International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

# A Survey on FPGA and ASIC Implementations using RB multiplication to derive

KAMMARI VAMSHI KRISHNA[1] &MAHABOOB BASHA[2]

[1]M-Tech Dept of ECE, Geethanjali Engineering College NANNUR-V, KURNOOL-DIST
Mail Id:- bplvamshi@gmail.com

[2] Assistant Professor Dept ECE, Geethanjali Engineering College NANNUR-V, KURNOOL DIST Mail Id:- syedmahaboob45@gmail.com

## 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. In this paper, we have proposed a novel 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 PSFG suitably and performed efficient feed-forward cut-set retiming to derive three novel multipliers which not only involve significantly less time-complexity than the existing ones but also require less area and less power consumption compared with the others. Both theoretical analysis and synthesis results con firm the efficiency of proposed multipliers over the existing ones. The synthesis results for field programmable gate array (FPGA) and application specific integrated circuit (ASIC) realization of the proposed designs and competing existing designs are compared. It is shown that the proposed high-throughput structures are the best among the corresponding designs, for FPGA and ASIC implementation.

**Keywords:** - Galois Fields (GF (2 )), FPGA & ASIC Implementations

## 1. INTRODUCTION

Multiplication over GF (2 ) is a basic operation frequently came across in modern cryptographic systems such as the Elliptic Curve Cryptography(ECC) and error control coding. Also multiplication over a Galois field can be used to perform other field operations, e.g. division, exponentiation, and inversion. Arithmetic operations in the GF (2 ) have several applications in computer algebra and theory of coding. Multiplication over GF (2 ) 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 ) 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 ) arithmetic operations for the benefits like low-cost and high-throughput rate. There are different types of bases to represent field elements, those are polynomial basis, normal basis, triangular basis and RB, and the choice of representation of field elements has a major impact on the performance of the arithmetic circuits. Several algorithms for basic arithmetic operations in GF (2 ) are suitable for both hardware and software implementations have been recently developed. Because of several advantages of the RB based multipliers they have gained significant 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 .Several digit-level serial/parallel structures for RB multiplier over GF (2 $m$ ) have been reported in the last few years . An efficient serial/parallel multiplier using redundant representation has been presented. A bit-serial word-parallel (BSWP) architecture for RB multiplier has then been reported. Several other RB multipliers have also been developed for reducing the complexity of implementation and for high-speed realization

## 2. IMPLEMENTATION

FPGA

Real-time computation, portability and flexibility are crucial for practical brain-machine interface (BMI) applications. In this work, we proposed Hardware Processing Modules (HPMs) as a method for accelerating BMI computation. Two HPMs have been developed. One is the field-programmable gate array (FPGA) implementation of spike sorting based on probabilistic neural network (PNN), and the other is the FPGA implementation of neural ensemble decoding based on Kalman filter (KF). These two modules were configured under the same framework and tested with real data from motor cortex recording in rats performing a lever-pressing task for water rewards. Due to the parallelism feature of FPGA, the computation time was reduced by several dozen times, while the results are almost the same as those from Matlab implementations. Such HPMs provide a high

performance coprocessor for neural signal computation.

We implement our design on an FPGA platform, as their reconfigurable nature provides the user ample flexibility, allowing for customized architectures tailored to a specific problem and input data size. Another property of FPGAs that is important for our design is that they allow the design to scale upward easily as process technology allows for everlarger gate counts. Overall, our system is able to achieve a speedup of 5.58× as compared to software implementations on the experimental platform we selected. The DTC architecture was implemented on a Xilinx ML310 board which is a Virtex-II Pro-based embedded development platform. It includes an Xilinx XC2VP30 FPGA with two embedded PowerPC processors, 256 MB DDR DIMM, 512 MB compact flash card, PCI slots, ethernet and standard I/O on an ATX board. The XC2VP30 FPGA contains 13696 slices and 136 Block RAM modules. We used 256 MB DDR DIMM PPC 405 OCM BRAM PLB Bus DTC MODULE D D R OCM BUS PERIPHERALS Figure 4. Experimental setup Xilinx XPS 8.1i and ISE 8.1i softwares to implement our architecture on the board. The experimental setup for the DTC architecture. The figure does not show the entire peripheral components supported by the XC2VP30 FPGA, only those relevant to the design. The DTC unit is implemented as a custom peripheral which is fed by the PowerPC. The PowerPC reads in input data stored in DDR DIMM, initializes the DTC component, and supplies class ID data at regular intervals. The OCM BRAM block stores the instructions for the PowerPC operation. While implementing the design, several tradeoffs were considered. The use of floating point computations complicate the design and increase the area overhead, hence we decided to perform the division operations using only fixed-point integer computations. To verify the correctness of our assumptions, we implemented a version of ScalParC that uses only fixed point values. It was found that the decision trees generated by both the fixed-point and floating point versions were identical, thus validating our choice of a divider performing fixed point computations. The divider output was configured to produce 32 integer bits and 16 fractional bits, a choice made keeping in mind the size of the dataset and precision required to produce accurate results. The divider was also pipelined in

order to handle multiple input class IDs at the same time.

## ASIC

ASTRI ASIC Implementation CCG transforms innovative ideas and designs into ICs and products. This involves various design processes covering architecture, digital logic, analog circuitry, physical, component simulation, system testing and software. The Group works closely with other groups and customers to transform their architecture designs and logic forms into a production ready silicon and system platform. The support model is flexible enough to balance amongst the various trade-offs based on diversified design scenarios and maximal design value. The Group has been developing Analog IP's for various IC applications. Both Analog IP blocks for SoC application and pure Analog base IC's are supported. Some of the examples are multi-channel ADC for video application, Network Controller, Motor Driver and Ultra-low power timing control IC. Over the years, multiple patents have been filed and granted for several analog circuit designs in the area of low power and area saving. These innovations contributed to the success of ASTRI's and our customers' ICs.

## 3. EXPERIMENTAL RESULTS

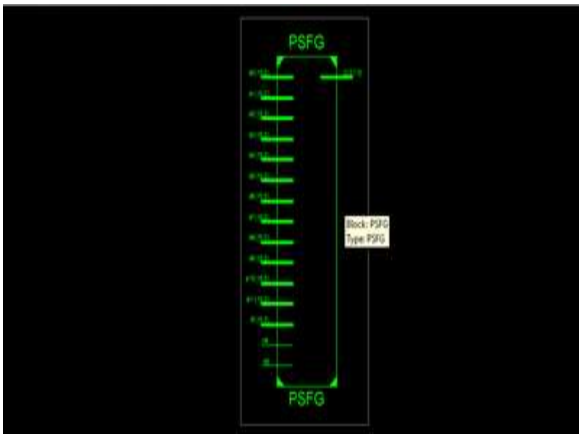


**Fig:-1** PSFG

**Fig:-2** Simulation Results

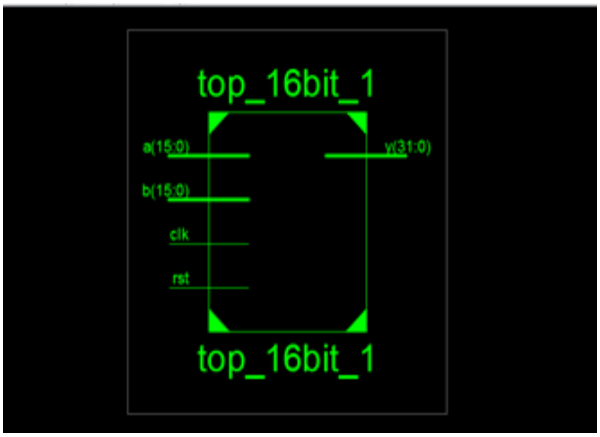


Fig:-3 Processer

Fig:-4 Results

## 4. CONCLUSION

We have proposed a novel recursive decomposition algorithm for RB multiplication to derive high-throughput digit-serial multipliers. 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-count proposed structures can be chosen depending on the requirement of the application environments. Finite field multipliers play a very important role in the areas of digital communication especially in the areas of cryptography, error control coding and digital signal processing.

## 5. REFERENCES

[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 digitserial/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-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.

[7] C.-Y. Lee, J.-S.Horng, I.-C.Jou, and E.-H. Lu, "Lowcomplexitybit-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