Grenze International Journal of Engineering and Technology, July 2018

Reversible Logic based Modified Design of AES-CBC Mode

Rohini S. H[1], Jyoti R H[2] and Rajashekar B.Shettar[3]
[1]Dept. of E&C, B.V.B.C.E.T, Hubli,Karnataka India,
[2]Dept. of E&C, K.L.E.Technological University, Karnataka,India,
[3]Department. of E&C, BVBCET, Hubli,Karnataka India,
{ Rohini H,Rajashekar.Shettar, rohini_sh,raj}@bvb.edu, {Jyoti R H, jyotihirekumbi369}@gmail.com

***Abstract*—Advanced encryption standard (AES) is the most widely used secure symmetric algorithm nowadays. AES is a block cipher, in which different operations are performed on group of bits called a block. In order to encrypt N number of blocks, different modes of operations have been proposed. There are five modes of operations of AES proposed namely, Electronic Code Book(ECB) ,Cipher Block Chaining(CBC), Cipher Feedback(CFB),Output Feedback(OFB) and Counter (CTR) mode. Based on the analysis, CBC mode of operation is found to be the best. In CBC mode initialization vector (IV) is used. Initialization vector should be same as that of size of block. IV is XORed with the first plaintext block. The XORed result is encrypted with the key. The encrypted result (ciphertext) is used as IV to the next proceeding blocks. CBC performs operations on blocks of standard size (i.e, 128). We identified that existing CBC requires more computational time as it operates on n-block plaintexts and also more hardware. So we tried to modify the existing CBC in order to reduce the hardware used, computational time and also to improve the security by using equal key and message size. Shannon's theorem states that a one-on-one relationship between each message bit to each key bit (hence both key and message length equal) would give the best security. To improve the security of the original CBC mode, message size is increased from standard block size of 128 bits to 256 bits and key size is made as equal as the message block size. We get more security by the use of larger key size and the increased throughput from the larger input block size compared to original AES of 128 bits. In our proposed work IV and XOR operation is not used. The first stage ciphertext is used as key for the next stage and so on. We designed and simulated 512 bit encryption using both already existing CBC and our proposed CBC. In the modified CBC 512 bit plaintext is divided into two blocks of each 256 bits instead of four blocks of each 128 as in existing CBC. The hardware required and delay of both are compared with existing work and found to be less. In order to combat power attacks in conventional algorithm, reversible logic is used to implement the design.**

***Index Terms*— Cipher Block Chaining(CBC), Cipher Feedback(CFB), Ciphertext, Initialization Vector, Output Feedback(OFB).**

I. INTRODUCTION

Nowadays security is of utmost importance as cyber attacks are continuously developing. In order to make AES algorithm more secure, different modes of operations are proposed. The five modes of operations are

Grenze ID: 01.GIJET.4.2.508

namely Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback(CFB),Output Feedback(OFB) and Counter (CTR) mode [1]. ECB is the simplest mode of operation in which input message is divided into number of blocks. Each block is encrypted separately independent of each other. Blocks with identical message generate identical ciphertexts. In order to overcome such type of problems complex modes of operations are proposed. CBC is one of them [7] .

Many hardware implementations for AES were found in literature. These implementations were done for the standard AES of 128 block size with 128,192 ,256 bits key size, such as the work proposed in [9][10].

AES is a block cipher in which only one block is encrypted one at a time. In order to encrypt number of blocks, different modes of operations were proposed. The currently existing block cipher cryptographic algorithms like Data Encryption Standard(DES), Triple DES(TDES) and AES, in which plaintext is encrypted with key length need to be fixed. If the length of the plaintext is more than the key used, then the plaintext is divided into number of blocks, with each block of length same as the length of the key. If the key is not altered, the identical plaintext blocks will produce identical ciphertexts. So to overcome such type of problem, CBC have been proposed in paper [1].

The different modes of operations are explained in [2]. It describes operation details, different parameters affecting modes of operations, strengths and weakness of different modes of operations. CPU time, encryption time and memory requirements are evaluated for the same to check the performance of each mode.

In the paper [11] Chaotic Cipher Block Chaining mode (CCBC) is proposed, in which security of algorithm is enhanced by using different secret keys generated by chaotic generator. The size of key and block used are 512 bits.

The paper [3] modified the existing CBC using Merkle-Hellman cryptosystem to enhance the security level. Initially the first plaintext block is encrypted using original CBC method and then the output obtained after CBC encryption is encrypted further using Merkle-Hellman encryption in which varying key and IV are used to make the existing CBC still more stronger.

The paper [12] proposed AES Rijndeal in the Cipher Block Chaining(CBC) mode. The area is optimized and implemented on XILINX Vertex2P.

The paper [4] proposed two different modified CBC methods namely , the Key Stream Protection Chain mode (KSPC) and Output Dual Chaining mode (ODC). Their security level is discussed against various attacks.

A. Reversible Logic Gates

Reversible logic is widely used nowadays and has got more popularity due to their ability to reduce the power dissipation which is the main requirement in low power VLSI design. It is n-input and n-output device. In reversible logic, outputs can be determined from the inputs and vice versa. We can implement one or more applications using single reversible logic gate. Feynman gate is shown in **Figure 1**. The inputs are A, B and the outputs are X, Y where Y=A, X=A ⊕ B. One of the outputs of Feynman gate is XOR gate operation and the other output is known as garbage which is used to maintain the reversibility.

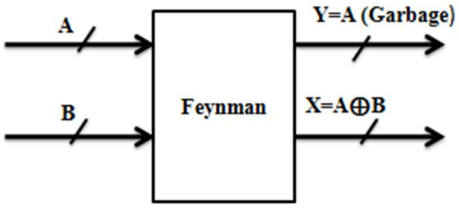

Figure 1. Feynman Gate

II. IMPLEMENTATION DETAILS OF PROPOSED IDEA

In order to provide higher level of security, the identical blocks of plaintexts need to result with the different ciphertexts. It can be done using one of the modes of operation namely CBC.

A. Implementation of Standard CBC

In the existing CBC initialization vector (IV) is used and should be of same size as that of plaintext block. The longer message is divided into number of blocks (each block with size 128 bit). Initially, the first block

is XORed with initialization vector and the result obtained is encrypted using the key, the key may be of size 128,192 or 256. The ciphertext generated after encryption is used as initialization vector to the next stage. The same key is used for all the proceeding stages of encryption. The same procedure is followed for all the remaining blocks. The ciphertexts generated at each stage (C1,C2……CN) are concatenated to form the final ciphertext of overall input message [5]. The block diagram of standard cipher block chaining mode is shown in **Figure 2.**

We have implemented standard CBC for comparison with our proposed CBC. In the standard CBC, We have taken 512 bit input message and is divided into four blocks with each block of size 128 bit (i.e, 128x4=512 bits). The key size used is 256 bit and IV is of size 128 bit as that of plaintext. The encryption is done for four plaintext blocks.

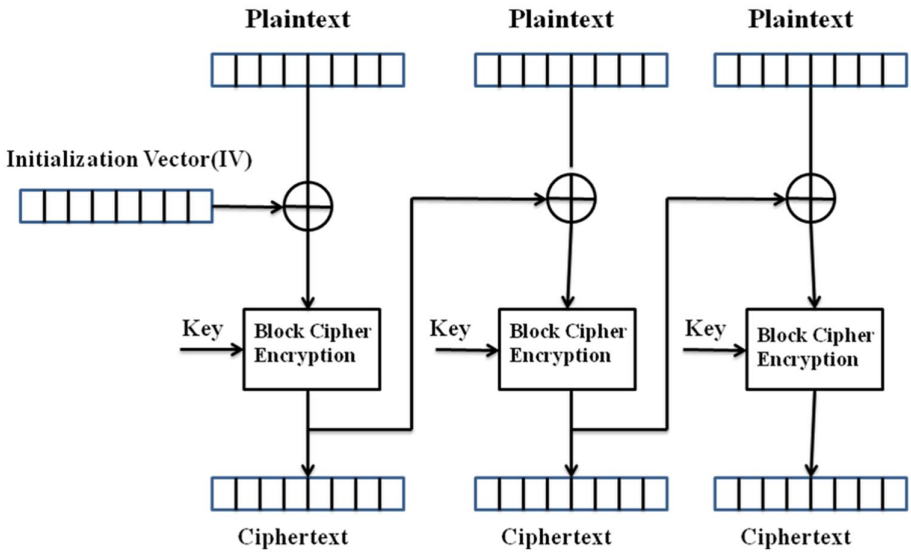

Figure 2. Block diagram of standard cipher block chaining mode

B. Proposed Cipher Block Chaining

From the literature, we can point out that, in order to achieve higher security in CBC mode of operation, initialization vector must be random and non predictable and key must be changed for each encryption block. Hence the existing CBC is modified in order to improve security, reduce hardware required and computational time. The modified CBC uses no initialization vector. The same key is not used for all the encryption blocks. The block size used is 512 bit. This 512 bit message block is divided into two 256 bit plaintexts p1 and p2. The key size used is 256 bit same as the size of plaintext. Initially the first plaintext block p1 is encrypted using 256 bit key. The ciphertext generated after first encryption is used as key to the encryption of next plaintext block P2 and ciphertext C2 is generated. Finally the generated ciphertexts C1, C2 are concatenated to form 512 bit ciphertext corresponding to 512 bit plaintext. We used reversible logic to mitigate the power attacks in conventional AES as reversible gates offer ideally zero internal power dissipation. The block diagram of encryption of n blocks using CBC mode of operation is shown in in **Figure 3**.

There are four transformations in the encryption of AES namely, Byte Substitution, Shift Row, Mix Column and Round Key Addition.

Byte Substitution

The data is arranged in the form of matrix of four rows and the number of columns of the matrix depends on the size of data. For example 128 bit data is arranged in the form of 4x4 matrix and 256 data is arranged in the form of 4x8.The matrix consists of four rows of bytes, each containing N bytes, where N is the block length divided by 32.The data in the matrix is substituted by the standard S-Box .

Shift Row Transformation

In shift row transformation, the rows of the matrix are cyclically shifted by its row number to the left.

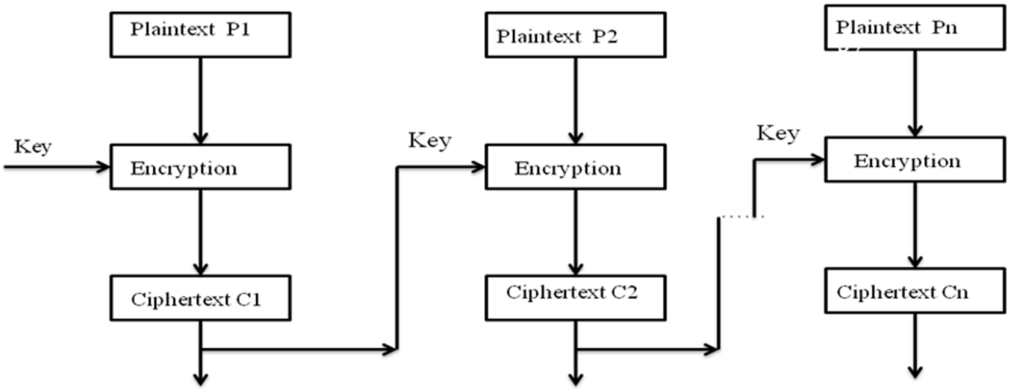

Figure 3. Block diagram of proposed cipher block chaining mode

- The Row 0 is not shifted.
- The Row 1 by 1 byte.
- The Row 2 by 2 byte.
- The Row 3 by 3 byte.

The shift row transformation of 8 -bit data is shown in **Figure 4**. It is implemented using reversible logic gate Feynman. In Fig 2.2 N is the amount to be shifted .The same procedure is repeated N times. The same procedure is followed for 48, 64 and 128 bit data transformation in case of 192,256,512 respectively.

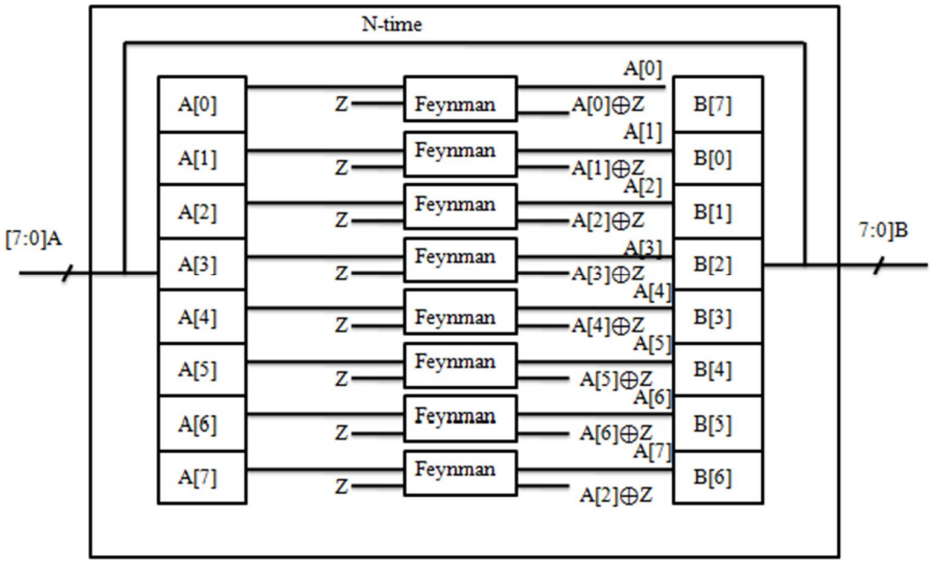

Figure 4. Reversible Implementation Of Shift Row Transformation

Mix Column Transformation

The Mix column performs operations on the columns of the matrix. Each row of bytes in the matrix is multiplied with the corresponding columns of constant matrix of 4x4.Mix column transformation is simulated using reversible logic gates. The fixed matrix used in our design is given below.

02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02

AddRound Key

The number of rounds of AddRound Key varies according to the key size and block size used. In the first round of encryption, the main key is XORed with the plaintext. In the remaining rounds, except final round the sub keys obtained for different rounds are XORed with the output obtained from the mix column transformation. In the final round, the last round sub key obtained is XORed with the output of shift row transformation.

III. Results and Discussions

We have implemented our modified CBC along with standard CBC for comparison. The existing CBC performs operations on standard block size of 128 bits and key size of 256 bits where as our modified CBC used 256 plaintext and 256 bit key size. The simulation result of 256 plaintext and key is shown in **Figure 5**. No initialization vector and the same key is used in proposed CBC. Attempt is made to increase the security level by using plain text size same as that of key size.We tried to reduce the hardware required and the computational time as the number of encryption blocks are reduced. The encrypted output of our proposed CBC is shown in **Figure 6.**The comparison is done for the our proposed CBC and the standard CBC w.r.t security, hardware required ,delay and the corresponding gates ,quantum cost and garbage outputs used.

A. Simulation result of 256 bit plaintext and key

Plaintext: 54732067544F4E2068204B20776E6954616D75466F656E7774796E752020656F
Key: 4537027645F4E6820204B20776569546167894666F656E76D4796E752020656F7
Encrypted : 163f41a97f7f215671179d677b0518a080377512626de422de1220742c9b6f18

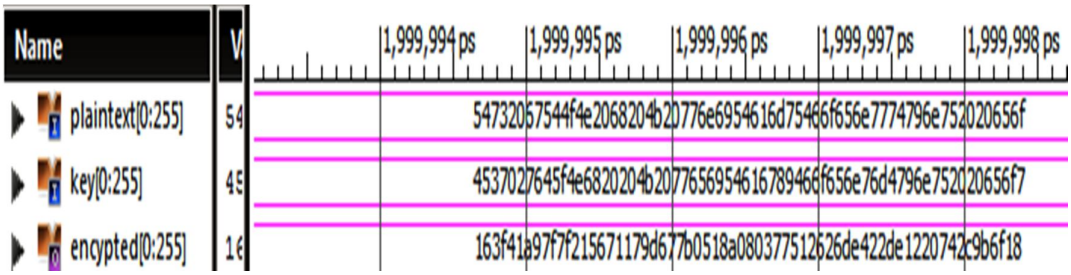

Figure 5. Simulation Result Of 256 Bit

B. Simulation result of 512 bit plaintext and key using CBC mode

- Plaintext: 64122a356c8790765d421c3e3a56447897862a285f3e7c5f3c87691b7c3a51234567890323abcd56efab3216453c4789706057432f3e4a5c6d8f9e4789706432
- Key :34a21a356c8790765d421c3e3a5944e807862ae87f3e7c5f3c87691b7c3a5123
- Encrypted Output: 12b53853cd3b104b06c6cbf09cb80979524eed09a818a0b1029acd8742061bd118664d18cf45f3cdbb71a6d1c1e661c3513a08594cb1d85dfb4ea26f262c38d1

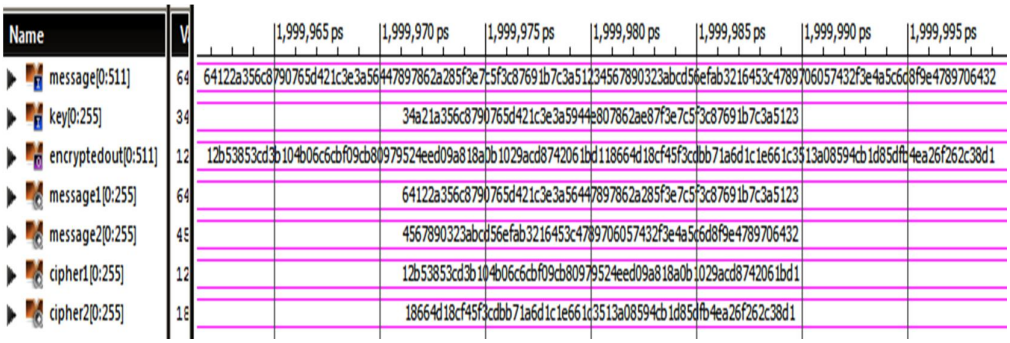

Figure 6. Encrypted output of 512 bit message

TABLE I. COMPARION OF STANDARD AND PROPOSED CBC

Papers	Maximum combinational path delay	Hardware Required	Security
Paper [2]	164.326ns	More	Less(Same key is used)
Proposed CBC	120.922ns	Less (XOR not used, less no of encyption blocks)	More (Different keys for each encryption block and IV is not used,equal key and message size)

TABLE II. COMPARISON OF PROPOSED CBC FOR DIFFERENT PARAMETERS

Parameters	Proposed CBC
Number of Feynman gates used	368
Quantum Cost	368
Garbage	368

IV. CONCLUSION

We have implemented standard CBC and our proposed CBC and the comparison is done w.r.t hardware required, delay, security. The design is simulated using Xilinx 14.2.The coding is done in verilog. By modifying the standard CBC, we tried to improve the security, reduce the hardware as well as computational time. Our proposed CBC provides more security compared to 512 message encryption using standard CBC as key and plaintext sizes are taken same and also different keys are used for each encryption block. Design is implemented using reversible logic to achieve power efficient encryption or decryption so that power attacks can be minimized.

ACKNOWLEDGMENT

The authors wish to thank, head of the department, staff members, teaching and non-teaching staff for the successful completion of the paper.

REFERENCES

[1] Vaidehi, M., and B. Justus Rabi. "Design and analysis of AES-CBC mode for high security applications." Current Trends in Engineering and Technology (ICCTET), 2014 2nd International Conference on IEEE, 2014.
[2] Alfadel, Mahmoud, El-Sayed M. El-Alfy, and Khaleque Md Aashiq Kamal. "Evaluating time and throughput at different modes of operation in AES algorithm." Information Technology (ICIT), 2017 8th International Conference on. IEEE, 2017.
[3] Padhmavathi, B., et al. "Improvement of CBC encryption technique by using the Merkle-Hellman Knapsack Cryptosystem." Intelligent Systems and Control (ISCO), 2013 7th International Conference on. IEEE, 2013.
[4] Huang, Yi-Li, et al. "Building a block cipher mode of operation with feedback keys." Industrial Electronics (ISIE), 2013 IEEE International Symposium on. IEEE, 2013.
[5] Blazhevski, Dobre, et al. "Modes of Operation of the AES Algorithm." (2013): 212-216.
[6] Abidi, Abdessalem, et al. "Summary of Topological Study of Chaotic CBC Mode of Operation." Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), 2016 IEEE Intl Conference on. IEEE, 2016.
[7] Desai, Akshay, et al. "Parallelization of AES algorithm for disk encryption using CBC and ICBC modes." Computing, Communications and Networking Technologies (ICCCNT), 2013 Fourth International Conference on. IEEE, 2013.
[8] Moh'd, Abidalrahman, Yaser Jararweh, and Lo'ai Tawalbeh. "AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation." Information Assurance and Security (IAS), 2011 7th International Conference on. IEEE, 2011.
[9] Abidi, Abdessalem, et al. "Summary of Topological Study of Chaotic CBC Mode of Operation." Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and

15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), 2016 IEEE Intl Conference on. IEEE, 2016.
[10] Srinivas, NS Sai, and Md Akramuddin. "FPGA based hardware implementation of AES Rijndael algorithm for Encryption and Decryption." Electrical, Electronics, and Optimization Techniques (ICEEOT), International Conference on. IEEE, 2016.
[11] Nag, K. Sowmya, H. B. Bhuvaneswari, and A. C. Nuthan. "Implementation of advanced encryption Standard-192 bit using multiple keys." (2013): 2-26.
[12] Hue, Ta Thi Kim, Thang Manh Hoang, and Safwan Al Assad. "Design and implementation of a Chaotic Cipher block chaining mode for image encryption." Advanced Technologies for Communications (ATC), 2013 International Conference on. IEEE, (2013).
[13] Naiem, Ghada Farouk, et al. "An efficient implementation of CBC mode Rijndeal AES on an FPGA." Radio Science Conference, 2008. NRSC 2008. National. IEEE, 2008.