DESIGN AND IMPLEMENTATION OF FAULT FREE AHL MULTIPLIER FOR CRYPTOGRAPHY APPLICATIONS

[1]Dasari Bhavani, [2]Dr.Abdul Rahiman Sheik

[1]M.Tech, Dept of ECE, NRI Institute of Technology, Agiripalli, Vijayawada, India.
[2]Professor, Dept of ECE, NRI Institute of Technology, Agiripalli, Vijayawada, India.

ABSTRACT: In VLSI circuits, mostly used circuits are arithmetic circuits. In those mainly multipliers. Multipliers are designed by using the different types of adders. The most significant mathematical functions in systems, such as Fourier transforms, Discrete Cosine Transforms (DCT), are Digital multipliers. Depending upon the circuits components, the speed of the circuit will be estimated. The important components in multipliers are microprocessors, Digital Signal Processors (DSPs), and embedded systems, and along with Convolutional Neural Networks (CNN) and filtering. In this analysis, Design and implementation of fault free AHL multiplier circuit for cryptography applications is to be implemented. Fundamentally, multipliers are important computational circuits, along with DSP. This error-free AHL multiplier utilizes an adder circuit which regulates carry propagation. The main intent of CRC (Cyclic Redundancy Check) is to detect and correct errors. From the results, it can observe that it is simulated using Xilinx technology. Hence, this analysis reduces the errors in effective way.

KEY WORDS: Digital Signal Processing (DSP), AHL (Adaptive Hold Logic) multiplier, CRC (Cyclic Redundancy Check).

I.INTRODUCTION

In the present generation, the advanced computing applications, communication applications, power utilization applications have been more popular. They mainly depend on the size, cost and chip quality of the circuit [1]. Generally, in integrated chip, power consumption plays very important role. Generally, finite fields are most often used in communication systems such as error correcting codes and cryptography.

Mathematical functions are implemented on array elements [2].
Two foundations are usually implementing a method that consists of a common base and a polynomial base. Implement the hardware using ordinary bases to implement the cheap squaring operation.

Similarly, polynomial basis is used in software implementations, and similarly cheap squaring operations are performed [3]. An energy usage in CMOS (Complementary Metal-Oxide-Semiconductor) includes dynamic and static power as well as short-circuits current usage. The use of dynamic force is usually based on the dynamic force used in loading the lifting capacity.

The power consumption of systems is directly proportional to their accuracy of multiplication. If the device needs higher accuracy, it will consume more power and conversely. Additionally, these systems may require sections or modules that are less accurate than the rest of the device. Keeping the accuracy stable for the modules that improves the energy consumption for entire device [4].

Therefore, changing the multiplier precision based on the needs of modules or section of the overall system will have a significant effect on minimizing system energy consumption [5]. This system of configuring and modifying multiplier accuracy based on systems or applications that needs to be attained by characterizing the accuracy based on approximation techniques using the various adder sub-modules of the multiplier module. Different program levels or applications require reconfigurable multipliers [6].

Transistor geometries are scaled to integrate many systems into small spaces, facilitating implementation of difficult high-speed applications in hardware. This power has transformed electronics as well as industry [7]. Many examiners, designers, and engineers have developed many innovative techniques and ideas to reduce power consumption.

Therefore, engineers must plan for energy consumption as a factor almost as significant as power, and in some cases, it is more significant than space. Low-power models are appropriately performed in difficult design of Very Large Scale Integration (VLSI) circuits. New low-power design techniques for VLSI are always needed as the demand for faster, cheaper, and more valid electronics, which operate on remote power supplies and enable high-end applications that can grow continuously [8].

Multiplier has a significant part in today's generation of digital signal processing. Multipliers are most commonly used in many applications, not just DSPs. Difficult multiplications and additions are implemented in DSP. The main focus is on reducing system latency. Several pipeline units have been implemented in modern digital signal processors, supercomputers and vector processors [9]. A multiplication function is implemented to produce a high significant time. Therefore, pipeline architecture is employed to apply high evaluation operations within the system.

Multiplication is basic mathematical operation for regular DSP applications such as the Fast Fourier Transform (FFT) [10]. Equal cluster multipliers are often used to achieve high execution speed. Therefore, these multipliers has high power. Multiplier deployment is a core concern in the current VLSI framework. Designers are planned to develop powerful multipliers for planning low-power DSP models.

This requires an oscillating network for the power supply. Here, the main issues or design requirements that can be considered in adiabatic CMOS circuits. Execution requires an integrated force supply and an energy-efficient plan of time. Addition, subtraction, multiplication, and division are the main functions of the arithmetic model, which can be performed each frame. Whether it runs into a lot of computational problems depends on how fast the incremental activity can run.

Multipliers are the most important device drawbacks in hybrid DSP models. The most important tasks in modern drawing preparation are moving, folding, and internal elements. DSP models generally require multipliers that contain sophisticated digitalized communication systems.

II. LITERATURE SURVEY

V. S. Chirde and U. Jadhav.et.al [11], In VLSI, transistors scaling performs a key role in minimizing power consumption and improves speed from a technology node to another node. However, transistor sizes continue to shrink, many specifications raised such as short-channel effects, subthreshold conditions, body effects, and aging. Negative Bias Temperature Instability

(NBTI) improves the threshold Voltage (Vth) if pMOS is negatively biased (Vgs=-Vdd). This impact slows down the device. This article proposes design with Adaptive Hold Logic (AHL) circuitry to mitigate fading effect. AHL circuits are utilized to demonstrate the impacts of transistor aging. The circuits were designed with the Tanner EDA (Electronic Design and Automation) 13.0 tool by using the 22nm technology node.

T. Pardhu and N. A. Reddy.et.al [12], in this analysis, new techniques can be used to design low-power multipliers. This model presents a hybrid full adder and compressor. This adder allows the majority of multiplier partial product bits to be generated with NAND gates rather than the AND gates and inverters utilized in signal multipliers such as the Baugh-wooley multiplier, reducing power utilization and all the transistors are required. In this article, the design an 8×8 array and Baugh-wooley multiplier, utilizes these new adders, and a tree multiplier by utilizing a compressor, delay and area of these multipliers are compared. The 8x8 implementation, the array multiplier reduces power consumption by 7.8% and Baugh-Wooley multiplier compared with transistor count by 7.8% while increasing time delay. The tree multipliers have lower power consumption, 7.3% fewer transistors, and extended delays than traditional tree multipliers. Simulation outputs are observed using 0.18nm technology.

I.C.Lin, Y.-H.Cho and Y.M.Yang.et.al [13], Digital multipliers are the important mathematical operation system. The complete evaluation of these model based on the multiplier throughput. On the other hand, the pMOS transistor is negatively biased (V gs = -V dd), the temperature instability effect of the negative bias, enhances the V_{th} of pMOS transistor and slowing down the multiplier. A similar phenomenon, positive bias temperature instability, occurs if nMOS transistors are positively biased. The impacts slow down the transistors and an extended period can lead the device to fail because of a extension in period. Hence, it primarily develops reliable and efficient multipliers. This paper presents an aging-aware multiplier design using a new AHL device. This multiplier provides high flow by variable latency and allows adaptive hold logic circuitry have to be reduce degeneration evaluation over time.

S. Murugeswari and S. K. Mohideen.et.al [14] This article shows to modify existing well-known multipliers such as the Wallace and the truncated multiplier to improve power and area. The existed Wallace multiplier models, the Modified Carry-Save Adders (MCSA) are restored with carry-save adders, and MCSA full adders are also performed by utilizing multiplexers. Similarly, the common full adders in the shortened multipliers were restored with multiplexer-based full adders to attain small area and performance. The 8x8 multiplier is simulated in Models are synthesized in Xilinx10.1. The obtained result shows that the described modified multiplier has lower performance and smaller area with the existing multipliers.

Huapeng Wu.et.al [15], Bit-parallel finite field multiplication is based on polynomials can be achieved in two steps: polynomial multiplication and reduction module of the irreducible polynomial. Here, it presents an difficulty in upper bound modular polynomial. If the area is produced an irreducible in trinomial, then the closed expressions for coefficient of the products are explaining by using coefficient of multiplicand. The difficulty in multiplier architecture is complex track expansion, calculated as well as compared with existed methods for the similar array class. In addition, it presents the analytic form of the bit-parallel square function and its complexity also explained by using the irrevocable trinomial. It is maintained by solving inverse multiplication by using polynomial basis and it is better option for utilization in ordinary basis.

Jianing Su and Zhenghao Lu.et.al [16], This article presents parallel VLSI structures for GF(2 ^{14}) and GF(2 ^{16}) multipliers. The proposed parallel structure is based on the original finite field decomposition. Parallel structure allows the finite array multiplication to be completed in a few clock cycles at the cost of an acceptable increase in logic space. Mapping matrices and heuristic search algorithms of binary and composite field representations of GF(2 ^{14}) and GF(2 ^{16}) is presented. Two BCH (Binary Coded Hexadecimal) decoders based on GF (2^{14}) and GF (2^{16}) is described in parallel Galois multiplier structure is performed on Field Programmable Gate Array (FPGA). The complexity and data throughput description explains if it is related to finite field multiplication with high data throughput is required.

Y. Ma, T. Endoh and T. Shibata.et.al [17], A vertical MOSFET-based digital core circuit with vector matching functions have been described to achieve high-speed operation with low power consumption. Circuit design using planar as well as vertical Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET) models is implemented using 180nm CMOS technology and circuit operation is verified by NanoSim hardware simulation. Compared to conventional planar MOSFET packages, the power consumption of vertical MOSFET-based circuits is reduced by more than 30% regardless of operating frequency. In addition, due to the reduced circuit delay time, vertical MOSFET-based circuits achieve maximum operating frequencies than planar MOSFET packages up to 360MHz under the same simulation conditions. This described core circuits are used in flexibility and an independent vector matching circuit, also in a unit circuit of multi-core vector matching system.

Heiko Hinkelmann, Peter Zipf, Jia Li, Guifang Liu, Manfred Glesner.et.al [18], Multiplication is an important function in virtually all DSP systems. Few DSP models require various types of multiplications, especially integer multiplication or Galois Field (GF). As the operation allocates the structural similarities, there is an opportunity to effectively combine them into a single reconfigurable VLSI circuit in competitive area, performance and power utilization. It analyzes and discusses in detail of ten reconfigurable multiplier alternatives for various designs that combines integer and GF multiplication. The output is compared to the initial model and shows area savings up to 20% with a slight improvement in latency and also power consumption with 25%.

A.Hosseinzadeh, H.Namin, Wu and M.Ahmadi.et.al [19], A new serial-in-parallel-out finite field multiplier with redundant presentation is described. The described architectures have either less difficulty and less comparable delays or lower critical path delays, as well as less difficulty when compared with previously described models, by utilizing the similar representation, shown to be equivalent. For the class of fields the optimal Type I normal basis exists. The described multipliers are advantageous compared to the common basis multipliers. The modern multiplier of digit-level versions are recorded in this document

D.V.Poornaiah and P.V.A Mohan.et.al [20], This paper presents new model of multiplier-accumulator (MAC) VLSI model is expanded highly for second-order modified Booth algorithms. The effective designs, the Sign Extension Bit Minimization Algorithm (SEBMA) and the Sign Bit Update Algorithm, are also provided to minimize the added sign bit extensions and allow arbitrary word length input operands with different data formats. 3-Multiple bit transcoded parallel multipliers and MAC. A few characteristics of described multiplier-accumulator cell ability to perform various related computations: (i) Multiplication, (ii) accumulation (addition/subtraction), (iii) addition of carry bits because of existence of negative partial product terms compensation, and (iv) addition of the minimum number of sign-extended bits simultaneously Computation time is reduced by 50% and area is saved by 15% compared to the multiplier-accumulator cell. To check the described concept, recoded CMOS 3-bit, 16 bit MAC cell depended on 1 /spl mu/m CMOS standard cell technology rule was subjected to worst-case cycling the time is 35 ns, designed for a capacitive load of 50 pF.

III. EXISTED SYSTEM

Below figure (1) shows CRC-based error detection for finite field multiplier scheme. To execute the modules: the sum module, the α module, and the continuity module. The α module multiplies the elements of G F(2m) α as well as subtracts output of f (x) . The Pass-Thru multiplies the G F(2m) and G F(2) elements. The sum module adds two GF(2m) using m 2-input XOR gates. The multiplication utilizes a total of 'm − 1' sum factors, 'm − 1' alpha factors, and 'm' passage factors to obtain the result.

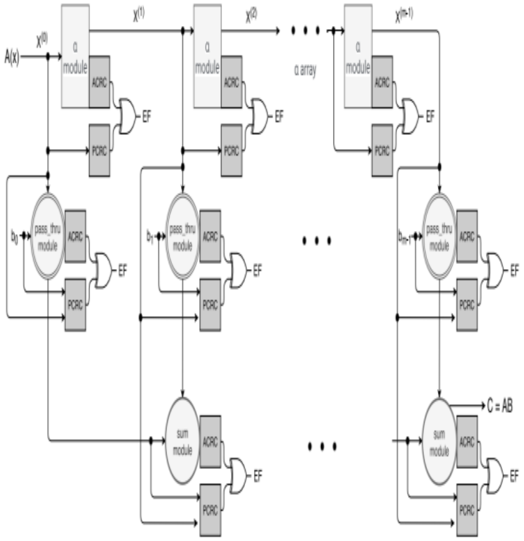

Fig. 1: FINITE FIELD MULTIPLIER WITH THE ERROR DETECTION SCHEMES BASED ON CRC

Error detection scheme of finite field multipliers is shown in Figure 1. If Actual CRC (ACRC) and Predicted CRC (PCRC) are related to its signatures. For clarity, it is shown in Figure 1. Therefore, it is described in this overview, CRC-5, 5 EFs are calculated in the module. In Fig. 2, α is explained clearly to the describe CRC signature works with every finite field multiplier.

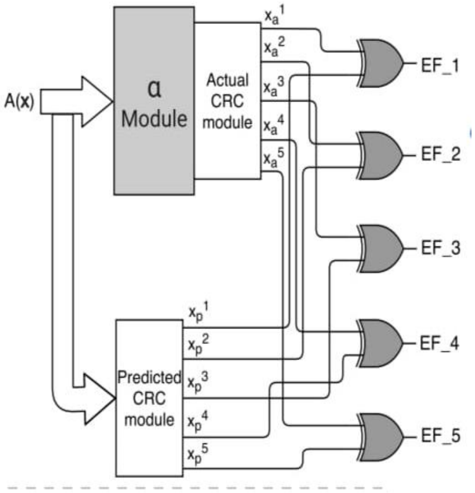

Fig. 2: ERROR-DETECTION CONSTRUCTION FOR MODULES

IV. PROPOSED SYSTEM

The block input for register multiplier contains of Root as well as Load M_r. Multiplier registers are usually connected to partial product generators. Similarly, the inputs of multiplicand register are shifting as well as compression bits. This shifts the information and loads it efficiently. The result contains outputs and stores the overall output.

Multiplication is important mathematical function in processors. It is difficult and also utilizes a large amount of processor space and power. Normally, the output of multiplying two operands of n bit size needs 2n bits. In the binary representation of the number, the MSB (Most Significant Bit) bits contain the product value, and the lower bits contain the smaller value. Few multipliers are designed with a constant size and compute the MSB (Most Significant Bit) bits of multiply functions.

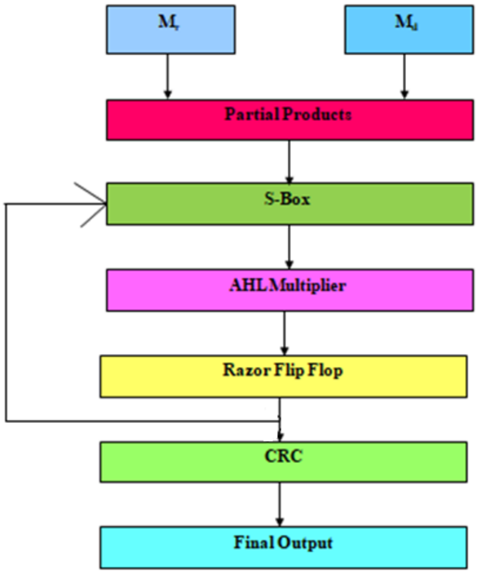

Fig. 3: BLOCK DIAGRAM OF PROPOSED SYSTEM

Design of circuit Multipliers "shift and add" calculation. The calculation is a fractional item is made for every piece in multiplier. Partial Product Generation (PPG) is utilized to produce propagator and generator signals. The subsequent PPG is shifted left by one bit position. The multiples of the multiplicand using the multiplier bits are generated. The weight of the partial product depends on the corresponding bit position of the multiplier.

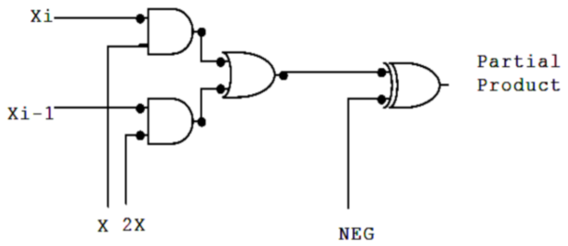

Fig. 4. PARTIAL PRODUCT GENERATOR CIRCUIT

S-boxes (substitution boxes) are the basic components of symmetric key models that perform permutations. In block ciphers, it is commonly utilized to complicate the relation of key and ciphertext. Commonly the S-box considers a certain numbers of input bits (m) and modifies into a certain outputs bits (n). However, n is not significantly equal to m.

The AHL is the most essential part of the variable-latency adder design. It helps to increase the speed of operation of the system.

Cyclic Redundancy Check (CRC) is a model used to find corrupted information or errors in data. A CRC uses a generator polynomial on both sender and receiver sides.

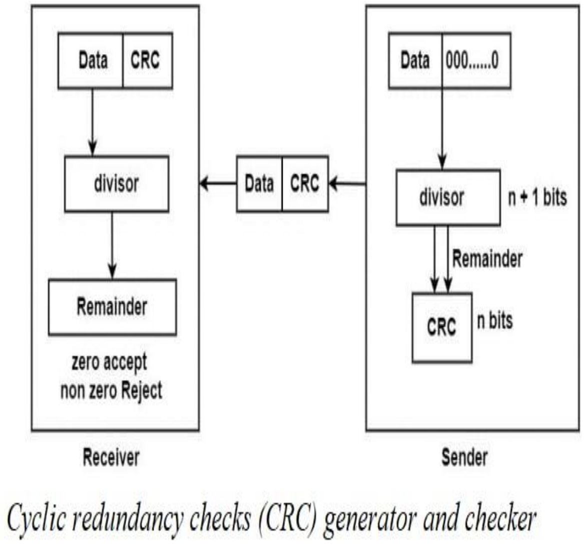

Fig. 5: CRC GENERATOR AND CHECKER

V. RESULTS

The below fig (6) shows the RTL schematic of existed system.

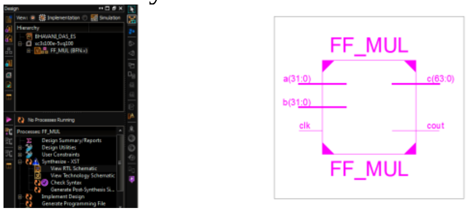

Fig. 6: RTL SCHEMATIC OF EXISTED SYSTEM

The below fig (7) the shows the RTL schematic of existed system.

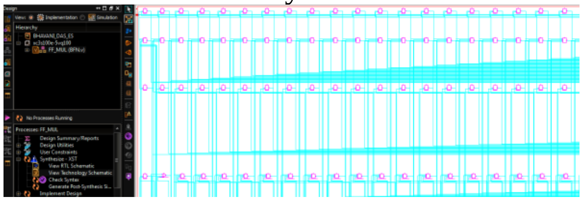

Fig. 7: TECHNOLOGY SCHEMATIC OF EXISTED SYSTEM

The below figure (8) is the output waveform of the existed system.

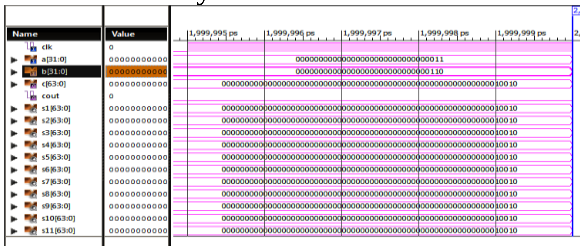

Fig. 8: OUTPUT WAVEFORM OF EXISTED SYSTEM

The below fig (9) the RTL schematic of proposed system is shown. The system is a combination of inputs and outputs.

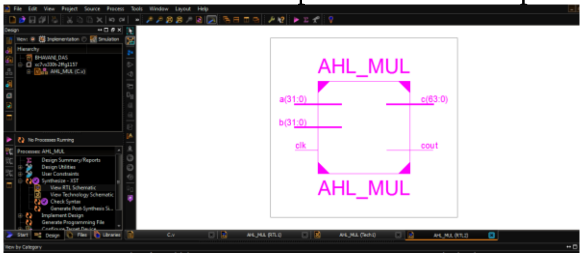

Fig. 9: RTL SCHEMATIC OF PROPOSED SYSTEM

In figure (10) the RTL schematic is shown. It is a combination of LUTs, K-Map, Equation, Truth table and buffers.

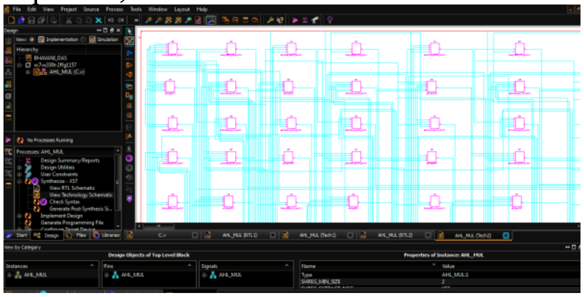

Fig. 10: TECHNOLOGY SCHEMATIC OF PROPOSED SYSTEM

The below figure (11) is the output waveform of the proposed system.

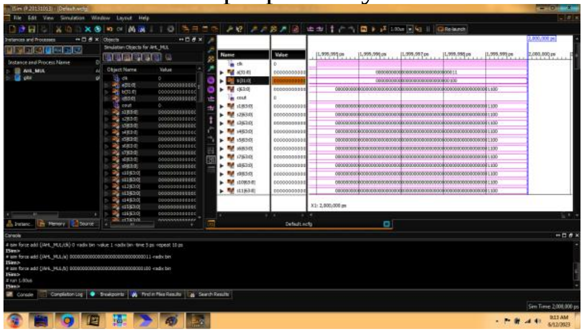

Fig. 11: OUTPUT WAVEFORM OF PROPOSED SYSTEM

Table. 1: COMPARISON OF PARAMETERS

S.NO	Parameters	Existed System	Proposed System
1	Total delay	110.363 ns	39.027 ns
2	Logic delay	60.608 ns	2.795 ns

3	Route delay	49.765 ns	36.232 ns

The below figure (12) shows the comparison of total delay.

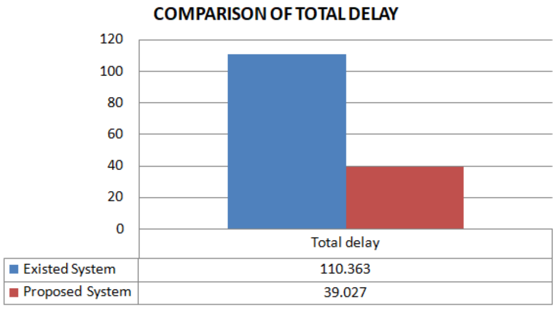

Fig. 12: COMPARISON OF TOTAL DELAY

The below figure (13) shows the comparison of logic delay.

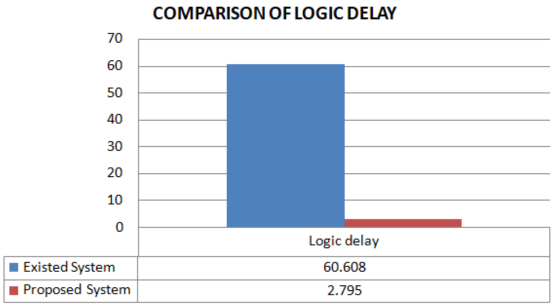

Fig. 13: COMPARISON OF LOGIC DELAY

The below figure (14) shows the comparison of route delay.

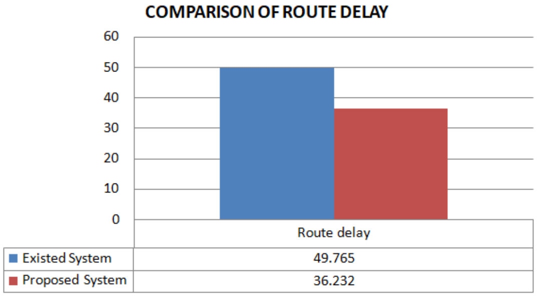

Fig. 14: COMPARISON OF ROUTE DELAY

VI. CONCLUSION

In this analysis, Design and implementation of fault free AHL multiplier circuit for cryptography applications is implemented. High speed and low power consumption are the significant goals in integrated circuits. The framework implementation is based on the multiplier design. The designs with AHL circuits have been proposed to mitigate the age impacts. AHL circuits are used to demonstrate the effects of transistor aging. Depending on Razor flip-flops and ADL, timing violations are mitigated. Fixed latency increases the clock cycle usage. So, this analysis decreases errors in an efficient manner.

VII. REFERENCES

[1] B. V. Mahesh and T. Srivasarao, "Performance Evaluation of FFT through Adaptive Hold Logic (AHL) Booth Multiplier," 2023 International Conference for Advancement in Technology (ICONAT), Goa, India, 2023, pp. 1-6, doi: 10.1109/ICONAT57137.2023.10080290.

[2] B. N. Vangapandu and A. Chalil, "FPGA Implementation of High-Performance Montgomery Modular Multiplication with Adaptive Hold Logic," 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2022, pp. 506-511, doi: 10.1109/ICCMC53470.2022.9754043.

[3] X. Wang, H. Wen and Y. Zhu, "Modeling and Simulation Test for Voltage Multiplier and an LLC Resonant Inverter as a Voltage Equalizer," 2019 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Macao, China, 2019, pp. 1-5, doi: 10.1109/APPEEC45492.2019.8994589.

[4] Y. G. Desale and V.V. Ingale, "Design of Power Efficient Bit Serial Finite Field GF(2m) Multiplier," 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), Bombay, India, 2019, pp. 1-4, doi: 10.1109/I2CT45611.2019.9033682.

[5] M. V. Archana and K. E. Suresh, "Reliable Multiplier Design with Adaptive Hold Logic for Aging Awareness," 2018 International Conference on Emerging Trends and Innovations In Engineering And

Technological Research (ICETIETR), Ernakulam, India, 2018, pp. 1-4, doi: 10.1109/ICETIETR.2018.8529121.

[6] P. Hosseinzadeh Namin, C. Roma, R. Muscedere and M. Ahmadi, "Efficient VLSI Implementation of a Sequential Finite Field Multiplier Using Reordered Normal Basis in Domino Logic," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 26, no. 11, pp. 2542-2552, Nov. 2018, doi: 10.1109/TVLSI.2018.2851958.

[7] G. Jain, M. Jain and G. Gupta, "Design of radix-4,16,32 approx booth multiplier using Error Tolerant Application," 2017 6th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2017, pp. 314-320, doi: 10.1109/ICRITO.2017.8342444.

[8] A. V. Aravind and S. Murugan, "VLSI design of 128 point finite field FFT multiplier," 2017 International Conference on Communication and Signal Processing (ICCSP), Chennai, India, 2017, pp. 0724-0727, doi: 10.1109/ICCSP.2017.8286456.

[9] S. Lakshmy, M. Vadivel and D. Upadhyay, "Performance analysis of aging-aware multiplier using various adders," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2016, pp. 2167-2170, doi: 10.1109/ICCSP.2016.7754565.

[10] P. K. Parveen and C. Priya, "Multiplier design using MTCMOS with adaptive hold logic," 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), Ramanathapuram, India, 2016, pp. 162-166, doi: 10.1109/ICACCCT.2016.7831621.

[11] V. S. Chirde and U. Jadhav, "Design of a multiplier with Adaptive Hold Logic (AHL) circuit to reduce aging effects," 2015 International Conference on Computer, Communication and Control (IC4), Indore, India, 2015, pp. 1-5, doi: 10.1109/IC4.2015.7375608.

[12] T. Pardhu and N. A. Reddy, "Design of ultra low power multipliers using hybrid adders," 2015 International Conference on Communications and Signal Processing (ICCSP), Melmaruvathur, India, 2015, pp. 0049-0054, doi: 10.1109/ICCSP.2015.7322536.

[13] I.C.Lin, Y.-H.Cho and Y.M.Yang, "Aging-Aware Reliable Multiplier Design With Adaptive Hold Logic," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 23, no. 3, pp. 544-556, March 2015, doi: 10.1109/TVLSI.2014.2311300.

[14] S. Murugeswari and S. K. Mohideen, "Design of area efficient and low power multipliers using multiplexer based full adder," Second International Conference on Current Trends In Engineering and Technology - ICCTET 2014, Coimbatore, India, 2014, pp. 388-392, doi: 10.1109/ICCTET.2014.6966322.

[15] Huapeng Wu, "Bit-parallel finite field multiplier and squarer using polynomial basis," in IEEE Transactions on Computers, vol. 51, no. 7, pp. 750-758, July 2012, doi: 10.1109/TC.2012.1017695.

[16]Jianing Su and Zhenghao Lu, "Parallel structure of GF (214) and GF (216) multipliers based on composite finite fields," 2011 9th IEEE International Conference on ASIC, Xiamen, 2011, pp. 768-771, doi: 10.1109/ASICON. 2011.6157318.

[17] Y. Ma, T. Endoh and T. Shibata, "A vertical-MOSFET-based digital core circuit for high-speed low-power vector matching," 2011 International SoC Design Conference, Jeju, Korea (South), 2011, pp. 203-206, doi: 10.1109/ISOCC.2011.6138745.

[18] Heiko Hinkelmann, Peter Zipf, Jia Li, Guifang Liu, Manfred Glesner, “On the design of reconfigurable multipliers for

integer and Galois field multiplication", Microprocessors and Microsystems, Volume 33, Issue 1, 2009, Pages 2-12, ISSN 0141-9331,https://doi.org/10.1016/j.micpro.2008. 08.003.

[19] A.Hosseinzadeh, H.Namin, Wu and M.Ahmadi, "A New Finite-Field Multiplier Using Redundant Representation," in IEEE Transactions on Computers, vol. 57, no. 5, pp. 716-720, May 2008, doi: 10.1109/TC.2007.70834.

[20] D.V.Poornaiah and P.V.A Mohan, "Design of a 3-bit Booth recoded novel VLSI concurrent multiplier-accumulator architecture," Proceedings of the 8th International Conference on VLSI Design, New Delhi, India, 1995, pp. 392-397, doi: 10.1109/ICVD.1995.512145.