International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Diffusion of Cipher Blocks at Bit Level in Parallel AES to Improve Bit – Ratio Test thus Increasing Cryptanalysis Complexity

Amin B. Mobhani[Å*] and Shailendra K. Mishra[Å]

[Å]Computer Science & Engineering Department, Gujarat Technological University, At&PO: Limbda, Vadodara, India

Accepted 20 May 2014, Available online 01 June 2014, **Vol.4, No.3 (June 2014)**

Abstract

Information is an intelligible data through which knowledgeable and useful things can be conveyed or represented in a proper manner. With the advancement of technology, transmission of information over the network has become a trend. Hence information must be transmitted securely over the network. Data security was not a problem if a secured channel was provided for every single transmission. Hence it became a necessity to convert the information in an unintelligible form before transmitting it over an unsecure channel. Encryption is a technique through which original information can be converted into unintelligible form. As time evolved, various encryption algorithms were employed so that information can be securely transmitted over an unsecure channel. Hence even if an intruder gets access to the encrypted text he/she cannot gain any information from that text. But as the new algorithms were designed, all the algorithms were challenged and their cryptanalysis became possible. In the year 1998, Advanced Encryption Standards (AES) was proposed and later it was widely accepted as the most secure encryption algorithm that can be used for encrypting the information so that it can be transmitted securely over an unsecure channel. To make AES more faster a new scheme called Parallel AES, was employed which takes four blocks of 16bytes each at a time to generate four blocks of 16bytes of cipher text thus providing diffusion of blocks at byte level. By doing this parallel AES stood to be much faster than sequential AES. In this research we are further increasing the complexity of cryptanalysis by implementing parallel AES to provide diffusion of blocks at bit level. The proposed scheme will diffuse 32 blocks of data with the 8 blocks of key thus generating 32blocks of cipher text.

Keywords: *Cryptography, Information Security, Encryption Algorithm, Parallel AES, Bit Level Diffusion, Transformation Function, Bit-Ratio Test*

1. Introduction

Information is an intelligible data through which knowledgeable and useful things can be conveyed or represented in proper manner. Safeguarding this information from intruders and attackers is the main aim of information security. Information can either be stored physically or electronically. Data that are stored physically can easily be stored in locker and can be safeguarded using a key to the locker. But data that are stored electronically are more difficult to safeguard. Data that are stored electronically are generally transferred from sender to receiver over the network. Intruders or attackers can exploit the data passing over the network by attacks that are possible over the network. Through this unauthorized access to the data, intruder or attacker can disclose, modify, and fabricate (many other actions) the data. The aim of intruder or attacker is either to make the data unintelligible or not useful for the receiver of the data or to extract the information from the critical data.

The aim of information security is to provide a mechanism so that it becomes almost impossible for the intruder or attacker to access the data i.e. to transfer the data through the secure channel. But if the sender is sending information over an unsecure channel then the aim of information security lies in providing such a mechanism that even if an attacker gets access to the data he/she cannot extract any information from the accessed data. This mechanism stands useful if it provides three parameters of security i.e. confidentiality, integrity and authentication.

(i) Confidentiality: - Means the information is received from the intended sender.

(ii) Integrity: - Means the data has not been changed during its transit from sender to receiver.

(iii) Authentication: - Means that data is accessed by the authorized person.

The mechanism to make the data unintelligible or no useful for the intruder or attacker can be achieved using cryptography. Cryptography is study of techniques of secure communication between sender and receiver in the presence of third party who is not the part of communication system. Modern cryptography intersects with the discipline of mathematics and computer science. The original message which can read with meaning is

*Corresponding author: **Amin B. Mobhani**

called plain text. To send this message over the network its readable format is transformed into unreadable format called cipher text. Encryption is a technique of converting a message from plain text to cipher text. Decryption is a technique through which our message can be obtained by restoring plain text from cipher text. Many algorithms are available for encryption and decryption. In such algorithms a key is used to control the process of encryption and decryption. Based on the key, there are two types of cryptography:

1) Symmetric Key Cryptography: encryption and decryption are done with the same key.

2) Asymmetric Key Cryptography: encryption and decryption are done with different key. The key has also basically two types: public key and private key.

2. Related Literature Review

In October 2000, NIST decided to propose Rijndael as the Advanced Encryption Standard (AES). A prime feature of Rijndael is its ability to operate on varying sizes of keys and data blocks. It provides extra flexibility in that both the key size and the block size may be 128, 192, or 256 bits. AES is strong against differential, truncated differential, linear, interpolation and Square attacks. AES can be operated in 5 different modes has been discussed by Morris Dworkin in 2001.

- Electronic code book mode (ECB)
- Cipher block chaining mode (CBC)
- Output feedback mode (OFB)
- Counter mode (CTR)
- Cipher feedback mode (CFB)

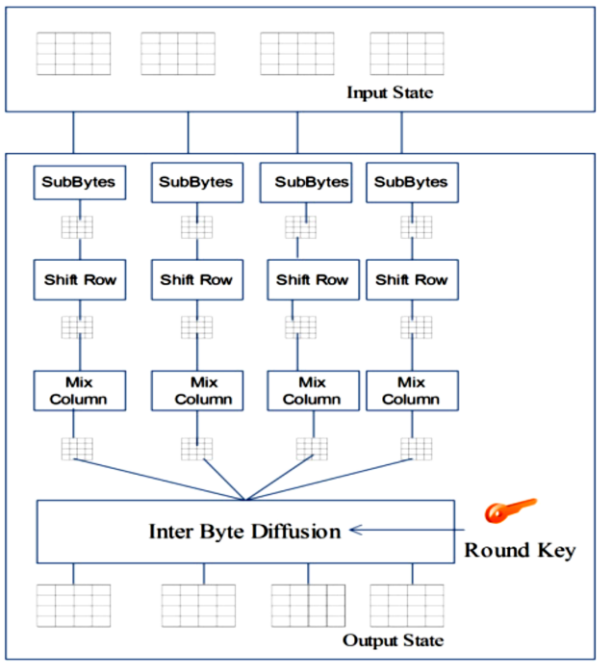

Figure1: Structure of each round at encryption site

In 2012, Shashank Srivastava et al. discussed that CFB, OFB and CBC modes cannot be used to achieve parallelism as each block encryption is dependent upon the previous cipher text block. Using ECB mode, encryption of each plaintext block can be performed simultaneously. Implementing AES using CTR mode to achieve parallelism creates pattern at block level which makes it vulnerable to differential cryptanalysis. Hence AES-ECB and AES-CTR modes can be used to achieve parallelism. Intra-block diffusion is provided by AES-CTR mode but to wipe out pattern at block level inter-block diffusion is necessary. To achieve parallelism in AES authors have proposed a scheme which takes 4 blocks of plaintext of 128bits each and generates 4 cipher blocks of 128bits each and to wipe out pattern at block level, they performed inter-block diffusion by adding a round key with all the four sub-blocks in a specified manner at the end of each round of parallel AES.

The first three rounds of parallel AES is same as the sequential AES but it performed in parallel for four blocks at a time. InterByteDiffusion is the last transformation of each round. After mixed column transformation of four sub states of 16 byte (4 * 4 matrixes) is created which acts as input states for InterBlock Diffusion transformation. This transformation diffuses the bytes of each state (Block) with others three blocks with adding round key.

3. Proposed Work

Parallel AES is a scheme that provides parallelism in encryption and decryption of data. Parallel AES approach is much faster than sequential AES.

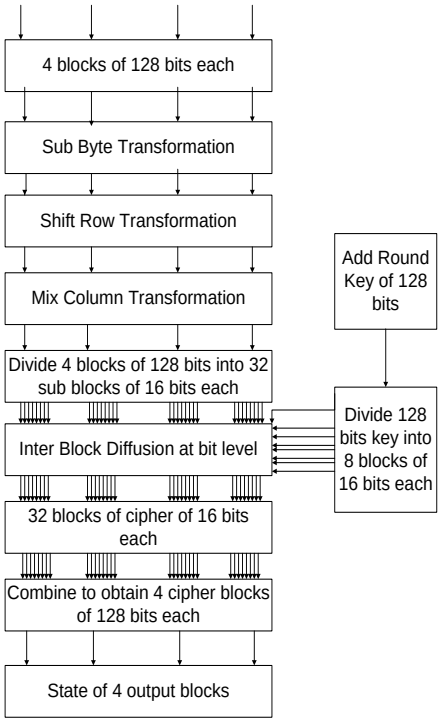

Figure 2: Design of one round of Parallel AES at Bit Level

Using Inter Cipher Block Diffusion at Byte level parallel AES wipes out the pattern at byte level creating difficulties in its cryptanalysis. The complexity of cryptanalysis can be increased by diffusing the Cipher Blocks internally at Bit Level. The objective behind the

Table 1: Comparison of Time Complexity

Name of File	No. of Bytes	Time Taken (Milli Seconds)							
		AES		PAES		BDPAES		BitDPAES	
		Encr	Decr	Encr	Decr	Encr	Decr	Encr	Decr
File 01	19775	74	88	61	90	70	81	598	687
File 02	39550	108	172	94	142	110	160	1151	1247
File 03	59639	130	220	174	245	154	225	1710	1931
File 04	79885	171	280	183	275	291	362	2388	2572
File 05	100886	262	437	261	355	365	461	3189	3248

Table 2: Bit-Ratio Analysis

Name of File	No. of Bytes	Bit Ratio Analysis			
		AES	PAES	BDPAES	BitDPAES
File 01	19775	43.6428	43.6428	43.4734	43.6643
File 02	39550	43.6611	43.6611	43.5139	43.7740
File 03	59639	43.6400	43.6400	43.4759	43.7551
File 04	79885	43.6214	43.6214	43.4987	43.7532
File 05	100886	43.6376	43.6376	43.5122	43.7986

idea of implementing Parallel AES at bit level is to improve its susceptibility against Brute Force attack. In AES and PAES, an attacker needs to try 2^{128} possibilities to crack the cipher text but in contrast to crack the cipher generated by Bit Level Parallel AES, an attacker needs to try 2^{128}(key possibilities) + 2^{128}(diffusion possibilities) which will make it more strong against Brute Force Attack.

Initially four input blocks of 128bits each are fed as an input to the Parallel AES. These four blocks goes through three AES transformations i.e. SubByte, ShiftRow and MixColumn. The result of mix column transformation is divided into sub blocks i.e. each block of 128bits is divided into 8 sub blocks of 16bits each to obtain 32 sub blocks of 16bits each. Similarly 128bits key size is divided into 8 sub key blocks of 16bits each. Note that for each round a new key is generated from a previous key using AES key expansion algorithm. After that a transformation function will be applied between 32 sub blocks and 8 sub key blocks to obtain 32 cipher blocks of 16bits each. These 32 cipher blocks of 16bits each are again combined in a manner that it will produce 4blocks of 128bits each. Above description is of one round. Above described round can be repeated as per key size.

Algorithm 1: Pseudo code for transformation function at encryption side

- Plain text bits(j): 512
- Key bits(e):128
- Transformation function: $S_{ibd,i} = S_{m,j} \oplus K_e$

```
for (i=0 ; i<512; i++)
{
    if(i>=0 && i<=127)
    {
        j= (4*i) mod 512
        e= i mod 128
    }
    else if (i>=128 && i<=255)
    {
        j= [(4*i)+1] mod 512
        e= i mod 128
    }
    else if (i>=256 && i<=383)
    {
        j= [(4*i)+2] mod 512
        e= i mod 128
    }
    else
    {
        j= [(4*i)+3] mod 512
        e= i mod 128
    }
}
```

Notations:

S_m: State after dividing mix column results into sub blocks.

S_{ibd}: State after inter block diffusion at bit level.

K_e: Count of bit position of sub blocks of key at encryption side.

j: Count of bit position after dividing mix column results into sub blocks.

i: Count of bit position where result of Inter Block Diffusion is to be stored.

4. Results & Analysis

4.1 Comparison of Encryption and Decryption time

Here we have compared the time complexity of three forms of AES encryption algorithm. The results are shown below in tabular form:

From table 1 it is clear that encryption and decryption time of BitDPAES (Bit Level Diffusion Parallel AES) is more than BDPAES (Byte Diffusion Parallel AES), PAES (Parallel AES) and AES (Advanced Encryption Standards) but in contrast it will provide more security.

Statement of justification: Think of two security systems A & B. System A is costing, say, Rs. 1000 and System B

is costing, say, Rs. 1500. But System B is proving more security than System A. So it is obvious that organizations will go with hiring System B for securing their important data.

4.2 Bit Ratio Test

Bit - Ratio (in %) = {(Total number of bits changed in the file after encryption) ÷ (Total number of bits present in the file)} × 100 [4].

Table 2 shws comparison of Bit-Ratio test for three forms of AES.

Bit Level diffusion deals with diffusion of cipher bits with the key bits using some transformation function. Hence there is higher probability of getting more bits changed in the encrypted text and so there are more chances of improved Bit-Ratio test at Bit Level Diffusion. From above result it is clear that Bit-Ratio performance of BitDPAES is better than other three forms of AES.

Conclusions

Parallel AES is a scheme that provides parallelism in encryption and decryption of data. Parallel AES approach is much faster than sequential AES in terms of Encryption and Decryption time. Using Inter Cipher Block Diffusion at Byte level parallel AES wipes out the pattern at byte level creating difficulties in its cryptanalysis. The complexity of cryptanalysis can be increased by diffusing the Cipher Blocks internally at Bit Level. Diffusing the blocks at bit level the Bit-Ratio analysis might get increased and hence that will make AES more strong against Brute-Force and selected Key Attacks thus increasing the complexity of cryptanalysis.

The future prospect of our proposed scheme is it can be implemented on more fast computing configurations and tools in order to reduce the encryption and decryption time at bit level. Our proposed scheme can also be extended to encrypt more than one file at a time. Diffusion between different files at byte or bit level may also be the area of further research.

References

Mohammed AbuTaha, Mousa Farajallah, Radwan Tahboub, Mohammed Odeh(2011), Survey Paper: Cryptography Is The Science Of Information Security, IJCSS, pages 298-309.

Ajay Kakkar, M.L.Singh, P.K.Bansal(2012), Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication in Multinode Network, IJET, pages 87-90.

Mukund S. Wankhade, Pravin D. Soni(2013), Advanced Cryptanalytic Algorithm for Data Security, IJAIEM, pages 321-324.

Sukalyan Som, Mohit Kundu, Sabyasachi Ghosh(2012), A Simple Algebraic Model based Polyalphabetic Substitution Cipher, IJCA, pages 53-56.

Shashank Srivastava, Avinash Kumar Singh, G.C.Nandi(2012), Inter Cipher Block Diffusion: A Novel Transformation for Proposed Parallel AES, ICCCS, pages 872-879.

J. Daemen, V. Rijmen(2010), AES Proposal Rijndael[EB OL], http://www.daimi.au.dk/~ivan/rijndael.pdf.

Morris Dworkin(2001), Recommendation for Block Cipher Modes of Operation, book published in Gaithersburg, MD: U.S.Dept. of Commerce, Technology Administration, NIST.

William Stallings (2010), Cryptography and Network Security, Fifth Edition, book published in Prentice Hall, ISBN: 0130914290.