Abstract—The low power high speed parallel architecture for cyclic convolution based on fermet number transform (FNT) operated at ultra low voltages are presented. The power consumption, Delay and Area of this new novel 4-2 Compressor Architecture is compared with Existing architecture.

Therefore the proposed 4-2 compressor architectures shows better performance. In the proposed architecture the outputs are efficiently used to improve Low power, high speed, performance, and less delay. 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. To perform the (FNT) and (IFNT) the techniques used are code Conversion method without Addition (CCWA) and Butterfly Operation without Addition (BOWA). Here the Point wise Multiplication in the Convolution is accomplished by Modulo $2^t n + 1$ Partial Products Multipliers (MPPM) and Output partial products which are Inputs to the IFNT. Thus Modulo $2^t n + 1$ Carry save Propagation Additions are avoided in the FNT and the IFNT except their final stages and the Modulo $2^t n + 1$ 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. This will be done by using Very Large Scale Integration (VLSI) technology. The synthesis results using 180nm SOC Technology is been used. Therefore the proposed one has less Power better Throughput Performance and involves less hardware complexity.

I. INTRODUCTION

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]

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 their 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. 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 in FNT with its integer power 2. Fermat number is a positive integer of the form $F_n=2^{2^t}$ 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 nppm. The CCWA and BOWA both consists of novel modulo $2^n+1$ 4-2 compressor in the diminished-1 representation of X i.e., $X = X - 1$[9].

II. CODE CONVERSION WITHOUT ADDITION

It is 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 been performed by modulo $2^n+1$ 4-2 compressor.

10, 11, 12, 13 are four inputs applied to modulo $2^n+1$ 4-2 compressor. Outputs obtained are sum vector $H_0^*$ and carry vector $H_1^*$ in the diminished-1 representation [5].

- 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

As we used two full adder the complexity increases and power is more, area occupied is more delay is more. In order to Obtain Low power high speed, less area we proposed Novel Architecture of xor-xnor, mux style 4-2 compressor [6].

- 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 existing one.

III. 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.

IV. 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 Dadda tree [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.

V. 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 $\{B_i\}$ ($i=1, 2 \ldots N-1$). 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.

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

![Parallel FNT structure](image)

![Parallel IFNT structure](image)

Fig 6: Structures for FNT and IFNT ($N=2^N+1$)

It has $\log_2N+1$ stages of operations.

The efficient FNT structure involves $\log_2N+1$ 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 $\log_2N-1$ 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.

Implementation:

4-2 compressor and also for the existing architecture in order 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.

IMPLEMENTATION:

VERILOG CODE

SIMULATION

SYNTHESIS

LOW POWER CIRCUIT

LAYOUT

PHYSICAL DESIGN WITH ASIC FPGA AND SOC

RESULTS OF OLD FULL ADDER 4-2 COMPRESSOR:

RESULTS OF PROPOSED 4-2 COMPRESSOR:

Existing compressor RTL POWER

Proposed 4-2 compressor RTL POWER
REFERENCES


