

Design of Low Power, High Speed Parallel Architecture of Cyclic Convolution Based on Fermat Number Transform (FNT)

Ramya.B^{#1} and K. Sanath Kumar^{*2}

*M.Tech & ECE& Sreenidhi Institute of Science and Technology
Central Institute of tool Design, India*

Abstract

Low power, High speed parallel architecture of cyclic convolution (FNT) in diminished-1 number system. For Designing of Low Power we are being using the Novel Architecture Technique of XOR-XNOR Mux style 4-2 Compressor. The power consumption, Delay and Area of this new novel 4-2 Compressor Architecture is compared with Existing architecture. In the proposed architecture the outputs are efficiently used to improve Low power, high speed, performance, less and delay. Here Fermat number transform is used for the digital computation requiring the order of $N \log N$ Additions, Subtractions and bits shifts but the no multiplications are been performed In addition to that the implementation of FNT is exact with no round off errors and Truncation errors. The Binary Arithmetic in FNT performs the Exact Computation. To perform the cyclic convolution in FNT some techniques are implemented. The Techniques are code Conversion method without Addition (CCWA) and Butterfly Operation without Addition (BOWA) are proposed to perform the FNT and its Inverse (IFNT) except their final stages in the Convolution. Here the Point wise Multiplication in the Convolution is accomplished by Modulo 2^{n+1} Partial Products Multipliers (MPPM) and Output partial products which are Inputs to the IFNT. Thus Modulo 2^{n+1} Carry save Propagation Additions are avoided in the FNT and the IFNT except their final stages and the Modulo 2^{n+1} multiplier. Thus the Power and Execution delay of the entire FNT will be reduced which is only because of usage of above techniques in the Design. Therefore the proposed one has less Power better Throughput Performance and

involves less hardware complexity. This will be done by using Very Large Scale Integration (VLSI) technology and various Cad tools available, so as to implement hardware. The synthesis results using 180nm SOC Technology is been used.

Keywords: Fnt, ccwa, bowa, novel 4-2 compressor, mppm.

1. Introduction

Now the Present World is facing challenges in order to reduce the Power, delay and area, so that the reliability and portability will increase. Here the cyclic convolution is performed based on FNT, is used in DSP (digital signal processing) Applications for Security of information transmission and reception purpose. For obtaining low power we are being using Novel architecture of xor-xnor, mux style 4-2 compressor [8] is used rather than 4-2 compressor of full adder, in full adder 4-2 compressor the complexity is more because it contains large number of gates therefore power consumption is more and area is more, delay is more. All these are overcome by using xor-xnor, mux style 4-2 compressor. Generally Convolution is a basic operation in DSP [1] but when finite word length is calculating for the convolution there exists round off and truncation errors and is very computational expensive operation. Therefore to reduce computational complexity we are opting for cyclic convolution or circular convolution, it is simpler and easy and produces less output samples and it is one of the most important and efficient operation in DSP.

Cyclic convolution can be performed efficiently using FNT rather than both DFT and FFT. The cyclic based on FFT is widely used operation in signal processing in a complex domain even if both the sequences are real and also the FFT of length N requires $(n/2)\log n/2$ complex multiplications which consumes more computational time. whereas cyclic convolution based on DFT requires large number of operations. The direct computation of DFT is proportional to N^2 . In such case the Number-theoretic transform [2] was introduced as a generalization of the DFT. For residue ring of integers in order to implement fast cyclic convolution and correlation without roundoff errors and better efficiency than the FFT. However there is one interesting case of the NTT [3] is Fermat number transform.

The cyclic convolution based on FNT is simple and less computational complexity because the expensive multiplications in FFT and DFT can be replaced by bit shifts in FNT with its integer power 2. Fermat number is a positive integer of the form $F_n = 2^{2^n} + 1$ where t is nonnegative integer. FNT [4], [5] is suitable to digital computation therefore fnt implementation is exact without roundoff errors. The Fermat number transform has been used in many applications such as video processing, digital filtering, and multiplication of large numbers and also in Pseudo random generator.

Important operations of cyclic convolution based on FNT with the unit root 2 includes i) ccwa (code convolution without addition) ii) bowa (butterfly operation

without addition) and mppm. The CCWA and BOWA both consist of novel modulo 2^n+1 -2 compressor in the diminished-1 representation of X i.e., $X=X-1$ [9].

2. Code Conversion Without Addition

It is the first stage in FNT. Here CC converts the normal binary code (NBC) into the diminished-1 representation. The delay and area of CC of n -bit NBC is close to the ones of an n -bit carry propagation adder. To reduce the cost we propose the CCWA which is performed by modulo 2^n+1 4-2 compressor.

I_0, I_1, I_2, I_3 are four inputs applied to modulo 2^n+1 4-2 compressor. Outputs obtained are sum vector Ho^* and carry vector $H1^*$ in the diminished-1 representation [5].

1. The existing 4-2 compressor:

Compressors are the basic components in many applications particularly in partial product summation in multipliers. Multiplication is a basic arithmetic operation in applications such as DSP which rely on efficient implementation of ALU and floating point units to execute operations like convolution and filtering.

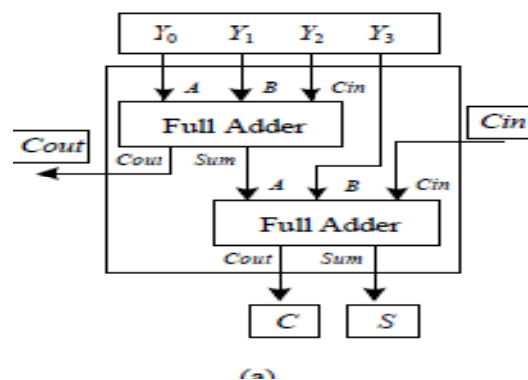


Fig. 1: Existing 4-2 compressor.

In this 4 inputs [I_0, I_1, I_2, I_3] and 2 outputs [Carry, Sum] are generated. Here the full adder performs as 4-2 compressor which accepts 4 inputs and gives 2 outputs but in the full adder the number of gates is more. As we used two full adders the complexity increases and power is more, area occupied is more hence delay is more. In order to obtain low power, high speed, less area we proposed a Novel Architecture of xor-xnor, mux style 4-2 compressor [6].

2. Proposed novel architecture of 4-2 compressor:

In this proposed new compressor architecture the design of low power, high speed, delay and area of these new compressor architecture are compared with the existing one.

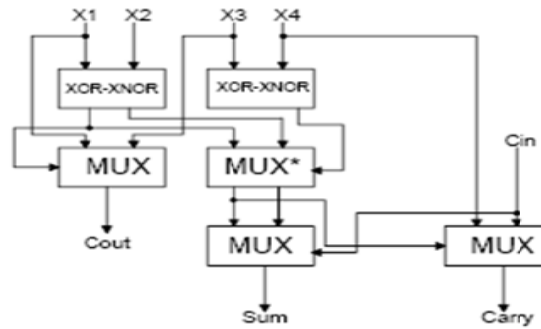
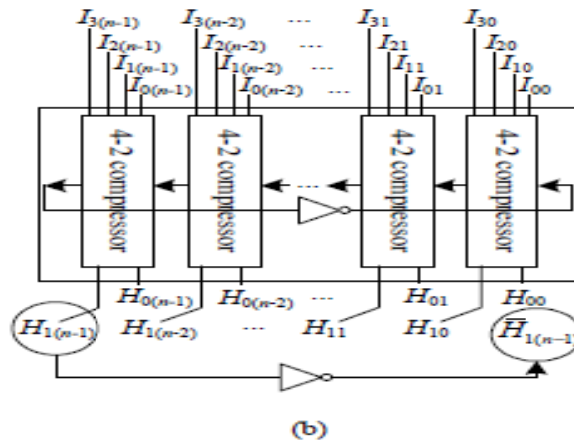


Fig 7. Proposed 4-2 Compressor Architecture

Fig. 2: modulo $2n+1$ 4-2 compressor.

In this each full adder are broken into their constituent XOR blocks .It consists of 4 inputs X_1, X_2, X_3, X_4 and 2 outputs carry, sum along with cin and cout, cin is previous output from compressor and cout is the output to the compressor to the next stage. Both the Xor and Xnor values are computed efficiently used to reduce delay .This is due to availability of the selection bit at the mux block so that before the arrival of input. Thus the time required for switching of transistors is reduced.

Fig. 3: modulo $2n+1$ 4-2 compressor.

The equations of output in the proposed architecture are shown below

$$\begin{aligned}
 Sum &= (x_1 \oplus x_2) \cdot x_3 \oplus x_4 + (x_1 \oplus x_2) \cdot (x_3 \oplus x_4) \cdot Cin + \\
 &\quad \overline{(x_1 \oplus x_2) \cdot x_3 \oplus x_4 + (x_1 \oplus x_2) \cdot (x_3 \oplus x_4) \cdot Cin} \\
 Cout &= (x_1 \oplus x_2) \cdot x_3 + \overline{(x_1 \oplus x_2) \cdot x_1} \\
 Carry &= (x_1 \oplus x_2 \oplus x_3 \oplus x_4) \cdot Cin + \\
 &\quad \overline{(x_1 \oplus x_2 \oplus x_3 \oplus x_4) \cdot x_4}
 \end{aligned}$$

In this Modulo 2^n+1 4-2 compressor, the novel architecture of 4-2 compressor [7, 8] [fig 2] as shown above is called for required number of times to perform the CCWA. Outputs are sum vector $H0^*$ & $H1^*$. The MSB $H1^*$ is complimented and connected back to its LSB. The obtained results consisting of two diminished-1 values.

3. Butterfly Operation Without Addition

BOWA is the one of operation performed in FNT after the CCWA has been performed. It consists of two modulo 2^n+1 4-2 compressors, a multiplier and some inverters as shown below in fig 4. It can be performed without carry propagation chain so as to reduce delay and area. Here the designed low power 4-2 compressor of novel architecture thus the power generated will be less.

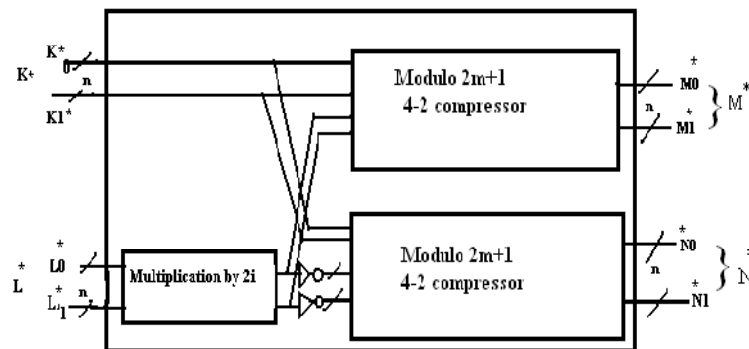


Fig. 4: Butterfly operation without Addition.

K^*, L^*, M^*, N^* are corresponding to two inputs and two outputs of previous BO in the diminished-1 number system respectively.

1. MODULO 2^n+1 PARTIAL PRODUCT MULTIPLIER

After performing the calculations of CCWA and BOWA both of them will produce the carry-save order then MPPM[10] is used perform point wise multiplications so that final carry-propagation addition of two partial products in multiplier is avoided therefore the execution delay will be reduced. Modulo 2^n+1 multiplier is proposed by Efstathiou, there are $n+3$ partial products. An full adder based Daddatree [7] reduces the $n+3$ partial products into two summands. Dadda multiplier is faster than other multipliers therefore it gives the fast performance than other multipliers. In the proposed cyclic convolution based on FNT of parallel architecture, the BOWA accepts four operands in diminished-1 number system. Every point wise multiplication produce two partial products rather than one product. It takes away the final modulo 2^n+1 adder of two partial products in the multiplier thus the final modulo 2^n+1 adder is removed and modulo 2^n+1 partial product multiplier is used to save the area and delay.

2. Parallel Architecture Of Cyclic Convolution

Parallel Architecture of cyclic convolution for cyclic is designed by using CCWA, BOWA and MPPM as shown below. Point wise multiplication and generates N pair of partial products. Later IFNT of partial products are performed to produce sequence $\{P_i\}$ of the cyclic convolution.

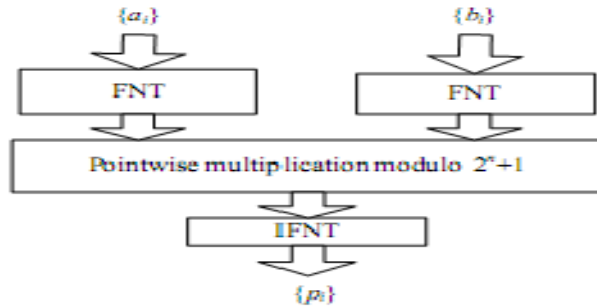
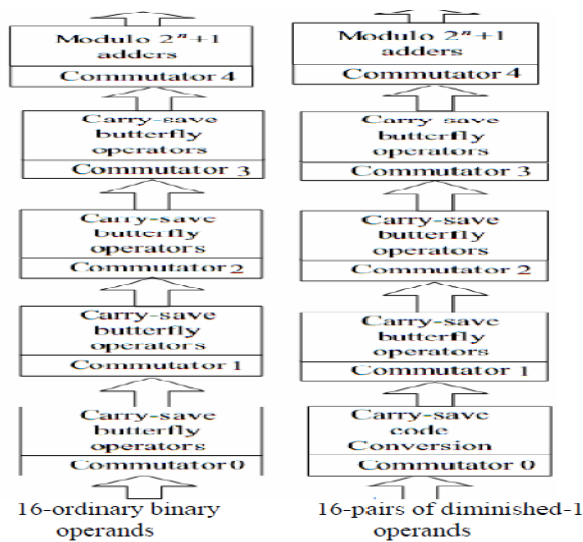


Fig. 5: Parallel Architecture of cyclic convolution based on FNT [9].

It consists of Two FNTS , IFNT and point wise multiplication modulo 2^n+1 .It has two input sequences $\{a_i\}$ and $\{b_i\}$ produce two sequences $\{A_i\}$ and $\{B_i\}$ ($i=1, 2 \dots N-1$). Sequences $\{A_i\}$ and $\{B_i\}$, then A_i and B_i applied to N MPPM to perform the point wise multiplication and generates N pair of partial products.



(a) Parallel FNT structure b) Parallel IFNT structure

Fig. 6: Structures for FNT and IFNT (Ft=28+1)

Later IFNT of partial products are performed to produce sequence $\{P_i\}$ of the cyclic convolution.

4. Explanation

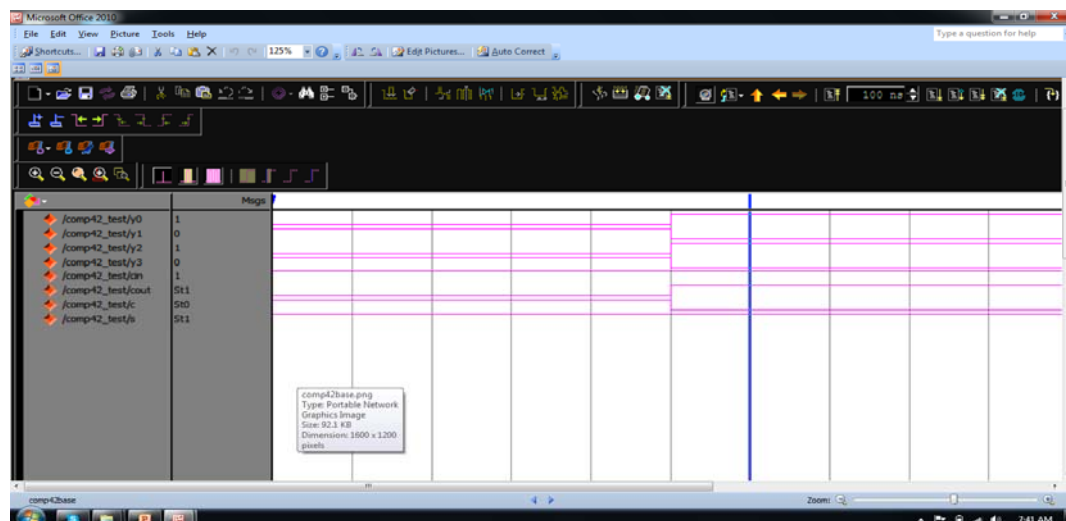
It has $\log_2 N + 1$ stages of operations.

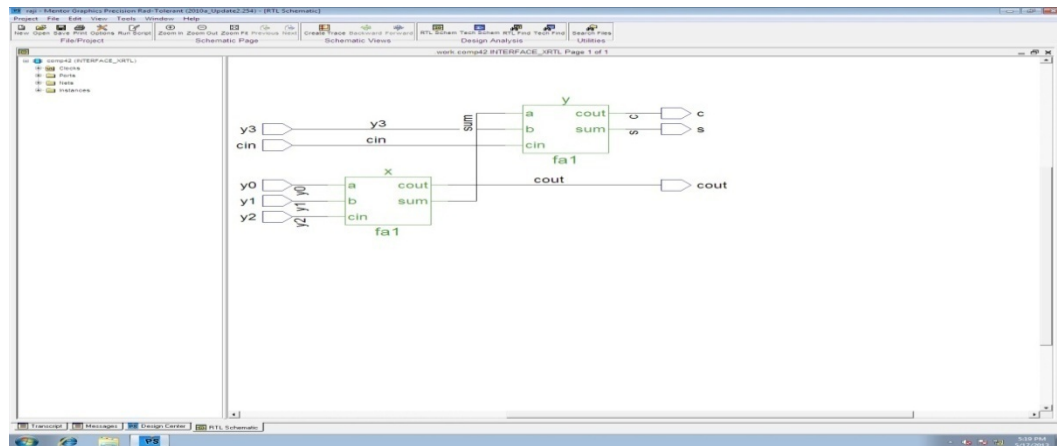
The efficient FNT structure involves $\log_2^{2N} + 1$ stages of operations. The original operands are converted into the diminished-1 representation in the CCWA stage, containing the information of modulo $2^n + 1$ addition or subtraction in the first butterfly operation stage of the previous FNT structure. Then the results are sent to the next stage of BOWA. After $\log_2^{2n} - 1$ stages of BOWAs, the results composed of two diminished-1 operands are obtained. The final stage of FNT consists of modulo $2^n + 1$ carry-propagation adders which are used to evaluate the final results in the diminished-1 representation.

5. Implementation

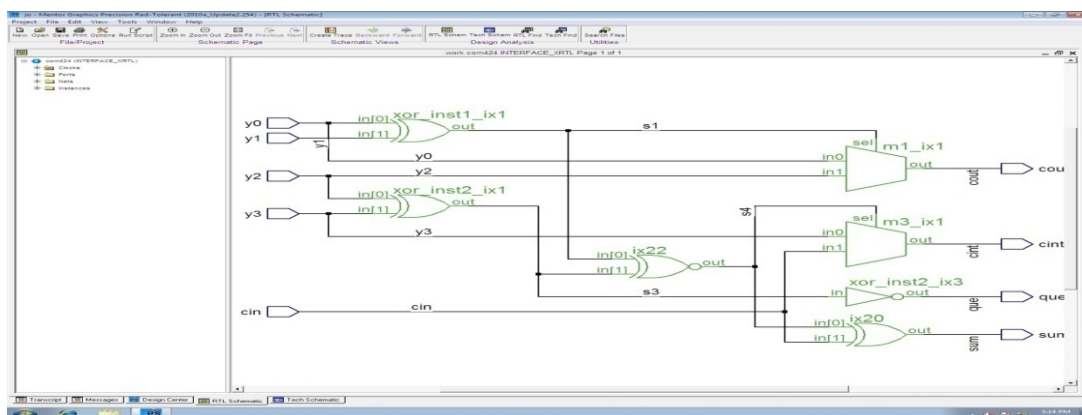
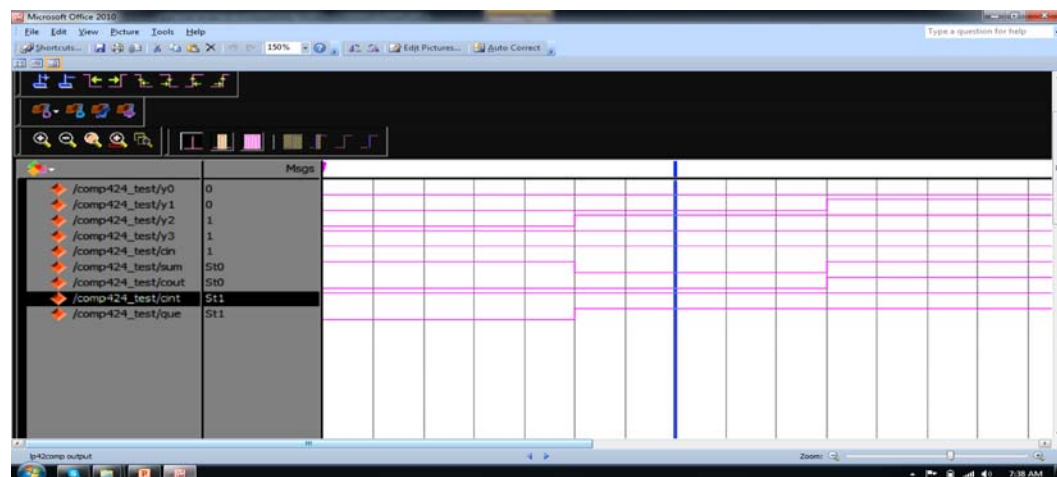
4-2 compressor and also for the existing architecture in order to simulate both the codes and compare the low power calculations for both the architectures. All this has been done as follows. Verilog code is written and then simulated using QuestaSim tool from Mentor Graphics. The System-on-Chip (SOC) approach is adopted using Cadence tools, SOC Encounter software the Power and Area Analysis is done and reduced by Xilinx Xpower/RTL Precision Synthesis tool and the power and area is optimized.

6. Results of old full adder 4-2 Compressor:





7. Results of Proposed 4-2 Compressor



Existing compressor RTL POWER

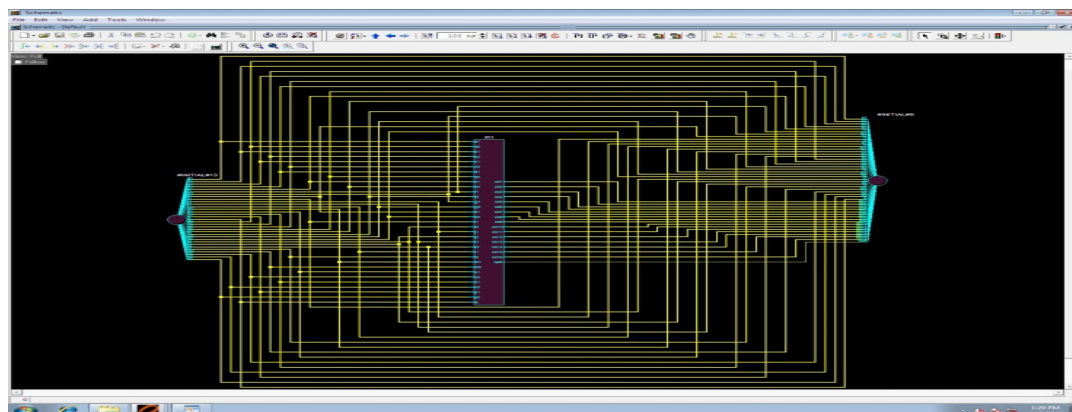
Report RTL Power					
Generated by: Encounter(R) RTL Compiler v07.20-p004_1 (Nov 29 2007)					
Generated on: Feb 01 2012 12:42:18					
Module: comp42					
slow_highv1 1.0					
Technology libraries: slow_normal 1.0					
tpz973gfc 230					
Operating conditions: slow (balanced_tree)					
Wireload mode: segmented					
File	Row	Leakage (mW)	Internal (mW)	Net (mW)	
/home/kadence/c52lab/oldwork/_oldrtl/comp42.v	5	17.59	1172.02	1189.60	
/home/kadence/c52lab/oldwork/_oldrtl/comp42.v	6	17.59	1375.03	1392.62	

Proposed 4-2 compressor RTL POWER

Report RTL Power					
Generated by: Encounter(R) RTL Compiler v07.20-p004_1 (Nov 29 2007)					
Generated on: Feb 01 2012 13:23:03					
Module: com424					
slow_highv1 1.0					
Technology libraries: slow_normal 1.0					
tpz973gfc 230					
Operating conditions: slow (balanced_tree)					
Wireload mode: segmented					
File	Row	Leakage (mW)	Internal (mW)	Net (mW)	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	5	5.53	598.29	603.82	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	6	5.53	446.15	451.69	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	7	3.79	315.09	318.88	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	8	3.79	405.31	409.10	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	9	3.79	422.97	426.75	
/home/kadence/c52lab/newwork/_newrtl/comp424.v	10	4.92	1128.56	1133.47	

Here the existing compressor RTL Power is 1189.60 where the proposed 4-2 compressor as 603.88, thus is reduced and high speed and less delay and area.

The schematic of FNT architecture in Questasim software



References

- [1] J. G. Proakis and D. G. Manolakis, Digital signal processing: principles, algorithms, and applications, Prentice Hall, New Jersey, 2007.
- [2] A. B. O'Donnell, C. J. Bleakley, "Area efficient fault tolerant convolution using RRNS with NTTs and WSCA", Electronics Letters, 2008, 44(10), pp.648-649
- [3] R. Conway, "Modified Overlap Technique Using Fermat and Mersenne Transforms", IEEE Trans. Circuits and Systems II: Express Briefs, 2006, 53(8), pp.632 – 636
- [4] H. H. Alaeddine, E. H. Baghious and G. Madre et al., "Realization of multi-delay filter using Fermat number transforms", IEICE Trans. Fundamentals, 2008, E91A(9), pp. 2571-2577
- [5] L. M. Leibowitz, "A simplified binary arithmetic for the Fermat number transform," IEEE Trans. Acoustics Speech and Signal Processing, 1976, 24(5):356-359
- [6] C. Cheng, K.K. Parhi, "Hardware efficient fast DCT based on novel cyclic convolution structures", IEEE Trans. Signal processing, 2006, 54(11), pp. 4419- 4434
- [7] K. Prasad and K. K. Parhi, "Low-power 4-2 and 5-2 compressors," in Proc. of the 35th Asilomar Conf. on Signals, Systems and Computers, vol. 1, 2001, pp. 129–133.
- [8] C. H. Chang, J. Gu, M. Zhang, "Ultra low-voltage low-power CMOS 4-2 and 5-2 compressors for fast arithmetic circuits" IEEE Transactions on Circuits and Systems I: Regular Papers, Volume 51, Issue 10, Oct. 2004 Page(s):1985 – 1997
- [9] H. T. Vergos, C. Efstathiou, D. Nikolos, "Diminished modulo $2n + 1$ adder design", IEEE Trans. Computers, 2002, 51(12), pp. 1389-1399
- [10] C. Efstathiou, H. Vergos, G. Dimitrakopoulos, et al., "Efficient diminished-1 modulo $2n + 1$ multipliers", IEEE Trans. Computers, 2005, 54(4), pp. 491-496
- [11] M. Nagamatsu, S. Tanaka, J. Mori, et. al. "15-ns 32×32 -b CMOS multiplier with an improved parallel structure", IEEE Journal of Solid-State Circuits, 1990, 25(2), pp. 494-497

Books

- [12] Essentials of VLSI Circuits and systems by Kamran Eshraghian, Douglas A. Pucknell, Sholeh Eshraghian.
- [13] Modern VLSI Design, System - on - Chip Design Third Edition Wayne Wolf, Pearson Education.
- [14] Barbe, D.F. (Ed.) (1982) Very Large Scale Integration – Fundamentals and applications, Springer - Verlag, West Germany / USA.