International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 7
March 2018

# Design a Redundant Adaptive Multiplier for High Speed Applications

[1] B.SIVANAGARAJU, [2] V.SEKHAR
[1] M.tech-student, Dept of ECE, vikas group of institutions, Nunna, Vijayawada, A.P, India.
[2] Assistant professor, Dept of ECE, vikas group of institutions, Nunna, Vijayawada, A.P, India

**ABSTRACT: In this paper, our focus is on digit-level architectures for RBmultipliers. Basically, redundant multiplier requires large number of hardware resources while embedding the F2m in cyclotomic field. Two variants of multiplication algorithms along with their corresponding architecture are presented here.It is shown that the proposed architectures have highly regular structures and thus suitable for hardware implementation. Comparisons with existing digit-level RB architectures the proposed architectures outperform the area-delay product as a measure of performance. At last it can observe that the proposed system gives better redundancy compared to existed system.**

**KEY WORDS: Digit-level architecture, finite field arithmetic, multiplication algorithm, redundant representation.**

## I.INTRODUCTION

Finite field computation has recently gained growing attention due to its wide range of applications in coding theory, error control coding, and especially in cryptography, where ElGamal and elliptic curve cryptography (ECC),two out of the three well-known cryptosystems, are based on finite field arithmetic. Finite field computation is performed using arithmetic operations in the underlying finite field. Among the basic field operations, multiplication plays a fundamental role as more complicated operations, namely, field exponentiation and field inversion can be carried out with consecutive use of field multiplication.

Similar to linear algebra, the concept of representation bases is also used in finite field arithmetic to represent field elements.

The choice of representation system—mainly affected by thehardware in use and the requirements of the cryptosystem, has a great impact on computational performance. A few number of representation systems for extension binary fields have been proposed in the literature, such as polynomial basisnormal basis (NB), redundant basis (RB), and dual basis. In both NB and redundant representation, squaring Operation can be performed by applying a simple permutation operation on the coordinates. This makes them more efficient for the hardware implementations of cryptographic algorithms that utilize frequent squaring or exponentiation, such as point addition/doubling in ECC. Moreover, redundant representation is of a special interest due to its unique feature in accommodating ring type operations. This not only offers almost cost-freesquaring operation but also eliminates the need for modular reduction in multiplication.

The idea of embedding a field in a larger ring was first put forward by GAO Et Al. for performing fast multiplication using NB. Later on, Wu *et al.* introduced redundant representation, also known as RB, and finite field multiplication using this representation system. In efforts to Increase the multiplication speed or to reduce the hardware complexities, several architectures have been proposed afterward, such as comb-style architecture and linear feedback Shift register (LFSR)-based architectures. More recently, Xie *et al.* proposed

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 7
March 2018

a recursive decomposition scheme for digit-level serial/parallel structures to achieve less area–time–power complexities.

Despite the structure of the architecture in use, the main drawback of redundant representation is that it contains a certain amount of redundancy as embedding field F2*m* of size *m* in cyclotomic field F*(n)*2 of size *n*, *(n >m)*, is not a one-to-one mapping operation. As a result, redundant representation requires more bits to represent a field element, where the number of representation bits depends on the size of the cyclotomic field in which the underlying field is embedded.

The main intent of this paper is to focus mainly on digit-level architectures forRB multipliers. Here a specific feature of redundant representation is used for a class of finite fields to reduce the architectural complexity of RB multipliers and compensate the inherent redundancy in the representation system. There are two variants which are used in multiplication algorithms corresponding to the architecture presented. From the proposed architectures it can be observed thatit consists of highly regular structures and it is suitable for hardware implementation.

## II. EXISTED SYSTEM

In this paper, we mainly focus on digit-level architectures for RB multipliers. Here a specific feature of redundant representation is used for class of finite fields. This reduces the architectural complexity of RB multipliers and as well it compensate the inherent redundancy in the representation system. Here we presented two variants of multiplication algorithms along with their corresponding architecture. From the Existed architectures it can observe that it has highly regular structures and these are suitable for hardware implementation. The entire process is done when area-delay product is used to measure the performance. So the comparison between performances of the existed multipliers will give results according to system. But they are not reliable because it consists of several optimal NB (ONB) multipliers. At last the hardware realizationsof the existedmultipliers consists of three practical digitsizes. From figure (1) we can observe the existed system architecture.

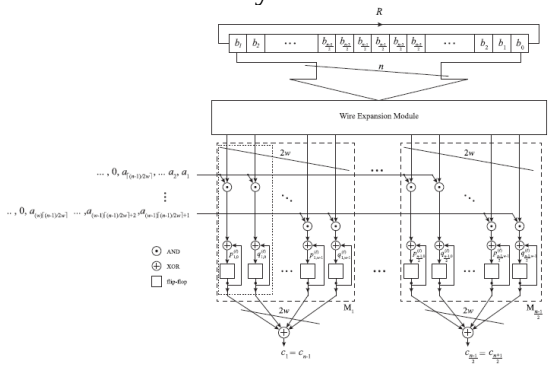


**Fig. 1. Existed architecture for digit-level SIPO RB multiplier, DL-SRB-*a***

In this section, we first present a new algorithm forRB multiplication. Based on this algorithm, we propose twonew optimized digit-level serial-in parallel-out (SIPO) architectures.These architectures are adopted for a class of finitefields in which *n* can be expressed as $n = Tm + 1$, where$T \geq 2$ and is an even number. As will be seen in theremainder of this section, this condition enables us to devisean architecture that significantly reduces the complexity of themultiplier

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 7
March 2018

## III. PROPOSED SYSTEM

The high performance redundant adaptive multiplier gives the less delay. A dual logic level share its logical operation depends on the preference of the logical operation is executed. Its consists of the three layers and the parts are depends on the bit size. In 2 bit size there are 3 Parts in 3 bit size there are 5 parts and 4 bit size there are 7 parts increase the bit size the parts are double in the architecture.In the architecture the main operation is depends on the third layer. In the third layer there are two levels of operations can be done. In that depend on the preference one level of operation is performed and the second one vice versa. From below figure (2) we can see the architecture of proposed system.

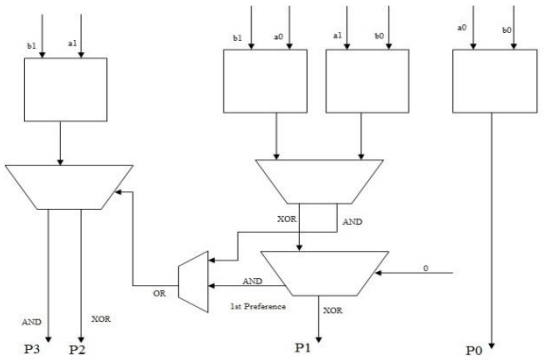


**Fig. 2. 2 x 2 Architecture of Redundant adaptive Multiplier**

The Redundant adaptive multiplier architecture is depends on the third layer operation .In the third layer two levels of operations are performed. Depends on the preference one level of operation is performed next the one but in the third layer AND & XOR operations are performed .In the AND gate one gate is used to perform the operation but in the XOR five gates are used for the operation is performed. Due to that first preference is goes to AND gate and the second preference goes to XOR gate so for that purpose depending on which operation is done performed quickly that operation is preferred first after that second operation is performed. In that architecture in third layer is first preference AND to do operation next XOR operation is performed.

In the Redundant adaptive multiplier architecture first layer consists of no. Of AND gates and the operation is performed in the first layer is AND. In the second layer two operations are performed first one is XOR and second one is AND operation.In the third layer three operations are performed AND, XOR and OR operations.In the internal operation of 2 x 2 redundant adaptive multiplier it consists of three layers and three parts. The inputs given to the first layer in the first part a0, b0 inputs given to the first layer AND gate and the result is goes down. In the second parta0, b1 and a1, b0 inputs is given to the first layer two AND gates the outputs of the AND gates is given to the inputs of the second layer multiplexer. In this multiplexer two operations are performed XOR, AND. The multiplexer having two outputs one output is XOR and second output is AND. The XOR output is given to the one input of the third layer multiplexer and AND output is given to the one input of the third layer OR gate. In this Redundant adaptive multiplier architecture operation is depends on the third layer. In this third layer two level of operations are performed depend on the preference of

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 7
March 2018

level of operation is performed and the second is performed vice versa. So in the third layer first preference is goes to AND gates next the XOR gate to perform the operations. In the third layer multiplexer XOR output is goes down AND output is given to the one input of OR gate and second input of the OR gate is coming from second layer multiplexer AND output.

## IV. RESULTS

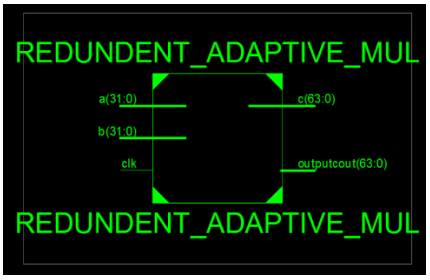


**Fig. 3. RTL schematic**

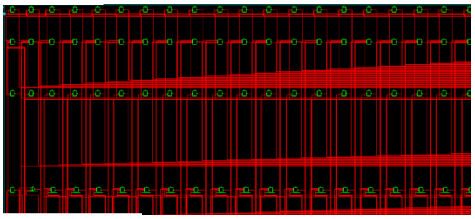

**Fig.4. technology schematic**

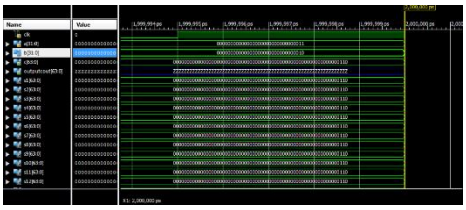

**Fig. 5. Output**

## V. CONCLUSION

In this paper 2×2 architecture of redundant adaptive multiplier is proposed. Here the relationship between extension degree *m* and the size of the smallest cyclotomic field, (*n*) should be greater than or equal to 2. In this case, a specific feature ofredundant representation was used to alleviate the redundancyproblem in this representation system. So both new architectures have the lowest delay cost compared with the existing RB architectures. The proposed architecture gives high performance compared to existed architecture.

## VI. REFERENCES

[1] Ing-Chao Lin, Member, IEEE, Yu-Hung Cho, And Yi-Ming Yang"Aging-Aware Reliable Multiplier Design With Adaptive Hold Logic" IEEE Transactions On Very Large Scale Integration(VLSI)Systems.

[2] H. Abrishami, S. Hatami, B. Amelifard, and M. Pedram, "NBTI-aware flip-flop characterization and design," in *Proc. 44th ACM GLSVLSI*, 2008, pp. 29–34

[3] S. V. Kumar, C. H. Kim, and S. S. Sapatnekar, "NBTI-aware synthesis of digital circuits," in *Proc. ACM/IEEE DAC*, Jun. 2007, pp. 370–375.

[4] A. Calimera, E. Macii, and M. Poncino, "Design techniqures for NBTItolerantpower-gating architecture," *IEEE Trans. Circuits Syst., Exp.Briefs*, vol. 59, no. 4, pp. 249–253, Apr. 2012.
[5] K.-C. Wu and D. Marculescu, "Joint logic restructuring and pin reorderingagainst NBTI-induced performance degradation," in *Proc. DATE*,2009, pp. 75–80.
[6] Y. Lee and T. Kim, "A fine-grained technique of NBTI-aware voltagescaling and body biasing for standard cell based designs," in *Proc. ASPDAC*,2011, pp. 603–608.
[7] M. Basoglu, M. Orshansky, and M. Erez, "NBTI-aware DVFS: A newapproach to saving energy and increasing processor lifetime," in *Proc.ACM/IEEE ISLPED*, Aug. 2010, pp. 253–258.
[8] K.-C. Wu and D. Marculescu, "Aging-aware timing analysis and optimizationconsidering path sensitization," in *Proc. DATE*, 2011, pp. 1–6.
[9] K. Du, P. Varman, and K. Mohanram, "High performance reliablevariable latency carry select addition," in *Proc. DATE*, 2012, pp. 1257–1262.
[10] A. K. Verma, P. Brisk, and P. Ienne, "Variable latency speculativeaddition: A new paradigm for arithmetic circuit design," in *Proc. DATE*,2008, pp. 1250–1255.