FIR FILTER DESIGN BASED ON LOW LATENCY SYSTOLIC MONTGOMERY MULTIPLIER

[1]**R.AMBIKA,** ***Assistant Professor,***
Dept of electronics and communication, PSNA CET, dindigul, Tamilnadu, INDIA
ambika.theni@gmail.com

Abstract **-In this paper the Finite Impulse Response (FIR) is designed using the montgomery multiplier. This multiplier is widely used in many cryptographic applications like RSA and elliptic curve cryptography. Here the multiplication is decomposed into number of independent units using an efficient algorithm to introduce the parallel processing. To reduce the latency a novel pre computed addition technique is followed. Since the Montgomery is a systolic multiplier it contains the features of regularity, modularity and unidirectional data flow and more suitable for VLSI design implementations. The important characteristic of this multiplier is it has an inbuilt truncation which compresses the LSB part and also consumes less area and power than existing designs. The proposed multiplier have clock cycle latency of (2N-1) where N=(m/L), m is the word size and L is the digit size.**

Keywords-**FIR, Montgomery multiplier, Truncation**

1. INTRODUCTION

Finite-Impulse-Response (FIR) digital filters are widely used as it plays a vital role in various digital signal processing (DSP) applications [1]. Although the FIR filter contains a guaranteed stability and linear phase, it has the higher complexity and power consumption than that of the infinite impulse response (IIR) filter. To design low complexity and low-power linear phase FIR filters many efforts have been practiced. Real-time realization of these filters with desired level of accuracy is a challenging task as the complexity of FIR grows with the filter order. The precision of computation is also an important factor in signal processing. The main area and power minimization can be obtained by using multiplier. Polynomial basis multipliers are popularly used because they are relatively simple to design, and offer scalability for the fields of higher orders. Efficient hardware design for polynomial-based multiplication is therefore important for real-time applications [2].

Systolic designs represent an attractive architectural paradigm for efficient hardware implementation of computation intensive DSP applications. It has the features like simplicity, regularity and modularity of structure. In addition, by using pipelining or parallel processing it possess significant potential to yield high-throughput rate by exploiting high-level of concurrency. For high speed VLSI implementation, the architecture based on polynomial basis (PB) multiplier is followed. Such architecture is a systolic array in which, a basic cell is repeated in an array and signals flow unilaterally between neighbors. It requires large area and latency for fully pipelined operation. PB systolic array multipliers can be classified into four categories: bit-serial, bit-parallel, hybrid, and digit-serial. Bit-serial architecture has minimum area and minimum throughput among all the categories. Bit parallel has largest area and maximum throughput. For moderate throughput and resource constrained application, hybrid, and digit serial architectures are used. In digit serial architecture, an m bit word is broken into N=(m/L) digits. In every clock cycle, "L" bits of multiplier and multiplicand are processed to produce one m-bit product every N cycles.

2. TRUNCATED MULTIPLIER WITH PP TRUNCATION AND COMPRESSION

The proposed truncated multiplier consists of several operations such as deletion, reduction, truncation, rounding, and final addition as shown in fig 1. The first step of deletion operation is performed which removes all the unnecessary PP bits. Those bits are those which are need not to be generated, are deleted. An example of 8 × 8 unsigned fractional multiplication is considered here which is in the form of eight product bit truncation. The next step is deletion, where as many possible PP bits are deleted till the deletion error of E_D' is bounded by $-1/2$ ulp $\leq$

$E_D' \leq 0$. 1/4 ulp leads the deletion error as −1/4 ulp ≤ The correction bias constant injection [4] of ED'≤1/4 ulp. Per-column reduction is performed after the deletion of PP bits, and two rows of PP bits is generated.

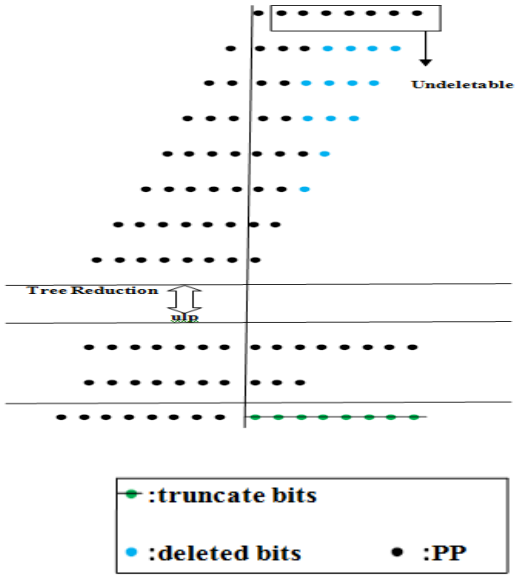


Fig 1: 8 × 8 truncated multiplication with eight product bits truncated-Deletion, reduction, truncation, and rounding plus final addition.

Next the truncation is performed in which the first row of n − 1 bits from column 1 to column n – 1 is removed. Truncation error of $-1/2 \text{ ulp} < E_T' \leq 0$ is introduced by truncation. The truncation error is, adjusted by injection of another bias constant [6] of 1/4 ulp where the error is bounded by $-1/4 \text{ ulp} < E_T' \leq 1/4 \text{ ulp}$. The completion of deletion, reduction, and truncation, the addition of PP bits is done using a CPA which generates the final product of P bits. The bits left after deletion and truncation can be safely removed before final addition as they do not affect the carry bit to column n + 1 during the rounding process. A final bias constant [8] of 1/2 ulp is added before addition by CPA to achieve the rounding error as $-1/2 \text{ ulp} < E_R' \leq 1/2 \text{ ulp}$.The rounding process involves the removal of bit at column n after the final CPA .Thus the faithfully rounded truncated multiplier has the total error of $-\text{ulp} < E = (E_D + E_T + E_R) \leq \text{ulp}$. As the total error is no more than 1 ulp [6] the proposed truncated multiplier design achieves faithful rounding. Furthermore, the three bias constants 1_D, 1_T and 1_R, finally can be collected and added as a single constant bit column n + 1, as the overall height of the PP matrix should not be increased. The overall filter design using the truncated multiplier requires an adder and a delay element to complete the design.

3. PROPOSED FILTER DESIGN USING MONTGOMERY MULTIPLIER

The proposed filter design using Montgomery multiplier follows the bit parallel systolic architecture. This structure consists of four systolic arrays, as each array correspond to one of the unit. The first systolic array consists of 5 PEs. Where as four PEs and a delay cell are present in the second, third, and fourth systolic arrays.

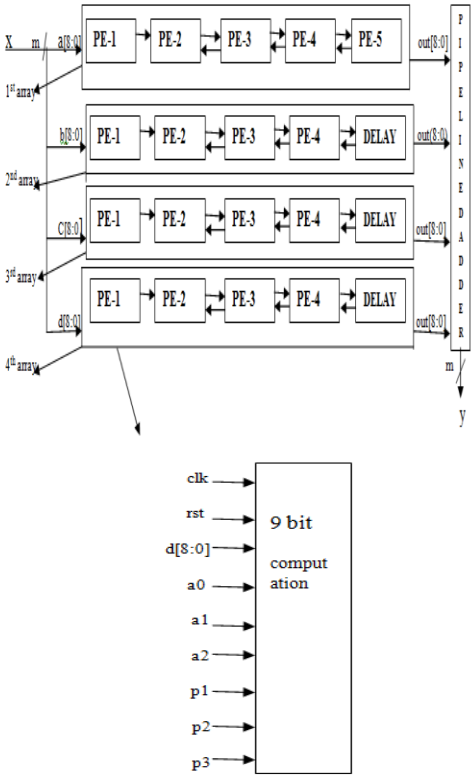
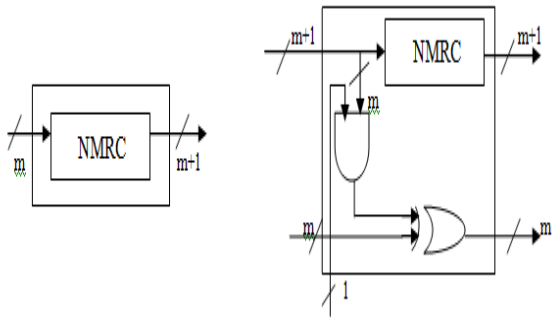


Fig 2: Proposed Systolic Structure

Here to meet the data dependence requirement the delay cell is required. Besides a systolic adder for the final addition of the four arrays can also be used which consists of four addition cells (ACs).We can also use a pipelined adder-tree for a low latency implementation which consists of three ACs[2]. Concurrently, the four arrays receive the data and functions. Hence the adder tree receives its first input after five cycles and in two cycles yields its first output. The detailed design of the proposed structure of the PEs is shown in Fig 2. One NMR cell (NMRC) novel modular reduction cell is present in

the PE-1 array, as shown in Fig 3(a) The regular PE, consists of one AND cell, one XOR cell, and one NMRC as shown in Fig. 3(b). Bit multiplication and bit addition is computed by the AND cell and XOR cell." m" number of AND gates and XOR gates are working in parallel in each AND cell and XOR cell.



(a) (b)

Fig 3: (a) Design of PE-1 (b) Design of Regular PE

The duration of a PE is $T_X+T_{A=}\max(T_X,T_X+T_A)$, where T_A is the delay of an AND gate and T_x is the delay of NMRC[2]. The systolic signal flow graph which shows the multiplication process occurs in this Montgomery multiplier is given below in the fig 4.

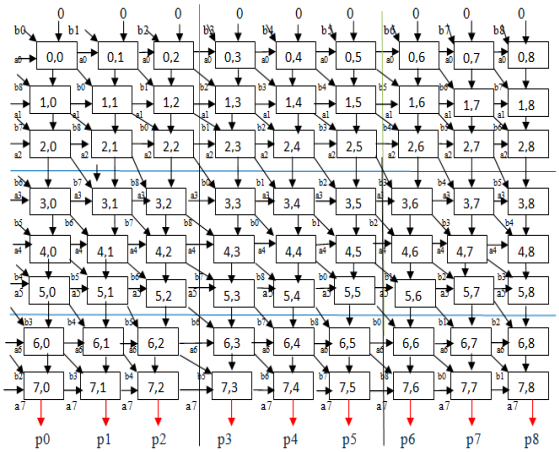


Fig 4: Systolic signal flow graph (SFG) for multiplication

Signal Flow Graph of Fig 4 is partitioned in both directions into a set of N basic cells [4].Each partition contains L*L basic cells. A D flip-flop is added to each signal line intersecting a dashed line at the point of intersection.

4. IMPLEMENTATION RESULTS

The FIR filter is designed using ISIM simulator with VHDL code and it is also implemented using Xilinx ISE Design Suite 13.2 in FPGA. The simulated screen shot is given in Fig 5.

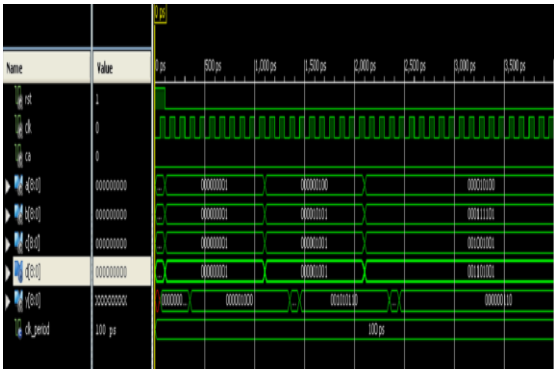


Fig 5: Screen Shot of Simulated Filter Output

Here the given input signal is divided and given to the arrays of PE as a,b,c and d.It gets processed alog the PEs and the final result of Y is obtained from the pipelined adder.The following figures show the synthesis result.

fir Project Status (02/20/2014 - 17:48:34)			
Project File:	firfilter.xise	Parser Errors:	No Errors
Module Name:	fir	Implementation State:	Placed and Routed
Target Device:	xc3s250e-5pq208	•Errors:	No Errors
Product Version:	ISE 13.2	•Warnings:	953 Warnings (953 new)
Design Goal:	Balanced	•Routing Results:	All Signals Completely Routed
Design Strategy:	Xilinx Default (unlocked)	•Timing Constraints:	All Constraints Met
Environment:	System Settings	•Final Timing Score:	0 (Timing Report)

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	151	4,896	3%	
Number of 4 input LUTs	119	4,896	2%	
Number of occupied Slices	163	2,448	6%	
Number of Slices containing only related logic	163	163	100%	
Number of Slices containing unrelated logic	0	163	0%	
Total Number of 4 input LUTs	150	4,896	3%	
Number used as logic	119			
Number used as a route-thru	31			
Number of bonded IOBs	47	158	29%	
Number of BUFGMUXs	1	24	4%	
Average Fanout of Non-Clock Nets	1.95			

Fig 6: Area Analysis Of FIR filter

The above power and delay analysis result shows that the power consumption by this design is about 0.804W and delay is about 5.690ns.

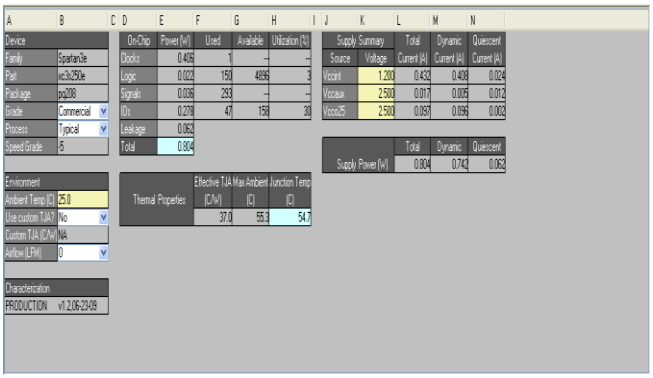


Fig 7: Power Requirement Of FIR Filter

```
--------------------------------------------------------------------------------
Delay:               5.690ns (Levels of Logic = 11)
  Source:            n_2 (FF)
  Destination:       n_0 (FF)
  Source Clock:      clk rising
  Destination Clock: clk rising

  Data Path: n_2 to n_0
                              Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDR:C->Q             4    0.514   0.651  n_2 (n_2)
     LUT4:I0->O           1    0.612   0.000  Mcompar_e_cmp_le0000_lut<0>
     MUXCY:S->O           1    0.404   0.000  Mcompar_e_cmp_le0000_cy<0>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<1>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<2>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<3>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<4>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<5>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<6>
     MUXCY:CI->O          1    0.052   0.000  Mcompar_e_cmp_le0000_cy<7>
     MUXCY:CI->O          2    0.289   0.380  Mcompar_e_cmp_le0000_cy<8>
     INV:I->O            32    0.612   1.073  n_not00011_INV_0 (n_not0001)
     FDR:R                      0.795          n_0
    ----------------------------------------
    Total                      5.690ns (3.586ns logic, 2.104ns route)
                                       (63.0% logic, 37.0% route)
```

Fig 8: Delay Analysis

5. CONCLUSION

This paper describes the design and implementation of FIR filter design using systolic montgomery multiplier. The following table provides the comparison between different filter design using truncated and Montgomery multiplier.

Table 1 Comparative Analysis

Design	Area	Power	Delay
FIR filter Using Truncated Multiplier	61 FA 1 HA	2.141W	12.850ns
FIR filter Using Montgomery Multiplier	59 FA 4 HA	0.804W	5.690ns

Thus the FIR filter based on Montgomery multiplier offers better power and latency results than earlier design.

6. REFERENCES

[1]Pramod Kumar Meher, *Senior Member, IEEE*, Shrutisagar Chandrasekaran, *Member, IEEE*, and Abbes Amira, *Senior Member, IEEE* "FPGA Realization of FIR Filters by Efficient and Flexible Systolization Using Distributed Arithmetic" IEEE Transactions On Signal Processing, Vol. 56, No. 7, July 2008 3009

[2] Jiafeng Xie, Jian jun He, and Pramod Kumar Meher "Low Latency Systolic Montgomery Multiplier for Finite Field Based on Pentanomials "IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 21, No. 2, February 2013 385

[3]Shen Fu Hsiao, Jun Hong Zhang Jian, and Ming Chih Chen,"Low Cost FIR Filter Designs Based on Faithfully Rounded Truncated Multiple Constant Multiplication/Accumulation,"*IEEE transactions on circuits and systems II*: Exp.Briefs, vol. 60, No. 5, May 2013

[4] Somsubhra Talapatra, Hafizur Rahaman, and Jimson Mathew"Low Complexity Digit Serial Systolic Montgomery Multipliers for Special Class of GF(2^m)" IEEE Transactions On Very Large Scale Integration (Vlsi) Systems, Vol. 18, No. 5, May 2010.

[5]C.-Y. Lee, J.-S. Horng, I.-C. Jou, and E.-H. Lu, "A digit-serial multiplier for finite field GF(2^m) ," *IEEE Trans. Very Large Scale Integr.(VLSI) Syst.*, vol. 13, no. 4, pp. 476–483,Apr.2005.

