International Journal of Research
Available at https://edupediapublications.org/journal
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

Hybrid Double Multiplication Architectures using new SOBL Mastrovito Multiplier

M. Rajyalakshmi [1], Dr. Ch. Ravikumar [2]
1 PG Scholar, Dept of ECE, Prakasm Engineering College, AP, India
2 Professor and Head of Electronics Department ,Prakasam Engineering Colege,AP,India

Abstract: Serial-bit level multiplication scheme has important internal feature. As a result of the multiplication of each clock cycle to generate a bit of it one has the ability to output. However, GF(2^m) is based on the representation of the general use of the multipliers in the existing serial bit-level computational complexity, which limits its usefulness for many applications; Thus, the optimum use of the serial bit-level representation on the basis of polynomial coefficient is needed. In this paper, we propose a new serial bit-level Mastrovito multiplier schemes. We are in terms of the complexities of the time, the proposed multiplier schemes available in the literature have shown to outperform existing serial bit-level schemes. In addition, the proposed use of multiple schemes, we present a new hybrid-double multiplication architectures.

The serial bit-level patterns and schemes presented by the proposed hybrid-double multiplication architectures are implemented over GF(2^{163} and GF(2^{233}) , theoretical and experimental results are presented.

Keywords— *serial-out, polynomial basis, bit-level multiplier, Mastrovito multiplier, hybrid-double multiplication*

1. Introduction

Finite field arithmetic has been widely applied in applications of different fields like error-control coding, cryptography, and digital signal processing [1], [2], [3], [4]. The arithmetic operations in the finite fields over characteristic two GF(2m) have gained widespread use in public-key cryptography such as point multiplication in elliptic curve cryptography [5], [6], and exponentiation-based cryptosystems [7], [8]. The finite field GF(2m) has 2m elements and each of its elements can be represented by its m binary coordinates based on the choice of field-generating polynomial. For such a representation, the addition is relatively straight-forward by bit-wise XORing of the corresponding coordinates of two field elements. On the other hand, the multiplication operation requires larger and slower hardware. Other complex and time-consuming operations such as exponentiation, and division/inversion are implemented by the iterative application of the multiplication operations. Much of the ongoing research in this area is focused on finding new architectures to implement the arithmetic multiplication operation more efficiently (for example [9], [10], [11]). Finite field multipliers with different properties are obtained by choosing different representations of the field elements. With the advantages of low design complexity, simplicity, regularity, and modularity in architecture, the standard or polynomial basis (PB) representation, is extensively used for cryptographic applications [12], [13]. In the PB, a multiplier requires a polynomial multiplication followed by a modular reduction. In practice, these two steps can be combined into a single step by using the so-called Mastrovito matrix [14], [15].

The properties and complexities of the PB multipliers depend heavily on the choice of a field-generating polynomial. In this paper, we first consider an irreducible polynomial with ω, $\omega \geq 3$, non-zero terms (denoted by ω-nomials). We then obtain a further optimized structure for the special irreducible trinomial ($\omega = 3$). The implementation of finite field multipliers can be categorized, in terms of their structures, into three groups of parallel-level, digit-level and bit-level types. The bit-level multiplier scheme, which processes one bit of input per clock cycle, is area-efficient and suitable for resource-constrained and low-weighted devices.

The bit- level type multiplication algorithms when the PB is used are classified as least significant bit first (LSB-first), and most significant bit first (MSB-first) schemes [16]. The bit-level multiplier can be further categorized into two types of either parallel or serial output. In the traditional parallel-out bit-level (POBL) multipliers [16], all of the output bits of the multiplication(fromthefirstbittothelastbit)aregenerate dattheendofthelastclockcycle.

Serial-out bit level(SOBL)multipliers, on the other hand, generate an output bit of the product sequentially, after a certain number of clock cycles. A multiplication scheme based on serial-out architecture, i.e., SOBL, has certain advantages as

International Journal of Research
Available at https://edupediapublications.org/journal
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

compared to the traditional parallel-out architecture .For instance ,combining SOBL with a traditional LSB-first POBL one, would make fast exponentiation and inversion possible [17], [18].

The author of [19], has proposed a SOBL multiplication architecture that is constructed by the trinomials and the ω-nomials irreducible polynomials in GF(2^m) using PB representation. In this paper, alternative schemes for the serial-out multiplication in the PB over GF(2^m) for both trinomial and ω-nomial irreducible polynomial are developed.

We have proposed a new scheme for the SOBL multiplication architecture in the PB over GF(2^m) for the ω-nomials, then we further optimized it for the irreducible trinomials. Both schemes have lower critical path delay compared to previously published results.

We extended the traditional POBL multiplier schemes presented in [16] to propose two new LSB-first/MSB-first POBL double multiplication architectures, which perform two multiplications together after 2m clock cycles

II . PRELIMINARIES

The binary extension field GF(2^m) can be viewed as an m-dimensional vector space defined over GF(2^m) [1]. A set of m linearly independent vectors (elements of GF(2^m)) is chosen to serve as the basis of representa- tion. An explicit choice for a basis is the ordered set αm−1, ···, α2, α, 1. where α ∈ GF(2m) and is a root decoding time. Technical standards, in memory devices become larger and more powerful error correction codes are needed. Euclidean geometry to overcome the problems in this paper as they use more modern codes.

of an irreducible polynomial P(x). This basis is called the polynomial basis (PB). Each element is represented by a polynomial of degree m−1, whose coefficients are the binary digits 0 or 1. All arithmetic operations are performed modulo 2. A straightforward GF(2m) multiplication computa- tions consists of two parts, the product of two field elements, followed by a modular reduction [20], [21]. Suppose A = (am−1, ···, a1, a0), B = (bm−1, ···, b1, b0) are two arbitrary field elements, i.e., A, B ∈ GF(2m), then to obtain the field multiplication of A and B, AB is computed first; it is then followed by the modular reduction, i.e., C , AB mod P(α). In [14], [15], Mastrovito has proposed an efficient dedicated parallel multiplication method that combines the two parts of the product and the modular reduction into a single step. He showed that the coordinates of C are obtained from the matrix-by-vector product of M and b.

$$c = [cm−1, ···, c1, c0]T = M·b$$

where T denotes the transposition; the column vector b = [bm−1, ···, b1, b0]T contains the coordinates of the multiplier B = (bm−1, ···, b1, b0) ∈ GF(2m), and M is an m × m binary matrix whose entries depend on the coordinates of A ∈ GF(2m). This equation was implicitly used in [22], [23], and [24] to derive the parallel-level multiplier and is now used in this work to design a new SOBL multiplier. Sunar and Koc¸ [22] have studied the Mastrovito matrix M, and have presented a formulation for the Mastrovito algorithm using the irreducible trinomials. Halbuto˘gullari and Koc¸ in [23] have presented a new architecture for the Mastrovito multiplication and have also shown that the coefficient of the product AB can be obtained from the matrix-by-vector product of d , [d2m−2, ···, dm, dm−1, ···, d0]T = Z·b, where Z is a 2m−1×m binary matrix

III. PROPOSED MULTIPLIER ARCHITECTURES

In this section, an approach to the architecture design of the SOBL multiplier for both the ω-nomials and the irreducible trinomials is presented in detail.

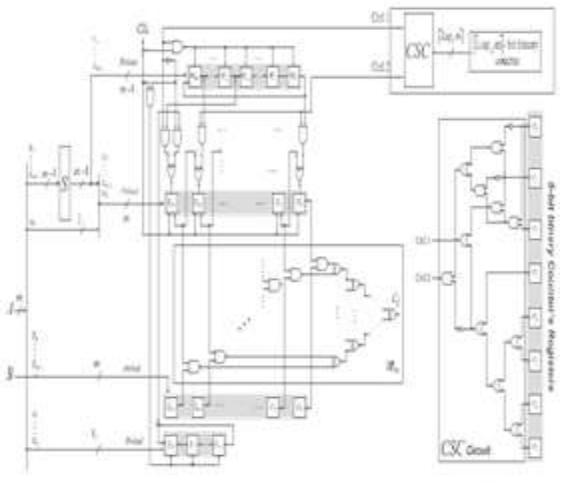

Figure1: Proposed Mastrovito multiplier.

Both architectures are capable of generating an output bit with a total of one computational clock cycle. We remark that the bit-level structure multiplier is considered as an iterative architecture.

International Journal of Research
Available at https://edupediapublications.org/journal
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 01
January 2017

Thus, for any bit-level (or digit-level) multiplier, a main control unit that generates a counter is required to generate the load, start, complete, and other control signals. In our approach, additional control signals are needed in computation of the multiplication product, which can also be generated from the main control unit. However, in order to provide a complete and in-depth view of the components involved in our approach, a binary counter that generates the necessary control signals for the computation of the multiplication product is included in our architecture. In our model, a series carry synchronous counter is used, which is implemented with a register for every bit and an AND gate for every bit except the first and last bit. The carry- in to carry-out delay in the series carry synchronous counter is (dlog2 me−2)TA, where TA denotes the delay ofthe2-inputANDgate.Wefurtherremarkthattheloop iterations of the Algorithm 1 are mapped into hardware clock counter that are also denoted by j.

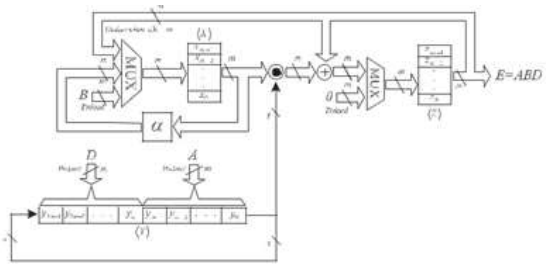

Figure2:Proposed LSB first system POBL system

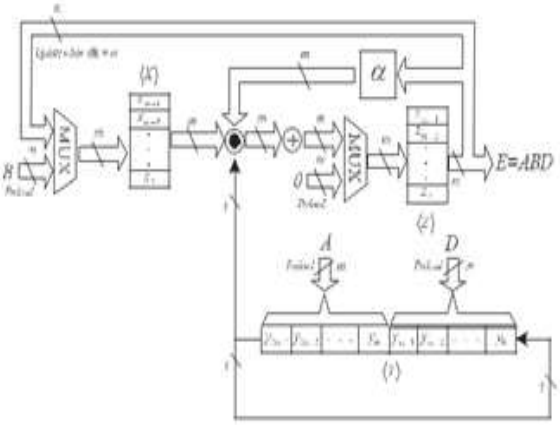

Figure3:Proposed MSB firstsystem POBL system

we first extend the traditional parallel-out bit-level (POBL) multiplier schemes presented in [16] to propose new POBL double multiplication architectures. We then, propose new hybrid-double multiplication architectures using PB over GF(2m). Note that all the presented architectures can be easily modified to extend their structure into the digit-level. However, for the sake of simplicity, in this work we did not investigate on the techniques for the digit-level structures.

IV.SIMULATION RESULTS

In these section we are presenting the simulation results produced after executing the proposed method in Models sim 16.1 ISE. We write the entire code in VHDL.

Figure 4: waveform for mastrovito multiplier

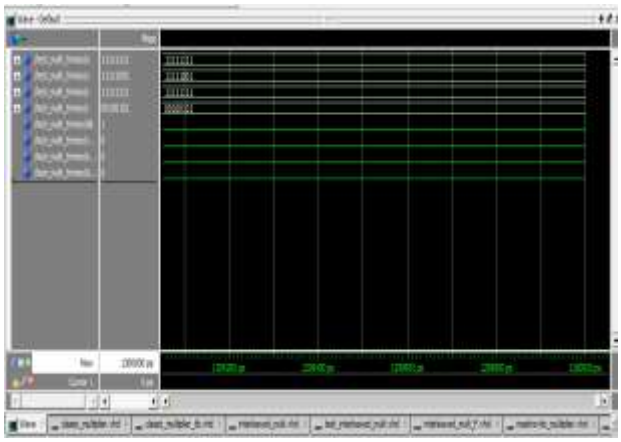

Figure 5: wave form for Mastrovito_trinom multiplier

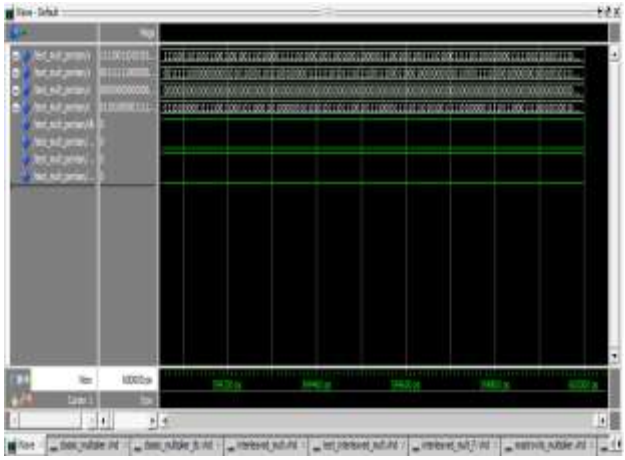

Figure6: wave form for mastrovito_pentanom multiplier

Type of multiplier	Bit latency	Total latency	Critical path delay
LSB First POBL	163	163	T_A+T_x
MSB first POBL	163	163	T_A+T_x
Existed SOBL	1	163	$T_A+11\ T_x$
Proposed SOBL	1	163	$T_A+8\ T_x$

Table 1.Comparison of proposed method with existing for GF(2^163)

Type of multiplier	Bit latency	Total latency	Critical path delay
LSB First POBL	233	233	T_A+T_x
MSB first POBL	233	233	T_A+T_x
Existed SOBL	1	233	$T_A+10\ T_x$
Proposed SOBL	1	233	$T_A+8\ T_x$

Table 1.Comparison of proposed method with existing for GF(2^233)

CONCLUSION

We have presented new hardware schemes for the serial- out bit-level (SOBL) multiplier in PB representation over GF(2^m) for both the ω-nomial and the irreducible trinomial. Compared to previously published results in terms of time complexities, the work presented here out perform the existing SOBL multiplier schemes. We have also extended the traditional POBL multiplier schemes to new POBL double multiplication architectures, which perform two multiplications after 2m clock cycles. Then, we proposed three hybrid-double multiplication architectures in PB over GF(2^m). These hybrid multiplier structures perform two multiplications with latency comparable to the latency of a single multiplication, i.e., after m + 1 clock cycles. We have obtained the space and time complexities of the presented multipliers and have compared them with their counterparts. For the practical purposes, all the schemes presented in this work have been implemented in ASIC technology over both GF(2^163) and GF(2^233),and the area, timing ,power consumption, and energy results have been presented.

REFERENCE

[1] R. Lidl, and H. Niederreiter, Introduction to Finite Fields and Their Applications. 2nd Ed., Cambridge Univ. Press, Cambridge, UK, Aug. 1994.

[2] R. E. Blahut, Theory and Practice of Error Control Codes. Addison- Wesley, Reading, MA, May 1983.

[3] A. J Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone, and T. Yaghoobian, Applications of Finite Fields. Kluwer Academic Publishers, Boston, MA, 1993.

[4] R. E. Blahut, Fast Algorithms for Digital Signal Processing. 1st Ed., Addison-Wesley, Reading, MA, Sept. 1985.

[5] V. S. Miller, "Use of Elliptic Curves in Cryptography," In Proc. of Advances in Cryptology-CRYPTO'85, LNCS, 1986, vol. 218, pp. 417-426.

[6] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Com- putation, vol. 48, no. 177, pp. 203-209, Jan. 1987.

[7] T. Elgamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469-472, Jul. 1985.

[8] W. Diffie, and M. Hellman, "New Directions in Cryptography," IEEE Trans. Inf. Theory, vol. 22, no. 6, pp. 644-654, Nov. 1976.

[9] M. A. Hasan, A. H. Namin, and C. Negre, "Toeplitz Matrix Approach for Binary Field Multiplication Using Quadrinomials," IEEE Trans. VLSI Systems, vol. 20, no. 3, pp. 449-458, Mar. 2012.

[10] H. Wu, "Bit-Parallel Polynomial Basis Multiplier for New Classes of Finite Fields," IEEE Trans. Computers, vol. 57, no. 8, pp. 1023- 1031, Aug. 2008.

[11] A. Hariri, and A. Reyhani-Masoleh, "Bit-Serial and Bit-Parallel Montgomery Multiplication and Squaring over GF(2m)," IEEE Trans. Computers, vol. 58, no. 10, pp. 1332-1345, Oct. 2009.

[12] I.S.Hsu, T.K.Truong, L.J.Deutsch, and I.SReed, "A Comparison of VLSI Architecture of Finite Field Multipliers Using Dual, Normal, or Stnadard Basis," IEEE Trans. Computers, vol. 37, no. 6, pp. 735-739, Jun. 1988.

[13] D.Hankerson, A.Menezes, and S.Vanstone, Guide to Elliptic Curve Cryptography. New York: Springer-Verlag, 2004.

[14] E. D. Mastrovito, "VLSI Designs for Multiplication over Finite Field GF(2m)," Proc. Sixth Symp. Applied Algebra, Algebraic Al- gorithms, and Error Correcting Codes (AAECC-6), pp. 297-309, Jul. 1988.

[15] E. D. Mastrovito, "VLSI Architectures for Computation in Galois Fields," PhD thesis, Link¨oping Univ., Link¨oping, Sweden 1991.

[16] T. Beth, and D. Gollmann, "Algorithm Engineering for Public Key Algorithms," IEEE J. Selected Areas in Communications, vol. 7, no. 4, pp. 458-466, May 1989.

[17] R. Azarderakhsh, and A. Reyhani-Masoleh, "Low-Complexity Multiplier Architectures for Single and Hybrid-Double Multipli- cations in Gaussian Normal Bases," IEEE Trans. Computers, vol. 62, no. 4, pp. 744-757, Jan. 2012.

[18] R. Azarderakhsh, K. J¨arvinen, and V. Dimitrov, "Fast Inversion in GF(2m) with Normal Basis Using Hybrid-Double Multipliers," IEEE Trans. Computers, in process.

[19] A. Reyhani-Masoleh, "A New Bit-Serial Architecture for Field Multiplication Using Polynomial Bases," In Proc. of CHES 2008, Aug. 2008, LNCS 5154, pp. 300-314.

[20] H. Wu, "Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis," IEEE Trans. Computers, vol. 51, no. 7, pp. 750- 758, Jul. 2002.

[21] F. Rodriguez-Henriguez, and C,. K. Koc,, "Parallel Multipliers Based on Special Irreducible Pentanomials," IEEE Trans. Comput-ers, vol. 52, no. 12, pp. 1535-1542, Dec. 2003.

[22] B. Sunar, and C,. K. Koc,, "Mastrovito Multiplier for All Trinomi- als," IEEE Trans. Computers, vol. 48, no. 5, pp. 522-527, May 1999.

[23] A. Halbuo¨gullari, and C,. K. Koc,, "Mastrovito Multiplier for General Irreducible Polynomial," IEEE Trans. Computers, vol. 49, no. 5, pp. 503-518, May 2000.1

[23] L. Chen, X. Mao, Y. Xue, and L. L. Cheng, "Speech emotion recognition: Features and classification models," Digit. Signal Process. A Rev. J., vol. 22, no. 6, pp. 1154–1160, 2012.

[24] T. Zhang, and K. K. Parhi, "Systematic Design of Original and Modified Mastrovito Multipliers for General Irreducible Polyno- mials," IEEE Trans. Computers, vol. 50, no. 7, pp. 734-748, Jul. 2001.

AUTHOR'S BIOGRAPHY:

1. **M.Rajyalakshmi-** received the B.Tech degree in Electronics and communication Engineering from JNTU Kakinada, in 2013 and Doing Maters with specialization in VLSI and Embedded systems in Prakasam Engineering college ,Kandukur, A.P ,INDIA. Her main areas of research in Engineering is VLSI and Embedded systems .

2. **Dr.CH.RAVIKUMAR-** received Doctorate from KL University. Currently working as Head of the Electronics Department in Prakasam Engineering College, Kandukur, A.P.India His main areas of research in Engineering are VLSI and Digital image processing.