

## Modified 128-EEA2 Algorithm by Using HISEC Lightweight Block Cipher Algorithm with Improving the Security and Cost Factors

Alyaa Ghanim Sulaiman<sup>1</sup>, Sufyan Salim Mahmood AlDabbagh<sup>2</sup>

<sup>1</sup> Department of Software Engineering, University of Mosul, Iraq

<sup>2</sup> Department of Computer Science, University of Mosul, Iraq

---

### Article Info

#### Article history:

Received Jan 9, 2018

Revised Mar 2, 2018

Accepted Mar 18, 2018

---

#### Keywords:

AES-128

Cost

EEA2

HISEC

---

### ABSTRACT

128-EEA2 (Evolved Packet System Encryption Algorithm 2) is a confidentiality algorithm which is used to encrypt and decrypt block of data based on confidentiality key. This confidentiality algorithm 128-EEA2 is based on the AES-128 which is the block cipher algorithm of 128 bit in CTR mode. In this paper, we are going to replace the AES-128 block cipher algorithm by HISEC block cipher algorithm for two reasons such as reducing cost and ameliorate security factor.

Copyright © 2018 Institute of Advanced Engineering and Science.  
All rights reserved.

---

### Corresponding Author:

Sufyan Salim Mahmood Al-Dabbagh,  
Computer Science Department, College of computer science and mathematics,  
Mosul University, Mosul, Iraq.  
Email: sufyansalim\_77@yahoo.com

---

## 1. INTRODUCTION

Beyond 2006, the 3GPP (third generation partnership project) introduced the second set of 4G/LTE cryptographic algorithms 128-EEA2 and 128-EEI2 for confidentiality and integrity respectively. This second set is based on the AES-128 (Advanced Encryption Standard) block cipher algorithm in CTR (Counter Mode) which provide confidentiality to EPS in LTE network [1]. The necessity of the confidentiality protected mode in LTE cryptographic algorithm EEA2 is to create a mask of data before encrypting it that will save time because it run quickly through using the bitwise operations. Based on study [2], AES-128 has drawbacks in its view design and need to improve. Apparently, AES-128 was released before more than a decade whereas the technology was changing year by year. So, with the recent new technology and emerging of huge applications like big data's applications in addition to the applications have run with 64-bit and a lot of other applications, it has become a necessity for designing a new contemporary algorithm for the current demands. Especially young Rijndael that has faded and its sun had set as it has been believed by many researchers. Therefore, AES-128 can be replaced by HISEC lightweight block cipher algorithm to improve the security and decreasing the cost.

## 2. LTE CONFIDENTIALITY ALGORITHM EEA2

Ghizlane ORHANOUE in 2010 inferred that the confidentiality protected mode is necessary in LTE cryptography algorithm EEA because there are some advantages of using this type of ciphering algorithm such as creating a mask of data before encrypting it which this operation is saving time in running time

through using bitwise operations[3]. In Figure (1) below represents the EEA in Encryption/Decryption operations [8].

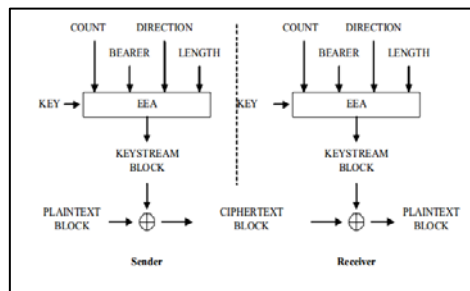


Figure 1. Encryption/Decryption Operation by using EEA [3].

The AES-128 algorithm encrypts each counter block that is obtained in 128 bits of keystream. And each counter block is divided into two parts, the most significant bits and the least significant bits of 64 bits in each. The most significant 64 bits are initialized, as presented before and the least significant 64 bits are initialized by setting zero value to all bits. The least significant 64 bits is part of the counter T is incremented by one mod  $2^{64}$  to generate subsequent counter blocks, each result is formed in another 128 bits of keystream. [1][3].

The role of AES-128 () function is to perform AES-128 encryption under the control of the confidentiality key. The TRUNC () function is responsible of truncating the final output of the operation of AES-128 encryption to the same length as the last plaintext block and then returning the most significant bits. The Figure (2) shows the EEA encryption/decryption mechanism.

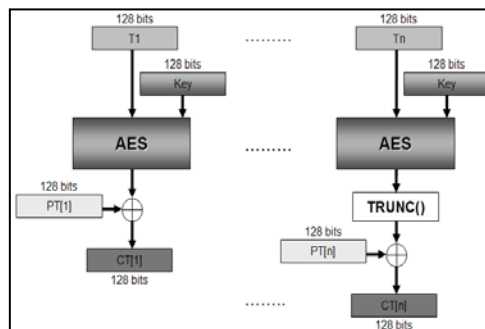


Figure 2. EEA2 (Encryption/Decryption) Mechanisms. [1][3]

### 3. OVERVIEW ON AES-128 ALGORITHM

AES-128 is defined as a symmetric block cipher of 128-bit block size which includes three different key sizes (128 bits, 192 bits, or 256 bits). The 128-bit also called AES-128-128, the 192 bits are called AES-128-192, and the last 256 bits are called AES-128-256, as shown in Figure (3). [4]

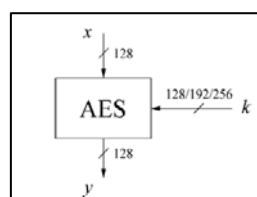


Figure 3. Inputs/Outputs AES-128 Algorithm. [5]

The number of rounds is different according to AES-128 key length. Table 1 represents the size of key, size of block and the round number how they differ with different rounds:

Table 1. Size of Key, Block and Round. [6]

|         | Key Length<br>( <i>NK words</i> ) | Block Size<br>( <i>Nb words</i> ) | Number of Rounds<br>( <i>Nr</i> ) |
|---------|-----------------------------------|-----------------------------------|-----------------------------------|
| AES-128 | 4                                 | 4                                 | 10                                |
| AES-192 | 6                                 | 4                                 | 12                                |
| AES-256 | 8                                 | 4                                 | 14                                |

Rijndael was chosen as the AES-128 in Oct 2000, and in Nov 2001 AES-128 was formally confirmed as the US federal standard. AES-128 algorithm performs the four primary functions are:

- SubBytes()
- ShiftRows()
- MixColumns()
- AddRoundKey()

The internal structure of AES-128 is represented in Figure (4).



Figure 4. Internal Structure of AES-128. [7]

#### 4. PROPOSED LIGHTWEIGHT ALGORITHM (HISEC)

HISEC used the same characteristics of PRESENT but different method for bit permutation. The structure of HISEC algorithm looks like the structure of feistel with some modifications [9] [10] [16]. The HISEC is constructed from sixty-four bits and eighty-bit size of the key and there are fifteen rounds in each round, there are operations like: Substitution box, Bit permutation, XOR, Rotation and key update. Moreover, there is XOR between the cipher text and key in the last round. The HISEC have four layers as following:

- First Layer: in this layer, the 64-bit plaintext is XOR with the 64-bit key. The plaintext divides into two parts. Each part is 32-bit and the results after XOR of each part will be as inputs to the second layer (Substitution box).
- Second Layer: this layer is the most important layer. It produces the confusion property and it gives the nonlinearity to the algorithm. It has 16 4-bit S-boxes and divides them into two parts, each part 8 S-boxes. The output of this layer will be as inputs to the third layer (bit permutation). Also, this

layer uses one S-box and repeats it 16 times. The characteristics of the S-box are the same with good S-box. The values of S-box as shown in Table 2.

Table 2. S-Box Values

|      |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
|------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| X    | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| S(X) | F | C | 2 | 7 | 9 | 0 | 5 | A | 1 | B | E | 8 | 6 | D | 3 | 4 |

- Third Layer: This layer produces the diffusion which is also important part for any strong encryption algorithm. This method of bit permutation applies on two sides and each side is 32-bit.
- Fourth Layer: this layer applies the rotation and XOR operations on both sides. First of all, rotate the left 32-bit and then XOR with right 32-bit. The result will keep in left 32-bit. The next step is to rotate the right 32-bit and XOR with new left 32-bit and the result will keep in right 32-bit.

The key schedule details of updated key procedures in [18]. The Figure (5) shows all layers of HISEC in details.

### 5. SECURITY DISCUSSION

The important tool is cryptanalysis that it can measure the security of any algorithm. Differential, integral and boomerang attacks are applied in this paper for both algorithms (AES-128 and HISEC).

#### 5.1. Differential Cryptanalysis

The minimum active S-box is the most robust way to check the resistance against differential attack [13] [14] [15]. Table 3 explains in term of different cryptanalysis that HISEC is safer than AES algorithm.

Table 3. Active S-Box for (HISEC, AES-128)

| Algorithms  | Active S-boxes |    |    |     |     |
|-------------|----------------|----|----|-----|-----|
|             | 4              | 8  | 12 | 16  | 20  |
| AES-128[19] | 25             | 50 | 75 | 100 | 125 |
| HISEC [18]  | 17             | 43 | 96 | 124 | 166 |

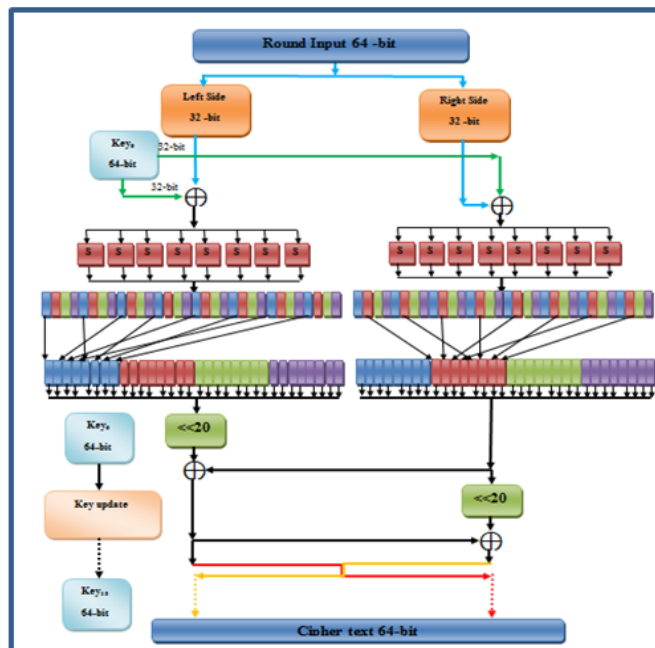


Figure 5. All Layers Together in Details

**5.2. Integral Cryptanalysis**

This another attack that the designer should consider it when he designs an algorithm. Building distinguisher table is the significant step in this attack. After building that table, it can know the round that attack can reach [14]. Table 4 shows the HISEC is stronger than AES-128 algorithm regarding of integral cryptanalysis.

Table 4. Integral Attack for (HISEC, AES-128)

| Algorithms   | Maximum round |
|--------------|---------------|
| AES-128 [17] | 5             |

**5.3. Boomerang attack**

Knowing the active S-boxes number in every step is the first stage to amount this attack. While the second step is to calculating the prospect of recognizer of Boomerang attack. Depending on [15] [18], such attack can reach round 5 with probability of  $2^{-48}$ . Moreover, we calculated the distinguisher probability of boomerang for AES-128 as following:

- In the fourth round there are 25 active S-boxes and in the second round there are 5 active S-boxes.
- Applying equation (1) in order to get the probability.
- The ultimate probability is  $((2^{-2})^{25})^2 \times ((2^{-2})^5)^2 = 2^{-100} \times 2^{-20} = 2^{-120}$ .

Table 5 shows the HISEC algorithm is more secure than AES-128 algorithm in the term of boomerang attack.

Table 5. Maximum round of boomerang attack for HISEC and AES-128 algorithm

| No. | Algorithms | Maximum round | Probability |
|-----|------------|---------------|-------------|
| 1.  | AES-128    | 6             | $2^{-120}$  |
| 2.  | HISEC      | 5             | $2^{-48}$   |

**6. COST DISCUSSION**

This cost is also significant part for designing algorithm. The cost calculation details in [16][17][18]. The Table (6) shows that the cost of HISEC algorithm is less cost than AES-128.

Table 6. Cost for HISEC and AES-128

| Algorithm    | Plaintext | Key | S-box    | Cost    |
|--------------|-----------|-----|----------|---------|
| HISEC [18]   | 64        | 80  | 16- 4bit | 1694 GE |
| AES-128 [20] | 128       | 128 | 8 – 8bit | 2400 GE |

**7. CONCLUSION**

This paper tries to exchange AES-128 algorithm with HISEC algorithm. Also, the dissection of differential, integral and boomerang attacks are shown for AES-128 and HISEC against. The analysis showed that HISEC is more secure than AES-128 algorithms. Moreover, we calculated the cost of HISEC in GE and we compared it with AES-128 algorithm. The comparison showed that the cost of HISEC is less than AES-128 algorithm. Theoretically and from the results above, it can use lightweight block cipher algorithms to secure LTE/4G. Finally, this paper opens the door for deep research to use lightweight algorithms to secure LTE/4G. Our future works, implement the HISEC lightweight algorithm in hardware to verify the results.

**REFERENCES**

[1] Sulaiman, A. G., & Al Shaikhli, I. F. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. *International Journal of Computer Science and Telecommunications*, 5(7), 7-10.

[2] Omar A. Dawood, Othman I. Hammadi. (2017). Analytical Study for Some Drawbacks and Weakness Points of the AES-128 Cipher (Rijndael Algorithm). *The 1<sup>st</sup> International Conference on Information Technology in Erbil*.

[3] Ghizlane Orhanou, S. E. H., Youssef BENTALEB and Jalal LAASSIRI. (2010). EPS Confidentiality and Integrity mechanisms Algorithmic Approach. *IJCSI International Journal of Computer Science*, 7(4).



[4] Conrad, E. (1997). *Advanced Encryption Standard*.

[5] Pelzl, Christof Paar. Jan.(2010).*Understanding Cryptography*:Springer.

[6] Information, F., & 197, P. S. P. (November 26, 2001). Announcing the ADVANCED ENCRYPTION STANDARD (AES-128).

- [7] Stallings, w. (2011). *Cryptography and Network Security Principles And Practice*.
- [8] Sulaiman, Alyaa Ghanim.(2014).*Comparative Study On 4G/LTE Network Security Algorithms*.IIUM, Malaysia.
- [9] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems - CHES 2007." Vol. 4727, Springer Berlin / Heidelberg, 2007, pp. 450-466.
- [10] A. Bogdanov and K. Shibutani, "Generalized Feistel networks revisited," *Designs, Codes and Cryptography*, vol. 66, pp. 75-97, 2013/01/01 2013.
- [11] E. Biham and A. Shamir, "Differential Cryptanalysis of DES Variants," in *Differential Cryptanalysis of the Data Encryption Standard*, Springer New York, 1993, pp. 33-77.
- [12] J.-S. Kang, et al., "Practical and Provable Security against Differential and Linear Cryptanalysis for Substitution-Permutation Networks," *ETRI Journal*, vol. 23, pp. 158-167, 2001.
- [13] Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. *CRYPTO 1990*. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1990).
- [14] L. Knudsen and D. Wagner, "Integral Cryptanalysis," in *Fast Software Encryption*. vol. 2365, J. Daemen and V. Rijmen, Springer Berlin Heidelberg, 2002, pp. 112-127.
- [15] D. Wagner, "The Boomerang Attack," in *Fast Software Encryption*. vol. 1636, Springer Berlin Heidelberg, 1999, pp. 156-170.
- [16] S. Panasenko and S. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches," *International Journal of Computer Theory and Engineering*, vol. vol 3., 2011.
- [17] B. Sun et al., "New Insights on AES-128 Like SPN Ciphers," *In Proceedings, Part I, of the 36th Annual International Cryptology Conference on Advances in Cryptology CRYPTO*, Vol. 9814. Springer-Verlag, 2016, pp. 605-624.
- [18] S.S.M. Aldabbagh et al., "HISEC: A New Lightweight Block Cipher Algorithm". *In Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)*.2014, pp. 151-156.
- [19] Rijmen, V. et al., "On the Four-Round AES-128 Characteristics." *Pre-proceedings of WCC*, 2013, pp. 15-19.
- [20] Moradi, A., Poschmann, A., Ling, S., Paar, C., Wang, H.: Pushing the Limits: a Very Compact and a Threshold Implementation of AES-128. In: *Advances in Cryptology EUROCRYPT 2011 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, vol. 6632, 2011, pp. 69.

#### BIOGRAPHIES OF AUTHORS (10 PT)

|   |  |
|---|--|
|  | <p>Alyaa Ghanim Sulaiman received her bachelor degree in computer science from Mosul university in 2002. She received her master degree in information technology from International Islamic University Malaysia (IIUM) in 2014. She is working at Mosul university as assistant lecturer. Her research interests include security, cryptography and LTE/4G. She is expert in LTE/4G security algorithms.</p>  |
|  | <p>Sufyan Salim Mahmood Al-Dabbagh received his bachelor degree and master degree in computer science from Mosul university in 1999 and 2003 respectively. He received his PhD degree in information technology from International Islamic University Malaysia (IIUM) in 2015. He is working at Mosul university as deputy dean of computer science and mathematics college. His research interests include security, cryptography and LTE/4G. He is expert in block cipher in general and in lightweight block cipher in more specific.</p> |