Advances and Applications in Mathematical Sciences
Volume 21, Issue 3, January 2022, Pages 1287-1301

SECURE HYBRID ENCRYPTION SCHEME BASED ON SPN AND FEISTEL STRUCTURES

C. P. ARYA, R. RATAN and N. VERMA

Scientific Analysis Group
Defence Research and Development Organization
Delhi 110054, India
E-mail: ramratan_sag@hotmail.com
carya28@gmail.com
neelamverma123@gmail.com

Abstract

A hybrid encryption scheme based on SPN and Feistel structures is proposed. In this scheme, the round functions of AES are modified by considering block size 3×3 instead of 4×4. A mathematical logic is formulated to get back the byte element for each round for decryption process. The cryptographic strength of proposed encryption scheme is analysed with respect to avalanche criterion, randomness tests, and cryptanalytic complexity. It is found that the proposed hybrid encryption scheme possesses similar cryptographic characteristics as of AES and has high cryptanalytic complexity.

1. Introduction

In modern era of information technology, the information over open channels can be accessed by an unintended person, the safeguard of vital information is an important task. There are various ways to achieve the security of information by applying the concepts of cryptography, steganography, spread spectrum and secret sharing. The paper is concerned to cryptography to study symmetric key based block ciphers. There are several block cipher specific encryption schemes based on different basic structures [25]. The block ciphers such as AES [13, 35], 3-Way [12], ICEBERG [31], PRESENT [10], PRIDE [3], PRINCE [11], RECTANGLE [36] and PRINT cipher [21] etc. are based on SPN network. In this structure a plaintext and a key are taken as input and then apply on them round

2020 Mathematics Subject Classification: 94A60.
Keywords: Information security, Encryption, block cipher, Avalanche criterion, Randomness.
Received June 17, 2021; Accepted October 11, 2021

functions using substitutions and permutations to produce a cipher text. The block ciphers such as Blowfish [27], Camellia [5], DES [1] and SIMON [9] etc. are based on Feistel structure. Feistel structure was developed by Horst Feistel. In this structure a plaintext and a key is taken as input and plaintext is divided into two equal halves. Round function is applied on half of the plaintext and the output is XORed with other half to produce the cipher text. The Feistel based ciphers are self-invertible. Among all the block ciphers based on SPN, AES is the more efficient and highly secure. A symmetric block cipher which has been developed by Belgium cryptographers Joan Daemen and Vincent Rijmen was submitted to NIST for AES competition in 1997 [1, 13]. After five year's rigorous evaluation process, Rijndael algorithm was declared winner and won the AES title in 2001. AES takes 128 bit as input block with 128 bit, 192 bit or 256-bitkey and gives out 128-bit cipher text. Number of rounds for key length 128 bit, 192 bit and 256 bit are 10, 12 and 14 respectively. It also has key scheduling algorithm which provide random key to each round. The round functions for the AES are Addroundkey, Subbyte, Shiftrow and Mixcolumn [1, 13, 29]. In Subbyte, each byte is replaced with another byte using S-box. The last three rows of the state matrix are shifted cyclically in the Shiftrows. In Mixcolumn, each column of the state matrix are multiplied by a polynomial of degree 4 over the field $GF(2^8)$ under modulo $x^4 + 1$ to get new column. Some customized ciphers designed based on AES are reported in the literature [4, 15, 16, 18, 23, 32]. The light weight design of ciphers are reported for small devices with hardware constraints [23, 24]. The hybrid encryption schemes consisting of two or more algorithms are designed and reported [2, 19, 20, 33]. The key dependent S-box are introduced in the AES [16, 23, 28]. The effect of parameters in AES is also reported in the literature [7, 14, 17, 30].

In this paper, it is attempted to develop a hybrid encryption scheme consisting of SPN and Feistel structures which leads to robust design of block cipher. In proposed hybrid encryption scheme, the AES and DES remain main source of inspiration to design complex structure because some transformations from AES are used with some new transformations and idea of dividing plaintext into equal halves and applying round transformation is from Feistel structure. Although it is not purely Feistel structure because round function is applied in one half partition but in proposed scheme, round function is used on both half partitions. The strength of proposed hybrid

encryption scheme is analyzed with respect to avalanche criterion, randomness tests and computing complexity. It is to be found that the proposed hybrid encryption scheme reflects similar cryptographic characteristics as of AES and high cryptanalytic complexity.

Rest of paper is organized in following manner: The proposed encryption scheme is presented in Section 2. Polynomial generation over field $GF(2^8)$ which is required for rowmix and columnmix round transformations is discussed in Section 3. Decryption process of proposed encryption scheme is explained in Section 4. Computation of byte element required for addition operation in decryption is illustrated in Section 5. Security analysis of proposed encryption scheme is discussed in Section 6. Paper is concluded in last the last followed by the references.

2. Hybrid Encryption Scheme

Hybrid encryption scheme proposed is based on SPN and Feistel structures. It is attempted to form a hybrid structure which consists of partial structures of SPN and Feistel to develop a new block cipher with high cryptographic security and cryp1analytic resistivity against attacks. Like AES, it composes of round transformations such as Subbytes, Partition, Shiftrows and Addround key. Subbytes will play same role as that of in AES with S-box table. Like Feistel structure, new round transformation Partition is introduced which is composed of three transformations such as partition of block into two equal halves, and addition of an element to both halve which gives two blocks of size 3×3, apply rowmix in first block and mixcolum in second block. After this remove the last element from both blocks. Finally concatenate these blocks to get final round output block of size 4×4. Then Shiftrows and addround is applied on the block of size 4×4. same as in AES. In the algorithm S-box and key scheduling algorithm are kept same as those of AES. After analysis it is decided to fix rounds 10 like AES. Because after 10 rounds proposed algorithm give sufficient amount of confusion and diffusion same as that of in AES.

Proposed hybrid encryption scheme consists of four round transformations (i) Subbyte (ii) Partition (iii) Shiftrows (iv) Addround key. Each round transformation is explained below:

2.1.1. Subbyte: In subbyte a byte of block is replaced by new byte using S-box table.

2.1.2. Partition: This round transformation makes the proposed algorithm different from the structure of AES. It is composed of following operations.

(a) Change 4×4 block into a 1×16 block.

(b) Divide 1×16 block into two equal halves of size 1×8.

(c) Add an element to right side of these two blocks. Element to be added is taken from key.

(d) Form blocks of 3×3 from above blocks.

(e) Apply rowmix transformation on first block and mixcolumn transformation on second block.

(f) Form blocks of 1×9 from these blocks of 3×3.

(g) Delete last element of each block.

(h) Concatenate these two blocks which gives a block of 1×16.

(i) Form a block of 4×4.

2.3. Shiftrows: First row of state matrix of size 4×4 remains as it is. The second, third and fourth row are shifted like AES.

2.4. Addround key: This transformation is same as in AES, i.e., XOR the block of 4×4 and key in each round. Key expansion algorithm of AES is used to get a key in each round.

Structure of hybrid encryption is shown in Figure 1.

3. Polynomial Selection

For mixing the row and column of a block, there is a requirement of polynomial of degree 2 over $GF(2^8)$ because each row or column of block can be represented as the polynomial of degree 2 over $GF(2^8)$. Each row and column is multiplied by this polynomial under modulo $x^3 + 1$ [6]. Thus after applying transformations for each row and column using polynomial multiplication, the new column vectors and row vectors are obtained.

There are several polynomials of degree 2 over $GF(2^8)$ but all these are not invertible under modulo x^3+1 being reducible over $GF(2^8)$. A polynomial to be used in encryption process should have its inverse polynomial which is to be used in decryption process. The polynomial $a(x) = \{03\}x^2 + \{04\}x + \{02\}$ over $GF(2^8)$ is used in encryption process and its inverse polynomial $b(x) = \{19\}x^2 + \{F3\}x + \{B8\}$ under modulo x^3+1. The $b(x)$ is used in decryption process. The coefficients of polynomials are written in hexadecimal form. The polynomial $a(x)$ has branch number 3 which is the maximum branch number of polynomial of degree 2.

Same polynomials are used for rowmix and columnmix round transformations 2.1.2(e).

4. Decryption of Hybrid Encryption Scheme

The decryption of proposed hybrid encryption scheme is composed of four different round transformations (i) Inv-subbyte (ii) Inv-partition (iii) Inv-shiftrows (iv) Addround key.

4.1. Inv-Subbyte: For this transformation like AES, each byte of state matrix is replaced by new byte with the help of inverse S-box table.

4.2. Inv-partition: This round transformation comprises of following operations

(a) Make cipher block of 1×16 from the block of 4×4.

(b) Partition cipher block of 1×16 into two halves of 1×8.

(c) Add an element to each block.

(d) Form blocks of 3×3 from each block.

(e) Apply Invrowmix on first block and Invcolumnmix on second block.

(f) Form blocks of 1×9 from first and second blocks.

(g) Delete last elements from both the blocks.

(h) Concatenate of these two blocks.

(i) Finally change size of block of 1×16 into block of 4×4.

4.3. Inv-shiftrow: First row of state matrix remains as it is. Second third and fourth rows of the state matrix are shifted like AES.

4.4. Addround key: A state matrix is added to state matrix of key.

Structure of decryption of hybrid encryption is shown in Figure 2.

5. Element Computation for Decryption

It is a very important and crucial step in which an element is to be added. Unlike encryption, it cannot be added any element in decryption. The element to be added will be determined by relating cipher block and element which already has been added in encryption process. The process of finding element, to be added in decryption, is discussed in following paragraph:

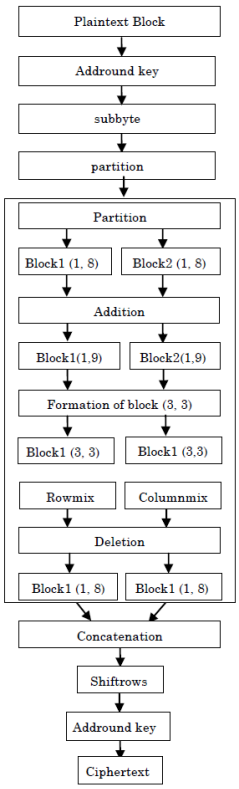

Figure 1. Encryption Structure.

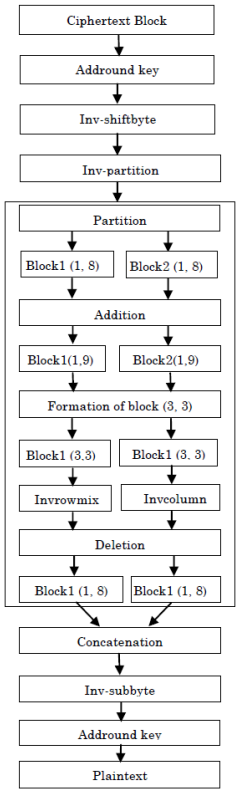

Figure 2. Decryption Structure.

Suppose B be cipher block to be decrypted. Let c be the element which has been added after partition of block in encryption process. Suppose that after adding c last column of block of 3×3 is $[c_0 \ c_1 \ c]$.

Let $a(x) = a_2x_2 + a_1x + a_0$ be a polynomial over $GF(2^8)$ by which each column of block in round transformation is multiplied. Multiply above column by $a(x)$, it gives $[d_0 \ d_1 \ d]$

$$\begin{bmatrix} a_0 & a_2 & a_1 \\ a_1 & a_0 & a_2 \\ a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c \end{bmatrix} = \begin{bmatrix} d_0 \\ d_1 \\ d \end{bmatrix}$$

Let $b(x) = b_2x_2 + b_1x + b_0$ is inverse of $a(x)$

$$\begin{bmatrix} b_0 & b_2 & b_1 \\ b_1 & b_0 & b_2 \\ b_2 & b_1 & b_0 \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ d \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c \end{bmatrix}$$

$$c_0 = b_0d_0 + b_2d_1 + b_1d \quad \text{(a)}$$

$$c_0 = b_1d_0 + b_0d_1 + b_2d \quad \text{(b)}$$

$$c = b_2d_0 + b_1d_1 + b_0d \quad \text{(c)}$$

Here, the aim is to find an element d which is to be added to each block after partition of block in decryption. From equation (c) the element is determined as $d = b_0^{-1}(b_2d_0 + b_1d_1 + c)$ where, $b_0 - 1$ is the inverse of $b_0 \bmod (x^8 + x^4 + x^3 + x + 1)$.

An element c is chosen from the key in such way that it can be retrieved from key to choose an element to be added in decryption. Different element c for encryption and corresponding element d for decryption will be chosen for each round from round key. Thus this element will change in every round. In decryption, we apply Invrowmix on first block and Invcolumnmix on second block and remaining step will be same as of encryption.

6. Analysis of Cryptographic Strength

6.1. Avalanche Criterion: Avalanche criteria shows a drastic change in output for a small change in input. In cryptography, avalanche criteria indicate drastic change in cipher output for a one-bit change in input key. For a block cipher, study of avalanche criteria for a change in key or in plaintext is carried out to see changes in cipher output.

6.1.1. Avalanche criterion on plaintext: The change in output is observed if one input bit in plaintext is changed.

For this data set 1000 plaintexts of 128 bits have been constructed. The change in output is observed in 1 to 10 rounds by changing in each bit of plaintext at one time. In this way observed effect of each bit of 128 bits on the output in each round for the proposed algorithm and AES.

A plaintext gives 129 plaintexts if one bit of plaintext of 128 bits is changed at a time. Thus 1000 plaintexts will give 129000 plaintexts. After observing the changes in output of these plaintexts, it is found that 10 rounds give sufficient diffusion. It is shown in the Figure 3 that effect of each bit of plaintexts of 128 bits on the bits of cipher text is analyzed for proposed algorithm as well as AES. It is clear from the Figure 3 that the number of change in output bits initially is not sufficient but after 10 rounds it approaches to the almost expected value. There is almost same graph for proposed and AES algorithm. It has been observed in the analysis that there is sufficient diffusion in data after 10 rounds.

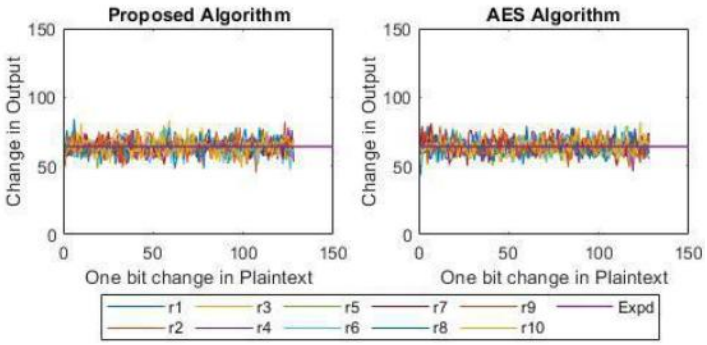

Figure 3. Avalanche effect on output for one-bit change in plaintext after different rounds.

6.1.2. Avalanche criterion on key: The output is observed if one bit of key is changed. For this data set 1000 keys of 128 bits have been constructed. The change in output is observed in 1 to 10 rounds by changing in each bit of key at one time. In this way effect of each bit of 128 bits on the output in each round is observed for proposed and AES algorithm.

A key gives 129 keys if one bit of key of 128 bits is changed. Thus total 12900 keys will be formed in this way. After observing the change in output of these keys, it is found that 10 rounds give sufficient confusion. The effect of each bit of key on the bits of cipher text is observed and plotted in Figure 4 for proposed algorithm and AES. It has been found that number of in output bits is initially not close to expected value (Expd) but it is approaching to expected value after 10 rounds. Hence there is sufficient confusion in the data after 10 rounds.

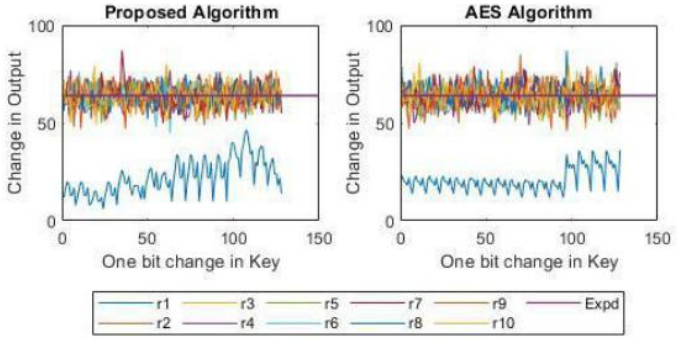

Figure 4. Avalanche effect on output for one-bit change in key.

6.1.3. Average change in output bits for plaintext: Average changes of output bits in 10 rounds is observed for proposed and AES algorithm. For this date set 1000 plaintexts have been generated and observe the average change in output bits by changing in each input bit of a plaintext. Then the average change in output bits in 10 rounds by changing one input bit of plaintext has been observed for each plaintext of 1000 plaintexts. This has been shown in Figure 5. It is clear that the average changes in output bits in 10 rounds are close to expected value (64). It also ensures that there is sufficient diffusion in 10 rounds to resist the cryptanalytic attack.

6.1.4. Average change in output bits for key: Average changes of output bits in 10 rounds are observed for proposed and AES algorithm. For

this data set of 1000 keys has been constructed and observe the average change in output bits by changing each input bit of key. Then average change in output bits in 10 rounds by changing each input bit of a key is observed for each key. The average effect of each bit of a key is shown in Figure 6. It is observed that average changes in output bits in 10 rounds are closed to expected value in both proposed algorithm as well as AES. Thus, it is concluded that there is enough diffusion and confusion in output after 10 rounds. Therefore 10 rounds have been fixed for the proposed algorithm like AES.

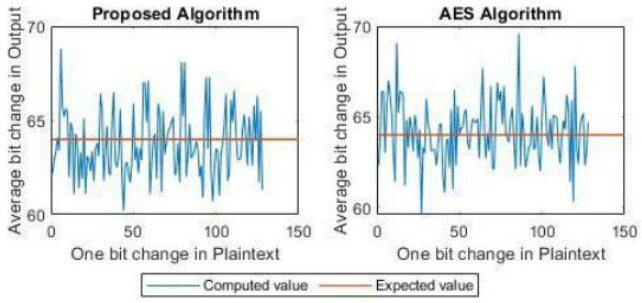

Figure 5. Average change in output for one-bit change in plaintext.

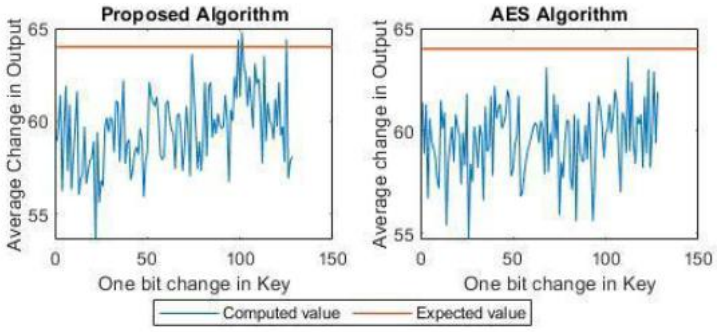

Figure 6. Average Change in output for one-bit change in key.

6.2 Randomness Testing: In order to test randomness of output of the algorithm there is NIST test suite [26]. This suite consists of set of 15 tests that has to be passed by the data if it is random. The data set of 12900 plaintexts and 100 keys have been constructed for the randomness testing. Then stream of output data of length 16512000 bits of proposed and AES algorithm has been generated for each key. Thus 100 data files of length 16512000 have been generated. Then randomness testing is studied using

NIST test suit for each cipher output data file. Test results are shown in Table 1.

Table 1. Randomness testing performance.

S. N.	Name of Test	Proposed Hybrid Encryption		AES Encryption	
		Passed	Failed	Passed	Failed
1	Frequency Test	100	0	100	0
2	Binary Derivative Test	100	0	100	0
3	Change Point Test	100	0	100	0
4	Poker Test	100	0	100	0
5	Runs Test	100	0	100	0
6	Linear Complexity Test	100	0	100	0
7	Longest Run of Ones Test	100	0	100	0
8	Binary Matrix Rank Test	100	0	100	0
9	Approximate Entropy Test	100	0	100	0
10	Lempel Ziv compression Test	100	0	100	0
11	Non-overlapping Template Matchings Test	100	0	100	0
12	Linear Complexity Profile Test	100	0	100	0

It is found that the output bit streams of proposed encryption passed all the tests of randomness. Hence, the output of proposed hybrid encryption is random as similar to AES secure against statistical attacks.

6.3 Cryptanalytic Strength: The mathematical operations used in proposed hybrid encryption are defined on Galois field $GF(2^8)$ like AES. Partition round function makes proposed algorithm different from AES. Add and delete functions are used in partition functions in which an element is added and deleted respectively. Addition and deletion of an element in each round of encryption and decryption makes is mathematically and statistically stronger. The mathematical and statistical analysis becomes very complex because of this operation. When an element is added then it has 256 choices but it is being changed in each round. Therefore, there are 256 choices for first round and corresponding to each choice, there are 256 choices in second

round and so on. In this way, there are 25610 total combinations of the choices for 10 rounds. Hence, this extra complexity added in the proposed algorithm enhances additional security of proposed hybrid encryption in comparison to AES. Because of this, reduced round of attack [8] will become very less effective. Row mix column mix together with the addition and deletion function and s-box provides high nonlinearity and algebraic degree [22, 34] which help to achieve proposed algorithm good resistance against differential and linear attacks.

7. Conclusions

A hybrid encryption scheme based on combination of SPN and Feistel structures has been proposed. Its design is motivated by SPN structure in which SPN functions are dominating. The idea of dividing plaintext into to equal parts has been taken from Feistel structure. The round functions of AES have been used for block size of 4×4 and modified round functions for block size of 3×3 is introduced. In order to apply AES modified round function mixcolumn and mixrow on the half of the plaintext, operations of addition of an element and then deletion of it, has been enforced in each round to get smooth flow of the algorithm. Because of this operation, it makes the hybrid encryption scheme different from AES and enhances the cryptographic strength of proposed hybrid encryption scheme. This makes all possible attacks on it weak and difficult. The avalanche criterion has been carried out for different plaintexts and keys for proposed encryption scheme and AES to check diffusion and confusion characteristics. It has been seen that there is sufficient diffusion and confusion in proposed encryption scheme like AES. The NIST random tests on number of data sets generated from the proposed algorithm are carried out. The cipher output data of proposed encryption scheme have passed all the randomness tests. Finally, it has been shown that the proposed hybrid encryption scheme possesses same cryptographic characteristics as of AES and has high resilient to possible cryptanalytic attacks.

References

[1] Data Encryption Standard (DES), FIPS Standard FIBS PUB 46, (1977).

[2] N. Aghajanzadeh, Aghajanzadeh, Fatemeh and H. R. Kargar, Developing a new Hybrid

Cipher using AES, RC4 and SERPENT for encryption and Decryption, International Journal of Computer Applications 69(8) (2013), 53-62.

[3] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar and T. Yalçin, Block ciphers - focus on the linear layer (feat. PRIDE), In: Juan A. Garay and Rosario Gennaro (eds) Advances in Cryptology - CRYPTO 2014, Lecture Notes in Computer Science 8616 (2014), 57-76.

[4] K. M. Ali and M. Khan, A new construction of confusion component of block ciphers, Multimedia Tools and Applications 78(22) (2019), 32585-32604.

[5] K. Aoki et al., Camellia: A 128-Bit Block Suitable for Multiple Plateforms- Design ans Analysis. In: Stinson D. R., Tavsres S. (eds) Selected Areas in Cryptography SAC 2000. Lecture Notes in computer Science 2012 (2001).

[6] M. Artin, Algebra, Massachusetts Institute of Technology, Mathematics Department, Cambridge USA, Prentice Hall Inc., 1991.

[7] C. P. Arya, R. Ratan and N. Verma, On AES S-boxes with variable modulus and translation polynomials, Proc. CIACIS-21 (to appear).

[8] N. G. Bardeh and S. Rønjom, Practical Attacks on Reduced-Round AES, In: J. Buchmann, A. Nitaj, T. Rachidi, (eds) Progress in Cryptology - AFRICACRYPT, Lecture Notes in Computer Science 11627 (2019).

[9] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks and L. Wingers, The simon and speck lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, DAC '15, New York, NY, USA, (2015).

[10] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: An ultra-lightweight block cipher, In: Pascal Paillier and Ingrid Verbauwhede (eds) Cryptographic Hardware and Embedded Systems – CHES 2007, Lecture Notes in Computer Science 4727 (2007), 450-466.

[11] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knežević, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen and T. Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In: Xiaoyun Wang and Kazue Sako (eds) Advances in Cryptology - ASIACRYPT 2012, Lecture Notes in Computer Science 7658 (2012), 208-225.

[12] J. Daemen, R. Govaerts and J. Vandewalle, A new approach to block cipher design, In: Ross J. Anderson (eds) Fast Software Encryption – FSE'93, Lecture Notes in Computer Science 809 (1994), 18-32.

[13] J. Daemen and V. Rijmen, The Design of Rijindeal: AES- The Advanced Encryption Standard, Springer Verlag, (2002).

[14] S. Das, J. K. MSU, Zaman and R. Ghosh, Generation of AES with various modulus and additive constant polynomial and testing their randomization, Precedia Techol., 10 (2013), 957-962.

[15] O. A. Dawood, A. M. S. Rahma and A. M. J. Abdul Hossen, The new block cipher design (Tigris Cipher), I. J. Computer Network and Information Security 12 (2015), 10-18.

[16] A. Fammy, M. Shaarawy, K. El-Hada, G. Salma and K. Hassanain, A Proposal for A Key-Dependent AES, 3rd International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, (2005).

[17] O. Grosek, S. S. Mangliveras, T. Tapuska and W. Wei, Is Rijndeal Really Independent of the Field Polynomial, Tatra Mt. Math. Publ. 33 (2006), 51-69.

[18] N. Hamdy, K. Shehata, Eldemerdash and Haitham, Design and implementation of encryption unit based on customized AES algorithm, International Journal of videos and Image Processing and Network Security 11(1) (2011), 33-40.

[19] S. Harris, Exploring Cipherspace: Combining stream ciphers and block ciphers, IACR Cryptology Eprint Archive (2008), 473-473.

[20] V. S. Janakiraman, R. Ganesan and M. Gobi, Hybrid Cryptographic algorithm for robust network security, ICGST-CNIR 7(1) (2007).

[21] L. R. Knudsen, G. Leander, A. Poschmann and M. J. B. Robshaw, PRINTcipher: A block cipher for IC-printing. In: Stefan Mangard and François-Xavier Standaert (eds) Cryptographic Hardware and Embedded Systems - CHES 2010, Lecture Notes in Computer Science 6225 (2010), 16-32.

[22] M. Kontak and J. Szmidt, Nonlinearity of the Round Function, Control and Cybernetics 36(4) (2007), 1037-1044.

[23] G. N. Krishnamurthy and V. Ramaswamy, Making AES Stronger: AES with Key Dependent S-Box, IJCSNS International Journal of Computer Science and Network Security 8(9) (2008), 388-398.

[24] M. Kumar, S. K. Pal and A. Panigrahi, FeW: A lightweight block cipher, Turk. J. Math. Comput. Sci. 11(2) (2019), 58-73.

[25] A. Mileva, V. Dimitrova, O. Kara and M . J. Mihaljević, Catalog and Illustrative Examples of Lightweight Cryptographic Primitives, In: Hernandez-Castro J. (eds) Security of Ubiquitous Computing Systems. Springer Cham (2021), 21-47.

[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert and J. Dray, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST Special Publication, SP 800-22 Revision-1a (2010). http://www.nist.gov.

[27] B. Schneier, Description of a new variable-length key, 64-bit block cipher (Blowfish), In: Anderson R. (eds) Fast Software Encryption, FSE 1993, Lecture Notes in Computer Science 809 (1994).

[28] A. Seghier, J. Li, D. A. Zhi, DA and Sun, Advanced encryption standard based key dependent S-box cube, IET Information Security 13(6) (2019), 552-558.

[29] W. Stallings, Cryptography and Network Security, Fourth Edition, Pearson Education, (2003).

[30] S. D. Sinha and C. P. Arya, Algebraic construction and cryptographic Properties of Rijndael Substitution Box, Defence Science Journal 62(1) (2012), 32-37.

[31] F. X. Standaert, G. Piret, G. Rouvroy, J. J. Quisquater and J. D. Legat, ICEBERG: An

involutional cipher efficient for block encryption in reconfigurable hardware, In: Bimal K. Roy and Willi Meier (eds) Fast Software Encryption - FSE 2004, Lecture Notes in Computer Science 3017 (2004), 279-299.

[32] A. A. Thinn, and M. M. S. Thwin, Modification of AES algorithm by using second key and modified subbytes operation for text encryption, Computational Science and Technology (2019), 435-444.

[33] C. G. Thorat and V. S. Inamdar, Implementation of new hybrid lightweight cryptosystem, Applied Computing and Informatics, (2018).

[34] T. Tiessen, L. R. Knudsen, S. Kibble and M. M. Lauridsen, Security of the AES with a secret S-box, Int. Workshop on fast software encryption (FSE) 2015, Lecture Notes in Computer Science 9054 (2015), 175-189.

[35] Advanced Encryption Standard (AES), Federal Information Processing Standards Publications (FIPS 197) 26 Nov. (2001).

[36] W. T. Zhang, Z. Z. Bao, D. D. Lin, V. Rijmen, B. H. Yang and I. Verbauwhede, Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms, Science China Information Sciences 58(12) (2015), 1-15.