Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

11th International Conference on Electrical Engineering
ICEENG 2018

DESIGN AND SIMULATION OF NEW AND FAST AUTHENTICATED ENCRYPTION ARCHITECTURE (AESSEA3)

Ayman Yousry El Hadary [*], Mohamed Helmy Megahed,[**]

and Mohamed Hassan Abdel Azeem [*]

ABSTRACT

Authenticated Encryption (AE) is a very important technique that ensures the security of data transportation. AE combines encryption and authentication to provide both privacy and authenticity of the data. In this paper, design, analysis and simulation of a fast and new Authenticated Encryption architecture called Authenticated Encryption SSEA3 (AESSEA3) is introduced on the basis of unpredictability concept. Unpredictability is a concept based on dynamic use of encryption algorithms, where instead of using single encryption algorithm for producing the ciphertext, multiple encryption algorithms are used in the same structure. Pseudo Random Number Generator (PRNG) is used to select which encryption algorithm will be used. Two double AES-256 are used with only 3 rounds to add the unpredictability concept which provide high speed and high security level. The plaintext enters one Double AES-256 and RC4 output enters the other Double AES-256. Also, the security increased by Xoring between the two outputs from the two algorithms to get the ciphertext. The proposed algorithm is faster than AGEIS which is one of the fastest AE algorithms. A new structure for AE is introduced to confirm authenticity. Tag partitioning concept is used. The proposed algorithm can resist different types of cryptanalysis attacks.

KEY WORDS

Authenticated Encryption (AE), Block and Stream Cipher, Double AES-256, AESSEA3, Unpredictability.

---

* Electronics and Communications Department, AASTMT, Cairo,Egypt

** Communications Department, CIC, Cairo, Egypt.

I. INTRODUCTION

Protection of a data requires the protection of both confidentiality and authenticity. Authenticated Encryption (AE)[1] is a technique used to provide both security and authenticity of transported files and data.AE algorithms generally receive the Message (m) and then generate both Ciphertext (C) and Authentication Tag (T) during the encryption process[2] to ensure data integrity. In this paper, the design, analysis and simulation of a new and fast Authenticated Encryption Architecture (AESSEA3) is provided based on the unpredictability concept, for secure chatting and transported files and data over 4G Mobile communication network which facing many types of attacks. Unpredictability concept [3], is based on the use of two or more encryption algorithms, where instead of using one Encryption Algorithm to get the ciphertext, multiple encryption algorithms are used. Pseudo Random Number Generator (PRNG) [4] output is used as a selector to choose which Encryption Algorithm will be used to encrypt the plaintext block. Two Double AES-256 are used with only 3 rounds to provide the unpredictability concept. The plaintext block enters one Double AES-256 algorithm and the RC4 output enters the other Double AES-256 algorithm. Also, the security of the algorithm is increased by using 'exclusive OR' for Xoring between the two outputs from the two algorithms to get the ciphertext. In the proposed algorithm, instead of using 5 rounds AES as in AGEIS [5] which is a fast AE algorithm, we use only 3 rounds AES to achieve faster AE. AGEIS is faster than AES CCM, GCM and OCB modes. A new Authenticated Encryption (AE) schemes introduced to confirm authenticity. For ensuring fast performance for the designed algorithm a new concept of Tag Partitioning is used. Instead of sending the whole file in case of wrong calculated Tag, the Tag partition ensures the transmission of small part of the whole file. NIST tests [6] show that our proposed algorithm output passed all NIST tests. The proposed algorithm can resist different types of cryptanalysis attacks such as linear, differential, algebraic, correlation, related key, sliding attack, truncated differential cryptanalysis and other types of attacks [7- 14]. The speed of encryption of the proposed algorithm is measured which is 60 Mbits/Sec to encrypt a file on Laptop Dell Inspiron 15R and the operating system is Windows 7 of 64-bit, Processor Intel® Core™ i7-5400U CPU @ 1.80 GHz and RAM of 8GB. The speed of decryption is slightly lower than the encryption where the decryption algorithm is double size the encryption algorithm in both software and hardware to provide the same speed of encryption. In this paper, a new Authenticated Encryption architecture shown in Figure (3) with the followings:

1) One RC4[4] algorithms as inputwith key size of 512 bits which is noted $RC4_1$ and the output is 256 bits.
2) Two Double AES-256 algorithms with only 3 rounds and each output of 256 bits which are noted DBAES1 and DBAES2.The Double AES-256 has 512 bits key length.
3) One RC4 algorithm to select which Double AES-256 Algorithm is used to encrypt the plaintext which is noted $RC4_2$ with key size of 512 bits and output of this RC4 is 1 bit.
4) The total key size of the cryptosystem is 2048 bits.
5) XOR between the outputs of *the two Double AES-256 which is C_{out} which is 256 bits.*

The introduced AE algorithm provides four contributions.

1) High Speed and Minimum time delay, by using AES-256 with only 3 rounds.
2) High security level, by using both block cipher and stream cipher where the paintext is encrypted by block cipher and both outputs of the two algorithms are Xored.
3) Dynamic Security by using Unpredictability concept, by using two algorithms that are running randomly using RC4 as PRNG to choose which algorithm is used to encrypt plaintext while the other algorithm encrypts the output from RC4.
4) Tag partitioning, to reduce the time delay of retransmitting the wrong blocks during transmission where every 1024 blocks plaintext has a Tag.

OUTLINE OF THE PAPER

Section 2 introduces the related work. Section 3 introduces the design principals. Section 4 presents AESSEA3 architecture. Section 5 presents the Security of AESSEA3. Section 6 presents the performance analysis. Section 7 introduces a comparison between AGEIS and AESSEA3. And section 8 concludes the paper.

II. RELATED WORK

In this section, related works which will be employed in the introduced design is presented as the following:

Unpredictability

If the used Encryption Algorithm structure is not static (Dynamic) which is not deterministic algorithm, the cryptanalyst will face a big problem which will be very hard to solve. Using two encryption algorithms with alternating use for encrypting the plaintext blocks will make the algorithm dynamic and unpredictable [3]. The PRNG controlling output is used to choose which Encryption Algorithm will be used to encrypt plaintext; this controlling output is unknown to the attacker. Unpredictability makes Encryption Algorithms very immune to different types of cryptanalysis.

SSEA3

SSEA3 [3] Spread Spectrum Encryption Architecture is a type of symmetric key cipher systems. It consists of Two AES-256 encryption algorithms with only 3 rounds to achieve unpredictability and high speed. SSEA3 architecture is based on the unpredictability concept. Unpredictability concept is a concept based on dynamic use of encryption algorithms, producing the ciphertext, multiple encryption algorithms are used in the same structure. Two AES-256 encryption algorithms with two different S-Boxes are used in SSEA3 to overcome the synchronization problem between these two encryption algorithms. To ensure different algorithms output, Different S-Boxes are used. Each round has 16 subkeys of the 3 rounds. The subkeys are dynamic (not fixed). At every plaintext block the encryption algorithm will keep changing from algorithm one to algorithm two based on the output from RC4. The two outputs from the two AES-256 encryption algorithms are XORED to produce ciphertext output.SSEA3 is a high speed secure encryption algorithm with structure that can resist quantum computers (QC) [15, 16]. As in Fig.1, SSEA3 architecture has two AES-256 encryption algorithms and two session keys for the cryptosystem. The PRNG output selects one of the two algorithms to encrypt the plaintext. The output from RC4 is used to enter the other algorithm that is not used by

the plaintext. The outputs from the two encryption algorithms are XORed to produce ciphertext as shown in Fig.1.

AEGIS

AEGIS [5] is AE online mode of operation which provides both authenticity and confidentiality in one shot. AEGIS is constructed on the basis of using AES encryption round function. In AEGIS the message used to update the state of the cipher text as shown in Fig.2. It has three configurations (AEGIS-128, AEGIS-128L, and AEGIS-256). In AEGIS-128 the algorithm processes 16-byte message block with 5 AES round functions. AEGIS-128L processes 32-byte message block with 8 AES round functions. And AGEGIS-256 uses 6 AES round functions to process 16-byte message. It is clear that AEGIS-128 is the lighter and the fastest algorithm. The computational cost of AEGIS is about the half of the AES. Usually AEGIS is used for network communication to protect a packet while leaving the packet header unencrypted.

III. DESIGN PRINCIBALS

The designed AESSEA3 algorithm is generally based on the unpredictability concept. This concept is based on dynamic use of encryption algorithms, where instead of using single encryption algorithm for producing the ciphertext, multiple encryption algorithms are used in the same structure. Pseudo Random Number Generator (PRNG) is used to select which encryption algorithm will be used. Two Double AES-256 is used with only 3 rounds to confirm the unpredictability concept which leads to high security level for the algorithm. The plaintext enters one Double AES-256 and RC4 output enters the other Double AES-256. The proposed AESSEA3 is faster than AGEIS. In this paper, the design and simulation of a new AE block cipher algorithm which depends on SSEA3 algorithm, with the following design principles:

1) **New AE architecture.**
2) **Unpredictability concept, provided by:**

a) Using two algorithms that are running randomly using RC4 as PRNG to choose which algorithm is used to encrypt plaintext while the other algorithm encrypts the output from RC4.

b) XOR between the two outputs from the two encryption algorithms.

3) **Tag partitioning, to reduce the time delay of retransmitting thewrong blocks during transmission.**

IV. AESSEA3 ARCHITECTURE

1) System Components

a) Two double AES-256, we use Two Double AES-256 encryption algorithms with two different S-Boxes. Each algorithm has Double AES-256 encryption algorithms with only 3 rounds. Double AES-256 in each algorithm is used to increase the speed by taking a plaintext block of 256bits. The encryption algorithm will keep changing from algorithm one to algorithm two based on RC4 output. The outputs from the two encryption algorithms are XORed to get

the ciphertext. The unpredictability concept is introduced in the proposed algorithm.

b) RC4 as PRNG, We use RC4 stream cipher algorithm as PRNG to choose one algorithm to receive the plaintext block at every clock. The PRNG chooses where the plaintext goes to algorithm one or algorithm two. The output from RC4 stream cipher algorithm is used to enter the algorithm that is not used by the plaintext.
c) Key schedule, there are four keys with key size of 512 bits. The key schedule of AES-256 generates the subkeys of the three rounds AES-256 as in standard.

2) Encryption Process

Fig.3. shows that the introduced architecture has two double AES-256 algorithms. The RC4 stream cipher shown in the figure is used as PRNG to choose which algorithm will encrypt the plaintext. The other output from RC4 algorithm is encrypted with the second algorithm. The output from the first algorithm and the output from the second algorithm are XORed to get ciphertext of 256-length.

3) Decryption Process

In the decryption process, first step, we encrypt the output from the RC4 by using the other algorithm which is not used to encrypt the plaintext block. Second step, the encrypted output from this algorithm is XORed with the received ciphertext to get C_i. Third step, decrypt C_i using the inverse Double AES-256 which was used in the encryption process to get the plaintext, as shown in Fig.4.

4) Authenticated Encryption

Authenticated Encryption (AE) [1] is a technique used to provide both security and authenticity of transported files and data. AE scheme generally receive the Message (m) and then generate both Ciphertext (C) and authentication Tag (T) during the encryption process to ensure data integrity. The designed Authenticated Encryption architecture is new. This new architecture depends on Tag Partitioning to make the verification of the Tag is faster.

5) Tag Partitioning

Tag partitioning is used to reduce the size of transmitting tag with every plaintext block. Instead, in the designed authenticated encryption architecture, the plaintext file is divided into segments each segment is of 1024 blocks each one contains 32 bytes. At the end of encrypting each segment, an Authentication Tag (AT) is created and attached to the relative segment in the padding [17] of the IP communication protocol to reduce the size of transmission then sent to the receiver side. Therefore, Tag partitioning decrease the time delay of transmission which will make the algorithm faster. Tag partitioning concept consists of the following:

a) Generating Tag, after encrypting the plaintext blocks relative to each segment, Xoring is done to these encrypted ciphertext blocks (C_1, C_2, C_3… C_{1024}) as shows in Figure (5). Authentication Tag (AE) is the result of this Xoring process. The used algorithm to encrypt the plaintext blocks is known to the receiver side. AT = {$C_1 \oplus C_2 \oplus C_3 \oplus \ldots \oplus C_{1024}$}.

b) Tag Checking, to verify the Authentication Tag at the receiver side, Xoring is done to the ciphertexts (C_1, C_2, C_3,…, C_{1024}) relative to each segment. To get these ciphertexts, the encrypted part of the $RC4_1$ output is XORed with the received ciphertext C_{out}, as shown in Figure (6). The seed of the RC4 is known to the receiver side, and the used double AES-256 for encrypting the RC4 output is also known. After receiving the AT from the transmitter side, a comparison is done to compare between the received AT with the created AT at the receiver side. If there is an error between these two tags, the relative segment is retransmitted.

$AT^{\backslash} = \{C_1^{\backslash} \oplus C_2^{\backslash} \oplus C_3^{\backslash} \oplus \ldots \oplus C_{1024}^{\backslash}\}$ (1)
If $AT = AT^{\backslash}$ (2)

Then the Tag is correct
Otherwise retransmit segment

6) Mathematical Model

a) Encryption
For i = 1 or 2 (3)
RC_2 selects which E_1 or E_2 encrypts plaintext (4)
$E_i (P_m) = C_1$ (5)
$E_i (RC_1) = C_2$ (6)
$C_{out} = C_1$ XOR C_2 (7)
As shown in Figure (3), the output Ciphertext (C_{out}) is a function of two inputs which are the encrypted plaintext (C_1) and the encrypted $RC4_1$ (C_2), as shown in equations (3) and (4) where:
E_i is the Encryption Algorithm number **i** (i=1 or 2).
P_m is the plaintext block number **m** (m=1 to 1024).
RC_1 is the output from $RC4_1$ algorithm.

b) Decryption
For i = 1 or 2 (8)
RC_2 selects which E_1 or E_2 encrypts $RC4_1$ (9)
$E_i (RC_1) = C_2$ (10)
C_2 XOR $C_{out} = C_1$ (11)
$Dec_i (C_1) = P_m$ (12)

As shown in Figure (4), in decryption process, the receiver side has the **C_2** which is the $RC4_1$ output that is encrypted using the one encryption algorithm. The **C_2** is XOR between the received Ciphertext **C_{out}** to get the encrypted plaintext **C_1**. Decryption is done to get the plaintext **P_m** by using inverse AES, as shown in equation (10) where:

Dec_i Is the decryption process (inverse AES) of algorithm number i (i=1 or 2).
RC_1 is the output from $RC4_1$ algorithm.
P_m Is the plaintext block number **m** (m=1 to 1024).

c) System Analysis

1. The security level of the proposed algorithm is very high due to the unpredictability concept where the algorithm is computationally secure.
2. The speed of the proposed algorithm is faster than AGEIS where the proposed algorithm processes 32 bytes as AGEIS but with only 3 rounds AES not 5 rounds AES.
3. The security level of Tag generation is high where only the receiver knows the output from $RC4_1$.
4. The cryptanalyst faces many problems such as:
   - $RC4_1$ and $RC4_2$ outputs are not known to the attacker.
   - The attacker does not know which algorithm was used to encrypt the plaintext.
   - Double encryption is used where the proposed algorithm XOR between the two double AES-256 outputs.
   - The overall key length size is 2048 bits.

V. SECURITY OF AESSEA3

1) Security of the AESSEA3 Encryption Architecture

Attacks due to the unpredictability concept where the attacker The proposed algorithm (AESSEA3) is secured against many cryptanalysis is confused which algorithm is used to encrypt the plaintext blocks. AESSEA3 is immune to many cryptanalysis attacks such as:

a) Boomerang Attack.
b) Algebraic Attacks.
c) Slide and Related-Key Attacks.
d) Cross-site Tracing Attack(XST).
e) Interpolation Attack.
f) Higher Order Differential Attacks.
g) Integral Attack (Square attack).
h) Related Key Attacks.
i) Saturation Attack.
j) Forgery Attack .
k) Key-Recovery Attack.

2) Security of Message Authentication

In the introduced algorithm (AESSEA3) the attackers do not have the $RC4_1$ output sequence; also this output is not shared on the communication channel. So, the attackers cannot generate the Authentication Tag which is very hard to predict.

3) Proof of Security From Cryptanalysis Point of View

According to Kerckhoff's principle which states that "A cipher should be secure when the cryptanalyst knows all details of the enciphering process and deciphering process except the value of the secret key". In the proposed Encryption Algorithm architecture, the cryptanalyst knows everything about the encryption algorithm and the overall architecture of the algorithm, but he does not know anything about either the secret keys (2048 bits) used neither the algorithm used to encrypt plaintext nor PRNG controlling sequence. Shannon classifies the security of any Encryption Algorithm to two types:

a) Unconditionally secure "means security against an enemy who has unlimited time and computational resources".
b) Computationally secure "means security against an enemy who has a specified limited amount of time and computational resources".

4) AESSEA3 Cryptanalysis

AESSEA3 is immune to linear cryptanalysis, differential cryptanalysis and algebraic attacks [3].

Proof of Security

1) Linear Cryptanalysis

Linear Cryptanalysis tries to use the advantage of high probability repetition of linear expressions involving plaintext bits and "ciphertext" bits. The idea is to determine the operation of a part of the cipher with an expression that is linear where the linearity is referring to a mod-2 bit-wise operation. Such an expression is of the form:

$$x_1 \oplus x_2 \oplus x_3 \oplus \ldots\ldots\ldots \oplus x_n \oplus y_1 \oplus y_2 \oplus y_3 \oplus \ldots\ldots\ldots \oplus y_n = 0 \qquad (13)$$

Where

x_i represents the *i*-th bit of the input $X = [X_1, X_2, ...]$ and Y_j represents the *j*-th bit of the output $Y = [Y_1, Y_2, ...]$

This equation is representing the exclusive-OR "sum" of u input bits and v output bits. The approach in linear cryptanalysis is to determine expressions of the form above which have a high or low probability of occurrence. Consider that if we randomly selected values for u + v bits and placed them into the equation (11) above, the probability that the expression would hold would be exactly 1/2. It is the deviation or bias from the probability of 1/2 for an expression to hold that is exploited in linear cryptanalysis, the further away that a linear expression is from holding with a probability of 1/2, the better the cryptanalyst is able to apply linear cryptanalysis.

Discussion: Linear cryptanalysis is based on that the algorithm is fixed where the algorithm in AESSEA3 keeps changing for every plaintext; therefore, linear cryptanalysis is impossible to be applicable.

2) Differential Cryptanalysis

Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. For example, consider a system with input $X = [X_1\ X_2\ ...\ X_n]$ and output $Y = [Y_1\ Y_2\ ...\ Y_n]$. In an ideally randomizing cipher, the probability that a particular output difference Δy occurs given a particular input difference Δx is $1/2^n$ where n is the number of bits of x. Differential cryptanalysis seeks to extract a scenario where a particular output difference Δy occurs given a particular input difference Δx with a very high probability P_D (i.e., much greater than $1/2^n$). The pair (Δx, Δy) is referred to as a differential. The two inputs to the system are x' and x'' and the corresponding output are y' and y'' respectively. The input difference is given by

$\Delta x = x' \oplus x''$, hence $\Delta x = [\Delta x_1, \Delta x_2 \ldots\ldots]$ where $\Delta x_i = x_i' \oplus x_i''$, similarly $\Delta y = y' \oplus y''$, hence $\Delta y = [\Delta y_1, \Delta y_2 \ldots\ldots]$ where $\Delta y_i = y_i' \oplus y_i''$

Differential cryptanalysis is a chosen plaintext attack, which means that the attacker is able to select inputs and examine outputs in an attempt to derive the key. For differential cryptanalysis, the attacker will select pairs of inputs, x' and x'', to satisfy a particular Δx, knowing that for that Δx value, a particular Δy value occurs with high probability.

Discussion: Differential cryptanalysis depends on the fact that the algorithm is fixed where in AESSEA3 the algorithm keeps changing for every plaintext; therefore, the differential cryptanalysis is impossible to be applicable.

3) Algebric Cryptanalysis

It is composed of two steps as the following:

a) Collecting Step, The cryptanalyst expresses the cipher as a set of simple equations in a number of variables. These variables include bits (or bytes) from the plaintext, ciphertext and the key.
b) Solving Step, The cryptanalyst uses some data input such as plaintext ciphertext pairs, and then, substitutes these values in the corresponding variables in the set of equations collected in step (***a)*** and try to solve the resulting set of equations, thereby recovering the key. The algebraic equation of AESSEA3 has 768 unknown bits of the key which is very impossible to solve by equations of plaintext and ciphertext pairs.

Discussion: Algebraic cryptanalysis depends on the fact that the algorithm is fixed where in AESSEA3 the algorithm keeps changing for every plaintext; therefore, the algebraic attack is impossible to be applicable.

VI. AESSEA3 PERFORMANCE ANALYSIS

The speed of encryption of the proposed algorithm is measured which is 60 Mbits/Sec to encrypt a file on Laptop Dell Inspiron 15R and the operating system is Windows 7 of 64-bit, Processor Intel® Core™ i7-5400U CPU @ 1.80 GHz and RAM of 8GB. The speed of decryption is almost same as the encryption where the decryption algorithm is double size the encryption algorithm in both software and hardware to provide the same speed of encryption.

The Tag block is transmitted every 1024 plaintext blocks on the IP protocol padding to lower the transmitted data size overheads and to increase the speed of transmitted data.

VII. COMPARISON BETWEEN AGEIS AND AESSEA3

Table 1. COMPARISON BETWEEN AGEIS AND AESSEA3

No.	*Point of Comparison*	*AGEIS*	*AESSEA3*
1	Algorithm	One AES-256	Double AES-256
2	Encryption	Block Cipher	Block Cipher and Stream Cipher
3	Decryption	One AES-256	Double size the Encryption
4	Key size	256 bits	2048 bits
5	Speed	5 rounds AES 36 M bits/Sec	3 rounds AES 60 M bits/Sec
6	Tag Partitioning	No	Yes
7	Tag	Retransmit whole file	Retransmit only wrong segment

Example of Tag Partitioning:
For ordinary authenticated encryption architecture such as (AGEIS), if the transmitter needs to transmit a file of 10 M bits then if the calculated tag is different than the received tag, therefore, the file must be sent again.
For AESSEA3, if the transmitter needs to transmit a file of 10 M bits then if the calculated tag partition is different than the received tag partition, therefore, the segment must be sent again which is 1024 X 256 bits equals 256 K bits.

VIII. CONCLUSION

In this paper, the design and simulation of AESSEA3, new authenticated encryption block cipher architecture is done. This new architecture has high security level and it is immune to many types of cryptanalysis attacks. Also, the algorithm speed is faster than AGEIS where AGEIS is faster than AES CCM, GCM and OCB modes. The speed of the proposed algorithm is 60Mbits/Sec software implementation and the decryption process needs double size of encryption size to maintain the same speed. Also, Tag Partitioning concept is introduced to reduce the time of retransmission of wrong authenticated file.

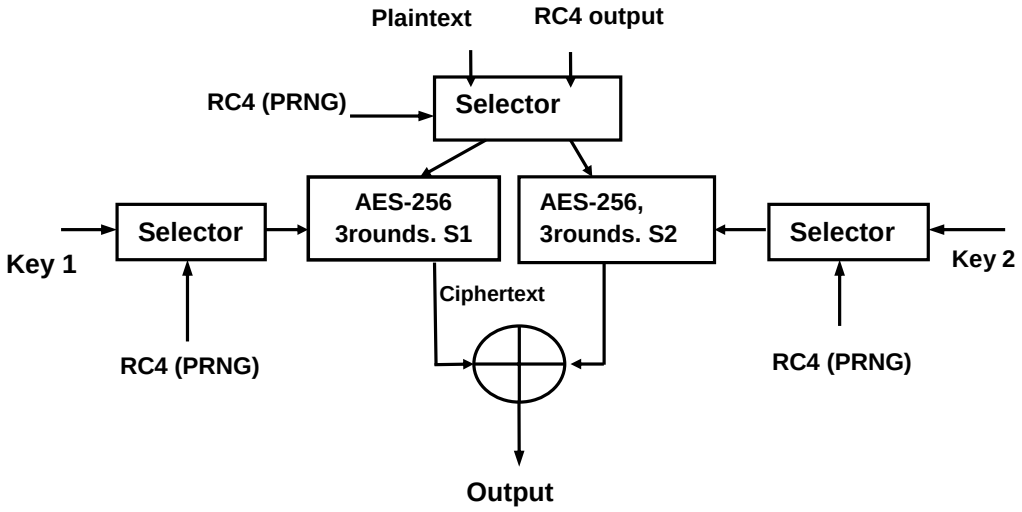

Fig.1. SSEA3 Encryption Architecture

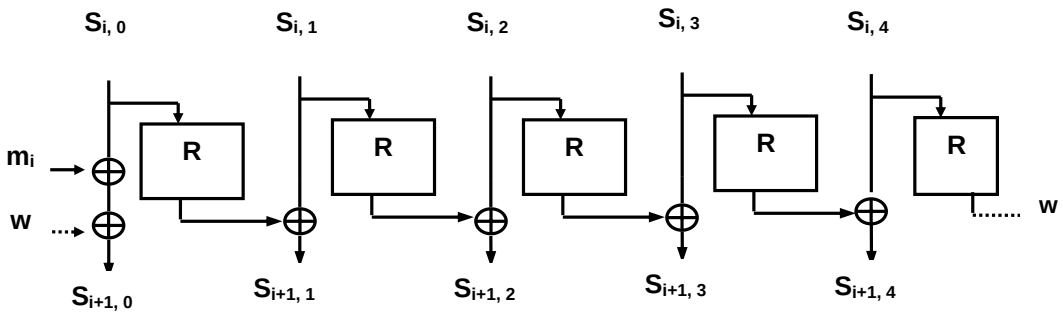

Fig.2. State update function in AEGIS-128L. R indicates AES rounds and w is temporary 16-byte word.

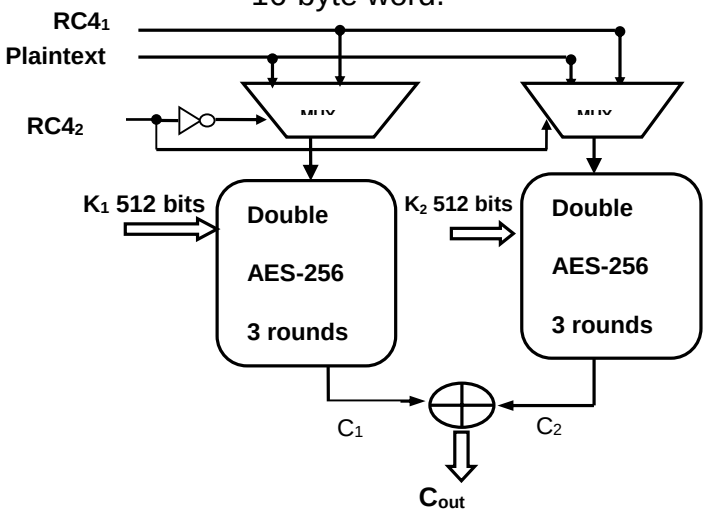

Fig.3. Encryption process

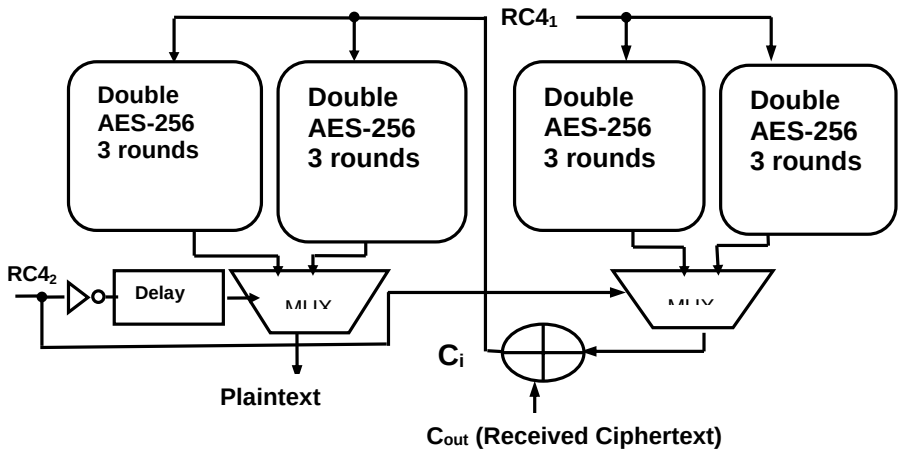

Fig.4. Decryption process

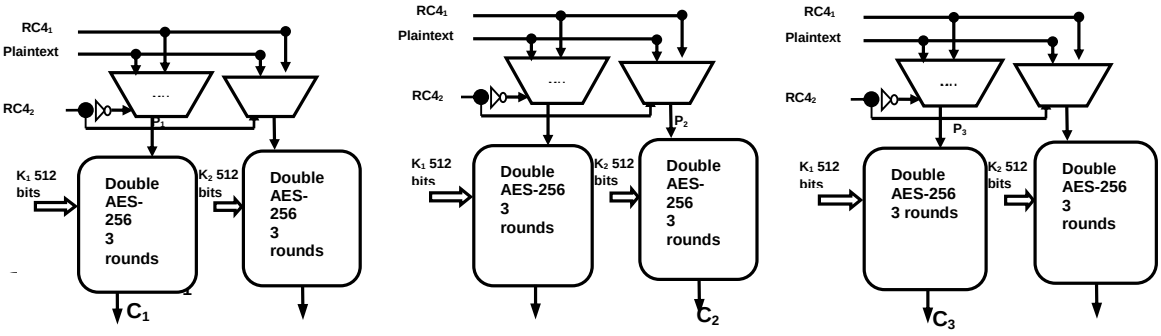

Fig.5. Generating the Authentication Tag (AT)

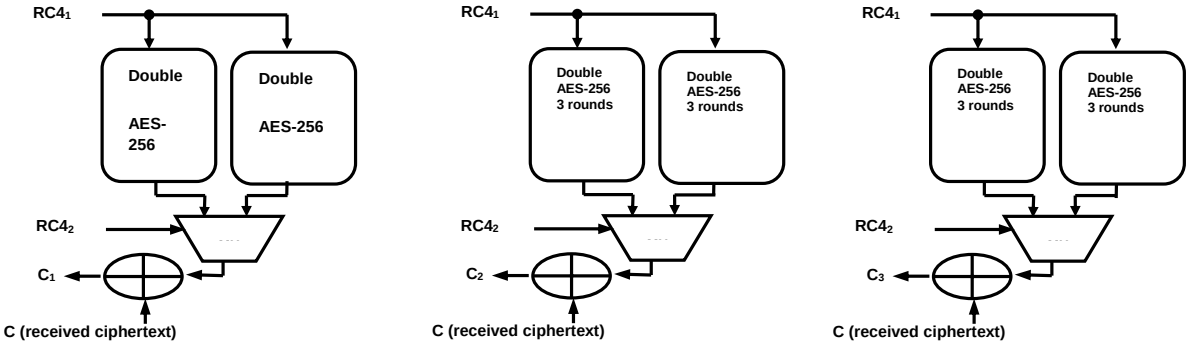

Fig.6. Checking the Authentication Tag

REFRENCES

[1] M. Bellare, P. Rogaway, D. Wagner, “A Conventional Authenticated-Encryption Mode”, April 13, 2003

[2] Mihir Bellare, Chanathip Namprempre, “Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm”, Dept. of Computer Science & Engineering, University of California at San Diego, 9500 Gilman Drive, La Jolla, California 92093, USA.

[3] Mohamed Helmy Mostafa Megahed, “SurvSecSecurity Architecture for Reliable Surveillance WSN Recovery from Base Station Failure”, PhD Thesis, Ottawa University, Ottawa, Canada, 2014

[4]A.G.Chefranov,“Pseudo-Random Number Generator RC4 PeriodImprovement”,Eastern Mediterranean University, Famagusta, North Cyprus and Taganrog State University of Radio Engineering, Taganrog, IEEE2006.

[5] Hongjun WuA, Bart Preneel, “Fast Authenticated Encryption Algorithm (Full Version)”, School of Physical and Mathematical Sciences Nanyang Technological University, SAC 2013

[6] J K M Sadique Uz Zaman, Ranjan Ghosh,“Review on fifteen Statistical Tests proposed by NIST ”, Institute of Radio Physics and Electronics, University of Calcutta92, Acharya Prafulla Chandra Road, Kolkata – 700 009, INDIA, 18th October, 2012.

[7] M. Matsui, “Linear Cryptanalysis Method for DES Cipher”, Advances in Cryptology-EUROCRYPT'93, T. Helleseth, Ed., LNCS 765, Springer-Verlag, pp. 386-397, 1994.

[8] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo1, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee.“HIGHT: A New Block Cipher Suitable for Low-Resource Device”.MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

[9] MARTINVöRöS,“ALGEBRAIC ATTACKS ON CERTAIN STREAM CIPHERS”, Master’s Thesis, Bratislava, 2007.

[10] E. Biham, “New Types of Cryptanalytic Attack Using Related Keys”,Journal of Cryptology, Volume 7, Number 4, pp. 156-171, 1994.

[11] E. Biham, A. Shamir, “Differential Cryptanalysis of the Data Encryption Standard”, Springer-Verlag, 1993.

[12] GustavoBanegas,“Attacks in Stream Ciphers: A Survey”,Department of Computer Science, Federal University of Santa Catarina,and August 26, 2014.

[13] E. Biham, “New Types of Cryptanalytic Attack Using Related Keys”,Journal of Cryptology, Volume 7, Number 4, pp. 156-171, 1994.

[14] Srđan Đorđević, S. Bojanić and O. Nieto-Taladriz,“BDD-based Cryptanalysis of LFSR Stream Ciphers”,Proceedings of Small Systems Simulation Symposium 2010, Niš, Serbia, 12-14 February 2010.

[15] Marco A. Barreno,“The Future of Cryptography under Quantum Computers”,Dartmouth College Computer Science Technical Report TR2002 – 425,July 21, 2002.

[16] Antal Nemes,Viktoria Villanyi and Peter Sziklai, “Quantum Resistant Cryptography”,Budapest Faculty of Science, 2012.

[17]www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfip.pdf