# LOW-POWER DESIGN FOR A DIGIT-SERIAL POLYNOMIAL BASIS FINITE FIELD MULTIPLIER USING FACTORING TECHNIQUE

THATI YASHWANTH RAO[1], RUPA KUMAR DHANAVATH[2]
*[1]P.G Student, VLES*
*2 Assistant Professor, Department of Electronics and Communication Engineering, Nagole Institute Of Technology And science.*

**Abstract**: In CMOS-based application-specific integrated circuit (ASIC) designs, total power consumption is dominated by dynamic power, where dynamic power consists of two major components, namely, switching power and internal power. In this paper, we present a low-power design for a digit-serial finite field multiplier in GF(2m ). In the proposed design, a factoring technique is used to minimize switching power. To the best of our knowledge, factoring method has not been reported in the literature being used in the design of a finite field multiplier at an architectural level. Logic gate substitution is also utilized to reduce internal power. Our proposed design along with several existing similar works have been realized for GF on ASIC platform, and a comparison is made between them. The synthesis results show that the proposed multiplier design consumes at least 27.8% lower total power than any previous work in comparison The proposed architecture of this paper is analysis the logic size, area and power consumption using tanner tool.

**Index Terms**— Digit-serial architecture, elliptic curve (EC) cryptography, factoring method, finite field multiplier, low-power design

## I. INTRODUCTION

ACCORDING to Moore's law, the number of transistors on a chip doubles almost every two years. As a result, more functions and more complicated designs can be implemented on one chip, which leads to more power density and more heat on the circuits. Higher power density on the circuit reduces the reliability of the system and the battery life of the battery-based devices. Thus, power and energy consumptions of the circuit gain the same or probably more importance than area, especially for most compact portable devices that work by battery. Nowadays, lots of information are exchanged through networks, thus providing security services over networks is crucial for protecting information. Among security technologies, public key cryptography is popular and important, since it can provide certain unique security services, such as key exchange and digital signature. There are two public key cryptography techniques, in practice, namely, Rivest–Shamir– Adleman (RSA) and elliptic curve (EC) cryptosystem. Since EC cryptosystem uses shorter key compared with RSA to provide the same level of security, it is probably the more widely used technique in resource-constrained devices. Since EC used in an EC cryptosystem is defined over finite fields, low-power design of finite field arithmetic results in an EC cryptosystem, which consumes lower power and makes it more suitable for wireless applications. Binary extension field, denoted by GF(2m), is very attractive for hardware implementation, because it offers carryfree arithmetic. Multiplication operation has been paid most attention by researchers, because addition is simply bitwise XOR operation between two field elements, and the more complex operations, inversion, can be carried out with a few multiplications. In GF(2m), there are various methods to represent field elements, such as polynomial basis (PB), normal basis, and dual basis. PB is probably the most popularly used basis, because it is adopted as one of the basis choices by organizations that set standards for cryptography applications [1], [2]. Thus, a large number of architectures for efficient implementation of PB finite field multipliers have been proposed. In addition, new representations based on PB called shifted PB (SPB) [3] and generalized PB [4] have been proposed for efficient implementation of multipliers over GF(2m). The choice of the irreducible polynomial p(x) affects the complexity of a finite field multiplier. Various types of irreducible polynomials include trinomials, pentanomials, all one polynomials, and equally spaced polynomials. Standard organizations recommend irreducible polynomials with less number of nonzero terms (irreducible trinomials and pentanomials) for practical use as these types of irreducible polynomials can provide multipliers with lower complexity. PB finite field multiplier architectures can be categorized into bit-serial [5]–[7], bit-parallel [8]–[11], and digit-serial architectures. Bit-parallel structure is fast, but it is expensive in terms of area. In EC cryptography, the binary extension field size, m, is required to be on the order of 102, and thus a bit-parallel structure requires a very high I/O bandwidth, which is usually not available in the small portable and wireless devices. Bit-serial architecture is area efficient, but it is too slow for many applications. Power optimization were also considered in some of these works [12]–[18].

**Existing System:**

Binary extension field, denoted by GF(2m ), is very attractive for hardware implementation, because it offers carry free arithmetic. Multiplication operation has been paid most attention by researchers, because addition is simply bitwise XOR operation between two field elements, and the more complex operations, inversion, can be carried out with a few multiplications. In GF(2m ), there are various methods to represent field elements, such as polynomial basis (PB),normal basis, and dual basis. PB is probably the

most popularly used basis, because it is adopted as one of the basis choices by organizations that set standards for cryptography applications. Thus, a large number of architectures for efficient implementation of PB finite field multipliers have been proposed. In addition, new representations based on PB called shifted PB (SPB) and generalized PB have been proposed for efficient implementation of multipliers over GF(2m ). The choice of the irreducible polynomial p(x) affects the complexity of a finite field multiplier. Various types of irreducible polynomials include trinomials, pentanomials, allone polynomials, and equally spaced polynomials. Standard organizations recommend irreducible polynomials with less number of nonzero terms (irreducible trinomials and pentanomials) for practical use as these types of irreduciblepolynomials can provide multipliers with lower complexity.PB finite field multiplier architectures can be categorizedinto bit-serial, bit-parallel, and digitserialarchitectures. Bit-parallel structure is fast, but it is expensivein terms of area. In EC cryptography, the binary extension field size, m, is required to be on the order of 102 , and thus abit-parallel structure requires a very high I/O bandwidth, whichis usually not available in the small portable and wirelessdevices. Bit-serial architecture is area efficient, but it is tooslow for many applications. Power optimization were alsoconsidered in some of these works.

**Proposed System:**

A factoring technique is adopted in design of a digit-serial PB multiplier in GF(2m). To the best of our knowledge, a factoring method has not been reported in the literature being used in the design of a finite field multiplier at an architectural level. A logic gate substitution technique is also used in our design to reduce the internal power consumption of the proposed digit-serial multiplier. The synthesis results show that our new design has both the lowest dynamic power consumption and the lowest total power consumption among several similar existing works.

**Binary Extension Field GF(2m ):**

A finite field is defined as a set of finite many elements, where addition and multiplication are the operations defined on the set. A binary extension field, GF(2m), is generated by a degree mirreducible polynomial, p(x) =xm+pm−1xm−1+⋯+p2x2+p1x+1, where pi is either 0 or 1. p(x) also specifies a PB{1,x,x 2 ,...,x m−1}. Each element of GF(2m) can be represented as a polynomial of degree at mostm−1 over GF(2m) with respect to the PB. For instance, an element A∈GF (2m) can be expressed as

A(x)=am−1xm−1+am−2xm−2+⋯+a2x2+a1x+a0(1)

With

ai∈GF(2), 0≤i ≤m−1.

Multiplication of two field elementsA(x)andB(x)of thebinary extension field can be given by

C(x)=A(x)B(x)modp(x). (2)

**Digit-Serial PB Multiplication:**

In digit-serial multiplication, the bits of one operand aredivided into digits of sizek while the bits of the other input operand are processed in parallel. Only one digit of the firstoperand is accessible in each clock cycle.

Power Dissipation for CMOS-Based Circuits:

Power consumption in a CMOS-based design contains twomajor components: static power and dynamic power.For a CMOS-based design, dynamic power plays a dominantrole in the total power consumption.

**Multiplier Architecture:**

An architecture diagram for the proposed digit-serial PBmultiplier in GF(2m) is shown in Fig. 2. There are threemodules, as shown in Fig. 2, namely, k × m multiplier, constant multiplier, and field adder.

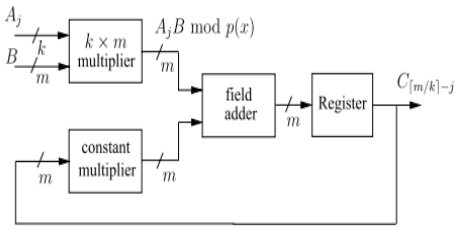



Fig. 2. Proposed digit-serial PB multiplier in GF(2m).

1. k × m multiplier takes one operand B of m-bit and the other operand Aj of k-bit. Note that Aj changes for different clock cycles j. Thus, it has higher switching activity compared with operand B. A straightforward realization of this module was used. For the comparison purpose, it is given in Algorithm 1. Note that a modification to this algorithm using a factoring method is proposed in Section III-B. The three steps in Algorithm 1 are, respectively, realized with the circuit blocks from left to right, as shown in Fig. 3(a).

2. Constant multiplier module realizes multiplication between a field element and the constant xk .

3. Field adder module implements finite field addition using m two-input XOR gates formed as a one-layer network.

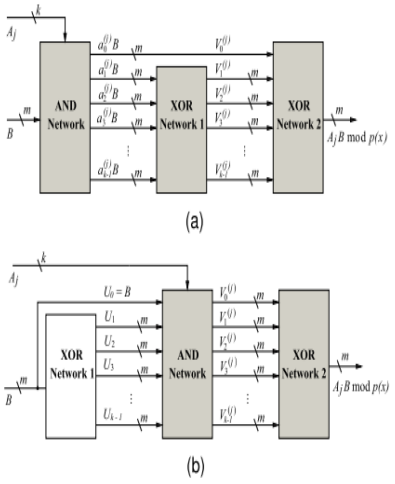
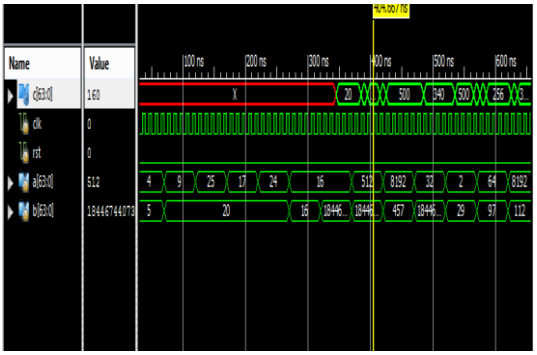


Fig. 3. k × m multiplier. (a) Without applying factoring. (b) With applied factoring method (the shaded modules indicate high switching activity).

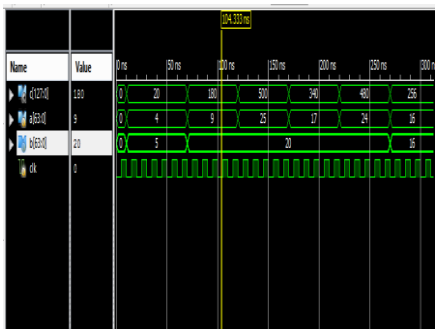
Consider Algorithm 2 as the modified version of Algorithm 1 for the operation by k × m multiplier module. While in Algorithm 1, transitions of high activity input Aj are involved in all the three steps, Step 1 in Algorithm 2 (Ui = Bxi mod p(x),i = 0, 1,..., k − 1) is not affected by Aj and it also does not depend on the cycle j, which means there is no input data transitions involved in this step in Algorithm 2 for all the cycles j = 0, 1,..., m/k− 1.

The two designs of k × m multiplier are shown in Fig. 3 both of which include three submodules: AND network, XOR network 1, and XOR network 2. The circuit shown in Fig. 3(a) first computes a(j) i B,i = 0, 1,..., k − 1 in AND network, and then computes (a(j) i B)xi mod p(x) = V(j) i at XOR network 1. In this circuit, input Aj that has higher switching activity compared with input B affects all the three submodules, which results in larger number of high activity nets (outputs of the shaded modules), and thus causes higher switching activity in the k × m multiplier. Factoring can be applied to decrease the switching activity of the k ×m multiplier by reducing the logic depth connected to high activity input Aj . In Fig. 3(b), the proposed design is obtained from Fig. 3(a) by applying a factoring technique. As shown in Fig. 3(b), the logic depth connected to input Aj is reduced by switching the submodules AND network and XOR network 1. In XOR network 1, it computes Ui = Bxi mod p(x),i = 1, 2,..., k − 1. Then at AND network, V(j) i = a(j) i Ui,i = 0, 1,..., k − 1 are obtained. As shown in Fig. 3(b), input Aj with high switching activity does not propagate through submodule XOR network 1. Therefore, the number of nets with high switching activity is minimized, which results in lower switching activity in the proposed design.

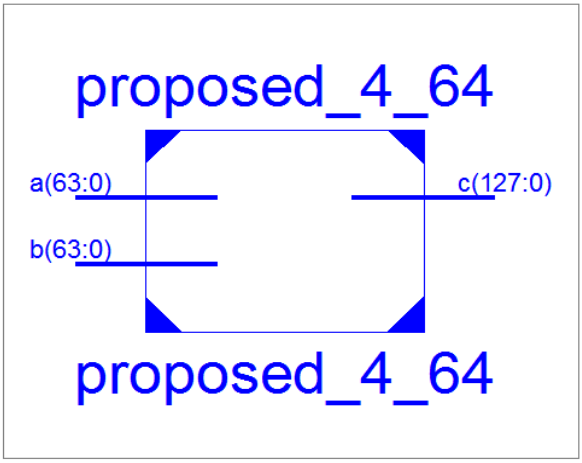
## II. SIMULATION RESULTS




**EXISTING METHOD**




**PROPOSED METHOD**




**RTL SCHEMATIC**

| Device Utilization Summary (estimated values) | | | |
|---|---|---|---|
| Logic Utilization | Used | Available | Utilization |
| Number of Slices | 345 | 4656 | 7% |
| Number of 4 input LUTs | 617 | 9312 | 6% |
| Number of bonded IOBs | 202 | 232 | 87% |

**DESIGN SUMMARY**

## III. CONCLUSION

The factoring technique has been adopted for a new architecture level design that minimizes the switching activities and, consequently, reduces the power consumption of a digit-serial PB multiplier in GF(2m). The logic gate substitution technique has also been utilized to further reduce the power consumption of the digit-serial PB multiplier. Moreover, the area complexity of the finite field multiplier has been reduced. The VLSI experimental results show that the new architecture consumes about 27.8% lower power and 31.6% lower energy and achieves 43% lower EA product compared with the best previous work. The proposed low-power digit-serial PB multiplier is suitable for implementing low-power EC cryptosystems in embedded systems with limited power resources. The proposed digit-serial PB multiplier can also be used as an IP core for fast implementation of EC cryptosystems.

## IV. REFERENCES

[1]. C. F. Kerry, "Digital signature standard (DSS)," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, FIPS PUB 186-4, 2013.
[2]. IEEE Standard Specifications for Public-Key Cryptography, IEEE Standard 1363-2000, Aug. 2000, pp. 1–228.
[3]. H. Fan and Y. Dai, "Fast bit-parallel GF(2n) multiplier for all trinomials," IEEE Trans. Comput., vol. 54, no. 4, pp. 485–490, Apr. 2005.
[4]. A. Cilardo, "Fast parallel GF(2m ) polynomial multiplication for all degrees," IEEE Trans. Comput., vol. 62, no. 5, pp. 929–943, May 2013.
[5]. T. Beth and D. Gollman, "Algorithm engineering for public key algorithms," IEEE J. Sel. Areas Commun., vol. 7, no. 4, pp. 458–466, May 1989.
[6]. L. Song and K. K. Parhi, "Efficient finite field serial/parallel multiplication," in Proc. Int. Conf. Appl. Specific Syst., Archit. Processors (ASAP), Aug. 1996, pp. 72–82.
[7]. M. Nikooghadam and A. Zakerolhosseini, "Utilization of pipeline technique in AOP based multipliers with parallel inputs," J. Signal Process. Syst., vol. 72, no. 1, pp. 57–62, Jul. 2013.