ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Area Efficient Finite Field Multipliers Using Redundant Basis

G Prashanth Kumar [1], B Subhaker [2]

P.G Student, Department of Electronics and Communication Engineering, St. Martins Engineering College Hyderabad, Telangana, India

Assistant Professor, Department of Electronics and Communication Engineering, St. Martins Engineering College Hyderabad, Telangana, India

ABSTRACT: Redundant basis (RB) multipliers over Galois Field 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 confirm the efficiency of proposed multipliers over the existing ones.

KEYWORDS: ASIC, digit-serial, finite field multiplication, FPGA, high-throughput, redundant basis.

I. INTRODUCTION

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 de- rived. By identifying suitable cut-sets, we have modified the PSFG suitably and performed effi -cient 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 confirm 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.

Finite field multiplication is a basic operation frequently encountered in modern cryptographic systems such as the elliptic curve cryptography (ECC) and error control coding. Moreover, multiplication over a finite field can be used further to perform other field operations, e.g., division, exponentiation, and inversion. 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. Besides, a low-end microprocessor cannot meet the real-time requirement of different applications since word-length of these processors is too small compared with the order of typical finite fields used in cryptographic systems. Most of the real-time applications, therefore, need hardware implementation of finite field arithmetic operations for the benefits like low-cost and high-throughput rate.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

The choice of basis to represent field elements, namely the polynomial basis, normal basis, triangular basis and redundant basis (RB) has a major impact on the performance of the arithmetic circuits .The multipliers based on RB have gained significant attention in recent years due to their several advantages. Not only do they offer free squaring, as normal basis does, but 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 years after its introduction by Wu. An effi cient serial/parallel multiplier using redundant representation has been presented.

A bit-serial word-parallel (BSWP) architecture for RB multiplier has been reported by Namin. Several other RB multipliers also have been developed by the same authors in for reducing the complexity of implementation and for high-speed realization.We fi nd that the hardware utilization efficiency and throughput of existing structures of can be improved by efficient design of algorithm and architecture.

In this paper, we aim at presenting efficient digit-level serial/parallel designs for high-throughput finite field multiplication over GF(2^m) based on RB. We have proposed an effcient
recursive decomposition scheme for digit-level RB multiplication, and based on that we have derived parallel algorithms for high throughput digit-serial 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 complexities than the corresponding existing designs. Field programmable gate array (FPGA) has evolved as a mainstream dedicated computing platform. FPGAs however do not have abundant number of registers to be used in the multiplier. Therefore, we have modified the proposed algorithm and architecture for reduction of register-complexity particularly for the implementation of RB multipliers on FPGA platform.

Apart from these we also present a low critical-path digit-serial RB multiplier for very high throughput applications.
The rest of the paper is organized as follows: The proposed algorithm for finite field RB multiplication over GF(2^m) is presented.

II. MATHEMATICAL FORMULATION

Brief Review of Existing Digit-Serial RB Multiplier

Assuming x to be a primitive nth root of unity, elements in finite field GF(2^m) can be represented in the form:

$$A= a_o + a_1 x + a_2 x^2 +\ldots\ldots\ldots\ldots + a_{n-1} x^{n-1}$$

For a finite field GF(2^m) when (m+1) is a prime and 2 is a primitive root modulo (m+1) there exists a type I optimal normal basis (ONB) where is an element of GF(2^m) and n=m+1.

Let A,B € GF(2^m) be expressed in RB representation as

$$A = \sum_{i=0}^{n-1} a_i x^i$$
$$B = \sum_{i=0}^{n-1} b_i x^i$$

Where a_i , b_i € GF(2). Let be the product of and ,which can be expressed as follows

$$C= A B$$
$$= (\sum_{i=0}^{n-1} b_i x^i) A$$
$$= \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} b_{(i-j)n} x^i) a_j$$
$$= \sum_{i=0}^{n-1} (\sum_{j=0}^{n-1} b_{(i-j)n} a_j) x^i$$

In the recently proposed RB multipliers, both operands A and B are decomposed into a number of blocks to achieve digit-serial multiplication, and after that the partial products corresponding to these blocks are added together to obtain the desired product word. The existing digit-serial RB multiplication algorithm is stated as follows:

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Existing Algorithm Existing digit-serial multiplication algorithm [13] and [14]

Inputs: $A = (\underbrace{a_0 \dots a_{w-1}}_{A'_0} \underbrace{a_w \dots a_{2w-1}}_{A'_1} \dots \underbrace{a_{(t-1)w} \dots a_{n-1}}_{A'_{t-1}})$

$= (A'_0, \dots, A'_{t-1})$,

and $B = \underbrace{b_0 \dots b_{w-1}}_{B'_0} \underbrace{b_w \dots b_{2w-1}}_{B'_1} \dots \underbrace{b_{(t-1)w} \dots b_{n-1}}_{B'_{t-1}}$

$= (B'_0, \dots, B'_{t-1})$

are two RB representation elements, for $t = \lceil n/w \rceil$.

Output: $C = A \cdot B = (c_0, \dots, c_{n-1})$

1. Initialization: $t = \lceil n/w \rceil, r_{e,i}^{(-1)} = 0$ for $e = 0, \dots, t-1$ and $i = 0, \dots, n-1$

2. For all values of $i = 0, 1, 2, \dots, n-1$, do

3. For all values of $e = 0, 1, 2, \dots, t-1$, do

4. For $g = 0$ to $w-1$, do

5. $r_{e,i}^{(g)} = r_{e,i}^{(g-1)} + a_{ew+g} b_{(i-ew-g)n}$

6. End For

7. End For

8. $c_i = \sum_{e=0}^{t-1} r_{e,i}^{(w-1)}$

9. End For

Step 5 of existing algorithm refers to the computation of digit-wise partial products for the digit-serial multiplication where operands A and B are decomposed into a number of digits, and step 8 refers to the addition of those partial products to compute the product word.

Although the existing algorithm of [13] and [14] is the most efficient one out of all reported algorithms for digit-serial multiplication, we find that the hardware utilization efficiency and throughput of existing structures of [13]-[14] could be improved further by efficient design of algorithm and architecture. Particularly, due to its larger number of digit-wise partial products (step 5), and extra time for addition of those partial products (step 8), which not only increases the average computation time (ACT) to perform the multiplication but also involves extra hardware resources for storage and addition of larger number of partial products.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

Proposed Digit-Serial RB Multiplication Algorithm

Alternatively, we can write (5) in a bit-level matrix-vector form as

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

Proposed digit serial multiplication algorithm

Algorithm 1 Proposed digit-serial multiplication algorithm

Inputs: A and B are the pair of elements (in RB representation) in $GF(2^m)$ to be multiplied.

Output: $C = A \cdot B$

1. Initialization step

    1.1 $D = 0$

2. Multiplication step

    2.1. For $u = 0$ to $Q - 1$

    2.2. For $v = 0$ to $P - 1$

    2.3. $D = D + B_v A_u^T$

    2.4. End For

    2.5. End For

3. Final step

    3.1. $C = D$

where step 2.3 refers to the digit-serial multiplication process. According to our proposed algorithm, we generate less number of partial products, and partial products are accumulated as soon as they are computed, which not only shortens the ACT, but also significantly reduces register and adder complexities of proposed structures over that of existing ones.

III. DERIVATION OF PROPOSED HIGH THROUGHPUT STRUCTURES FOR RB MULTIPLIERS

A. PROPOSED STRUCTURE

the RB multiplication can be represented by the 2-dimensional SFG (shown in Fig. 1) consisting of Q parallel arrays, where each array consists of $(P-1)$ bit-shifting nodes (S node), P multiplication nodes (M nodes) and $(P-1)$ 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 Q positions for the de-gree reduction requirement. Functions of M nodes and A nodes are depicted in Fig. 1(c) and 1(d), 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 Q arrays of Fig. 1 can be performed by bit-by-bit XOR of the operands in $(Q-1)$ number of A nodes as depicted in Fig. 1. The

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

desired product word is obtained after the addition of Q parallel output of the arrays.

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 P 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.

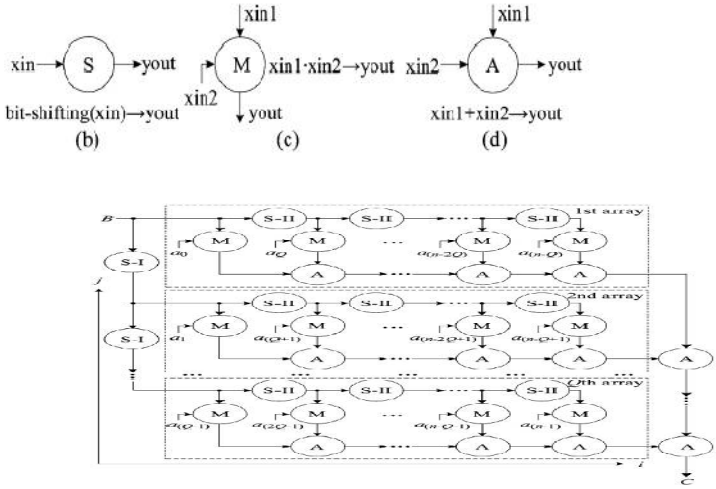

Fig.1 . Signal-flow graph (SFG) for parallel realization of RB multiplication

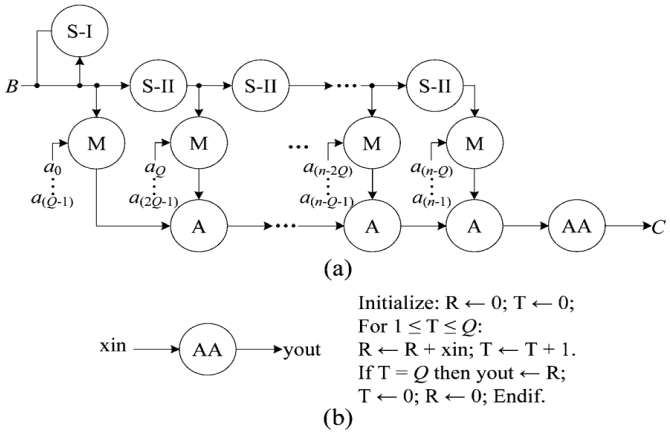

Fig2 Processor-space flow graph (PSFG) of digit-serial realization of finite field RB multiplication over GF(2^m) (a) The proposed PSFG. (b) Functional description of add-accumulation (AA) node.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

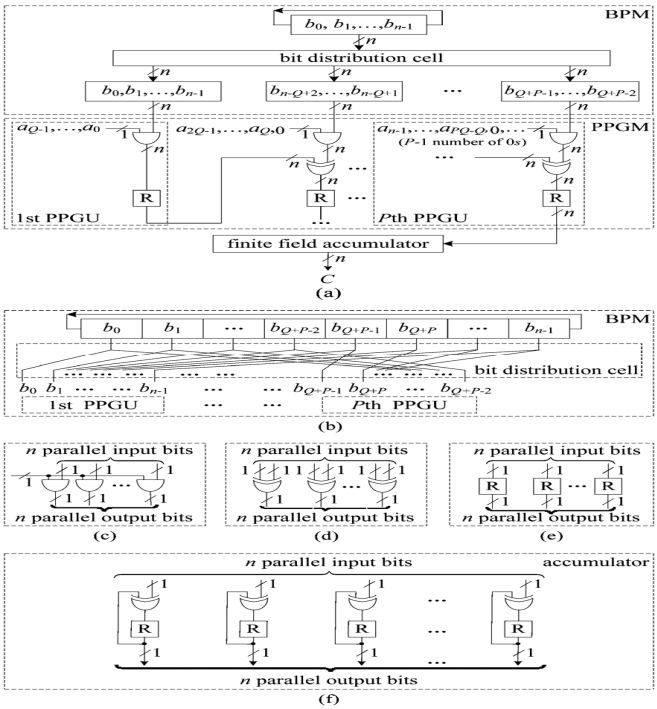

Fig.3Proposed structure-I (PS-I) for RB multiplier, where "R" denotes a register cell. (a) Detailed structure of the RB multiplier. (b) Structure of the bit-permutation module (BPM). (c) Structure of the AND cell in the partial product generation module (PPGM). (d) Structure of the XOR cell in the PPGM. (e) Structure of the register cell in the PPGM. (f) Structure of the finite field accumulator.

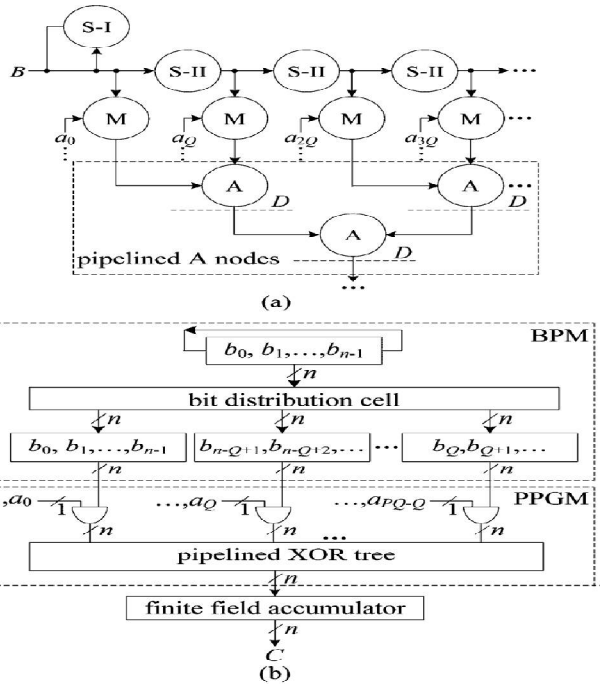

Fig 4. Proposed structure-II (PS-II) for RB multiplier, where "R" denotes a register cell. (a) Modified PSFG. (b) Structure of RB multiplier.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

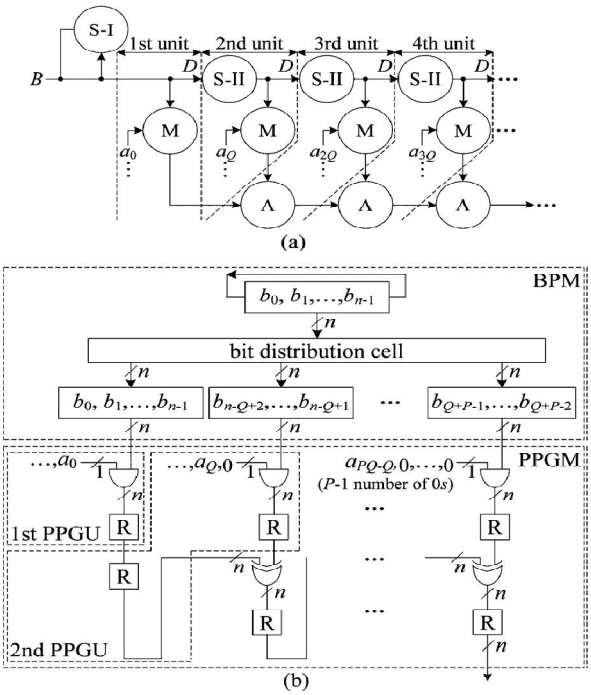

Fig.5Novel cut-set retiming of PSFG and its corresponding structure: PS-III.(a)Cut-set retiming. (b) BPM and PPGM of PS-III.

Comparisons of multipliers

In order to compare the hardware requirements of the above discussed multipliers some notations need to be considered. Let R be the number of multiplication nodes, S be the number of parallel arrays, n be the integer and n=m+1 in GF (2 m). The hardware requirements are compared on the number of AND gates, XOR gates and Registers required implementing the multiplication and it is represented below.

Multipliers	Registers	AND Gates	XOR Gates
4.1	n	Rn	R(n-1)
4.2	(R+1)n	Rn	(2R-1)n
4.3	Rn+2n	Rn	Rn

Table1 comparision of multipliers.

the RB multiplication can be represented by the 2 dimensional Signal Flow Graph (SFG), in which it is considered that TA and TX are the delay of an AND gate and an XOR gate respectively. The time duration of critical path is calculated from SFG represented by Tcp, and with this Average Computation Time (ACT) is calculated for above discussed multipliers shown in below.

Multipliers	Critical Path	ACT
4.1	$T_A + [\log_2 n]\, T_X$	ST_{cp}
4.2	$T_A + T_X$	$ST_{cp} + [\log_2 R]\, T_X$
4.3	$T_A + T_X$	ST_{cp}

Table2 comparison of critical path.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

VI. SIMULATION RESULTS

The below figures shows the simulation result for the proposed structures.

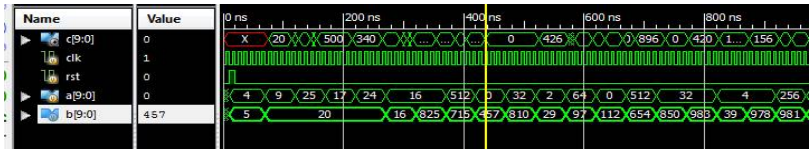

Fig 6. simulation results for proposed structure1.

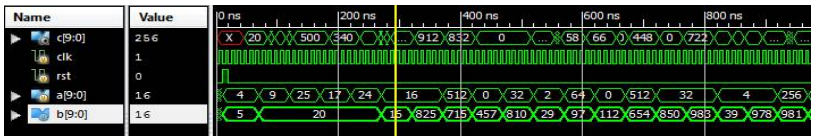

Fig7.simulation result for proposed structure2.

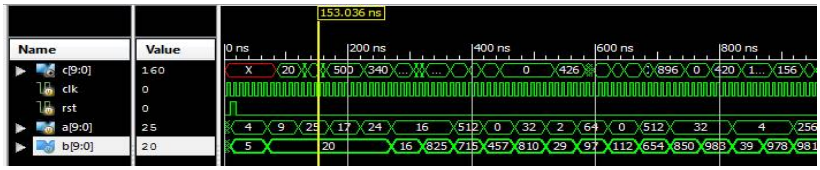

Fig.8simulation result for proposed structure3.

V. CONCLUSION

RB multipliers over GF (2 m) are very popular in Elliptic Curve Cryptography because of their negligible hardware cost for squaring and modular reduction. Word Level RB multiplier is the most efficient among all multipliers in terms of hardware utilization. Digit serial RB multiplication in a bit level matrix vector form is most efficient in terms of area-time complexities. Future works can be done to find out new methods to obtain partial products in lesser time and with less hardware requirements.

RB multipliers over GF (2 m) are very popular in Elliptic Curve Cryptography because of their negligible hardware cost for squaring and modular reduction. Word Level RB multiplier is the most efficient among all multipliers in terms of hardware utilization. Digit serial RB multiplication in a bit level matrix vector form is most efficient in terms of area-time complexities. Future works can be done to find out new methods to obtain partial products in lesser time and with less hardware requirements.

REFERENCES

[1] Alessandro Cilardo, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano, ―Elliptic Curve Cryptography Engineering,‖ proc. of IEEE, vol.94, no.2, pp.395-406, Feb.2006.
[2] N.R.Murthy and M.N.S.Swamy, ―Cryptographic applications of brahmagupta-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.149-166, 1998.
[4] P.K.Meher, ―On efficient implementation of accumulation in finite field over GF (2 m) and its applications,‖ IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.17, no.4, pp.541-550, 2009.
[5] L.Song, K.K.Parhi, I.Kuroda, and T.Nishitani, ―Hardware / software codesign of finite field data path 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 fields GF (2 m) yielding 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, ―Lowcomplexity bit parallel systolic Montgomery multipliers for special classes of GF (2 m),‖ IEEE Trans. Comput., vol.54, no.9, pp.1061-1070, Sep.2005.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 12, December 2016

BIOGRAPHY

.G Prashanth Kumar (2014-2016): Pursuing M.Tech in Embedded Systems from St. Martins Engineering College Afflicted to Jawaharlal Nehru Technical University (JNTUH), Hyderabad. He completed his B.Tech in Electricals and Electronics Engineering from TRR College of Engineering (TRRCE), Patancheru.

B Shubhaker: He did his B.Tech(ECE) in Tirumal Engineering College, Bogaram in 2008. He completed his M.Tech (Systems and Signal Processing) in JNRU College of Engineering in 2014. He is currently working as an Assistant Professor in Department of Electronics & Communication and Engineering in St. Martins Engineering College. He guided 4 projects to final year B.E/B.Tech students and guided for M.Tech students with good teaching experience. His area of interest in Electronics is Digital Communication, Radar systems.