ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Design and Implementation of the Algorithm for RB Multiplication to Derive High-Throughput Digit-Serial Multipliers

V.Latha
honeyvlatha@gmail.com
M.Tech (VLSI Design)
Department of ECE
Sri Venkatesa Perumal College of Engineering & Technology,
R.V.S.Nagar, K.N.Road,
Puttur, Chittoor, AP-517583.

Mr.G.Sunil, M.Tech
sunilgone@gmail.com
Associate Professor
Department of ECE
Sri Venkatesa Perumal College of Engineering & Technology,
R.V.S.Nagar, K.N.Road,
Puttur, Chittoor, AP-517583.

Abstract
Redundant basis(RB) multipliers over Galois Field(GF(2^m)) have gained huge popularity in elliptic curve cryptography (ECC) mainly because of their negligible hardware cost for squaring and modular reduction.Different techniques used so far for theimplementation of redundant basis (RB) multipliers over Galois Field are explored here. Based on review the Word Level Redundant Basis (RB) multiplier is the most efficient among all multipliers in terms of hardware utilization.To obtain high throughput digit serial implementation an efficientrecursive decomposition algorithm was implemented here.The digit serial Redundant Basismultiplication in a bit level matrix vector form is most efficient in terms of area-time complexities.

Keywords- ***Galois Fields (GF (2^m)), Redundant Basis (RB) multiplier,High throughput.***

I.INTRODUCTION

Multiplication over GF(2^m) is a basic operation frequently came across in modern cryptographic systems such as the EllipticCurve Cryptography(ECC) and error control coding [1]–[3]. Also multiplication over a Galois field can be used to perform other field operations,e.g.division, exponentiation, and inversion [4]–[6].Arithmetic operations in the GF(2^m) have several applications incomputer algebra and theory of coding, data manipulations.Multiplication over GF(2^m) can be implemented on a general purpose machine, but it is expensive to use a general purpose machine to implement cryptographic systems in cost sensitive consumer products. As compared to the order of GF(2^m) the word length of low end microprocessors used in cryptographic systems is too small, therefore,they cannot meet the real time requirements of different applications. Most of the real-time applications, therefore, need hardware implementation of GF(2^m) arithmetic operations for the benefits like low-cost and high-throughput rate.

There are different types of basis to represent field elements, those are polynomial basis, normal basis, triangular basis and redundant basis,and the choice of representation of field elements has a major impact on the performance of the arithmetic circuits [7]–[9], [15]. Several algorithms for basic arithmetic operations in GF(2^m) are suitable for both hardware and software implementations have beenrecently developed.

Because of several advantages of the RB based attention in recent years.Like normal basis multipliers, RB multipliers offer free squaring,they also involve lower computational complexity and can be implemented in highly regular computing structures [10]– [14].Several digit-level serial/parallel structures for RB multiplier over GF(2^m) have been reported in the last few years[10]–[14].An efficient serial/parallel multiplier using redundant representation has been

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

presented [10].A bit serial word parallel(BSWP) architecture for RB multiplier has been reported[11].Several other RB multipliers have also been developed for reducing the complexity of implementation and for high-speed realization [12]–[14].In this paper,we aim at presenting efficient digit level serial/parallel designs for high-throughput finite field multiplication over based on RB.We have proposed an efficient recursive decomposition scheme for digit-level RB multiplication,and based on that we havederived parallel algorithms for high throughput digitserial multiplication.We have mapped the algorithm to three different high speed architectures by mapping the parallel algorithm to a regular 2-dimensional signal- flow graph (SFG) array,followed by suitable projection of SFG to 1-dimensional processor-space flow graph (PSFG), and the choice of feed-forward cut-set to enhance the throughput rate.

Our proposed digit-serial multipliers involve significantly less area-time-power designs.Field complexities than the corresponding existing programmable gate array (FPGA) has evolved as a mainstream dedicated computing platform. The hardware utilization efficiency and throughput of exist structure so can be improved by efficient design of algorithm.

II.THERECURSIVE DECOMPOSITION DIGIT SERIAL MULTIPLICATION ALGORITHM

Inputs: A and B are the pair of elements in GF(2^m) to be multiplied.
Output:C=A.B
1. Initialization
1.1 Y=0;
2.Multiplication
2.1 For u=0 to Q-1
2.2 $Y=Y+BuAu^T$
End For
End For
3.Final step
C=Y
A bit level matrix vector form

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} b_0 & b_{n-1} & \cdots & b_1 \\ b_1 & b_0 & \cdots & b_2 \\ \vdots & \vdots & \ddots & \vdots \\ b_{n-1} & b_{n-2} & \cdots & b_0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}.$$

III.DERIVATION OF PROPOSED HIGH THROUGHPUT STRUCTURE FOR RB MULTIPLIERS

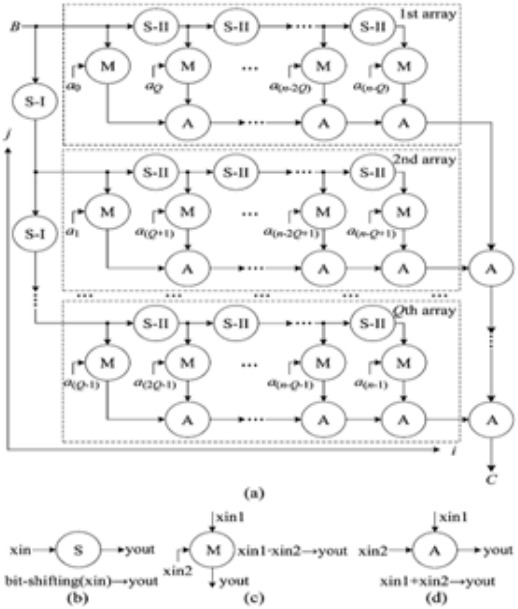


Fig.1. Signal- flow graph (SFG) for parallel realization of RB multiplication.(a)The proposed SFG.(b) Functional description of S node,where S-I node performs circular bit-shifting of one position and S-II node performs circular bit-shifting by positions.(c) Functional description of M node.(d) Functional description of A node.

The RB multiplication can be represented by the 2-dimensional SFG (shown in Fig.1) consisting of parallel arrays, where each array consists of bit-shifting nodes (S node), multiplication nodes (M nodes) and addition nodes (A nodes). There are two types of S nodes (S-I node and S-II node). Function of S nodes is depicted in Fig.1(b),where S-I node performs circular bit-shifting by one position and S-II node performs circular bit- shifting by positions for the degree reduction requirement. Functions of M nodes and A nodes are depicted in Fig.1(c) and 1(d),

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

respectively. Each of the M nodes performs an AND operation of a bit of serial-input operand A with bit-shifted form of operand B, while each of the A nodes performs an XOR operation.

The final addition of the output of arrays of Fig. 1 can be performed by bit-by-bit XOR of the operands innumber of A nodes as depicted in Fig. 1. The desired product word is obtained after the addition of parallel output of the arrays.

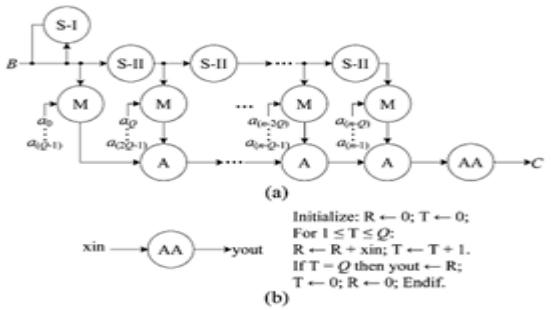


Fig2. Processor-space flow graph (PSFG) of digit-serial realization of finite field RB multiplication overGF(2^m).(a)The proposed PSFG.(b)Functional description of add- accumulation (AA) node.

For digit-serial realization of RB multiplier, the SFG of Fig. 1 can be projected along j-direction to obtain a PSFG as shown in Fig. 2, where input bits are loaded in parallel to multiplication nodes during each cycle period. The functions of nodes of PSFG are the same as those of corresponding nodes in the SFG of Fig. 1 except an extra add-accumulation (AA) node. The function of the AA node is, as described in Fig. 2(b), to execute the accumulation operation for Q cycles to yield the desired result thereafter.

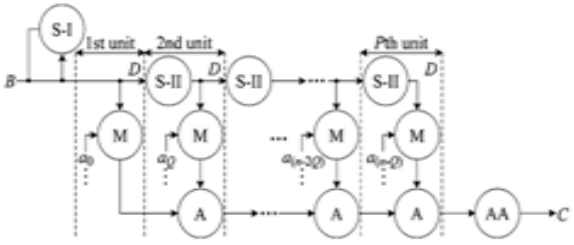


Fig. 3. Cut-set retiming of PSFG of finite field RB multiplication over (GF(2^m)) Where "D " denotes delay.

For efficient realization of a digit-serial RB multiplier, we can perform feed-forward cut-set retiming in a regular interval in the PSFG as shown in Fig. 3. As aresult of cut-set retiming of the Fig. 3, the minimum duration of each clock period is reduced to(TA+TX), whereTA andTX denote the delay of an AND gate and XOR gate.The PSFG of Fig.3 is mapped to the high throughput digit serial RB multiplier shown in fig.4 Referred to as proposed structure–I (PS-I).

Regular PPGU:

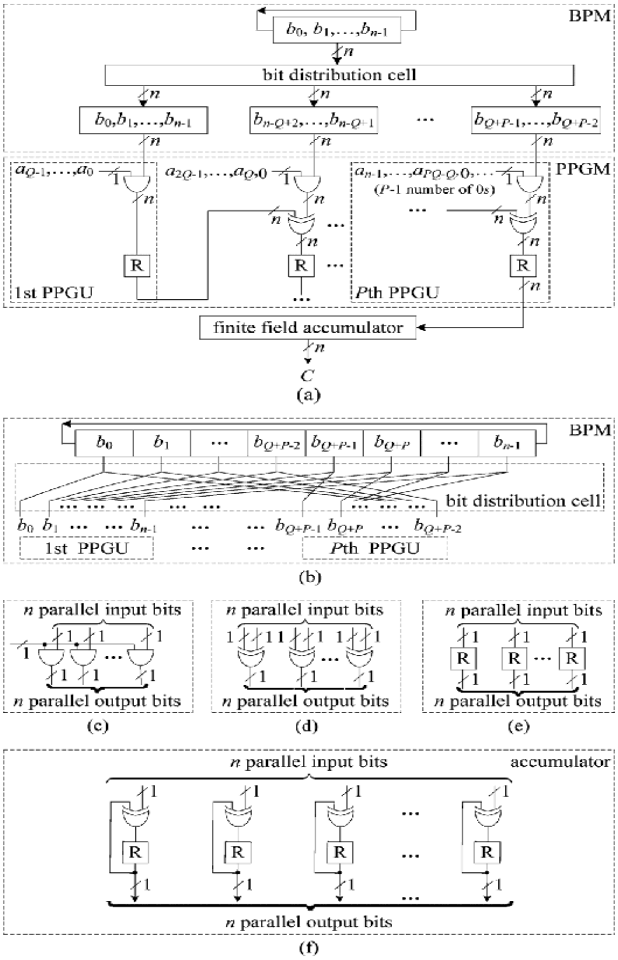


Fig.4.PS-I for RB multiplier where.(a)Structure of the RB multiplier.(b)Structure of the bit permutation module (BPM). (c)Structure of AND cell in PPGM . (d)Structure of XOR cell in PPGM.(e)Structure of register cell in PPGM.(e)Structure of register cell in PPGM.(f)Structure finite field accumulator.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

PS-I contains bit permutation module (BPM),partial product generation(PPGM)and finite field accumulatormodule.Operand B to feed its output topartial product generation units (PPGU) s according to the S nodes of PSFG of Fig. 3, as shown in Fig. 4(b).

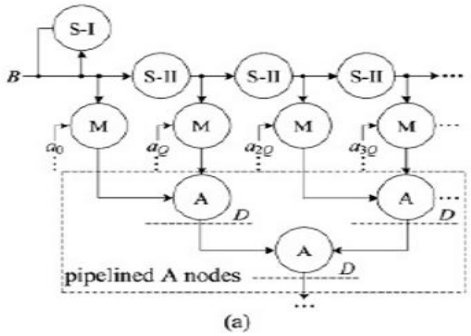
The AND cell, XOR cell and register cell of PPGM perform the function of M node, A node and delay imposed by the retiming of PSFG of Fig.3, respectively .Structures and functions of AND cell, XOR cell an register cell are shown in Fig. 4(c), (d), and (e), respectively. The input operands are fed to PPGU in staggered manner to meet the timing requirement in systolic pipeline.

The accumulator consists of parallel bit-level accumulation cells [as shown in Fig. 4(f)].The newly received input is then added with the previously accumulated result and the result is stored in the register cell to be used during the next cycle. The duration of minimum cycle period of the PS-I is(TA+TX) .The successive output are produced at the interval of Q cycles thereafter.

The pipelined XOR tree:

We can further transform the PSFG of Fig. 3 to reduce the latency and hardware complexity of PS-I.To obtain the proposed structure, serially-connected A nodes of the PSFG of Fig. 3 are merged into a pipeline form of A nodes as shown within the dashed-box in Fig. 5(a).

These pipelined A nodes can be implemented by a pipelined XOR tree, as shown in Fig. 5(b).



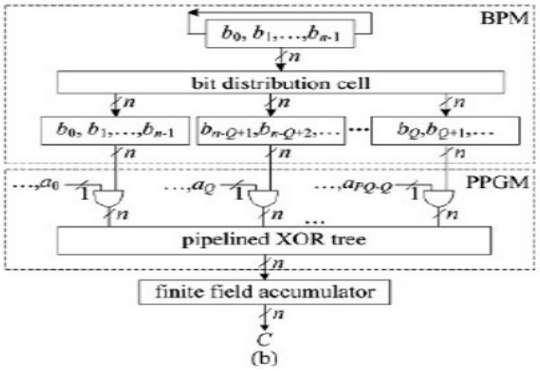


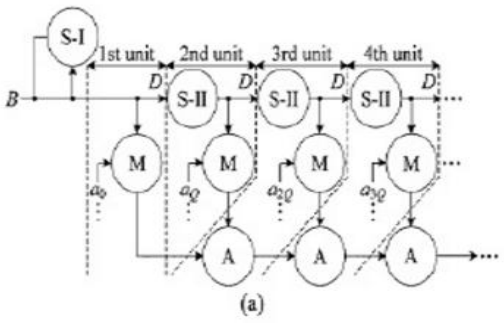
Fig.5.The pipelined tree for RB multiplier, where (a) Modified PSFG.(b) Structure of RB multiplier.

Since all the AND cells can be processed in parallel, there is no need of using extra "0"s on the input path to meet the timing requirement in systolic pipeline. The critical path and throughput of PS-II are the same as those of PS-I. Similarly, PS-II can be easily extended to larger values of d to have low register-complexity structures.

They have been derived for area constrained implementation and particularly for implementation in FPGA platform where registers are not abundant. The results of synthesis show that proposed structures can achieve saving of up to 94% and 60%, respectively, of ADPP for FPGA and ASIC implementation, respectively, over the best of the existing designs.

Novel Cut-set retiming:

Since the S nodes of Fig.3 perform only the bit-shifting operations they do not involve any time consumption.Therefore, we can introduce a novel cut-set retiming to reduce the critical path further,as showninFig.6(a).



ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

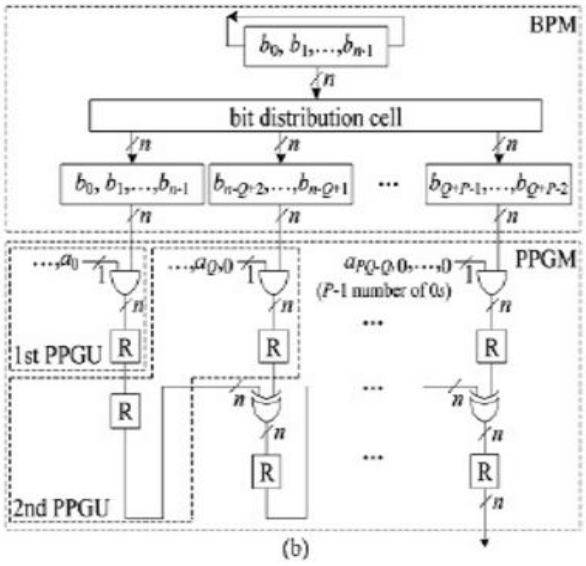


Fig.6. Novel cut-set retiming of PSFG and its corresponding structure:PS-III.(a) Cut-set retiming. (b) BPM and PPGM of PS-III.

It can be observed that the cut-set retiming allows to perform the bit-addition and bit-multiplication concurrently, so that the critical-path is reduced to $\max\{T_A,T_X\}=T_X$, i.e ,the throughput of the design is increased.It consist of (P+1)PPGUs .The proposed structure yields the first output of desired result (P+Q+1) cycles after the first input is fed to the structure,while the successive outputs are available in each Q cycles.

The proposed structures have different area-time-power trade-off behavior. Therefore, one out of the three proposed structures can be chosen depending on the requirement of the application environments.

IV. EXPERIMENTAL RESULTS

The simulation process has been carried out for different architectures.The simulation has been extended up to our requirement i.e.32-bit. The code has been written in Verilog hardware description language.

The top module has been synthesized and simulated in Xilinx ISE Design Suite 10.1 andModelsim 6.4b.The design was implemented in Spartan-3E kit.

Simulation results:

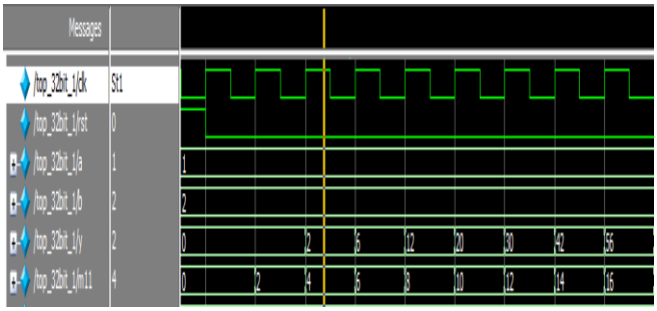


Fig.7.Simulation results of merged regular PPGU

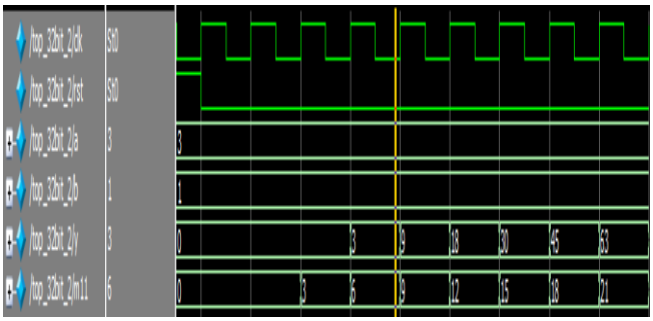


Fig.8.Simulation results of pipelined tree:

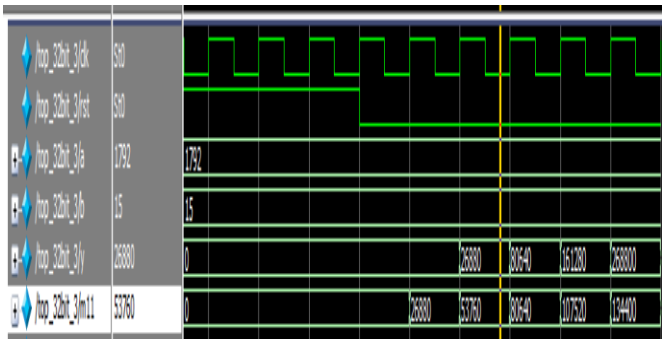


Fig.9.Simulation results of novel cut-set retiming:

RTL Schematics:

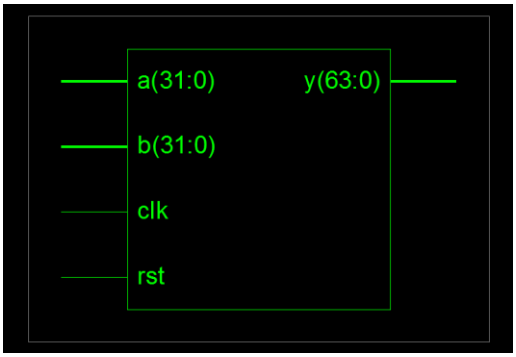


Fig.10.Schematic diagram of merged regular PPGU

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

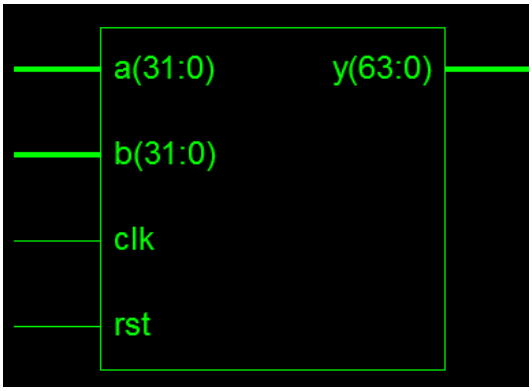


Fig.11.Schematic diagram of pipelined tree

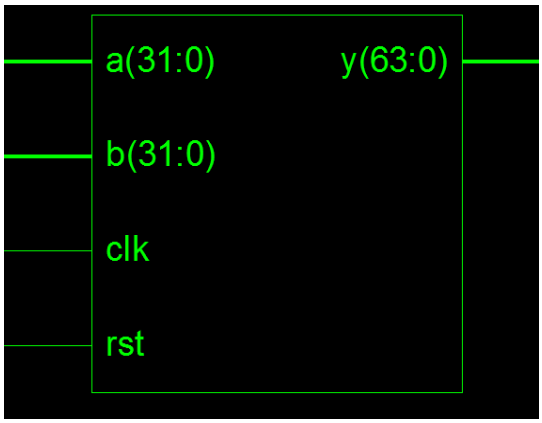


Fig.12.Schematic diagram of novel cut-set retiming

Technology Schematics:

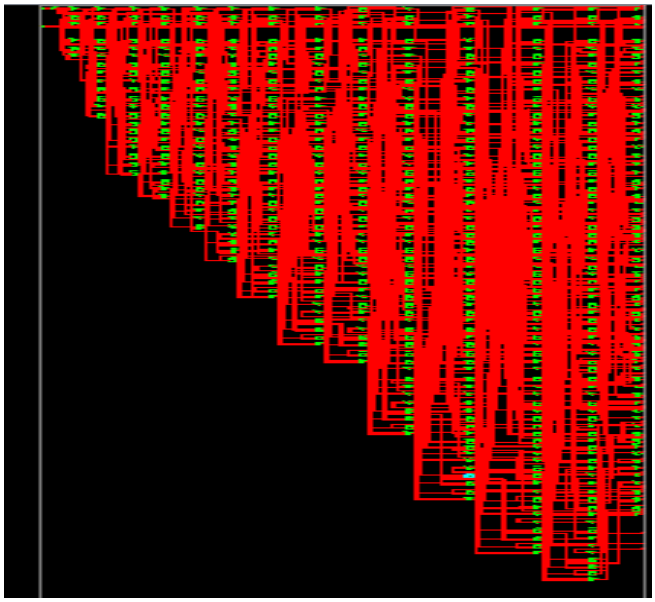


Fig.13.Technology schematic of merged regular PPGU

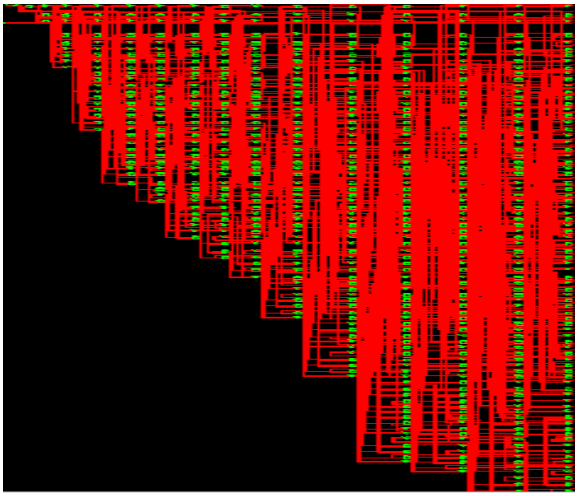


Fig.14.Technology schematic of pipelined tree:

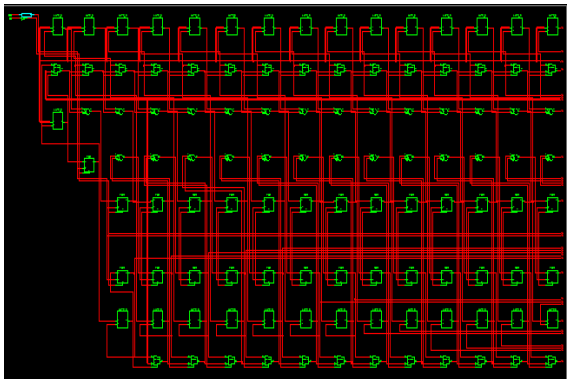


Fig.15.Technology schematic of novel cut-set retiming:

Table I:Comparisons of three techniques:

Device utilization summary and delay			
Logic Utilization	Regular PPGU	Pipelined tree	Cut-set retiming
Number of Slices:	1142	1580	195
Number of Slice Flip Flops:	192	448	192
Number of 4 input LUTs:	2068	2788	272
Number of bonded IOBs:	130	130	130
Number of GCLKs:	1	1	1
Minimum period:	10.592ns	10.592ns	10.592ns

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

V.CONCLUSION

Here a novel recursive decomposition algorithm for RB multiplication to derive high-throughput digit-serial multipliers was implemented.Digit serial RB multiplication in a bit level matrix vector form is most efficient in terms of area-time complexities.By suitable projection of SFG of proposed algorithm and identifying suitable cut-sets for feed-forward cut-set retiming, three novel high- throughput digit-serial RB multipliers are derived to achieve significantly less area-time-power complexities than the existing ones. Moreover, efficient structures with low register countproposed structures can be chosen depending on the requirement of the application environments.

BIBLIOGRAPHY

[1] I. Blake, G. Seroussi, and N. P. Smart, Elliptic Curves in Cryptography, ser. London Mathematical Society Lecture Note Series.. Cambridge, U.K.: Cambridge Univ. Press, 1999.

[2] N. R. Murthy and M. N. S. Swamy, "Cryptographic applications of brahmaqupta-bhaskara equation," IEEE Trans. Circuits Syst. I, Reg.Papers, vol. 53, no. 7, pp. 1565–1571, 2006.

[3] L. Song and K. K. Parhi, "Low-energy digit-serial/parallel finite field multipliers," J.VLSI Digit.Process., vol. 19, pp. 149–C166, 1998.

[4] P. K. Meher, "On efficient implementation of accumulation in finite field over and its applications," IEEE Trans. Very Large ScaleIntegr. (VLSI) Syst., vol. 1 7, no. 4, pp. 541–550, 2009.

[5] L. Song, K. K. Parhi, I. Kuroda, and T. Nishitani, "Hardware/software codesign of finite field datapath for low-energy Reed-Solomncodecs,"IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 8, no. 2, pp. 160– 172, Apr. 2000

[6] G. Drolet, "A new representation of elements of finite fieldsyielding small complexity arithmetic circuits," IEEE Trans.Comput.,vol. 47, no. 9, pp. 938–946, 1998.

[7] C.-Y. Lee, J.-S.Horng, I.-C.Jou, and E.-H. Lu, "Low- complexitybit-parallel systolic montgomery multipliers for special classes of ," IEEE Trans. Comput., vol. 54, no. 9, pp. 1061–1070, Sep.2005.

[8] P. K. Meher, "Systolic and super-systolic multipliers for finite field based on irreducible trinomials," IEEE Trans. Circuits Syst.I, Reg. Papers, vol. 55, no. 4, pp. 1031–1040, May 2008.

[9] J. Xie, J. He, and P. K. Meher, "Low latency systolic montgomery multiplier for finite field based on pentanomials," IEEE Trans.Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 2, pp.385–389, Feb. 2013.

[10] H. Wu, M. A. Hasan, I. F. Blake, and S. Gao, "Finite field multiplier using redundant representation," IEEE Trans. Comput., vol. 51, no. 11,pp. 1306–1316, Nov. 2002.

[11] A. H. Namin, H. Wu, and M.Ahmadi, "Comb architectures for finite field multiplication in F_{2m} ," IEEE Trans. Comput., vol. 56, no. 7, pp. 909–916, Jul. 2007.

[12] A. H. Namin, H. Wu, and M. Ahmadi, "A new finite field multiplier using redundat representation," IEEE Trans. Comput.,vol. 57,no. 5,pp.716–720, May 2008

[13] A. H. Namin, H. Wu, and M. Ahmadi, "A high-speed word level finite field multiplier in F_{2m} using redundant representation," IEEE Trans.Very Large Scale Integr.(VLSI)Syst.,vol.17, no.10,pp.1546–1550,Oct. 2009.

[14] A. H.Namin,H.Wu, and M.Ahmadi, "An efficient finite field multi-plier using redundant representation," ACM Trans. Embedded Comput.Sys., vol. 11, no. 2, Jul. 2012, Art. 31.