Indian Journal of Science and Technology, *Vol 9(38), DOI: 10.17485/ijst/2016/v9i38/90314, October 2016*
*ISSN (Print) : 0974-6846*
*ISSN (Online) : 0974-5645*

# FPGA Implementation and Analysis of the Block Cipher Mode Architectures for the PRESENT Light Weight Encryption Algorithm

**A. Prathiba* and V. S. Kanchana Bhaaskaran**

School of Electronics Engineering, VIT University Chennai, Chennai - 600127, India; prathi_communication@yahoo.co.in, vskanchana@gmail.com

## Abstract

**Objective:** This paper presents the Field Programmable Gate Array (FPGA) implementations of the different block cipher mode architectures of the ISO standardized light weight block cipher PRESENT, designed for resource constrained devices. **Methods/ Statistical Analysis:** The performance evaluations compare the implementations of the different block cipher modes, namely Electronic Code Book (ECB) mode, Cipher Block Chaining (CBC) mode, Cipher Feedback Mode (CFB), Output Feed Back Mode (OFB) and CounTeR (CTR) mode for the PRESENT cipher. The throughput of encryption of three successive 64 bit blocks of data ranges from 565.312Mbps to 574.784Mbps for the modes other than the cipher feedback mode in the Spartan-3 FPGA. The throughput for providing confidentiality through encryption in the cipher feedback mode arrives as 68.912 Mbps, 155.392Mbps and300.8 Mbps for a 64 bit block of data for the input streams of size 8 bits, 16 bits and 32 bits respectively. **Findings:** The throughput of the block cipher mode hardware architectures of the light weight cipher PRESENT demonstrates the high speed performance of the cipher in encryption/decryption of data as blocks and streams. **Application/ Improvement:** The significance of the proposed work is to know the hardware performance of the different modes of operation for the light weight block cipher PRESENT. The performance estimation of the block cipher modes operations of the PRESENT cipher definition in hardware have been carried out for the first time.

**Keywords:** Block Cipher Modes, FPGA, Internet of Things (IoT), Light Weight Cipher

## 1. Introduction

Internet of Things (IoT) devices expects smart security solutions with reduced resource utilization, adequate security and better speed performance. The demand for the security of smart devices is addressed by the light weight cryptography. There lack wide system architectures and variety of implementations for the light weight cryptographic representations. The proposed work aims at one such solution of implementation of the different block cipher mode architectures of the ISO standardized light weight block cipher PRESENT[1] and estimate its performance.

The PRESENT algorithm is a light weight block cipher algorithm which has the input block size of 64 bits. The key length can be either 80 bits or 128 bits. It consists of the round operations namely; add round key, substitution and permutation. The total numbers of rounds are 31 with the final 31$^{st}$ round with only add round operation. The algorithm is defined for its hardware efficiency.

The different block cipher modes namely, modes Electronic Code Book (ECB) mode, Cipher Block Chaining (CBC) mode, Output Feed Back (OFB) Mode, the cipher feedback mode and the CounTeR (CTR) mode aims at security (CFB) enhancement by making the successive encryption and decryption dependent on the current encryption and decryption[2,3]. The mode of operation of an algorithm aims at providing services such as confidentiality and/or authentication. It helps in handling information security of multiple blocks by the use of single block cipher's operation. Also, the related key attacks, known plain text attacks can be prevented by the use of

**Author for correspondence*

different possible modes of operation. Hence to resists the attacks which reveal the information about the cipher which employ the same set of key for encrypting similar plain texts, the various mode architectures which will not expose the key and output data dependency has been proposed for the symmetric block ciphers.

The block RAM based 8 bit AES FPGA implementations of the CFB/OFB and the ECB modes have been carried out to improve the throughput in reference[4]. An authenticated AES encryption scheme by the combination of OCB and ECB in FPGA is done in[5]. Further explorations of improving the security levels have been attempted by the novel block cipher mode designs[6]. An architecture supporting the modes ECB, CBC, CFB, OFB and CTR for the AES results in the throughput of up to 480.27 Mbps, 423.906 Mbps and 379.284 Mbps for 128, 192 and 256 bit keys respectively[7]. The AES modes applicable for sound and images and their entropy calculation are done to estimate the effectiveness of the individual modes in the audio and image encryptions[8]. A comparison review of the modes of operation for the encryption algorithms namely, AES, Two fish and RC6 to evaluate their application for disk storage device is studied in[9]. The vulnerability of AES block cipher modes are quantified for its resistance to power in the designed low power and high speed hardware architectures. The CTR mode has been found to be better in power resistance with balance in area and power[10]. The FPGA implementation architectures for the different types of modes of the block cipher algorithms, its performance analysis such as speed, area, power resistance, security features etc, have been analyzed in the[11-19]. The cryptographic solutions and its optimization mechanisms are widely carried out in literature[20-22].

The proposed work incorporates the different block cipher architectures for the PRESENT cipher definition in hardware and puts the performance in place. Such a hardware performance analysis for the PRESENT light weight cipher definition have been attempted in the proposed work.

The paper is structured as follows. Section 2 presents the specifications of different block cipher modes of operation and Section 3 describes the FPGA design methodology. The implementation results for various architectures are in Section 4 and comparisons with other block ciphers are in Section 5. Finally, conclusions are in Section 6. The following section details the different block cipher modes employed in the current work with its block diagrams.

## 2. Block Cipher Modes of Operation

The traditional block cipher modes of operation with its typical encryption and decryption procedure for each of the modes are discussed in this section. The proposed implementation addresses the encryption modes ECB, CBC mode, CFB mode, OFB mode and the CTR mode. The CFB mode works on streams of plain text of lengths. The stream length addressed in the proposed work are s = 8, 16 and 32.The modes ECB, CBC, OFB and CTR process 64 bit block of data as a whole. The encrypt block and the decrypt block corresponds to PRESENT encryption and decryption respectively. Among the modes some of the modes namely, CFB, OFB and CTR utilize the encryption definition for both encryption and decryption of data blocks.

### 2.1 Electronic Code Book Mode

The electronic code book mode operates on each blocks of data independently for encryption and decryption i.e., parallelization is possible in both encryption and decryption. The block diagram representation of the ECB mode is shown in Figure 1. In the ECB mode encryption/decryption of plain text/cipher text can be carried out in parallel for any number of blocks. Figure 2 shows the decryption of C1, C2 and Cn to yield P1, P2 and Pn respectively.

The data blocks P1, P2 and Pn are fed in the encryption blocks result in the three cipher text blocks C1, C2 and Cn respectively. This mode performs encryption and decryption possible for any number of blocks with the disadvantage of being vulnerable to known plain text

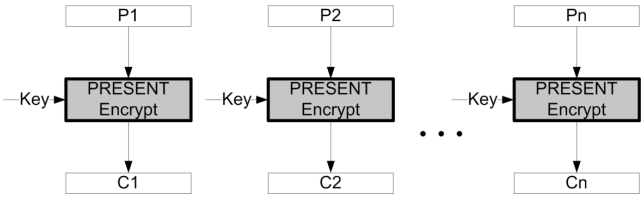


**Figure 1.** ECB mode encryption

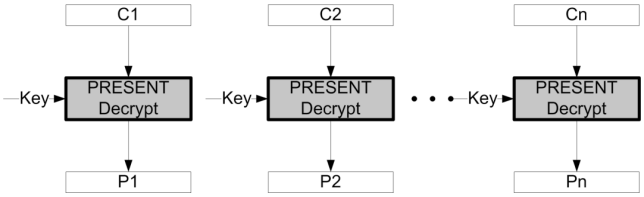


**Figure 2.** ECB mode decryption

attacks. The same plain text and key combination results in the same cipher text in the electronic code book mode of operation, resulting in the compromise in the security. The mathematical equations relating the encryption and decryption are given in equations (1) and (2).

$$\text{Encryption:} \quad C_j = E(K,P_j) \text{ for } j = 1,\ldots\ldots..N \qquad (1)$$

$$\text{Decryption:} \quad P_j = D(K,C_j) \text{for } j = 1,\ldots\ldots..N \qquad (2)$$

## 2.2 Cipher Block Chaining Mode

In the cipher block chaining mode, a chain is established between the successive encryption/decryption blocks. The encryptions and decryptions of multiple blocks are interdependent on the previous plain texts/ cipher texts as shown in Figure 3 and 4. The decryption is concurrent whereas the encryption demands the previous block encryption to be completed for the current encryption. The expression for plain text and cipher text involved in this mode are given by the equations (3) and (4).

$$\text{Encryption:} \quad \begin{array}{l} C_1 = E(K,[P_1 \text{EXOR} IV]) \\ C_j = E(K,[P_j \text{EXOR } C_{j-1}]) \text{ for} \\ j = 2,\ldots\ldots\ldots N \end{array} \qquad (3)$$

$$\text{Decryption:} \quad \begin{array}{l} P_1 = D(K,C_1) \text{EXOR IV } P_j = D(K,C_j) \\ \text{EXOR } C_{j-1} \text{ for } j = 2,\ldots\ldots\ldots N \end{array} \qquad (4)$$

## 2.3 Cipher Feedback Mode

The cipher feedback mode has a structure similar to the stream cipher which operates on streams of bits such as

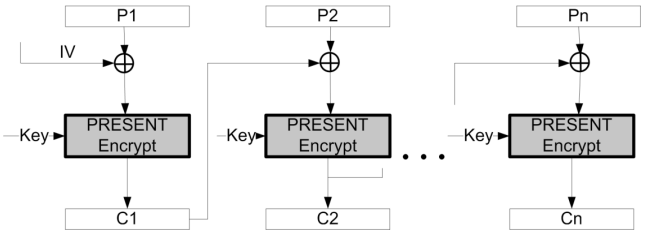


**Figure 3.** CBC mode encryption

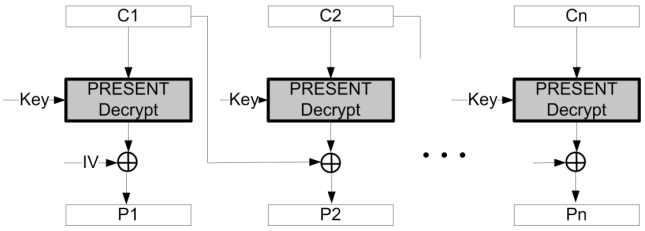


**Figure 4.** CBC mode decryption

s = 8/16/32 for a 64 bit block cipher algorithmic definition. For s = 8 the encryption and the corresponding number of decryption needed to complete encryption / decryption of a block of 64 bit data is 8. The respective numbers of encryption/decryption for s = 16, 32 are 4, 2 respectively. In this mode encryption function is employed for both encryption and decryption of data blocks. The equations that define the stream of encryption and decryption are given in equations (5) and (6) and the respective block diagrams are given in Figure 5 and 6.

$$\text{Encryption:} \quad \begin{array}{l} I_1 = IV \\ O_j = E(K,I_j) \\ C_j = P_j \text{EXOR MSB}_s(O_j) \\ I_j = \text{LSB}_{b-s}(I_{j-1}) || C_{j-1} \end{array} \qquad (5)$$

$$\text{Decryption:} \quad \begin{array}{l} I_1 = IV \\ O_j = E(K,I_j) \\ P1 = C_j \text{EXOR MSB}_s(O_j) \\ I_j = \text{LSB}_{b-s}(I_{j-1}) || C_{j-1} \end{array} \qquad (6)$$

## 2.4 Output Feedback Mode

The output feedback mode has the output of the first stage of encryption fed as input to the second stage as in

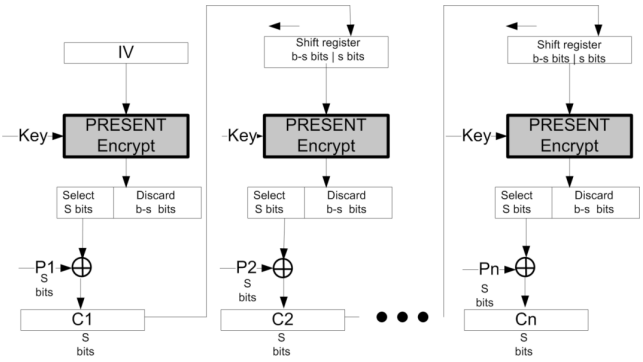


**Figure 5.** CFB mode encryption (s=8/16/32)

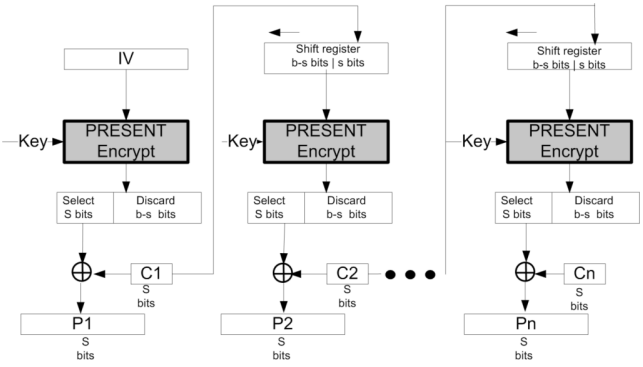


**Figure 6.** CFB mode decryption (s=8/16/32)

Figure 7 and 8 for encryption and decryption, respectively. The expressions relating the cipher text and the plain text for each of the encryption and decryption are given in the equations (7) and (8).

$$\text{Encryption:} \quad \begin{aligned} &I_j = \text{Nonce} \\ &O_j = E(K,I_j) \\ &C_j = P_j \text{ EXOR } O_j \\ &Ij = O_{j-1} \\ &\text{for } j = 2,\ldots\ldots\ldots N \end{aligned} \tag{7}$$

$$\text{Decryption:} \quad \begin{aligned} &I_j = \text{Nonce} \\ &O_j = E(K,I_j) \\ &P_j = C_j \text{ EXOR } O_j \\ &\text{for } j = 2,\ldots\ldots\ldots N \end{aligned} \tag{8}$$

## 2.5 Counter Mode

In the counter mode of operation the random count value is used as the nonce input for the first stage of encryption. In every successive stage of encryption the counter is incremented and given as the input to every stage of encryption. The equations governing the counter mode are given in equations (9) and (10) with the figures depicted in Figure 9 and 10.

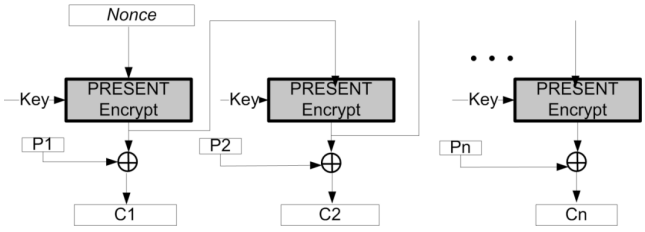


**Figure 7.** OFB mode encryption

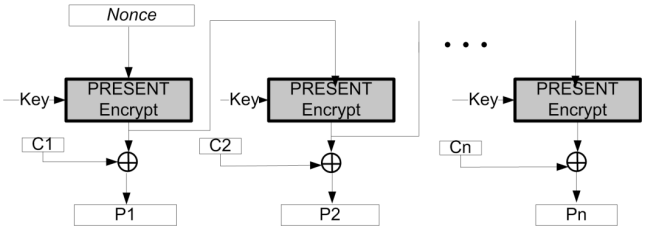


**Figure 8.** OFB mode decryption

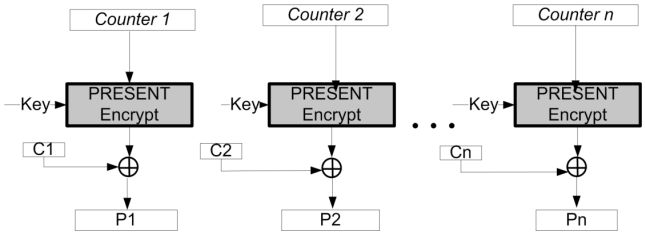


**Figure 9.** CTR mode encryption

$$\text{Encryption:} \quad C_j = P_j \text{ EXOR } E(K,[T_j]) \tag{9}$$

$$\text{Decryption:} \quad Pj = Cj \text{ EXOR } E(K,[Tj]) \tag{10}$$

# 3. Design Methodology and Design Environment

The architectural definition of all the modes are defined in VERILOG HDL and implemented in the xc3s4000l-4fg900. The throughput estimation is done based on the results of synthesis in the typical FPGA. The coding specification for each of the modes is defined in the similar manner in order to have a fairer comparison of the results. The design methodology employed to evaluate the speed performance of the various modes is that the modes are allowed to perform three block encryptions serially. The architectural design of the mode structures features the encryption/decryption hardware and the sub key generation. The area utilization mentioned and the throughput estimation involves both the encryption/decryption operation and the key generation for every mode. The modes CFB, OFB and CTR uses only encrypt function for performing both encryption and decryption. The applications of each of the modes are tabulated in Table 1 and 2 give the possibility of parallelism of the encryption and decryption structure for the individual modes. Wherever the cipher text/plain text generation is dependent on the successive operations the parallelism is not possible.

The following section details the implementation results of the different modes of operation in the Spartan-3 FPGA.

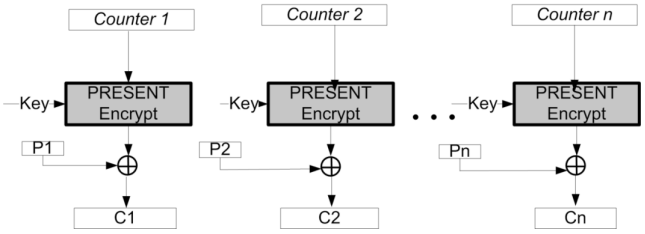


**Figure 10.** CTR mode decryption

**Table 1.** Applications of each mode of operation

| Mode | Application |
|---|---|
| ECB | Secured single key transmission |
| CBC | Authentication and block transmission |
| CFB | Authentication and stream transmission |
| OFB | Authentication and block transmission |
| CTR | High speed applications |

## 4. Implementation Results and Discussion

Table 3 gives the delay incurred for each of the modes for performing a single block of 64 bit information. Since the CFB mode operates on streams of information the results are shown for the stream size of 8, 16 and 32 denoted as s_8, s_16 and s_32, respectively. The results hence have three set of delay values for encrypting 64 bit block data with varying steam sizes. The CFB mode has incurred the larger encryption delay than the other modes of operation to provide confidentiality. Figure 11 shows the bar chart representation of the delay values. All the other four modes ECB, CBC, OFB and CTR work on blocks of 64-bit data. Results summarized for these modes operate on three successive block data encryption. The area utilization in terms of slices and its 4 input LUTs in the SPARTAN 3 FPGA are presented for the designed mode architectures in Table 4. As can also be observed the resource utilization is large for the CFB mode structure.

The information shown in Table 5 features the randomness of the cipher text after every encryption for each of the modes. It can be clearly visualized that, other than the ECB mode all other modes have no possible

**Table 2.** Modes Parallelizable/ non-parallelizable encryption and decryption

| Mode | Parallelizable | |
|---|---|---|
| | Encryption | Decryption |
| ECB | Yes | Yes |
| CBC | No | Yes |
| CFB | No | Yes |
| OFB | No | No |
| CTR | Yes | Yes |

**Table 3.** Delay comparison of the different modes of operation

| Mode | | Encryption Delay (ns) |
|---|---|---|
| ECB | | 113.338 |
| CBC | | 112.477 |
| CFB | s = 8 | 810.908 |
| | s = 16 | 411.913 |
| | s = 32 | 212.584 |
| OFB | | 113.211 |
| CTR | | 113.211 |

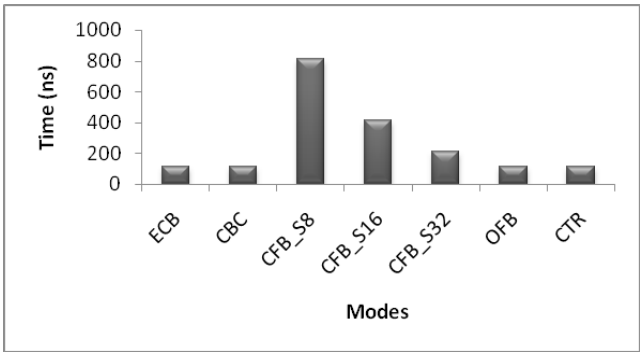


**Figure 11.** Encryption time for each mode of operation

**Table 4.** Resource utilization comparison of the different modes of operation

| Mode | | Encryption | |
|---|---|---|---|
| | | Slices | 4 input LUTs |
| ECB | | 2266 | 4156 |
| CBC | | 2225 | 4090 |
| CFB | s = 8 | 16844 | 30980 |
| | s = 16 | 8645 | 15872 |
| | s = 32 | 4395 | 8062 |
| OFB | | 2279 | 4171 |
| CTR | | 2279 | 4171 |

estimation of cipher texts produced by the encryption process. This is due to the fact that the modes cipher text generation is dependent on many values namely, the previous cipher text, initial vector values, nonce values, etc. Hence, it is difficult to predict the information by cryptanalysis techniques in the modes of operations namely, CFB, CBC, OFB and the CTR modes.

The changes in the plain text for each of the modes for encrypting three blocks of information has been calculated for the same set of inputs, keys, initial vectors and nonce values wherever applicable in the different modes. The change between the inputs and the outputs are presented for the cipher feedback mode, which operates on streams of input data. Apart from the ECB mode all the other modes produce different cipher texts for every encryption irrespective of the same plain text and the same key. The identical plain texts result in different random cipher texts in case of the modes other than the ECB. Table 5 shows the cipher texts for the plain texts for successive encryptions. It can be observed that for the same plain text there is difference in the cipher texts for every successive encryption. The first set of simulations

has been conducted to compare the modes of operations. Figure 12 shows the throughput comparisons for every mode for different block sizes.

## 5. Comparison with other Block Ciphers

Direct comparison of the hardware architecture of the block ciphers is a trivial task, The results significantly vary depending on the block size, architectural mechanisms employed, types of architecture namely serial, loop, optimization mechanisms namely, pipelining, unrolling, typical FPGAs selected etc. Hence the comparison details the maximum possible implementation information for the comparison of the proposed work with that of the relevant. The comparison of the modes of operation for the different block sizes are shown in Table 6. It can be observed that the throughput of the proposed work shows a high throughput even in the less frequency of operation as compared to the relative works and hence it is highly applicable for high frequency applications. The resource utilization for the 64 bit PRESENT block cipher mode architectures also show the reduced area occupancy in terms of slices and 4- input LUTs as compared to the AES implementation with 8 bit and 64 bit implementations as compared in Table 6. Note that in the implementations with reduced slice utilization has involved the usage of BROMs/BRAMs in the architecture. The proposed implementations have employed only the slices and LUTs in the

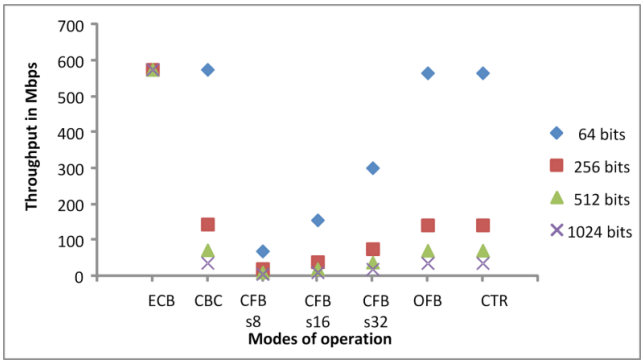


**Figure 12.** Throughput comparisons of the modes for different block sizes

**Table 5.** Avalanche effect for each of the modes

| Mode | | Encryption 1 | Encryption 2 | Encryption 3 |
|---|---|---|---|---|
| | Plain text | 00000000_00000000 | 00000000_00000000 | 00000000_00000000 |
| ECB | Cipher text | 5579c138_7b228445 | 5579c138_7b228445 | 5579c138_7b228445 |
| CBC | Cipher text | 5579c138_7b228445 | 4edf45fd_6fcc369a | 900f59f3_f6041920 |
| OFB | Cipher text | 5579c138_7b228445 | 4edf45fd_6fcc369a | 900f59f3_f6041920 |
| CTR | Cipher text | 5579c138_7b228445 | 38cbdc86_3843c72f | e4612cb7_ae919c90 |
| CFB_S8 | Cipher text | 55638a61_f5c90f78 | – | – |
| CFB_S16 | Cipher text | 5579 a147_ dffb8283 | – | – |
| CFB_S32 | Cipher text | 5579c138_ efc47c35 | – | – |

**Table 6.** Comparison with related works

| Related works | Supported Block size | Algorithm | Architecture | Encrypted block size (128 bit) | Slices | BRAMs | BROMs | LUTs | Frequency (MHz) | Through put (Mbps) |
|---|---|---|---|---|---|---|---|---|---|---|
| ECB [4] | 8–bit | AES | serial | 1 | 169 | 3 | – | – | – | 45.09 |
| CFB/OFB [4] | 8–bit | AES | serial | 1 | 106 | 3 | – | – | – | 82.18 |
| OCB [5] | 128–bit | AES | serial | 1 | 3552 | 1 | 3 | – | 50 | 493 |
| ECB [5] | 128–bit | AES | serial | 1 | 3552 | 1 | 3 | – | 50 | 6400 |
| all modes [7] | 128–bit | AES | serial | 1 | 7452 | – | – | 4045 | – | 480.427 |
| ECB [10] | 128–bit | AES | single round basic loop architecture | 2000 | 1059 | – | – | 1167 | – | – |

(*continued*)

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| CBC [10] | 128–bit | AES | single round basic loop architecture | 2000 | 1075 | – | – | 1171 | – | – |
| CFB [10] | 128–bit | AES | single round basic loop architecture | 2000 | 1073 | – | – | 1169 | – | – |
| OFB [10] | 128–bit | AES | single round basic loop architecture | 2000 | 1082 | – | – | 1181 | – | – |
| CTR [10] | 128–bit | AES | single round basic loop architecture | 2000 | 1080 | – | – | 1187 | – | – |
| Proposed work [ECB] | 64–bit | PRESENT | serial | 1 | 2266 | – | – | 4156 | 8.981 | 574.784 |
| Proposed work [CBC] | 64–bit | PRESENT | serial | 1 | 2225 | – | – | 4090 | 8.981 | 574.784 |
| Proposed work [CFB] | 64–bit (s=8) | PRESENT | serial | 1 | 16844 | – | – | 30980 | 1.233 | 68.912 |
| Proposed work [CFB] | 64–bit (s=16) | PRESENT | serial | 1 | 8645 | – | – | 15872 | 2.428 | 155.392 |
| Proposed work [CFB] | 64–bit (s=32) | PRESENT | serial | 1 | 4395 | – | – | 8062 | 4.7 | 300.8 |
| Proposed work [OFB] | 64–bit | PRESENT | serial | 1 | 2279 | – | – | 4171 | 8.833 | 565.312 |
| Proposed work [CTR] | 64–bit | PRESENT | serial | 1 | 2279 | – | – | 4171 | 8.833 | 565.312 |

chosen FPGA and no BROMs/BRAMs were involved in the implementation.

## 6. Concluding Remarks

This paper presents the mode specific implementations of the 64-bit PRESENT light weight block cipher. The slices and throughputs vary from around 225 to 16844 slices and 68.912 Mbps to 574.784 Mbps respectively, depending on the modes employed and the implementing techniques used. The implementation achieves a minimum of 4090 4-input LUTs in ECB mode architecture to 30980, 4-input LUTs in CFB mode architecture with a stream size of 8 bits.

If the key expansion in the design is pre-computed and used later by the encryption/ decryption processing, then the slices can be further decreased and the throughput will be much improved.

## 7. References


1. Bogdanov A. PRESENT: an ultra-lightweight block cipher, In: Proceedings of the 9th inter- national workshop on cryptographic hardware and embedded systems. Vienna, Austria: Springer-Verlag. 2007:4727:450–66.
2. Dworkin M. Recommendation for Block Cipher Modes of Operation NIST Special Publication 800-38A 2001 Edition. 2010, p. 1-13.
3. Block cipher mode of operation.https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation, Date accessed: 30/08/2016.
4. Huang CW. Block RAM Based Design of 8-bit AES Operation Modes. Procedia Engineering. 2012; 29:2848–52.
5. Chit CU, Glesner M. An FPGA implementation of the AES-Rijndael in OCB/ECB modes of operation. Microelectronics Journal. 2005; 36(2):139–46.
6. Tarhuni MA. Enhanced Counter ModeThe 9th Asia-Pacific Conference on Communications, APCC Malaysia, 2003, 2, p. 701–05.
7. Grabowski JS, Youssef A. An FPGA Implementation of AES with Support for Counter and Feedback Modes. International Conference on Microelectronics, Cairo 2007, p. 39 – 42.
8. Huang CW. The Five Modes AES Applications in Sounds and Images. Sixth International Conference on Information Assurance and Security (IAS), August Atlanta, GA, 2010, p.28 –31.

9. Alomari MA. A study on encryption algorithms and modes for disk encryption. International Conference on Signal Processing Systems, Singapore, 2009, p. 793–97.
10. Jayasinghe D. Advanced Modes in AES: Are they Safe from Power Analysis based Side Channel Attacks. 32nd IEEE International Conference on Computer Design (ICCD), Seoul, 2014, p. 173–180.
11. Jaffe J. A first-order DPA attack against AES in counter mode with unknown initial counter, Cryptographic Hardware and Embedded Systems - CHES of Lecture Notes in Computer Science, Springer Berlin Heidelberg. 2007; 4727:1–13.
12. Rogawayet P. OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption. Eighth ACM Conference on Computer and Communications Security ACM CCS, ACM Press, Colorado, 2001. p. 196–205.
13. Kohno T. CWC: A high-performance conventional authenticated encryption mode, Proceedings of FSELNCS Springer- Verlag, 2004; 3017:408–26.
14. David A, McGrew M, Viega J. The Security and Performance of the Galois/Counter Mode (GCM) of Operation, Progress in Cryptology-INDOCRYPT, Springer-Verlag, 2004; 3348:345–55.
15. Lopez-Trejo E. Efficient FPGA implementation of CCM mode using AES. International Conference on Information Security and Cryptology Lecture Notes in Computer Science, Seoul, Korea, Springer-Verlag, 2005; 3935:208–215.
16. Chakraborty D, Sarkar P. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. Information Security and Cryptology, Springer, 2006, p. 88–102.
17. Sung J. Concrete security analysis of ctr-ofb and ctr-cfb modes of operation. Proceedings of Information Security and Cryptology - ICISC 2001Lecture Notes in Computer Science, Springer- Verlag, 2002, p. 103–13.
18. Menezes A, Oorschot PV, Vanstone S. Handbook of Applied Cryptography, by CRC Press, 1996.
19. Krovetz T, Rogaway P. The OCB Authenticated-Encryption Algorithm. Internet Draft draft-krovetz-ocb-00, CFRG Working Group, 2005.
20. Sasi SW, Sivanandam N. A Survey on Cryptography using Optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3):216–21.
21. Isha, Luhach AK. Analysis of Lightweight Cryptographic Solutions for Internet of Things. Indian Journal of Science and Technology. 2016 Jul; 9(28):1–7.
22. Alomari MA, Samsudin K, Ramli AR. Implementation of a Parallel XTS Encryption Mode of Operation. Indian Journal of Science and Technology. 2014 Nov; 7(11):1813–19.