Volume 8, No. 3, March – April 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

The AES-256 Cryptosystem Resists Quantum Attacks

Sandeep Kumar Rao*, Dindayal Mahto, Dr. Dilip Kumar Yadav and Dr. Danish Ali Khan
Department of Computer Applications,
National Institute of Technology, Jamshedpur India

Abstract: Privacy of information can be maintained using two cryptographic techniques i.e. symmetric key cryptography and asymmetric key cryptography. For securing data using symmetric key cryptography, Advanced Encryption Standard (AES) is one of the trusted cryptographic algorithms. AES is a block cipher based symmetric key cryptographic algorithm which can resist conventional computers as well as quantum computers. In recent years, many researches have been done that exploit the property of quantum mechanics to solve mathematical problems that are ever difficult for conventional computers. Many of the cryptographic algorithms can be broken if large scale quantum computers are ever made. This paper depicts the proof of AES-256 using Grover's algorithm which can resist quantum.

***Keywords*:** AES,RSA, ECC, Quantum Key Distribution (QKD), Quantum bit commitment, Quantum Cryptography.

I. INTRODUCTION

Today, we are living in the era of information technology where securing the sensitive information is very crucial matter. Many of cryptographic algorithms (symmetric key based and asymmetric key based) are available for providing better protection to the sensitive information. AES being a block cipher based symmetric key cryptography algorithm which is used for (Encryption/Decryption) of information for providing the confidentiality and integrity to the data. The key sizes of AES is 128, 192 and 256 bits for 10, 12, and 14 round respectively. AES-128 bit is sufficient for securing the information to the conventional computers. AES-128 bit is difficult to break by classical computers as it requires 5×10^{21} years, but in post quantum computing era, AES-128 may be broken. However, as per Grover's algorithm, AES-256 cannot be broken by quantum computer.

Modern conventional cryptosystems are based on mathematical models which introduce security holes in the systems, related to increasing in the power of computers. For this reason various research and effort has been made for creating a new foundation for cryptographic system i.e. Quantum cryptography. Quantum cryptography technology is totally depends on law of quantum mechanics.

This paper's motive is to present how symmetric key based AES-256 can exist in quantum cryptographic system.

II. ADVANCED ENCRYPTION STANDARD (AES)

In 2001, Advanced Encryption Standard was published by the National Institute of standard and Technology (NIST). It is a symmetric block cipher that is proposed to replace the Data Encryption Standard (DES) as the accepted standard for extensive range of applications. All operations are performed on 8-bit bytes in AES. The arithmetic operations of addition, multiplication and division are performed over the Galvois Field (2^8).

General Structure

The AES is referred as AES-128, AES-192, or AES-256, which is based on key length. AES encryption takes a plaintext block size of 128 bits or 16 bytes. The key size of algorithm can be 16, 24, or 32 bytes (128,192, or 256 bits). The input size to the (encryption / decryption) is a single 128-bit block. This block is represented as a 4×4 square matrix of bytes. This block is copied to the state array and it is modified at each stage of (encryption / decryption). After the last stage, state is copied to the output matrix.

Similarly, key is also represented as square matrix of bytes and key is expanded as a key schedule words. The total key schedule is 44 words for 128-bit key and the ordering of bytes in the matrix is by column. The cipher contains N rounds depending on key length i.e. 10, 12 and 14 rounds for 128-bit, 192-bit, and 256-bit key respectively.

The AES Encryption involves following steps:

1. Initial Round: AddRoundKey
2. Rounds: SubBytes, ShiftRows, MixColumns, and AddRoundKey
3. Last Round: SubBytes, ShiftRows, and AddRoundKey

Figure 1 shows the overall Encryption and Decryption of AES and [17, 20] can be referred for all the details.

In further section, it can be seen that AES-256 is Quantum resistant cryptographic algorithm.

III. QUANTUM COMPUTING

In recent years, there have been many researches done on quantum computers that exploit the quantum mechanical phenomenon for solving the mathematical problems which are difficult for conventional computers [7].

In 1994, Peter Shor's algorithm showed that a new technology, quantum computers exploiting the physical properties of matter and energy to perform calculation [19].

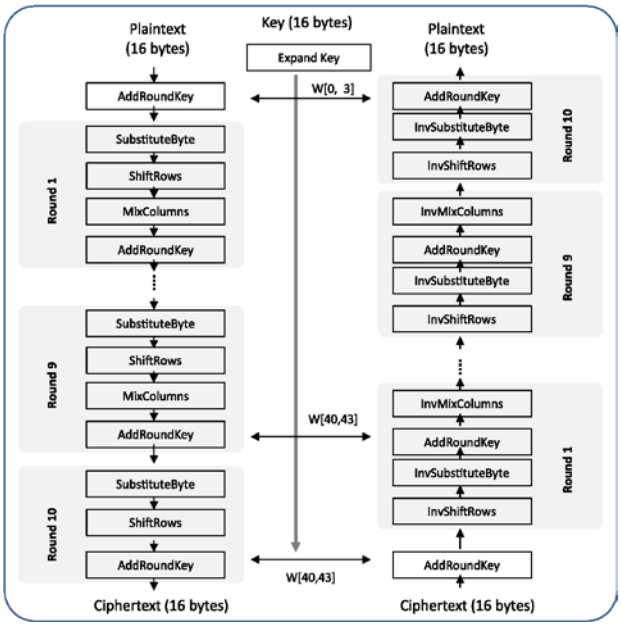

Figure 1: AES Encryption and Decryption

Before Shor's algorithm, it was not clear that quantum computers are physical possibility but now scientists believe that it is a merely a significant challenge. Some experts even predict that within next 20 years or so years, sufficiently large quantum computer will be built [16].

Effect of Quantum Computing

After the discovery of Shor's algorithm, Quantum algorithm gaining exponential speed up for several problems like physics simulation, number theory and topology. And many speed-ups have been made for different class of problems i.e. searching, collision finding and Boolean function's evaluations. In this case, Grover's search algorithm provides quadratic speed-up for unstructured search problems [10]. However, this speedup does not make cryptographic system outdated; it may have the effect of requiring larger key size even in symmetric key cryptography.
It can be clearly understand by the Table 1, which cryptographic algorithm is affected and also which one requires larger key sizes.

Table 1: Impact of Quantum computer on Cryptographic algorithm

Cryptographic Algorithm	Type	Purpose	Effect of Quantum Computer
AES	Symmetric Key	Encryption/Decryption	Larger Key size needed
RSA	Public Key	Signature, Key establishment	No Longer Secured
SHA-2, SHA-3	Hash Function		Larger Output needed
Elliptic Curve Cryptography	Public Key	Signature, Key exchange	No Longer Secured
DSA (Finite Field Cryptography)	Public Key	Signature, Key exchange	No Longer Secured

IV. QUANTUM CRYPTOGRAPHY

Quantum cryptography can be also referring as "Quantum key Distribution". Since increasing use of communication network technology also increase computer abuses and security problems. Modern digital network technology is totally depends on conventional cryptographic system to protect the confidentiality and integrity of data across the network.

Most of the cryptographic algorithms are based on factorizing the integers into the prime which is intractable but these cryptographic algorithms lead to security holes by the increasing of computing power.

For that reason many research has been done and also is going on to establish the new foundation of cryptographic science in communication network technology that is quantum cryptography.

Quantum cryptography's security exploits the law of quantum mechanics [2, 3, 4]. The concept of quantum cryptography is developed by Charles H. Bennett and Gilles Brassard in 1984 (BB84) as a part of research between physics and information at IBM [8]. This was the first quantum distribution scheme.

Quantum cryptography relies on the two pillars of quantum mechanics:

- **The Heisenberg Uncertainty principle –** there is no possibility of measurement of the quantum state of the system without disturbing that system.
- **Photon polarization principle-** it specify the orientation or polarization of light photons in specific direction.

Heisenberg Uncertainty principle prevents the attempts of eavesdropper in a cryptosystem using quantum cryptography.

In Photon polarization principle, a photon filter with correct polarization can detect the polarized photon otherwise it will be destroyed (no-cloning theorem).

According to Bennett and Brassard, an encryption key is created depending on the amounts of photon reaching to recipient and how it is received.

Here the fact is that light can behave as the characteristics of particles rather than light waves. The photon can be polarized at different orientation and these can be used to represent the bits which are in the form of 0 and 1. The

representation of bits through polarized photons led to the foundation of quantum cryptography which comes as the underlying principle of quantum key distribution.

A. Quantum Key Distribution (QKD)

Quantum cryptography's main motive is to securely distributing the key. It allows a bit string to be agreed between two parties using BB84 protocol[9] in which it establish a common key sequence with the help of polarized photon[8]. Each of photon is in a state and can be represented by four symbols, which are mentioned in Fig.2.

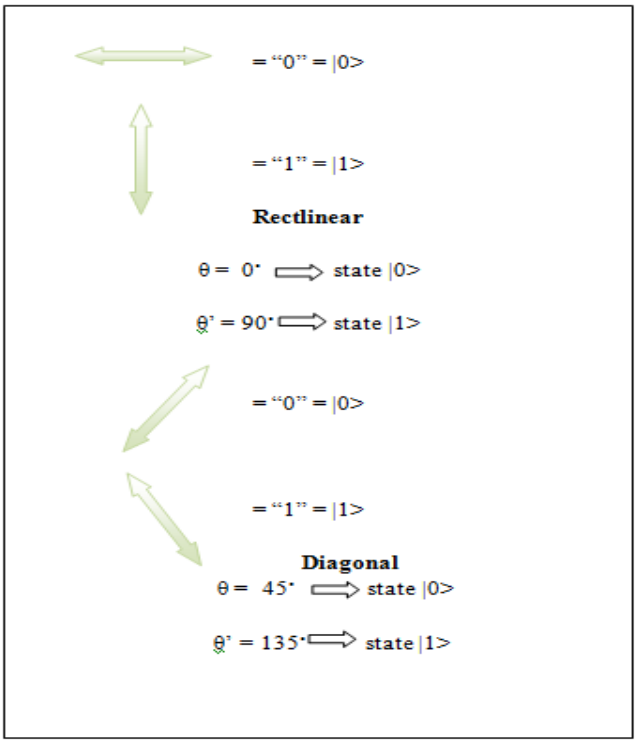

Figure 2: Photon symbols

—, |, /, \, In this first two photon state is emitted by a polarizer with rectilinear orientation and other two photon state is emitted by a polarizer with a diagonal orientation[4].
For example: +(0)= — , +(1)= | , x(0)=/, x (1)= \
Here +, as a horizontal-vertical detector basis and x, as a diagonal detector basis.

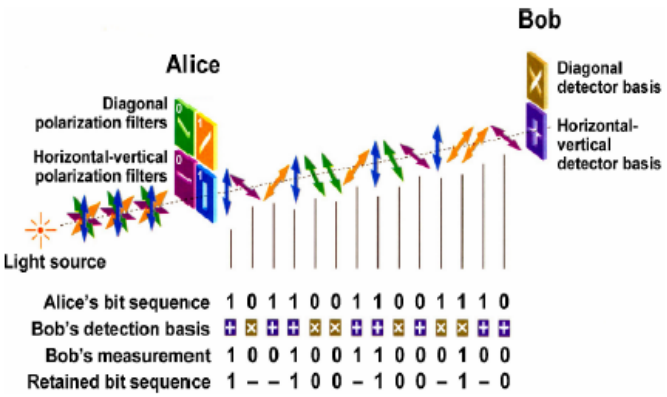

Figure 3: Communication of photon [18]

In Figure 3 Alice sends random sequence of photons and if Bob wants to get binary number send by Alice, he needs to get each photon on the same basis.

In this case Eavesdropping is impossible because a qubit cannot be copied (no-cloning theorem). For more details [4, 18] can be referred about key distribution.
The Quantum key distributed as follow:

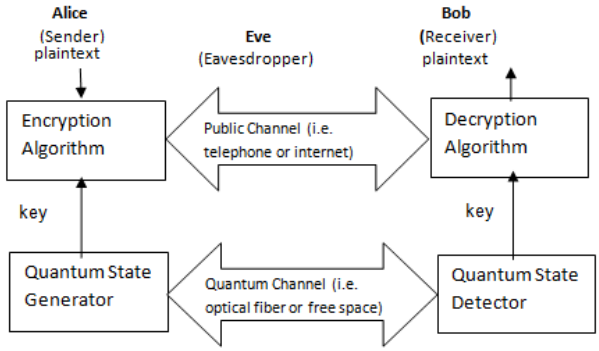

Figure 4: Distributing key over quantum channel

It is clear from the Figure 4, that in quantum cryptography, Alice sends encrypted information via public channel (Internet or Intranet) and sends secret key via quantum channel (optical fiber or free space) using QKD protocol.

B. Quantum-resistant cryptographic algorithm

Most of security protocols and cryptographic algorithm are vulnerable to attacks but some can be still believed to be safe from quantum attacks.

Following are the security protocols or algorithms that are highly vulnerable to quantum attacks:

The cryptosystem which is built on the mathematical complexities of integer factoring and discrete logarithms are more susceptible to quantum attacks example: RSA, Digital Signature Algorithms, Diffie Hellman Key Exchange, Elliptic Curve Diffie-Hellman, Elliptic Curve Digital Signature Algorithm and others. Almost all type of today's public key cryptography in the field of security products and protocols uses these types of ciphers. A security analysis of ECC and RSA using classical computer has been shown and said that ECC is efficient than RSA [12-15]. However ECC is also not a quantum-resistant.

However, there are some classes of cryptographic systems which are beyond RSA, DSA and ECDSA, are quantum-resistant [5]. List of quantum-resistant cryptography schemes are mentioned below:

- **Hashed-based cryptography:** Merkle's hash-tree public-key signature system which is built on a one-message signature idea of Lamport and Diffie (1979).
- **Code based cryptography:** McEliece's Goppa code public key encryption system (1978).
- **Lattice-based cryptography:** Hoffstien-Pipher-Silverman "NTRU" public key encryption system (1998).
- **Multivariate-quadratic-equations cryptography:** Patarin's "HFE^{v}" public-key signature system (1996), which generalized the proposal given by Matsumoto and Imai.
- **Secret-key cryptography:** Rijandael's cipher (1998) renamed as "AES" AES is an example of symmetric key cryptographic algorithm.

C. Security challenges to quantum cryptography

There are some certain numbers of challenges to quantum cryptography [6].

- **Impossibility of quantum bit commitment:** Bit commitment captures the functionality of two-party. In bit commitment, Alice send bit "b" to Bob, but she wants to prevent Bob from reading until she reveal it by concealing or hiding.
- **Impossibility of securing two-party computation:** If there is a leakage in any quantum protocol, it will be very bad even after approximate correctness and security.
- **Zero-knowledge against quantum adversaries:** Quantum rewinding is impossible in quantum cryptography because of the no-cloning theorem.

V. AES: QUANTUM-RESISTANT CRYPTOGRAPHY

AES is quantum resistant that can be proved by Grover's algorithm [1, 10]. Grover's algorithm is a quantum algorithm which finds out the particular output value with a high probability to a given input value into a black box function using just O($\sqrt{N}$) evaluation of function, where N is the size of function domain. A general computation can't solve a problem in a fewer than O(N) because in worst case scenario, the Nth member will be the correct member.

According to Bennett, Bernstein, Brassard, and Vazirani [1], it is proved that there is no quantum solution to the problem which evaluates the function fewer than O($\sqrt{N}$) times and it also proves that Grover's algorithm is asymptotically optimal. Grover's algorithm provides quadratic speedup rather than exponential speedup. Using Grover's algorithm, 128-bit symmetric cryptographic key can take roughly a 2^{64} iteration and a 256-bit key can take 2^{128} iteration.

As a result, AES with 256 bits key can resist to quantum attacks.

From the above description it can be said that **AES** which is block cipher based symmetric key algorithm developed by Rijndael is totally quantum safe.

VI. COMPARISONS OF AES TO OTHER CRYPTOGRAPHIC SYSTEM

Now it is clear that AES is quantum safe cryptographic system. From the Table 2, it can be observed that at what extent AES is quantum safe [11].

Table 2: Comparison of AES to other cryptographic system in conventional and quantum security level

Algorithm	Key Length	Key Strength/ Security Level	
		Classical Computing (bits)	Quantum Computing (bits)
AES-128	128 bits	128	64
AES-256	256 bits	256	128
RSA-1024	1024 bits	80	0
RSA-2048	2048 bits	112	0
ECC-256	256 bits	128	0
ECC-384	384 bits	256	0

VII. CONCLUSION

This paper studies the quantum resistance techniques for AES-256. Some of the popular public key cryptographic techniques like RSA, ECC, can be broken on quantum computing based on shor's algorithm [19]. As per the Grover's algorithm [10], some of the popular symmetric key cryptographic techniques like DES, AES-128, IDEA, can also be broken on quantum computing.

However, AES-256 can resist quantum computing attacks [10]. Comparison analysis shows that the difficulty level for breaking the AES-128 bit on conventional computers is same as the difficulty level for breaking the AES-256 on quantum computers.

In nutshell, AES-256 will not be breakable in post quantum computing era.

VIII. REFERENCES

[1]. Bennett C.H., Bernstein E., Brassard G., Vazirani U. (1997).: The strengths and weaknesses of quantum computation. SIAM Journal on Computing. 26(5): 1510–1523.

[2]. Bennett, C. H.: Quantum cryptography using any two non-orthogonal states. Physics Review Letter, 68, 1992 p. 3121-3124.

[3]. Bennett, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J.: Experimental quantum cryptography. Journal of Cryptology, 5(1), 1992 p. 3-28.

[4]. Bennett, Ch. H., & Brassard, G.: Quantum cryptography: public key distribution and coin tossing. IEEE Conference on Computer, Systems, and Signal Processing, 1984, pp. 175-90.

[5]. Bernstein, D.J., Johannes, B., and Erik, D., eds.: Post-quantum cryptography. Springer Science & Business Media, 2009.

[6]. Broadbent, A., and Christian, S..: Quantum cryptography beyond quantum key distribution. Designs, Codes and Cryptography 78.1 (2016): 351-382.

[7]. Chen, L., et al.: Report on post-quantum cryptography. National Institute of Standards and Technology Internal Report 8105 (2016).

[8]. Elliot, C.: Quantum Cryptography. IEEE Security & Privacy Journal, 2004, pp. 57-61.

[9]. Gisin, N., et al.: Quantum cryptography. Reviews of modern physics 74.1 (2002): 145.

[10]. Grover, L. K.: From Schrödinger's equation to the quantum search algorithm. American Journal of Physics 69.7 (2001): 769-777.

[11]. http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf.

[12]. Mahto, D., Khan, D. A., and Yadav, D. K.: Security Analysis of Elliptic Curve Cryptography and RSA. Proceedings of the World Congress on Engineering. Vol. 1. 2016.

[13]. Mahto, D. and Yadav, D. K. "Enhancing security of one-time password using Elliptic Curve Cryptography with biometrics for e-commerce applications," Proc. of the 2015 Third International Conference on Computer, Communication, Control and Information Technology (C3IT), Hooghly, 2015, pp. 1-6.

[14]. Mahto, D. and Yadav, D. K., "Enhancing security of one-time password using Elliptic Curve Cryptography with finger-print biometric," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 1737-1742.

[15]. Mahto D., Yadav D.K., "Security Improvement of One-Time Password Using Crypto-Biometric Model" In: Nagar A., Mohapatra D., Chaki N. (eds) Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics. Smart Innovation, Systems and Technologies, vol 44. Springer, New Delhi

[16]. M. Mosca, Cybersecurity in an era with quantum computers: will we be ready? IACR Cryptology ePrint Archive Report 2015/1075, 2015. http://eprint.iacr.org/2015/1075.

[17]. Rao, S.K., Mahto, D., and Khan, D. A.: A Survey on Advanced Encryption Standard. International Journal of Science and Research, Vol. 6(1), pp. 711-724, 2017

[18]. Sharbaf, M.S.: Quantum cryptography: An emerging technology in network security. Technologies for Homeland Security (HST), 2011 IEEE International Conference on. IEEE, 2011.

[19]. Shor, P.: Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. SIAM J. Comput., 26 (5), 1997, pp. 1484–1509. http://dx.doi.org/10.1137/s0036144598347011.

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