International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 4 Volume No.6 July – 2022
DOI:10.46647/ijetms.2022.v06i04.0054 ISSN: 2581-4621

An Area Energy-Efficient VLSI Architecture using Hybrid Wide-Operand adder

Ms. E.pramila[1], Mrs.T.mangaiyarthilagam[2], Mrs.Nranjana CP[3]
[1]*UG - Applied Electronics, Selvam College of Technology, Namakkal , Tamilnadu*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, Selvam Collegeof Technology, Namakkal, Tamilnadu*
[3]*Assistant Professor, Department of Electronics and Communication Engineering, Selvam Collegeof Technology, Namakkal, Tamilnadu*

ABSTRACT

Consumer electronics markets have raised demand for high-speed, low- power adders with big operands for use in new portable systems. Traditional fast adder architectures, such as parallel-prefix adders, consume a lot of power when I have a lot of operands. One of the most promising ways for achieving a trade-off between delay and power consumption for the addition of big operands is the hybrid design. This reduces the area of the summation blocks at the significant positions without sacrificing speed. Furthermore, My provides a new hybrid adder architecture for large operands, based on the conceptthat in large parallel- prefix adders, the least significant carriers are produced considerably sooner than the most significant ones. As a result, the authors avoid incorporating fast architectures associated with the application of carries to the final summing least-significant bits, which has no effect on the critical path. of the carries is generated and propagated within the proposed adder's carry network to reduce delay. VLSI implementation results using 45-nm-TSMC technology reveal that the suggested adder saves more than 12% of energy and reduces the area-delay-product by more than 5% when compared to state-of-the-art other operand adders. The post- synthesis results of the proposed adder reported is much fasterthan the CS3A for 32-,64- and 128- bit architecture respectively. Moreover, it has a lesser area, lower power dissipation and smaller delay than the adder. Also, the proposed adder achieves the lowest ADP and PDP than the existing adder techniques.

Keywords: *high speed ,low power adders*

1. Introduction

To achieve optimal system performance while maintaining physical security,it is necessary to implement the cryptography algorithms on hardware modular arithmetic such as modular exponentiation, modular multiplication and modular addition is frequently used for the arithmetic operations in various cryptography algorithms therefore, the performance of the cryptography algorithm depends on theefficient implementation of the congruential modular arithmetic operation. The most efficient approach to implement the modular multiplication and exponentiation is the Montgomery algorithm whose critical operation is based on three-operand binary addition. The three-operand binary addition is also a primary arithmetic operation inthe linear congruentialgenerator (LCG) based pseudo-random bit generators (PRBG) such as coupled LCG (CLCG), modified dual- CLCG (MDCLCG) and coupled variable input LCG (CVLCG) Modified dual-CLCG (MDCLCG) is the most secure and highly random PRBG method among all the LCG-based and other existing PRBG methods. It is polynomial-time unpredictable and secure if n _32-bits. Therefore, the security of the MDCLCG enhances with the increase of operandsize. However, the area and critical path delay increases linearly since its hardware architecture consists of four three-operand modulo-2n adders, two comparators, fourmultiplexers area. Hence, theperformance of the MDCLCG can be improved by theefficient implementation of the three-operand adder. The three-operand binar addition can be carried out either by using two two-operand adders or one three- operand adder.

The three-operand binary addition can be carried out either by using two two- operand adders or one three- operand adder. Carry-save adder (CS3A) is the area- efficient and widely adopted technique to perform the three- operand binary additionin the modular arithmetic used in cryptography algorithms and PRBG methods. However, the longer carry propagation delay in the ripple-carry stage of CS3A seriously influences the performance of the MDCLCG and other cryptography architectures on IoT based hardware devices. In order to shorten the critical path delay, a parallel prefixed two-operand adder such as Han-Carlson (HCA) can also be used for three-operand binary addition. It reducesthe critical path delay in the order of O(log2 n) but increases the area in the order ofO(n log2 n) [15]. There fore, it is necessary to develop an efficient VLSI architectureto carry out the fast three- operand binary addition with minimum hardware resources. Hence, a new high- speed area-efficient adder technique is proposed using pre-compute bitwise addition followed by carry-prefix computation logic to performthe three- operand addition in this paper that consumes considerably less gate area while minimizing the propagation delay in comparison to the HCA-based three- operand adder (HC3A). Furthermore, the proposed adder architecture is implemented with the Verilog HDL ,and then synthesized with commercial available 32nm CMOS technology library.Also, the area-delay and power-delay products of the proposed adder technique are measured and compared withrespect to the existing CS3A and HC3A three-

operand adder techniques.

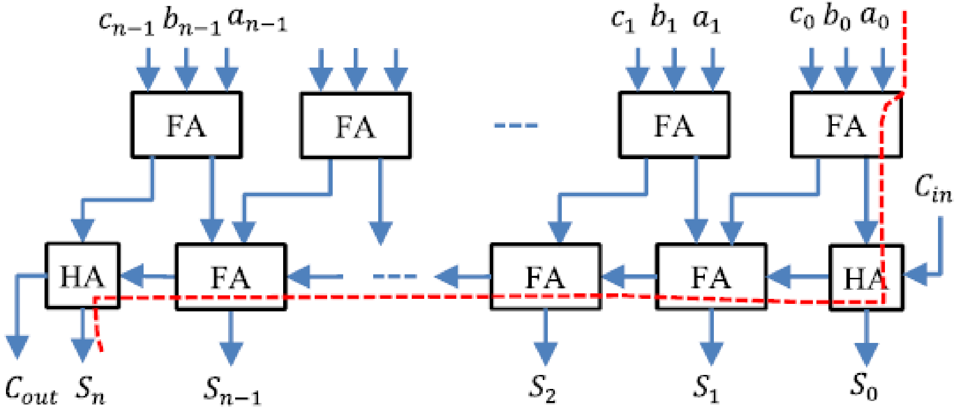


Fig. 1.1 Three-operand carry-save adder (CS3A).

The synthesis result of the proposed adder architecture along with other exiting adder techniques is also reported in this section. Further, the proposed adder is incorporated in the modified dual-CLCG application to measure the performance metrics mentioned in Section IV, and validate the results with post-synthesis simulated results. Also,the proposed design is prototyped on Artix7 FPGA chip to validate the design with real-time captured signals on Chip scope using an integrated logic analyzer.

2. Proposed Methods or Methodology:

In my proposed research we have I replace the below bit addition logic and base logic block instead of existing work. The post-synthesis results of the proposedadder reported is much faster than the CS3A for 32-,64- and 128- bit architecture respectively. Moreover, it has a lesser area, lower power dissipation and smaller delay than the CS3A adder. Also, the proposed adder achieves the lowest ADP and PDP than the existing adder techniques.

The first stage of a PPF adder, named the preparation unit, produces generate(g), alive (a), and propagate
(p) signals. Let X = xn − 1xn − 2…x0 and Y = yn − 1yn − 2…y0 be the two operands. The g, a, and p signals foreach bit position can be calculated as follows :

$$gi = xi \,.\, yi$$
$$ai = xi + yi$$
$$pi = xi \oplus yi$$

In the above formulas, i is the bit position, and ‘ . ’, ‘ + ’, and ‘⊕’ denote bitwise AND, OR, and exclusive-OR operations, respectively. The second stage accommodates the main network, a tree structure, of parallel prefix adders. The associative operator o is applied to associate pairs of consecutive generate and propagate bits as follows: gi + 1, ai + 1 o gi , ai = gi + 1 + Sgi · ai + 1, ai + 1 · ai . Thenotation (Gi: j, Ai: j) is used when the o operatoris applied to a series of consecutivepairs of generate and propagate bits from the j-bit to ith bit positions (j < i) Gi:j , Ai: j) = gi,ai o gi -1,ai-1o..ogi,ai Through the iterative application of (4) and s(5) in the second stage of the PPF adder, the carry-out signal of any i bit-position (Ci + 1) can be obtained as (Ci + 1 = Gi: 0). In the last stageof the PPF adder (the sum production part), the value of the sum is produced from the input carries at eachbit position (the outputs of the PPF tree structure) and the corresponding p signals. Based on the node numbers, the depth of the PPF, and the fan-out of each node, distinct topologies with different characteristics have been introduced for designingparallel Prefix adders.

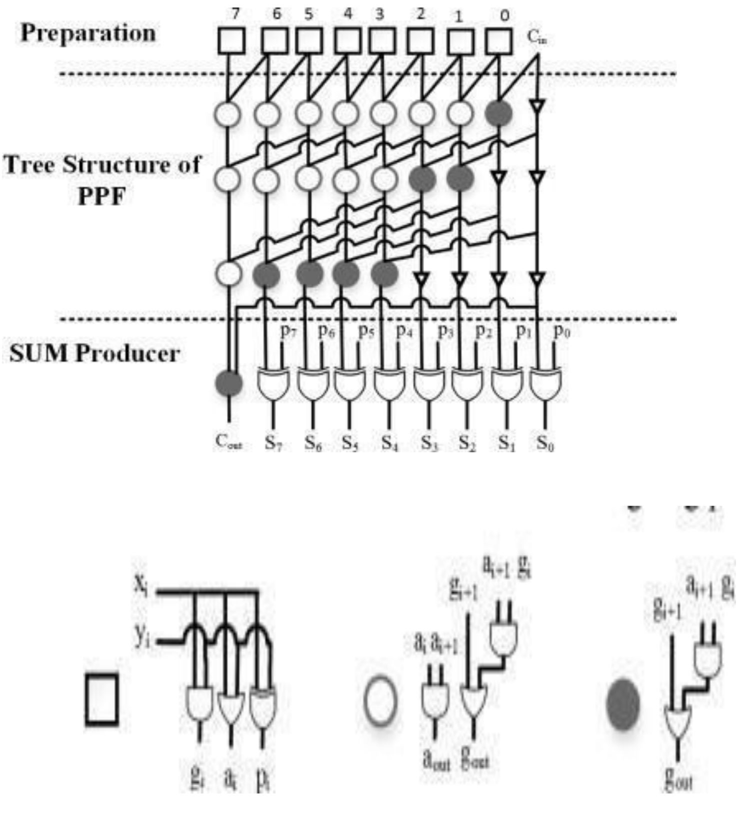


Fig.2.1 8-bit wide band Three operand adder structure

As an example, the Brent-Kung structure occupies the least area, while Sklansky is the fastest one. In order to increase the speed of PPFs, the depth of the treestructure should be reduced, which requires increasing the number of nodes and interconnections or the nodes' fan-outs. As a result, faster adder structures, like Kogge- Stone, consume more power and area in comparison with other similar structures. Fig. 1 shows the structure of an 8-bit wide band Three operand adder. PPFs are not efficient for large operands due to their high power- consumption. Therefore, hybrid PPF-based structures are usually used for wide adders. One of these efficient adders is presented in [28], which is composed of a parallel- prefix/carry select architecture and a skip adder (PPF/CSSA). This wide adder can improve the speed by balancing the delays of the PPF network and CSL/CSSAblocks.The structure of [28] for a 64-bit adder is shown in Fig. 2.1 It consists of three maintypes of blocks: preprocessing, PPF, and sum production blocks. In the sum production blocks, illustrated in Fig. 3, two 4-bit RCAs are used for each possible value of the input carry (0 or 1). The carry-in of the second RCA is produced directly from PPF signals, improving the speed of this 64-bit adder in comparison with adders of similar bit width.

3. Results and Discussion

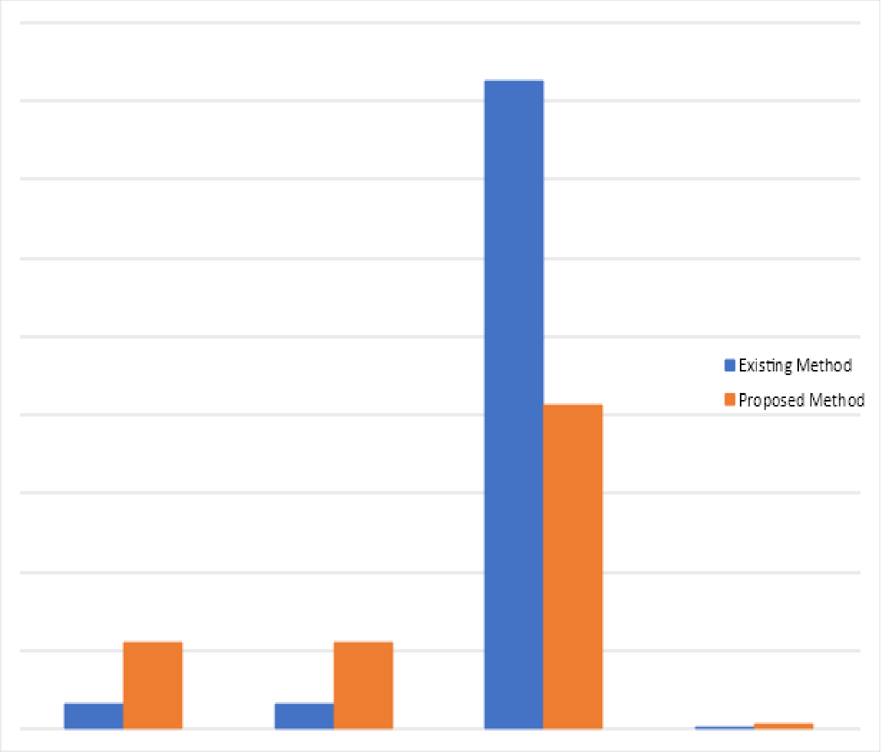
The existing adder circuit is the three- operand adder. The three-operand adder circuit consist of five mainblocks, which are bit addition logic, base logic, PG logic(Black cell and grey cell) and sum logic. In this existingadder consumes high powercompared the proposed hybrid adder circuit.

The three-operand binary addition is one of the critical arithmetic operation inthe congruential modular arithmetic architectures and LCG-based PRBG methods such as CLCG, MDCLCG and CVLCG. It can be implemented either by using twostages of two-operand adders or one stage of three-operand adder. Carry-save adder(CSA) is the commonly used technique to perform the three-operand binary addition. It computes the addition of three operands in two stages. The first stage is the arrayof full adders. Each full adder computes “carry” bit and“sum” bit concurrently fromthree binary input ai , bi and ci. The second stage is the ripple-carry adder that computes the final *n*-bit size “sum” and one-bit size “carry-out” signals at the outputof three-operand addition. The “carry-out” signal is propagated through the*n* numberof full adders in the ripple-carry stage. Therefore, the delay increases linearly with the increase of bit length.This section presents a new adder technique and its VLSI architecture to perform the three-operand addition in modular arithmetic. The existing adder technique is a parallel prefix adder. However, it has four-stage structures instead three-stage structures in prefix adder to compute the addition of three binary input operands such as bit-addition logic, base logic, PG (propagate and generate) logic and sum logic.

Output Results Performance

Performance Analysis			
S.NO	Parameters	Existing method	Proposed method
1	Luts	16	55
2	Flip Flops	16	55

3	Power in Mw	413.23	206.49
4	Combination Delay in ns	1.322	2.993



Conclusion

For big operands, a new efficient adder structure based on the PPF and improved sum producer blocks is introduced. In My paper, two forms of these latterblocks were introduced to Improve performance and reduce area cost. The first typeof sum-producer block has a simpler construction and lower hardware cost because the complement of the carry-in is ready sooner. The second type of sum producer has a CSL architecture with an efficient design. To boost performance, the complements of the carry bits are produced and transmitted in the proposed structure. Experimentresults show that the suggested 16-bit adder may improve energy and ADP by roughly 12% and 5% percent, respectively, when compared to the corresponding state of the art. This architectureprovides a new hybrid adderarchitecture for large operands, based on the concept that in large parallel-prefix adders, the least significant carriers are produced considerably sooner than the mostsignificant ones. As a result, the authors avoid incorporating fast architectures associated with the application of carries to the final summing least-significant bits, which has no effecton the critical path.

Reference

1.H. Ling, "High-speed binary adder," IBM J. Res. Develop., vol. 25, no. 3,pp.156–166, Mar. 1981.
2.P. L. Montgomery, "Modular multiplication without trial division," Math.Comput., vol. 44, no. 170, pp. 519–521, Apr. 1985.
3. N. Weste and K. Eshraghian, Principles of CMOS VLSI Design—A SystemsPerspective. Reading, MA, USA: Addison-Wesley, 1985.
4. T. Han and D. A. Carlson, "Fast area-efficient VLSI adders," in Proc.IEEE 8thSymp. Comput. Arithmetic (ARITH), May 1987, pp. 49–56.
5 .T. Kim, W. Jao, and S. Tjiang, "Circuit optimization using carry-saveadder cells," IEEE Trans. Comput.- Aided Design Integr. Circuits Syst.,vol. 17, no. 10, pp.974–984, Oct. 1998.
6.B. Parhami, Computer Arithmetic: Algorithms and Hardware Design. NewYork,NY, USA: OxfordUniv. Press, 2000.
7.D. L. Harris, "Parallel prefix networks that make tradeoffs between logic levels,fanout and wiring racks," U.S. Patent 0 225 706 A1,Nov. 11, 2004.
8.R. Jackson and S. Talwar, "High speed binary addition," in Proc. Conf. Rec. 38th Asilomar Conf. Signals, Syst. Comput., vol. 2. Pacific Grove, CA, USA, Nov.2004, pp. 1350–1353.
9. R. S. Katti and S. K. Srinivasan, "Efficient hardware implementation of a new pseudo-random bit sequence generator," in Proc. IEEE Int. Symp. Circuits Syst., Taipei, Taiwan, May 2009, pp. 1393–1396.
10. S. Muthyala Sudhakar, K. P. Chidambaram, and E. E. Swartzlander, "Hybrid Han-Carlson adder," in Proc. IEEE 55th Int. Midwest Symp. Circuits Syst. (MWSCAS), Boise, ID, USA, Aug. 2012, pp. 818–821.
11. A. Rezai and P. Keshavarzi, "High-throughput modular multiplication and exponentiation algorithms using multibit-scan–multibit-shift technique,"IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 23, no. 9,pp. 1710–1719, Sep. 2015.
12.S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, "Low-cost high-performance VLSI architecture for montgomery modular multiplication," IEEE Tran .Very Large ScaleInteger. (VLSI) Syst., vol. 24, no. 2, pp. 434–443,Feb. 2016.
13. Z. Liu, D. Liu, and X. Zou, "An efficient and flexible hardware implementationof the dual-field elliptic curve cryptographic processor," IEEE Trans. Ind. Electron.,vol. 64, no. 3, pp. 2353–2362, Mar. 2017.
14.S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery modular multiplication," IEEE Trans. Very Large ScaleIntegr. (VLSI)Syst., vol. 25, no. 5, pp. 1658–1668, May 2017.
15. Z. Liu, J. GroBschadl, Z. Hu, K. Jarvinen, H.Wang, and I. Verbauwhede, "Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the Internet of Things," IEEE Trans. Comput., vol. 66, no. 5, pp. 773–785, May 2017.
16. A. K. Panda and K. C. Ray, "Design and FPGA prototype of 1024-bit Blum- Blum-Shub PRBG architecture," in Proc. IEEE Int. Conf. Inf.Commun. Signal Process. (ICICSP), Singapore, Sep. 2018, pp. 38– S43.
17. K. S. Pandey, D. K. B. N. Goel, and H. Shrimali, "An ultra-fast parallel prefix adder," in Proc. IEEE 26th Symp. Computs. Arithmetic (ARITH),Kyoto, Japan, Jun. 2019, pp. 125–134.
18. A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 66, no. 3, pp. 989–1002, Mar. 2019.
20. K. S. Pandey, D. K. B. N. Goel, and H. Shrimali, "An ultra-fast parallel prefixadder," in Proc. IEEE 26th Symp. Computs. Arithmetic (ARITH),Kyoto, Japan, Jun. 2019, pp. 125–134.