ISSN 2347 - 3983
Volume 8. No. 7, July 2020
International Journal of Emerging Trends in Engineering Research
Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter158872020.pdf
https://doi.org/10.30534/ijeter/2020/158872020

FPGA Implementation of Low Power High Speed BTED Algorithm for 8 Bit Error Correction in Cryptography System

Ramesha M[1], Dankan Gowda V[2], Sridhara S.B[3], Naveena Pai G[4], Bharathi Gururaj[5]
[1] Assistant Professor, GITAM School of Technology, GITAM University, Bengaluru, India, rameshmalur037@gmail.com
[2]Assistant Professor, B.M.S. Institute of Technology and Management, Bengaluru, India, dankan.v@bmsit.in
[3] Professor, Vijaya Vittala Institute of Technology, Bengaluru, India, sridharasb1947@gmail.com
[4]Assistant Professor, Yenepoya Institute of Technology, Mangalore, India, naveenpai@yit.edu.in
[5]Assistant Professor, ACS College of Engineering, Bengaluru, India, bharathigururaj@gmail.com

ABSTRACT

There are so many Error Correction Codes (ECC) have been using since decades to rectify one bit or multiple bits errors in the memory designs. To overcome the MCUs issue, Bose–Chaudhuri–Hocquenghem (BCH), Reed-Solomon codes and Punctured Difference Set (PDS) codes have been currently employed. In these conventional codes encoding and decoding is more complicated and need extra power, additional area, and huge delay and also in case of Content Addressable Memory (CAM) inserting cannot be employed due to tight coupling in between the cells. To substantiate the MCUs, issue a single-error rectification and two-fold location of integrated current Sensors are employed. To practically correct the MCUs error the new method called Bit Transition Encoder and Decoder (BTED) scheme is employed which are two dimensional matrix codes of data size 32 bits, which divides the information into the numerous sub information's like symbols of each 4-bits. The proposed BTED algorithm is implemented on Artix-7 FPGA development board and which is comparatively less delay and power in comparison with various existing methodologies. The simulation results shows that there is 18% improvement in delay, 15% in power reduction and 67% improvement in hardware resources utilizations compared to conventional algorithms.

Key words: BTED, Error Correction Codes, Cryptography, Security Issues.

1. INTRODUCTION

In memories, errors occur and those errors are identified and rectified by different approaches like Hamming codes and self-checking methods. However these approaches are not capable of the present production requirement of precision and extreme speed memories [1]. In these approaches it's easy to identify errors but it is hard to rectify them because rectifying errors again a fault error will generate a false positive error that cannot be recognized and because of this reason, it becomes a huge issue. The system developed for figuring out the faults must assure that output codes given are not the fault codes [2]. The choice of the output data code is an extremely critical task [3]. The selected code that has high error recognition capability that can reduce fault by realizing the fault steady property; however, it includes a wide number of outputs and also more system cost. To select a code of fewer error detection capacities would encompass fewer supplementary outputs at the same time, to achieve shortcoming secureness, it may be necessary to alter the circuit structure. To obtain accurate output result the decision of the generated code can be examined by the particular circuit. Figure.1 depicts a well-known structured design of a concurrent error detection plan [4].

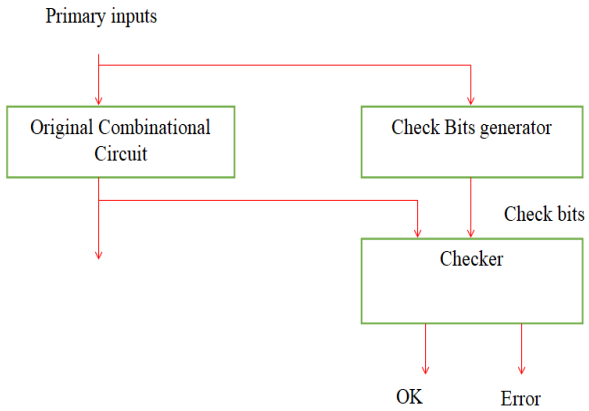

Figure 1: Architecture for concurrent error detection.

Table 1: Error Correction capability of different existing schemes

Techniques used for correction of errors	Data bit size	Redundant bits	error correction capability
DMC(Decimal Matrix Codes)	32	6	4
Matrix Code	32	8	2
Hamming Code	32	7	1

The results show that error modification capacity is increased by employing decimal matrix codes (DMC) to 4 bits. Error Correction capability of different existing schemes described in Table.1.The Hamming code occupies more area as long as cut registers and four input LUT's are compared with Matrix and Decimal Matrix Codes. However the Matrix Codes have less delay, control and occupies less area than cut registers and four inputs LUT's than the other two codes. However, it has a significant load that it rectifies only 2 bit errors [5].The DMC has a fundamental advantage that it consumes less power and has intermediate delay and area between the other two codes [6]. In the DMC, most importantly, the gap and sort out lattice are accomplished, that is the information N-bit is separated into K picture of length m-bits. The articulation can be composed as (N=K × m) where (K= K1 × K2, lines and sections). It's not important to change the physical structure of the memory to actualize the DMC [7], [8]. It can accept 32-piece of information for instance and clarify the DMC plot.

Absolute 32 bits are separated into 8 pieces of size 4 bits. From D0 to D31 are 32 data bits, check bits are 10 Horizontal (Ho-H9) and 16 vertical bits. The recognition and rectification capacity relies upon the how we pick the estimations of k and m. Exchange off happens in picking these qualities for greatest execution [9], [10]. Consequently, m and k should be carefully changed as per the enlarge review capacity and furthermore lessen the amount of overabundance bits. Right now, this circumstance, when m = 8 and k = 2×2, at that point just 1-piece issue is cured, right now tedious bits is 40[11] [12]. At the point when m = 2 and k = 4×4, at that point 2-piece flaw is helped, right now monotonous bits is 32. At the point when m = 4 and k = 2×4, at that point 5-piece deficiency is cured, right now monotonous bits is 36. The particular ultimate objective to overhaul the steadfastness of memory, the slip-up cure limit is at first considered, so k = 2 × 4 and m = 4 are utilized to create [13][14].

2. BTED ENCRYPTION AND DECRYPTION ALGORITHM

BTED algorithm is implemented in the projected BTED encryption and decryption to enhance the safety level, capability of errors location identification and their corrections. In this algorithm, the power consumed is not more than other detections approaches. It includes bitwise integer subtraction and integer addition. In the bitwise algorithm, all bits are divided into symbols of each 4bits and it has been arranged in the form of matrix for final execution. The N-bit word is defined in separate forms of m bit symbols (N = n × m). The created symbols are placed in a two-dimensional matrix of n= n1 × n2 (n1- a range of columns, n2- a range of rows). Employing decimal number addition on symbols per row the horizontal redundant bits 'H' is achieved. A binary operation on the bits per column provides vertical redundant bits 'V'. The divided symbol and arrange-matrix are represented in a logical format. Figure.2 depicts encoder module having 32-bit input and producing an output of 20-bit horizontal redundant number and 16-bit vertical redundant number.

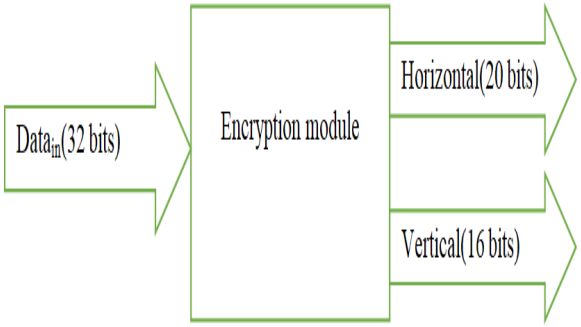

Figure 2: Proposed encryption module with 32 bits input and 20bits of horizontal and 16 bits of vertical

3. WORKING OF BTED ALGORITHM

The horizontal and vertical check bits are produced from input message bit 12345678 and this is 32-bit random number which can be the tag id. The output 2198e is a 20-bit horizontal number and 444c is the 16-bit vertical number of an encoder module as shown in Figure.2. The 32-bit word is given as input to the encoder module; it produces an output frame of 68-bit length. The frame consists of a 16-bit vertical redundant number, a 20-bit horizontal redundant number, and 32-bit input. In the BTED technique, a 32-bit word is taken as input, where data bits are characterized in cells from D0 to D31. This 32-bit word is taken as eight symbols of 4-bits each, n1= 2 and n2 = 4 are selected at the same time. Bits from H0 to H19are horizontal check bits and V0 to V15 are vertical check bits. The data is 32 bit in word (D0 to D31) and it is divided into 8 symbols and every symbol is 4 bits as exhibited below Table 2 and 3.

Table 2: Direction of horizontal, vertical check and data bits

D15	D14	D13	D12	D11	D10	D9	D8	D7	D6	D5	D4	D3	D2	D1	D0
D31	D30	D29	D28	D27	D26	D25	D24	D23	D22	D21	D20	D19	D18	D17	D16
D47	D46	D45	D44	D43	D42	D41	D40	D39	D38	D37	D36	D35	D34	D33	D32
D63	D62	D61	D60	D59	D58	D57	D56	D55	D54	D53	D52	D51	D50	D49	D48
V_{15}	V_{14}	V_{13}	V_{12}	V_{11}	V_{10}	V_9	V_8	V_7	V_6	V_5	V_4	V_3	V_2	V_1	V_0
V_{31}	V_{30}	V_{29}	V_{28}	V_{27}	V_{26}	V_{25}	V_{24}	V_{23}	V_{22}	V_{21}	V_{20}	V_{19}	V_{18}	V_{17}	V16
H15	H14	H13	H12	H11	H10	H9	H8	H7	H6	H5	H4	H3	H2	H1	H0
H31	H30	H29	H28	H27	H26	H25	H24	H23	H22	H21	H20	H19	H18	H17	H16
H39	H38	H37	H36	H35	H34	H33	H32								

Table 3: Characterization of symbols along with Data Bits

symbol 0= D_0 to D_3	symbol 1= D_7 to D_4	symbol 2= D_{11} to D_8
symbol 3= D_{15} to D_{12}	symbol 4= D_{19} to D_{16}	symbol 5= D_{23} to D_{20}
symbol 6= D_{27} to D_{24}	symbol 7= D_{31} to D_{28}	symbol 8= D_{35} to D_{32}
symbol 9= D_{39} to D_{36}	symbol 10= D_{43} to D_{40}	symbol 11= D_{47} to D_{44}
symbol 12= D_{51} to D_{48}	symbol 13= D_{55} to D_{52}	symbol 14= D_{59} to D_{56}
symbol 15= D_{63} to D_{60}	----------	----------

Bits from H_0 to H_{39} are called check bits in direction of horizontal and V_0 to V_{31} are called check bits in vertical direction. As shown in Equation (1) to (8) by decimal addition in horizontal redundant bits 'H' are obtained. Figure.3 shows proposed 32 bits BTED structure and its internal modules along with their widths.

$$H_4\ H_3\ H_2\ H_1\ H_0 = D_3\ D_2\ D_1\ D_0 + D_{11}\ D_{10}\ D_9\ D_8 \quad (1)$$
$$H_9\ H_8\ H_7\ H_6\ H_5 = D_7\ D_6\ D_5\ D_4 + D_{15}\ D_{14}\ D_{13}\ D_{12} \quad (2)$$
$$H_{14}\ H_{13}\ H_{12} H_{11}\ H_{10} = D_{19}\ D_{18}\ D_{17}\ D_{16} + D_{27}\ D_{26}\ D_{25}\ D_{24} \quad (3)$$
$$H_{19} H_{18}\ H_{17} H_{16}\ H_{15} = D_{23}\ D_{22}\ D_{21}\ D_{20} + D_{31}\ D_{30}\ D_{29}\ D_{28} \quad (4)$$
$$H_{24} H_{23}\ H_{22} H_{21}\ H_{20} = D_{43}\ D_{42}\ D_{41}\ D_{40} + D_{35}\ D_{34}\ D_{33}\ D_{32} \quad (5)$$
$$H_{29} H_{28}\ H_{27} H_{26}\ H_{25} = D_{47}\ D_{46}\ D_{45}\ D_{44} + D_{39}\ D_{38}\ D_{37}\ D_{36} \quad (6)$$
$$H_{34} H_{33}\ H_{32} H_{31}\ H_{30} = D_{59}\ D_{58}\ D_{57}\ D_{56} + D_{51}\ D_{50}\ D_{49}\ D_{48} \quad (7)$$
$$H_{39} H_{38}\ H_{37} H_{36}\ H_{35} = D_{63}\ D_{62}\ D_{61}\ D_{60} + D_{55}\ D_{54}\ D_{53}\ D_{52} \quad (8)$$

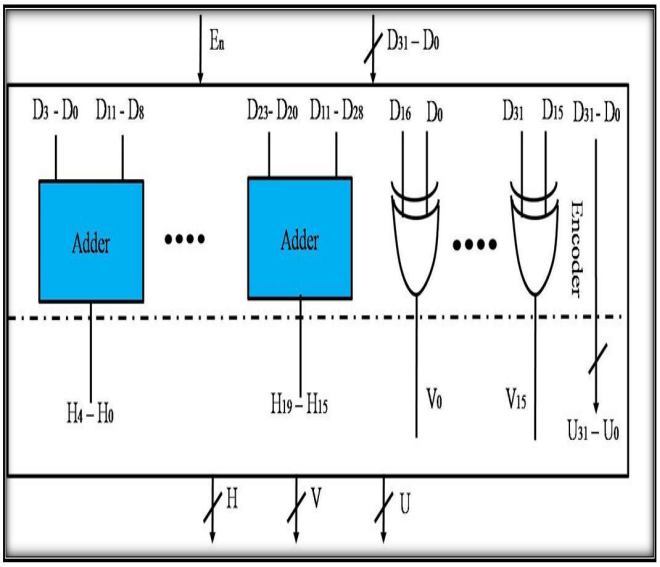

Figure 3: Proposed 32 bits BTED structure and its internal modules along with their widths

Similarly, remaining horizontal redundant bits are obtained. Here '+'represents bitwise integer addition. The vertical redundant bits 'V' may be obtained from XOR operation as given below in the table 4:

Table 4: Vertical redundant bits 'V' obtained from XOR Operation

$V_0=D_0\oplus D_{32}$	$V_1=D_1\oplus D_{33}$	$V_2=D_2\oplus D_{34}$	$V_3=D_3\oplus D_{35}$
$V_4=D_4\oplus D_{36}$	$V_5=D_5\oplus D_{37}$	$V_6=D_6\oplus D_{38}$	$V_7=D_7\oplus D_{39}$
$V_8=D_8\oplus D_{40}$	$V_9=D_9\oplus D_{41}$	$V_{10}=D_{10}\oplus D_{42}$	$V_{11}=D_{11}\oplus D_{43}$
$V_{12}=D_{12}\oplus D_{44}$	$V_{13}=D_{13}\oplus D_{45}$	$V_{14}=D_{14}\oplus D_{46}$	$V_{15}=D_{15}\oplus D_{47}$
$V_{16}=D_{16}\oplus D_{48}$	$V_{17}=D_{17}\oplus D_{49}$	$V_{18}=D_{18}\oplus D_{50}$	$V_{19}=D_{19}\oplus D_{51}$
$V_{20}=D_{20}\oplus D_{52}$	$V_{21}=D_{21}\oplus D_{53}$	$V_{22}=D_{22}\oplus D_{54}$	$V_{23}=D_{23}\oplus D_{55}$
$V_{24}=D_{24}\oplus D_{56}$	$V_{25}=D_{25}\oplus D_{57}$	$V_{26}=D_{26}\oplus D_{58}$	$V_{27}=D_{27}\oplus D_{59}$
$V_{28}=D_{28}\oplus D_{60}$	$V_{29}=D_{29}\oplus D_{61}$	$V_{30}=D_{30}\oplus D_{62}$	$V_{31}=D_{31}\oplus D_{63}$

The encoding is performed via decimal and binary addition operations. The encryption calculates the discharged bits employing XOR gates and multi-bit adders. The horizontal redundant bits are H19-H0 and vertical bits are represented as V31-V0. Data bits are directly taken from D63 to D0.

4. RESULTS AND DISCUSSION

The proposed work is intended and established for hardware prototype module having low power, low area and reduced delay employing ECC, BTED encryption and decryption by point addition and point doubling to produce 256 points to form S-Box. The advanced prototype module comprises 256 points key generation, read-only storage memory creation; BTED encryption and decryption possesses lessor amount of hardware resources. The point on the ECC curve is the 32bits data "d" which is applied for BTED encryption, which employs integer addition between various symbols to obtain

encryption output. BTED encryption specifies 20 bits horizontal bits and 16 bits vertical bits and these 2 bits information is for error bit detection in decryption sections.

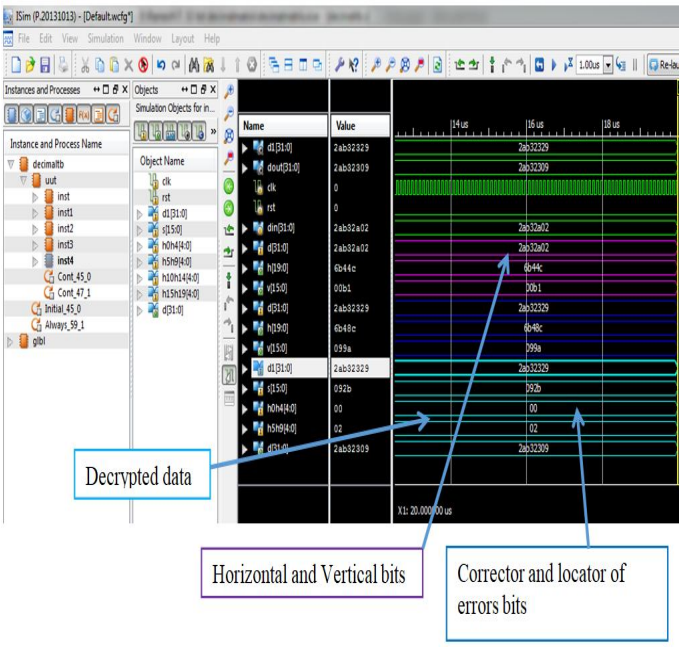

Figure 4: BTED Decryption output in Vivado Xilinx Ism simulator

The simulation result of BTED Decryption output on Vivado Xilinx Ism simulator as shown in Figure.4. Here the vertical bits of the encryption module is given as input to decryption module which contains the same integer operation to obtain 16 bits conditional bits for identification of error bit at the error locator. The‘s’ symbolized in the Figure.4 is the syndrome bits which is obtained by performing XOR operation between ‘v’ and ‘vd’ as depicted in Figure.4. The horizontal bits of encryption unit are given as input to decryption module which performs the same integer operation to obtain 16 bits conditional bits for identification of error bit at error locator. In the Figure.4 the condition bits are indicated by ‘h’ which is obtained by performing XOR operation between ‘h’ and ‘hd’ and is indicated in Figure.4. The ‘v’ and ‘h’ are inputs to the error locator and error detector modules and it illustrates the outputs of encryption and decryption. There are several other parameters are taken to considerations for comparison purpose namely total power, delay and device utilization summary are indicated in the Table 5 for different ECC’s. This proposed research work has satisfactory performance in terms of power and speed compared to other ECC’s.

Table 5: Power, slices registers, slice FF’s, LUT’s and delay Comparison summary of the proposed techniques

Type of ECC used	Slice Registers	Slice flip flops	LUTs	Bounded I/O	Delay(ns)	Power Utilization
Proposed work	1628	637	934	44	27.190	0.086W
Punctured distinction set (PDS) codes [1]	2391	926	982	NA	76.23	221.1mW
Decimal Matrix Codes [2]	2093	784	1932	NA	45.89	10.8mW
Matrix Codes [3]	1782	1027	1027	NA	70.1	24.7mW
Matrix Code [4]	3291	2081	4581	96	140.548	0.121W
Hamming code	7621	3201	2682	84	170.133	0.163W

5. CONCLUSION

In the proposed research work, the projected processor for a generation of S-Box and its encryption and decryption has been discussed. Various techniques have been adopted in the design of the processor to minimize the power consumption, area and also to enhance the speed. The bit transition encryption and decryption has also been discussed. The Encoder re-use approach reduces the area overhead of additional circuits. Simulation and synthesis outcomes exhibit that Bitwise Matrix Code requires 0.1mW of power and has a delay of about 3.109ns and the area utilization is reduced by 45%. The design is tested and demonstrated on Artix-7 FPGA prototype boards.

Simulation and synthesis shows that the projected base band-processor can complete it’s fruitfully with a power consumption of about 5mW on 1.2V supply. In this proposed work a method for mapping any alphanumerical characters and any type of data for error correction is done by employing a non- singular matrix is showed. The mapping focuses are disorganized and decoded by employing the ECC approach and displays in Read Only Memory.

REFERENCES

1. Arunkumar, S.S. Tyagi, Manisha Rana, Neha Aggarwal, Pawan Bhadana, Manav Rachna, **A Comparative Study of Public Key Cryptosystem based on ECC and RSA.** *International Journal on Computer Science and Engineering (IJCSE),* ISSN: 0975-3397, Vol. 3 No. 5 May 2011, pp-1904-1909.
2. O. Srinivasa Rao, **Efficient Mapping Methods for Elliptic Curve Cryptosystems**, *International Journal of Engineering Science and Technology*, Vol. 2(8), 2010, ISSN: 0975-5462, 3651-3656.
3. C. Wang, M. Daneshmand, M. Dohler, X. Mao, R. Q. Hu and H. Wang, **Guest Editorial - Special**

Issue on Internet of Things (IoT): Architecture, Protocols and Services. *IEEE Sensors Journal*, vol. 13, issue. 10, pp. 3505–3510. https://doi.org/10.1109/JSEN.2013.2274906

4. S.Raza, **Secure communication for the Internet of Things - a comparison of link-layer security and IP sec for 6LoWPAN**, *Security and Communication Networks*, vol. 7, no. 12, pp. 2654–2668. https://doi.org/10.1002/sec.406
5. Gonzalez G. Organero M, Kloos C. **Early in infrastructure of all Internet of Things in space for learning**, *8th IEEE International Conference on Advance Learning Technologies*, pp-381-383.
6. Dankan V Gowda, Ramachandra A C, Thippeswamy M N, Pandurangappa C, Ramesh Naidu P ,**Synthesis and Modelling of Antilock Braking System using Sliding Mode Controller**, Journal of Advanced Research in Dynamical and Control Systems', Vol 10(12),Pages:208-221.
7. Dankan V Gowda, Ramachandra A C, Thippeswamy M N, Pandurangappa C, Ramesh Naidu P, **Modeling and Performance Evaluation of Anti-lock Braking System,** Journal of Engineering Science and Technology, Taylor's University, Vol 14(5), Pages: 3028-3045.
8. Kishore, D.V., Gowda, D.V., Shivashankar, Mehta, S.: **MANET topology for disaster management using wireless sensor network**. *International Conference on Communication and Signal Processing*, April 6–8, 2016, India. https://doi.org/10.1109/ICCSP.2016.7754242
9. Dankan V Gowda, D. V. Kishore, Shivashankar, A. C.Ramachandra, and C. Pandurangappa, **Optimization of motorcycle pitch with non linear control**, in Proceedings of the *1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology* (RTEICT '16), pp. 1656–1660, Bangalore, India, May 2016.
10. Ramesha, M. & Ramana, T. **Performance analysis of fbmc transceiver architecture over OFDM system.** *Far East Journal of Electronics and Communications.*17.1353-1372.10.17654/EC017061353.
11. Ramesha, M. & Ramana, T, **A Novel Architecture of FBMC Transmitter using Polyphase Filtering and its FPGA Implementation**. *Indian Journal of Science and Technology*. 9.10.17485/ijst/2016/v9i48/94148.
12. Trinidad, Emmanuel. (2019). **Juxtaposition of Extant TV White Space Technologies for Long-Range Opportunistic Wireless Communications.** *International Journal of Emerging Trends in Engineering Research*.7. 209-215. 10.30534/ijeter/2019/17782019.
13. B, Sridhara & M, Ramesha & Patil, Veeresh. **Adaptive Scheduling Design for Time Slotted Channel Hopping Enabled Mobile Adhoc Network.** *International Journal of Advanced Computer Science and Applications*.11. 10.14569/IJACSA.2020.0110333.
14. Lakshmi, Boggula. (2019). **Energy Efficient Routing Mechanism for Harsh Environment in Wireless Sensor Networks**. *International Journal of Emerging Trends in Engineering Research*. 234-238. 10.30534/ijeter/2019/04792019.