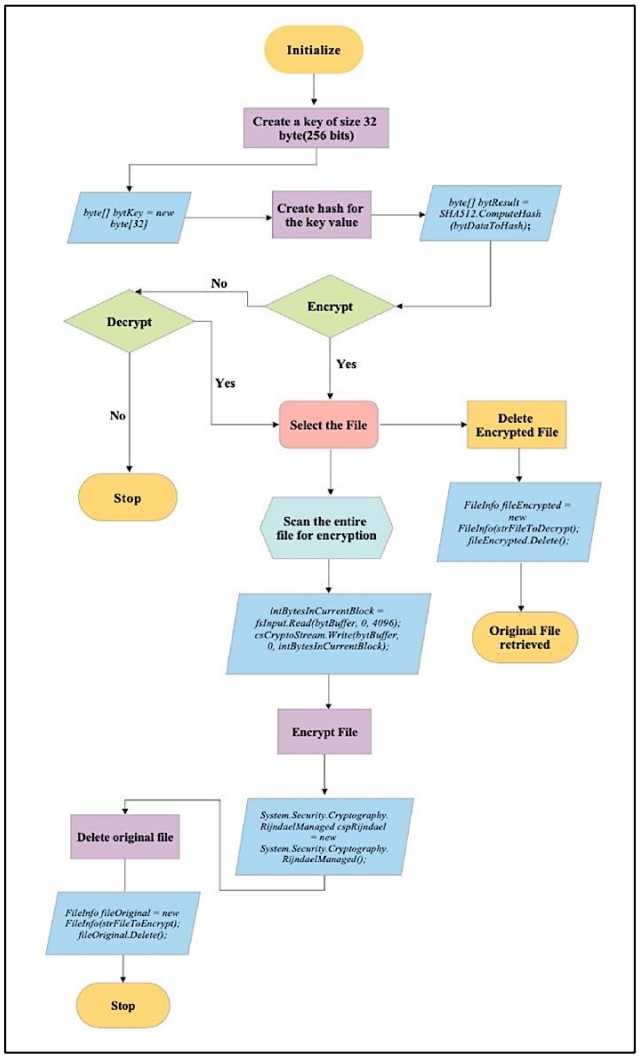

Fig. 5 Flow chart of Pseudo algorithm for AES-256

Algorithm 2: AES-256 Encryption

Input: File to be encrypted, Secret Key
Output: Encrypted file

Key Generation:

1. **Function**: *CreateKey(string strPassword)*
   Convert *strPassword* to an array and store in *chrData*
2. Declare hash to be used and store in *bytResult[]*
   System.Security.Cryptography.SHA512Managed()
3. Declare *bytKey[]*
4. Store first 256 bits of 512 to *bytKey[]*
5. for i = 0 to i <= 31
   bytKey[i] = bytResult[i]
6. return *bytKey*[]
7. Declare Initialization vector, *bytIV*

Encryption:

8. **Function:** *EncryptFile(string strInputFile,*

string strOutputFile, bytKey, bytIV, CryptoAction Direction)
9. Declare variables for encryption process
bytBuffer = new byte[4097]
10. Declare your Encryption scheme,
System.Security.Cryptography.RijndaelManaged
11. while *lngBytesProcessed < lngFileLength*
12. Read file with the input filestream.
fsInput.Read(bytBuffer, 0, 4096)
13. end while
14. Delete original file
fileEncrypted.Delete()
15. End

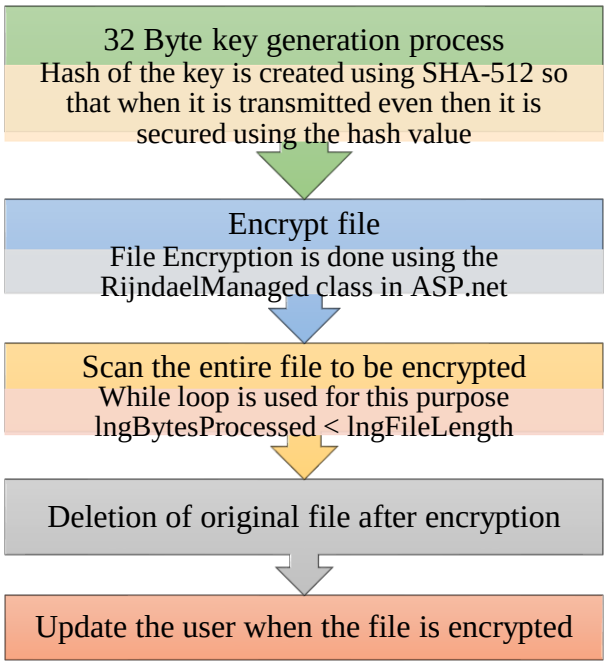

Fig. 6 Step wise implementation of AES-256 encryption algorithm

7.1 Implementation results

The process to be executed for encryption of files and data implemented using the pseudo code discussed in the previous section is shown in Fig. 7.

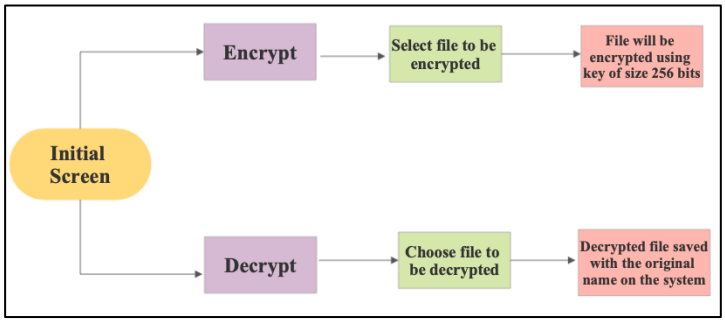

Fig. 7 Encryption and decryption process

A. Execution of the AES-256 Algorithm using ASP.net will display two options on the screen for encryption or decryption.

B. After clicking on the encrypt button any file can be selected which needs to be encrypted. The file content will be scanned entirely and the encrypted file will be stored in the same folder, the name of the new encrypted file can be selected by the user. A progress bar will show the progress of the file being encrypted and after process completion the message will be communicated to the user.

C. The encrypted file will not be opened by clicking on it until the decryption process is executed and the file is decrypted using the decrypt option of the initial screen.

7.2 Analysis of AES Encryption and Decryption

The estimated time in microseconds required to encrypt a file using AES is projected in Fig. 8. It shows the time required for encrypting file using key sizes-128,192 and 256. As per the analysis of the graph it can be stated that as the file size increases the time required for encryption also increases but still the process does not take much time even in conventional computer systems. Fig. 9 shows the time required in microseconds to decrypt a file encrypted using AES in classical computer system if the decryption key is known. The estimated time required to decrypt a large file is greater as compared to a file of smaller size.

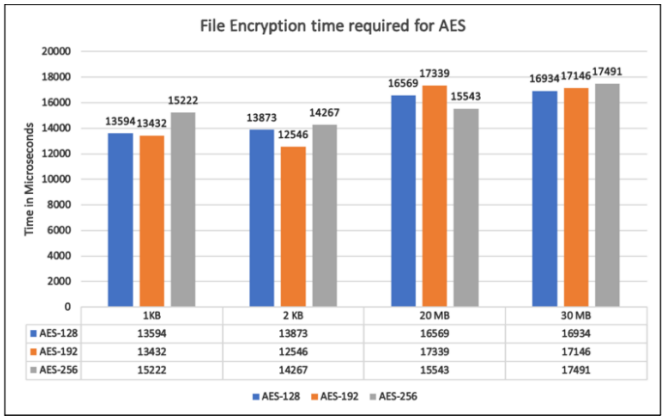

Fig. 8 Estimated file encryption time by AES

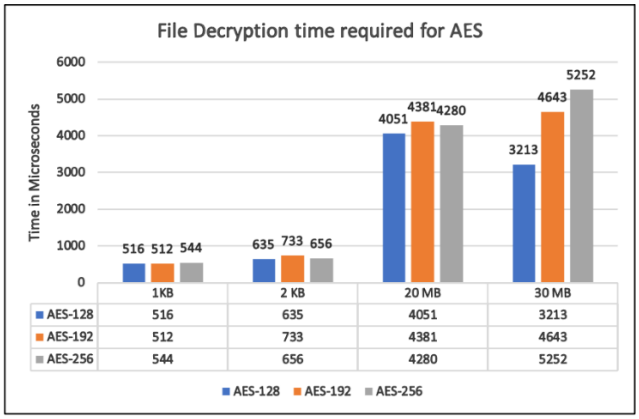

Fig. 9 Estimated file decryption time by AES

8. Conclusion

Researchers are constantly working on the development of mechanisms and also on the capabilities of the quantum computer to break those mechanisms so that the limitation of known attacks do not yield us in further difficulties. In this paper we have discussed about many such security schemes and their susceptibility to the known quantum attacks. According to a study published by the researchers of a encryption focused Canadian Company- Kryptera in 2019, a Quantum computer with 2953 logical qubits can break AES-128 and for breaking down AES-256 a quantum computer with 6681 logical qubits will be required which is so far not achieved by any leading companies working on quantum

computers. A comparison analysis is also Therefore, in the quantum era the secret key algorithm- AES-256 is considered to be safe if the key size is increased which also ensures its security against the attacks which are possible on the classical computers. Further, the implementation results of AES-256 shows that it is capable of encrypting files on the system with a strong encryption scheme and cannot be decrypted if the key is not known. The time required to encrypt and decrypt the files in a traditional computer system is also computed after the implementation. The parameters which affect the overall functioning and time required to encrypt the files in the system include the size of file and specifications of the system being used for both encryption and decryption process.

9. Future Scope

Quantum supremacy is still to be achieved by the companies working towards it, however Google in 2019 declared that it has reached quantum supremacy with it's quantum computer Sycamore which uses 53 Qubits to perform the tasks. It was stated by google that Sycamore has solved problems which are virtually impossible to solve using the most efficient classical supercomputers. It successfully completed a complex computation in 200 seconds which would take 10,000 years to finish by using the most powerful supercomputer as stated by a team of researchers working on this in a study published in journal Nature. With the advent of quantum era, other security applications and technologies like blockchain can also be susceptible to attacks by the quantum computer since the hash values which are calculated for ensuring the security of the blockchain can easily be calculated with the algorithms used by quantum computer. Therefore, a security mechanism and cryptographic schemes can be built by using AES-256 which can enhance the security of the technologies working for ensuring security for various systems like cloud technologies and increase their security to overcome the challenges which might lead to the data to be insecure in future.

Conflict of Interest

The Authors declare no conflict of interest.

References

[1] Gorjan Alagic (NIST), Jacob Alperin-Sheriff (NIST), Daniel Apon (NIST) et. al. "Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", NISITIR 8309, NIST, U.S. Department of Commerce, July 2020 [online]. Available: https://doi.org/10.6028/NIST.IR.8309

[2] Sandeep Kumar Rao, Dindayal Mahto, Dr. Dilip Kumar Yadav and Dr. Danish Ali Khan, "The AES-256 Cryptosystem Resists Quantum Attacks", International Journal of Advanced Research in Computer Science, 8 (3), March-April 2017, 404-408.

[3] X. Bonnetain, M. Naya-Plasencia, and A. Schrottenloher, "Quantum Security Analysis of AES", *ToSC*, vol. 2019, no. 2, pp. 55-93, Jun. 2019.

[4] Brandon Rodenburg and Stephen P. Pappas," Blockchain and Quantum Computing", MITRE, Case Number 17-4039 ,2017.

[5] Awadhesh Kumar and R.R. Tewari," Expansion of Round Key Generations in Advanced Encryption Standard for Secure Communication", International Journal of Computational Intelligence Research ISSN 0973-1873 Volume 13, Number 7 (2017), pp. 1679-1698.

[6] Deepraj Soni, Kanad Basu, Mohammed Nabeel and Ramesh Karri, " A Hardware Evaluation Study of NIST Post-Quantum Cryptographic Signature schemes", CSRC, NIST, 2019.

[7] Stephan S. Clarke, "Quantum Computing: A Mathematical Analysis of Shor's Algorithm", DigitalCommons@SHU, Sacred Heart University, 2020.

[8] Mandviwalla, A., Ohshiro, K., & Ji, B., "Implementing Grover's Algorithm on the IBM Quantum Computers", IEEE International Conference on Big Data (Big Data), 2018. doi:10.1109/bigdata.2018.8622457

[9] Matthew Campagna et. al., "Quantum Safe Cryptography and Security-An introduction, benefits, enablers and challenges", ETSI (European Telecommunications Standards Institute), White paper, 2018. ISBN No. 979-10-92620-03-0.

[10] Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner, Daniel Smith-Tone, "Report on post quantum cryptography", NISTIR 8105, NIST, U.S. Department of Commerce, April 2016 [online]. Available: http://dx.doi.org/10.6028/NIST.IR.8105.

[11] Craig Gidney and Martin Eker̊a, " How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Quantum-The open journal for quantum science, 2021.

[12] Adrian Cho, "IBM promises 1000-qubit quantum computer—a milestone—by 2023",

Science. https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023 (accessed 15,september,2020).

[13] Stallings, W.: Cryptography and network security: principles and practices. Pearson Education India, 2006.

[14] Arute, F., Arya, K., Babbush, R. *et al.* Quantum supremacy using a programmable superconducting processor. *Nature* **574,** 505–510 (2019). https://doi.org/10.1038/s41586-019-1666-5.

[15] Richard Evers, Alastair Sweeny, "Reducing the Time to Break Symmetric Keys", ISBN: 978-1-927736-35-7 , March 2019 [online]. Available: https://kryptera.ca/paper/2018-03/

[16] Moolchand Sharma , Vikas Choudhary , R. S. Bhatia , Sahil Malik , Anshuman Raina & Harshit Khandelwal (2020): Leveraging the power of quantum computing for breaking RSA encryption, Cyber-Physical Systems, DOI: 10.1080/23335777.2020.1811384

[17] Yu-Long Gao, Xiu-Bo Chen, Yu-Ling Chen, Ying Sun, Xin-Xin Niu And Yi-Xian Yang, "A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain", Special Section On The Internet Of Energy: Architectures, Cyber Security, And Applications (Part II), IEEE access, Volume 6, 2018.

[18] Wicaksana, Arya & Anthony, Anthony & Wicaksono, Adjie. (2020). Web-app realization of Shor's quantum factoring algorithm and Grover's quantum search algorithm. TELKOMNIKA (Telecommunication Computing Electronics and Control). 18. 1319. 10.12928/telkomnika.v18i3.14755.

[19] Bernstein D.J. (2009) Introduction to post-quantum cryptography. In: Bernstein D.J., Buchmann J., Dahmen E. (eds) Post-Quantum Cryptography. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-88702-7_1

[20] Braeken, A. Public key versus symmetric key cryptography in client–server authentication protocols. Int. J. Inf. Secur. (2021). https://doi.org/10.1007/s10207-021-00543-w

[21] Tawfeeq M. Tawfeeq Al-Flaih and Marwa Adeeb Al-jawaherry, " Design and implementation elliptic curve digital signature algorithm using multi agent system ", International Journal of Computer Science and Information Security (IJCSIS), Vol. 15, No. 12, December 2017.

[22] Sattath, O. On the insecurity of quantum Bitcoin mining. Int. J. Inf. Secur. 19, 291–302 (2020). https://doi.org/10.1007/s10207-020-00493-9

[23] Samir El Adib and Naoufal Raissouni, "AES Encryption Algorithm Hardware Implementation Architecture: Resource and Execution Time Optimization", International Journal of Information & Network Security (IJINS),Vol.1, No.2, June 2012, pp. 110-118, ISSN: 2089-3299.

[24] Das, A.K. A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks. Int. J. Inf. Secur. 11, 189–211 (2012). https://doi.org/10.1007/s10207-012-0162-9

[25] Priyadarshini Patil, Prashant Narayankar, Narayan D.G., Meena S.M.,A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish, Procedia Computer Science, Volume 78,2016,Pages 617-624,ISSN1877-0509, https://doi.org/10.1016/j.procs.2016.02.108.(https://www.sciencedirect.com/science/article/pii/S1877050916001101)

[26] Jaques S., Naehrig M., Roetteler M., Virdia F. (2020) Implementing Grover Oracles for Quantum Key Search on AES and LowMC. In: Canteaut A., Ishai Y. (eds) Advances in Cryptology – EUROCRYPT 2020. EUROCRYPT 2020. Lecture Notes in Computer Science, vol 12106. Springer, Cham. https://doi.org/10.1007/978-3-030-45724-2_10

[27] Abdullah, AkoMuhamad. "Advanced encryption standard (aes) algorithm to encrypt and decrypt data." Cryptography and Network Security 16 (2017).

[28] Grassl M., Langenberg B., Roetteler M., Steinwandt R. (2016) Applying Grover's Algorithm to AES: Quantum Resource Estimates. In: Takagi T. (eds) Post-Quantum Cryptography. PQCrypto 2016. Lecture Notes in Computer Science, vol 9606. Springer, Cham. https://doi.org/10.1007/978-3-319-29360-8_3

[29] A. Mandviwalla, K. Ohshiro and B. Ji, "Implementing Grover's Algorithm on the IBM Quantum Computers," 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 2531-2537, doi: 10.1109/BigData.2018.8622457.

[30] de Lima Marquezino F., Portugal R., Lavor C. (2019) Grover's Algorithm for Unstructured Search. In: A Primer on Quantum Computing. SpringerBriefs in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-030-19066-8_3

[31] Nene M.J., Upadhyay G. (2016) Shor's Algorithm for Quantum Factoring. In: Choudhary R., Mandal J., Auluck N., Nagarajaram H. (eds) Advanced Computing and Communication Technologies. Advances in Intelligent Systems and Computing, vol 452. Springer, Singapore. https://doi.org/10.1007/978-981-10-1023-1_33

[32] Bonnetain X., Naya-Plasencia M., Schrottenloher A. (2020) On Quantum Slide Attacks. In: Paterson K., Stebila D. (eds) Selected Areas in Cryptography – SAC 2019. SAC 2019. Lecture Notes in Computer Science, vol 11959. Springer, Cham. https://doi.org/10.1007/978-3-030-38471-5_20

[33] Dong, X., Dong, B. & Wang, X. Quantum attacks on some feistel block ciphers. Des. Codes Cryptogr. 88, 1179–1203 (2020). https://doi.org/10.1007/s10623-020-00741-y

[34] Băetu C., Durak F.B., Huguenin-Dumittan L., Talayhan A., Vaudenay S. (2019) Misuse Attacks on Post-quantum Cryptosystems. In: Ishai Y., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science, vol 11477. Springer, Cham. https://doi.org/10.1007/978-3-030-17656-3_26

[35] Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt & Gerd Leuchs (2016) Attacks on practical quantum key distribution systems (and how to prevent them), Contemporary Physics, 57:3, 366-387, DOI: 10.1080/00107514.2016.1148333

[36] Xavier Bonnetain, María Naya-Plasencia, André Schrottenloher. Quantum Security Analysis of AES. IACR Transactions on Symmetric Cryptology, Ruhr Universität Bochum, 2019, 2019 (2), pp.55-93. ⟨10.13154/tosc.v2019.i2.55-93⟩

[37] S. Guerrini, M. Chiani and A. Conti, "Secure Key Throughput of Intermittent Trusted-Relay QKD Protocols," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-5, doi: 10.1109/GLOCOMW.2018.8644402.

[38] Shivlal mewada, Pradeep Sharma and S. S. Gautam, " Classification of Efficient Symmetric Key Cryptography Algorithms", International Journal of Computer Science and Information Security, Vol. 14, No. 2, Feb 2016.

[39] Mark Kristian C. Ledda, Bobby D. Gerardo, Alexander A. Hernandez, "Enhancing IDEA Algorithm using Circular Shift and Middle Square Method", ICT and Knowledge Engineering (ICT&KE) 2019 17th International Conference on, pp. 1-6, 2019.

[40] Li, R., Jin, C. Meet-in-the-middle attacks on 10-round AES-256. Des. Codes Cryptogr.80, 459–471 (2016). https://doi.org/10.1007/s10623-015-0113-3

[41] Narayan, Vipul, and A. K. Daniel. "FBCHS: Fuzzy Based Cluster Head Selection Protocol to Enhance Network Lifetime of WSN." ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 11.3 (2022): 285-307.

[42] Awasthi, Shashank, et al. "A Comparative Study of Various CAPTCHA Methods for Securing Web Pages." 2019 International Conference on Automation, Computational and Technology Management (ICACTM). IEEE, 2019.

[43] Irfan, Daniyal, et al. "Prediction of Quality Food Sale in Mart Using the AI-Based TOR Method." Journal of Food Quality 2022 (2022).

[44] Narayan, Vipul, and A. K. Daniel. "Novel protocol for detection and optimization of overlapping coverage in wireless sensor networks." Int. J. Eng. Adv. Technol 8 (2019).

[45] Narayan, Vipul, et al. "To Implement a Web Page using Thread in Java." (2017).

[46] Narayan, Vipul, and A. K. Daniel. "A novel approach for cluster head selection using trust function in WSN." Scalable Computing: Practice and Experience 22.1 (2021): 1-13.

[47] Choudhary, Shubham, et al. "Fuzzy approach-based stable energy-efficient AODV routing protocol in mobile ad hoc networks." Software Defined Networking for Ad Hoc Networks. Cham: Springer International Publishing, 2022. 125-139.

[48] Narayan, Vipul, and A. K. Daniel. "Energy Efficient Protocol for Lifetime Prediction of Wireless Sensor Network using Multivariate Polynomial Regression Model." Journal of Scientific & Industrial Research 81.12 (2022): 1297-1309.

[49] Narayan, Vipul, and A. K. Daniel. "Design consideration and issues in wireless sensor network deployment." (2020): 101-109.

[50] Vimal Kumar and RakeshKumar, "An Optimal Authentication Protocol using Certificateless ID- based Signature in MANET "Book Chapter publication in Springer, CCIS series, Vol.536, pp.110-121, 2015.

[51] Vimal Kumar and Rakesh Kumar, "Prevention of Blackhole Attack using Certificateless Signature (CLS) Scheme in MANET," Book Chapter publication in IGI-Global Advances in Information Security, Privacy, and Ethics (AISPE) series, pp.130-150, 2016.

[52] Vimal Kumar and Rakesh Kumar, "An Adaptive Approach for Detection of Black hole in Mobile Ad hoc Network," Procedia Computer Science, Elsevier, vol.48, pp. 472-479, Dec. 27-28, 2014.

[53] Kumar, Vimal, Mahima Shankar, Aanjay Mani Tripathi, Vikash Yadav, Anjani Kumar Rai, Uzair Khan, and Mayur Rahul. "Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme." Journal of Scientific & Industrial Research 81, no. 10 (2022): 1061-1072.