International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

An Area Efficient With Serial-In Parallel-Out by Using Rb Multiplier

Beeram Varalakshmi & K. Babu Rao

[1]PG StudentDept. Of ECE,Universal College of Engg & Tech. Perecherla, Guntur, A P, India 522438.

[2]Assistant Professor, ECE Dept. Universal College of Engg & Tech. Perecherla, Guntur, A P, India 522438.

ABSTRACT: *Redundant Based Multiplier Over Gaulois Field (GF (2 m)) has 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. Based on a specific feature of redundant representation in a class of finite fields, two new multiplication algorithms along with their pertaining architectures are proposed to alleviate this problem. Considering area-delay product as a measure of evaluation, it has been shown that both the proposed architectures considerably outperform existing digit-level multipliers using the same basis. It is also shown that for a subset of the fields, the proposed multipliers are of higher performance in terms of area-delay complexities among several recently proposed optimal normal basis multipliers. The main characteristics of the post place & route application specific integrated circuit implementation of the proposed multipliers for three practical digit sizes are also reported.*

Index Terms—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 the hardware 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 basis normal basis (NB), redundant basis (RB), and dual basis. In both normal basis (NB) and redundant representation (RB), squaring operation can be performed by applying a simple permutation operation on the coordinates. This makes them high efficient for the hardware implementations of cryptographic algorithms which utilize frequent squaring or exponentiation, like point addition/doubling in ECC. Moreover, redundant representation is of a special interest because of

its unique feature in accommodating ring type operations. This not only offers almost cost-free squaring operation but also eliminates the need for modular reduction in multiplication.

II.EXISTED SYSTEM

Fig. 1 shows the architecture, hereafter referred to as digit-level symmetrical Redundant Basis RB type−*a* multiplier. From top to bottom, the architecture contains an *n*-bit circular shift register which should be initialized with the coordinates of operand *B*. This shift register provides inputs to a wire expansion module with *n* inputs and $w(n-1)$ outputs followed by $((n-1)/2)$ identical modules shown inside the dashed boxes.

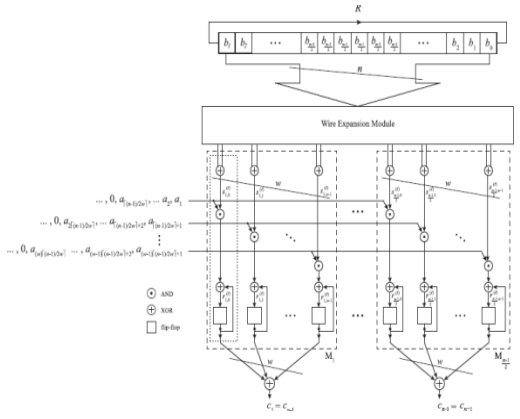

Fig. 1.Existed architecture for digit-Level SIPO RB multiplier

At the bottom, there is a network of XOR gates adding $2w$ outputs of each module together to form output coordinates. Each module is made of a layer of $2w$ AND gates receiving the outputs of the wire expansion module as their first input set. The second input set is received from certain bits of operand *A* in a digit-serial fashion. Each AND gate is followed by an XOR gate connected immediately to a flip-flop.

The output of the flip-flop is fed back to the XOR gate forming an accumulation unit together. Two AND gates along with their respective accumulation units form a structure responsible to realize the operations. One of these structures is shown in the Fig. 1 inside a dotted block for $j = 0$ and $k = 0$. In total, the architecture contains $w(n - 1/2)$ such structures, each of which consists of two AND gates, two XOR gates, and two flip-flops to generate and store each clock cycle.

III.PROPOSED SYSTEM

Recently, a new scheme is proposed which is based on the Error Correction Codes (ECC). In this technique, each filter can be equivalent of a bit and by using addition parity check bits can be computed. The operation of this technique is the output of the sum of the several inputs is the sum of the individual outputs. So, this is valid for any linear operation. It is assumed that there is only a single error on the system at any given point in time. There are three main contributions. They are

1) Error Correction Code is assessed to protect the parallel FFTs which show its effectiveness in terms of overheadand protection effectiveness.

2) A new technique is proposed based on the use of Parseval orsum of squares (SOSs) checks combined with parity FFT.

3) A new technique is proposed on which the ECC is usedon the SOS checks instead of the FFTs.

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

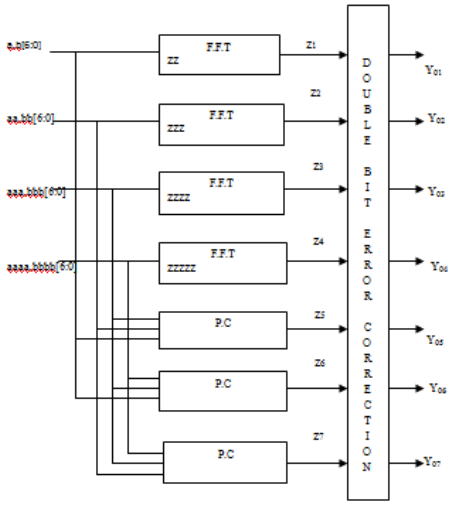

Fig 2. Parallel FFT protection using ECCs.

This scheme is evaluated by using FPGA implementations to assess the protection overhead. The protection overhead can be reduced by combining the use of ECCs and parseval checks. For the less error prone applications technique two can be used with Partial summation block replacing the Parseval check. Both the new techniques proposed uses minimum hardware resources compared to the existing design by the modification of Partial summation block for Sum of Squares.

IV.RESULTS

The below figures shows the simulation results of an encoder based radix-16 booth multiplier for improving speed and area efficiency. The proposed is designed an encoder-based radix-16 booth multiplier for
improving speed and area efficiency in XILINX 14.7 Using VERILOG HDL code and simulated using Model sim 6.5e To evaluate the efficiency of the proposed architecture

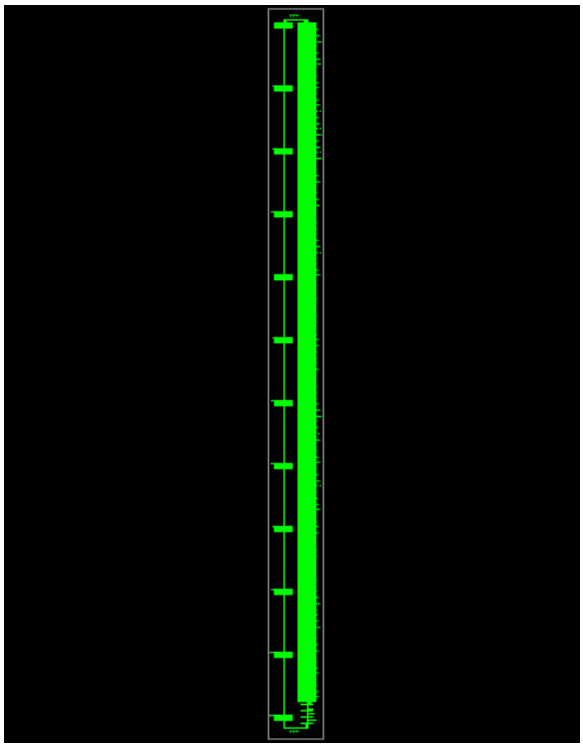

Figure3 :RTL Schematic view.

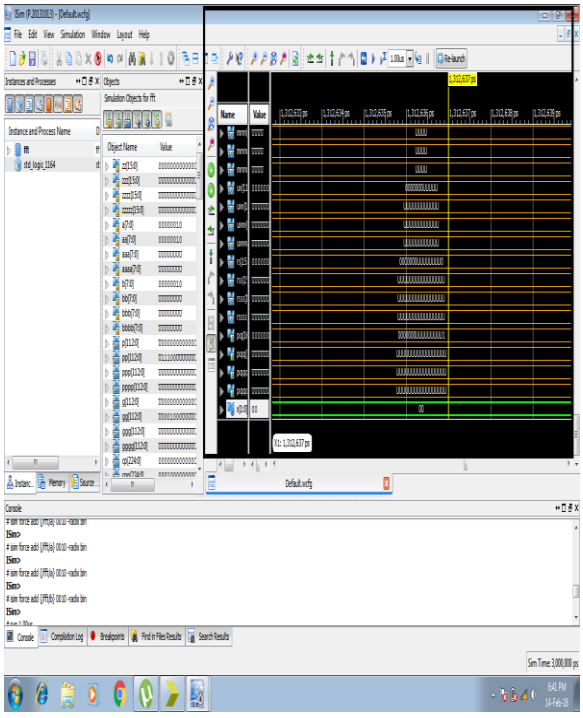

Figure 4 :Input1.

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

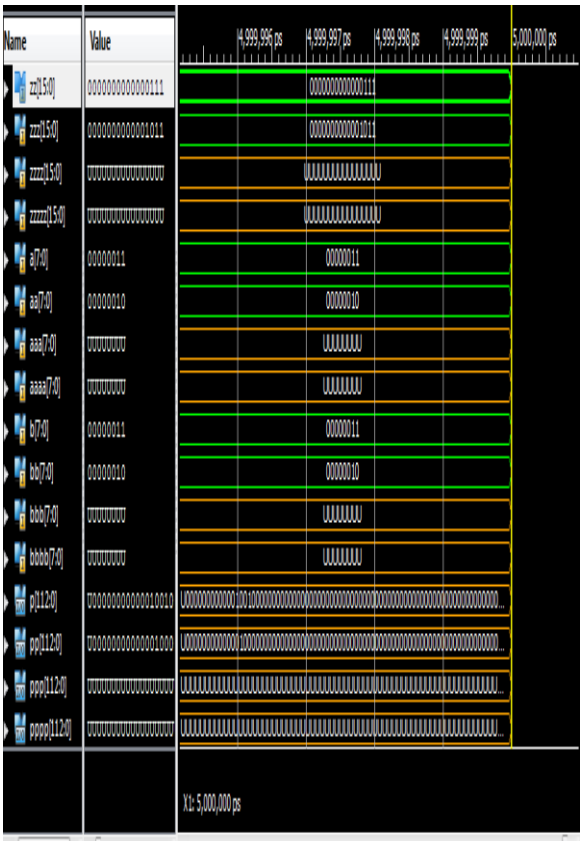

Figure 5 :Input2.

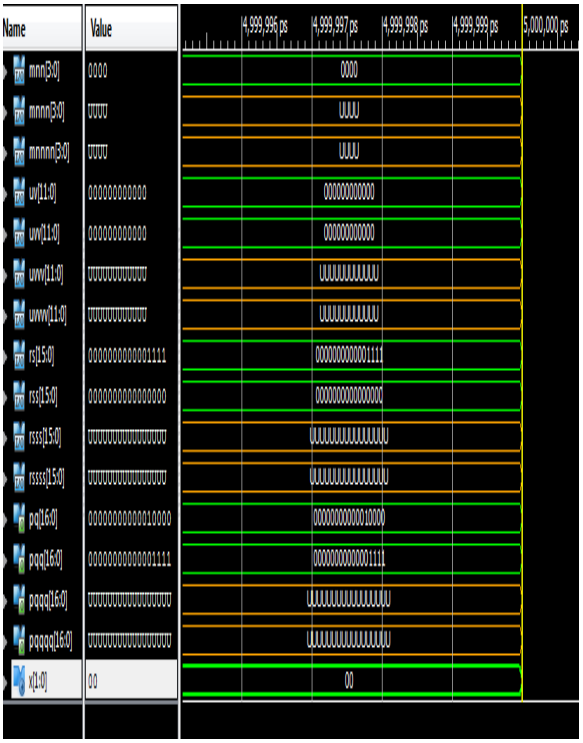

Figure 6 : Output.

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. The detection and location of the errors can be done using an SOS check per FFT or alternatively using a set of SOS checks that form an ECC. This technique can detect and correct only single bit error and it reduces area results in high speed compared to existing techniques.Future works can be done to find out new methods to obtain partial products in lesser time and with less hardware requirements.

VI.FUTURESCOPE

The Simulations can be extended to 24 bit, 32 bit word lengths. The complete FPGA and ASIC flow of the proposed FFT using radix-16 algorithm is to be carried out. The proposed designs can still be optimized to give better results. Folding technique can also be used more efficiently in the proposed architectures. Different higher radix FFT algorithms can be combined to get better results. Last but not the least, the multiplier-less concept along with the use of folding and pipelining can be extended to various types of computation extensive applications and might result in area, power consumption, and delay reduction.

VII.REFERENCES

[1] T. ElGamal, "A public key cryptosystem and a signature scheme basedon discrete logarithms," *IEEE Trans. Inf. Theory*, vol. 31, no. 4,pp. 469–472, Sep. 2006.

[2] I. F.Blake, G. Seroussi, and N. P. Smart, *Elliptic Curves in Cryptography*(London Mathematical Society Lecture Note Series). Cambridge, U.K.:Cambridge Univ. Press, 1999.

[3] A. J. Memezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbookof Applied Cryptography* (Discrete Mathematics and Its Applications).Boca Raton, FL, USA: CRC Press, 1996.

[4] T. Itoh and S. Tsujii, "A fast algorithm for computing multiplicativeinverses in *GF(2m)* using normal basis," *Inf. Comput.*, vol. 78, no. 3,pp. 171–177, 1988.

[5] C. Rebeiro, S. Roy, D. Reddy, and D. Mukhopadhyay, "Revisitingthe Itoh–Tsujii inversion algorithm for FPGA platforms," *IEEE Trans.Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 8, pp. 1508–1512,Aug. 2011.

[6] E. D. Mastrovito, "VLSI architectures for computations in Galois fields,"Ph.D. dissertation, Dept. Electr. Eng., Linköping Univ., Linköping,Sweden, 1991.

[7] J. Omura and J. Massey, "Computational method and apparatus for finitefield arithmetic," U.S. Patent 4 587 627, May 6, 1986.