High-Speed and Area-Efficient Novel Galois Field Multiplier Design for ECC Application

[1]S. Siddique, [2]S.Vijay

[1]M.Tech Scholar, Department of Electronics and Communication Engineering, Priyadarshini Institute of Technology and Management, Vatticherukuru Mandal, Guntur Dist., Andhra Pradesh, India.

[2]Assistant Professor, Department of Electronics and Communication Engineering, Priyadarshini Institute of Technology and Management, Vatticherukuru Mandal, Guntur Dist., Andhra Pradesh, India.

ABSTRACT: Due to rapid development in secured technological devices, the efficient implementation of a large field-size elliptic curve cryptosystem (ECC) is becoming demanding in many critical applications. In modern cryptographic systems, secure and efficient encryption is paramount. This paper presents High-Speed and Area-Efficient Novel Galois Field multiplier Design for ECC Application of a digital multiplier model capable of efficiently performing binary multiplication using a structured modular approach is described. This proposed system contains multiple functional blocks, including detection units, substitution boxes (S-Boxes), registers, a partial product generator, and an adder. The detection units identify the presence of 0's and 1's in both the multiplier and multiplicand to optimize computational effort. Registers are used for temporary data storage and synchronization during the S-Box performs logical transformations or bit encodings to simplify partial product formation. The partial product generator and adder subsequently produce the final product through systematic summation. This system enhances the efficiency, delay and speed of multiplication operations in digital systems, making it suitable for use in Elliptic Curve Cryptography applications.

Keywords: Galois Field (G.F), Multiplier, S-Box, Registers Elliptic Curve Cryptography (ECC) Algorithm

I. INTRODUCTION

Traditionally, the confidentiality provided by widely adopted public-key cryptosystems relies on the hardness of factoring large integers or computing discrete logarithms in a cyclic group. However, the recent advances in quantum computing pose a severe concern to the security of traditional public-key cryptographic schemes, since the employed computationally hard problems can be easily solved with a quantum computer[1]. As a consequence, the design Of quantum-computing resistant cryptographic primitives has gained importance lately, especially thanks to the U.S. National Institute of Standards and Technology (NIST) initiative, which aims at selecting a portfolio of primitives for standardization. In particular, the design of public-key cryptosystems that are resistant to attacks performed with quantum computers imposes a change in the underlying computationally hard problem.

The Internet of Things (IoT) provides the means to automate various processes in different fields of life. It is the first evolution of the internet [2]. Since its inception in the late nineties, IoT has expanded to engulf the entire earth, extending its horizons beyond it. The number of connected devices is growing day by day. The growth is exponential and will soon overtake the population on the earth[3].

Billions of smart devices, from servers to sensors, communicating amongst different platforms, present diverse sets of challenges such as interoperability of technologies, security & privacy, longevity & support, etc. [4]. These devices can be categorized into resource-rich, such as servers, tablets, etc., and resource-constrained, such as connected sensors, RFID tags, etc. As IoT devices are deployed openly to collect confidential data, they are easy targets for attackers and susceptible to many security attacks. All these circumstances make the cybersecurity of IoT devices a major challenge. The security requirements of IoT are classified into three operational levels. These are functional, information,

and access levels. Lightweight cryptography is considered the main security mechanism for IoT.

Cryptographic algorithms can be used to secure data from such threats. Symmetric and asymmetric algorithms are available for this purpose. Still, asymmetric algorithms can provide a base for multiple security services such as confidentiality, data integrity, availability, privacy, non-repudiation, authentication & authorization, etc. Among security standards, elliptic curve cryptography (ECC) is the first-choice asymmetric key cipher [5]. Numerous security protocols including BLE 4.2, 6LoWPAN, TLS, and CoAP, have employed ECC. The degree of security offered by ECC relies on the key sizes and the difficulty of the elliptic curve discrete logarithm problem (ECDLP). There isn't a known sub-exponential algorithm for figuring out ECDLP. Therefore, much smaller key sizes are needed to offer adequate security than other public key cryptosystems[6].

Crypto-processors are used to implement cryptographic algorithms in hardware. It helps accelerate the encryption, enhances tamper, provides key protection, and allows users true end-to-end encryption. Due to the vulnerable nature of the wireless channel, encryption parameters cannot be trusted with such communication [7]. It makes use of crypto-processors all the more necessary. ECC's elliptic curve scalar multiplication (ECSM) is expensive. With the advancement of technology, the size of sensors and other devices is becoming smaller. To accommodate these devices, the crypto-processor should also be made lightweight. The performance of ECCP can be improved by reducing the computation time for ECSM. This can be achieved by improving the underlying finite field multipliers and inversion algorithm[8].

Nowadays elliptic curve cryptography (ECC) based cryptographic systems are preferred over Rivest, Shamir, and Adleman (RSA) scheme due to much smaller key lengths which further translate into lower storage, bandwidth, and transmission cost. Different standardization bodies recommended 10-30× smaller key lengths for ECC as compared with RSA[9]. Elliptic curve point multiplication (ECPM) over a well-chosen elliptic curve (EC) is the primary operation and is also the main computational part of almost all ECC-based security protocols. Usually, it is done by combining point doubling (PD) and point addition (PA) group operations which further require low-level finite field (FF) arithmetic primitives such as finite field addition/subtraction (FFAS), finite field multiplication (FFM), and finite field inversion/division (FFID) [10]. Among these, FFID is the most time-critical operation and it is required if EC points are taken in affine coordinates (x,y) representation. However, fortunately, this FFID operation can be eliminated from EC group operations such as PD and PA using the projective coordinates representation at the cost of extra FFM operations. Therefore, in the projective space, FFM is the most time-critical operation which limits the execution performance of the ECC-based cryptographic processor[11].

Multiplication in Z2[x] conceptually works like long multiplication between integer numbers, except for the fact that the carry is always discarded instead of added to the more significant position[12]. This property derives from the fact that the addition in Z2 corresponds to the logical XOR. For this reason, the multiplication operation in Z2[x] is also commonly referred to as carry-less multiplication.

II. LITERATURE SURVEY

F. Haroon and H. Li. Et al.,[13] effective cryptographic solutions in Internet of

Things (IoT) applications has underscored the necessity for algorithms designed for resource-limited applications. IoT devices need optimized cryptographic solutions that strike a balance between strong security and computational efficiency due to their limited hardware capabilities, especially when dealing with large polynomial multiplication in cryptography. In this paper, a cost-efficient reconfigurable modular polynomial multiplier is proposed for general modulus polynomials.

Y. G. Desale and V.V. Ingale, et al.[14] presents the VLSI implementation of a Bit serial multiplier for multiplication in binary Finite Field GF(2m) and is based on Shift and Add algorithm. The polynomial base representation is used. The multiplier generates the result by shifting one of the multiplicand. Form bit inputs; it produces output after m-1 clock cycles. The value of m can vary up to 283 bits. Multiplier is designed using Verilog HDL. The designed Multiplier is simulated using NG Spice. The proposed design is synthesized in CADENCE Encounter. Using the low power VLSI methodology power consumption is reduced.

C. Yu and M. Ciesielski, et al.[15] presents a computer algebra technique that performs verification and reverse engineering of GF(2m) multipliers directly from the gate-level implementation. The approach is based on extracting a unique irreducible polynomial in a parallel fashion and proceeds in three steps: 1) determine the bit position of the output bits; 2) determine the bit position of the input bits; and 3) extract the irreducible polynomial used in the design. We demonstrate that this method is able to reverse engineer GF(2m) multipliers in m threads.

S. Ren, Q. -M. Cai, X. Cao, B. Luo, Y. Zhu and J. Fan, et al.[16] aiming at the problem of high computation complexity in the hardware implementation of the Galois Field (GF) multiplier in commonly used Reed-Solomon (RS) coding algorithms, a half-multiplier based on this matrix method is redesigned and the RS coding module is also optimized. The simulated results are provided to show that the hardware resource of using the designed encoder can decrease by about 15% than that of using the Xilinx official encoder, while the accuracy of the coding keeps the same level.

I. Kabin, Z. Dyka, D. Klann and P. Langendoerfer, et al.[17] introduce an accelerator for the ECC kP operation in two different types of Galois fields i.e. GF(p) and GF(2n). In order to ensure fast execution of the multiplication in both cases we integrated the carry bit separation technique to speed-up the multiplication in GF(p). The two most important contributions of this paper are that the partial multiplier applied is used for both types of Galois field and the second one is that our design is resistant against Horizontal Collision Correlation Analysis. The latter was verified in 20 test runs per supported elliptic curve.

V. D. R, D. Sharma, S. G. K. Reddy and M. Rao, et al.[18] presents two new approaches to realize three-operand multiplier architecture for Galois Field (2N) polynomial operations, referred to as Cascade and One-Shot Mixed mode configurations. A meta-heuristic approach enabled with a single-objective fitness run was employed to design optimal solutions in the form of non-homogeneous recursive sequences in Karatsuba multiplication, targeted for three-operand multiplication in Galois Field (GF). The proposed architectural designs offered improvement in compute-latency of 12.77% and footprint complexity of 61.97% with benefits in the area-delay product (ADP) of 70.72%, and power savings of 83.62% and 51.23% improvement in PPA compared to the existing state-of-the-art (SOTA) designs.

G. R. K. Reddy, S. G. K. Reddy, V. D R and M. Rao, et al.[19] introduce a novel technique referred to as M-term Non-Homogeneous Hybrid Overlap-free Karatsuba polynomial multiplier (MNHOKA), which surpasses existing state-of-the-art (SOTA) designs, including Karatsuba multiplier (KA), M-Term Karatsuba-like multiplier (MKA), Composite M-term Karatsuba-like multiplier (CMKA), and Overlap-free Karatsuba multiplier (OKA), across various operand sizes. In this paper, a detailed analysis of the proposed MNHOKA and its corresponding M-Term Non-homogeneous Hybrid Karatsuba Algorithm (MNHKA) is presented, highlighting its performance improvements on both Cadence 45 nm process and the ZYNQ ZCU-104 FPGA board for popular bit widths.

D. R. Vasanthi, S. Gopala Krishna Reddy and M. Rao, et al.,[20] introducing a novel hetero-blend recursive multiplier that harnesses the strengths of the contemporary state-of-the-art (SOTA) designs. The heterogeneous-blend recursive multiplier (HRM) adeptly merges the footprint efficiency of the Karatsuba multiplier (KM) and the compute-latency benefits of the overlap-free KM (OKM) at higher stages, while at lower bounds, it capitalizes the optimal balance of footprint and compute-latency benefits of the schoolbook multiplier (SBM). To further enhance the performance, HRM integrates the heterogeneous term division throughout its stages which is a characteristic find taken from the prior work on M-term nonhomogeneous Karatsuba multiplier (MNHKA).

J. Xie, C. -Y. Lee, P. K. Meher and Z. -H. Mao, et al.[21] propose novel bit-parallel and digit-serial finite field multipliers over GF(2m) based on RNB. By efficient transformation of the core multiplication algorithm using a unique circular shifting feature, we have derived an efficient algorithm for low-complexity systolic mapping. Both bit-parallel and digit-serial structures of the multipliers are then obtained and optimized to enhance the area-time efficiency. We have also utilized the unique feature of the proposed multiplication algorithm to obtain the systolic multipliers by Karatsubalike decomposition. Detailed analysis and comparison show the superior performance of the proposed implementation.

R. Amiri and O. Elkeelany, et al. [22] propose and develop a concurrent reconfigurable cryptosystem to encrypt and decrypt stream of data using ECC on FPGA. First, we present hardware design and implementation to map a plain message on the elliptic curve based on isomorphic transformation, then second, we architect the elliptic curve ElGamal public-key encryption method by using point addition and multiplication on Koblitz elliptic curve on FPGA. Our proposed cryptosystem is synthesized and implemented on Intel Cyclone 10 GX and Xilinx Kintex-7 FPGAs to evaluate throughput, and it achieves 25.73-57.1 Mbps.

A. A. Asaker, Z. F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran and F. E. Abd El-Samie, et al.[23] presents a novel high-security iris recognition system using elliptic curve cryptography. In this system, the original IrisCode is partitioned out into binary-shards then every binary-shard is represented by a point over the elliptic curve and encrypted via elliptic curve cryptography. As a result, the protected IrisCodes can be stored and transmitted from the local iris readers to the centralized server as well as between various servers more securely. The proposed iris recognition system is evaluated using CASIA-IrisV3 database in terms of accuracy, security, and privacy.

Y. Genç and E. Afacan, et al.[24] propose a new message encryption algorithm using an elliptic curve over finite fields. This new method converts each character of the message to its hexadecimal Unicode value and then separates the value divided into blocks that contain one character. Unicode contains many more characters than ASCII. In the Unicode table, the hexadecimal values of the characters range from one to six digits. The proposed new encryption algorithm can encrypt not just by using the values in the ASCII table but all values in the Unicode table, thus can use different alphabets and characters.

T. Gu, K. Lim, G. H. Choi and X. Wang, et al.[25] Lidar information based authentication scheme was proposed to authenticate vehicles locally without the involvement of a trusted authority and infrastructures. However, their scheme used the real identity of vehicles for communication which may lead to identity privacy threats. In this paper, we propose a Lidar information-based scheme using Elliptic Curve Cryptosystem (ECC). This new scheme generates anonymous identities or pseudonyms for each vehicle for communication.

III. FRAMEWORK OF HIGH-SPEED AND AREA-EFFICIENT NOVEL GALOIS FIELD MULTIPLIER DESIGN FOR ECC APPLICATION

In this section framework of high-speed and area-efficient novel Galois Field multiplier design for ECC application is observed. The block diagram shows proposed ECC encryption process. The given block diagram represents a digital multiplier architecture that performs multiplication between two binary inputs the multiplier and the multiplicand. The process begins with both inputs being fed into their respective detection units that identify the positions of 0's and 1's in each binary number. The purpose of this detection stage is to control further processing steps and eliminate unnecessary computations when a bit is zero. After detection, the outputs are temporarily stored in registers, which hold the processed data and ensure proper synchronization with the system clock during computation.

The data from the registers is then passed to the S-Box (Substitution Box), which performs logical transformations or encoding operations on the input bits. The S-Box may be used to substitute bit patterns, optimize signal transitions, or perform modified Booth encoding to reduce the number of partial products, thereby improving speed and efficiency.

After transformation, both the multiplier and multiplicand are input to the partial product generator, which produces all the intermediate products based on the multiplier bits. Each '1' in the multiplier corresponds to the multiplicand being added (with appropriate bit shifting). These partial products are then sent to the adder, which combines them into a single final result. The adder may use techniques like carry-save addition or array addition to enhance performance. The final output from the adder is the product, representing the multiplication result of the two binary inputs.

It is a non- linear substitution byte. Each Byte is replaced by another byte. This substitution Byte uses S-BOX for generating the cipher text. This S-box involves two process. First one is used to take the multiplicative inverse of finite field of the matrix (i.e input data). Secondly, the Affine Transformation is applied to the output of multiplicative inverse. Area reduction is possible in this finite field and finite field is used to create a compact field AES implementation. In new technology, the S-Box can be obtained from its truth table by using two level logic such as sum of products and product of sum.

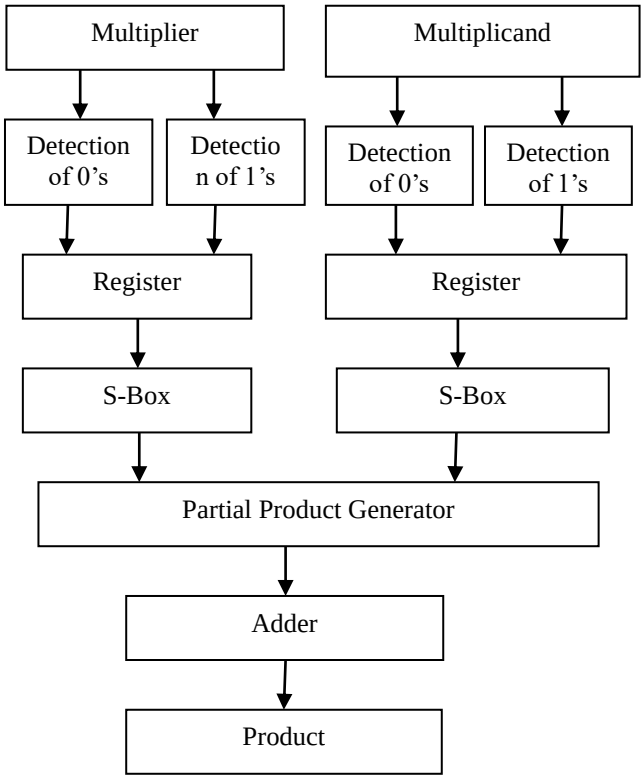

Figure.1: Framework of High-Speed and Area-Efficient Novel Galois Field Multiplier Design for ECC Application

A Galois field multiplier is a specialized multiplier that performs multiplication operations within a Galois field (GF), a finite field used in various applications like cryptography, error correction, and coding theory. A Galois field, also known as a finite field, is a mathematical structure consisting of a finite set of elements along with operations like addition, subtraction, multiplication, and division.

In the world of digital circuits, registers play a vital role in data storage and temporary memory. In this section, we will explore the concept of registers and their significance in modern electronics. Registers serve as small, high-speed storage components within a circuit, allowing for the temporary storage of data during the execution of various operations. Registers act as small, fast memory units that can store binary data in the form of bits. They are typically constructed using flip-flops, which are fundamental building blocks of digital circuits. Unlike the main memory in a computer system, registers provide faster access to data since their proximity to the processor reduces data transfer time. Registers serve as temporary storage for data that is being processed or transferred within a circuit. The data stored in registers can be manipulated, modified, or transferred to other registers as required by the circuit's design and functionality. These temporary memory banks ensure the smooth flow of data within a digital circuit, facilitating efficient data processing.

In VLSI (Very Large-Scale Integration), an adder is a fundamental digital circuit that performs arithmetic addition on binary numbers. It takes two or more binary inputs and produces a sum output and, typically, a carry output, using logic gates to implement the addition operation. Key types include the simple Half Adder (two inputs, sum and carry) and the more common Full Adder (three inputs, including a carry-in, to produce sum and carry-out). VLSI designers use various adder architectures, such as Ripple Carry Adders, Carry Look-Ahead Adders, and Carry Select Adders, to optimize for speed, area, and power consumption.

In the context of Very Large Scale Integration (VLSI), a "product" is a fabricated integrated circuit (IC) or microchip that is the result of the VLSI design and manufacturing process. These complex chips are designed to perform specific functions and are the core components of modern electronic devices.

IV. RESULT ANALYSIS

In this section, result analysis of High-Speed and Area-Efficient Novel Galois Field multiplier Design for ECC Application is observed.

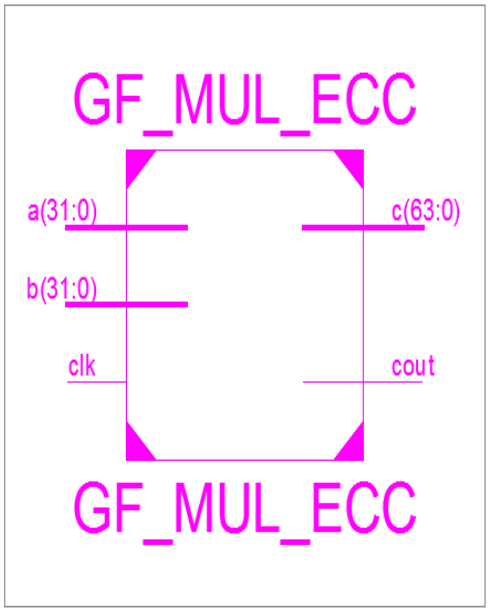

Figure.2: RTL Schematic

An RTL (Register Transfer Level) schematic visually represents the flow of data between registers in a digital circuit, illustrating how data is transformed and passed between them through combinational logic, crucial for verifying functionality before detailed design.

Technology schematics are architecture-specific designs that use technology-specific/ target FPGA specific components like LUTs, carry logic, I/O buffers, and other technology-specific components.

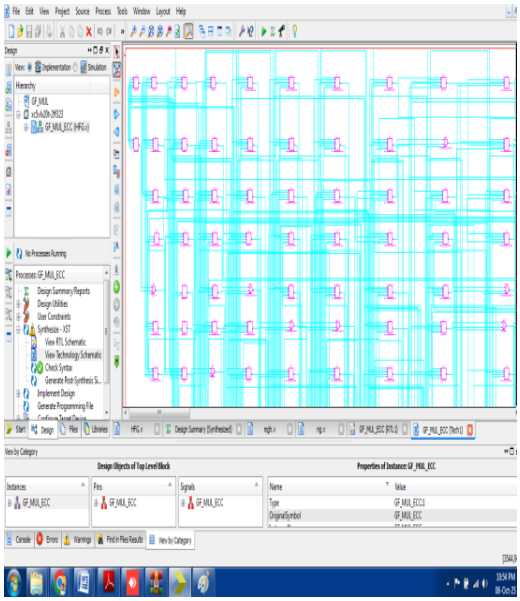

Figure.3: Technology Schematic

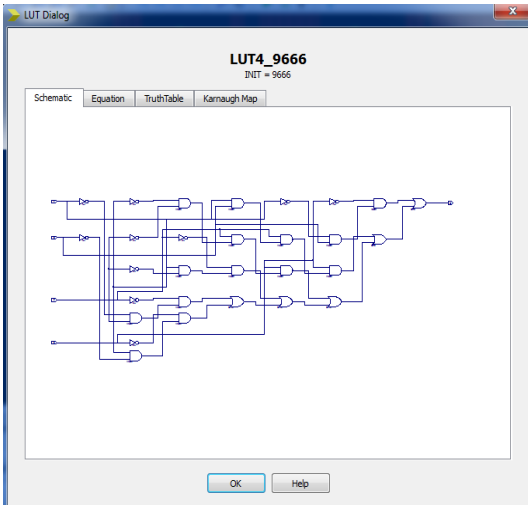

Figure.4: LUT

In Very Large Scale Integration (VLSI) circuits, especially in Field-Programmable Gate Arrays (FPGAs), Lookup Tables (LUTs) are fundamental building blocks used to implement combinational logic. LUTs essentially function as programmable truth tables, where the output value for a given combination of inputs is stored in a memory cell.

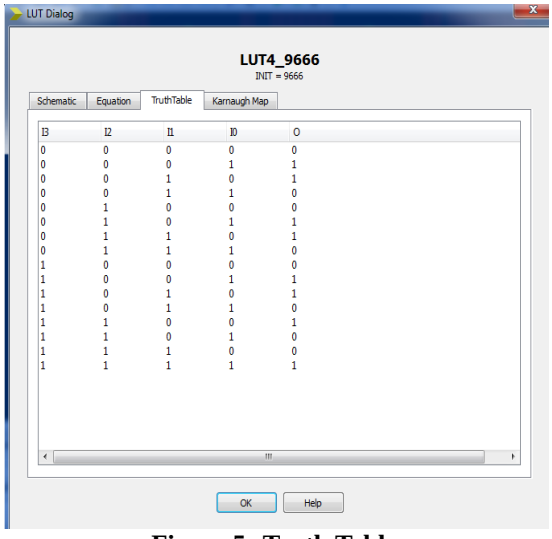

Figure.5: Truth Table

Karnaugh map (K-map), also known as a Veitch diagram, is a powerful tool used in digital logic design to simplify Boolean expressions and minimize logic circuits. It offers a visual representation of Boolean functions, aiding in the optimization of circuits by reducing the number of gates required.

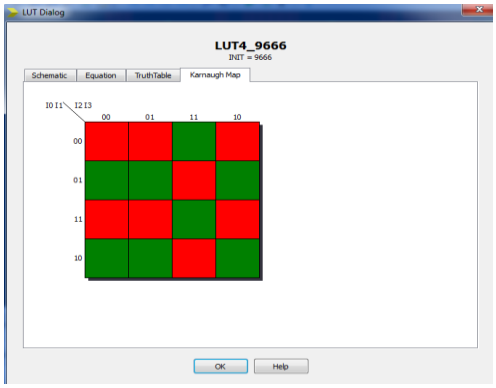

Figure.6: K Map

An output waveform is the shape of a signal (such as voltage or current) produced by a circuit or device, often visualized as a graphical representation of the signal over time. It can take a variety of shapes, including sine waves, square waves, and more complex patterns, depending on the characteristics of the input signal and the device.

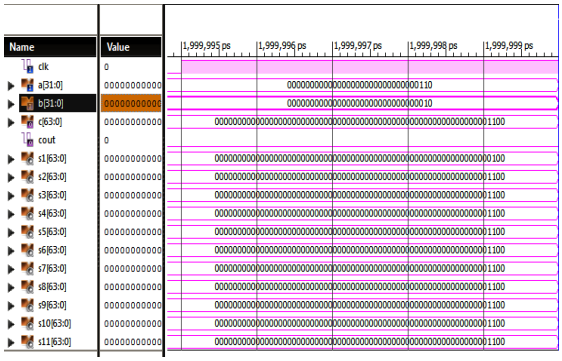

Figure.7: Output Waveform

Table:1 Performance Comparison

Parameters	Total Delay	Logic Delay	Route Delay	Memory Used
Existing System	73.259ns	18.524ns	54.735ns	584624kb
Proposed System	56.862ns	9.502 ns	47.360ns	400248kb

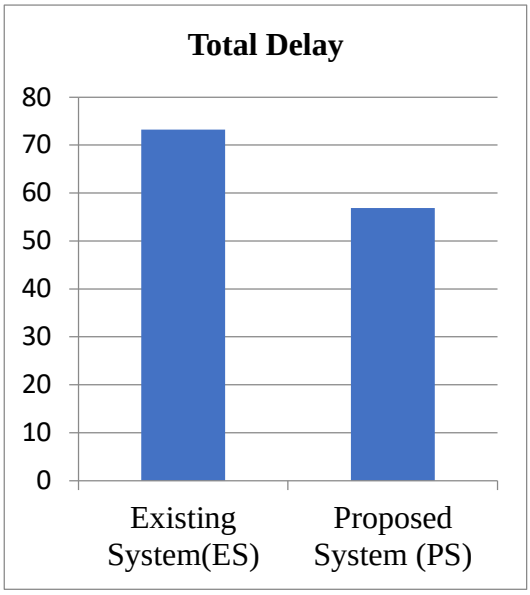

Figure.8: Total Delay Graph

In Figure 8, total delay comparison graph is observed between existing system and proposed system. The proposed system shows low total delay when compared with existing system.

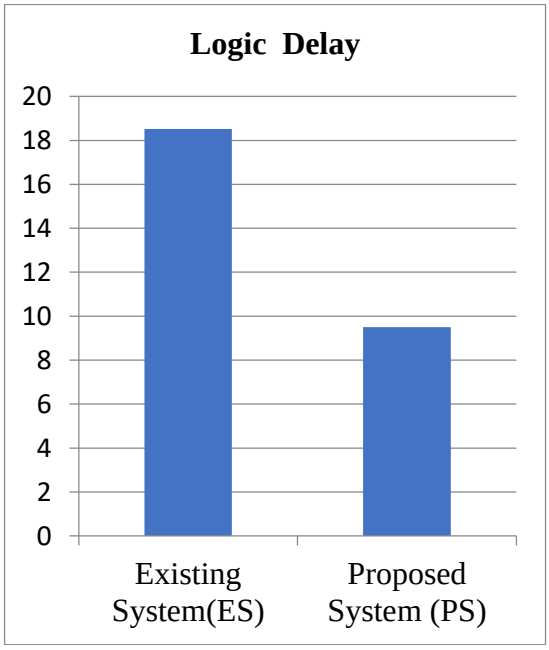

Figure.9: logic Delay Graph

Logic delay used comparison graph is observed in Figure 9, between existing system and proposed system. The proposed system shows low logic delay when compared with existing system.

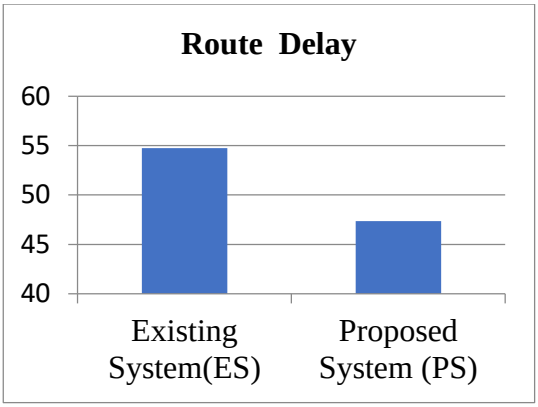

Figure.10: Route Delay Graph

In Figure 10, route delay comparison graph is observed between existing system and proposed system. The proposed system shows low route delay when compared with existing system.

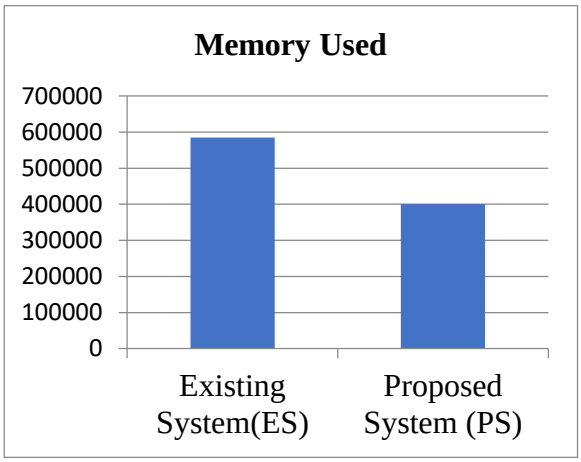

Figure.11: Memory Used Comparison Graph

Memory usage in the system is compared by using comparison graph which is observed in Figure 11, between existing system and proposed system. The proposed system shows low memory usage when compared with existing system.

V. CONCLUSION

The Internet of Things (IoT) is connecting the world in a way humanity has never seen before. With applications in healthcare, agricultural, transportation, and more, IoT devices help in bridging the gap between the physical and the virtual worlds. These devices usually carry sensitive data which requires security and protection in transit and rest. The designed digital multiplier architecture successfully demonstrates an organized and efficient method for binary multiplication. By integrating detection, register, and S-Box stages prior to partial product generation, redundant computations are minimized, and processing speed is enhanced. The modular structure ensures better adaptability and scalability for various bit-width operations. Furthermore, the S-Box is used for encoding contributes to reduced hardware complexity and enhanced performance compared to existing multiplier designs. Overall, this model provides an optimized solution for implementing high-speed and low-power multiplication in modern digital and embedded systems.

VI. REFERENCES

[1] H. Inumarty and M. A. Basiri M., "Reconfigurable Hardware Design for Polynomial Galois Field Arithmetic Operations," *2020 24th International Symposium on VLSI Design and Test (VDAT)*, Bhubaneswar, India, 2020, pp. 1-5, doi: 10.1109/VDAT50263.2020.9190485.

[2] X. Wu, C. Wei, Y. Li and X. Huang, "An Efficient Overlap-Free Karatsuba Finite-Field Multiplier on FPGA," *2024 3rd International Conference on Electronics and Information Technology (EIT)*, Chengdu, China, 2024, pp. 218-222, doi: 10.1109/EIT63098.2024.10762429.

[3] I. Zholubak and V. Hlukhov, "Validation of Multipliers for Elements of Extended Galois Fields GF(pn) and Multipliers VHDL-descriptions Generator," *2023 IEEE 18th International Conference on Computer Science and Information Technologies (CSIT)*, Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/CSIT61576.2023.10324200.

[4] R. C. S. A, S. E. P. Pushpa, M. K, S. S and V. P, "Area Optimized Implementation of Galois Field Fourier Transform," *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, Erode, India, 2022, pp.

736-743, doi: 10.1109/ICSCDS53736.2022.9761047.
[5] D. Pradhan, B. K. Meher and P. K. Meher, "Digit-Size Selection for FPGA Implementation of Generic Digit-Serial Multiplication Over GF(2m)," *2023 1st International Conference on Circuits, Power and Intelligent Systems (CCPIS)*, Bhubaneswar, India, 2023, pp. 1-6, doi: 10.1109/CCPIS59145.2023.10291975.
[6] G. Yang, F. Kong and Q. Xu, "Optimized FPGA Implementation of Elliptic Curve Cryptosystem over Prime Fields," *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 2020, pp. 243-249, doi: 10.1109/TrustCom50675.2020.00043.
[7] A. Yadav, P. Sharma and Y. Gigras, "A Comparative Study of Elliptic curve and Hyperelliptic Curve Cryptography Methods and an Overview of Their Applications," *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurugram, India, 2024, pp. 01-06, doi: 10.1109/ISCS61804.2024.10581015.
[8] P. More, S. Sakhare and P. Sawane, "Implementation and Analysis of ECC (Elliptic Curve Cryptography) Security Routing Protocol in NS2," *2023 3rd Asian Conference on Innovation in Technology (ASIANCON)*, Ravet IN, India, 2023, pp. 1-5, doi: 10.1109/ASIANCON58793.2023.10270716.
[9] M. Bedoui, B. Bouallegue, B. Hamdi and M. Machhout, "An Efficient Fault Detection Method for Elliptic Curve Scalar Multiplication Montgomery Algorithm," *2019 IEEE International Conference on Design & Test of Integrated Micro & Nano-Systems (DTS)*, Gammarth, Tunisia, 2019, pp. 1-5, doi: 10.1109/DTSS.2019.8914743.
[10] V. Kumar, J. P. Singh, D. Ghosh and A. Kumar, "A Comprehensive Review and Analysis of Two-Way Authentication and Novel Elliptic Curve-Based Encryption," *2024 International Conference on Emerging Systems and Intelligent Computing (ESIC)*, Bhubaneswar, India, 2024, pp. 718-721, doi: 10.1109/ESIC60604.2024.10481613.
[11] K. Banerjee, J. Kaur and N. Tiwari, "Torsion Point Cryptography: Enhancing Data Security with Elliptic Curves," *2023 IEEE International Carnahan Conference on Security Technology (ICCST)*, Pune, India, 2023, pp. 1-6, doi: 10.1109/ICCST59048.2023.10474229.
[12] M. S. Khan, T. M. Chen, M. Sathiyanarayanan, M. Mujeerulla and S. P. Raja, "Application of Lenstra-Lenstra-Lovasz on Elliptic Curve Cryptosystem Using IOT Sensor Nodes," in *Journal of ICT Standardization*, vol. 12, no. 4, pp. 381-407, December 2024, doi: 10.13052/jicts2245-800X.1242.
[13] F. Haroon and H. Li, "Reconfigurable and Compact Modular Polynomial Multiplier in Galois Field for the Security of IoT," *2025 IEEE Cloud Summit*, Washington, DC, USA, 2025, pp. 189-192, doi: 10.1109/Cloud-Summit64795.2025.00037.
[14] 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.
[15] C. Yu and M. Ciesielski, "Formal Analysis of Galois Field Arithmetic Circuits-Parallel Verification and Reverse Engineering," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 38, no. 2, pp. 354-365, Feb. 2019, doi: 10.1109/TCAD.2018.2808457
[16] S. Ren, Q. -M. Cai, X. Cao, B. Luo, Y. Zhu and J. Fan, "Design of High Performance Reed-Solomon Encoder Based on A Novel Half-multiplier," *2022 International Applied Computational Electromagnetics Society Symposium (ACES-China)*, Xuzhou, China, 2022, pp.

1-2, doi: 10.1109/ACES-China56081.2022.10065001.
[17] I. Kabin, Z. Dyka, D. Klann and P. Langendoerfer, "Fast and Secure Unified Field Multiplier for ECC Based on the 4-Segment Karatsuba Multiplication," *2019 IEEE East-West Design & Test Symposium (EWDTS)*, Batumi, Georgia, 2019, pp. 1-6, doi: 10.1109/EWDTS.2019.8884393.
[18] V. D. R, D. Sharma, S. G. K. Reddy and M. Rao, "Design of Cascade and One-Shot Mixed-Mode Recursive Multipliers for GF(2N) Polynomials," *2025 IEEE International Symposium on Circuits and Systems (ISCAS)*, London, United Kingdom, 2025, pp. 1-5, doi: 10.1109/ISCAS56072.2025.11043771.
[19] G. R. K. Reddy, S. G. K. Reddy, V. D R and M. Rao, "MNHOKA - PPA Efficient M-Term Non-Homogeneous Hybrid Overlap-free Karatsuba Multiplier for GF (2n) Polynomial Multiplier," *2023 IEEE 41st International Conference on Computer Design (ICCD)*, Washington, DC, USA, 2023, pp. 38-45, doi: 10.1109/ICCD58817.2023.00016.
[20] D. R. Vasanthi, S. Gopala Krishna Reddy and M. Rao, "HRM: M-Term Heterogeneous Hybrid Blend Recursive Multiplier for GF(2n) Polynomial," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 32, no. 8, pp. 1447-1460, Aug. 2024, doi: 10.1109/TVLSI.2024.3393860
[21] J. Xie, C. -Y. Lee, P. K. Meher and Z. -H. Mao, "Novel Bit-Parallel and Digit-Serial Systolic Finite Field Multipliers Over GF(2m) Based on Reordered Normal Basis," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 9, pp. 2119-2130, Sept. 2019, doi: 10.1109/TVLSI.2019.2918836.
[22] R. Amiri and O. Elkeelany, "FPGA Design of Elliptic Curve Cryptosystem (ECC) for Isomorphic Transformation and EC ElGamal Encryption," in *IEEE Embedded Systems Letters*, vol. 13, no. 2, pp. 65-68, June 2021, doi: 10.1109/LES.2020.3003978.
[23] A. A. Asaker, Z. F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran and F. E. Abd El-Samie, "A Novel Iris Cryptosystem Using Elliptic Curve Cryptography," *2021 9th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC)*, Alexandria, Egypt, 2021, pp. 155-158, doi: 10.1109/JAC-ECC54461.2021.9691307.
[24] Y. Genç and E. Afacan, "Implementation of New Message Encryption using Elliptic Curve Cryptography Over Finite Fields," *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, Taiz, Yemen, 2021, pp. 1-6, doi: 10.1109/ICOTEN52080.2021.9493519.
[25] T. Gu, K. Lim, G. H. Choi and X. Wang, "A Lidar Information-based Privacy-Preserving Authentication Scheme Using Elliptic Curve Cryptosystem in VANETs," *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA, 2022, pp. 525-526, doi: 10.1109/CCNC49033.2022.9700693.