Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

THREE OPERAND BINARY ADDER OF LOW POWER AND HIGH SPEED VLSI ARCHITECTURE

ASHA CN,
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

JAYALAXMI H,
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

SAPNA KUMARI C,
Dept. of Electronics and Communication Engineering, Nitte Meenakshi Institute of Technology, Bangalore

NAGAPUSHPHA KP
Dept. of Electronics and Communication Engineering, Acharya Institute of Technology, Bangalore

Abstract

Addition is one of the most vital and initial operations among all arithmetic operations and is utilized in many of the mathematical equations. In digital world, the addition operation can be performed by several adders. These adders produce carries with preferred power and delay. One of the most basic functional units for performing modular arithmetic in different cryptography and PRBG (pseudorandom bit generator) algorithms is Three-operand binary adder. Because of ripple-carry stage, the Carry save three-operand Adder (CS3A) has long propagation delay. In addition, a parallel prefix two-operand adder (PP2A) like HCA (Han-Carlson) is used in the addition of three-operands. Hence new higher speed and less power adder architecture is presented in this paper using the pre-computing bitwise addition follow by carry-prefix computation logic for performing binary addition of three operands that can consume less power and low area and adder delay is drastically reduced to O(log2 n). The ISE Xilinx 14.7 software is used for simulation and synthesizing these processes. The simulation results of presented adder will represent that it will have less power dissipation, lesser area and less delay compared to CS3A adder. More over the presented adder will achieve least PDP (power-delay-product) and ADP(area-delay-product) than previous three-operand adder methods.

Keywords: Carry Save Adder (CSA), Three-operand binary adder, VLSI architecture, Han-Carlson adder (HCA), low power, and high speed.

I. INTRODUCTION

In arithmetic operations, one of the most essential components is Adders. In digital circuits, binary adders are utilized in subtraction, addition and Floating point consequently, the adders become as fundamental elements, however optimization of their tasks is the most tough task in digital architectures. The computer arithmetic algorithms have been developed n-bit adders delay and lower limits on area; generally the former can differ linearly with the size of adder and the latter has an O (log2 (n)) behaviour. The implementation of cryptography algorithms on the hardware is essential for achieving optimal performance of system by maintaining the system physical security. Often the modular arithmetic like modular multiplication, addition and exponentiation is utilized for arithmetic operations in different cryptography methods [2]. Therefore, the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

cryptography algorithm performance is relying on congruential modular arithmetic operation effective implementation. Montgomery algorithm is the most effective technique for the implementation of modular exponentiation and multiplication and its critical operations depends on the binary addition of three operands. The binary addition of three-operands is a fundamental arithmetic operation in LCG (Linear Congruential Generator) based PRBG like CLCG (Coupled CLCG) [3, 4], CVLCG (Variable input LCG) and MDLCG (Modified Dual LCG). Among all the LGGs based and earlier PRBG techniques, the MDCLG is highly random and most secured PRBG technique.

The RCA (Ripple Carry Adder) can require linear number of gates [5], where as quick adders like Prefix Adders, CLA (Carry Look-Ahead Adders), etc. has logarithmic delays. These boundaries are indicating that often no effective adder is designed with sub-logarithmic delay; besides unreliable adders are implementing with sub-logarithmic delays. The unreliable adders can be utilized in cryptographic attacks; the reliable adders can be building with unreliable adders while adding error-detecting and correcting techniques [6].

The binary addition of three-operand is performed using one 3-operand adder or 2 two-operand adder. The CS3A is the widely adopted and area efficient method for performing the binary addition of three-operand in modular arithmetic utilized in PRBG techniques and cryptographic algorithms [7]. For shortening the delay of critical path, a PP2A like HCA is utilized for performing the addition of three-operand [8]. Hence the development of an effective VLSI architecture is essential for performing the binary addition of three-operand with minimal hardware resources. Thus a new area-effective and high speed adder is presented with pre-computing bit wise addition follow by carry-prefix computation logic for performing addition of three-operand that can significantly consume less gate area by reducing the propagation delay compared to CS3A.

Increasing market demands of battery-powered portable consumer electronics is one of the factors that drive the demand of low power chips. The requirement of lighter, durable and smaller electronic products indirectly results low consumption of power. In most of the portable systems, the life of battery will be emerging as a product differentiator. As a largest and heaviset element in several portable systems, the batteries won't have same growth in rapid density than electronic circuits. The power dissipation major source is gaining importance in these higher performance battery-powered digital systems like cell phones, laptops, individual digital assistants, etc. In these systems one of the major concerns is low consumption of power, since it can directly affect the performance through affecting the life span of battery. As a active and rapidly growing filed, the low power VLSI design become crucial in these scenarios. Though, reducing the frequency of clock is only feasible at the architecture level and basically frequency is considered as constant at circuit level for satisfying the requirements of speed. Certain basic logic requirements to implement the design of low power circuits are stated as follows:

• Reduction of Switched Capacitance

• Reduction of Switching Activity

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

• Reduction of Short-Circuit Current

• Reduction of Supply Voltage

The paper is organized as: literature survey is described in Section II, the presented three-operand adder architecture is highlighted in Section III. The presented adder synthesis results with earlier adder methods and validated results are demonstrated in section IV. The conclusion of presented adder is described in section V.

II. LITERATURE SURVEY

K. Panda et. al. [9] presents a modified Montgomery modular radix-2 iterative multiplier for the effective implementation of 1024-bit BBS (Blum Blum Shub) generator hardware. The BBS effective implementation technique depends on the larger integer multiplication that can make it as computationally expensive. The two-operand adders are replaced with three-operand adders by this approach. For three-operand addition, most generally utilized adder is CSA that can experience the higher critical path delays. The results of this 1024-bit BBS implementation is operates at high frequency (71.2 MHz) and achieved improvement in latency.

Z. Liu et. al. [10] presented a flexible and efficient dual-filed ECC processing with hardware-software method. This presented processor supports arbitrary elliptic curve. An MALU (Modular Arithmetic Logic Unit) is designed that performs general modular arithmetic operation and high efficiency is attained. This design is implemented with 55nm CMOS process in FPGA (Field Programmable Gate Array) platforms as well as ASIC (application-specified integrated circuit). After the implementation the processor can take 0.60ms (163bits ECC) to 6.75 ms (571bits ECC) for completing single point multiplication. The advantages of this ECC processor are high flexibility and hardware efficiency compared to other processors.

S. S. Erdem, et. al. [11] demonstrated Montgomery algorithm as a quick modular multiplication algorithm which is often utilized in the applications of cryptography. The author has been investigated the Montgomery algorithm digital-serial implementation for larger integers. The detailed analysis and upper bound are provided to the intermediate results which are obtained in digital serial computing process. An effective digital-serial Montgomery Modular Multiplier (MM) framework is presented based on this analysis with CSA and its complexity is presented. In this approach, CSAs can be utilized for performing two final tasks: First task is is addition of carry save vectors represents the modular products and second task is subtraction of modulus from the addition.

Tsiaras et al. [12] presents the procedure of applying multiple numbers to the LNS (Logarithmic Number System). This approach depends on data setting to highest value of input. This presented multi-operand adders is integrated and texted in cases of 4, 8, 16 & 11-bit lengths for efficiency and complexity using the process of a 65-nm library 0.9V UMC CMOS. Voicu et al. [13] presented two less expensive Stacked Hybrid adders with similar characteristics and make an easy way for quick-acting hardware production.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

Based on the principle of anticipated computation, the extension of N-bit is applied to the equivalent line K which can make addition of two N /K-bit in every phase. Narule et al. [14] presented addition of floating point with less delay. The internal width can be made in compliance with IEEE Std754 that is especially sensitive to delays. The compound adder and LZA (leading Zero Anticipator) are utilized for refining full type composition. The presented version reduced the delay in contrary to the targeted three operand adder.

S.-R. Kuang, et. al. [15] presents a multiplication method using Montgomery Modular to perform modular multiplication very quickly. The Montgomery Modular multiplication (MM) can be utilized in the process of encryption using PKC (Public Key Cryptography). The MM with larger integers consumes huge time in PKC. Hence several algorithms are presented for performing MM very fast and Montgomery's algorithm is one among them. This approach replaced the complicated divisions in MM with sequence of modular shifting additions. The Montgomery algorithm is divided in to two types depends on input and output operands representation. The two types are SCS-MM (Semi- Carry-Save Montgomery modular Multiplication) and FCS-MM (Full Carry-Save MM). This technique uses carry save adder for multiplication process. This carry save addition increases critical path delay.

III. HIGH SPEED AND LOW POWER THREE-OPERAND ADDER ARCHITECTURE

The addition of three-operand in modular arithmetic is performed using a new adder mechanism and its VLSI design, which is shown in this section. A parallel prefix adder (PPA) is the adder mechanism which is proposed. The prefix adder, on the other hand, uses four-stage structures rather than three-stage structures for computing the binary addition of 3 input operands. The 4 stages are

1).Bit-addition logic

2).Base logic

3).PG (propagate and generate) logic, and

4).Sum logic.

Stage 1 (Bit-addition logic): during first step, an array of full adders performs bitwise addition of 3 n-bit binary input operands, with each full adder computing "sum (S I and "carry (cyi)" signals as shown in Fig. Each F block in first stage takes three input bits a, b, c and performs bit addition logic and gives the two outputs sum(s) and carry(c). The logic expression and the logic circuit used in the calculation of sum and logic is shown below:

$$S_i^{|} = a_i \oplus b_i \oplus c_i$$

$$Cy_i = a_i . b_i + b_i . c_i + c_i . a_i$$

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

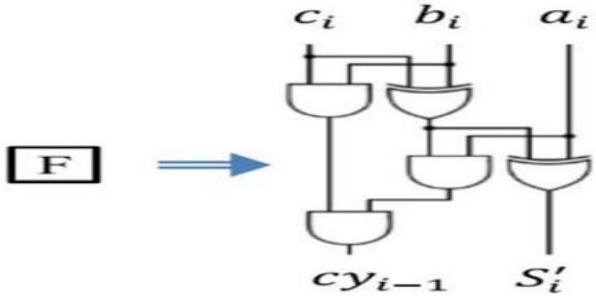

Fig. 1: BIT ADDITION LOGIC

Stage 2: Base logic

In second stage we have base logic , which takes two input signals sum and carry and computes the output signals Propagate(P_{in}) and Generate(G_{in}).

Each cell in second stage takes output Sum (S) bit of present full adder and carry output of previous full adder and computes the propagate and generate signals. The proposed the method uses n+1cells. In the suggested adder mechanism, the external carry-input signal (C_{in}) is considered for the addition of three-operands. While computing the G0 (S_0 C_{in}) in the base logic first saltire-cell , this extra carry-input signal (C_{in}) is used as an input to the base logic. Thelogic expression and logic circuit diagram used in the computation of P and G is shown below:

$$G_{i:i} = G_i = S_i . Cy_{i-1,}$$

$$G_{0:0} = G_0 = S_0^{|} . C_{in}$$

$$P_{i:i} = P_i = S_i^{|} \oplus C_{in}$$

$$P_{0:0} = P_0 = S_0^{|} . C_{in}$$

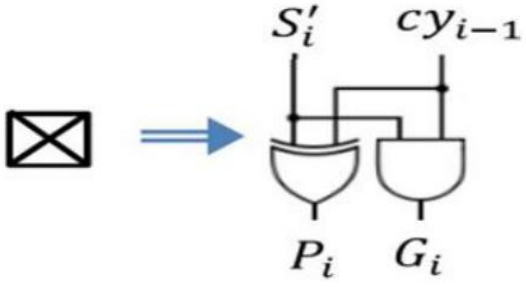

Fig. 2: BASE LOGIC

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

Stage 3: PG Logic

The carry computation step, also known as "generate and propagate logic" (PG), is a mixture of grey and black cell logics that pre-computes the carry bit. The Logical diagrams of grey and black cells which can compute the carry creates $G_{i:j}$ and propagate $P_{i:j}$ signals using the logical expression, and the logic circuit diagram is shown below,

$$G_{i:j} = G_{i:k} + P_{i:k}.G_{k-1:j}$$

$$P_{i:j} = P_{i:k}.P_{k-1:j}$$

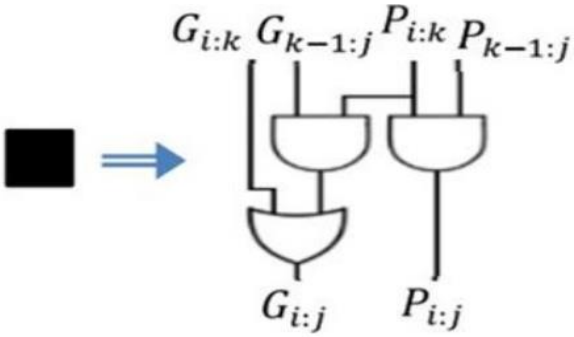

Fig. 3: PG LOGIC

Stage 4: Sum Logic

Fourth stage is the final stage in the proposed three operand adder. It takes carry generate and carry propagate signals from the previous stage and computes the Sum (S_i) using the logic expression and logic circuit shown below

$$S_i = (P_i \oplus G_{i-1:0})$$
$$S_0 = P_0$$
$$C_{out} = G_{n:0}$$

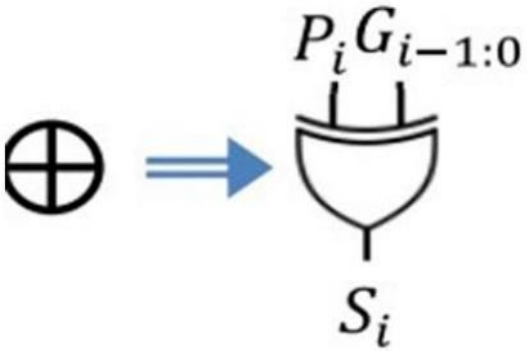

Fig. 4: SUM LOGIC

The Fig. 5 represents the presented three-operand binary adder VLSI architecture and its internal structure. This new adder model will perform 3 n-bit binary inputs addition in 4

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

different stages. During 1st stage, the 3 n-bits input binary operands bitwise addition is carried out with a array of full adders.

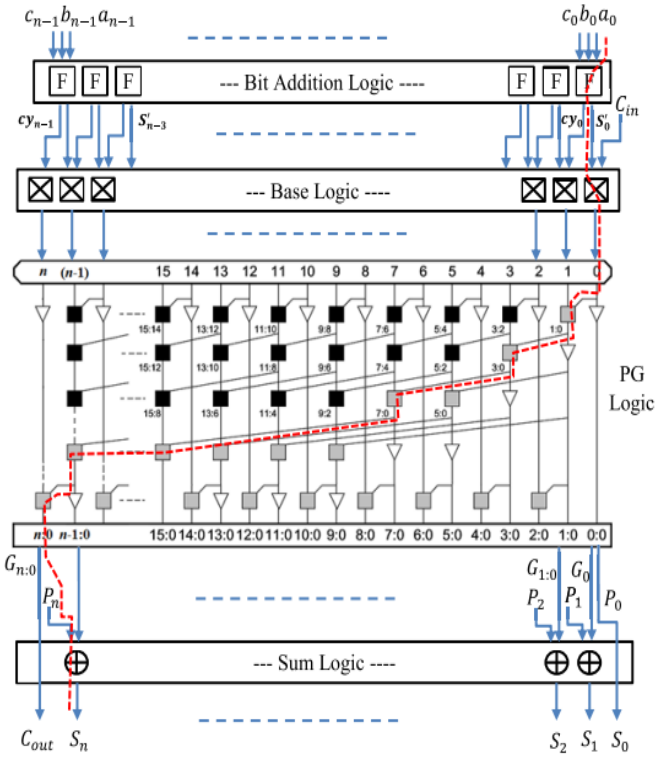

Fig. 5: PROPOSED THREE-OPERAND ADDER

IV. SYNTHESIS AND SIMULATION RESULTS

For fair comparison, the same style of coding using Xilinx 14.7 ISE tool and Verilog HDL coding will be adopted to design HC3A and CS3A and presented binary addition of 3-operand adders. More over all of these designs will be synthesized by Synopsys Design Compiler in the same SAED 32 nm CMOS technology for obtaining area of core, power and timing for distinctive size of word. The properties of physical synthesis analysis are compromised with maximum combinational gate delay, consumption of area, area of core, ADP, PDP are represented in Table 1. The results in table 1will alter with the adopted coding style of HDL and the available options of optimization in synopsis tool.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

Table 1: PHYSICAL SYNTHESIS RESULTS AND COMPARISONS OF THREE-OPERAND ADDER TECHNIQUES

Metrics	CS3A	HC3A	High Speed and Low Power 3 operand adder (HS and LP 3 operand Adder)
Area (μm^2)	829.16	178.9	139.01
Delay (ns)	2.12	1.05	0.80
Power (μW)	94.89	67.46	70.85
Area X Delay (μm^2 X ns)	1757.82	1545.79	788.79
Power X Delay (μW X ns)	107.38	99.63	48.18

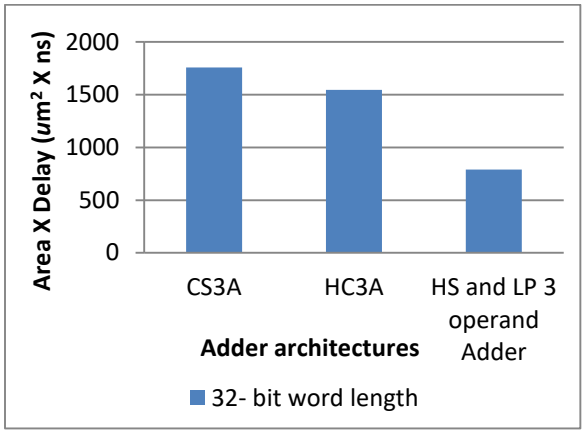

Fig. 6: AREA-DELAY PRODUCT (ADP) OF 32 BIT LENGTH

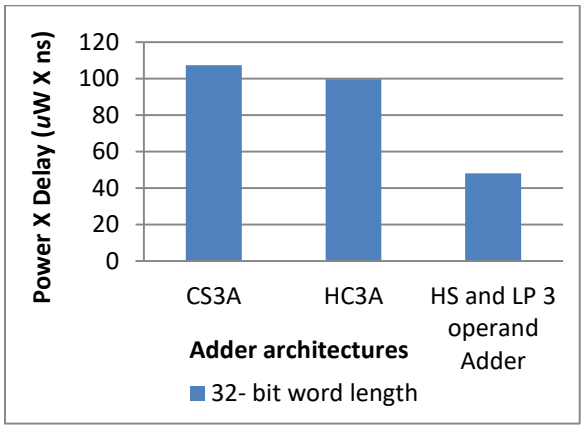

Fig. 7: POWER-DELAY PRODUCT (PDP) OF 32 BIT LENGTH

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

32 bit length input sequence is taken for the implementation of the described High Speed and Low Power three operand adder and it is clear that described method acquires less power, less area and less delay which automatically increases the speed. ADP and PDP plots are represented for 32 bit input sequence in Fig. 6 and Fig. 7 respectively. RTL View of 32-Bit HC binary adder is shown in below Fig. 8.

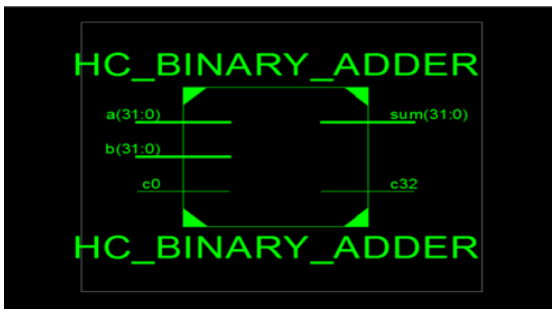

Fig. 8: RTL View of 32-Bit HC binary adder

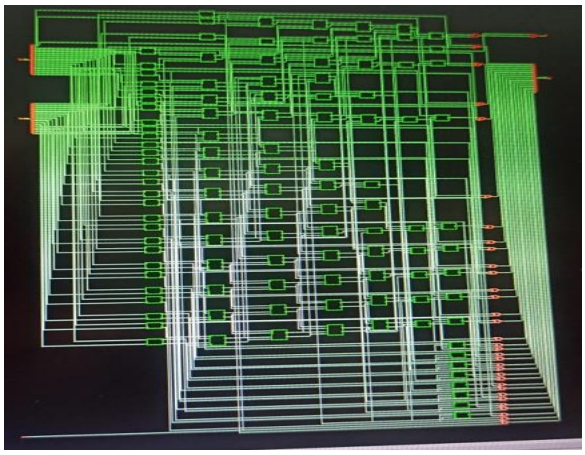

Fig. 9: SYNTHESIS LAYOUT

Fig. 10: PHYSICAL IMPLEMENTAION

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

Synthesis layout and physical implementation are shown in above Fig. 9 and Fig. 10 respectively.

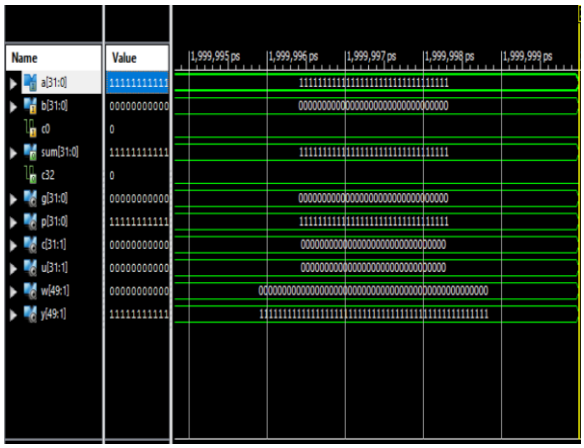

Fig. 11: SIMULATION RESULT OF 'HS & LP 3 OPERAND ADDER'

Above Fig. 11 shows the simulation result of High Speed and Low Power three operand adder (HS and LP 3 operand adder).

V. CONCLUSION

In this paper, Three Operand Binary Adder of High Speed and Low Power VLSI Architecture is implemented. The presented addition of three-operand adder method is a PPA which can use four-stage structures for computing the binary addition of 3-operands. For fair comparison, the same style of coding using Xilinx 14.7 ISE tool and Verilog HDL coding is adopted to design HC3A and CS3A and presented binary addition of 3-operand adders. The novelty of this presented method is the reduction of area and delay in prefix computation phases in bit-addition logic and PG logic which can lead to reduction in ADP and PDP. From the results of physical synthesis, it can be clear that the performance of presented adder architecture is increased up to 3 to 9 times quicker than the related architecture of CS3A. This can be concluded that this adder is significantly better in terms of delay and power compared to other adders.

REFERENCES

[1] Jinping Fan, Yujie Gu, Masahiro Hachimori and Ying Miao, "Signature Codes for Weighted Binary Adder Channel and Multimedia Fingerprinting" IEEE Transactions on Information Theory Year: 2021

[2] Titouan Coladon, Philippe Elbaz-Vincent, Cyril Hugounenq, "MPHELL: A fast and robust library with unified and versatile arithmetics for elliptic curves cryptography", 2021 IEEE 28th Symposium on Computer Arithmetic (ARITH), Year: 2021

[3] Amit Kumar Panda, Kailash Chandra Ray, "A Coupled Variable Input LCG Method and its VLSI Architecture for Pseudorandom Bit Generation", IEEE Transactions on Instrumentation and Measurement, Volume: 69, Issue: 4, Year: 2020

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online): 0493-2137
E-Publication: Online Open Access
Vol:55 Issue:04:2022
DOI 10.17605/OSF.IO/CFA43

[4] 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.

[5] ASHISH BAGWARI, ISHA KATNA, “Low Power Ripple Carry Adder Using Hybrid 1-Bit Full Adder Circuit”, 2019 11th International Conference on Computational Intelligence and Communication Networks (CICN), Year: 2019

[6] F. Jafarzadehpour, A. S. Molahosseini, A. A. Emrani Zarandi, and L. Sousa, “New energyefficient hybrid wide-operand adder architecture,” IET Circuits, Devices Syst., vol. 13, no. 8, pp. 1221–1231, Nov. 2019.

[7] A Krishna Vamsi, N Udaya Kumar, K Bala Sindhuri, G Sai Chandra Teja, “A Systematic Delay and Power Dominant Carry Save Adder Design”, 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Year: 2018

[8] Nagesh N. Nazare, R. J. Nayana, Pradeep S. Bhat, B.S. Premananda, "Design and Analysis of Low-Power 16-bit Parallel-Prefix Adiabatic Adders”, 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Year: 2018

[9] 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. 38–43.

[10] Z. Liu, D. Liu, and X. Zou, “An efficient and flexible hardware implementation of the dual-field elliptic curve cryptographic processor,” IEEE Trans. Ind. Electron., vol. 64, no. 3, pp. 2353–2362, Mar. 2017.

[11] S. S. Erdem, T. Yanik, and A. Celebi, “A general digit-serial architecture for montgomery modular multiplication,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 5, pp. 1658–1668, May 2017

[12] Tsiaras, G., &Paliouras, V. “Multioperand logarithmic addition/subtraction based on Fractional Normalization”, 2017 6th International Conference on Modern Circuits and Systems Technologies (MOCAST), 2017

[13] Voicu, G. R., &Cotofana, S. D. “High Performance, Cost-Effective 3D Stacked WideOperand Adders”, IEEE Transactions on Emerging Topics in Computing, 5(2), 179–192, 2017

[14] Narule, O., & Palsodkar, P. “Implementation of three operand floating point adder”, 2016 International Conference on Communication and Signal Processing (ICCSP), 2016

[15] S.-R. Kuang, K.-Y. Wu, and R.-Y. Lu, “Low-cost high-performance VLSI architecture for montgomery modular multiplication,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 24,no. 2, pp. 434–443, Feb. 2016.