International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Analysis of High Efficiency Low Density Parity-Check Code Encryption

[1]Sk. Reshma, [2]Sk. Sajida, [3]Sk. Reshma, [4]Sk. Affroz Banu, [5]D. Pratap Kumar
[1,2,3,4]B.Tech-Scholar, Dept of ECE, ST. Mary's Women's Engineering College, Guntur, India.
[5]Assistant Professor, Dept of ECE, ST. Mary's Women's Engineering College, Guntur, India.

ABSTRACT: *In this study, we propose a low power, high efficient Low Density Parity-Check Code (LDPC) Decoder Architecture for error detection and correction applications. LDPC codes have been adopted in latest wireless standards such as satellite and mobile communications since they possess superior error detecting and correcting capabilities. As technology scales, memory devices become larger and more powerful and low power consumption based error correcting codes are needed. This study discusses the design and analysis of check node unit and variable node unit in LDPC decoder. The architecture is synthesized and Xilinx and simulated using modelsim which is targeted 90nm device. Synthesis report shows that the proposed architecture reduces the hardware utilization and power consumption when compared to the conventional architecture design.*

Keywords: LDPC Decoder, Node Architecture, Variable Node, Check Node

I.INTRODUCTION

Low Density Parity-Check (LDPC) codes are known to have excellent performance for high speed data transmission and low complexity. However, moderate-length or short length binary LDPC codes have been shown to have an early error floor and degraded decoding performance. These codes have been implemented in various standards such as WiMax (IEEE 802.16) and other high speed applications, where parallel implementations of iterative message-passing algorithms are ideally used in LDPC decoding. Reducing the complexity of the algorithm means to reduce the chip size and power consumption, at the same time increasing the throughput. Hence, Min-sum(Ms) algorithm was used to solve this issue. LDPC codes are suitable for iterative decoding, i.e an iterative decoder can perform consecutive decoding of both rows and columns. LDPC implements parallelism in the decoding process there by achieving high decoding throughput.

There are several decoding algorithms conventionally used. Out of these, the belief propagation (BP) algorithm attains an excellent decoding performance for the standard BP algorithms and numerous multiplicative, logarithmic computations are necessary to compute the check node. The min-sum (MS) algorithm, interchanges the product term with the min value. Even though performance is reduced, the hardware complexity of the BP algorithm is significantly it minimized, by replacing complex computations of check nodes with simple summation and comparison operations. The min-sum algorithm provides a less sensitivity in decoding performance under finite word-length implementations and do not require channel information. Due to these advantages, MS algorithm is widely used.

II.EXISTED DECODER ARCHITECTURE

The decoder using our method consists of two processing elements-Check Node Unit (CNU) and Variable Node Unit (VNU) as shown in **Fig.1**.The CNUs and VNUs are connected through the routing network. Input and output edges of the check node unit are labled by the connectivity given by parity-check matrix. The final outputs are taken from the VNU after the required numbers of iterations have been completed.

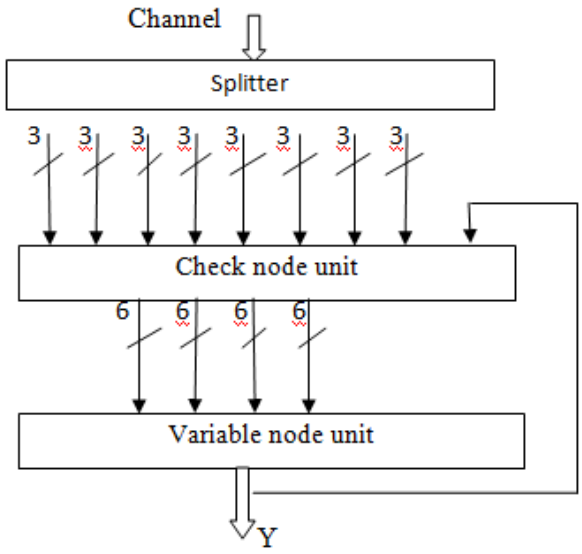

Fig. 1. LDPC decoder design overview

A. Check Node Architecture: The proposed check node module of LDPC is used in determining the strength of the received signal against noises in the channel. Four directional difference vectors are calculated with twelve SUB, four ADD and sorter and concatenator modules.

Then, the value of smallest difference is decided by using the sorter and concatenator units**.** In the proposed design, ADD and subtractor unit, there by reducing the hardware cost.

After addition and subtractions are determined on received sequences, the sorting and concatenation is performed on these sequences in order to compute the response of the check node unit in LDPC decoder. Each check node block produces 6 bit length of sequence and thus it produces 24 bit length sequence.

B. Variable Node Architecture: The variable node unit architecture computers the hard decision vector X. This vector is routed through the routing network to the check note block (CNB) the routing between two nodes has single-bit value and the routing network size is smaller compare to that used in sum product algorithm. The variable node processor unit is comprised of a flip-detection circuit, line buffer, multiplexed adder and concatenator. Initially the received signal Y from check node unit, is fed to the variable node block (VNB) through a register-feedback assembly.

The received values are 6-bit Signed-Magnitude (SM) values. Let [sn:mn] be n^{th} 4-bit value provided to the n^{th} VNB, where sn denotes hard decision value and mn denotes the magnitude of the same. The SM makes the correlation calculation simple to be implemented. The correlator circuit consists of an inverter followed by 1-bit multiplexer. The proposed VNA unit consists basic multiplexer, line buffer, summer and concatenator modules. The block datas received from CNU unit are divided in to four sub blocks. The first three sub module blocks are processed by adder

module and last sub module block is processed directly by multiplexer unit.

The signed bit input is applied to the shift operator. The multiplexers and line buffers help in producing the control signal, which is fed to the VNU. The use of simple computational methodologies along with less row and column weights reduces the operations thereby, resulting in significantly less power consumption.

III. PROPOSED SYSTEM

The below figure (2) shows the block formation of AES algorithm. Depending upon the online file processing applications the proposed system will use a prototype. Here this appliance is hosted by the online cloud data base which is provided by the cloud provider go daddy. Basically it is an US based cloud service provider. The main purpose of using this service is to run the applications in very fast way. In this model one system acts as microcontroller where the user can access the information from anywhere at any time from the internet. The main intent of this proposed system is to secure the data with confidentiality.

Let us discuss this with an example, if the user wants to access the information for uploading then he or she should have to register with their email-id and phone number to the system. Here the username and password should be created by the user not by the system. After the process of registration the user can login and upload the data with confidentiality. Before uploading the file to cloud the use will get an encryption file as individual blocks. Now at last click on the save button to use that file for future use. This is the normal way to secure data in cloud computing.

Coming to the medical applications, there is no need to carry hard copy or soft copy, instead of that the user can share the copy at anytime from anywhere. But here the important thing is to remember the secret file-id. The file id may in the form of numbers, alphanumeric characters and special characters. Here to upload a file there is no limit of length but it takes time to upload the file. In the proposed encryption algorithm we use 128 bit keys and they perform 10 rounds for this 128 bit keys in proposed system. Depending upon the file size, the file splits into different blocks.

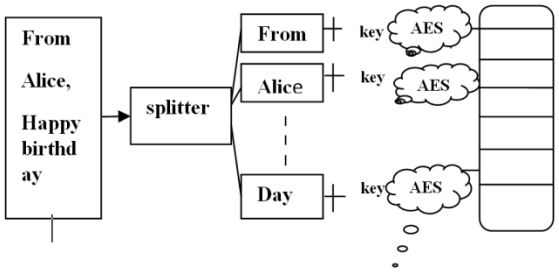

FIG. 2. PROPOSED SYSTEM

These blocks are encrypted individually and block wise encryption is uploaded to the cloud. The upload process is done in different locations by using block-id and file-id. Now in such a case if anyone like the cloud and wanted to get a file from the server then the clod doesn't give total information of that file because it is saved in different locations and the information is in encrypted form. So the person who knows the secret-id can get the total information

from the cloud. Here the proposed system provides the data by using online editing facility. In this process the user can edit the data and as well as upload the data without downloading. This process is done by only the actual users only the other users can only view the data. So from this we can say that the proposed system will secure the data in a confidential way.

IV.RESULTS

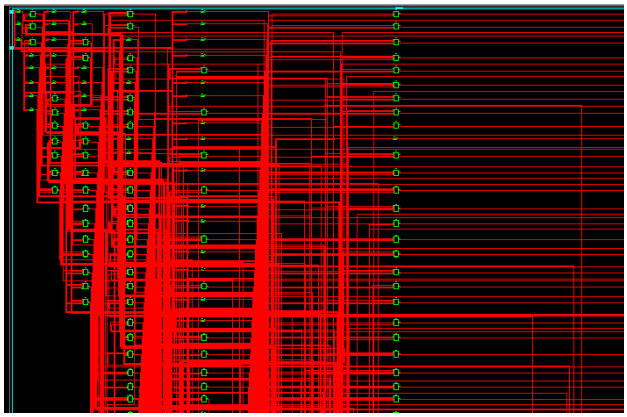

FIG 3.TECHNOLOGY SCHEMATIC

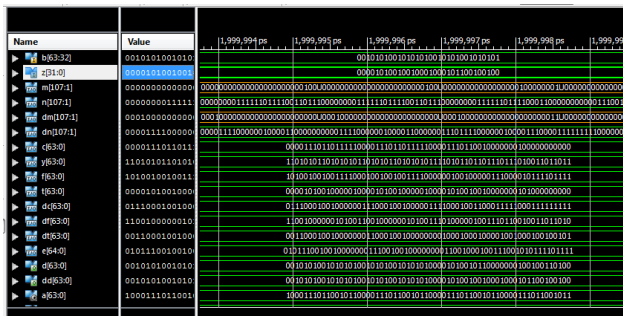

FIG 4. OUTPUT WAVEFORM

V.CONCLUSION

The proposed method is designed by using the novel method. As discussed earlier that LDPC Encryption algorithm performs four basic operations. In this the sub byte substitution method utilizes the less blocks of RAMs and as well as some modifications are done in mix column substitution. By using the sub byte and INV sub byte modules in proposed system there will be less delay and low power consumption. The proposed system provides better security compared to the existed one. 128 bit encryption is provided for the purpose of data confidentiality. Depending upon the performance of delay the proposed approach is analysed. So from this we can say that if the delay is increased then the size of file will be increased. This problem is overcome in our proposed system.

VI. REFERENCES

[1] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," 2001.

[2] S. K. Mathew, et al. "53 Gbps native GF(24)2 composite field AES-encrypt/decrypt accelerator forcontent-protection in 45nm High performance microprocessors, "IEEEJournalOfSoli d-StateCircuits,vol.46,no.4,pp.767 776,April2011.

[3] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient highperformance parallel hardware architectures for the AES GCM,"IEEETransactions on Computers, vol. 61, no. 8, pp. 1165-1178, August2012.

[4] S.-F. Hsiaso, M.-C. Chen and C.-S. Tu, "Memoryfree low cost Designs of Advanced Encryption Standard using common sub expression elemination for Sub functions in transformations,"IEEE Transactions on Circuits and Systems, vol. 53, no. 3, pp. 615-626,March 2006.

[5] X. Zhang and K. K. Parhi, "High speed VLSI architectures for theAES algorithm,"IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 12, no. 9, pp. 957-967, September 2004.

[6] S. K. Reddy S, R. Sakthivel and P. Praneeth, "VLSI implementation of AES crypto processor for high throughput,"International Journal ofAdvanced Engineering Sciences and Technologies,vol.6, no. 1, pp.022-026, 2011.

[7] Prerna Mahajan, Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security, Vol.13, Iss. 15, Vol. 1, 2013.

[8] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing", V2.1, http://www.cloudsecurity alliance. org/ guidance/ csaguide.v2.1.pdf, retrieved on 19th November 2015.

[9] Wentao Liu, "Research on cloud computing security problem and strategy", IEEE 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), 2012, pp. 1216-1219.

[10] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07- 02. http://www.info world. com/d/security-central/gartner- seven-cloudcomputing-security-risks-853, retrieved on 6th March 2016.

[11] Deyan Chen, Hong Zhao, "Data Security and Privacy ProtectionIssues in Cloud Computing", IEEE International Conference on Computer Science and Electronics Engineering, 2012, pp 647-651.

DEVARAPALLI.PRATAPKUMAR completed his M.Tech in Bapatla engineering college during 2008-2010. Having 8 years experience as assistant professor in St.Mary's women's engineering college. His area of interest is communication and signal processing.

SHAIK.RESHMA Studying B.Tech in St.Mary's women's engineering college during 2015-2018. Having IETE membership. Her interested area is in communication.

SHAIK.AFFROZ BANU Studying B.Tech in St.Mary's women's engineering college during 2014-2018. Having IETE membership. Her interested area is in communication.

SHAIK.SAJIDA Studying B.Tech in St.Mary's women's engineering college during 2014-2018. Her interested area is radar system.

SHAIK.RESHMA Studying B.Tech in St.Mary's women's engineering college during 2014-2018. Having IETE membership. Her interested area is in communication.