IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 2, February 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

High-Speed Area-Efficient VLSI design of Three-Operand Binary Adder

A. Priyanga[1], C.N. Marimuthu[2]

PG Scholar, Department of Electronics and Communication Engineering, Nandha Engineering College, Erode, Tamil Nadu, India[1]

Professor, Department of Electronics and Communication Engineering, Nandha Engineering College, Erode, Tamil Nadu, India[2]

ABSTRACT: Carry Save Adder (CSA) is the extensively used fashion to perform the three operand addition. This adder is that the start purposeful unit to perform fully completely different calculation in cryptography and pseudorandom bit generator (PRBG) rule. However, the ripple carry stage in the CSA leads to a high propagation delay of 0(n). Also, the complement of the carry is generated and propagated inside the carry network of the proposed adder in order to drop the detention. It is one of the foremost promising ways to achieve power consumption for the summation of big operands. This study presents a new replacement adder architecture, specifically designed for big operands, supports on the premise that in massive parallel-prefix adders the smallest significant carries are produced much sooner than the most-significant ones. This ends up in decrease of the area of the summation blocks while not compromising the speed. The results of the proposed adder reported is quicker than the CSA for 32-,64- and 128- bit design severally.

KEYWORDS: Three-operand adder, Pseudorandom bit generator (PRBG), carry save adder (CSA)

I. INTRODUCTION

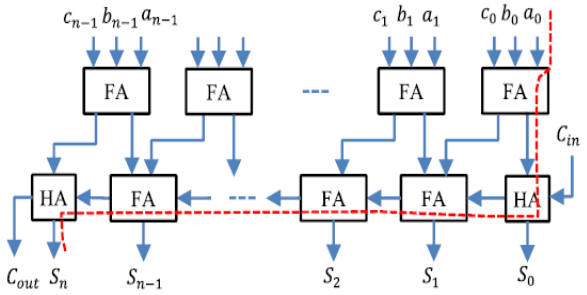
To achieve optimum system performance whereas maintaining physical security, it's necessary to implement the cryptography algorithms on hardware standard arithmetic like standard mathematical operation, standard multiplication and standard addition is often used for the arithmetic operations in varied cryptography algorithms so, and the performance of the cryptography formula depends on the economical implementation of the congruential standard operation. The foremost economical approach to implement the standard multiplication and mathematical operation is that the Montgomery formula whose important operation relies on three-operand binary addition. The three-operand binary addition is additionally a primary operation within the linear congruential generator (LCG) based mostly pseudo-random bit generators (PRBG) like coupled LCG (CLCG), changed dual-CLCG (MDCLCG) and matched variable input LCG (CVLCG) changed dual-CLCG (MDCLCG) is that the most secure and extremely random PRBG technique among all the LCG-based and alternative existing PRBG ways. It's polynomial-time unpredictable and secure if n _32-bits. Therefore, the safety of the MDCLCG enhances with the rise of quantity size. However, the region and important path delay will increase linearly since its hardware design consists of 4 three-operand modulo-2n adders, 2 comparators, four multiplexer's space. Hence, the performance of the MDCLCG will be bettered by the provident perpetration of the three-operand adder. The three-operand binary addition are applied either used as a pair of two-operand adders or 1 three-operand adder. The three-operand binary addition may be allotted either by mistreatment 2 two-operand adders or one three-operand adder. Carry-save adder (CS3A) is that the area-efficient and wide adopted technique to perform the three-operand binary addition at intervals the quality arithmetic used in cryptography algorithms and PRBG ways that. However, the longer carry propagation delay at intervals the ripple-carry stage of CS3A seriously influences the performance of the MDCLCG and different cryptography architectures on IoT based hardware devices. Therefore on dock the veritably important path detention, a prefixed two-operand adder like Han-Carlson (HCA) may be used for three-operand double addition. It reduces the vital path delay within the order of O(log2 n) however will increase the region within the order of O(n log2 n). Therefore, it's a necessity to develop associate economical VLSI style to carry out the short three-operand binary addition with minimum hardware resources. Hence, a novel high-speed space-efficient adder technique is planned practice pre-compute bitwise addition followed by carry-prefix computation logic to perform the three-operand addition throughout this paper that consumes considerably lower gate space whereas minimizing the propagation detention compared to the HCA- grounded three-operand adder (HC3A). The planned adder design is enforced with the Verilog HDL, then synthesized with industrial

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

obtainable 32nm CMOS technology library. Also, the area and power- delay of the planned adder fashion are measured and compared with reference to the present CS3A and HC3A three-operand adder ways.



The conflation result of the proposed adder armature along with other exiting adder ways is also reported in this section. Further, the proposed adder is incorporated in the modified binary-CLCG operation to measure the performance 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 compass using an intertwined sense analyser.

II. LITERATURE SURVEY

Developing a excessive-fast elliptic curve cryptography (ECC) processor that performs quick purpose multiplication with low hardware utilization may be a crucial demand within the fields of cryptography and network security. This paper presents field-programmable gate array (FPGA) implementation of a high-speed, low-area, side-channel attacks (SCAs) resistant error correction code processor over a primary field [1]. Elliptic Curve Cryptography (ECC) has been wide used for the digital signature to make sure the safety in communication. It's vital for the processor to support a range of cryptographhy standards to be compatible with totally different security applications. Thus, a versatile processor which may support totally different standards and algorithms is desired. During this paper, dual-field cryptography processor mistreatment the hardware-software approach is given. The projected processor will support arbitrary elliptic curve. It elaborate standard Arithmetic Logic Unit (MALU) is meant. [2]. this paper proposes a straightforward and economical Montgomery multiplication formula specified the affordable and superior Montgomery standard multiplier factor will be enforced consequently. The projected multiplier factor receives and outputs the info with binary illustration and uses solely one-level carry-save adder (CSA) to avoid the carry propagation at every addition operation. [3]. Verification of Associate in Nursing ECDSA signature needs a double scalar multiplication on Associate in Nursing elliptic curve. During this work, we tend to study the computation of this operation on a twisted Edwards curve with expeditiously calculable endomorphism,that permits reducing the quantity of purpose doublings by just about five hundredth compared to a traditional implementation [4]. During this work, we tend to study the computation of this operation on a twisted Edwards curve with expeditiously calculable endomorphism, That permits reducing the quantity of purpose doublings by just about five hundredth compared to a traditional implementation [5]. Pseudorandom bit generator (PRBG) is a necessary part for securing information throughout transmission and storage in varied cryptography applications. Among in style existing PRBG strategies like linear feedback register (LFSR), linear congruential generator (LCG), coupled LCG (CLCG), and dual-coupled LCG (dual-CLCG), the latter proves to be safer. This methodology depends on the difference comparisons that result in generating pseudorandom bit at a non-uniform interval. [6]. Parallel Prefix adder's area unit arguably the foremost unremarkably used arithmetic units. they need been extensively investigated at design level, register transfer level (RTL), gate level, circuit level similarly as layout level giving rise to a superfluity of mathematical formulations, topologies and implementations [7]. The requirement of hardware security for internet-of things applications demands an occasional hardware space, high speed and secure pseudorandom bit generator (PRBG). Amongst varied PRBGs, Blum-Blum-Shub (BBS) is that the verified cryptographically secure PRBG attributable to its massive prime resolve downside. The economical implementation of BBS methodology depends on the massive number standard multiplication that makes it computationally expensive [8]. Standard mathematical process with an oversized modulus and exponent may be a elementary operation in several public-key cryptosystems. This operation is typically accomplished by repetition standard multiplications. Montgomery standard multiplication has been wide accustomed relax the quotient determination. The carry–save adder has been utilized to scale back the important path [9].

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

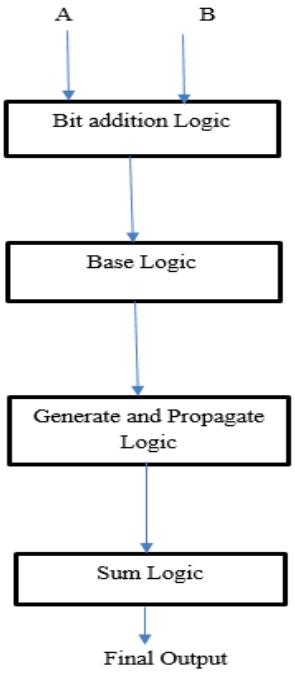
|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

III. THREE OPERAND ADDER BINARY TECHNIQUES

The three-operand binary addition is one among the important operation within the congruential standard arithmetic architectures and LCG-based PRBG ways like CLCG, MDCLCG and CVLCG. It is enforced either by mistreatment 2 stages of two-operand adders or one stage of three-operand adder. Carry-save adder (CSA) is that the usually used technique to perform the three-operand binary addition [11]. It computes the addition of 3 operands in 2 stages. The primary stage is that the array of full adders. Every full adder computes "carry" bit and "sum" bit at the same time from 3 binary input ai , bi and ci. The second stage is that the ripple-carry adder that computes the ultimate 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 variety of full adders within the ripple-carry stage[12].

Therefore, the delay will increase linearly with the rise of bit length[10]. The design of the three-operand carry-save adder is shown in Fig. one and therefore the important path delay is highlighted with a broken line. It shows that the important path delay depends on the carry propagation delay of ripple carry stage and is evaluated as follows,
TCS3A = (n+1)TFA = 3TX + 2nTG
Similarly, the overall space is evaluated as follows,
ACS3A = 2nAFA = 4nAX + 6nAG
Here, noble metal and TG indicate the world and propagation delay of basic 2-input gate (AND/OR/NAND/NOR) severally. AX and TX indicate the world and propagation delay of 2-input logic gate severally.



Therefore, the delay will increase linearly with the rise of bit length. The design of the three-operand carry-save adder is shown in Fig. one and therefore the important path delay is highlighted with a broken line. It shows that the important path delay depends on the carry propagation delay of ripple carry stage and is evaluated as follows,

TCS3A = (n+1)TFA = 3TX + 2nTG

Similarly, the overall space is evaluated as follows,

ACS3A = 2nAFA = 4nAX + 6nAG

Here, noble metal and TG indicate the world and propagation delay of basic 2-input gate (AND/OR/NAND/NOR) severally. AX and TX indicate the world and propagation delay of 2-input logic gate severally.

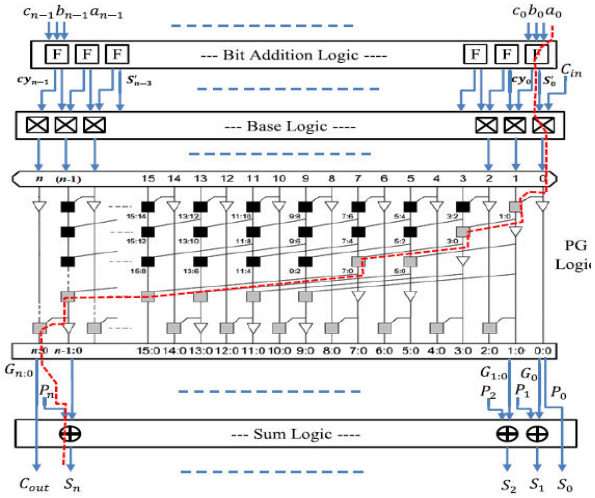
| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

IV. EXISTING SYSTEM

In this existing technique, 3 operand adder technique is employed. This adder circuit comprises 5 logic circuit. That area unit Bit-addition logic, Base logic, PG logic (Black cell and gray cell), and besides that add logic. Add logic circuit is that the ending of the 3 quantity adder circuit. The input of the bit addition logic circuit could be a,b,c then the output is add and carry. Then the output of add and carry is given to the input of next base logic circuit. In Base logic propogation and generation are generated. when the PG logic the ultimate add logic are dead. By mistreatment Xilinx ISE fourteen. The result are generated.



The logical expression of of these four stages area unit outlined as follows,
Stage-1: Bit Addition Logic
Si = ai^bi^ci ,
cyi = ai • Bi + Bi • ci + ci • ai
Stage-2: Base Logic
Gi:i = Gi = Si • cyi−1, G0:0 = G0 = S0•Cin
Pi:i = Pi = Si^cyi−1, P0:0 = P0 = S0^Cin
Stage-3: PG (Generate and Propagate) Logic
Gi: j = Gi:k + Pi:k • Gk−1: j ,
Pi: j = Pi:k • Pk−1: j
Stage-4: add Logic
Si = (Pi^Gi−1:0) , S0 = P0, Cout = Gn:0

V. PROPOSED SYSTEM

The hardware security within the field of IoT applications demands stream-cipher based mostly high rate, light-weight cryp- tography technique for quickest encryption/ decoding. Key generator or pseudorandom bit generator (PRBG) is that the primary element within the stream-cipher based mostly encryption/ decoding. changed dual-CLCG (MDCLCG) is that the most effective PRBG technique amongst the prevailing PRBG ways that is appropriate for stream-cipher based mostly hardware security. However, the protection strength of the MDCLCG technique lin- early depends on the bit size of the congruential modulus. it's polynomial-time unpredictable and secure if n ≥ 32- bits.

The hardware design of the MDLCG technique is supported LCG, as shown in Fig. five during which three-operand modulo- 2n adder is that the primary machine arithmetic block. The MDCLCG design given in [10] is developed with four three-operand modulo-2n carry-save adders (CS3A) and 2 magnitude comparators together with four registers and multiplexers. The longer carry propagation gate delay in CS3A adder influences the performance of MDCLCG design with associate degree increase of bit size. Therefore, in this section, the performance metrics of the MDCLCG square measure measured by replacement the CS3A adder with the HHC3A and planned adder architectures.

By considering the operation of three-operand modulo-2n addition in MDCLCG technique, the design of the planned adder is additional redesigned. Therefore, the area (AP3OA) and time (TP3OA) quality of the planned adder design are often evaluated for three-operand modulo-2n addition as follows,

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

TP3OA ≈ 4TX + two log2 nr + one TG

Here, s log2 n one and nr n one. Similarly, the area (Amgc) and time (Tmgc) quality of the magnitude comparator is evaluated in [10] that is additional highlighted as follows,

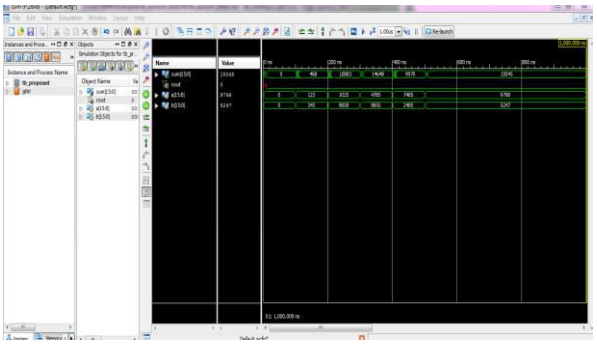
Amgc ≈ (n−1) [9AG + 4AN]
Tmgc ≈ fourTX + 4 log2 n TG
Therefore, the area and time quality of the MDCLCG design victimization the planned adder and therefore the magnitude comparator are often evaluated as follows,

TMDCLCG ≈ T3oa + Tmx
4TX 2 log nr 2 TG
AMDCLCG = four Amx + A3oa + Arg + 2Acmp + AX
≈ (16n − 7) AX + +4 (3n − 2) associate degree + 4nAFFg

It is ascertained that the planned adder is quicker than the CS3A, HC3A and HHC3A primarily based MDCLCG architectures. Similarly, it consumes sixteen.5% less space and fifteen.1% less power than the HC3A- primarily based MDCLCG design. Moreover, it achieves all-time low ADP and PDP than the CS3A and HC3A primarily based MDCLCG architectures. it's reportable the reduction of forty eight.7% and 36.2% ADP as compared to the CS3A and HC3A primarily based MDCLCG architectures.

VI. RESULT AND DISCUSSION

The existing adder circuit is that the 3 adder. The 3 adder circuit comprises 5 main blocks, that area unit bit addition logic, base logic, PG logic (Black cell and gray cell) and add logic. During this existing adder consumes high power compared the projected hybrid adder circuit.



Simulation Wave for Existing TOA

The three-operand binary addition is one among the important operation within the congruential standard arithmetic architectures and LCG-based PRBG ways like CLCG, MDCLCG and CVLCG. It is enforced either by mistreatment 2 stages of two-operand adders or one stage of three-operand adder. Carry-save adder (CSA) is that the usually used technique to perform the three-operand binary addition. It computes the addition of 3 operands in 2 stages. The primary stage is that the array of full adders. Every full adder computes “carry” bit and “sum” bit at the same time from 3 binary input ai , bi and ci. The second stage is that the ripple-carry adder that computes the ultimate 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 variety of full adders within the ripple-carry stage. Therefore, the delay will increase linearly with the rise of bit length.

VII. CONCLUSION

In this paper, a high-speed area-efficient adder technique and its VLSI design is planned to perform the three-quantity binary addition for economical computation of standard arithmetic employed in cryptography and PRBG applications. The planned 3-operand adder technique may be a parallel prefix adder that uses four-stage structures to reckon the addition of three input operands. The novelty of this planned design is that the reduction of delay and space within the prefix computation stages in PG logic and bit-addition logic that results in an overall reduction in crucial path delay, area-delay product (ADP) and power-delay product (PDP). For the honest compar- ison, the thought of

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 11, Issue 2, February 2022 ||

| DOI:10.15680/IJIRSET.2022.1102017 |

hybrid Han-Carlson two-operand adder is extended to develop a hybrid Han-Carlson three-operand adder (HHC3A) topology. The same cryptography vogue adopted in planned adder design is extended to implement the HHC3A, HC3A and CS3A mistreatment Verilog HDL. Further, of these styles area unit synthesized mistreatment commercially out there 32nm CMOS technology library to get the core space, temporal order and power for various word size. From the physical synthesis results, this can be clear that the planned adder design is three to nine times quicker than the corresponding CS3A adder design. Moreover, a pointy reduction in space utilization, temporal order path and power dissipation is ascertained within the planned adder as compared to the HC3A adder. it's additionally price noting that the planned adder has considerably less ADP and PDP compared to different three-operand adder techniques. It has 55.1%, 71.6% and 82.7% reduction on ADP, and 55.1%, 71.8% and 82.9% reduction on PDP over CS3A adder for 32- 64- and 128- bit architectures severally.

Further, a 32- bit MDCLCG design given in literature is intended with the planned adder design by exchange its CS3A three-operand adder design, and prototyped on commercially out there FPGA device for planning on a semiconductor device. The performance metrics reportable that the planned adder primarily based MDCLCG design is a pair of.34 times quicker than CS3A-based MDCLCG design that creates it appropriate to develop a high rate light-weight hardware security system within the field of IoT.

REFERENCES

[1] Amit Kumar Panda, Rakesh Palisetty & Kailash Chandra Ray, "High Speed Area Efficient VLSI Architecture of Three Operand Binary Adder", IEEE Trans.Vol.67 No.11, Nov 2020.
[2] A. Kumar Panda and K. Chandra Ray, "A coupled variable input LCG technique and its VLSI architecture for pseudorandom bit generation," IEEE Trans. Instrum. Meas., vol. 69, Apr. 2020.
[3] Xifan Tang,Edouard Giacomin, Giovanni De Michelli, "FPGA-SPICE:A Simulation based Architecture Evaluation based Framework for FPGAs" ,IEEE Trans.Vol.27 No.3, Mar 2019.
[4] A. K. Panda and K. C. Ray, "Design and FPGA prototype of 1024-bit Blum-Blum-Shub PRBG design," in Proc. IEEE Int. Conf. Inf.Commun. Signal Process. (ICICSP), Singapore, Sep. 2018, pp. 38–43.
[5] S. S. Erdem, T. Yanik, and A. Celebi, "A general digit-serial architecture for montgomery standard multiplication," IEEE Trans. Very Large ScaleIntegr. (VLSI) Syst., vol. 25, no. 5, pp. 1658–1668, May 2017.
[6] Shh-Lun Chen,Min-Chun Tuan,Ho-Yin Lee and Ting-Lan Lin, "VLSI Implementation of a Cost-Efficient Micro Control Unit With an Assymetric Encryption for Wireless Body Sensor Networks", IEEE Trans.Vol.5,Apr 2017.
[7] Shh-Lun Chen,Min-Chun Tuan,Tse-Yen-Liu,Chia-Wei-Shen, "VLSI Implementation of a Cost- Efficient Near-lossless CFA Image Compressor for Wireless capsule Endoscopy", IEEE Trans.Vol.4,Jan 2017.
[8] 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
[9] D. L. Harris, "Parallel prefix networks that create tradeoffs between logic levels, fan out and wiring racks, "Nov. 11, 2004.
[10] B. Parhami, "Computer Arithmetic: Algorithms and Hardware Design" New York, NY, USA: Oxford Univ. Press, 2000.
[11] C N Marimuthu and P Thangaraj "Low power high performance multiplier," Proc. ICGST-PDCS, 2008
[12] C N Marimuthu, P Thangaraj and Aswathy Ramesan - "Low power high performance multiplier," International Journal of Computer Science and Information Technology 2.3 (2010) 12-22

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details