ISSN 2278-3091
Volume 9, No.4, July – August 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse27942020.pdf
https://doi.org/10.30534/ijatcse/2020/27942020

Design and Development of Low Power BTED Cryptography Algorithm on FPGA

Ramesha M [1], Sridhara S.B [2], Anne Gowda A B [3], Anughna N [4], Bharathi Gururaj [5]
[1] Assistant Professor, GITAM School of Technology, GITAM University, Bengaluru, India, rameshmalur037@gmail.com
[2] Professor, Vijaya Vittala Institute of Technology, Bengaluru, India, sridharasb1947@gmail.com
[3] Assistant Professor, GITAM School of Technology, GITAM University, Bengaluru, India, annegowda.ece@gmail.com
[4]Resarch Scholar, GITAM School of Technology, GITAM University, Bengaluru, India, anughna.7@gmail.com
[5]Assistant Professor, ACS College of Engineering, Bengaluru, India, bharathigururaj@gmail.com

ABSTRACT

The Complementary Metal Oxide Semiconductor technology has reduced to Nano-Size which is acceptable to build larger number of transistors on single IC. Integration of electronics modules on a single chip has been increasing rapidly and also proportional rate of errors in memory designs also enhanced due to ionizing effects from the atmosphere. In all the memory designs, the main challenging task is the identification of single bit error correction and Multiple Bit Upsets (MCUs) have turned into a major issue compare to single-bit error location and correction. To avoid the Multiple Bit Upsets issue a two-fold location integrated sensors are deployed in Integrated Chips. In real time applications to correct MCUs error the novel Bit Transition Encoder and Decoder (BTED) scheme is used. This technique contains a matrix code of two dimensional which having a data size of 32 bits. These 32 bits are again divided into sub information symbols of size 4 bits each. The proposed technique is analyzed and implemented on a hardware platform like Artix-7 FPGA development board. Finally comparisons are made with various existing methodologies by considering parameters like area, power, delay and some other parameters.

Key words: Cryptography, Decoder, Encoder, FPGA, Security

1. INTRODUCTION

In the recent days data encryption and decryption becoming major concern for the transmission process and storage in memory devices. Whenever developing the memory devices on a single chip is challenging task. The proportion of increasing the data leads to more errors in a memory design [1]. To reduce the error associated with respect to memory devices on a single integrated chip various error correction coding techniques are used. The commonly used techniques are Decimal Matrix Codes, Matrix Code and Hamming Codes etc. [2]. These codes having their own error correction capability, redundant bit and maximum data bit size associated with respect each technique. The Decimal Matrix Codes having a 4-bit error correction capability, length of 6-bit redundant bit size and maximum data bit of length 32-bits. Similarly, hamming code having a 1-bit error correction capability, length of 7-bit redundant bit size and maximum data bit of length 32-bits [3].Developing an efficient error correction capability algorithm with more efficient, high security, and low power is the major concern associated with the Bit Transition Encoder and Decoder (BTED) algorithm. This BTED technique is a novel method to address the issues like security and hacking related to data [4]. A synchronous key is generated by utilizing duplication which includes point multiplying and point expansion mechanism. Figure 1 shows the architecture for the error correction mechanism associated with the BTED scheme.

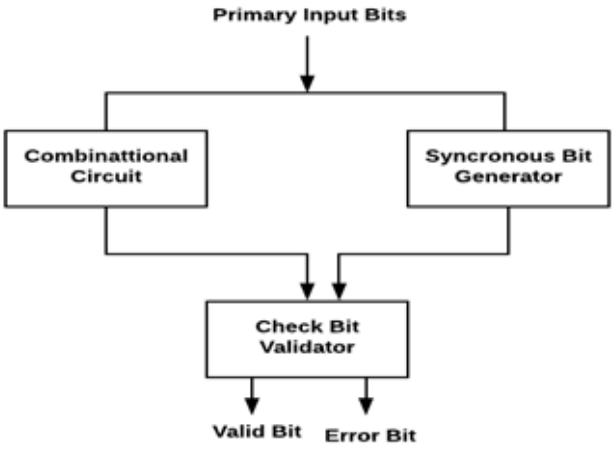

Figure 1: Architecture for BTED error detection mechanism

2. PROPOSED METHODOLOGY

In the advanced encryption standard (AES) algorithm, encrypted and decrypted bits are of length 128,192 and 256 bits for 8, 10, 12 round operations respectively. In this algorithm the secret message is of length 128 bits and it is denoted as N_k-8.The byte substitution, shift rows, add round key and Mix columns process is based on 4 byte substitutions and it is divided into 4x4 arrays such as 16 bytes. Each byte value is retrieved by subsequent S-Box values, which is generated via elliptic-curve cryptography (ECC) mechanism [5]. Further, S-Box is encrypted and decrypted by the usage of Bit Transition Encoder and Decoder (BTED) for enhanced security [6]. The substitution of s-box can be formed by employing simply two arithmetic operations which includes addition and doubling to minimize the FPGA hardware resources and for faster operations of encryption and decryption [7].

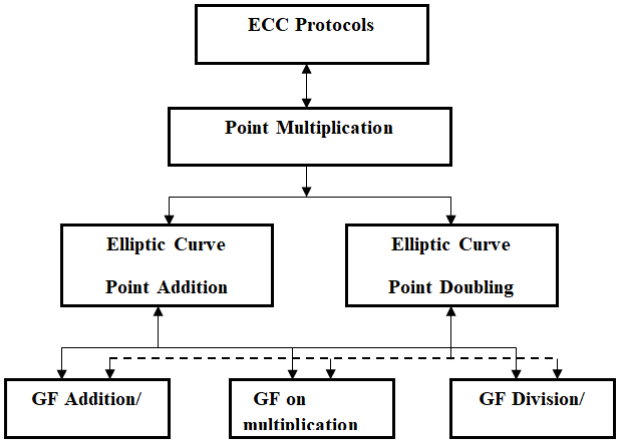

Figure 2: The hierarchical demonstration of elliptic-curve cryptography (ECC)

Figure 2 shows the hierarchical demonstration of ECC and the communication between the various levels concerned on it. The computations necessary for ECC are mainly divided into 3 levels: the topmost level deals with the code protocols like Elliptic Curve Digital Signature Algorithm (ECDSA) and Elliptic-curve Diffie–Hellman (ECDH) key agreement protocol etc. [8][9]. The second level deals with elliptic curve scalar multiplication(SM), where SM is a combination of 2 alternative operations: Point Addition (PA) and Point Doubling (PD), the last level or base level deals with the sector operations of the ECC [10],[11].These operations are executed over finite fields. The common sector operations are field addition, field subtraction and field division/inversion. One explicit importance for cryptography is referred to as elliptic group mod p, where p is a prime number. This is defined as given in equation (1)

$$4a^3+27b^2 \pmod p \neq 0 \quad (1)$$

Where 'a' and 'b' are two non-negative integers which are considered as, a=1, b=1 and p=563.Then $E_p(a, b)$ indicates the elliptic group mod p whose elements (x, y) are pairs of non-negative integers which are considered as less than p, as given in equation. (2)

$$y^2=[x^3+ax+b] \pmod p \quad (2)$$

The above equation (2) is separated into LHS and RHS to find the initial point on the elliptic curve.

$$LHS= y^2 \bmod p \quad (3)$$

$$RHS=[x^3+ax+b] \pmod p = [x^3+x+1] \pmod p \quad (4)$$

Figure 3 shows the proposed 32 bits BTED structure and its internal modules along with their widths. The decoder is composed of various sub-blocks where every block performs their functions such as error calculative block, error locating block and error-correcting block. From the Figure 3, it is indicated that the redundant bits are recomposed from the received data (D) bits and to obtain the syndrome bits H and S data bits are compared with the initial bits. These bits are used to identify errors and corrected by inverting the errors bits last. The syndrome bits are obtained from the output of the reused BTED encryption, without altering the entire system. By employing the reuse technique, the area of chip can be reduced. The enable signal En is employed to differentiate the read and write operation of the memories. Only when necessary these bits are enabled, therefore depending on these criteria, we can say that area of additional bits are reduced and thus provides higher performance when compared to others.

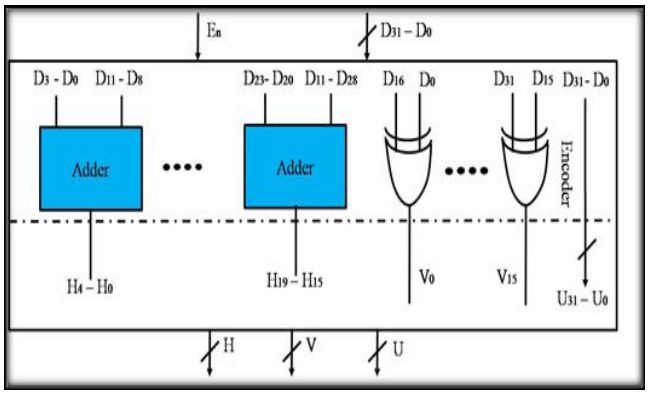

Figure 3: Proposed 32 bits BTED structure and its internal modules along with their widths

The BTED decoder employed in the configuration is represented in Figure.4 which contains a disarray mini-computer, an error locator and an error corrector. Every module can be sort out by using the same process. The extra bits that are obtained from the data bits 'D' are compared with each other and the first arrangement of recurring bits is to obtain the error bits ΔH and S. The error locator employs ΔH and S to differentiate and realize the error bits. At last, the error corrector adjusts the error bits by remodeling the estimations of error bits. The 'En' flag is employed for guaranteeing encoder as a part of the decoder.

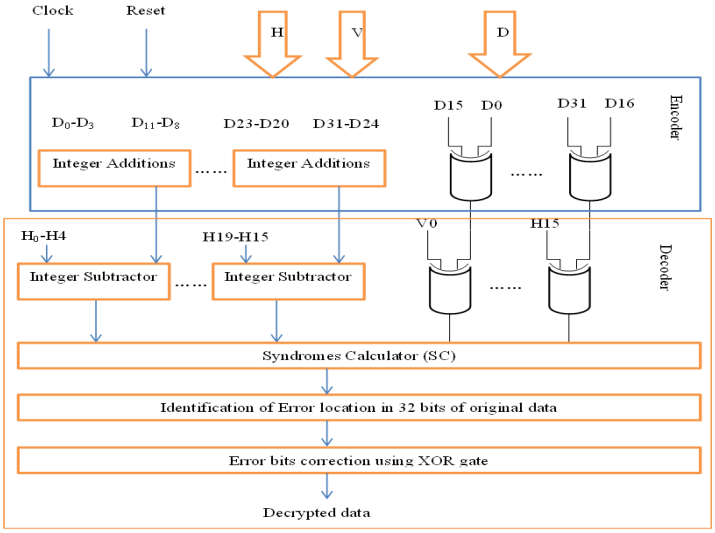

Figure 4: Proposed BTED Decryption block diagram and its internal modules and their routings

3. RESULTS AND DISCUSSION

The Register Transistor Logic (RTL) diagram for BTED error correction and decryption low power for 8-bit architecture module as indicated in Figure.5. The projected design is verified in Cadence 180nm technology for evaluation of actual power consumption which is the sum of dynamic and static power. The 20 bits of horizontal and 16 bits vertical encrypted data which are obtained from integer addition and XOR operation are employed in the decryption phase as check bits. These check bits are useful for integer addition and XOR operation and also for the generation of various codes in syndrome symbols, for every 5 bits. The BTED algorithm by employing the error surveyor module, the error bit will be recognized in each symbol. The corrupted bits are corrected by employing XOR operation between horizontal, vertical and symbol bits and its corresponding equation is given below.

$$D_{correct} = D_{[i]} \oplus S_{[i]} \quad (5)$$

Where 'i' is the integer number it varies from 0 to 4.

Since the input data size is of 32 bits the equation (5) will be utilized for 8 times and it contains x, y, and secrete character. Therefore 32/4 bits provides 8 symbols and every symbol is of length 5 bits. The final stage is decryption and the arrangement of Elliptic-Curve Cryptography (ECC) point which as x, y and secrete character. The proposed work is described using Verilog HDL code and implemented on Artix-7 FPGA board. The input output signal conditions are verified using Chip scope pro analyzer tool and it is the integrated part of Vivado Xilinx 2018.1 ISE tool. The entire work is tested in the Cadence package tool of 180nm technology to obtain the overall power analysis. The overall power analysis is the sum of static and dynamic power. By employing the RC encounter in the Cadence tool, the chip-level design and RTL diagram for each phase is obtained and it is depicted in Figure 5.

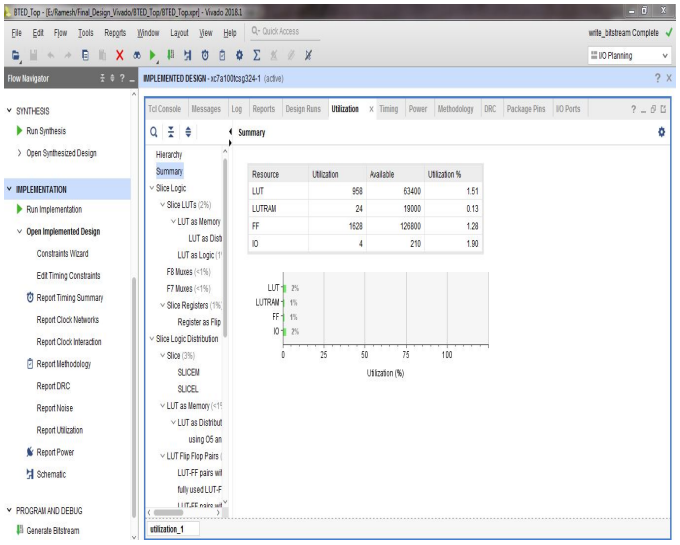

Figure 5: Hardware utilizations in terms slices registers, slice FF's, LUT's and delay summary of the proposed techniques.

The design approach is depicted in Figure.5 which describes the stages executed towards realizing the objectives of the analysis. The performance of the digital encryption and decryption architecture is achieved by the derivation of Verilog HDL-code based on Error Correction Codes (ECC) and Bit Transition Encoder and Decoder (BTED) systems. The experimentation of the Verilog HDL is done by employing Vivado Xilinx 2018.development tools. Table1 shows the Error Correction Capability and Coding efficiency of different ECC's. From the Table1 it is concluded that the proposed method has better Error correction capability and coding efficiency compared to Matrix code and Hamming code.

Table 1: Performance comparison for different error correction codes

Type Of Code Used	Slice Register	Slice Flip Flops	Flip flop pair	Area in Vivado Xilinx	Area in cadence	Delay	Dynamic power in Vivado Xilinx	Total power in cadence
BTED	34	34	166	NA	8589	5.74	1.43	1.43
Matrix Code	164	32	291	77933.7	NA	7.1	24.7	NA
Hamming Code	1350	32	2682	58409.4	NA	6.7	20.5	NA

4. CONCLUSION

The obtained results illustrate that the mapping approach keeps away from the errors obtained in the memory devices regularity in the resultant disorganized data that is modified from the plaintext grid and consequently enhances the difficulty of decoding by considering intruder it would be extremely difficult to build on which it focuses the alphanumerical characters are mapped. It is thus systematic that the proposed mapping approach can enhance the framework, ensuring the confidentiality of messages and provides superior performance in such a manner. The projected BTED is compared with absolutely understood codes. For example, the current Hamming, Matrix Codes, and punctured distinction set (PDS) codes.

The obtained outcomes illustrate that the interim to disappointment mean time to failure (MTTF) of the projected scheme obtained as for all the ECC codes are 452.9, 154.6 and 122.6 percentage of Hamming, MC, and PDS respectively. In the meantime, the accepted overhead of the projected scheme obtained as for all the ECC codes are 73.1, 69.0 and 26.2 percentage of Hamming, Matrix Codes, and punctured distinction set (PDS) codes, on an individual basis. The foremost disadvantage of the projected design is that it requires a lot of repetitive bits for memory assurance.

REFERENCES

1. R. Naseer and J. Draper, **Parallel double error correcting code design to mitigate multi-bit upsets in SRAMs**, *ESSCIRC 2008 - 34th European Solid-State Circuits Conference*, Edinburgh, 2008, pp. 222-225. https://doi.org/10.1109/ESSCIRC.2008.4681832
2. Juan Antonio Maestro, Pedro Reviriego, Sanghyeon Baeg, Shijie Wen, Richard Wong (2013), **Soft error tolerant Content Addressable Memories (CAMs) using error detection code and duplication**, *Microprocessors and Microsystems* 37 (2013) 1103–1107. https://doi.org/10.1016/j.micpro.2013.10.003
3. G. Neuberger, F. G. de Lima Kastensmidt and R. Reis, **An automatic technique for optimizing Reed-Solomon codes to improve fault tolerance in memories**, in *IEEE Design & Test of Computers*, vol. 22, no. 1, pp. 50-58, Jan.-Feb. 2005. https://doi.org/10.1109/MDT.2005.2
4. Sanghyeon Baeg, Pedro Reviriego, Juan Antonio Maestro, Shijie and Richard Wong (2011), **Analysis of a Multiple Cell Upset Failure Model for Memories**. *ACM Transactions on Design Automation of Electronic Systems*, Vol. 16, No. 4, Article 45, 1084-4309.
5. Costas Argyrides, StephaniaLoizidou and Dhiraj K. Pradhan (2008), **Area Reliability Trade – Off in Improved Reed Muller Coding, *SAMOS 2008***, *LNCS 5114, 2008 Sp*ringer – Verlag Berlin Heidelber, pp. 116-125. https://doi.org/10.1007/978-3-540-70550-5_13
6. Ramesha, M. & Ramana, T.. (2016). **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.
7. 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.
8. 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.
9. 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.
10. V, Murugan. **High Security Distributed MANETs using Channel De-noiser and Multi-Mobile-Rate Synthesizer**. *International Journal of Advanced Trends in Computer Science and Engineering*. 9. 1346-1351. 10.30534/ijatcse/2020/68922020.
11. D.Y.C., Liew. **Developing Composite Indicators for Flood Vulnerability Assessment: Effect of Weight and Aggregation Techniques**. *International Journal of Advanced Trends in Computer Science and Engineering*. 8. 383-392. 10.30534/ijatcse/2019/08832019.