International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

A Study on Design and Implementation of Fault Tolerant Parallel FFTs using Error Correction Codes

MS.JANA SUJITHA&& MR.SIDDU PENCHALAIAH

1 PG Student, Dept. Of VLSI and Embedded systems, SKR College Of Engineering & Technology, AP
2 Asst. Professor, Dept. Of VLSI and Embedded systems, SKR College Of Engineering &Technology,AP.

Abstract_ The intricacy of correspondences and flag processsing circuits expands each year. This is made conceivable by the CMOS innovation scaling that empowers the joining of an ever increasing number of transistors on a solitary gadget. This expanded many-sided quality makes the circuits more helpless against blunders. In the meantime, the scaling implies that transistors work with bring down voltages and are more powerless to blunders caused by commotion and assembling varieties. Delicate mistakes represent a dependability danger to current electronic circuits. This makes insurance against delicate blunders a prerequisite for some applications. Interchanges and flag handling frameworks are no exemptions to this pattern. For a few applications, a fascinating alternative is to utilize algorithmic-based adaptation to internal failure (ABFT) procedures that endeavor to misuse the algorithmic properties to distinguish and remedy mistakes. Flag preparing and correspondence applications are appropriate for ABFT. One case is quick Fourier changes (FFTs) that are a key building hinder in numerous frameworks. A few security plans have been proposed to distinguish and amend blunders in FFTs. Among those, presumably the utilization of the Perceval or whole of squares check is the most broadly known. In present day correspondence frameworks, it is progressively basic to discover a few squares working in parallel. As of late, a procedure that endeavors this reality to actualize adaptation to internal failure on parallel channels has been proposed. In this concise, this system is first connected to ensure FFTs. At that point, two enhanced assurance plots that consolidate the utilization of blunder adjustment codes and Perceval checks are proposed and assessed.

Keywords: Error correction codes (ECCs), Fast fourier transforms (FFTs) and Soft errors.

1.Introduction

The difficulty of communications and signal processing circuits increases every year. This is made possible by the CMOS technology scaling that enables the addition of more and more transistors on a single device. This increased complexity makes the circuits more susceptible to errors. At the same time, the scaling means that transistors operate with lower voltages and are more vulnerable to errors caused by noise and

manufacturing variations. The meaning of radiation-induced soft errors also increases as technology scales. Soft errors can change the logical value of a circuit node creating a short term error that can affect the system operation. To ensure that soft errors do not affect the operation of a given circuit, a wide variety of techniques can be used. These contain the use of special manufacturing processes for the integrated circuits like, for example, the silicon on insulator. Another option is to design basic circuit blocks or complete design libraries to minimize the probability of soft errors. Finally, it is also probable to add redundancy at the system level to detect and correct errors. One typical example is the use of Triple Modular Redundancy (TMR) that triples a block and votes between the three outputs to detect and correct errors. For example TMR, the overhead is >200%. This is because the insecure module is virtual three times (which requires a 200% overhead versus the unprotected module), and additionally, voters are required to correct the errors making the overhead >200%. Another approach is to try to utilize the algorithmic properties of the circuit to detect/correct errors. This is typically referred to as Algorithm-Based Fault Tolerance (ABFT), this policy can decrease the overhead necessary to protect a circuit. Signal processing and communications circuits are well suited for ABFT as they contain normal structures and many algorithmic properties. Over the years, many ABFT techniques have been planned to protect the basic blocks that are commonly used in those circuits. Some works have considered the protection of digital filters. For example, the use of duplication using intense precision copies of the filter has been proposed as an option to TMR but with a lesser rate. In this brief, the security of parallel FFTs is considered. In particular, it is assumed that there can only be a single error on the method at any given point in time. This is a general statement while considering the protection against radiation-induced soft errors. There are three main contributions in this brief.

1) The estimation of the ECC method for the protection of equivalent FFTs showing its efficiency in terms of overhead and protection effectiveness.
2) The request of a new method based on the use of Parseval or sum of squares (SOSs) checks join with a parity FFT.
3) The proposal of a new method on which the ECC is used on the SOS checks as an alternative of on the FFTs.

2. EXISTING METHOD

The protection of filters has also been generally studied, occurrence of parallel filters to creates an opportunity to implement ABFT techniques for the whole collection of parallel modules as an alternative for each one independently. This has been studied for digital filters originally in where two filters were considered. In recent times, a broad scheme based on the use of error correction codes (ECCs) has been proposed. The design of filter implementation is complex. This will be denoted as c1 check. The same analysis applies to the other two redundant modules that will provide checks c2 and c3. Based on the differences observed on each of the checks, the module on which the error has occurred can be determined. The dissimilar patterns and the

corresponding errors are summarized in Table 1. Once the module in error is known, the error can be corrected by reconstructing its output using the residual modules. Related correction equations can be used to correct errors on the other modules. More advanced ECCs can be used to correct errors on many modules if that is required in a given application. The overhead of this technique, as discussed in, is lower than TMR as the number of redundant FFTs is related to the algorithm.

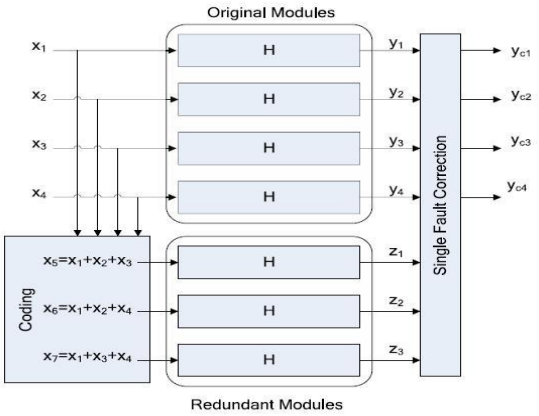


Fig.1. Parallel Filter Protection (Hamming Code)

To protect four FFTs, three redundant FFTs are required, but to protect eleven, the number of redundant FFTs in only four. This shows how the overhead reduces with the number of FFTs. In Section I, it has been mentioned that over the years, many techniques have been proposed to protect the FFT. One of them is the Sum of Squares (SOSs) check that can be used to detect errors. The SOS check is based on the Parseval theorem that states that the SOSs of the inputs to the FFT are equal to the SOSs of the outputs of the FFT except for a scaling factor. This relationship can be used to detect errors with low overhead as one multiplication is needed for each input or output sample (two multiplications and adders for SOS per sample). For parallel FFTs, the SOS check can be combined with the ECC approach to reduce the protection overhead. Since the SOS check can only detect errors, the ECC part should be able to implement the correction. This can be done using the equivalent of a simple parity bit for all the FFTs. In addition, the SOS check is used on each FFT to detect errors.

When an error is detected, the output of the parity filter can be used to correct the error. This is better explained with an example. The first proposed scheme is illustrated for the case of four parallel filters. A redundant (the parity) filter is added that has the sum of the inputs to the original filter as input.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

The two proposed techniques offer new alternatives to protect parallel filters that can be more capable than caring each of the filters independently. The proposed schemes have been evaluated using FPGA implementations to evaluate the protection overhead. The results explain that by combining the use of ECCs and Parsevalchecks, the safety overhead can be reduced compared with the use of just ECCs as proposed.

3. PROPOSED PROTECTION SCHEMES

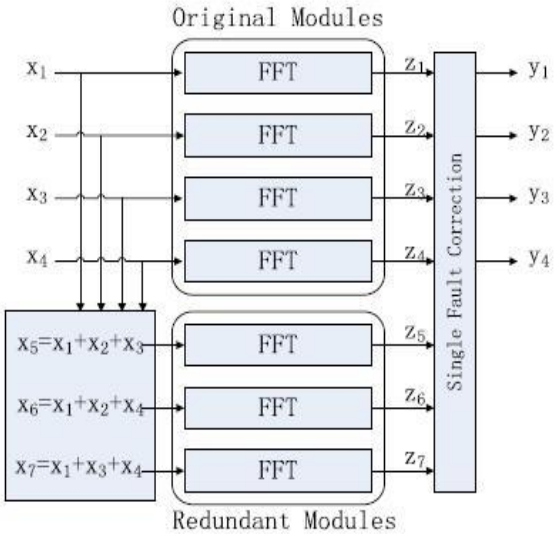
The initial point for our work is the protection scheme based on the use of ECCs that was presented in for digital filters. This scheme is shown in Fig. 2. In this example, a simple single error correction Hamming code is used. The new scheme consists of four FFT modules and three redundant modules is added to detect and correct errors. The inputs to the three redundant modules are linear combinations of the inputs and they are used to check linear combinations of the outputs. For example, the input to the first redundant module is,

$x5 = x1 + x2 + x3$(1)

Given that the DFT is a linear operation, its output z5 can be used to verify that,

$z5 = z1 + z2 + z3$ (2)

This shows how the overhead reduced with the number of FFTs. In this section, it has been mentioned that more than the years, a lot of techniques have been planned to protect the FFT. One of them is the Sum of Squares (SOSs) check that can be used to spot errors. The SOS check is based on the Parseval theorem that states that the SOSs of the inputs to the FFT are identical to the SOSs of the outputs of the FFT not including for a scaling aspect. This relationship can be used to detect errors through low overhead as one multiplication is needed for each input or output model (two multiplications and adders for SOS per sample).



International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

Fig.2. Parallel FFT protection using ECCs

The overhead of this technique, as discussed in, is poorer than TMR as the number of redundant FFTs is linked to the algorithm of the number of original FFTs. For example, to keep four FFTs, three redundant FFTs are needed, but to protect eleven, the number of unneeded FFTs in only four.

Parallel FFTs, the SOS check can be combined with the ECC approach to decrease the protection overhead. Since the SOS check can just detect errors, the ECC part should be able to apply the correction. This can be completed using the
equivalent of a simple parity bit for all the FFTs. In addition, the SOS check is used on every FFT to notice errors. When an error is detected, the output of the parity FFT can be used to exact the error. This is better explained with an example. In Fig. 2, the first proposed scheme is illustrated for the instance of four parallel FFTs.

This combination of a parity FFT and the SOS verify reduces the number of additional FFTs to just one and may, therefore, reduce the protection overhead. In the following, this scheme will be referred to as corresponding-SOS. Another possibility to combine the SOS check and the ECC approach is instead of using an SOS check per FFT, make use of an ECC for the SOS checks.

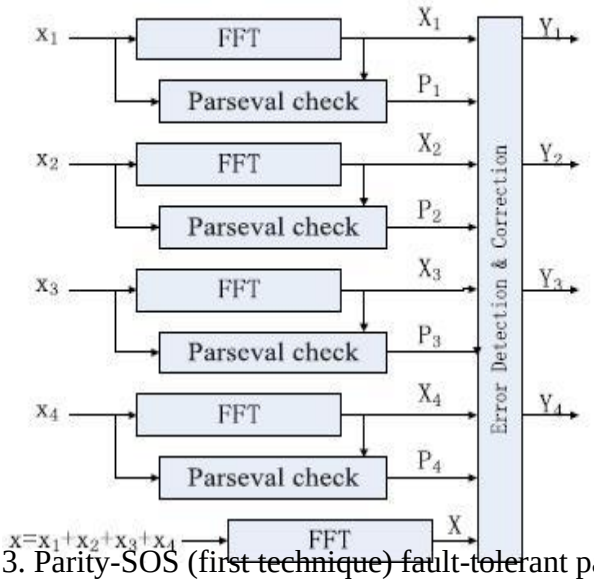


Fig.3. Parity-SOS (first technique) fault-tolerant parallel FFTs

A redundant FFT is added to facilitate has the sum of the inputs to the original FFTs as input. The SOS check is also added to each original FFT. In case an error is

detected (using P1, P2, P3, P4), the correction can be completed byre-computing the FFT in error using the output of the parity FFT (X) and the rest of the FFT outputs.

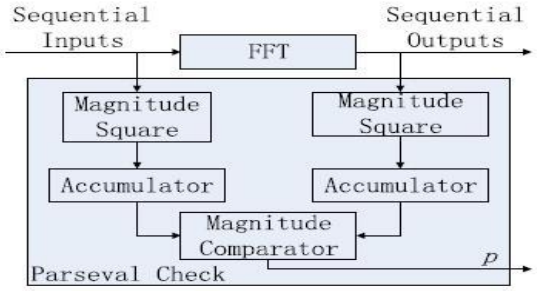


Fig.4. Implementation of the SOS check

$$X1c = X - X2 - X3 - X4 \quad (3)$$

The parity-SOS scheme, an additional parity FFT is used to correct the errors. This second technique is shown in Fig. 3. The main benefit over the first parity- SOS scheme is to reduce the number of SOS checks needed.

The overheads of the two proposed schemes can be initially estimated using the number of additional FFTs and SOS check blocks needed. This information is summarized for a set of k original FFT modules assuming k is a power of two. It can be observed that the two proposed schemes reduce the number of additional FFTs to just one.

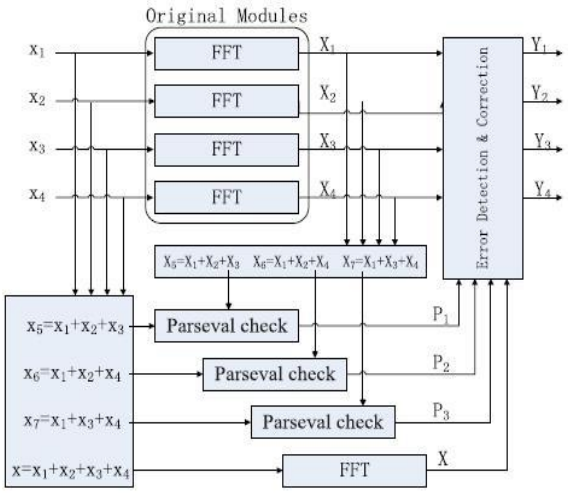


Fig.5. Parity-SOS-ECC fault-tolerant parallel FFTs

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

Table.1. Resources Usage for a Single FFT and SOS Check

	FFT	SOS Check
Slices	1367	494
Flip-Flop	1037	141
LUT-4	2530	974

Tables 1 explain the results when different number of parallel FFTs is protected. The point is to illustrate how the relative overheads of the different techniques vary with the number of parallel FFTs. In parentheses, the cost virtual to an unprotected implementation is also provided. The results show that all techniques have a rate factor of <2. This demonstrates that the ECC-based technique is also competitive to keep FFTs and requires a much lower cost than TMR. The parity-SOS-ECC technique has the lowest resource use in all cases and, therefore, is the best option to minimize the implementation cost.

The FFT and the various protection techniques have been implemented using Verilog. The results obtained are first table provides the resources needed to implement a single FFT and an SOS check. The results show that the FFT is more complex than the SOS check as expected. The difference will be much larger when a totally parallel FFT implementation is used. The parity-SOS-ECC scheme, the number of SOS checks also grows logarithmically and they are simpler to implement than FFTs. Therefore, it remains more competitive than the ECC scheme regardless of the number of FFTs protected.

To better illustrate this phenomenon, the number of slices required for the different schemes and number of FFTs is plotted. It can be observed that eight is the value for which parity-SOS and ECC have almost the same cost. In each simulation run, one error is inserted to mimic the behavior of soft errors that occur in isolation. For ECC protected parallel FFTs, a tolerance level of 1 is used for the equation checks. For the parity-SOS and parity-SOS-ECC schemes, the fault coverage is determined by the tolerance level τ used in the Parseval check.

4.Simulation results:

4.1.1For Parallel FFTs Using ECC:

Fig 4.1.1 Simulation result for the parallel FFTs using ECC

4.1.2 For Parallel FFTs using PSOS:

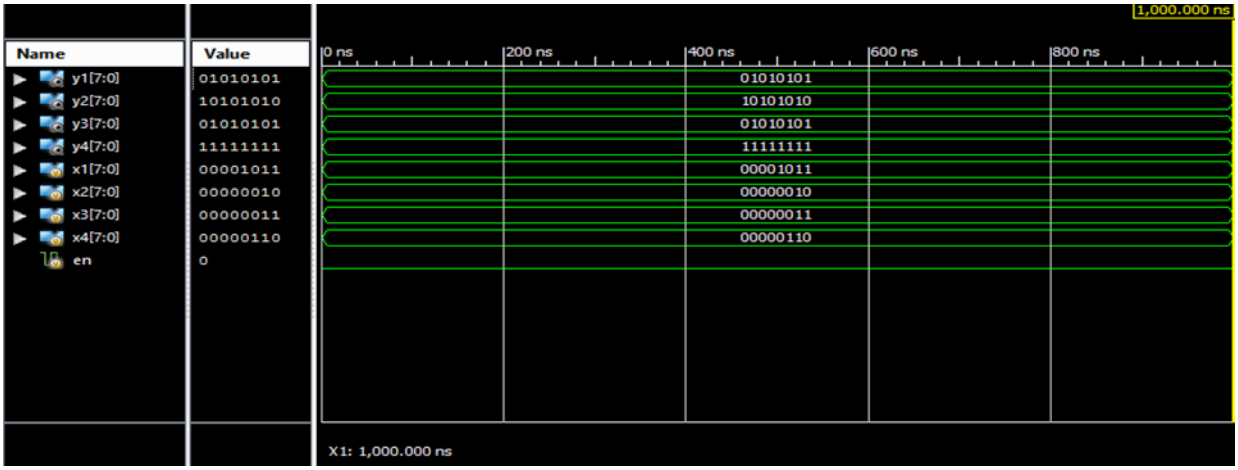
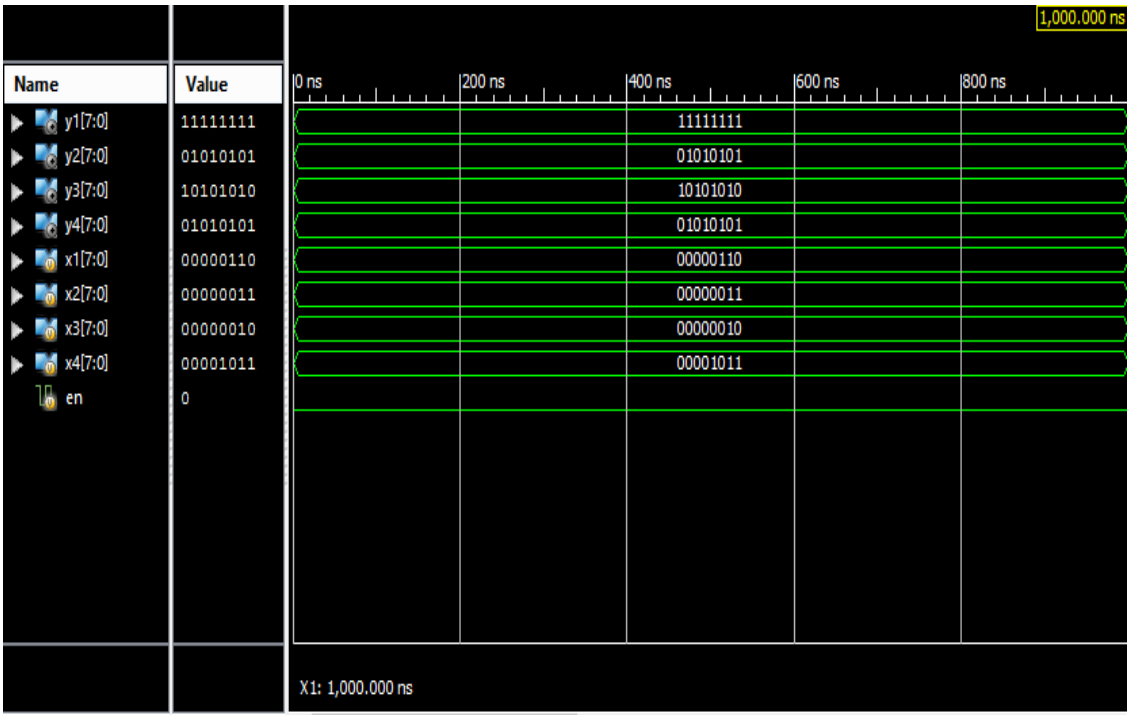


Fig 4.1.2 Simulation result for the parallel FFTs using PSOS



International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

4.1.3 For Parallel FFTs using ECC and PSOS:

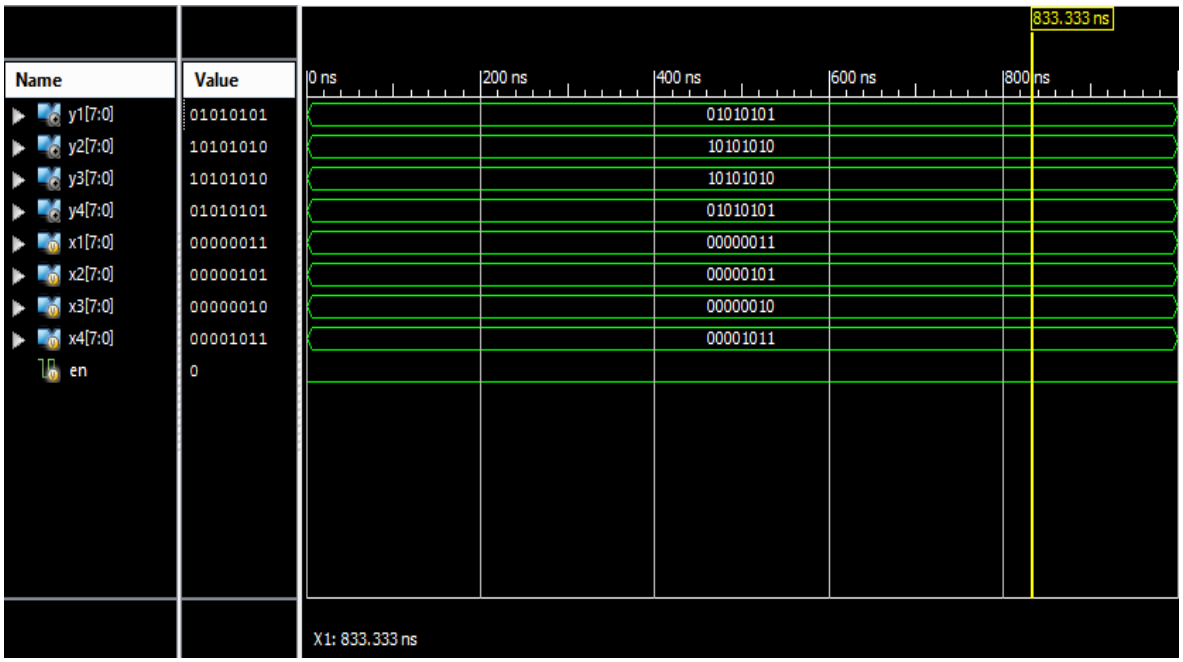


Fig 4.1.3 Simulation result for the parallel FFTs using ECC and PSOS

4.2 Synthesis Result:

4.2.1 Device Utilization Summary:

For Protection Of Parallel FFTs Using Parity-SOS-ECC:

fft_ecc_psos Project Status (08/15/2017 - 10:10:45)			
Project File:	faults.xise	**Parser Errors:**	No Errors
Module Name:	fft_ecc_psos	**Implementation State:**	Synthesized
Target Device:	xc7a100t-3csg324	• **Errors:**	
Product Version:	ISE 14.4	• **Warnings:**	
Design Goal:	Balanced	• **Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	• **Timing Constraints:**	
Environment:	System Settings	• **Final Timing**	

		Score:	

Device Utilization Summary (estimated values)			**[-]**
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice LUTs	27	63400	0%
Number of fully used LUT-FF pairs	0	27	0%
Number of bonded IOBs	63	210	30%

4.2.2 RTL Schematic:

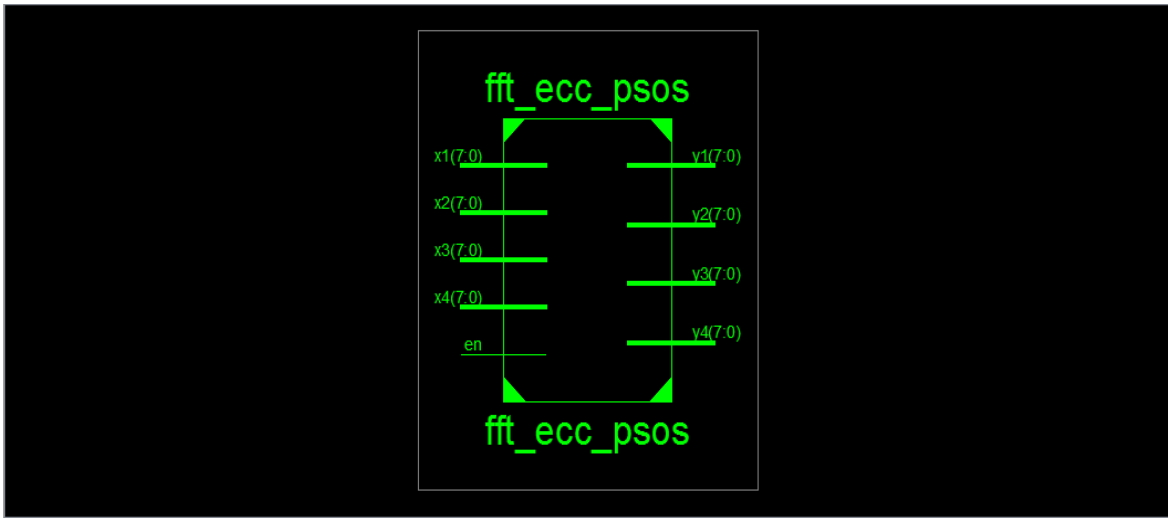


Fig 4.2.2 RTL Schematic with Basic Inputs and Outputs

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 20
SEPTEMBER 2018

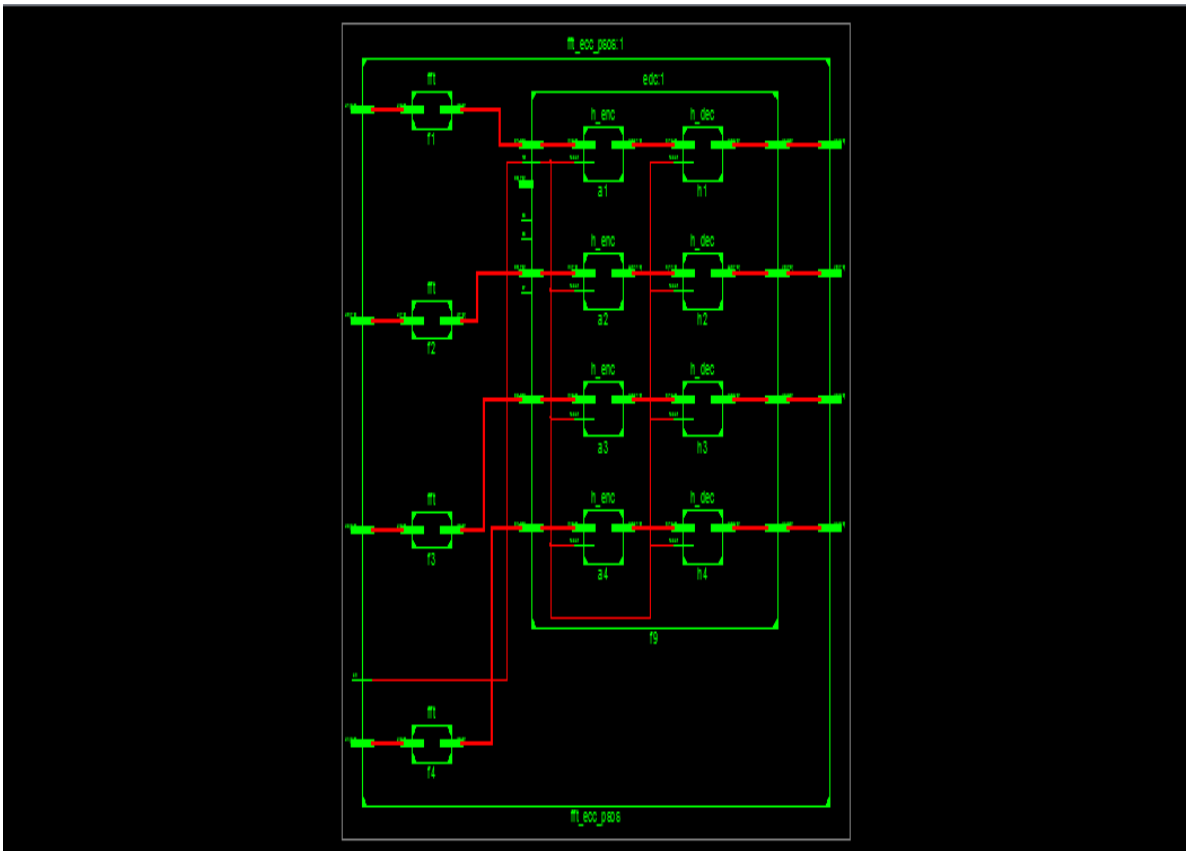


Fig 4.2.3 RTL Schematic for Parity-SOS-ECC

4.3.3 Technology Schematic:

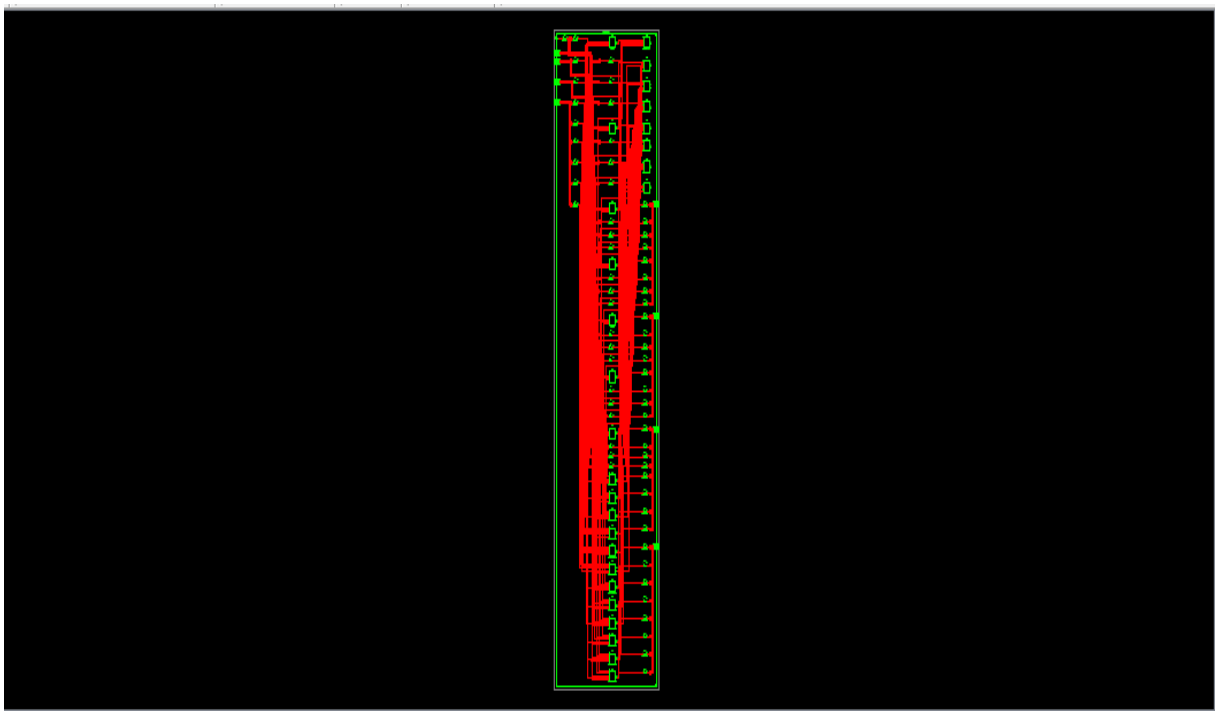


Fig 4.3.3 Technology Schematic for Parity-SOS-ECC

5.CONCLUSIONS

Detecting and correcting errors such as critical reliability are difficult in signal processing which increases the use of fault tolerant implementation. In modern signal processing circuits, it is common to find several filters operating in parallel. Proposed is an area efficient technique to detect and correct multiple errors. This brief has presented a new scheme to protect parallel FFT using cordic that is commonly found in modern signal processing circuits.

The approach is based on applying SOS-ECC check to the parallel FFT outputs to detect and correct errors. The SOS checks are used to detect and locate the errors and a simple parity FFT is used for correction. The 8 point FFT with the input bit length 32 is protected using the proposed technique. The detection and location of the errors can be done using an SOS check per FFT or alternatively using a set of SOS checks that form an ECC. This technique can detect and correct only multiple bit error and it reduces area results in high speed compared to existing techniques.

6.FUTURE WORK

The implemented design can be used as a basic block for further computation. The pipelined architecture can also be added to FFT for providing fast and better

performance. The proposed processor can be integrated with other components which can be used as a stand-alone processor for many applications.

REFERENCES

[1] Gao Z., et al., "Fault tolerant parallel filters based on error correction codes" (2015), IEEE Trans. on Very Large-ScaleIntegr. (VLSI) Syst., Vol.23, No.2, pp.384–387.

[2]Baumann R., "Soft errors in advanced computer systems" (2005), IEEE Des. Test Comput., Vol.22, No.3, pp.258–266.

[3]Gao Z., Yang W., Chen X., Zhao M., and Wang J., "Fault missing rate analysis of the arithmetic residue codes based fault tolerant FIR filter design" (2012), in Proc. IEEE IOLTS, pp.130–133.

[4] Hitana T., and Deb A. K., "Bridging concurrent and non-concurrent error detection in FIR filters" (2004), in Proc.Norchip Conf., pp. 75–78.

[5] Jou J. Y., and Abraham J. A., "Fault-tolerant FFT networks" (1988), IEEE Trans. Comput., Vol. 37, No. 5, pp.548–561.

[6] Kim E. P., and Shanbhag N. R., "Soft N-modular redundancy" (2012), IEEE Trans. Comput., Vol.61, No.3, pp. 323–336.

[7]Nicolaidis M., "Design for soft error mitigation" (2005), IEEE Trans. Device Mater. Rel., Vol. 5, No.3, pp. 405–418.

[8] Pontarelli S., Cardarilli G. C., Re M., and Salsano A.,"Totally fault tolerant RNS based FIR filters" (2008), inProc. 14th IEEE Int. On-Line Test Symp. (IOLTS), pp.192–194.

[9] Reddy.A.L.N., and Banerjee.P., "Algorithm-based fault detection for signal processing applications" (1990), IEEETrans. Comput., Vol. 39, No. 10, pp. 1304–1308.

[10] Reviriego P., Bleakley C. J., and Maestro J. A., "A novel concurrent error detection technique for the fast Fouriertransform" (2012), in Proc. ISSC, Maynooth, Ireland, pp.1–5.

Author's Profile:

Ms.JANA SUJITHA I received B.Tech in Electronics and Communication Engineering from Priyadarshini Institute Of Technology, Nellore affiliated to the Jawaharlal Nehru technological university Anatapur in 2014, and pursing M. Tech in VLSI and Embedded systems from SKR College of Engineering affiliated to

the Jawaharlal Nehru technological university Anantapur in 2018, respectively.

Mr.SIDDU PENCHALAIA Has Asst Professor Department of ECE.Qualification: M.Tech
SKR College of Engineering & Technology