International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

AN EFFICIENT 2- BIT ERROR COMPENSATION WITH SIDE CHANNEL SECURITY

Dr. R. Latha, E. Suruthi
K. Divya, R. Nithisha , R. Sangeetha, B. Subalakshmi
K.S.K College of Engineering And Technology,Kumbakonam-612 702

ABTRACT
Present energy economical error management code MBRBEC that's capable of correcting any style of error patterns as well as random mistake burst mistake and combination of random and burst errors that count up to 5 and at the equal time avoids disturbance. The planned MBRBEC encoder uses SEC–DED extended Hamming code (39 ,32) to cipher the initial message bits. Triplication mistake alteration theme is one among the quality mistake correction schemes employed in communication scheme to correct errors tend to propose. Triplication mistake alteration theme to accurate the mistake in on chip interconnection link. Victimization triplication mistake alteration theme each of the encoded communication bit is triplicate. Therefore if the initial SEC–DED extended performing code is n l wherever n is that the encoded communication and l is that the original message then the ultimate variety of bits within the triplication communication is 3n. This system support side channel security at time encoding & decoding process. Once encoded that result is forwarded to decode section here the data's are spitted as original, parity bit and to check error correction. As result we get original encoded data as output using Hamming code Algorithm.

Keywords - MBRBEC,SEC DED, Triplication Process

INTRODUCTION

A resource-efficient and side-channel secure Ring-LWE cryptographic processor is presented. A discrete Gaussian sampler with constant response time, high precision, and large distribution tails is designed. The Gaussian sampler is proven to be secure against side-channel timing attack according to the timing analysis attack results on a FPGA-based testing platform. A universal module MPE (Modular Processing Element) is designed to carry out all basic modular operations for Ring-LWE cryptography. With the shrinking feature size and increasing die size integration of large number of functional blocks storage elements and intellectual property IP in a single chip increases. As the number of functional blocks in a single chip increases the bus based communication becomes inefficient in a system-on-chip soc networks-on-chip NOC is a paradigm that provides solution to the communication problem in a SOC. in NOC the functional n blocks communicate through routers. Routers are interconnected using interconnection wires. In nano scale technology due to scaling of supply voltage increasing interconnect density and faster clock rates on chip interconnect wires suffer from three major problems.

They are:

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

(i) Delay;
(ii) Power consumption; and
(iii) Reliability.

The delay problem is due to capacitive coupling and is called capacitive crosstalk. While the gate delay reduces with scaling the global interconnection wire delay increases. Due to high parasitic capacitance and coupling capacitance power consumption is increased.

Moreover around 20–36% of the entire system power is consumed by interconnection network in several NoCs. Because of deep submicron noises DSM like transient mistake and magnetic attraction interference on chip interconnect wires area unit additional prone to discretional and rupture mistake. These mistakes have an effect on the consistency of the interconnection wires. The likelihood of adjacent multi wire fracture mistake error is far on top of the likelihood of multiple discretional multi wire discretional mistake. Thus finding and alteration of discretional yet as fracture mistake is very important to extend the consistency of the intelligence officer interconnect. So to possess an honest act within the style of on chip interconnection network delay power and dependability area unit the 3 major problems to be addressed.

Authority decrease method is planned at totally different levels of the look hierarchy from recursive point and scheme point to layout point and circuit point. The dominant supply of authority indulgence but is because of the electrical phenomenon current referred to as electrical phenomenon power and is given by:

$$\mathbf{P = \tfrac{1}{2}\, C_L V_{dd}^2 E(sw) f_{clk}}$$

where, P is the capacitive power dissipation
C_L is the physical capacitance at the output of the node
V_{dd} is the supply voltage
f_{clk} is the clock frequency and
E(sw) is the average number of output transitions per $1/f_{clk}$ time

In this proposed system, side channel Security and 2- bit inaccuracy compensation of SEC-DED. Hamming code algorithmic program the minimum acting distance of the SEC-DED extended acting code is four. The triplication of the encoded communication will increase the minimum acting space to twelve. Within the receiver facet only and 2 bit is detected and corrected. Most peoples understand equivalence bits. Parity is a further zero or one connected to a store unit or larger block of knowledge to help discover if misreckoning has occurred. For example with constant parity each store unit at the aspect of its parity will contain a decent vary of 1s. If the pc memory unit itself contains associate in nursing odd vary of one's then the parity is on the brink of one to make the complete vary even. Or else the parity is on the brink of zero. Clearly if anyone of the bits gets turn over the number of1s square measure progressing to be odd which we'll verify that the pc recollection unit contains misreckoning. There unit one or 2 of problems with parity bits. Initial if multiple errors occur at intervals a similar store unit our substantiation will not come back misreckoning. Jointly all the parity bits will do is check if misreckoning has occurred. It's no due to verify that bit is inaccurate so it isn't achievable to accurate the mistake. This system protects data bit from vulnerability using encoder and decoder method which was available in above mentioned algorithm.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

PROPOSED SYSTEM

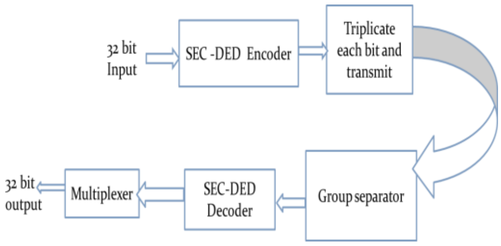


Fig:Block diagram

METHODOLOGY

1. Hamming code algorithm

Hamming code algorithm General algorithm for hamming code- is as follows:

K parity bits are added to an n-bit data word, forming a code word of n+k bits. The bit positions are numbered in sequence from 1 to n+k. Those positions are numbered with powers of two, reserved for the parity bits and the remaining bits are the data bits. Parity bits are calculated by XOR operation of some combination of data bits. Combination of data bits are shown below following the rule

Bit pos	1	2	3	4	5	6	7	8	9	10	11	12	13	..(n+k)
Parity	P1	P2	D1	P4	D2	D3	D4	P8	D5	D6	D7	D8	D9	...
P1	⊕		⊕		⊕		⊕		⊕		⊕		⊕	
P2		⊕	⊕			⊕	⊕			⊕	⊕			⊕
P4				⊕	⊕	⊕	⊕					⊕	⊕	⊕
P8								⊕	⊕	⊕	⊕	⊕	⊕	⊕
..k														

Fig: calculation of parity bit

P1 = XOR of bit positions (1, 3, 5, 7, 9, 11, 13...)
P2 = XOR of bit positions (2, 3, 6, 7, 10, 11...)
P4 = XOR of bit positions (4, 5, 6, 7, 13....)
P8 = XOR of bit position (8, 9, 10, 11, 12, 13...)
5. To examine for the error, check all parity bits by the checker bit.
C1= XOR of bit position (1, 3, 5, 7, 9, 11, 13...)
C2 = XOR of bit position (2, 3, 6, 7, 10, 11...)
C4 = XOR of bit position (4, 5, 6, 7, 13....)
C8= XOR of bit position (8, 9, 10, 11, 12, 13...)

Parity Bit with truth table

The goal of the hamming codes is to create a gaggle of bits that overlap such a single-bit error (the bit is logically flipped in value) throughout a data bit or a check bit is detected and corrected. whereas multiple overlaps is created, the technique is bestowed in hamming codes.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

Bit #	1	2	3	4	5	6	7
Transmitted bit	p_1	p_2	d_1	p_3	d_2	d_3	d_4
p_1	Yes	No	Yes	No	Yes	No	Yes
p_2	No	Yes	Yes	No	No	Yes	Yes
p_3	No	No	No	Yes	Yes	Yes	Yes

This table describes that parity bits cowl that transmitted bits among the encoded word. for example, p2 provides an honest parity for bits a combine of, 3, 6, and 7. It in addition details that transmitted bit is roofed by that parity bit by reading the column. for example, d1is coated by p1 and p2 but not p3 This table will have a dangling likeness to the parity-check matrix (H) among subsequent section.

	d_1	d_2	d_3	d_4
p_1	Yes	Yes	No	Yes
p_2	Yes	No	Yes	Yes
p_3	No	Yes	Yes	Yes

Furthermore, if the parity columns at intervals the on prime of table were removed then similitude to rows one, 2, and 4 of the code generator matrix (G) below are going to be evident. So, by choosing the bit coverage properly, all errors with a playing distance of 1 is also detected and corrected, that's that the aim of using a playing code.

Calculation Of Parity Bit From Data Expression

Input Data Word									Output Parity bits			
Bit No.	1	2	3	4	5	6	7	8	Bit No.	1	2	3
Data Word 1	1	1	0	0	0	1	0	0	Parity Bit	0	0	1
Data Word 2	0	0	1	1	1	0	1	1	Parity Bit	1	1	1
Data Word 3	0	1	0	1	0	0	0	1	Parity Bit	0	1	1

Table1

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

2. Encoder

Data word is useful as an input in the encoder circuit which performs XOR operations on the given data word and thus the essential parity bits are produce from the parity generator. Parity bits and data bits together form the code word. An encoder circuit of hamming code for 4 bit data word is shown below. Following this circuit pattern we can design an encoder circuit of hamming code for 8bit data word and realized it by means of tanner EDA tools.

Calculation Of Checker Bit After Code Expression

	Input Code Word												Checker Bit				
Bit No.	1	2	3	4	5	6	7	8	9	10	11	12		C1	C2	C3	C4
	0	0	1	1	1	0	0	1	0	1	0	0		0	0	0	0
	1	1	0	1	1	1	1	1	1	0	1	1		0	1	0	1
	0	1	0	1	1	1	1	1	0	0	0	1		0	1	1	0
	1	1	1	1	0	0	0	0	1	0	1	0		0	1	1	0

Table 2

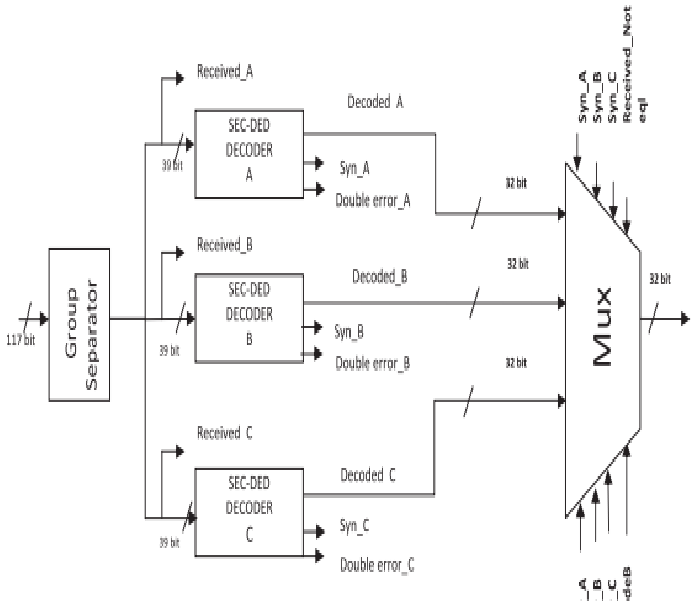
3. Decoder

In the decoder circuit code word is apply as input then check bits are produce by the checker bit generator to check the parity bits. These check bits locate the error in the code word by means of decoder circuit. The output of decoder enables a demultiplexer which is related to the input code word's. If no error occurs then the select line of demultiplexer flows the input form line i_0 and the i_1 is set to logic 1. So from the logic Nor-gate we can obtain the data. Now if an error occurs then the select line of the demultiplexer flows the code word from line i_1 and i_0 is set to logic 0. Thus inverting the bits the error bit is corrected and thus we can obtain the error free data. A decoder circuit of hamming code for 4 bit data word is also shown below

4. Multi Bit Random and Burst Error Correction code with crosstalk avoidance (MBRBEC)

The projected MBRBEC error correction code uses customary triplication error correction theme to avoid disturbance. Playacting single error correction-double error detection SEC-DED code is combined with triplication error correction theme to correct all error patterns up to 5 bits exploitation easy coding logic. The encoder and therefore the decoder diagram for the projected MBRBEC error correction code square measure figure five severally. The thirty two bit knowledge is encoded exploitation SEC-DED encoder and is triplicate. The triplicate information is transmitted. at the receiver the data bits unit of measurement received and separated into three groups. each cluster is decoded exploitation SCE-DED decoder to look out the errors. Based on data cryptography theory, the minimum playing distance of k will correct bðk 1Þ=2c errors. Therefore, MBRBEC code will correct up to 5 errors. The diagram of the projected MBRBEC encoder is shown in Fig. and also the flow sheet is shown in Fig.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019



4 or 5, the place of prevalence of errors in each the decoders are going to be same.

Design of the proposed MBRBEC decoder

The planned MBRBEC decoder utilizes the very fact that SEC–DED decoder corrects single error and detects double errors. SEC–DED decoder typically detects four errors if the syndrome price isn't zero.

If the prevalence of 4 errors produces syndrome price as zero, then SEC–DED decoder won't observe four errors. The entire diagram of the planned decoder is shown in Fig.. The received bits ar sorted as blood group, type B| and cluster C in group apparatus. The cluster apparatus could be a easy wired affiliation that separates the received bits into 3 teams (Received_A, Received_B, and Received_C) as shown.
The 3 received teams area unit given to the 3 SEC–DED decoders that cipher the syndrome values Syn_A, Syn_B, Syn_C and prevalence of double errors Double error_A, Double error_B, and Double error_C for the 3 teams. Supported the syndrome price, every SEC–DED decoder corrects the prevalence of single error and detects the prevalence of the double errors in every cluster. The decoded values (output from 3 decoders) Decoded_A, Decoded_B, and Decoded_C area unit given to the electronic device. The 3 received teams Received_A, Received_B, Received_C, and Decoded_A, Decoded_B area unit compared within the comparator as shown in Fig. 2b to get the signals Received_Not_eql and DecodeA_eql_DecodeB. Received_Not_eql signal are going to be ‘1’ if all the 3 teams FFarea unit totally different. J

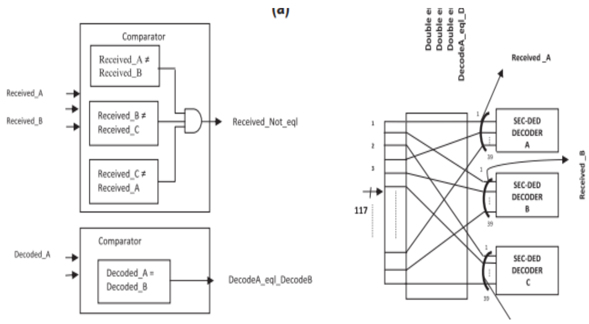
DecodeA_eql_DecodeB signal are going to be ‘1’ if decoded output from decoder A is adequate to decoded output from decoder B (if each the decoders have zero error or single error). The do able distribution of one, 2, 3, 4, and five bit errors among the 3 teams. for the

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

prevalence of errors up to five bits, the outputs of decoder A and decoder B are going to be the same:

(i) If each the decoders have error free outputs (either zero error or single error which is able to be corrected by SEC–DED decoder).

(ii) Each the decoders have two bit errors (for the burst errors of thence the decoded price are going to be same).



The elaborate diagram of the SEC–DED decoder. The syndrome values C1, C2, C3, C4, C5 and C6 ar computed from the received bits within the syndrome computation block. The syndrome values ar given to syndrome decoder unit that detects the error location for single error. The error is corrected within the xor block. The message decoder separates the thirty two message bits from the thirty-nine bits which incorporates thirty two message bits and seven parity bits. Double error is detected mistreatment syndrome values and overall bit.

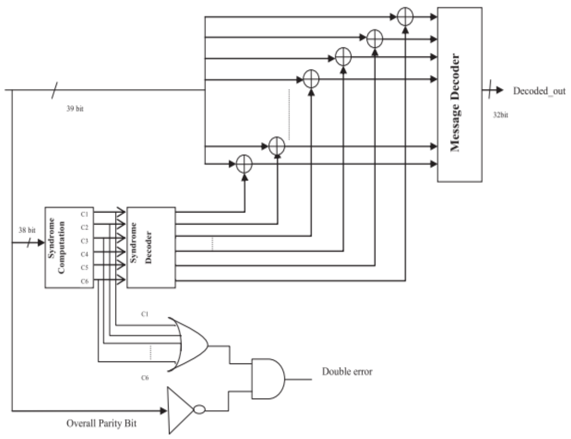
As shown in Fig. 4, supported double error detection Double error A, Double error_B, and Double error_C, syndrome values Syn_A, Syn_B, and Syn_C, Received_Not_eql and DecodeA_eql_DecodeB signals, the electronic device selects the decoded price that is error free because the single bit error are corrected by the SEC–DED decoder. The cryptography rule to find one, 2, 3, 4, and five bit errors is explained through a flow sheet shown in Fig. The cryptography rule consists of the subsequent steps

Step 1: Receive the bits and cluster the bits as 3 teams A, B and C victimisation cluster extractor.

Step 2: work out the signals Syn_A, Syn_B, Syn_C, Double error_A, Double error_B, Double error_C, Received_Not_eql and DecodeA_eql_DecodeB. Received_Not_eql signal is employed to handle sure things like (4,1, 0) (decoder A has four errors, decoder B has one error and decoder C has zero error), (4, 0, 1), (0,4,1), (0, 1,4) and (5, 0, 0). These error patterns area unit shown in
Table four columns three, 4, 7, 8 and 21. Decode A_ eql_DecodeB signal is employed to handle sure things like (4, 0, 0), (0,4, 0), (0,0, 4), (1,1,3), (1,3,1), (2,2,1) and (3,1,1). These error patterns area unit. As shown in Table one for one bit and a pair of bit errors, for all the columns except the last column, Double error_A isn't adequate to one.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 43-51 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

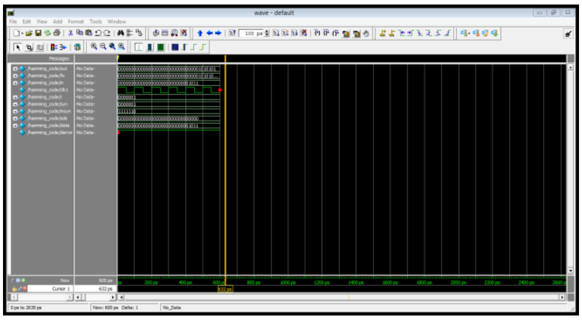
Hence, it follows the ‘No’ path **within the flow sheet and eventually** selects **one in every of** the **3** copies **that** is error free **exploitation** the signals Syn_A, Syn_B, Syn_C, Double error_A, Double error_B, Double error_C, Received_Not_eql and DecodeA_eql_DecodeB. For the last column Double error_A is **up to one**.



This case, Double error_B, Syn_B, Syn_C an

For Received_Not_eql signals are accustomed choose the decoded B that is error free. Similarly, as shown in Table 2–4 for three bit errors, four bit errors and five bit errors, the flow sheet follows ‘Yes’ path or ‘No’ path supported the incidence of double errors in type A. Syn_A, Syn_B, Syn_C, Double error A, Double error_B, Double error_C, Received_Not_eql and DecodeA_eql_DecodeB signals are accustomed choose the copy that is error free

SIMULATION OUTPUT



CONCLUSION

The future MBRBEC encoder uses SEC–DED extended hamming code 39 32 to encode the initial communication bits. Triplication error correction scheme is single of the standard mistake correction schemes used in communication system to accurate mistake. Suggest triplication error correction format to accurate the mistake in on chip interconnection link. Using triplication error correction scheme each of the encoded communication bit is triplicate. Thus if the initial SEC–DED extended hamming code is n l where n is the encoded communication and l is the creative communication then the final number of bits in the triplication communication is 3n. The triplication of the communication bit is used to exact the mistake and at the same time avoids crosstalk.

REFERENCE

[1] R. Ho et al., “High speed and low energy capacitively driven on-chip wires,” IEEE J. Solid-State Circuits, vol. 43, no. 1, pp. 52–60, Jan. 2008.

[2] E. A. M. Klumperink E. Mensink, B. Nauta, D. Schinkel, , E. van Tuijl, and “Power efficient gigabit communication over capacitively driven RC-limited on-chip interconnects,” IEEE J. Solid-State Circuits, vol. 45, no. 2, pp. 447–457, Feb. 2010.

[3] S. Hoppner et al., “An energy efficient multi-gbit/s NoC transceiver architecture with combined AC/DC drivers and stoppable clocking in 65 nm and 28 nm CMOS,” IEEE J. Solid-State Circuits, vol. 50, no. 3, pp. 749–762, Mar. 2015.

[4] J. Lee, W. Lee, and S. Cho, “A 2.5-Gb/s on-chip interconnect transceiver with crosstalk and ISI equalizer in 130 nm CMOS,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 59, no. 1, pp. 124–136, Jan. 2012.

[5] E. A. M. Klumperink, E. Mensink, B. Nauta, D. Schinkel and E.V. Tuijl, and “Low-power, high-speed transceivers for network-on-chip communication,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 17, no. 1, pp. 12–21, Jan. 2009.

[6] M. P. Flynn, J. Kang, J. Park, and S. Park, “A 9-Gbit/s serial transceiver for on-chip global signaling over lossy transmission lines,” IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 56, no. 8, pp. 1807–1817, Aug. 2009.

[7] M. P. Flynn and J. J. Kang, “Global signaling over lossy transmission lines,” in Proc. IEEE/ACM Int. Conf. Comput.-Aided Design (ICCAD, Nov. 2005, pp. 985–992.

[8] H. G. Rhew, M. P. Flynn, and J. Park, “A 22 Gb/s, 10 mm on-chip serial link over lossy transmission line with resistive termination,” in Proc. ESSCIRC (ESSCIRC), 2012, pp. 233–236.

[9] N. Tzartzanis and W. W. Walker, “Differential current-mode sensing for efficient on-chip global signalling,” IEEE J. Solid-State Circuits, vol. 40, no. 11, pp. 2141–2147, Nov. 2005.

[10] Maheshwari and W. Burleson, “Differential current-sensing for on-chip interconnects,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 12, no. 12, pp. 1321–1329, Dec. 2004.