Global Journals LaTeX JournalKaleidoscope™

Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

Robust Performance and Resistance to Attack for the Advanced Encryption Standard using Dynamic Rotation

Dr. Mohamed Abd Elhamid Ibrahim[1]

[1]

Received: 3 February 2015 Accepted: 4 March 2015 Published: 15 March 2015

Abstract

Recently, the Rijndael algorithm has been uniform by the National Institute of Standards and Technology (NIST) as the Advanced Encryption Standard (AES). This makes AES a vital and necessary data-protection mechanism for federal agencies in the US and other countries. In AES, rotation occurs in key expansion, ciphering, and deciphering. Rotation is vital for confusion and diffusion, which play an important role in any cryptography technique. Confusion and diffusion make breaking the key complex and difficult. This paper studies the effect of reconfiguring the structure of AES, especially replacing constant rotation with variable rotation. The resulting producing another cipher is called Dynamic Rotation for Advanced Encryption Standard (DRAES). DRAES with variable rotation raises the complexity of the algorithm, and thus, increases the time consumed for brute-force attacks. We measured the diffusion of AES and DRAES algorithms. DRAES reached acceptable level of diffusion faster than AES.

Index terms— AES, DRAES, confusion and diffusion.

1 Introduction

he National Institute of Standards and Technology (NIST), a non-regulatory federal agency, standardized the Advanced Encryption Standard (AES) as Federal Information Processing Standard (FIPS) 197. Prior to AES, the Data Encryption Standard (DES) was the federal standard for block symmetric encryption FIPS 46 in 197 [7].In June 2003 the US government has approved the use of 128, 192, 256 bit key AES for secret and 192, 256-bit key AES for topsecret information. Now, after the publication of FIPS 197, AES encryption remains the de facto standard for symmetric encryption, and non-brute-force attacks remain impossible [1,2], at least for the foreseeable future. To date, most attack methods have focused on weaknesses or characteristics in specific implementations, called side-channel attacks, not on the algorithm itself. However, AES has been remarkably resilient to these attacks [3][4][5][6].

In the last ten years, AES has been subject to very intensive cryptanalysis, with best currently known attacks breaking 7, 10, 10 rounds for respective key sizes 128, 192, 256,with very high complexities. In this work, we propose Dynamic Rotation AES (DRAES), a modification and enhancement of the rotation in AES.

The following section contains the evaluation of AES with constant rotation. Dynamic rotation with DRAES is presented in Section III. Diffusion analysis is assessed for both AES and DRAES algorithms in Section IV. Finally, Section V contains conclusions.

2 II. Evaluation of Advanced Encryption Standard

On the inside ofthe AES algorithm, processes are executed on a two-dimensional array of bytes called the state. The state consists of four rows of bytes, each containing Nb bytes, where Nb is the block length divided by word size (32 bits). Nb=4 for 128-bit block, Nb=6 for 192-bit block, Nb=5 for 160-bit block, and Nb=8 for 256-bit block.

The number of words in the key is called Nk. Ciphering is done by a series of mathematical operations iteratively. The number of rounds (iterations) is represented by Nr, where Nr =10 when Nk = 4, Nr = 12 when Nk = 6, and Nr = 14 when Nk = 8. In other words, the key length and the number of rounds differ from key size to key size as shown in Table 1. A block size of 128 bits is assumed. The components of the AES encryption algorithm are described next.

3 a) Sub Bytes Transform

In the Sub Bytes phase, the data in the plaintext are substituted by some pre-defined values from a substitution box. The substitution box, which is used commonly, is an AES substitution box (S-box table **??**.

Figure **??** demonstrates that the substitution box (S-box) is invertible and non-linear. Sub Bytes are the only nonlinear operation in AES. Nonlinearity is important for any encryption algorithm. s" 0,0 s" 0,1 s" 0,2 s" 0,3 s" 1,0 s" 1,1 s" 1,2 s" 1,3 s" 2,0 s" 2,1 s" 2,2 s" 2,3 s" 3 , 0 s" 3 , 1 s" 3 , 2 s" 3 , 3 s" r,c

4 S-box s r,c c) Mix Columns Transform

The Mix Columns transformation operates on the State column-by-column, treating each column as a four-term polynomial. The columns are considered as polynomials over GF (28) and are multiplied modulo x4 + 1 with a fixed polynomial c(x), given by c(x) = c 0 + c 1 x + c 2 x 2 + c 3 x 3 (3) Wherec 0 =0x02 , c 1 =0x01 , c 2 =0x02 , c 3 =0x03. This can be written as matrix multiplication: b(x) = c(x) ? a(x), Where W i isa word from the key schedule, and round is a value in the range 0 ? round ? Nr. In the AES encryption, the initial Round Key addition occurs when round = 0, the application of the Add Round Key transformation to the Nr rounds of the Cipher occurs when 1? round ? Nr. The process of Add Round Key transformation is demonstrated in Figure4, andFigure5 illustrates the AES encryption and decryption processes. The key is copied into the first four words of the expanded key. The remainder of the expanded key is filled in four words at a time. Each added word W [i] depends on the immediately preceding word, W [i-1], and the word four positions back **??**i -4]. In three out of four cases, a simple XOR is used. For a word whose position in the w array is a multiple of 4, a more complex function is used. Figure 7 illustrates the generation of the first eight words of the expanded key, using the symbol g to represent that complex function. The function g consists of the following sub functions:

? Rotation executes a one-byte circular left shift on a word. This means that an input word[b 0 , b 1 , b 2 , b 3] is transformed into [b 1 , b 2 , b 3 , b 0].

? SubWord achieves a byte substitution on each byte of its input word, using Sbox.

? The result of steps 1 and 2 is XORed with a Round constant (Rcon[j])

The round constant is a word in which the three rightmost bytes are always 0. The round constant is different for each round and is defined as Rcon

5 Dynamic Rotation AES (DRAES)

The main purpose of rotation is to mix all data elements in different columns of state. As such, rotation is important for confusion and diffusion [8], which both plays an essential role in cryptography. Confusion refers to making the output dependent on the key. Ideally, every key bit influences every output bit.

Diffusion is making the output dependent on previous input (plain and cipher ext). Ideally, every previous input bit influences each output bit. One aim of confusion is to make it very hard to find the key even if one has a large number of plain text-ciphertext pairs produced with the same key. Therefore, each bit of the ciphertext should depend on the entire key and in different ways on different bits of the key. The Rot Word rotation in key expansion occurs 10 times in DRAES similar to AES for key length of 128 bits (Nk= 4). Table 3 and Figure 8 show a comparison between AES and DRAES. [i-1] = (b0,i-1b1,i-1b2,i-1b3,i-1) 11. temp= (b0,i-1 ? b 1,i -1 ? b 2,i -1 ? b 3,i -1) 12. if (temp mod Nk == 0) 13. W[i-1]=(b1,i-1b2,i-1b3,i-1b0,i-1)

6 b) Add Round Key rotation in DRAES

The modification of rotation in the ciphering process is vital; the change from constant shift-row to variable shift-row make the rotation amount hard to guess, which increases confusion and diffusion. In AES, row 0 is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes. In DRAES, rotationamount is variable and done with the following procedure. Rotation b 0,i-1 b 1,i-1 b 2,i-1 b 3,i-1 B 1,i-1 B 2,i-1 B 3,i-1 b 0,i-1 Rotation b 0,i-1 b 1,i-1 b 2,i-1 b 3,i-1 B 1,i-1 B 2,i-1 B 3,i-1 b 0,i-1 B 2,i-1 B 3,i-1 B 0,i-1 B 1,i-1 B 1,i-1 B 2,i-1 B 3,i-1 b 0,i-1 b 3,i-1 B 0,i-1 B 1,i-1 B

7 c) DRAES in inverse cipher

The rotation in inverse cipher is the same process for the DRAES In cipher that described in sec. b Except for the shift row instead of shift row left, the shift row is right. Table 4 explain the variation between DRAES and AES for cipher 1,1 b 1,2 b 1,3 b 1,0 b 1,1 b 1,2 b 1,3 b 1,0 b 1,2 b 1,3 b 1,0 b 1,1 b 1,3 b 1,0 b 1,1 b 1,2 b 1,1 b 1,2 b 1,3 b 1,0 possible rotation for row 2 in state b 2,1 b 2,2 b 2,3 b 2,0 b 2,1 b 2,2 b 2,3 b 2,0 b 2,2 b 2,3 b 2,0 b 2,1 b 2,3 b 2,0 b 2,1 b 2,2 b 2,1 b 2,2 b 2,

8 VI. Draes with Confusion and Diffusion

A strong cipher should contain both Confusion and diffusion. Claude Shannon, develop this concepts [9]. Confusion and diffusion are two techniques that symmetric ciphers should satisfy to thwart cryptanalysis. In a block cipher with good diffusion, if one bit of the plaintext digit is changed, then affects many cipher text digits in a random mode. Cryptographic diffusion test is a kind of statistical test that evaluates a block cipher for diffusion. The performance analysis can be done with various measures such as Diffusion analysis of DRAES and AES VII.

9 Diffusion Analysis

Diffusion makes the ciphertext dependent on previous plaintext and ciphertext. Diffusion is important for any block cipher, more specifically AES and DRAES algorithms. The impact of diffusion can be measured by the Strict Avalanche Criterion (SAC) [10], which is satisfied when at least 50% of bits in the ciphertext are changed in response to a one-bit flip in the plaintext or key.

Table 5 shows the SAC for both DRAES and AES when changing a single bit of plaintext while keeping the key constant. Table 6 shows the SAC for both DRAES and AES when changing a single bit of key while keeping the plaintext constant. Table 7 shows the SAC for both DRAES and AES when changing 3 bits of plaintext while keeping the key constant. Table 8 shows the SAC for both DRAES and AES when changing 3 bits of key while keeping the plaintext constant.

10 Global Journal of C omp uter S cience and T echnology

Volume XV Issue VI Version I Year ( ) The outcome in Table 8 present Avalanche effect SAC is achieved for DRAES and AES in same first round, but SAC 60% for DRAES is greater than SAC for AES and greater in number of bits are altered (666 bits) than AES (599 bits).

V.

11 Conclusion

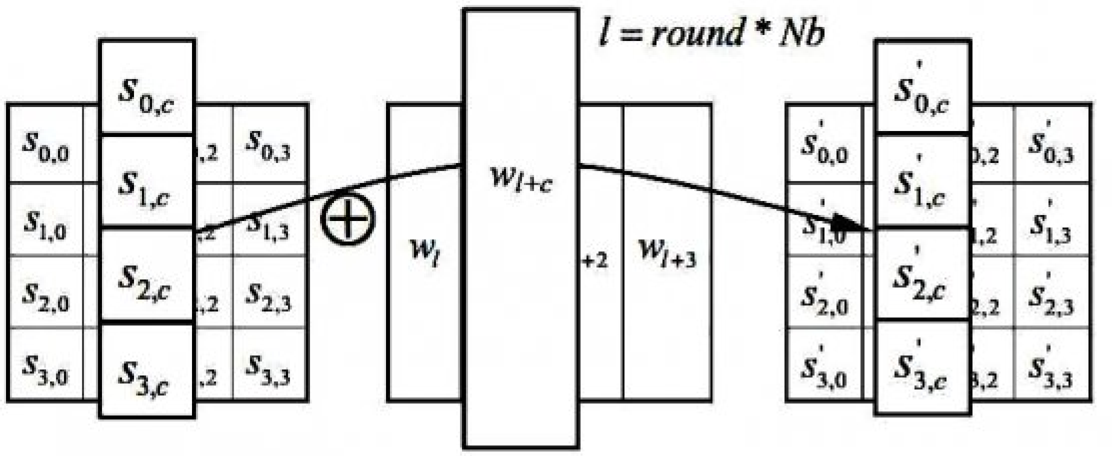
With Dynamic rotation for advanced encryption standard DRAES the confusion and diffusion is stronger than rotation that occur in AES, that mean that Rijndael is more safe and physically powerful with dynamic rotation when compared to Rijndael with constant rotation as shown from results from tables that related with diffusion analysis. [1,2]

12

Figure 1: Figure 1 :Figure 2

2 ShifRows ()

Figure 2: Figure 2 :



3

Figure 3: Figure 3 :

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

456

Figure 4: Figure 4 :Figure 5 :Figure 6 :

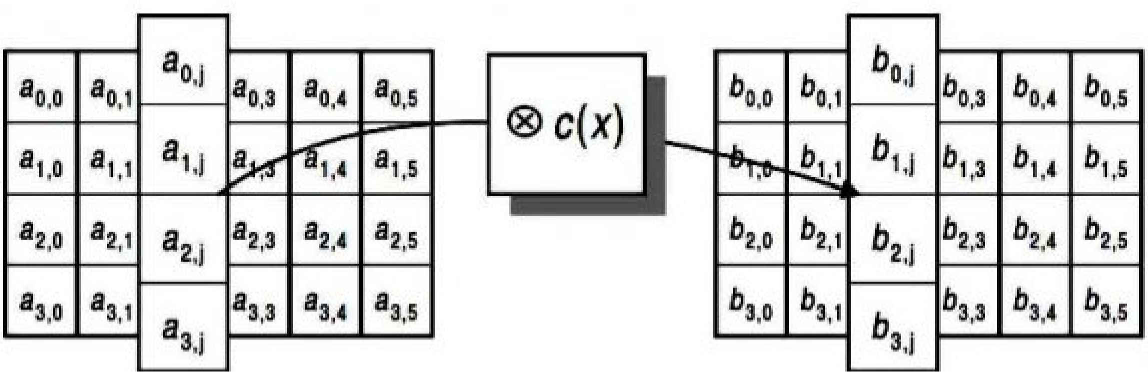


Figure 5:

7

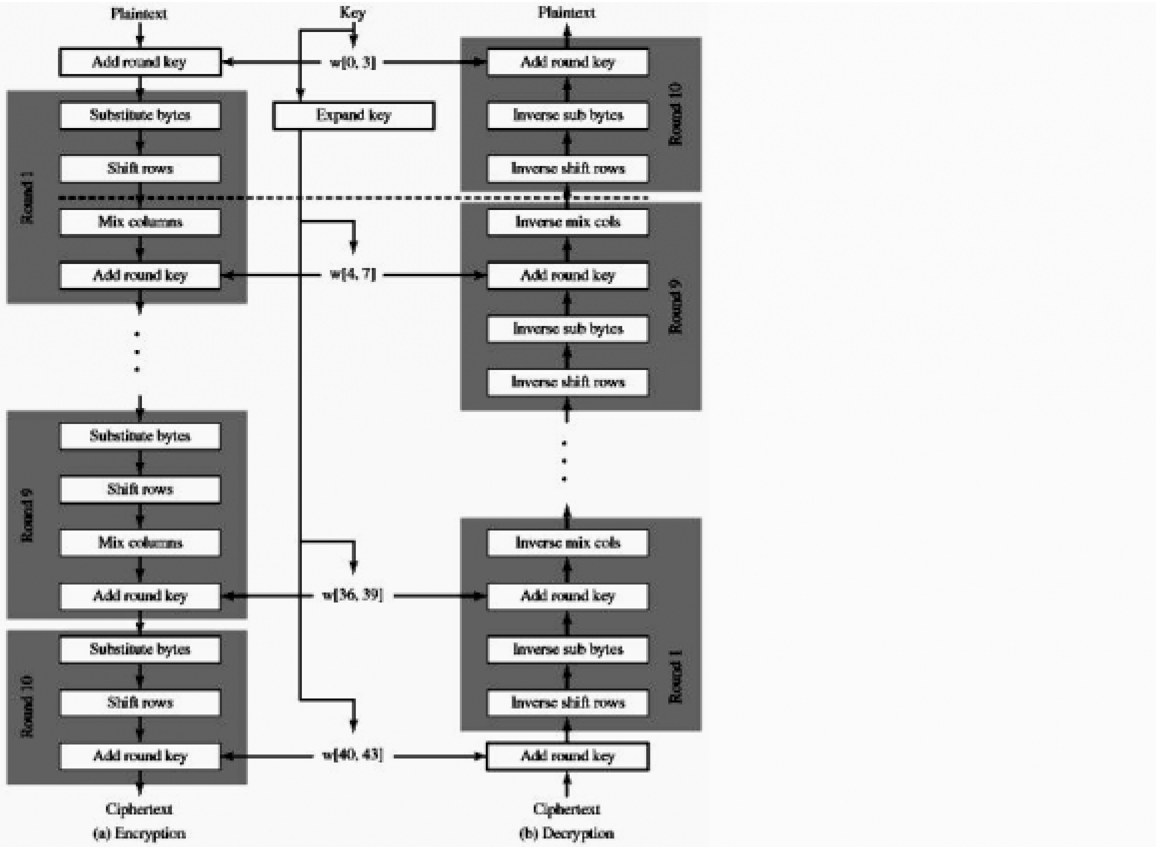


Figure 6: Figure 7 :

[1] Robust Performance and Resistance to Attack for the Advanced Encryption Standard using Dynamic Rotation

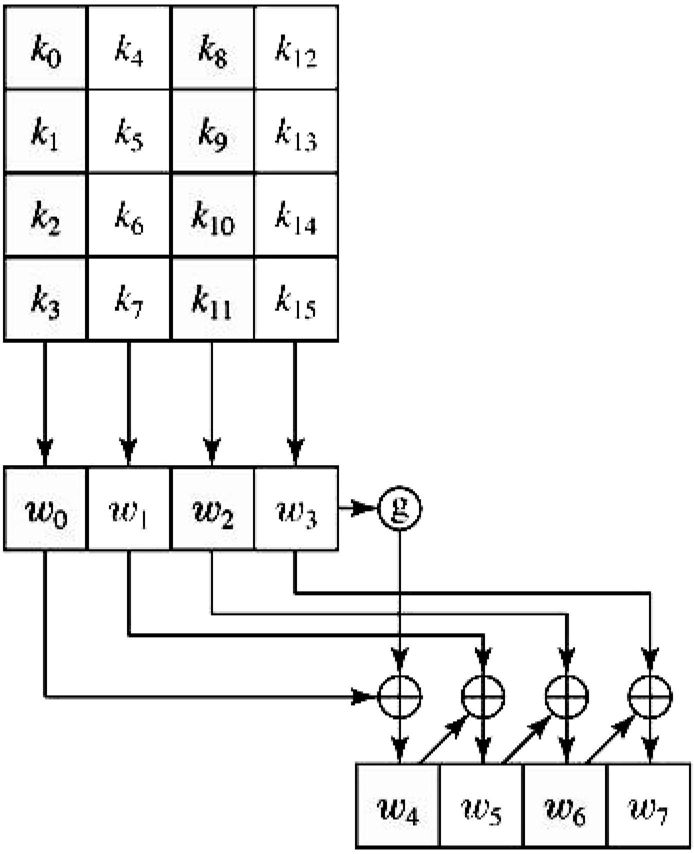


Figure 7:

1

Algorithm	Key length (Nk words)	Block Size (Nb words)	Number of rounds (Nr)
Aes-128-bit	4	4	10
Aes-160-bit	5	4	11
Aes-192-bit	6	4	12
Aes-256-bit	8	4	14

Figure 8: Table 1 :

2

j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

Figure 9: Table 2 :

3

DRAES	AES

Figure 10: Table 3 :

	III. If (Temp mod Nb=0)
	IV. Shift left by one-byte to enforce rotation
	V. else if (Temp mod Nb =1)
	VI. Shift left by one byte
	VII. Else if (Temp mod Nb =2)
	VIII. Shift left by Two byte
	IX. Else (Temp mod Nb =3)
	X. Shift left by three bytes
	XI. // end if and end of ShiftRows (state)
	8. MixColumns (state)
	9. AddRoundKey (state, RoundKey)
	10. // end for
length divided by 32	11. Sub Bytes (state) // final round state
3. NR=10 //number of round for key 128 bit, NR=12	12. Shift Rows (state)
for key 192 bit and NR=14 for key 256 bit	XII. read each row in state
4. Add Round Key(state, Round key)	XIII. Sum the elements in each row in Temp using
5. For round = 1 step 1 to Nr-1	Xor
6. Sub Bytes (state, s_box)	XIV. If (Temp mod Nb =0)
7. Shift Rows (state) // the rotation for each row	XV. Shift left by one byte // to enforce rotation
individually in state	XVI. else if (Temp mod Nb =1)
I. read each row in state	XVII. Shift left by one byte
II. Sum the elements in each row in Temp using Xor	XVIII. Else if (Temp mod Nb =2)

Figure 11:

4

DRAES	AES

Figure 12: Table 4 :

5

Round	Number of bit altered		SAC	Round	Number of bit altered		SAC
1	11	9%	N	1	16	13%	N
2	50	40%	N	2	72	57%	Y
3	77	61%	Y	3	61	48%	N
4	59	47%	N	4	63	50%	Y
5	60	47%	N	5	63	50%	Y
6	69	54%	Y	6	64	50%	Y
7	63	50%	Y	7	83	65%	Y
8	65	51%	Y	8	61	48%	N
9	60	47%	N	9	63	50%	Y
10	66	52%	Y	10	60	47%	N
		(a) AES		(b) DRAES			
As shown in							

Figure 13: Table 5 :

6

Round	Number of bit altered		SAC	Round	Number of bit altered		SAC
1	36	29%	N	1	64	50%	Y
2	63	50%	Y	2	60	47%	N
3	66	52%	Y	3	69	54%	Y
4	55	43%	N	4	61	48%	N
5	72	57%	N	5	67	53%	Y
6	65	51%	Y	6	58	46%	N
7	54	43%	N	7	68	54%	Y
8	63	50%	Y	8	66	52%	Y
9	63	50%	Y	9	70	55%	Y
10	66	52%	Y	10	67	53%	Y
		(a) AES			(b) DRAES		
The conclusion result in Table 6demonstrate Avalanche effect SAC is achieved more rapidly in				DRAES than AES in first round with SAC 50%, while t SAC for AES is completed in second round			

Figure 14: Table 6 :

7

Round	Number of bit altered		SAC	Round	Number of bit altered		SAC
1	28	22%	N	1	28	22%	N

Figure 15: Table 7 :

8

Round	Number of bit altered		SAC	Round	Number of bit altered		SAC
1	58	58%	Y	1	76	60%	Y
2	57	57%	Y	2	65	51%	Y
3	66	66%	Y	3	63	50%	Y
4	61	61%	Y	4	66	52%	Y
5	56	56%	Y	5	73	58%	Y
6	61	61%	Y	6	71	56%	Y
7	55	55%	Y	7	66	52%	Y
8	63	63%	Y	8	60	47%	N
9	65	65%	Y	9	63	50%	Y
10	57	57%	Y	10	63	50%	Y

(a) AES (b) DRAES

Figure 16: Table 8 :

.1 Global Journals Inc. (US) Guidelines Handbook 2015

www.GlobalJournals.org

[Vaudenay ()] *A CLASSICAL INTRODUCTION TO MODERN CRYPTOGRAPHY*, Serge Vaudenay . 2006. Springer Science+Business Media, Inc.

[Lokeshwari et al. (2012)] 'A CONFIGURABLE SECURED IMAGE ENCRYPTION TECHNIQUE USING 3D ARRAY BLOCK ROTATION'. G Lokeshwari , . S Dr , G Kumar , Aparna . *International Journal of Engineering Science and Technology (IJEST)* January 2012. 4 (01) .

[Biryukov et al. ()] 'Distinguisher and Related-Key Attack on the Full AES-256'. Alex Biryukov , Dmitry Khovratovich , Ivica Nikolic . *Advances in Cryptology-CRYPTO 2009: 29th Annual International Cryptology Conference*, (Santa Barbara, CA, USA) August 16-20, 2009. 2009. Springer. 5677.

[Barkan and Biham ()] 'In How Many Ways Can You Write Rijndael'. E Barkan , E Biham . *Advances in Cryptology -ASIACRYPT 2002: 8th International Conference on Theory and Application of Cryptology and Information Security*, Y Zheng (ed.) 2002. Springer-Verlag. 2501 p. .

[Kumar ()] 'Investigations in Brute Force Attack on Cellular Security Based on Des and Aes'. Neeraj Kumar . *IJCEM International Journal of Computational Engineering & Management* 2011. 14.

[Krishnamurthy and Ramaswamy ()] 'Making AES stronger: AES with key dependent S-box'. G N Krishnamurthy , V Ramaswamy . *IJCSNS International Journal of Computer Science and Network Security* 2008. 8 (9) p. .

[Lu et al. ()] 'New impossible differential attacks on AES'. Jiqiang Lu , Orr Dunkelman , Nathan Keller , Jongsung Kim . *Progress in Cryptology-INDOCRYPT 2008*, (Berlin Heidelberg) 2008. Springer. p. .

[Drakakis et al. ()] 'On the Nonlinearity of Exponential Welch Costas Functions'. Konstantinos Drakakis , Verónica Requena , Gary Mcguire . *IEEE TRANSACTIONS ON INFORMATION THEORY* 2010. 56 (3) .

[Mohan and Reddy (2011)] 'Performance Analysis of AES and MARS Encryption Algorithms'. H S Mohan , Reddy . *IJCSI International Journal of Computer Science Issues* July 2011. 8 (1) .

[Bernstein ()] 'Understanding brute force'. Daniel J Bernstein . *Workshop Record of ECRYPT STVL Workshop on Symmetric Key Encryption, eSTREAM report*, 2005. 36.