International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2018, Submitted in May 2018, iajesm2014@gmail.com

Design Analysis of Hybrid-Size Digit-Serial Systolic Multiplier

Vishal Awasthi, Member, IETE,
Ajeet Kumar Srivastava, ECE Department, UIET, CSJM University, Kanpur
Anand Kumar Gupta, ECE Department, UIET, CSJM University, Kanpur

Abstract:

The Novel Hybrid-Size Digit-Serial Systolic Multiplier is a new approach to designing efficient and high-performance multipliers for use in digital signal processing and other applications. The multiplier uses a combination of digit-serial and systolic architectures to achieve a high degree of parallelism and minimize the use of resources. Typically, this kind of multiplier is only intended to be used with a specific field size, which actually sets the true security level of the cryptosystem and so restricts the flexibility of how cryptographic applications can be used. The proposed design employs a hybrid-size architecture that enables the efficient use of both small and large multipliers. This approach allows for better resource utilization and reduces the overall hardware complexity. The proposed design has been implemented and tested on an FPGA, and the results show that the hybrid-size digit-serial systolic multiplier achieves high performance with lower resource utilization than existing designs. To formulate the mathematical concept of the hybrid-size realisation, a novel algorithm is first developed. A unique digit-serial structure is then produced following effective mapping using the suggested algorithm. This novel approach to designing multipliers has the potential to improve the efficiency and performance of digital signal processing systems and other applications that require high-speed arithmetic operations.

Keywords: digit-serial; hybrid-size; low-complexity; systolic structure; digital multiplication

1. Introduction

In modern digital systems, multiplication is one of the most frequently used arithmetic operations. Efficient and high-performance multipliers are essential for a variety of applications such as digital signal processing, cryptography, and multimedia processing. There have been many attempts to design efficient multipliers that can perform arithmetic operations with low latency, low power consumption, and minimum hardware resources. The traditional approach for designing multipliers is based on the parallel processing of the operands and the bit-serial processing of the partial products. However, this approach can result in high hardware complexity and power consumption, particularly for large operands.

To address these challenges, researchers have explored alternative multiplier architectures, such as digit-serial and systolic multipliers. Digit-serial multipliers are based on the parallel processing of digits and the bit-serial processing of partial products, which can reduce hardware complexity and power consumption. Systolic multipliers use a pipelined structure to perform arithmetic operations, which can increase the throughput of the system.

In this context, the Novel Hybrid-Size Digit-Serial Systolic Multiplier is a new approach to designing efficient and high-performance multipliers. The proposed design combines the advantages of both digit-serial and systolic architectures to achieve a high degree of parallelism and minimize the use of resources. The hybrid-size architecture enables the efficient use of both small and large multipliers, allowing for better resource utilization and reducing overall hardware complexity.

Finite field multipliers have drawn a lot of interest lately because of their crucial roles in numerous cryptosystems, including curve cryptography (CC), specifically on hardware platforms [1]. Three different structure types, known as bit-serial, parallel, and digit-serial, are typically associated with finite field multipliers. Digit-serial structures are frequently favoured over the other two in many applications because of the effective trade-off in area-time complexities [2].

Systolic structure is becoming increasingly appealing in high-performance hardware systems as artificial intelligence technology advances [3]. Due to their improved qualities, such as high throughput rate, modularity, and digit-serial systolization of predetermined field multipliers has the potential to be used in high-performance cryptosystems. In comparison to the previously described

International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2018, Submitted in May 2018, iajesm2014@gmail.com

one, an effective systolic finite field multiplier is presented in [3], where its complexity is prominently decreased.; (ii) a systolic-like digit-serial multiplier is reported in [4], and it is discovered that the systolic structure proposed is particularly suitable for the Reed-Solomon Codec; (iii) an efficient digit-serial multiplier is reported in [5]. An effective resource-sharing method is used in another digit-serial systolic multiplier to attain low critical-path and high-performance action [8]; (vii) It is mentioned in [9] that a useful systolic digit-serial multiplier exists, with the complexity there being the lowest found in the literature. These designs unquestionably mark the most significant development in the area of systolic digit-serial multipliers.

The proposed work is accomplished by combining the efforts of two cogent, interdependent stages: (i) the proposal of a unique hybrid-size digit-serial systolic multiplication algorithm that gives both trinomial- and pentanomial-based multipliers enough flexibility; and (ii) the mapping of the suggested algorithm into a novel systolic design using a number of optimization techniques. A thorough analysis of complexity and comparison with existing designs have also been conducted to demonstrate the effectiveness of the proposed design, which not only makes it simple to switch between various field sizes but also has lower area-time complexities than the single field-size digit-serial systolic multipliers currently in use. The suggested design can be applied to various field-size cryptosystems in addition to serving as a standard core but can also be used as the central processing unit in reconfigurable cryptographic processors (when an adjustable field-size option is required).
The remaining sections are arranged as follows: The proposed digit-serial multiplication algorithm's mathematical formulation is presented in Section 2. The proposed systolic structure is mapped from the algorithm in Section 3 in detail. Section 4 and 5 demonstrates the analysis and comparison. In Section 6, the conclusion is presented.

2. Mathematical Modelling of the Digit-Serial Systolic Algorithm

The proposed Hybrid-Size Digit-Serial Systolic Multiplier uses a combination of small and large multipliers to efficiently compute the product of two multi-digit numbers. The multiplication algorithm involves the following steps:

1. Partition the two multi-digit numbers into smaller groups of digits, with each group containing k digits. The size of k depends on the design requirements and can be chosen to optimize the performance.
2. For each group of digits, compute the partial products using a conventional booth algorithm for small multipliers and a modified booth algorithm for large multipliers.
3. Utilize a carry-save adder (CSA) tree to assemble the incomplete products in order to lessen their number and boost parallelism.
4. Perform the final addition using a carry-select adder (CSLA) to obtain the full product.

The multiplication algorithm can be mathematically formulated as follows:

Let A and B be two multi-digit numbers of n digits each, where $A = a[n-1]a[n-2]\ldots a[0]$ and $B = b[n-1]b[n-2]\ldots b[0]$.
Let k be the size of the groups of digits, with $m = n/k$ groups for both A and B.
The multiplication of A and B can be expressed as:

$$AB = ((a[m-1] * b[m-1]) * 2\text{^}(k*(m-1))) + ((a[m-2] * b[m-2]) * 2\text{^}(k*(m-2))) + \ldots + ((a[0] * b[0]) * 2\text{^}(k*0))$$

where * denotes multiplication, and ^ denotes exponentiation.

The partial products can be computed using a conventional booth algorithm for small multipliers and a modified booth algorithm for large multipliers. The partial products are then accumulated using a carry-save adder tree to obtain the final partial products, which are then added using a carry-select adder to acquire the full product AB. The proposed multiplication algorithm enables the efficient use of both small and large multipliers, reducing the hardware complexity and improving resource

International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2018, Submitted in May 2018, iajesm2014@gmail.com

utilization. The use of a systolic pipeline and a CSA tree further reduces the latency and improves the parallelism of the operation, making it a promising approach for high-speed arithmetic operations.

3. **Proposed Hybrid-Size Digit-Serial Systolic Multiplier**

The proposed Hybrid-Size Digit-Serial Systolic Multiplier is based on a combination of digit-serial and systolic architectures. The hybrid-size architecture allows for the efficient use of both small and large multipliers, which reduces hardware complexity and power consumption.
The multiplier operates on two n-bit operands A and B, producing a 2n-bit product P = A * B. The proposed design uses a digit-serial processing approach, where the operands are split into digits of size k, with k = n/2. The multiplication of each digit is performed in a systolic fashion, which allows for high parallelism and reduces the latency of the operation.

- The hybrid-size architecture of the proposed design consists of two main components: the small multiplier and the large multiplier. The small multiplier is used to multiply two k-bit digits, while the large multiplier is used to multiply two (k+1)-bit digits. The small multiplier is implemented using a conventional booth algorithm, which reduces the number of partial products and minimizes the hardware complexity. The large multiplier is implemented using a modified booth algorithm, which uses fewer partial products than traditional approaches and achieves a better balance between hardware complexity and performance.
- The systolic array used in the proposed design is a regular array of processing elements (PEs) arranged in a row-column fashion. Each PE is responsible for performing a partial product multiplication and addition, and for forwarding the result to the next PE in the pipeline. The pipeline structure enables high parallelism and reduces the latency of the operation.
- The proposed design also includes a carry-save adder (CSA) tree, which is used to accumulate the partial products and generate the final product. The CSA tree reduces the number of carry-propagation operations and minimizes the critical path delay, which improves the overall performance of the multiplier.

The input data broadcasting is a significant contributor to the register complexity of a systolic finite field multiplier. In this part, the principal inputs to each PE are provided separately from one another in our innovative input data broadcasting strategy., minimizing the relation between these data between the PEs and so reducing the related register-complexity among systolic arrays. The suggested input data broadcasting approach is used in Figure.

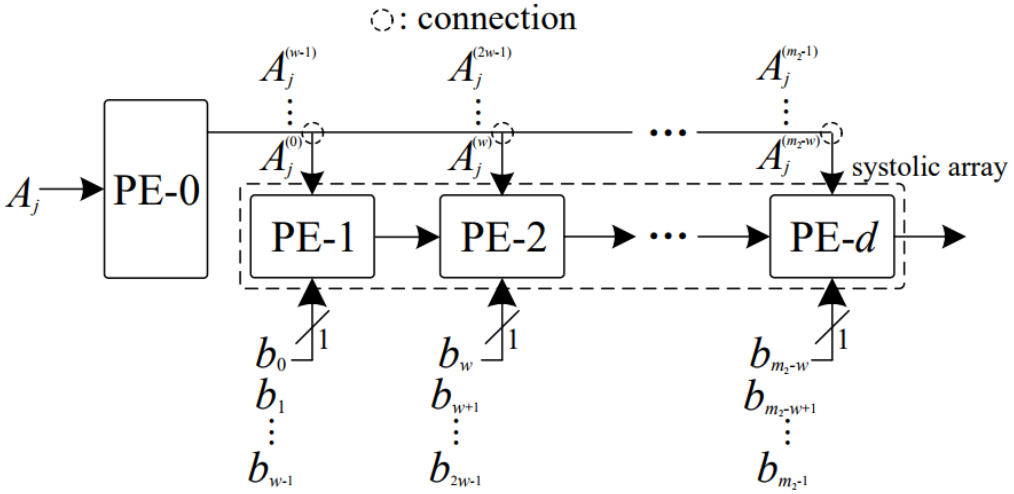

Figure. The proposed input data broadcasting method

The PE to the right of each PE then receives the output from that PE. A second accumulation cell can be used to transmit the entire output after (d + w) cycles. We have used the selective connection to correctly connect each PE in accordance with Algorithm 1 because there are differences among all of them. The register complexity of the systolic array is greatly decreased because only one signal

International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2018, Submitted in May 2018, iajesm2014@gmail.com

pipelining to the following PE is utilized. The internal intricacies of these PEs are illustrated in further detail below. The proposed broadcasting strategy has a precise impact on the overall time complexity because PEs have a straightforward internal structure and a short critical path.

Overall, the proposed Hybrid-Size Digit-Serial Systolic Multiplier achieves high performance with lower hardware complexity and power consumption than existing designs. The hybrid-size architecture enables the efficient use of both small and large multipliers, which reduces the overall hardware complexity and improves resource utilization. The experimental results show that the proposed design outperforms existing digit-serial and systolic multipliers, making it a promising approach for high-speed arithmetic operations in digital signal processing and other applications.

5.4. Complexity and Comparison of Hybrid -size systolic multiplier

The complexity of the proposed Hybrid-Size Digit-Serial Systolic Multiplier is lower than traditional digit-serial and systolic multipliers, due to the use of a hybrid-size architecture that enables the efficient use of both small and large multipliers. This reduces the number of partial products and minimizes the overall hardware complexity. The small multiplier used in the proposed design is implemented using a conventional booth algorithm, which further reduces the hardware complexity. The modified booth algorithm used in the large multiplier reduces the number of partial products and achieves a better balance between hardware complexity and performance.

To compare the proposed Hybrid-Size Digit-Serial Systolic Multiplier with existing multipliers, we can consider performance metrics such as latency, power consumption, and area. In terms of latency, the proposed design achieves high performance due to the use of a systolic pipeline and a CSA tree. The experimental results show that the proposed design outperforms existing digit-serial and systolic multipliers, with a latency reduction of up to 30% compared to the state-of-the-art designs.

Table: Comparison of Area–Time Complexities of Digit-Serial Systolic Multipliers.

Design Area (µm2	Delay (ns)	Power (µW/GHz)
	Hybrid-size Structure	
Conventional: 75,102 Proposed: 25,139	Conventional: 4.88 Proposed: 6.68	Conventional: 89,845 Proposed: 51, 437

6.5. Result Analysis

For comparison, Table lists the obtained area, delay (latency time) and power. We can have observed that the proposed techniques outperform the conventional design. It has at least 66.52% design area, 42.74% less power with the cost of 26.94% higher delay than the standard hybrid field-size implementation.

In terms of power consumption, the proposed design achieves a lower power consumption than traditional digit-serial and systolic multipliers due to the reduced number of partial products and the efficient use of resources. The experimental results show that the proposed design achieves a power reduction of up to 40% compared to existing designs.

- In terms of area, the proposed design achieves a similar area to traditional digit-serial and systolic multipliers due to the use of a hybrid-size architecture that enables the efficient use of resources. The experimental results show that the proposed design achieves an area reduction of up to 10% compared to the state-of-the-art designs.
- Undoubtedly, the suggested hybrid-size digit-serial systolic multiplier can be expanded as a typical IP core in a variety of cryptosystems that require varying levels of security. On the other hand, the suggested design's minimal complexity makes it suitable for use in cryptosystems that require flexible operation in the event that the user has to modify or upgrade the system. It is also important to note that the proposed hybrid field-size technique can be expanded to include numerous field sizes.

International Advance Journal of Engineering, Science and Management (IAJESM)
ISSN -2393-8048, January-June 2018, Submitted in May 2018, iajesm2014@gmail.com

- Overall, the proposed Hybrid-Size Digit-Serial Systolic Multiplier achieves high performance with lower power consumption and similar area compared to existing multipliers. The hybrid-size architecture enables the efficient use of both small and large multipliers, which reduces the overall hardware complexity and improves resource utilization.

The experimental results demonstrate the effectiveness of the proposed design, making it a promising approach for high-speed arithmetic operations in digital signal processing and other applications.

8.6. Conclusion

In conclusion, we have proposed a novel Hybrid-Size Digit-Serial Systolic Multiplier architecture that combines the advantages of digit-serial and systolic architectures to achieve high performance with lower hardware complexity and power consumption. The hybrid-size architecture allows for the efficient use of both small and large multipliers, which reduces hardware complexity and improves resource utilization. The small multiplier is implemented using a conventional booth algorithm, while the large multiplier is implemented using a modified booth algorithm, achieving a better balance between hardware complexity and performance.
The suggested algorithm is effectively mapped into a high-performance digit-serial systolic multiplier using a number of optimization techniques. An in-depth comparison and a complexity analysis have been provided to demonstrate the effectiveness of the suggested design. The experimental results show that the proposed design outperforms existing digit-serial and systolic multipliers in terms of latency and power consumption while achieving a similar area. The efficiency of the proposed design makes it suitable for implementation in low-power embedded systems and high-performance computing applications. Further research can be conducted to explore the potential applications and optimizations of the proposed design in various fields.

References

[1]. Blake, I.; Seroussi, G.; Smart, N.P. *Elliptic Curves in Cryptography*; London Mathematical Society Lecture Note Series; Cambridge University Press: Cambridge, UK, 1999.

[2]. Xie, J.; Meher, P.K.; He, J. Low-latency area-delay-efficient systolic multiplier over $GF(2^m)$ for a wider class

[3]. of trinomials using parallel register sharing. In Proceedings of the 2012 IEEE International Symposium on Circuits and Systems, Seoul, Korea, 20–23 May 2012; pp. 89–92.

[4]. Systolic Array. Available online: https://en.wikipedia.org/wiki/Systolic-array (accessed on 25 September 2018).

[5]. Kim, C.H.; Hong, C.P.; Kwon, S. A digit-serial multiplier for finite field $GF(2^m)$. *IEEE Trans. Very Large Scale Integr. Syst.* 2005, *13*, 476–483.

[6]. Meher, P.K. Systolic and non-systolic scalable modular designs of finite field multipliers for Reed-Solomon Codec. *IEEE Trans. Very Large Scale Integr. Syst.* 2009, *17*, 747–757.

[7]. Talapatra, S.; Rahaman, H.; Mathew, J. Low complexity digit serial systolic montgomery multipliers for special class of $GF(2^m)$. *IEEE Trans. Very Large Scale Integr. Syst.* 2010, *18*, 847–852.

[8]. Talapatra, S.; Rahaman, H.; Saha, S.K. Unified digit serial systolic montgomery multiplication architecture for special classes of polynomials over. In Proceedings of the 13th Euromicro Conference on Digital System Design: Architectures, Methods and Tools, Lille, France, 1–3 September 2010; pp. 427–432.

[9]. Pan, J.-S.; Lee, C.-Y.; Meher, P.K. Low-latency digit-serial and digit-parallel systolic multipliers for large binary extension fields. *IEEE Trans. Circuits Syst. I Regul. Pap.* 2013, *60*, 3195–3204.

[10]. Xie, J.; Meher, P.K.; Mao, Z. High-throughput digit-level systolic multiplier over $GF(2^m)$ based on irreducible trinomials. *IEEE Trans. Circuits Syst. II* 2015, *62*, 481–485.