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

Efficient Implementation of Bit Parallel Finite Field Multiplier Using Redundant Basis

Vasam Sathish
Department of Electronics & Communication Engineering,
DVR College of Engineering and Technology,
Hyderabad, Sangareddy District, Telangana, 502283, India.

Abstract:
Redundant basis (RB) multipliers over Galois Fieldhave gained huge popularity in elliptic curve cryptography(ECC) mainly because of their negligible hardware cost forsquaring andmodular reduction.we have proposed anovel recursive decomposition algorithm for RB multiplication to obtain high-throughput digit-serial implementation. Through efficient projection of signal-flow graph (SFG) of the proposed algorithm,a highly regular processor-space flow-graph (PSFG) is derived.By identifying suitable cut-sets, we have modified the PSFGsuitably and performed efficient feed-forward cut-set retiming toderive three novel multipliers which not only involve significantlyless time-complexity than the existing ones but also require lessarea and less power consumption compared with the others. Boththeoretical analysis and synthesis results confirm the efficiency ofproposed multipliers over the existing ones. It is shown that theproposed structures are the best among the correspondingdesigns, for FPGA implementation. It is shownthat the proposed designs can achieve savingsof area-delay-power product (ADPP) on FPGA implementationover the best of the existing designs, respectively.

Index Terms— Digit-serial, Finite field multiplication,FPGA, High-throughput, redundant basis.

I.INTRODUCTION

Finite Field multiplication over Galois Field($GF(2^m)$is a basic operation frequently encountered inmodern cryptographicsystems such as the elliptic curve cryptography (ECC) and error control coding[1]-[3]. Moreover, multiplication overa finite field can be used further to perform other field operations,e.g., division, exponentiation, and inversion. Multiplicationover can be implemented on a general purposemachine, but it is expensive to use a general purpose machineto implement cryptographic systems in cost-sensitive consumerproducts. Besides, a low-end microprocessor cannot meetthe real-time requirement of differentapplications since wordlength of these processors is too small compared with the orderof typical finite fields used in cryptographic systems. Most of thereal-time applications, therefore, need hardware implementationof finite field arithmetic operations for the benefits like low-costand high-throughput rate.The choice of basis to represent field elements, namely thepolynomial basis, normal basis, triangular basis and redundantbasis (RB) has a major impact on the performance of the arithmeticcircuits [5]. The multipliers based on RB [6] havegained significant attention in recent years due to their severaladvantages. Not only do they offer free squaring, as normalbasis does, but also involve lower computational complexityand can be implemented in highly regular computing structures.Several digit-level serial/parallel structures for RB multiplierover have been reported in the last years afterits introduction by Wu *et al.* An efficient serial/parallelmultiplier using redundant representation has been presentedin [3]. A bit-serial word-parallel (BSWP) architecture for RBmultiplier has been reported. Several otherRB multipliers also have been developed for reducing the complexity of implementation andfor

Cite this article as: Vasam Sathish, "Efficient Implementation of Bit Parallel Finite Field Multiplier Using Redundant Basis", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 4 Issue 12, 2017, Page 181-187.

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

high-speed realization. We find that the hardware utilizationefficiency and throughput of existing structures of canbe improved by efficient design of algorithm and architecture.In this paper, we aim at presenting efficient digit-levelserial/parallel designs for high-throughput finite field multiplicationover based on RB. We have proposed an efficientrecursive decomposition scheme for digit-level RB multiplication,and based on that we have derived parallel algorithms forhigh throughput digit-serial multiplication. We have mapped thealgorithm to three different high-speed architectures by mappingthe parallel algorithm to a regular 2-dimensional signal-flowgraph (SFG) array, followed by suitable projection of SFG to1-dimensional processor-space flow graph (PSFG), and thechoice of feed-forward cut-set to enhance the throughput rate.Our proposed digit-serial multipliers involve significantly lessarea-time-power complexities than the corresponding existingdesigns. Field programmable gate array (FPGA) has evolved asa mainstream dedicated computing platform. FPGAs howeverdo not have abundant number of registers to be used in themultiplier.

Therefore, we have modified the proposed algorithmand architecture for reduction of register-complexity particularlyfor the implementation of RB multipliers on FPGA platform.Apart from these we also present a low critical-path digit-serialRB multiplier for very high throughput applications.

II. DERIVATION OF PROPOSED HIGH-THROUGHPUT STRUCTURES FOR RB MULTIPLIERS

In this section, we derive the proposed multipliers from theSFG of the proposed Algorithm 1.

A. Proposed Structure-I

The RB multiplication can be representedby the 2-dimensional SFG (shown in Fig. 1) consisting ofparallel arrays, where each array consists of bit-shiftingnodes (S node), multiplication nodes (M nodes) andaddition nodes (A nodes). There are two types of S nodes (S-Inode and S-II node). Function of

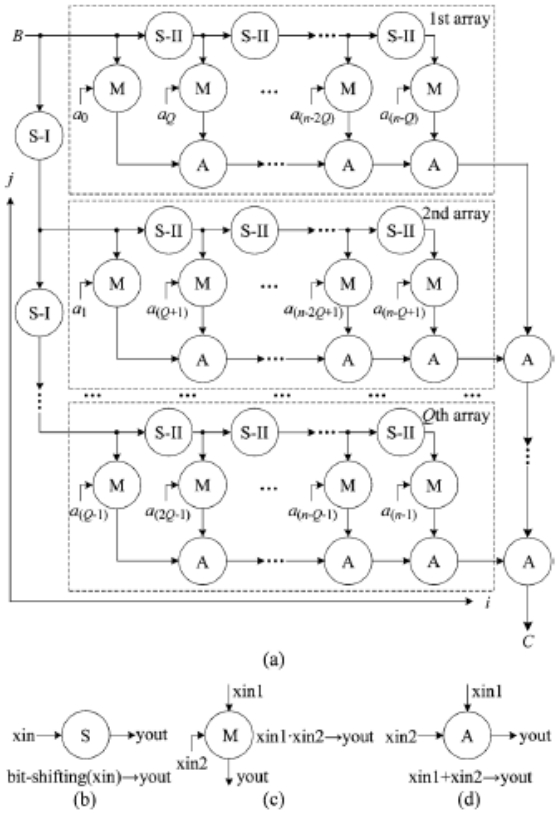

Fig. 1. Signal-flow graph (SFG) for parallel realization of RB multiplicationover based on (2) and (3). (a) The proposed SFG. (b) Functionaldescription of S node, where S-I node performs circular bit-shifting of one positionand S-II node performs circular bit-shifting by positions. (c) Functionaldescription of M node. (d) Functional description of A node.

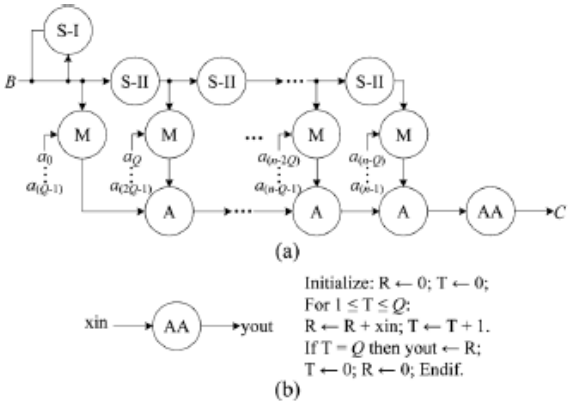

Fig. 2. Processor-space flow graph (PSFG) of digit-serial realization of finitefield RB multiplication over . (a) The proposed PSFG. (b) Functionaldescription of add-accumulation (AA) node.

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

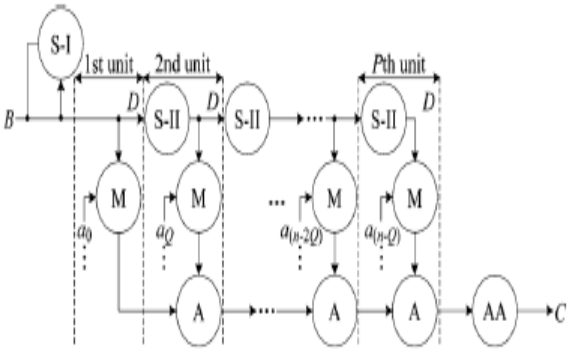

Fig. 3. Cut-set retiming of PSFG of finite field RB multiplication over, where denotes delay.

S nodes is depicted in Fig. 1(b),where S-I node performs circular bit-shifting by one position andS-II node performs circular bit-shifting by positions for the degreereduction requirement. Functions of M nodes and A nodesare depicted in Fig. 1(c) and 1(d), respectively.

Each of the Mnodes performs an AND operation of a bit of serial-input operandwith bit-shifted form of operand while each of the A nodesperforms an XOR operation. The final addition of the output ofarrays of Fig. 1 can be performed by bit-by-bit XOR of theoperands in number of A nodes as depicted in Fig. 1. Thedesired product word is obtained after the addition of paralleloutput of the arrays.For digit-serial realization of RB multiplier, the SFG of Fig. 1can be projected along -direction to obtain a PSFG as shown inFig. 2, where input bits are loaded in parallel to multiplicationnodes during each cycle period. The functions of nodes of PSFGare the same as those of corresponding nodes in the SFG of Fig. 1except an extra add-accumulation (AA) node. The function of theAA node is, as described in Fig. 2(b), to execute the accumulationoperation for cycles to yield the desired result thereafter.

For efficient realization of a digit-serial RB multiplier, we canperform feed-forward cut-set retiming in a regular interval in thePSFG as shown in Fig. 3. As a result of cut-set retiming of theFig. 3, the minimum duration of each clock period is reduced to, where and denote the delay of an AND gateand an XOR gate, respectively.

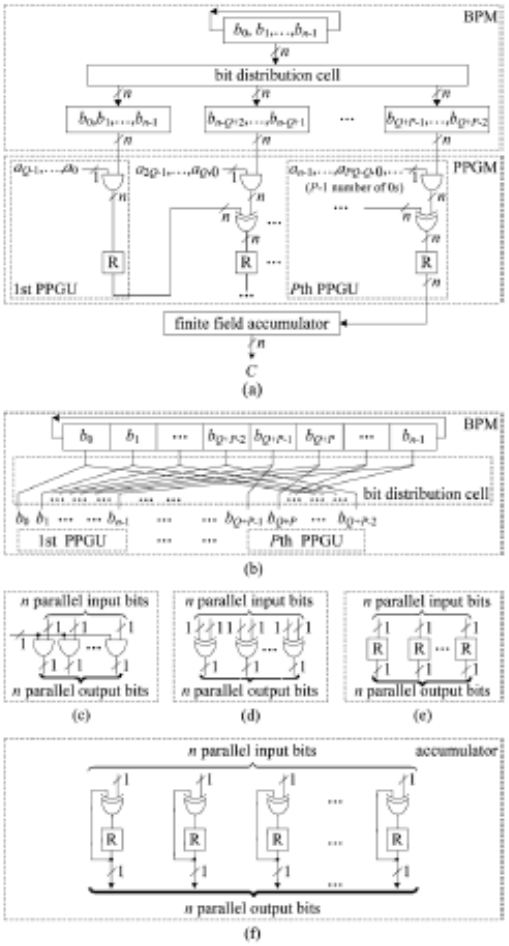

Fig. 4.Proposed structure-I (PS-I) for RB multiplier, where "R" denotes a registercell. (a) Detailed structure of the RB multiplier. (b) Structure of the bit-permutation module (BPM). (c) Structure of the AND cell in the partial productgeneration module (PPGM). (d) Structure of the XOR cell in the PPGM. (e)Structure of the register cell in the PPGM. (f) Structure of the finite field accumulator.

The PSFG of Fig. 3, is mapped to the high-throughput digit-serialRB multiplier (shown in Fig. 4), referred to as proposed structure-I (PS-I). PS-I contain three modules, namely the bit-permutation module (BPM), partial productgeneration module (PPGM)and finite field accumulator module. The BPM of Fig. 4 performsrewiring of bits of operand to feed its output to partialproduct generation units (PPGU)s according to the S nodes ofPSFG of Fig. 3, as shown in Fig. 4(b). The AND cell, XOR celland register cell of PPGM perform

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

the function of M node, Anode and delay imposed by the retiming of PSFG of Fig. 3, respectively.Structures and functions of AND cell, XOR cell andregister cell are shown in Fig. 4(c), (d), and (e), respectively. Theinput operands are fed to PPGU in staggered manner to meet thetiming requirement in systolic pipeline. The accumulator consistsof parallel bit-level accumulation cells [as shown in Fig. 4(f)].The newly received input is then added with the previously accumulatedresult and the result is stored in the register cell to be usedduring the next cycle. The duration of minimum cycle period ofthe PS-I is . The proposed digit-serial design gives thefirst output of desired product cycles after the pair ofoperands are fed to the structure, while the successive output areproduced at the interval of cycles thereafter.

B. Modification of Proposed Structure-I

For any integer value of P, we can have $(P = kd + l)$, where $0 \le l < d$ and $l < P$ Without loss of generality, for simplicity ofdiscussion, we can assume $l = 0$.The approach proposed here for $l = 0$ however can be easily extended to the cases where $l \neq 0$. Define $0 \le h \le k-1$ and $) \le f \le d-1$ such that (13) can be rewritten as

$$\overline{C_u} = \sum_{h=0}^{k-1} \sum_{f=0}^{d-1} B^{u+fhQ} a_{u+fhQ}$$

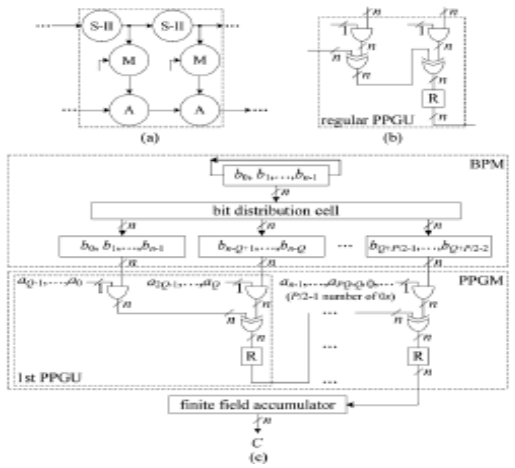

Fig. 5. PS-I for RB multiplier when d=2. (a) Proposed cut-set retiming ofPSFG when d=2. (b) Detailed internal structure of merged regular PPGU. (c)Corresponding PS-I for the case d=2.

Based on (14), we can modify the retiming of PSFG of Fig. 3to derive suitable digit-level architecture for RB multiplier over. For example, to obtain the proposed structure for d = 2 , a pair of S nodes, a pair of M nodes and a pair of A nodesof the PSFG of Fig. 3 can be merged to form a macro-node asshown within the dashed-lines in Fig. 5. Each of these macronodescan be implemented by a new PPGU to obtain a PPGM ofPPGUs. Accordingly, two regular PPGUs in the structure ofFig. 4 can be emerged into a new regular PPGUas shown in Fig.5(b), which consists of two AND cells and two XOR cells (thefirst PPGU requires only one XOR cell). The functions of ANDcell, XOR cell and register cell are the same as those describedin Fig. 4. The critical path of the structure of Fig. 5(c) amountsto $(T_A + 2T_X)$. The first output of desired product is availablefrom this structure after a latency of (P/2 +Q) cycles, while thesuccessive outputs are available thereafter in each cycles ofduration (TA+2TX). The technique used to derive the structurefor may be extended for any value of (P/d), to obtain a structureconsisting of PPGUs.The technique based on (4) can significantly reduce the registercomplexity of the proposed structure, since consecutivePPGUs of the PS-I can be merged together to formunits to be processed concurrently. This strategy is quite usefulfor FPGA-based implementation since the value of can bechosen appropriately, such that the PSFG nodes selected to beprocessed in a cycle can bemapped to a basic unit of FPGAwithlow register complexity.

C. Proposed Structure-II

We can further transform the PSFG of Fig. 3 to reduce the latencyand hardware complexity of PS-I. To obtain the proposed structure,serially-connected A nodes of the PSFG of Fig. 3 aremerged into a pipeline form of A nodes as shown withinthe dashed-box in Fig. 6(a). These pipelined A nodes can be implementedby a pipelined XOR tree, as shown in Fig. 6(b). Sinceall the AND cells can be processed in parallel, there is no need ofusing extra “0”s on the input path to meet the timing requirementin systolic pipeline. The critical path and throughput of PS-II arethe same as those of PS-I. Similarly, PS-II can

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

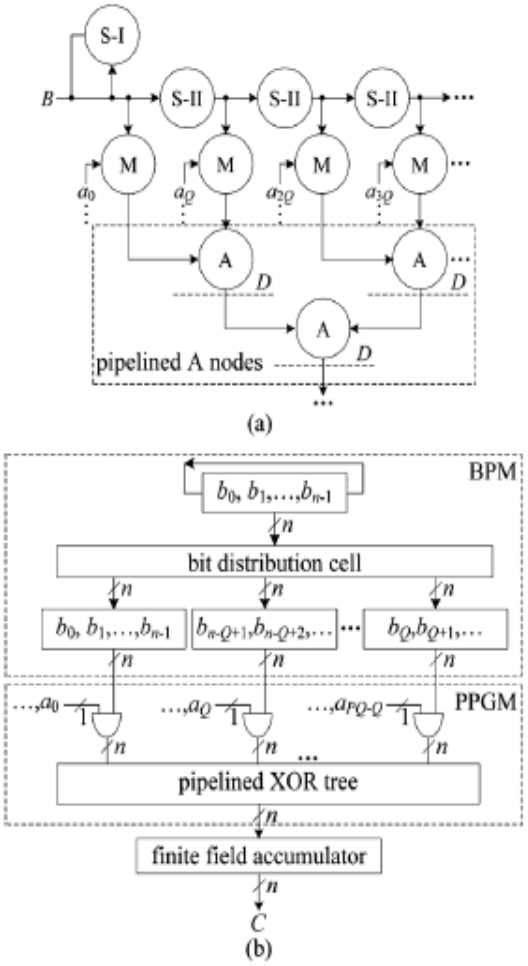

Fig. 6. Proposed structure-II (PS-II) for RB multiplier, where "R" denotes aregister cell. (a) Modified PSFG. (b) Structure of RB multiplier be easily extendedto larger values of to have low register-complexity structures.

D. Proposed Structure-III

Since the S nodes of Fig. 3 perform only the bit-shifting operationsthey do not involve any time consumption. Therefore,we can introduce a novel cut-set retiming to reduce the criticalpathfurther, as shown in Fig. 7(a). It can be observed that thecut-set retiming allows to perform the bit-addition and bit-multiplicationconcurrently, so that the critical-path is reduced to, i.e., the throughput of the design is increased.The proposed high-throughput structure (PS-III) of RBmultiplier thus derived is shown in Fig. 7(b). It consists ofPPGUs, and each PPGU consists of one AND cell, one XORcell and two register cells.

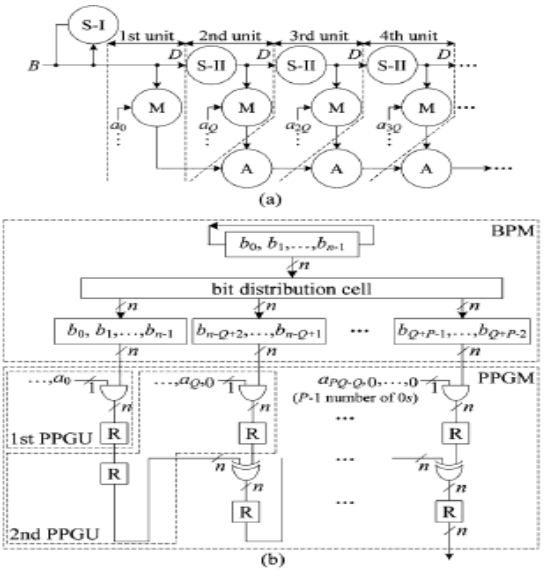

Fig.7. Novel cut-set retiming of PSFG and its corresponding structure: PS-III.(a) Cut-set retiming. (b) BPM and PPGM of PS-III.

The proposed structure yields the firstoutput of desired result cycles after the first input isfed to the structure, while the successive outputs are available ineach cycle.

III.RESULTS

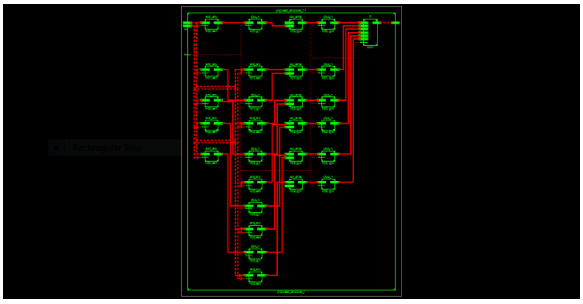

Fig.8. RTL Schematic for cut-set retiming of PSFG of finite field RB multiplication.

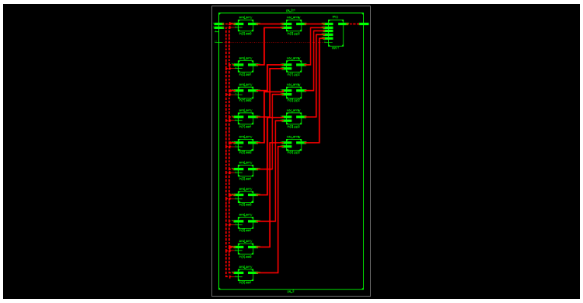

Fig.9. RTL Schematic for pipelined tree of PSFG of finite field RB multiplication.

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

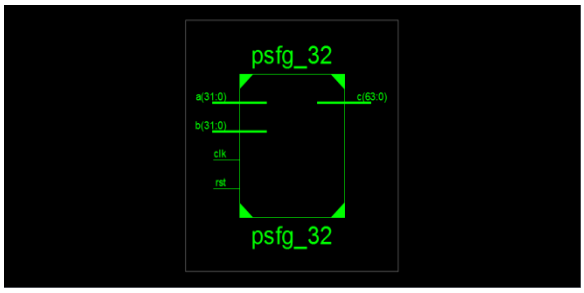

Fig.10. RTLf Schematic for novel cut-set retiming of32bit-PSFG of finite field RB multiplication.

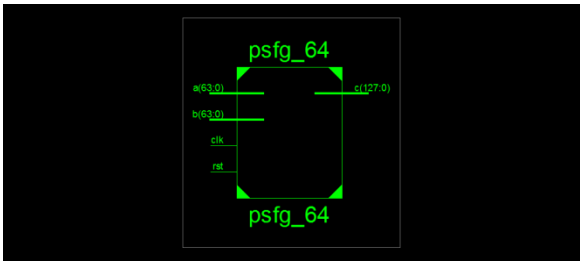

Fig.11. RTL Schematic for novel cut-set retiming of64bit-PSFG of finite field RB multiplication.

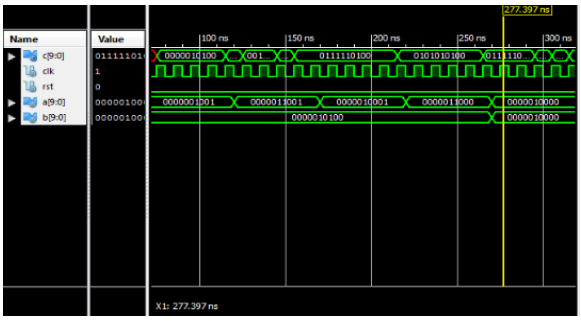

Fig.12. Simulation results for cut-set retiming of PSFG of finite field RB multiplication.

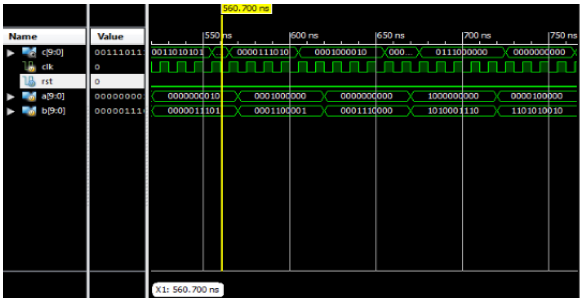

Fig.13. Simulation results for pipelined tree of PSFG of finite field RB multiplication.

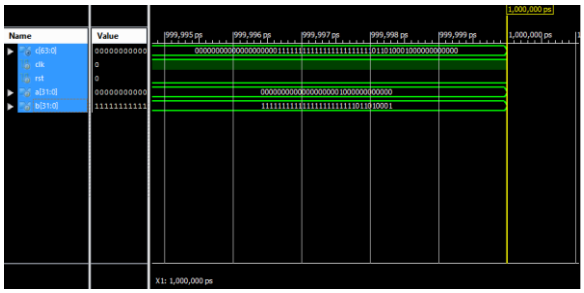

Fig.14. Simulation results for novel cut-set retiming of32bit-PSFG of finite field RB multiplication.

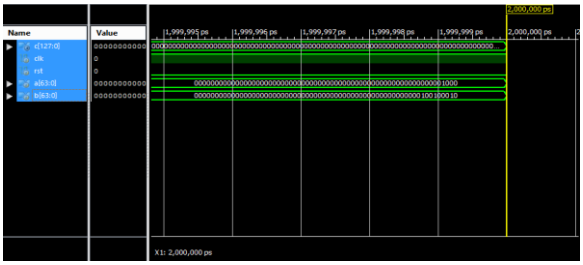

Fig.14. Simulation results for novel cut-set retiming of64bit-PSFG of finite field RB multiplication.

V.CONCLUSION

We have proposed a novel recursive decomposition algorithmfor RB multiplication to derive high-throughput digit-serial multipliers.By suitable projection of SFG of proposed algorithm andidentifying suitable cut-sets for feed-forward cut-set retiming,three novel high-throughput digit-serial RB multipliers are derivedto achieve significantly less area-time-power complexitiesthan the existing ones. Moreover, efficient structures with lowregister-count have been derived for area-constrained implementation;and particularly for implementation in FPGA platformwhere registers are not abundant. The results of synthesis showthat proposed structures can achieve saving of up to 94% and60%, respectively, of ADPP for FPGA and ASIC implementation,respectively, over the best of the existing designs. Theproposed structures have different area-time-power trade-offbehavior. Therefore, one out of the three proposed structurescan be chosen depending on the requirement of the applicationenvironments.

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

REFERENCES

[1] I. Blake, G. Seroussi, andN.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 ofbrahmaqupta-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 fieldmultipliers," J. VLSI Digit.Process., vol. 19, pp. 149–C166, 1998.

[4] P. K. Meher, "On efficient implementation of accumulation in finitefield over and its applications," IEEE Trans. Very Large ScaleIntegr. (VLSI) Syst., vol. 17, no. 4, pp. 541–550, 2009.

[5] L. Song, K. K. Parhi, I. Kuroda, and T.Nishitani, "Hardware/softwarecodesign of finite field datapath for low-energy Reed-Solomn codecs,"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.

Author Details

Vasam Sathish, received B.Tech Degree in Electrical & ElectronicsEngineering from Trinity College of Engineering and Technology Karimnagar, India. Presently pursuing M.Tech (VLSI & EMBEDDED SYSTEMS) from DVR College of Engineering and Technology, Hyderabad, Sangareddy district. Telangana, India.