# Hardware Efficient LDPC Coding Using Linear Feedback Shift Registers For Secured Transmission

**M.Valarmathi, Burimodhini**

***Abstract:** Low Density parity correcting codes are linear error correcting codes, a method of transmitting a message over a noisy channel. The main advantages at LDPC codes are these are reliable and high efficient. In this work LDPC encoder and decoder part of LDPC functioning for compiling a 8-bit message vector and it can be done using verilog code. For secure transmission, LFSR is proposed which provides bit scrambling which is used to encode the information signal at transmission side to make it unintelligible at the receiver side. The output of the LDPC encoder is given to the input of LFSR encoding block which gives the longer information bits called code word. This increases the security, reliability and hardware complexity of the information bits. Decoding is done by Berlekamp-massey algorithm. The proposed LDPC using LFSR encoding design has good performance in which 45 LUT's are being used instead of 72 LUT's used in normal LDPC encodes architecture which is optimized with high speed and area.*

***Index Terms:** LDPC using LFSR, Code Word, Berlekamp-massey algorithm.*

## I. INTRODUCTION

Robert Gallger created a code called Linear Density Parity Checker in 1960. These codes are overlooked over 30years due to gear multifaceted nature around by then. This coding was reconsidered by Mackay and Neal in the year 1990's over structure up on codes utilizing lacking uniformity test grid. LDPC codes keep starting late pulled in massive research interest because of their stunning oversight helping execution and exceedingly parallel disentangling plan. LDPC codes are preferred by electronic video broadcasting standard and when in doubt really considered in various certified applications, for example, attractive capacity, 10 Gb Ethernet, and high-throughput remote neighbourhood. LDP C codes are high reliable compare to the turbo code in most of the communication and digital storage system for error control. The LDPC codes having more advantages then turbo codes are: In LDPC codes long interleave is not required to obtain good error performance and LDPC decoding is not trellis based. Low-density parity-check codes contain 0'S and 1'S [1]. LDPC codes are linear codes which contains generator matrix G, parity check matrix H, which satisfies $HX^T=0$ [2]. Initially parity matrix is generated by regular matrix; by using Gaussian elimination method generator matrix can be created. LDPC consists of two types of parity matrices termed as regular and irregular matrix. In Tanner graph the nodes are subdivided within two disconnect classes. An edge of graph is connecting to a node of one class to a node of the other class along with there is no edges connecting nodes of the same class [3]. Parity check matrix consists of two nodes, 1) check nodes2) variable nodes [4].AWGN channel is used in LDPC codes only for some space limitations to determine the error rate [5].this error rate can depends upon the minimum amount of distance which is related to the code along with the minimum error events [6][7].LDPC are generally utilizing ECC (Error Correcting Codes) for having famous abilities. By utilizing Message Passing Algorithm, these codes can be decoded. Secure information bits is the main objective for the development of computer and communication networks. Random Number generators are used for this purpose. These are used in bank security, space communication LFSR is proposed which provides bit scrambling and use to encodes the signal at transmitter side to make it unintelligible at receiver side. The main advantage of the LFSR is it has used in cryptography and coding theory. It can be also known as pseudo-random number generator. It provides High binary sequences.

**Manuscript published on 30 June 2019.**
***** Correspondence Author (s)

**M.VALARMATHI**, Ece, Srmist, Chennai, India.
**B.MODHINI**, Ece, Srmist, Chennai, India

## II. LDPC DESIGN

The complete LDPC system is Split into three Main parts
1) LDPC Encoder
2) Additive White Gaussian Noise-channel
3) LDPC Decoder
The block diagram of LDPC was mentioned inFig1

### A. LDPC ALGORITHM

Low density parity check codes are linear codes which have length of C can be specified by either Generator matrix G or parity check matrix H. The Code-Word C is given by

$$C=KG \longrightarrow \qquad (1)$$

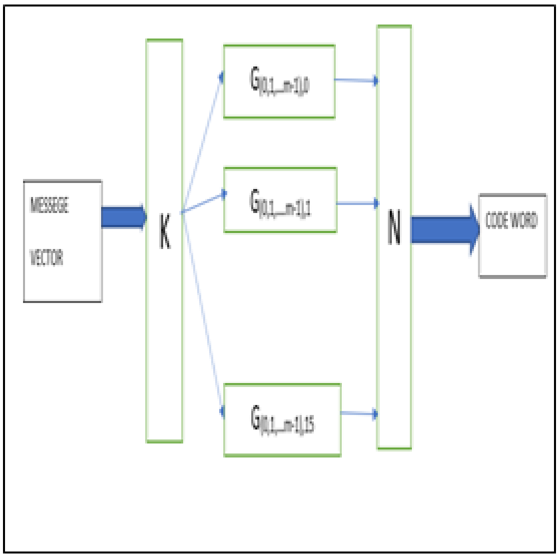
Here, "K" is Message Vector
G - Generated Matrix
The Reliable Codeword is shown by

$$HC^T=0 \longrightarrow \qquad (2)$$

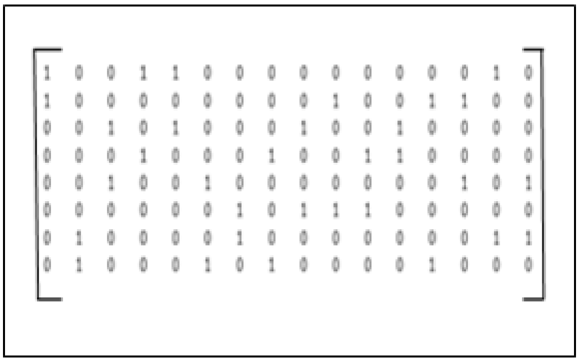
Here "H" is Parity Check Matrix. Here the codeword is inconsistent when equation (2) is not equal to "0".

### B. LDPC ENCODER

The LDPC encoder uses a generator matrix to encodes the information bits towards the code word. Here Both The matrices are correlated. The Block Diagram for LDPC encoder is mentioned in Fig.2



In LDPC coding two types of matrices are existed and it is termed as Regular Matrix, Irregular matrix. In this work we are utilizing ordinary framework of 8x16. The regular matrix is given in fig.3.

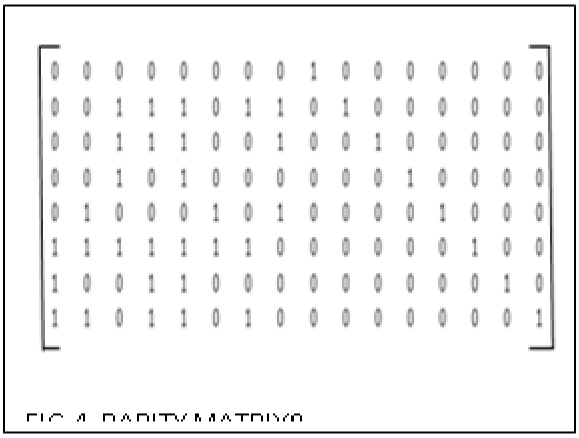


$$\begin{bmatrix}
1&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
1&0&0&0&0&0&0&0&0&1&0&0&1&1&0&0\\
0&0&1&0&1&0&0&0&1&0&0&1&0&0&0&0\\
0&0&0&1&0&0&0&1&0&0&1&1&0&0&0&0\\
0&0&1&0&0&1&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0\\
0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&1\\
0&1&0&0&0&1&0&1&0&0&0&0&1&0&0&0
\end{bmatrix}$$

The parity matrix is given by

H=[A | In-K] ⟶ (3)

Initially Parity Check Matrix is obtained, We are applying a method called Gaussian Elimination, for transferring parity matrix into standard form that is H=[A|In-k]. The H matrix place by starting rudimentary column tasks that is trading two lines or else adding one line to another modulo 2. The fig. 4



$$\begin{bmatrix}
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&1&1&1&0&1&1&0&1&0&0&0&0&0&0\\
0&0&1&1&1&0&0&1&0&0&1&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&1&0&0&0&0\\
0&1&0&0&0&1&0&1&0&0&0&0&1&0&0&0\\
1&1&1&1&1&1&1&0&0&0&0&0&0&1&0&0\\
1&0&0&1&1&0&0&0&0&0&0&0&0&0&1&0\\
1&1&0&1&1&0&1&0&0&0&0&0&0&0&0&1
\end{bmatrix}$$

FIG 4 PARITY MATRIX

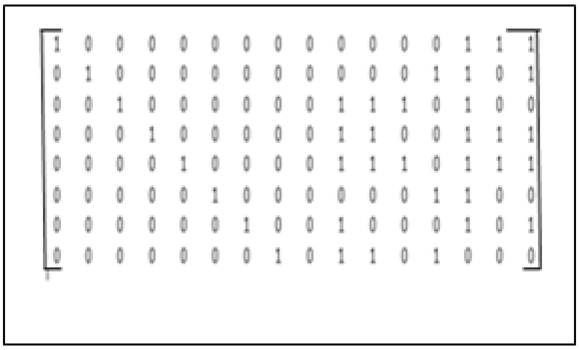
shows the example of Parity Matrix.

The gained parity matrix is converted to conventional form of generator matrix.

The Generator matrix is given by

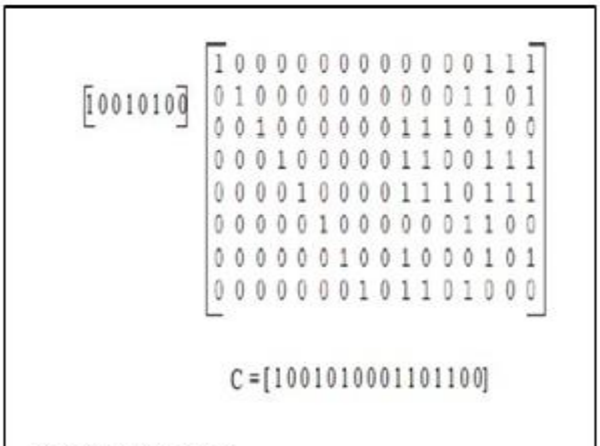
G = [IK | AT] ⟶ (4)

The generator matrix is matrix is mentioned in Fig.5.



$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1\\
0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&1&1&1\\
0&0&0&0&1&0&0&0&0&1&1&1&0&1&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0
\end{bmatrix}$$

When The Message vector [K] is multiplied with generator matrix [G] which mentioned above and the information message bits are encoded. i.e. C= [K][G] to obtained the codeword, Where K is the message vector, Let us consider K=[00001100]. We have to encode U and G and it is mentioned in fig 6.



$$[10010100]\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&0&1&1&1\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&1\\
0&0&1&0&0&0&0&0&0&1&1&1&0&1&0&0\\
0&0&0&1&0&0&0&0&0&1&1&0&0&1&1&1\\
0&0&0&0&1&0&0&0&0&1&1&1&0&1&1&1\\
0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&1&1&0&1&0&0&0
\end{bmatrix}$$

C=[1001010001101100]

FIG 6 ENCODING

After the multiplication of the message vector [U] along generator matrix[G]it has been observed that the codeword of 10 bits C=[100101101]. Using Verilog code we done the coding part of this LDPC using encoder and tested for different information bits. The Simulation Results for LDPC encoding are shown in Fig-9.

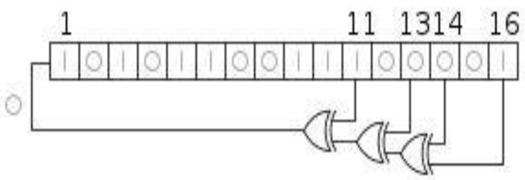
*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication (BEIESP)*

## III. LDPC ENCODING USING LFSR

LFSR provides Bit scrambling, Spread spectrum which is used to encodes the information signal at transmitter side to make it unintelligible at the receiver[8]. By using this method it can able to hide the information signal which can be retrieve by using different algorithms. Because of the advantages it is used in cryptography and coding theory.

### *C. LFSR*

Linear Feedback Shift Register(LFSR) is a shift register whose input bits is a linear function of its pervious state[9]. Exclusive-OR(EX-OR) is the most commonly used linear function of single bits. So Linear Feedback Shift Register is consistently a shift register here the input is forced by the XOR gates of few bits of the overall shift register value. A LFSR is Similar to device called State Machine. The XOR and XNOR are the only Linear function of Single Bits. The Initial value of the LFSR is called Seed, and because the operation of the register is totally intent on by its current (or previous) state. The basic block diagram of LFSR is given in Fig7.



$x^{16}+x^{14}+x^{13}+x^{11}+1$

FIG7. BASIC BLOCK DIAGRAM OF LFSR

The bits in the Linear Feedback Shift Register state which force the information is called taps. A most extreme extent Linear Feedback Shift Register brings a m-succession except if it includes each of the zeros, in which case it will nothing to show signs of change. A grouping of numbers formed by this strategy is arbitrary. A time of the grouping is ($2^n$ - 1), where n is the quantity of move registers utilized in the structure.

### *D. LDPC ENCODING USING LFSR*

The LFSR encoder comprises of three major blocks

1)5 bit parallel to shift register

2) Linear feedback shift register

3) The LFSR encoding module is planned as for the created polynomial given Generator polynomial is isolated by the approaching 4-bit message bits[10]. The division is done utilizing linear feedback shift register, the leftovers of this division is included with the first message bits to shape a "codeword". The block diagram of LDPC Encoding using LFSR is given in Fig.8. The simulation results for LDPC encoding Using LFSR is shown in Fig.10.

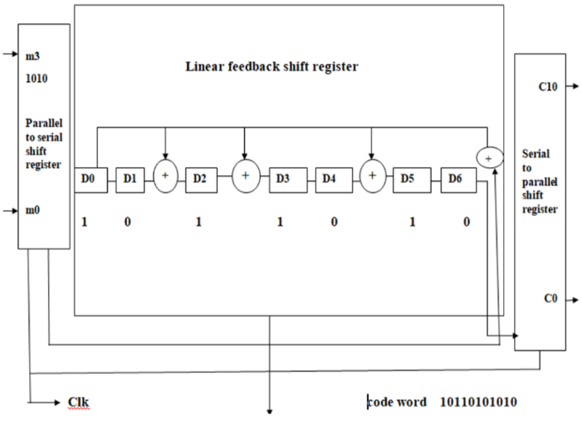

m3
1010
Parallel to serial shift register
m0
Linear feedback shift register
D0
D1
+
D2
+
D3
D4
+
D5
D6
+
1
0
1
1
0
1
0
Serial to parallel shift register
C10
C0
Clk
code word 10110101010

FIG.8. LFSR ENCODER

### *E.LFSR DECODING(BERLEKAMP-MASSEY ALGORITHM)*

LFSR's are widely used as pseudo-random number generator by reason of their simplicity. The Berlekamp-Massey algorithm which can give the shortest LFSR for considering a given binary output sequence. The Berlekamp-Massy algorithm will also discovers the minimal polynomial of a linearly regular sequence. It means that this algorithm have need all non-zero elements has a multiplicative inverse. The Berlekamp-Massey algorithm is an iterative algorithm which starts with assuming L=1.where L is the number of coefficients[11]. The simulation Results of LFSR Decoder is given in Figure-11.

## IV. SIMULATIONS AND EXPERIMENTAL RESULTS

The proposed solutions have been designed using Xilinx 14.5 software. From the fig 9, if reset is high then output resulted as low and if reset is low then input is encoded and finally gives the codeword .in this input is taken as10010100 and the obtained codeword is 1001010001101100 where the noise factor is 11111111s.From fig 10, it has been shown that the division of generator polynomial and message bit is placed and this remainder will added to the generator polynomial to form codeword. Here, the generator polynomial is 1010010 and the 4-bit message bit is given by 1010 .the codeword obtained from Lfsr encoding is 10100101100.fig 11 shows the results of Lfsr decoding by using Berlekamp-Massey algorithm to retrieve the original message bit as1010.The comparison of LDPC encoder and LDPC using LFSR encoding is shown in table 1. The table shows the timing and area analysis of proposed LDPC encoder and LDPC using LFSR encoding.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

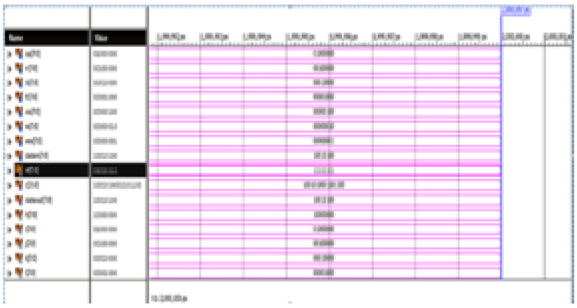


FIG 9. SIMULATION RESULTS FOR LDPC

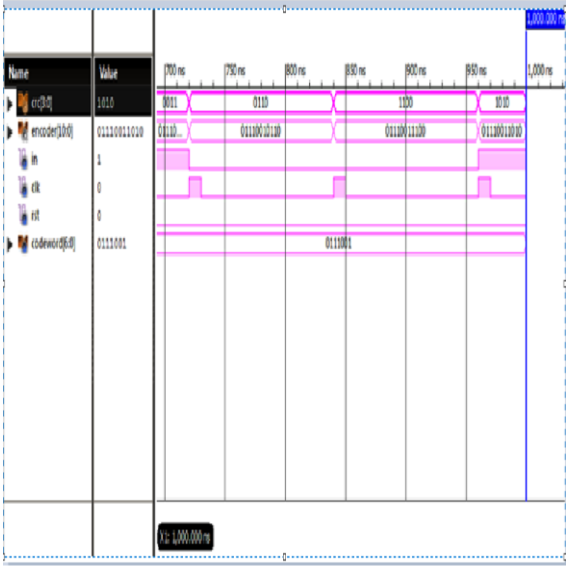
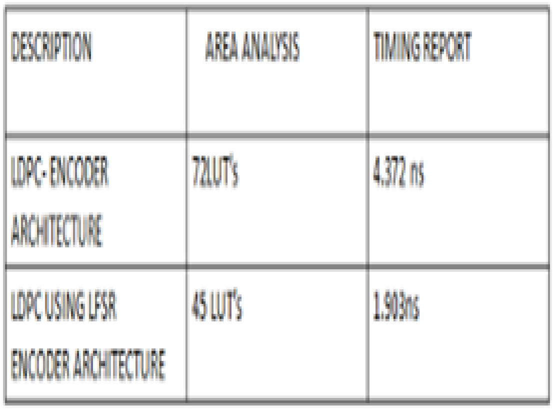


FIG10. SIMULATION RESULTS FOR LDPC USING LFSR ENCODING

TABLE1. COMPARISON TABLE OF LDPC-ENCODER &LDPC USING LFSR ENCODER



| DESCRIPTION | AREA ANALYSIS | TIMING REPORT |
|---|---|---|
| LDPC- ENCODER ARCHITECTURE | 72LUT's | 4.372 ns |
| LDPC USING LFSR ENCODER ARCHITECTURE | 45 LUT's | 1.903ns |

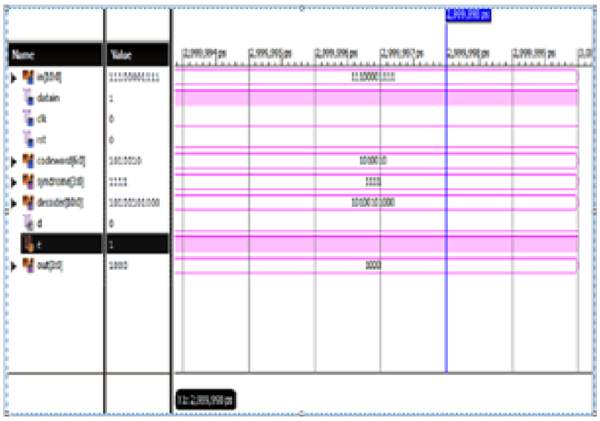


FIG11. SIMULATION RESULTS FOR LFSR DECODING

## V.CONCLUSION

LDPC coding is a better average mistake amending coding methodology which permits forward blunder update and therefore the transmission data rate is higher. In this paper normal LDPC encoder, LDPC using LFSR encoding and decoding has shown. LDPC Coding is used up as 8×16 and 7×4 parity check matrix along line weight related to 4 and segment weight related to 2. Coding is done on Xilinx along with the results. Coding pleasingly checked as multiple 8-bit message vectors. The result of this encoder is the input of the LDPC using LFSR encoding. Berlekamp-massey algorithm is used for decoding. So, it can be concluded that , LDPC using LFSR encoding has good performance in which 45 LUT's are being used instead of 72 LUT's used in normal LDPC architecture. The implementation time also less compared to the normal LDPC due to the feedback architecture, which neglects Hardware complexity So, the designed LDPC using LFSR encoding is optimized with less area and high speed.

## REFERNCES

1. R. M. Neal, "Near Shannon limit performance of low density parity check codes," vol. 32, no. August, pp. 1645–1646, 1996.
2. R. M. Tanner, "A Recursive Approach to Low Complexity Codes," vol. I, pp. 533–547, 1981.
3. I. Journal and C. Engineering, "DESIGN OF LDPC ARCHITECTURE USING," vol. 3, no. 4, pp. 1527–1531, 2014.
4. T. Richardson, "Error Floors of LDPC Codes," pp. 1426–1435.
5. H. Li, W. Huang, and J. C. Dill, "Construction of Irregular LDPC Codes with Low Error Floors."
6. L. Wei and S. Member, "Several Properties of Short LDPC Codes," vol. 52, no. 5, pp. 721–727, 2004.
7. K. M. M. Chennaiah, K. Prasadbabu, and S. Ahmedbasha, "IMPLEMENTATION OF BCH LFSR ENCODER DECODER," vol. 5, no. 1, pp. 21–30, 2017.
8. R. G. Gallager, ―Low density parity check codes,‖ IRE Trans. Inform. Theory, vol. IT-8, no.1, pp. 21–28, Jan. 1962
9. design and implementation of multibit LFSR on FPGA to generate pseudorandom sequence number
10. Softjin technology, "Data sheet for BCH encoderLFSR core', India, Dec 2000, www.softjin.com.
11. Erin Casey, "Berlekamp-Massey Algorithm" University Of Minnesota REU Summer 2000.

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication (BEIESP)*
*© Copyright: All rights reserved.*