International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 30th Nov 2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-11

Title: **VLSI DESIGN OF HIGH THROUGHPUT FINITE FIELD MULTIPLIER USING REDUNDANT BASIS TECHNIQUE**

Volume 06, Issue 11, Pages: 494–498.
Paper Authors

ARELLI SHRUTHI,B.SHIVA KUMAR
Vaagdevi College of Engineering, Bollikunta, Warangal, Telangana State, India.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

VLSI DESIGN OF HIGH THROUGHPUT FINITE FIELD MULTIPLIER USING REDUNDANT BASIS TECHNIQUE

[1]ARELLI SHRUTHI,[2]B.SHIVA KUMAR
[1]Pg Scholar, Department of ECE, Vaagdevi College of Engineering, Bollikunta Warangal, Telangana
[2]Assistant Professor, Department of ECE, Vaagdevi College of Engineering, Bollikunta Warangal, Telangana

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.

I INTRODUCTION

Finite field GF (2m) is a field that contains finitely many fields. It is especially useful in translate computer data, which present in the binary form. Finite Field has wide applications in cryptography and error control coding [1], [2]. The key arithmetic unit for multiple systems based on computations of finite field is finite field multiplier because the complex operations like division and inversioncan be broken down into successive multiplication operation. The most common arithmetic is multiplication which is useful to obtain efficient multipliers [3]. Both the hardware and software architectures are studied for computing multiplications over finite field [4]. The mostly used bases for finite fields are polynomial (PB), normal (NB), triangular (TB), and redundant (RB) [5]. Basis is a set of vectors that, in a linear combination, can represent every vector in given a vector space. Redundant basis is attractive due to its free squaring and modular reduction for multiplication [7]. A redundant representation is extracted from minimalcyclotomic ring and the arithmetic operation can be performed in the ring by embed the present field [9]. A number of structures have been designed for efficient finite field multiplication over finite field based on RB. Semi-systolic Montgomery multiplier ispresented in [4]. Super-systolic

multiplier has been reported by Pramod Kumar Mehar. Bit-Serial/Parallel multipliers [8], Comb style architectures are presented formerly and also several other RB multipliers are designed for hardware efficiency and throughput [6]. In this contribute, an efficient high-throughput digit-serial/parallel multiplier designs over finite field based on RB is presented. A novel recursive decomposition scheme is presented, based on that parallel algorithms are obtained for high-throughput digit-serial multiplication. By depicting the parallel algorithm to a regular two dimensional signal-flow-graph (SFG) array go after by projection of SFG to onedimensional processor-space flow graph (PSFG), the algorithm is mapped to three multiplier architectures. In this work, the implementation of 10- bit digit-serial RB multipliers is presented to obtain high-throughput

2. LITERATURE REVIEW

Multiplication is more complicated, whereas division or inversion can be broken down into a series of consecutive multiplication operations. Therefore in practice, a binary field (Galois field of characteristic two) multiplier becomes the key arithmetic unit and VLSI design core for the hardware systems, based on Galois field computations. The way in which GF (2) multiplication is performed is dependent on the representation bases in a binary field. Efficiency of Galois field multiplication depends on the choice of the basis to represent field elements. Bases that have been used for efficiently realizing Galois field multipliers include polynomial basis, normal basis (NB), dual basis, triangular basis, and redundant representation or redundant. Among these, redundant basis representation is especially interesting, because likewise normal basis multiplier it offers almost free squaring and also eliminates modular operation for multiplication. RB representation has high modularity and exhibits carry-free addition, which can be used to design high performance multipliers. The main idea of multiplication using redundant representation is to perform multiplication by embedding the field in a larger ring. The ring used here is a cyclotomic ring and has a very simple structure, such that the modular operation can be saved in a multiplication operation. The main drawback for redundant representation is that it uses more bits to represent an element as compared to other representation basis. The number of representation bits depends on the size of the cyclotomic ring. However, for the class of fields GF (2) for which there exists a type I optimal normal bases (ONB), the number of bits required for a redundant representation of a field element is slightly higher for large m—(m+1) bits compared to m bits used for the other bases. The work done in the field of redundant representation and RB multipliers over GF (2) in all these years is depicted

3 MATHEMATICAL FORMULATIONS

Redundant Basis Multipliers offers negligible hardware cost for squaring, provides lower computational complexities, and also can be implemented in highly regular computing structures.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Digit Serial RB Multiplier In Digit serial RB multiplier digit wise partial products for the digit serial multiplication where operands A and B are decomposed into a number of digits, and then the addition of those partial products is done to compute the product word. Assuming x to be a primitive nth root of unity, elements in GF (2) can be represented in the form:

A= $a0 + a1x + \ldots. + an-1x\ n-1$ (1) Where $ai \epsilon$ GF (2), for 0≤ i ≤ n-1, such that the set {1, x, 2 ,….., $x\ n-1$ } is defined as the RB for GF (2 m) elements, where n is a positive integer not less than m [6], [10]. For a GF (2), when (m+1) is prime and 2 is a primitive root modulo (m+1), there exists a type I optimal normal basis (ONB) [10], where x is an element of GF (2 m), and n=m+1. Let A, B ϵ GF (2) be expressed in RB representation as

A= $aix\ n-1\ i\ i=0$ (2)

B= $bix\ n-1\ i\ i=0$ (3) where a , $bi \epsilon$ GF (2). Let C be the product of A and B, which can be expressed as follows

C= A·B = $(x\ ibi)\ n-1\ i=0 \cdot A = (\ n-1\ i=0\ bix\ (i+j)\ )aj\ n-1\ j=0 = (\ n-1\ j=0\ b(i-j\ )n\ x\ i\ )aj\ n-1\ i=0 = (\ n-1\ i=0\ b(i-j\ )n\ aj\ )x\ n-1\ i\ j=0$ (4) where (i-j)n denotes modulo n reduction. Define C= $cix\ n-1\ i\ i=0$ where $ci \epsilon$ GF (2), then $ci = b\ i-j\ n\ aj\ n-1\ i=0$ (5)

Word Level RB Multiplier In Word Level RB Multiplier [13], both the operand A and B are decomposed into 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. Considering equations (1) to (5)

Then the operand A in RB representation in k= [n/w] words A= $a\ 0\ \ldots\ a\ w-1\ A0\ a\ w\ \ldots\ a\ 2w-1\ A1\ a2w\ \ldots\ a\ k-1\ w\ \ldots\ a\ n-10\ \ldots\ 0\ Ak-1$ Note that aj =0 if j > n-1 Replace j in (5) with hw+l $ci = ahw+lbi-hw-l\ k-1\ h=0\ w-1\ l=0$;

i =0,1,…..,n-1 (6) Define new signal $dh,i\ (-1)$ as follows: $dh,i\ (-1)$ =0 and $dh,i\ (l) = dh,i\ (l-1) + ahw+lbi-hw-l$;

for l=0,1,……,w-1 (7) then it follows from (7)

$dh,\ (w-1) = ahw+lbi-hw-l\ w-1\ l=0$ (8)

comparing (6) with (8), it follows: $ci = dh,i\ k-1\ (w-1)\ h=0$ (6) This multiplier is faster than previous defined multipliers, but has larger area complexities.

4.THERECURSIVE DECOMPOSITION DIGIT SERIAL MULTIPLICATION ALGORITHM

Inputs: A and B are the pair of elements in GF(2m) 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

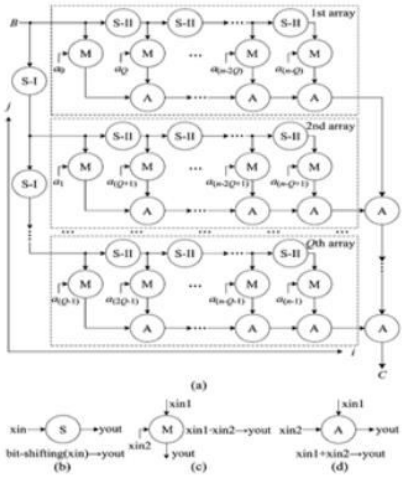
3.Final step C=Y A bit level matrix vector form

5.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

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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 bitshifting 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 ,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), Page 267 respectively. Each of the M nodes performs an AND operation of a bit of serial-input operand A with bitshifted 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.

SIMULATION RESULTS:

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

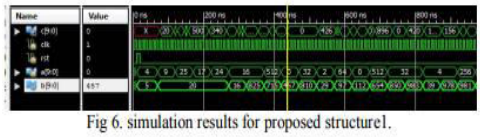


Fig 6. simulation results for proposed structure1.

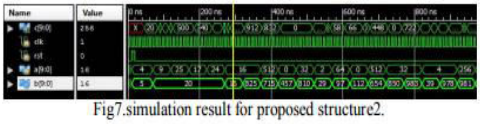


Fig7.simulation result for proposed structure2.

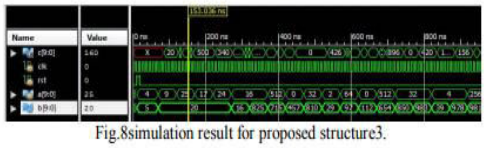


Fig.8simulation result for proposed structure3.

CONCLUSION RB multipliers over GF (2 ò) 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 ò) 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 ◌) 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 ◌) 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 ◌),‖ IEEE Trans. Comput., vol.54, no.9, pp.1061-1070, Sep.2005.