International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

High-Speed Area-Efficient VLSI Architecture Of Three-Operand Binary Adder

Mr. K. MAHESH BABU[1], KANDUKURI LAVANYA[2], LANKA BHAVANA[3], KANUGONDA NIKHITHA REDDY[4], KUPPAM VANAJA[5], KOLASALAGUNTA NITHEESH KUMAR[6]

[1]Assistant Professor, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.

[2,3,4,5,6]UG Students, Dept. of ECE, S V College of Engineering, Tirupati, A.P, India.

ABSTRACT

Three-operand binary adder is the basic functional unit to perform the modular arithmetic in various cryptography and pseudorandom bit generator (PRBG) algorithms and also used in many applications. Carry save adder (CS3A) is the widely used technique to perform the three-operand addition. In carry save adder at final stage uses ripple carry adder which will cause large critical path delay. Moreover, a parallel prefix two-operand adder such as Han-Carlson (HCA) can also be used for three-operand addition that significantly reduces the critical path delay with more area complexity. Hence, a new high-speed and area-efficient adder architecture is proposed using pre-compute bitwise addition followed by carry prefix computation logic to perform the three-operand binary addition that consumes substantially less area and less delay. When compare to existing design like three operand carry save adder and two operands based three operand Han-Carlson adder the proposed design consumes less area and less delay. The synthesis and simulation are verified by using Xilinx ISE 14.7 Tool.

Keywords: Three-operand adder, carry save adder (CSA), Han-Carlson adder (HCA), modular arithmetic.

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 the efficient implementation of

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal www.ijarst.in
ISSN: 2457-0362

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 binary addition is also a primary arithmetic operation in the linear congruential generator (LCG) based pseudo-random bit generators (PRBG) such as coupled LCG (CLCG), modified dual-CLCG (MDCLCG) and coupled variableinputLCG (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 for bit greater than 32-bits. Therefore, the security of the MDCLCG enhances with the increase of operand size. However, the area and critical path delay increases linearly since its hardware architecture consists of four three-operand modulo-2n adders, two comparators,four multiplexer's area in previous papers. Hence, the performance of the MDCLCG can be improved by the efficient implementation of the three-operand adder.

LITERATURE REVIEW

In 2019, A. K. Panda and K. C. Ray [1], proposed that pseudorandom bit generator (PRBG) is an essential component for securing data during transmission and storage in various cryptography applications. Among popular existing PRBG methods such as linear feedback shift register (LFSR), linear congruential generator (LCG), coupled LCG (CLCG), and dual-coupled LCG (dual-CLCG), the latter proves to be more secure. This method relies on the inequality comparisons that lead to generating pseudorandom bit at a non-uniform time interval. Hence, a new architecture of the existing dual CLCG method is developed that generates pseudo-random bit at uniform clock rate.

In 2015, A. Rezai and P. Keshavarzi [3], proposed that Modular exponentiation with a large modulus and exponent is a fundamental operation in many public-key cryptosystems. This operation is usually accomplished by repeating modular multiplications. Montgomery modular multiplication has been widely used to relax the quotient determination. The carry–save adder has been employed to reduce the critical path. This paper presents and evaluates a new and efficient Montgomery modular multiplication architecture based on a new digit serial computation.

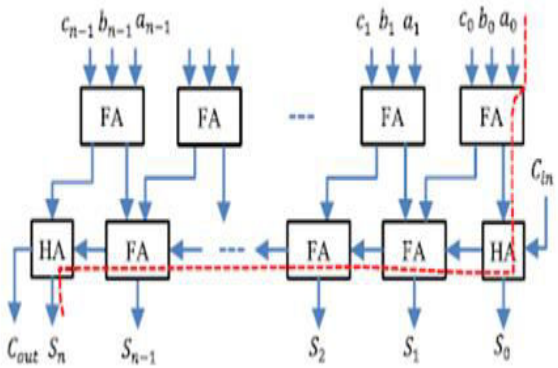
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

In 2017 S. S. Erdem, T. Yanik, and A. Celebi [5], an efficient digit-serial hardware architecture for Montgomery algorithm. As many previous works, carry-save adders are used to accumulate partial products to avoid carry propagation delay.The Montgomery algorithm is a fast modular multiplication method frequently used in cryptographic applications. This paper investigates the digit-serial implementations of the Montgomery algorithm for large integers.

EXISTING METHOD

The three-operand binary addition is one of the critical arithmetic operation in the congruential modular arithmetic architectures various existing methods and LCG-based PRBG methods such as CLCG, MDCLCG and CVLCG. It can be implemented either by using two stages 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 array of fulladders. Each full adder computes "carry" bit and "sum" bit concurrently from three binary input , $bi\ and\ ci$. 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 output of three-operand addition. The "carry-out" signal is propagated through the *n* number of full adders in the ripple-carry stage. Therefore, the delay increases linearly with the increase of bit length. The architecture of the three-operand carry-save adder is shown below figure.Where critical path delay is highlighted with a dashed line. It shows that the critical path delay depends on the carry propagation delay of ripple carry stage and is evaluated as follows.

Fig.1:Three-operand carry-save adder (CS3A) showing critical path delay.



The major drawback of the CS3A is the larger critical path delay which increases with an increase of bit length.

On the other hand, the hybrid Han-Carlson adder is designed with two Brent-Kung stages each at the beginning and the end, and with Kogge-Stone stages in the middle. Thisresultant a slightly higher delay (two gates delay) than the Han- Carlson adder,

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

with reduction in the hardware complexity when compare to other parallel prefix adders.

The two stages of two-operand Han-Carlson adders (HC2A- 1 and HC2A-2) compute the addition of three operands. The detailed architecture of two-operand Han-Carlson adder (HC2A). It has three stages such as base logic, PG (propagate and generate) logic and sum logic. The logical diagram of base cell in base logic and sum cell in sum logic.

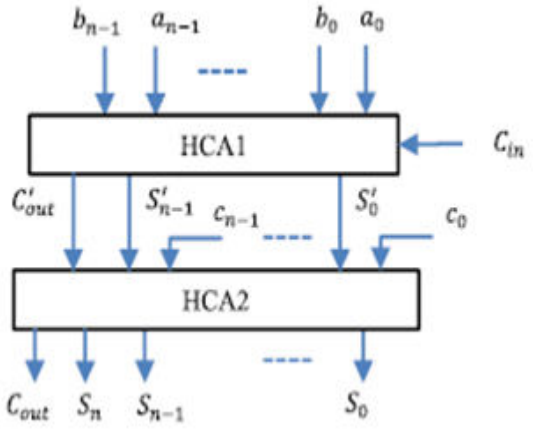


Fig.2: Block level architecture of HCA-based three-operand adder (HC3A).

Essentially, the Han-Carlson adder provides a reasonably good speed at low gate complexity as compared to other existing two-operand adder techniques. It has the lowest area delay product (ADP) and power-delay product (PDP) among all. Thus, the three-operand addition can be performed using Han-Carlson adder (HCA) in two stages, as shown in above figure. The detailed architecture of HCA-based three-operand adder (HC3A). The maximum combinational path delay of HC3A depends on the propagate chain, i.e. the number of black-grey cell stage in the PG logic of Han-Carlson adder.

PROPOSED METHOD

This section presents a new adder technique and its VLSI architecture to perform the three-operand addition in modular arithmetic. The proposed 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. The logical expression of all these four stages are defined as follows,

Stage-1: Bit Addition Logic:

$$S'_i = a_i \oplus b_i \oplus c_i,$$
$$cy_i = a_i \cdot b_i + b_i \cdot c_i + c_i \cdot a_i$$

Stage-2: Base Logic:

$$G_{i:i} = G_i = S'_i \cdot cy_{i-1}, \quad G_{0:0} = G_0 = S'_0 \cdot C_{in}$$
$$P_{i:i} = P_i = S'_i \oplus cy_{i-1}, \quad P_{0:0} = P_0 = S'_0 \oplus C_{in}$$

Stage-3: **PG (Generate and Propagate)**

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

Logic:

$$G_{i:j} = G_{i:k} + P_{i:k} \cdot G_{k-1:j},$$
$$P_{i:j} = P_{i:k} \cdot P_{k-1:j}$$

Stage-4: **Sum Logic:**

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

The proposed VLSI architecture of the three-operand binary adder and its internal structure is shown in above figure. The new adder technique performs the addition of three *n*-bit binary inputs in four different stages. In the first stage (bit-addition logic), the bitwise addition of three *n*-bit binary input operands is performed with the array of full adders, and each full adder computes "sum $(S\,i\,)$" and "carry $(cyi\,)$" signals. The logical expressions for computing sum $(Si\,)$ and carry $(cyi\,)$ signals are defined in Stage-1, and the logicaldiagram of the bit-addition logic is similar to full adder.

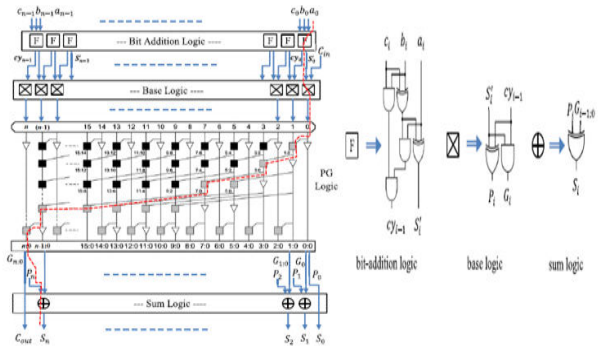
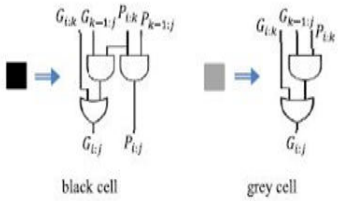


Fig.3: Proposed three-operand adderFig.4:Logical diagram of bit addition,base logic,sum logic



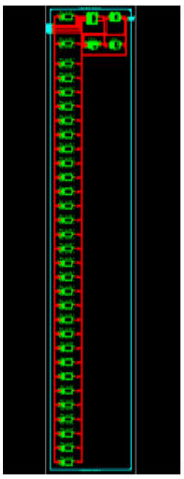


Fig.5: Logic diagram black-cell and grey-cell.Fig.6: RTL Diagram

METHODS OR TECHNIQUES USED

Xilinx Tools is a suite of software tools used for the design of digital circuits implemented using Xilinx Field Programmable Gate Array (FPGA) or Complex Programmable Logic Device (CPLD). The design procedure consists of (a) design entry, (b) synthesis and implementation of the design, (c) functional simulation and (d) testing and verification. Digital designs can be entered in various ways using the above CAD tools: using a schematic entry tool, using a hardware description language (HDL) – Verilog or VHDL or a combination of both. In this lab we will only use the design flow that involves the use of Verilog HDL.

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

RESULT

The proposed architectures have been designed under the design environment for comparing the results justifiably.

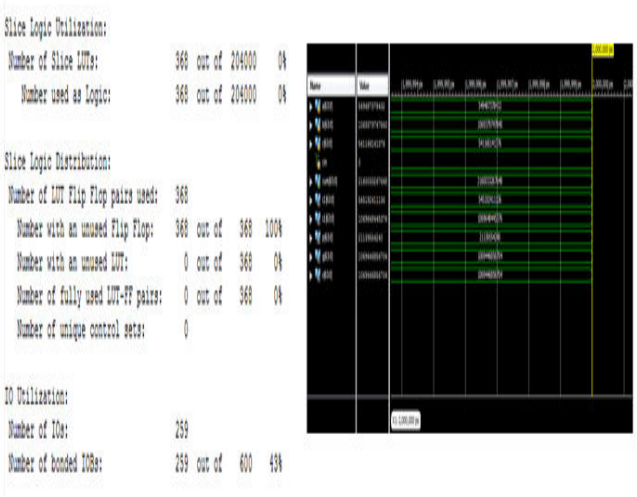
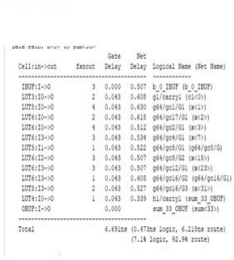


Fig.7: Area Report

Fig.8: Simulation result



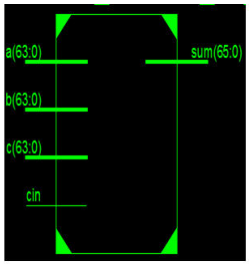


Fig.9: Delay Report Fig.10: Block Diagram

Table.1: Comparison between existing method and proposed method

	Area (in LUT's)	Delay (in ns)
CS3A	192	36.786
HC3A	444	9.622
Proposed Adder	**368**	**7.531**

APPLICATIONS

1. Arithmetic logic units.
2. High speed Multiplications.
3. Advanced Microprocessor design.
4. Pseudorandom bit generator (PRBG) algorithms.
5. Cryptography.

CONCLUSION

In this paper, a high-speed area-efficient adder technique and its VLSI architecture is proposed to perform the three-operand binary addition in various cryptography

algorithms. The proposed three-operand adder technique is a parallel prefix adder that uses four-stage structures to compute the addition of three input operands. The novelty of this proposed architecture is the reduction of delay and area in the prefix computation stages in PG logic and bit-addition logic that leads to an overall reduction in critical path delay. It also decreases the area complexity when compare to other parallel prefix three operand adders. Form the above comparison, the proposed three operand binary adder consists of less area and less delay when compare to existing in CS3A and HC3A three operand adder. The synthesis and simulation are verified by using Xilinx ISE tool.

The proposed 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. Hence, we can modify the PG (propagate and generate) and replace with other carry propagation stages to generate the sum value. By modifying these designs, we get improvement in the parameters like area and delay.

REFERENCES

[1] A. K. Panda and K. C. Ray, "Modified dual-CLCG method and its VLSI architecture for pseudorandom bit generation," *IEEE Trans. CircuitsSyst. I, Reg. Papers*, vol. 66, no. 3, pp. 989–1002, Mar. 2019.

[2] 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

[3] 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

[4] K. S. Pandey, D. K. B. N. Goel, and H. Shrimali, "An ultra-fast parallel prefix adder," in *Proc. IEEE 26th Symp.Comput. Arithmetic (ARITH)*, Kyoto, Japan, Jun. 2019, pp. 125–134.

[5] 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.

[6] S.-R. Kuang, J.-P.Wang, K.-C.Chang, and H.-W. Hsu, "Energy-efficient high-throughput montgomery modular multipliers for RSA cryptosystems," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 11, pp. 1999–2009, Nov. 2013.