International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.219-232
http://dx.doi.org/10.14257/ijsia.2017.11.1.18

Enhancing the Security of AES Algorithm using Quantum Three-Pass Protocol

Rajeev Kumar Gupta*, R. K. Pateriya and Ankita Patil

MANIT Bhopal, 462003, India
rajeevmanit12276@gmail.com, *pateriyark@gmail.com*,
ankitapatil12276@gmail.com

Abstract

In this paper, a hybrid cryptosystem is presented combining classical cryptography with quantum cryptography, in which the secure key distribution between the parties utilizing AES cipher is performed using quantum three-pass protocol. This protocol guarantees the absolutely secure key transmission whose security relies on the no-cloning theorem of quantum mechanics. The key is transmitted in the form of polarized photons, which is further encrypted by rotating each photon by a certain angle. This key is utilized by AES (Advance encryption Standard) cryptosystem which is a symmetric block cipher whose strength relies on the substitution box (S-box) that introduces non linearity into the cryptosystem. The S-box used in the existing AES is fixed which may pose security threats if scrutinized by an attacker. Hence, in this paper, a key-dependent S-box is also proposed which is tested to satisfy the properties such as avalanche effect, strict avalanche criteria and confusion property. The results show that the proposed algorithm is effective for generating a key-dependent S-box and since the S-box is not pre-calculated, it can strengthen the AES cryptosystem against attacks launched by the fixed S-box analysis.

Keywords*: AES, Avalanche effect, Quantum key distribution, Quantum three-pass protocol, S-box.*

1. Introduction

Cryptography plays an inevitable role to secure communication. In layman's words, cryptography means information security and the most effective way to ensure it is encryption-decryption techniques [5]. These techniques can be either symmetric or asymmetric based on the usage of the key, where a key is a numeric or may be some special symbol which is utilized to convert the plain text into cipher text and vice-versa [16]. In a symmetric cryptosystem such as AES, the communicating parties use a single key for both, enciphering-deciphering. The security of this technique is based on the secure key distribution between the participants. Hence, if the key gets exposed to an adversary, further secure communications are unachievable. Consequently, these cryptosystems suffer from the obvious weakness of distributing the key securely. Quantum cryptography, which is the implementation of quantum mechanics in cryptography, offers the solution to this problem facilitating quantum key distribution. It makes extensive use of the Heisenberg's uncertainty principle and no-cloning theorem which states that an arbitrary unknown quantum state can't be replicated [6]. [1]

These principles guarantee that it is impossible for an eavesdropper to intercept without disturbing the transmission with a high probability so as to let the channel's legitimate parties detect his presence over it [7,18]. Quantum cryptography is not enciphering and deciphering of a message, it only allows a secure distribution of the secret key using

Rajeev Kumar Gupta is the corresponding author.

ISSN: 1738-9976 IJSIA

polarized photons [13]. This concept was put forward in 1984 with BB84, the first known quantum key distribution protocol. Although this protocol facilitates eavesdropping detection, it suffers from the drawback of low qubit efficiency, which is the ratio of the length of the key bits shared between the parties to the length of the key bits originally generated by the sender. Hence, in this paper, quantum three-pass protocol is utilized for the secure key distribution for AES cryptosystem that exploits each photon in a superposition state and can provide a high qubit efficiency utilizing all the transmitted qubits unlike BB84, where a qubit is a polarized photon encoding a key bit [1,2].

The existing AES uses a static S-box which, if known by the attacker, can be proved as a security threat. Hence, many efforts have been emulated in order to improve the security and performance of the AES algorithm. In the presented work, a key-dependent S-box is generated by modifying the existing S-box and it is verified that the proposed S-box satisfies the cryptographic properties of a good S-box comparable to the existing AES S-box and due to being key-dependent, can enhance the security of AES against known S-box analysis attacks.

2. Quantum Cryptography

2.1 Preliminaries

The application of quantum mechanics in cryptography brings the concept of quantum cryptography in which photons are exploited for the transmission of the information where, a photon is an elementary light particle which can be polarized and carries a definite amount of energy. Polarization is a physical property and it emerges when the light is considered as an electromagnetic wave [18]. The photon can be polarized by passing it through a polarizing filter fixed to the desired angle and its measurement can be performed by a calcite crystal. The polarization of a photon can be expressed in general, as $x\,|\uparrow\rangle + y\,|\rightarrow\rangle$ where x and y are complex numbers such that $|x|^2 + |y|^2 = 1$[6]. A photon polarized rectilinearly can have the basis at 0^0 or 90^0 with respect to the horizon. The vector space for both the cases can be represented as follows:

$$|0\rangle \text{ or } |\rightarrow\rangle = \begin{pmatrix}1\\0\end{pmatrix} \quad \text{and} \quad |1\rangle \text{ or } |\uparrow\rangle = \begin{pmatrix}1\\0\end{pmatrix}$$

2.2 Photon Polarization

A photon can be linear-polarized using a polarizing apparatus which is called linear polarizer. The direction of the polarization can be determined by the orientation of the polarizer. If this photon has to be encrypted by rotation, then it is passed through a Faraday rotator for which, the rotation angle is controlled by the strength of the magnetic field which is parallel to the light beam. The output from a Faraday rotator is the polarized photon rotated by an angle θ [23]. The state of the photon is represented by $|\psi\rangle = \cos\theta \cdot |0\rangle - \sin\theta . |1\rangle$ which is a superposition state of $|0\rangle$ and $|1\rangle$.

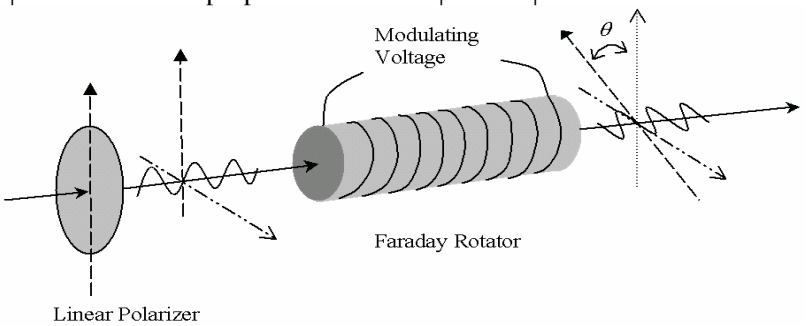


Figure 1. Experimental Realization of Photon Polarization

When the angle of polarization is 30^0, the state of photon is represented by
$|\psi\rangle = \cos 30^0 \cdot |0\rangle - \sin 30^0 . |1\rangle = (\sqrt{3}/2). |0\rangle - (1/2).|1\rangle$
Hence, if this photon is measured with a horizontal-vertical polarization base, 0 is obtained with the probability $(\sqrt{3}/2)^2$ and 1 with the probability $(1/2)^2$. Hence, the result of measurement depends on the angle θ.

2.3 Quantum Three-Pass Protocol

In the recent years, quantum three-pass protocol [22] has been a new addition to the quantum cryptographic protocols, which is based on the Shamir's three pass protocol of classical cryptography. This protocol utilizes photons in superposition state, and is featured as involving quantum channel only, unlike BB84 and other quantum cryptography protocols that also utilizes classical channel along with quantum channel for key distribution [1,2]. In this protocol, the Information in terms of classical bits is encoded in the form of photon polarization in such a way that the vertical polarization represents the binary bit value 1, and the horizontal polarization represents 0. With encoding n-bit information in n-photons, each polarized photon is rotated by an angle, which is randomly chosen for each photon. The rotation by an angle θj is performed such that

$$R(\theta j) = \begin{pmatrix} cos\ \theta j & sin\theta j \\ -sin\theta j & cos\theta j \end{pmatrix}$$

Hence, the encryption is performed in terms of the rotation operation and the set of angles (θj_1, θj_2..... θj_n) is considered as the encryption key while the decryption is performed by the decryption key (-θj_1, - θj_2.....- θj_n). This protocol involves no previously shared key between the sender and the receiver. For each session, both the parties generate their own random secret keys $K_{\theta s}$ and $K_{\theta r}$, respectively, such that $K_{\theta s}$ = $\{\theta s \mid 0 \le \theta s < \pi\}$) and $K_{\theta r} = \{\theta r \mid 0 \le \theta r < \pi\}$. Certainly, the eavesdropper doesn't get to know these secret keys [23].

It is assumed that the plain text is a set of photons in horizontal or vertical polarization state. Let the plain text to be sent is |0>. The encryption $E_{K\theta s}$ of this plain text P by the sender using his secret key $K_{\theta s}$ is performed as follows:

$$E_{K\theta s}[P] = R(\theta s).|0\rangle = R(\theta s) = \begin{pmatrix} cos\ \theta s & sin\theta s \\ -sin\theta s & cos\theta s \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$= \cos \theta s\ |1\rangle - \sin \theta s\ |0\rangle = |x1\rangle$$

For performing the decryption operation, the received photon is rotated by θs in the opposite direction. The decryption (rotation by - θs) is represented as follows:

$$= \begin{pmatrix} cos(-\theta s) & \sin(-\theta s) \\ -\sin(-\theta s) & \cos(-\theta s) \end{pmatrix} \begin{pmatrix} \cos\theta s \\ -\sin\theta s \end{pmatrix}$$

$$= \begin{pmatrix} cos^2\theta s + sin^2\theta s \\ sin\ \theta s . cos\ \theta s - cos\theta s sin\theta s \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

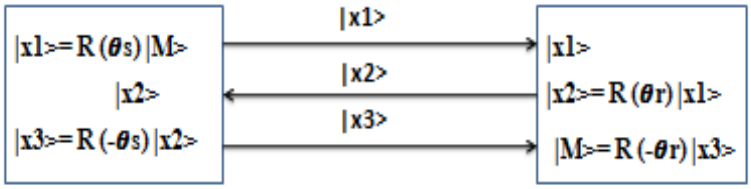


Figure 2. Quantum Three-Pass Protocol Procedures

2.3.1 Steps for QTPP

1. Using the technique mentioned above, the sender encodes the plain text, M in the form of photon polarization and using the key $K_{\theta s}$, performs the encryption ($E_{K\theta s}$) in the form of rotation as:

$E_{K\theta s}$ [M]: R (θs) |M> = cos θs |1⟩ - sin θs |0⟩ = |x1>

2. The receiver receives the photons transmitted in the above step and encrypts them using his own key $K_{\theta r}$ as follows:

$E_{K\theta r}$ [$EK_{\theta s}$ [M]]: R (θr) |x1> = cos (θs+ θr) |1⟩ - sin (θs+ θr) |0⟩ = |x2>

Where |x2> is a superposition state. The receiver sends |x2> back to the sender.

3. Now, the sender performs decryption (DK-$_{\theta s}$) on the received photons using the key K-$_{\theta s}$ resulting in the state |x3> and sends the resulting photons back to the receiver.

DK-$_{\theta s}$[$E_{K\theta r}$ [$EK_{\theta s}$ [M]]]: R(-θs)|x2> = cos θr|1⟩ - sin θr |0⟩ = |x3>

4. The receiver performs decryption operation on the received photons using the key K-$_{\theta r}$ as

DK-$_{\theta r}$ [$E_{K\theta r}$ [M]]: R(-θr)|x3> = | M>

Thus, the receiver obtains the plain text |M>.

2.3.2 Security Analysis of QTPP: In this protocol, the photons carrying the key bits are in superposition state. Hence, it is infeasible to obtain the original state with no knowledge of rotation angle. If the sender transmits the quantum state |1>, encrypting it with the rotation angle 45^0, if Eve intercepts this state, which is unknown to him and measure it in a horizontal-vertical polarization base, he will obtain the result as 0 or 1 with a probability of 50%. In QTPP, each photon is rotated by a randomly chosen angle θ, so Eve will obtain a 0 or 1 on the average when he measures a sequence of polarized photons. Only half of his measured result is correct since |x> is |0> or |1> anyway. Still, correct guessing of the entire key is hard to achieve.

3. AES Algorithm

AES is one of the best-known and most widely used symmetric block ciphers. It is an iterative algorithm in which iteration is considered as a round and the total number of rounds is 10, 12 or 14 for the key size of 128, 192 or 256 bits. AES algorithm operates on the fix sized plain-text blocks of 128 bits, each considered as a state and is represented by a 4 x 4 matrix. Similarly, the key is also taken as a square matrix of bytes. The state is modified at each stage of AES encryption/decryption process [21]. AES follows the two general properties of block ciphers: confusion and diffusion. Confusion means the transformations that change the dependence of the statistics of a cipher text on the statistics of its plaintext. Diffusion is the spreading of the influence of a plaintext bit onto many cipher text bits to hide the statistical structure of the plaintext. These two properties in AES are achieved by round repetition and using S-box [12]. Due to this, it is considered as one of the most secure cryptosystem. Considering AES-128, there is no known attack which is faster than 2^{128} complexity performing the exhaustive search. Although, recently AES-192 and AES-256 were shown to be broken by the attacks taking 2^{176} and 2^{119} times, respectively, these attacks are considered to be completely non-practical and don't seem to have the potential to present any real threat to the security of AES algorithm [4].

3.1 AES Operations

The following operations are performed on the input state in AES:

1. Add round key: In this stage, the 128 bits of the state are bitwise XORed with the round key of 128 bits. The round key is obtained from the key expansion of the cipher key. For decryption, the inverse of add round key operation is computed similarly.

2. Sub Bytes: It's a byte substitution operation performed on each byte of the state independently using a substitution table called S-box. The S box is a 16 x 16 table containing the permutation of all 256 8-bit values. Each byte of the state is substituted by another byte obtained from the S-box such that S(Ai) =B(i). The inverse of sub bytes is performed similarly but using the inverse S-box which is also pre-calculated.

3. Shift rows: In this stage, each row of the state obtained after sub bytes is shifted cyclically left based on the row index. The first row is left unchanged. Each byte of the 2nd, 3rd and 4th rows is shifted left by 1, 2 and 3 positions respectively. The inverse of shift row operation is performed similarly, but the rows are shifted in the right direction.

4. Mix column: This operation is performed on the state columns where each column is considered as a four-term polynomial over GF (2^8) which is multiplied by the modulo x^4+1 and the following polynomial, producing a modified state [12].

$$c(x) = 03.x^3 + 01.x^2 + 01.x + 02$$

The inverse of mix column is similar to mix column in which each column is multiplied by a fixed polynomial defined by,

$$(03.x^3 + 01.x^2 + 01.x + 02).d(x) \equiv 01\ mod(x^4 + 1)$$

It gives $$d(x) = 0B\ x^3 + 0Dx^2 + 09x + 0E$$

S-Box Generation

The Rijndael's S-box is constructed by the following steps:

1. The S-box is initialized with the byte values in ascending order row by row as {00}, {01}, {02}……{0F} for the first row, {10}, {11}….{1F} for the second row and so on.

2. Each byte in the S-box is mapped to its multiplicative inverse in the finite field GF(2^8). The value {00} is mapped to itself. The non-linearity in S-box is due to multiplicative inverse.

3. If each byte in the S-box contains 8 bits labeled as (b7, b6, b5, b4, b3, b2, b1, b0), then the following transformation is applied on each bit of each byte of the S-box:

$b_i' = b_i \oplus b_{(i+4)mod\ 8} \oplus b_{(i+5)mod8} \oplus b_{(i+6)mod\ 8} \oplus b_{(i+7)mod8} \oplus c_i$

Where, c_i is the i^{th} bit value of {63} in the binary form as (c7c6c5c4c3c2c1c0) = (01100011).

The inverse S-box is constructed by applying the inverse of the transformation in the above equation followed by taking the multiplicative inverse in GF (2^8). The inverse transformation is:

$b_i' = b_{(i+2)mod\ 8} \oplus b_{(i+5)mod8} \oplus b_{(i+7)mod8} \oplus d_i$ Where, byte d = {05} or 00000101.

4. Literature Survey

A number of research works have been carried out to modify AES S-box with the intent to enhance the security of AES cipher. In this section, a survey of a few algorithms is provided that have been presented to design the S-box.

Jasim *et al*. in [16] introduced an enhanced version of AES algorithm, quantum-AES which is based on the generation of dynamic quantum S-box utilizing the cipher key generated by quantum key distribution in both, online and offline mode. This QAES generates more complicated and unbreakable key that is utilized to generate dynamic s-box. Although QAES doesn't contradict the security of AES, it is slightly slower than AES.

Kazys *et al*. in [12] presented an algorithm for generating pseudo-random S-boxes as a function of the key. It ensures that any change in the secret key essentially changes the S-box structure which makes the AES cipher resistant against linear and cryptanalysis attacks. Another advantage this technique includes is that enormous number of S-boxes can be generated by changing the secret key.

Mona *et al*. in [15] presented an algorithm that uses chaotic logistic map to generate dynamic S-box based on the cipher key. The generated S-box increases the complexity of breaking the AES cipher and provides better results in security analysis in terms of

avalanche effect, strict avalanche criterion, non-linearity, bit-independence criterion and key sensitivity.

Shishir *et al*. in [19] designed a dynamic S-box which is based on the one-dimensional chaotic map and compared it with classical S-box in terms of confusion and proved that the proposed S-box has better performance.

Sliman *et al*. in [20] generated a new key-dependent S-box providing two cases to design the modified S-box. In 1st case, for any particular round, the first byte of the round key is xored with all the base S-box element. In 2nd case, all the bytes of the round key for any particular round are xored and the value thus obtained is xored with all the S-box elements to generate a new S-box that gets changed for each round. The simulation work proved that although the changes proposed consumed little extra time and more logic elements, but it performed high diffusion and confusion and increased the complexity of the AES algorithm several times, making AES much stronger.

Julia *et al*. in [11] modified the AES S-box by using the cipher key for S-box rotation to make it key-dependent. In this algorithm, for any particular round, all the bytes of the round key are xored and the result obtained is used to rotate the base S-box values to the right by the resultant value. The results proved that the enhanced AES version introduced confusion property without violating diffusion.

5. Proposed Work

AES block cipher system uses a pre-calculated S-box which may create security issues because of its being previously available. Hence, if the S-box is created based on the key, it can provide more security than the static S-box. In this work, a key-dependent S-box for AES is proposed which is based on the key distribution among the communicating parties performed by quantum three-pass protocol and the key shared is used to modify the existing AES S-box. The main strength of this approach lies in the fact that quantum three-pass protocol can provide absolutely secure key distribution since it utilizes polarized photons in superposition states for establishing the key whose security relies on no-cloning theorem stating that an unknown quantum state can't be replicated. The modified S-box thus generated is random, key dependent and is maintained secret so as to thwart the linear and differential cryptanalysis attack. The proposed approach takes place in the following three steps:

I. Key generation using the Linear Congruent Generator (LCG)
II. Key distribution by quantum three-pass protocol
III. Key-dependent S-box generation

Quantum three-pass protocol involves the distribution of a randomly generated cipher-key utilizing the rotation of polarized photons by certain random angles which is performed by both the communicating parties. Hence, a random number generator (Linear congruent generator) is employed in the proposed work to generate the random key. The key generated by the sender is then transmitted to the receiver using polarized photons by QTPP which is further utilized to modify the existing AES S-box to generate a new key-dependent S-box. For analysis, the AES algorithms with the existing and the modified S-box are realized in MATLAB R2012b and the results show that the proposed algorithm has a good cryptographic strength comparable to existing AES with the additional feature of being resistant to linear and cryptanalysis attacks, which need the s-box to be known [12].

Algorithm: Key dependent S-box generation

Input: s_box, key
x=$\sum_{i=1}^{n} key\,(i)$
for i=1:256


```
temp[i] =s_box[i]+x;
s_box[i]=mod(temp[i],256);
end
```

Inverse s-box generation:

```
For i=1:256
inv_s_box (s_box(i) + 1) = i - 1;
end
```

I. Key generation using LCG (Linear Congruent Generator)

For secure key exchange, the sender generates random 128 bits using the Linear Congruent Generator in CrypTool 1.4.30, since LCG is one of the best-known pseudorandom number generators which is fast and easily implemented. The generator is defined by the following recurrence relation:

$$X_{n+1} = (aX_n + c)(mod\ m)$$

Where, Xn is the sequence of random numbers, m is the modulus, a is the multiplier such that 0<a<m and c is the increment such that 0≤c<m. X_0 is the seed or start value. In the proposed work, we have taken m=100000000, c=0 and a=3425. The value obtained for the random key in hexadecimal form is as follows:

10 5E 6A 5C BA 93 E6 85 9F 21 F5 A5 CC 01 19 64

These values are converted into binary 128 bit values as:

{00010000010111100110101001011100101110101001001111100110100001011001111
10010000111110101101001011100110000000001000110010110010 0}

The above obtained bit sequence serves as the AES encryption-decryption key, Sk.

II. Key distribution by Quantum Three-Pass Protocol

1. The photons are generated using laser beam and polarized using calcite crystal such that the bit value 0 is represented by horizontal polarization and value 1 is represented by vertical polarization.

2. The key generated above is shared with the receiver using quantum three-pass protocol. For this, each photon generated above is rotated by a certain angle from a randomly generated key. The sender generates this random key K_s consisting of 128 random angles such that Ks = {θi : 0≤θi < π , i = 1, 2, 3, . . . , n}. In the presented work, the values for random angles are obtained by MATLAB using code

x=round (xmin+rand(1,n)*(xmax-xmin)) Where, xmin=0, xmax=180, n=128 Hence, random angles obtained are, K_s =

{122 71 66 178 7 159 164 143 18 47 60 122 25 130 19 118 89
140 129 163 160 60 126 36 5 134 90 86 163 110 111 155 145 104
33 43 160 5 88 30 176 128 90 85 11 123 8 13 94 17 147 147
130 27 119 93 175 117 144 82 78 149 15 24 31 70 150 145 11
72 95 75 118 113 53 78 3 177 30 19 67 36 88 61 171 166 9
133 48 76 99 170 75 177 54 126 120 97 126 120 32 23 180 31
6 101 159 120 34 66 83 177 28 154 116 68 34 77 87 22 106
41 69 105 45 52 111 48}

Consider the transmission of a key bit Sk=0. The encryption of a photon in the state |0>, in the form of rotation by an angle 122^0 is performed as:

$E[Sk_{K\theta s}]$ = R (θs) |x1> = R (122^0).|0> $= \begin{pmatrix} cos\ 122^0 & sin\ 122^0 \\ -sin\ 122^0 & cos\ 122^0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

= cos 122^0 |1⟩ - sin 122^0 |0⟩ = |x1>

3. Bob also generates a random key K_r (set of random angles) as

K_r = {148 177 131 62 105 19 163 158 147 47 107 4 77 56 29
32 76 17 108 85 125 126 115 6 12 58 96 118 73 148 129 174
96 59 19 110 140 76 16 48 28 51 79 95 82 158 93 170 115

172 43 122 52 121 125 12 46 40 120 152 62 140 122 1 108 70
165 0 83 76 83 139 58 141 85 6 32 130 85 27 61 109 35 133
44 165 48 138 34 52 16 104 123 98 77 116 117 122 114 170 38
128 43 21 109 81 83 119 139 63 119 75 152 150 46 110 105 97
157 48 57 21 169 116 86 115 98 117}

Bob encrypts photons obtained in the above process by rotating each photon by a corresponding angle from k_r, obtaining $K_r(K_s(Sk))$ and sends back to Alice.

$E_{K\theta r}[EK_{\theta s}[Sk]]$: R ($\theta$r) |x1> = cos ($\theta$s+ θr) |1⟩ - sin (θs+ θr) |0⟩ = |x2>
= cos (122^0+148^0)|1> - sin (122^0+148^0)|0> = cos 270^0 |0> - sin 270^0 |1>

4. Alice decrypts $K_r(K_s(Sk))$ by key ($-K_s$) obtaining $K_r(Sk)$

$D_{-ks}[E_{Kr}[Ek_s[Sk]]]$: R (-$\theta$s) |x2> = cos ($\theta$r) |1⟩ - sin ($\theta$r) |0⟩ = |x3>
= cos 148^0|0>-sin 148^0 |1>

5. Alice sends $K_r(Sk)$ to Bob.

6. Bob decrypts $K_r(Sk)$ by key ($-k_r$) as explained above and obtains the key Sk

$D_{-ks}[E_{Kr}[Sk]$ = R (-θr) |x3> = $\begin{pmatrix} cos(-148^0) & sin(-148^0) \\ -sin(-148^0) & cos(-148^0) \end{pmatrix} \begin{pmatrix} \cos 148^0 \\ -\sin 148^0 \end{pmatrix}$

= $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ = |0>

Thus, the transmission of a single key bit takes place by quantum three-pass protocol. The following table illustrates the transmission of a sample of 10-bit cipher key by this protocol.

Table 1. Transmission of Key Bits using Quantum Three-Pass Protocol

State of photon	Encryption by sender by θs (1st stage)	Encryption by receiver by (θs + θr) (2nd stage)	Decryption by sender by -θs {(θs + θr) – θs = θr} (3rd stage)	Decryption by receiver by - θr
| 0>	Cos 122^0 |0>-sin 122^0 |1>	Cos 270^0 |0>-sin 270^0 |1>	Cos 148^0 |0>-sin 148^0 |1>	| 0>
| 0>	Cos 71^0 |0>-sin 71^0 |1>	Cos 248^0 |0>-sin 248^0 |1>	Cos 177^0 |0>-sin 177^0 |1>	| 0>
| 0>	Cos 66^0 |0>-sin 66^0 |1>	Cos 197^0 |0>-sin 197^0 |1>	Cos 131^0 |0>-sin 131^0 |1>	| 0>
| 1>	Sin 178^0 |0>+cos 178^0 |1>	Sin 240^0 |0>+cos 240^0 |1>	Sin 62^0 |0>+cos 62^0 |1>	| 1>
| 0>	Cos 7^0 |0>-sin 7^0 |1>	Cos 112^0 |0>-sin 112^0 |1>	Cos 105^0 |0>-sin 105^0 |1>	| 0>
| 0>	Cos 159^0 |0>-sin 159^0 |1>	Cos 178^0 |0>-sin 178^0 |1>	Cos 19^0 |0>-sin 19^0 |1>	| 0>
| 0>	Cos 164^0 |0>-sin 164^0 |1>	Cos 227^0 |0>-sin 227^0 |1>	Cos 163^0 |0>-sin 163^0 |1>	| 0>
| 0>	Cos 143^0 |0>-sin 143^0 |1>	Cos 301^0 |0>-sin 301^0 |1>	Cos 158^0 |0>-sin 158^0 |1>	| 0>
| 0>	Cos 18^0 |0>-sin 18^0 |1>	Cos 165^0 |0>-sin 165^0 |1>	Cos 147^0 |0>-sin 147^0 |1>	| 0>
| 1>	Sin 47^0 |0>+cos 47^0 |1>	Sin 94^0 |0>+cos 94^0 |1>	Sin 47^0 |0>+cos 47^0 |1>	| 1>

After the secure exchange of the key between both the parties, the key can be utilized to compute the proposed S-box modifying the existing S-box.

III. Generating the Key Dependent S-Box

After the cipher key establishment among the parties, a new key-dependent S-box is computed by taking the S-box of the Rijndael AES algorithm as the base and applying the proposed algorithm as follows:

1. The key shared among the parties is:

Key =10 5E 6A 5C BA 93 E6 85 9F 21 F5 A5 CC 01 19 64

In decimal, key= 16 94 106 92 186 147 230 133 159 33 245 165 204 1 25 100

x= sum(key)= 1936

Now, applying temp= s_box + x

s_box=mod (temp,256);

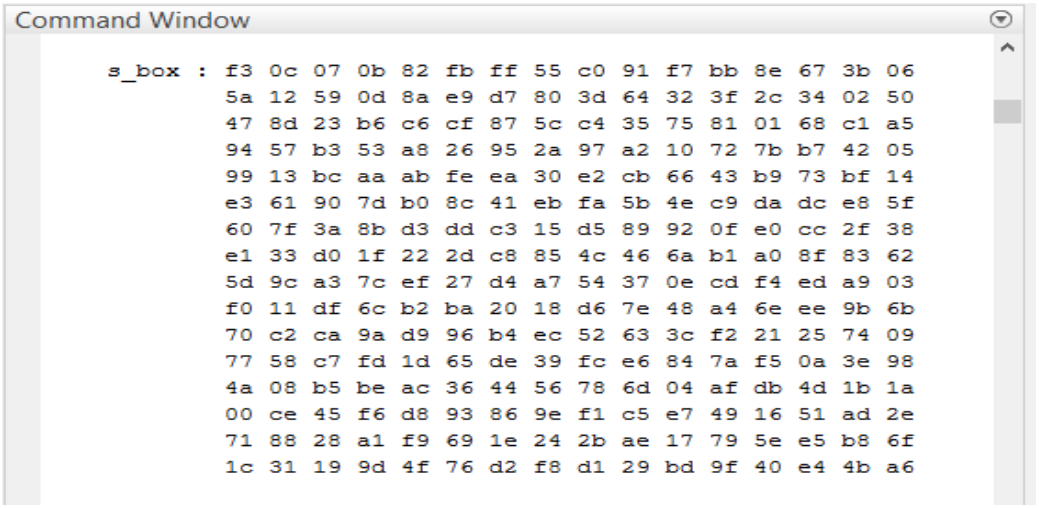


Figure 3. Key Dependent S-box with Key 10 5E 6A 5C BA 93 E6 85 9F 21 F5 A5 CC 01 19 64

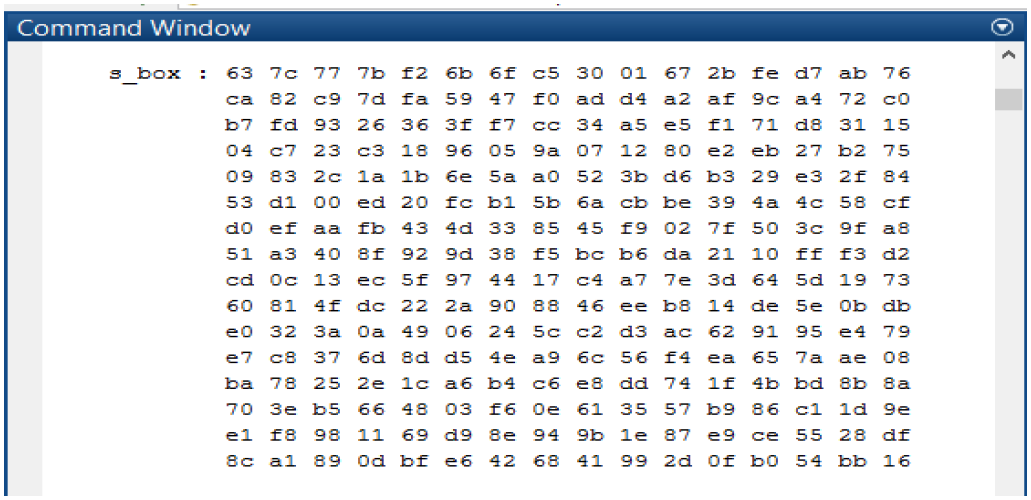


Figure 4. Existing AES S-Box

6. Results Analysis

An AES S-box follows certain properties such as completeness, avalanche effect and strict avalanche criterion due to which it is important in terms of security and can provide diffusion and confusion. In this section, these parameters are tested to evaluate and

compare the performance of AES using the proposed key dependent S-box and the existing AES. The following results are obtained executing both the algorithms on MATLAB R2012b.

a) **Completeness**

If a cryptographic transformation is complete, then each cipher-text bit must depend on all the plain-text bits. If there is at least one-pair of the plain text each of n bits and differing only in bit i, then the cipher text differs at least in bits j for all $i \leq 1$ and $j \leq n$.

Table 2. Relationship between Plain-Text and Cipher Text

Plain-Text	Cipher –Text	
	Existing AES	Proposed AES
00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff	110 111 91 212 194 227 51 173 255 242 149 237 47 168 226 226	145 91 89 142 71 228 67 24 27 145 186 53 59 53 133 45
01 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff	86 235 159 199 231 137 109 218 26 170 32 15 136 66 193 35	48 39 48 220 119 166 99 94 18 95 36 207 193 67 16 206

The table above shows that performing AES encryption on the plain-text randomizes the cipher-text output in both the algorithms independent of each others. Also, changing the plaint-text by only a single bit changes a large number of cipher-text bits showing that the proposed S-box follows completeness property.

b) **Avalanche Effect**

Avalanche effect is an important cryptographic property of block cipher stating that a function $f:\{0,1\}^n \rightarrow \{0,1\}^n$ satisfies the avalanche criterion if the change of one bit in the input bits results into the change of on an average half of the output bits [17]. A block cipher is considered to have poor randomization if it doesn't exhibit the avalanche effect to a significant extent [11].

Avalanche effect= no. of bits flipped in cipher text on changing 1-bit of plain-text or key / no. of bits in cipher text

Table 3. Avalanche Effect on Changing One Bit of Plain Text

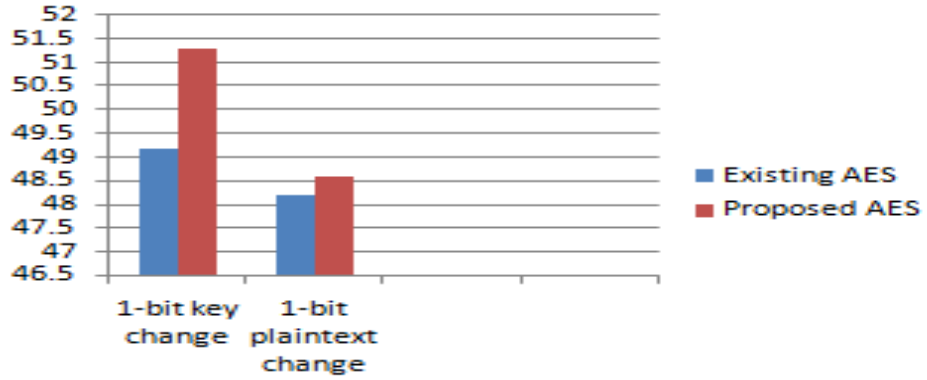
Existing AES	0.484	0.437	0.484	0.531	0.531	0.476	0.406	0.507
Modified AES	0.476	0.546	0.531	0.406	0.492	0.453	0.50	0.49

Taking the plain text= 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Table 4. Avalanche Effect on Changing 1-Bit of the Key

Existing AES	0.546	0.492	0.445	0.453	0.460	0.507	0.554	0.476
Modified AES	0.546	0.507	0.515	0.546	0.507	0.523	0.460	0.50

The following graph is obtained by performing AES encryption and taking the average of the avalanche effect observed in the above samples using the existing and the proposed algorithm.



Graph 1: Comparison of Avalanche effect with the existing and modified S-box

The graph above shows that the proposed algorithm is better than the existing AES algorithms in terms of the avalanche effect, since changing one-bit of input changes more number of output bits in case of proposed S-box. Also, the increment in the avalanche effect is more in case of changing 1 bit of the key as compared to that in changing one bit of the plain text.

c) Strict Avalanche Criterion (SAC)

SAC combines the avalanche effect and completeness, both the properties. For an S-box to satisfy SAC, with the change in one input bit, each of the output bit should get changed with a probability 0.50. This property is a measure of the confusion and diffusion and is a special case of avalanche effect. It is unrealistic to satisfy SAC for all the input values. Hence, an S-box can satisfy SAC with a small error range. The relative error Es for S-box is given by:

Es= max| $2K_{sac}$|-1 Where, K_{sac} is SAC parameter.

For table 3, Calculating the SAC error rate by Es= max| $2K_{sac}$|-1shows that the proposed S-box follows SAC with the error rate Es= 0.092 and the AES S-box, with Es= 0.062.

For table 4, Calculating the SAC error rate by Es= max| $2K_{sac}$|-1shows that both the S-boxes follow SAC with the error rate Es= (0.546*2)-1 =0.092.

Since the proposed S-box follows SAC with a small error rate, it also follows completeness property.

d) Correlation Coefficient

This parameter deals with the dependency of the output bits on the input bits. The correlation value is a measure of the confusion property of a block cipher. Correlation coefficient is a numeric value between -1 and 1 which is a measure of the degree of linear

relationship between two variables. In case of independent variables, it assumes the value 0.

Taking the key: 10 5E 6A 5C BA 93 E6 85 9F 21 F5 A5 CC 01 19 64

Correlation coefficients are obtained between a number of plain-text and the cipher-text pairs for both, the existing and the proposed algorithm and the following results are obtained:

Table 5. Comparison of Correlation Coefficients

Corr. Coeff. (AES S-box)	0.3200	-0.4499	-0.0492	-0.6438	0.2747	0.1379	-0.3548	-0.0736
Corr. Coeff. (Modified S-box)	-0.2588	0.1852	0.1434	0.1517	0.1964	-0.1073	0.0567	-0.1314

The value of correlation coefficient between 0 and 0.3 (0 and -0.3) shows a weak positive (negative) linear relationship, between 0.3 and 0.7 (-0.3 and -0) shows a moderate positive (negative) linear relationship and between 0.7 and 1.0 (-0.7 and -1.0) shows a strong positive (negative) linear relationship [20].

The results obtained above for the modified S-box indicates weak linear relationship between the plain-text and the cipher text. Hence, the proposed S-box follows the confusion property of the block cipher.

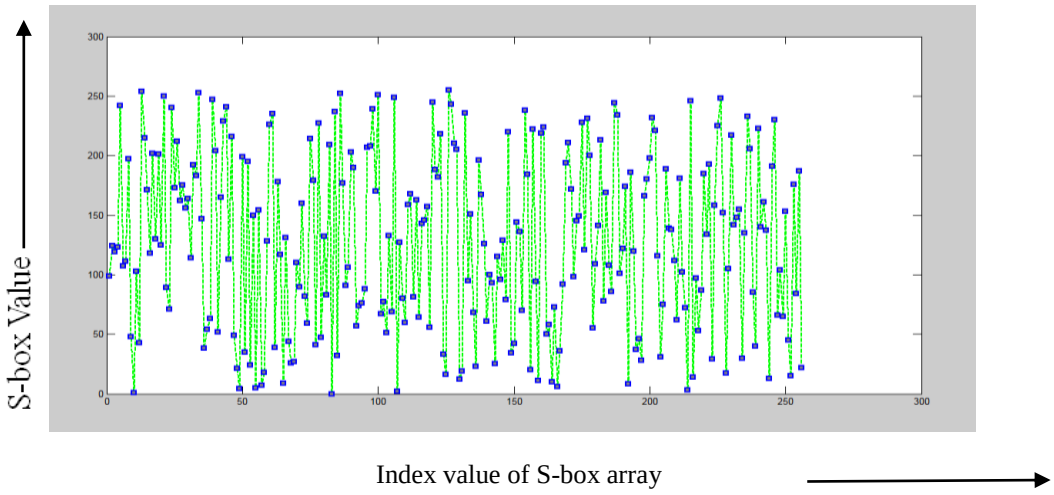


Figure 5. Elements of the AES S-Box

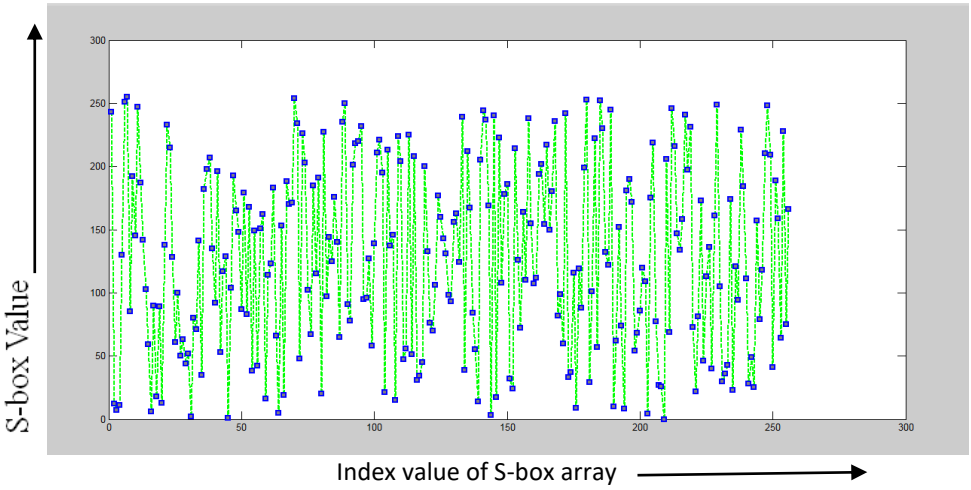


Figure 6. Elements of the Modified S-Box

It can be inferred from both the above graphs that the S-box obtained from the proposed algorithm contains the value at each index different from that in the existing AES S-box indicating the modification of each s-box value using the proposed algorithm.

7. Conclusion

The substitution box is the keystone of AES block cipher system which introduces non-linearity into the cryptosystem protecting it from the linear and differential cryptanalysis. However, a fixed S-box may enable an attacker to scrutinize the S-box properties and thus enable him to analyze its weak points which may consequently pose security threats to AES cipher. However, using a key dependent S-box can makes it difficult for an attacker to do offline analysis of the possible attacks on the S-box with the intention to break the security of AES. Hence, in this paper, a new approach is presented to generate a key dependent S-box for AES whose secrecy relies on the secure key distribution among the parties facilitated by quantum three-pass protocol. This protocol utilizes photons in superposition states for key distribution whose security is based on the fact that an unknown quantum state can't be cloned. The S-box thus generated is tested for avalanche effect, completeness, strict avalanche criterion and confusion property. The results show that the proposed S-box follows the properties of a good S-box and can be utilized to enhance the security level of AES cipher against the attacks launched by the fixed S-box analysis. It can also be concluded that quantum key distribution by quantum three-pass protocol can be employed to enhance the security of modern cryptosystems.

References

[1] A. A. Abdullah, R. Khalaf and M. Riza, A Realizable Quantum Three-Pass Protocol Authentication Based on Hill-Cipher Algorithm, Mathematical Problems in Engineering, 2015.
[2] A. A. Abdullah, Modified Quantum Three Pass Protocol Based On Hybrid Cryptosystem, Ph. D. thesis, Eastern Mediterranean University, 2015.
[3] A. Alabaichi and M. S. Mechee, Evaluation of a Dynamic 3D S-Box Based on Cylindrical Coordinate System for Blowfish Algorithm, J of Applied Sciences **15** (5) (2015), 728-740.
[4] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, Key Recovery Attacks of Practical Complexity on AES Variants With Up To 10 Rounds.
[5] B. R. Gangadari, S. R. Ahamed, R. Mahapatra and R. K. Sinha, *Design of cryptographically secure AES S-Box using cellular automata*, Proceedings of the International Conference on Electrical, Electronics, Signals, Communication and Optimization, 2015, 1-6.
[6] B. R. Auburn, Quantum Encryption – A Means to Perfect Security?, SANS Institute, 2003.

[7] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution, and Coin Tossing*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984, 175-179.
[8] Y.F. Chung, Z. Y. Wu , T.S. Chen, Unconditionally secure cryptosystems based on quantum cryptography, Information Sciences **178** (8) (2008), 2044-2058.
[9] G. Jakimoski and L. Kocarev, Chaos and cryptography: block encryption ciphers based on chaotic maps, *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, **48**(2) (2001), 163-169.
[10] J. Daernen, V. Rijrnen, *The Design of Rijndael AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.
[11] J. Juremi, R. Mahmod, S. Sulaiman and J. Ramli, Enhancing Advanced Encryption Standard S-Box Generation Based on Round Key, International Journal of Cyber-Security and Digital Forensics **1**(3) (2012) 183-188.
[12] K. Kazlauskas, J. Kazlauskas, Key-Dependent S-Box Generation in AES Block Cipher System, Informatica **20** (1) (2009), 23–34.
[13] M. Alshowkan, K. Elleithy, A. Odeh and E. Abdelfattah, *A new algorithm for three-party Quantum key distribution*, Proceedings of the Third International Conference on Innovative Computing Technology, 2013, 208-212.
[14] M. Matsui, *Linear cryptanalysis method for DES ciphers*, Advances in Cryptology—EUROCRYPT'93, Springer-Verlag, 1994, 386–397.
[15] M. Dara and K. Manochehri, A Novel Method for Designing S-Boxes Based on Chaotic Logistic Maps Using Cipher Key, World Applied Sciences Journal **28** (12) (2013), 2003-2009.
[16] O. K. Jasim, S. Abbas, El-Sayed M. Horbaty, Abdel-Badeeh M. Salem, Evolution of an Emerging Symmetric Quantum Cryptographic Algorithm, J of Information Security **6 (**2015), 82-92.
[17] P. Rodwald and P. Mroczkowski, *How to create good s-boxes?*, Proceedings of the 1st International Conference for Young Researchers in Computer Science, Control, Electrical Engineering and Telecommunications *ICYR* 2006, 18-20.
[18] M. S. Sharbaf, *Quantum cryptography: An emerging technology in network security*, Proceedings of the IEEE International Conference on Technologies for Homeland Security (HST), 2011, 13-19.
[19] S. Katiyar, N. Jeyanthi, Pure Dynamic S-box Construction, *International Journal of Computers* **1**, 2016.
[20] S. Arrag, A. Hamdoun, A. Tragha and S. E. Khamlich, Implementation of stronger AES by using dynamic S-box dependent of master key, J of Theoretical and Applied Information Technology, **53** (2) (2013).
[21] W. Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 2012.
[22] Kanamori and S. M. Yoo, Quantum Three-Pass Protocol: Key Distribution Using Quantum Superposition States, *International Journal of Network Security & Its Applications* **1**(2) (2009).
[23] Y. Kanamori, S. M. Yoo, D. A. Gregory and F. T. Sheldon, *On quantum authentication protocols*, Proceedings of the IEEE Global Telecommunications Conference, 2005.
[24] Y. Kanamori, S. M. Yoo, Don Gregory and F.T. Sheldon, Authentication Protocol Using Quantum Superposition States, *International Journal of Network Security* **9** (2) 2009, 101-108.
[25] Quantum Safe Cryptography and Security, ETSI White Paper **8**, 2015.

