Data based Transposition to Enhance Data Avalanche and Differential Data Propagation in Advanced Encryption Standard

Paul A.J.
Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India.

Saju A.
Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India.

Lekshmi R. Nair
Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India.

ABSTRACT
In symmetric block ciphers, substitution and transposition operations are performed in multiple rounds to transform plaintext blocks into ciphertext blocks. In advanced Encryption Standard (AES) the transposition of data is facilitated by shift row and mix column operations. In Matrix Array Symmetric Key (MASK) Encryption, a block cipher proposed by the author, the data transposition is achieved by data based rotations. The data based transposition procedure offers two advantages. First, it is simple to implement and secondly, the procedure produces a strong data avalanche effect and differential data propagation. In this paper the possibility of improvising the performance of AES using data based transposition in its diffusion rounds is examined. As a case study, the data based transposition procedure has been introduced in AES. The data avalanche and differential data propagation produced in AES have been observed. The paper describes the data based transposition procedure and the enhanced data avalanche and differential data propagation produced in AES. It has been shown that, the data avalanche effect and differential data propagation characteristics of AES have been improved.

General Terms
Encryption Algorithm, Diffusion Round, Symmetric Block Cipher, Cryptographic Transformation.

Keywords
Ciphertext, Data based transposition, Data avalanche, Differential data propagation, Plaintext, Secret key

1. INTRODUCTION
Advanced Encryption Standard is a symmetric block cipher with a block size of 128 bits and key size of 128, 192 and 256 bits. AES has been a symmetric key encryption standard since 2002 and has remained secure till date. Many attempts to crack AES have not been successful. The use of insecure communication channels requires some kind of encoding of information to deal with security attacks [1]. Encryption is a powerful tool to provide information security [2]. There are two classes of cryptographic procedures in use, referred to as i) Symmetric-key cryptography (SKC) and ii) Public key cryptography (PKC). Public-key algorithms are slow, whereas Symmetric-key algorithms generally run much faster [3]. Symmetric-key cryptography has been (and still is) extensively used to solve the traditional problem of communication over insecure channels [4]. The block ciphers such as DES (Data Encryption Standard) [5], AES [6], and EES (Escrowed Encryption Standard) [7] are used for information security services worldwide. DES, due to its smaller (56 bits) key size, has become vulnerable to brute force attack and is no longer secure. A desirable feature of a block cipher is that a small change either in the plaintext data block or in the secret key should produce a significant change in the output ciphertext [8] block, called avalanche effect. Also, differential data and key propagation through diffusion rounds of a cipher determine the cipher's strength against differential attacks. The differential data and key propagation should exhibit large variation between round outputs in a block cipher. The avalanche effect and differential data and key propagation is achieved by the use of powerful encryption primitives in cryptographic transformation algorithms. Even though the DES, with its key size of 56 bits, is not secure enough today, it exhibits strong avalanche properties that any good cipher is expected to have. Matrix based cryptographic transformation has been discussed in [9-12] that has high conversion speed and simple key generation procedure. In this paper, a data transposition procedure, based on data values in the data block, for symmetric block ciphers is presented. The procedure has been introduced in AES to enhance the data avalanche effect and differential data propagation through diffusion the cipher's diffusion rounds. The transposition procedure offers two significant advantages. First, the procedure is simple to implement and has high degree of complexity in determining the plaintext through crypt analysis. Secondly, the procedure produces a strong data avalanche effect making many bits in the output block of a cipher to undergo changes with one bit change in the data block thereby providing high security. A strong data avalanche facilitates better diffusion of changes in data values on the ciphertext generated by the cipher and enhances the security of the cipher. As a case study, the controlled data rotation procedure has been introduced in AES to evaluate the data avalanche and differential data propagation produced in the cipher. AES with 128 bits secret key and 10 rounds of diffusion operation is considered here.

This paper describes the data based transposition procedure and discusses the data avalanche effect and differential data propagation produced in AES. Rest of the paper is organized in the following sections. In section 2: block cipher structure is discussed and section 3: data based transposition procedure is explained. In section 4: results showing improved performance of modified AES are presented and conclusions are made in section 5:

2. BLOCK CIPHER STRUCTURE
The block structure of a typical symmetric key cipher consists of a substitution section and a transposition section. These two sections are executed repeatedly many times (iterative rounds), with initial plaintext data block, and the final round output produces the ciphertext data block as given in figure 1. Sub keys are added with data values in every round to facilitate

confusion during crypt analysis. The sub keys are derived from secret key using a complex key schedule program.

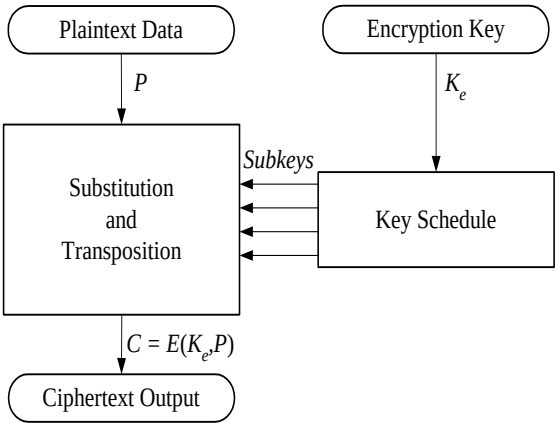

Fig 1: Block diagram of a typical block cipher.

3. DATA BASED TRANSPOSITION

The data based transposition is applied to left and right half data parts of a data block using right and left half data parts respectively. This is achieved by rotating one half data block number of times equal to a decimal digit extracted from the other half data block. To facilitate this, a data block in the diffusion section of a symmetric cipher is first bifurcated in to two equal parts, the left half part and the right half part. The procedure involved in this method is discussed in the following sub sections. Refer to Fig. 2: that shows the block diagram of data based rotation scheme.

3.1 Bifurcation of Data Block

Refer to figure 2 that show the block diagram of data based rotation scheme. The data block on which data based transposition has to be applied is first split into two data halves, left data half and the right data half. Both these data halves will have equal number of bytes. The input data block DB is bifurcated to left half data block, LHDB and right half data block, RHDB.

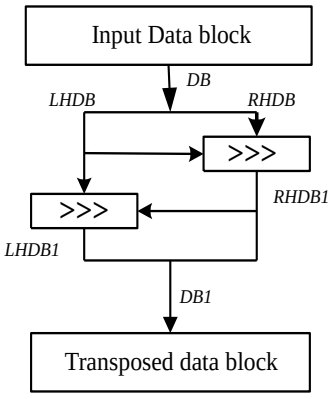

Fig. 2: Block diagram of data based rotation scheme.

3.2 Byte Sum of Left Half Data Block

The decimal values of all the bytes in the left half data block (LHDB) are added to get left data byte sum, LDBS. This addition can be performed by a loop as indicated in the pseudo code.

```
LDBS=0
For  i = 1 to Number of bytes in LHDB
  LDBS = LDBS + decimal value of LHDB(i)
EndFor
```

3.3 Number of Rotations of Right Half Data

Here the number of rotations to be applied on the right half data block is computed. From the byte sum, LDBS of left half data block, an integer number, RDRI (Right Data Rotation Integer) is obtained such that RDRI = LDBS MOD 6. This number lies in the range 0 to 5. The value of this integer depends on the decimal value of left half data block, LHDB.

3.4 Rotate Right Half Data Block

The Right Half Data Block, RHDB, is rotated right number of times equal to the integer value RDRI to get RHDB1. Left half data block LHDB is rotated right number of times equal to RDRI. If number of bytes in RHDB = 8, then pseudo code of this operation is as follows:

```
For i=1:(RDRI + 1)
   For j=8:-1:1
     RHDB(j+1)=RHDB(j)
   EndFor
   RHDB(1)=RHDB(9)
EndFor
RHDB1=RHDB
```

3.5 Byte Sum of Right Half Data Block

The decimal values of all the bytes in the right half data block, LHDB1, are added to get right data byte sum, RDBS. This addition can be performed by a loop as indicated in the pseudo code.

```
RDBS=0
For  i = 1 to Number of bytes in RHDB1
 RDBS = RDBS + decimal value of RHDB1 (i)
EndFor
```

3.6 Number of Rotations of Left Half Data

Here, the number of rotations to be applied on the left half data block is computed. From the byte sum RHDB1 of right half data block, an integer number, LDRI (Left Data Rotation Integer) is obtained such that LDRI = RDBS MOD 6. This number lies in the range 0 to 5. The value of this integer depends on the decimal value of right half data block, RHDB1.

3.7 Rotate Left Half Data Block

The Left Half Data Block, LHDB, is rotated right number of times equal to the integer value RDRI to get RHDB1. Left half data block LHDB is rotated right number of times equal to LDRI. If number of bytes in RHDB = 8, the pseudo code of this operation is as follows:

```
For i=1:(LDRI + 1)
   For j=8:-1:1
     LHDB(j+1)=LHDB(j)
   EndFor
   LHDB(1)=LHDB(9)
  EndFor
LHDB1=LHDB
```

3.8 Concatenate left and right data blocks

LHDB1 and RHDB1 are concatenated to get DB1 that provides the output data block generated from the transposition section.

4. RESULTS AND ANALYSIS

Advanced Encryption Standard algorithm has been modified by introducing the data based transposition procedure. AES has been tested to evaluate the following performance criteria.

- Data avalanche characteristics
- Differential data propagation through diffusion rounds

4.1 Data Avalanche Characteristics

The data avalanche refers to the number of bit changes in the output ciphertext block of a symmetric key cipher when one bit changes in the input plaintext block. A block of plaintext data (128 bits or 16 characters of plaintext) has been used as input to the AES cipher in this test. With a given secret key, K_1 the cipher has been executed. The output block produced in each round has been recorded. Then, with the same secret key, K_1 another plaintext data block that differs by one bit has been used to execute the cipher. The output block produced in each round has been recorded. The number of bit changes that occurred in each round with the two plaintext data blocks has been calculated. The number of bit changes, in each round, due to one bit change in the input plaintext data block has been plotted. The data avalanche has been obtained in the case of original AES and AES modified with data based transposition procedure for all ten diffusion rounds. With another key, K_2, the number of bit changes that occurred in each round with two plaintext data blocks has been calculated. Table 1 and Table 2 show the bit changes in round outputs due to one bit change in the input plaintext data block with keys K_1 and K_2 respectively. Figure 3: and Figure 4: show the data avalanche produced in AES and the same in AES with data based transposition procedure with keys K_1 and K_2 respectively for a one bit change in plaintext data block. It can be seen that the data avalanche has been enhanced in modified AES. A strong data avalanche is a desirable feature of a symmetric key encryption scheme as it facilitates enhanced security to the cipher against various attacks on the cipher.

Table 1. Data avalanche with key 1

Round	AES	Modified AES
1	48	56
2	50	52
3	47	52
4	51	58
5	36	53
6	49	53
7	37	47
8	46	41
9	47	49
10	56	57

Table 2. Data avalanche with key 2

Round	AES	Modified AES
1	3	38
2	53	51
3	48	48
4	50	39
5	55	48
6	48	57
7	48	50
8	42	50
9	42	48
10	54	53

.

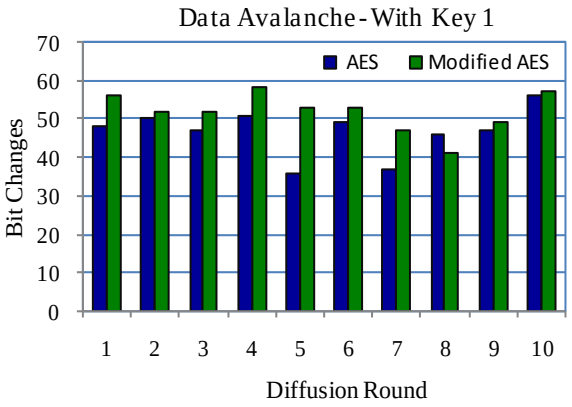

Fig. 3: Data avalanche with Key 1

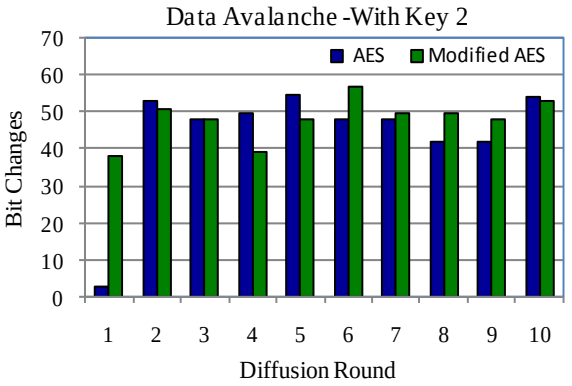

Fig. 4: Data Avalanche with Key 2

4.2 Differential Data Propagation

The differential data propagation through diffusion round outputs of a symmetric cipher refers to the change in data values between successive round outputs for a given change in the input plaintext data block. The differential propagation of data through round outputs in AES and modified AES are presented here. A block of plaintext data (128 bits or 16 characters of plaintext) has been used as input to the cipher in this test. With a given secret key, *K1*, the AES cipher has been executed. The output block produced in each round has been recorded. Then, with the same secret key value and another plaintext data block with one bit data change has been used to execute the AES cipher and modified AES cipher. The output block produced in each round has been recorded in both cases. The difference in byte values of the data blocks produced in respective round has been calculated. The differences in byte values showed how one bit change in secret key propagates through data in rounds. If the difference in byte value between round outputs due to one bit change (or for a given difference) in plaintext data value is not consistent then the cipher exhibits strength against differential crypt analysis. Fig. 5: and Fig. 6: show the variation of difference in byte-1 and byte -2 values of the data blocks produced by each round due to one bit change in plaintext data block value.

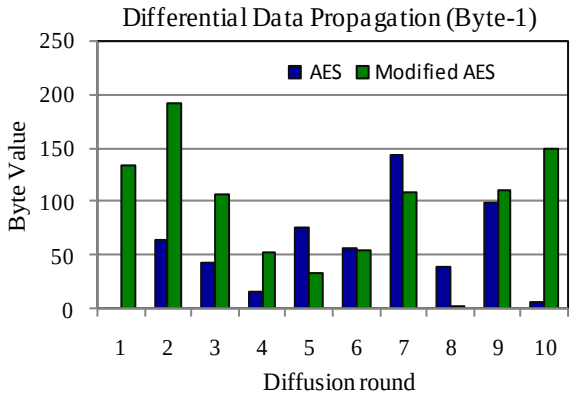

Fig. 5: Differential data propagation (Byte - 1)

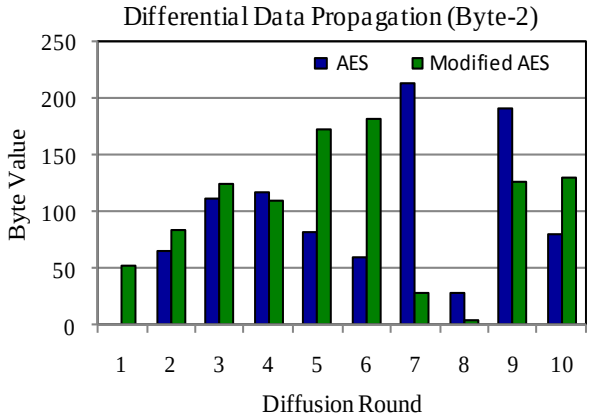

Fig. 6: Differential data propagation (Byte - 2)

All bytes in a block exhibited similar characteristics. The figures indicate that the differential data propagation is better in AES modified with data based transposition procedure. This is very important in ensuring resistance of the cipher against differential attacks.

5. CONCLUSION

It has been shown that the data based transposition procedure, incorporated in Advanced Encryption Standard, as a modification, have produced enhanced data avalanche and differential data propagation in its diffusion rounds. Propagation of differential data through bytes of data block in diffusion rounds should exhibit a random nature in order to facilitate strong resistance against differential attack on a symmetric cipher. A strong data avalanche facilitates better resistance against linear attack on a symmetric cipher. The enhanced data avalanche and differential data propagation characteristics facilitate higher resistance against linear and differential attacks on the modified cipher. The data based transposition procedure discussed in the paper could be incorporated in any symmetric cipher to enhance resistance of the cipher against linear and differential attacks.

6. REFERENCES

[1] William Stallings, "Network Security Essentials (Applications and Standards)," Pearson Education, pp. 2-80, (2004).

[2] Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in computing," Pearson Education, pp. 66-120, (2004).

[3] Jose J. Amador, Robert W. Green. "Symmetric-Key Block Ciphers for Image and Text Cryptography," International Journal of Imaging System Technology, Vol.15 – pp. 178-188, (2005).

[4] Dragos Trinca, "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography," Proceedings of The third International Conference on Information Technology-New Generations. (ITNG'06), 0-695-2497-4/2006, IEEE Computer Society, (2006).

[5] Data Encryption Standard : http://csrc.nist.gov/publications/fips/fips46-3/fips-46-3.pdf

[6] Advanced Encryption Standard: http://csrc.nist.gov/publications/fips/fips197/ fips- 97.pdf

[7] Escrowed Encryption Standard: http://csrc.nist.gov/publications/fips/fips1185/ fips-185.txt

[8] Krishnamurthy G.N, Ramaswamy V., Leela G.H, Ashalatha M.E, "Performance enhancement of Blowfish and CAST-128 algorithms and Security analysis of improved Blowfish algorithm using Avalanche effect," International Journal of Computer Science and Network Security, Vol.8, No. 3, March 2008, pp. 244-250.

[9] Paul A.J., Varghese Paul, P. Mythili, " Matrix Array Symmetric Key Encryption," Journal of Computer Society of India, Vol. 37, Issue No. 1, January – March 2007, pp. 48-53.

[10] Paul A.J., Varghese Paul, P. Mythili, "A Fast and Secure Encryption Algorithm for Message Communication," IETECH International Journal of Communication Techniques, Vol. 2, No. 3, 2008, pp 104-109.

[11] Paul A.J., Varghese Paul, P. Mythili, "Fast Symmetric Cryptography using Key and Data based Masking operations," International- Journal of Computational Intelligence - Research & applications, Vol 3, Number 1, January – June 2009, pp. 5-10.

[12] Paul A.J., P. Mythili, Poulose Jacob "Matrix based Key Generation to Enhance Key Avalanche in Advanced Encryption Standard", International Journal of Computer Applications, No. 2, article 1, pp. 31–34, 2011. Published by Foundation of Computer Science (USA).