International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 / https://doi.org/10.14445/22315381/IJETT-V70I8P234

Volume 70 Issue 8, 327-335, August 2022

Original Article

Design and Implementation of Effective Elliptic Curve Cryptography Accelerator using Hardware/Software Co-Design on Zynq Board

Kirit V. Patel[1], Mihir V. Shah[2], Pankaj P. Prajapati[3], Anil J. Kshatriya[4]

[1,2,3,4]*Department of Electronics and Communication, L. D. College of Eng., Gujarat Technological University, Ahmedabad, Gujarat, India*

[1]kirit@ldce.ac.in

Received: 25 May 2022 Revised: 02 August 2022 Accepted: 13 August 2022 Published: 27 August 2022

Abstract - *Today, billions of transactions share confidential information in the digital world of IoT (Internet of Things). The security of sharing confidential information has become a crucial issue in the open-ended network. ECC provides the best solution for higher security with less utilization of resources, and now ECC has become the worldwide acceptable solution for confidential data sharing. To achieve the best trade-off between scalability, flexibility, area consumption, and timing execution with main attention to achieve the best performance. The point addition and double point instructions for Point multiplication calculation in the Montgomery algorithm have been restructured to reduce the required clock cycles. This paper presents the design of an area and speed-improved Elliptic Curve Cryptography (ECC) co-processor accelerator with excellent performance. It is implemented on Zynq board 7000, which allows the hardware-software co-design. The simulation is carried out on the Xilinx Vivado platform. The accelerator can relieve the main processor of cryptography tasks, allowing the SoC to share confidential information on the Internet safely. The suggested cryptographic co-processor outperforms other hardware implementations.*

Keywords - *Field Programmable Gate Array, Galois Field (GF), Elliptic Curve Scalar Multiplication, National Institute of Standards and Technology, HW/SW- Hardware-Software, SoC (System On Chip).*

1. Introduction

Cryptography is classified into symmetric key cryptography and asymmetric cryptography based on the key used for encryption and decryption. The elliptic curve cryptography is asymmetric cryptography, also known as public-key cryptography and allows the use of two different keys for the encryption and decryption process. The public-key cryptography allows secure transactions, key agreements, and digital signatures over open-ended networks while maintaining data integrity. The most widely utilized approach is elliptic curve cryptography (ECC) [1]. In Internet-of-Things (IoT) applications such as health care, defense, banking, and the automobile industry, ECC has become more appealing. Because its hardware resources are ideal for financial services, smart homes, smart retail, and confidential systems [2], the ECC implementation requires high-performance criteria such as processing operations, power, and hardware must be optimized [3].

The basic flow of ECC is shown in fig. 1. On the transmitter side, the user's message is encrypted using the public key and generates the ECC ciphertext. The sender will generate the private key using the elliptic curve operation, and this private is used on the receiver side to decrypt the ciphertext and generate the original message [4].

Based on hardware computation, the ECC method can be divided into four levels of processing. The first layer computes finite field arithmetic operations such as subtraction, addition, squaring, multiplication, and inversion. Point doubling and point addition processes make up the second layer. The most computationally essential aspect of the ECC is scalar point multiplication, executed at the third layer. The encryption and decryption procedures are implemented at the architecture's fourth layer. All four layers decide the performance of the ECC system and can be designed differently to achieve the best results [5].

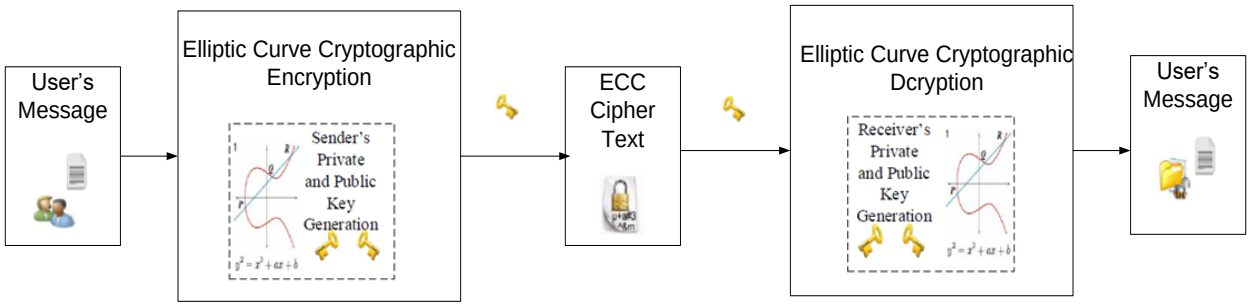

Fig. 1 Flow of ECC

The Edwards curve is a family of elliptic curves proposed by Harold Edwards. It supports Fast group operations and High immunity to side-channel attacks (SCAs). [6] The Twisted Edwards curve is a generalization of an Edwards curve defined in Eq. (1).

$$E : ax^2 + y^2 = 1 + dx^2 y^2 \qquad (1)$$

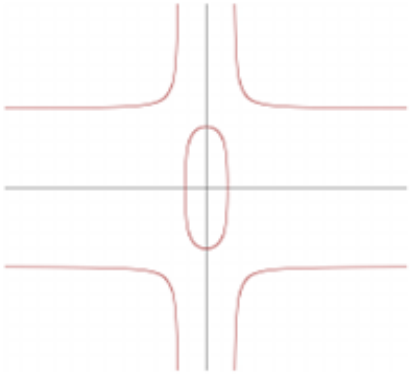

Fig. 2. Twisted Edward Curve[6]

Elliptic curve implementation using Twisted Edwards curve consumes less cost of cryptography point operation than Weierstrass Equation. The basic curve style is shown in fig. 2.

2. Literature Survey

Kalaiarasi M et al. [7] proposed a modified parallel algorithm in the reconversion yields with lesser time and clock cycle NIST supporting GF(2^{233}). The proposed architecture has been implemented on Xilinx Virtex-7 and Virtex-6 FPGA devices. Results achieved a lesser delay of 8.22 and 20.025µs and 956 clock cycles. Two multiplications operations are abridged using the reconstruction process 27.21% and 18.29% increase in time-area performance in Virtex-7 and Virtex-4 devices.

B.Panjwani [8] proposed a point-multiplication architecture based on the modified Montgomery-ladder algorithm for irreducible polynomials. To improve the computation speed, the modified Itoh–Tsujii algorithm was used for the finite field operation of point multiplication. Paper presented that the proposed architecture achieved time-are efficiency of about 42%–98% and 17%–86% over GF(2^{233}) and GF(2^{163}), respectively. Proposed a lightweight cryptographic core on a System-on-Chip (SoC), including authentication protocol and a key exchange protocol for low-cost devices using the resource sharing options. The design was simulated using 130nm technology using the HDL language. [9]

The enhanced architecture of the Montgomery Modular Multiplier has been proposed to improve the performance and reduce the area cost. They have designed 256-bit, and 1024-bit modular multipliers and the proposed design was synthesized on the Virtex-6 FPGA and implemented on the Nexys-3 board. The design utilized 1104 and 4450 LUTs, 143.82 and 49 MHz, and execution times of 1.79 µs and 20.53 µs, respectively. [10] Luis Parrilla et al. proposed a co-processor for Elliptic Curve Cryptography operations and implemented it on the hardware. This co-processor accelerates secure services and can be implemented in recent FPGA generations, a cryptographic co-processor to coexist on the same chip.[11] Proposed a high-performance Ed25519 architecture applicable for a higher security level. The proposed architecture gives about 21 times the speed with more than 6200 digital signature algorithms per second. The design was also implemented on Xilinx Zynq-7020 FPGA, improving the utilized area × time product. [12]

Panjwani presented a hardware-software co-design for the scalable hardware implementation over NIST recommended field sizes up to 521 bit. [13] Luis Parrilla et al. [14] proposed an ECC co-processor and achieved low area optimization. When implemented in Zynq devices, the developed design uses less than 3500 LUTs, while performing ECC scalar-point operation at around 400us at 50MHZ [14]. Philipp Koppermann et al. [15] proposed low latency hardware over a Curve25519. A variable-based Curve25519 scalar multiplication takes 13,639 cycles and may run at 115 MHz on Xilinx Zynq 7030 FPGA devices. The design enables the computation of a key in less than 120 seconds, FPGA-based Curve25519 implementations by a factor of 2.8 while consuming 24% less memory requirement.

Because point multiplication (PM) is the most complex and well operation in ECC, most published material focuses on increasing PM, and overall ECC performance can be improved [16]. A modular multiplier based on addition operation with the concept of Multi-Bit Scanning over the Galois field 576-bit [17]. A point multiplier that supports a binary field with a reconfigurable secure key with various prime field sizes of NIST recommended Galois Field. [18] The architecture uses the Twisted Edwards curve over a prime field. When compared to 5P using the Weierstrass curve with point addition, Edwards curve with points addition and doubling, and Edwards curve with computable and point addition methods, the proposed method saved 3.2 million, 7.2 million, and 4.2 million dollars, saving 17.2%, 31.9 %, and 21.4 %, respectively.[19]

3. Implementation of Proposed Design

The scalar point multiplication is the dominant function in elliptic curve cryptography which decides the performance of the ECC system in terms of area, speed, and complexity. In the Montgomery algorithm, the point addition (PA) and point double (PD) instructions for Point Multiplication calculation have been reorganized to reduce the overall set of required clock cycles. The restructured operations are described in the algorithm and implement architecture as shown in fig. 3.

Algorithm 1. Restructured PA and PD for Montgomery Algorithm

Algorithm: Montgomery Algorithm for Elliptic Curve Operation

Input : $P=(x_p, y_p) \in GF(2^m)$, $k= k_0, k_1 \ldots k_{n-1}$

Output: $Q(x_q, y_q)$

Step 1: Affine to Projective Conversion

$X_1 = x_p$, $Z_1 = 1$, $X_2 = x_p^2+b$, $Z_2= x_p^4$

Step 2: Elliptic Curve Group Operation

For(i from n-2 down to 0) do

If $k_i = 1$ then

Point Addition → P= P+Q

PA – Stage1 → $Z_1= X_2 \times Z_1^2$, PA – Stage2 → $X_1= X_1 \times Z_2$, PA – Stage3 → $T= X_1 \times Z_1$

PA – Stage4 → $X_1= X_1 \times Z_1$, PA – Stage5 → $Z_1=T^2$, PA – Stage6 → $T= x_p \times Z_1$

PA – Stage7 → $X_1= X_1 + T$

Return :$P(X_1,Z_1)$

Point Double → P= P+P

PD- Stage1→ $Z_2= Z_2^2$, PD- Stage2→ $T= Z_2^2$, PD-Stage3→ T= b x T

PD- Stage4→ $X_2= X_2^2$, PD- Stage5→ $Z_2= X_2 \times Z_2$, PD- Stage6 → $X_2= X_2^2$

PD- Stage7→$X_2 = X_2 +T$

Return :$Q(X_2,Z_2)$

else

Point Addition → P= P+Q

PA – Stage1 → $Z_2= X_1 \times Z_2$, PA – Stage2 → $X_2= X_2 \times Z_1$, PA – Stage3 → $T= X_2 \times Z_2$

PA – Stage4 → $X_2= X_2 \times Z_2$, PA – Stage5 → $Z_2=T^2$, PA – Stage6 → $T= x_p \times Z_2$

PA – Stage7 → $X_2= X_2 + T$

Return :$P(X_2,Z_2)$

Point Double → P= P+P

PD- Stage1→ $Z_1= Z_1^2$, PD- Stage2→ $T= Z_1^2$, PD-Stage3→ T= b x T

PD- Stage4→ $X_1= X_1^2$, PD- Stage5→ $Z_1= X_1 \times Z_1$, PD- Stage6 → $X_1= X_1^2$

PD- Stage7→$X_1 = X_1 +T$

Return :$Q(X_1,Z_1)$

End for.

Step 3: Reconversion

The PA and PD operations need 14 instruction stages, with 7 instructions used for each PA and PD operation. Six of the total instructions are used for modular multiplication, five for modular squaring, and the remaining three for modular addition. These restructured PA and PD operations improve the speed of Elliptic Curve point operation and reduce the execution time means improving the encryption and decryption process speed in cryptography. Restructured group operations architecture is shown in fig. 3. All the operations are classified into six stages. Two-point multiplication runs parallel with different stages of PA and PD operation.

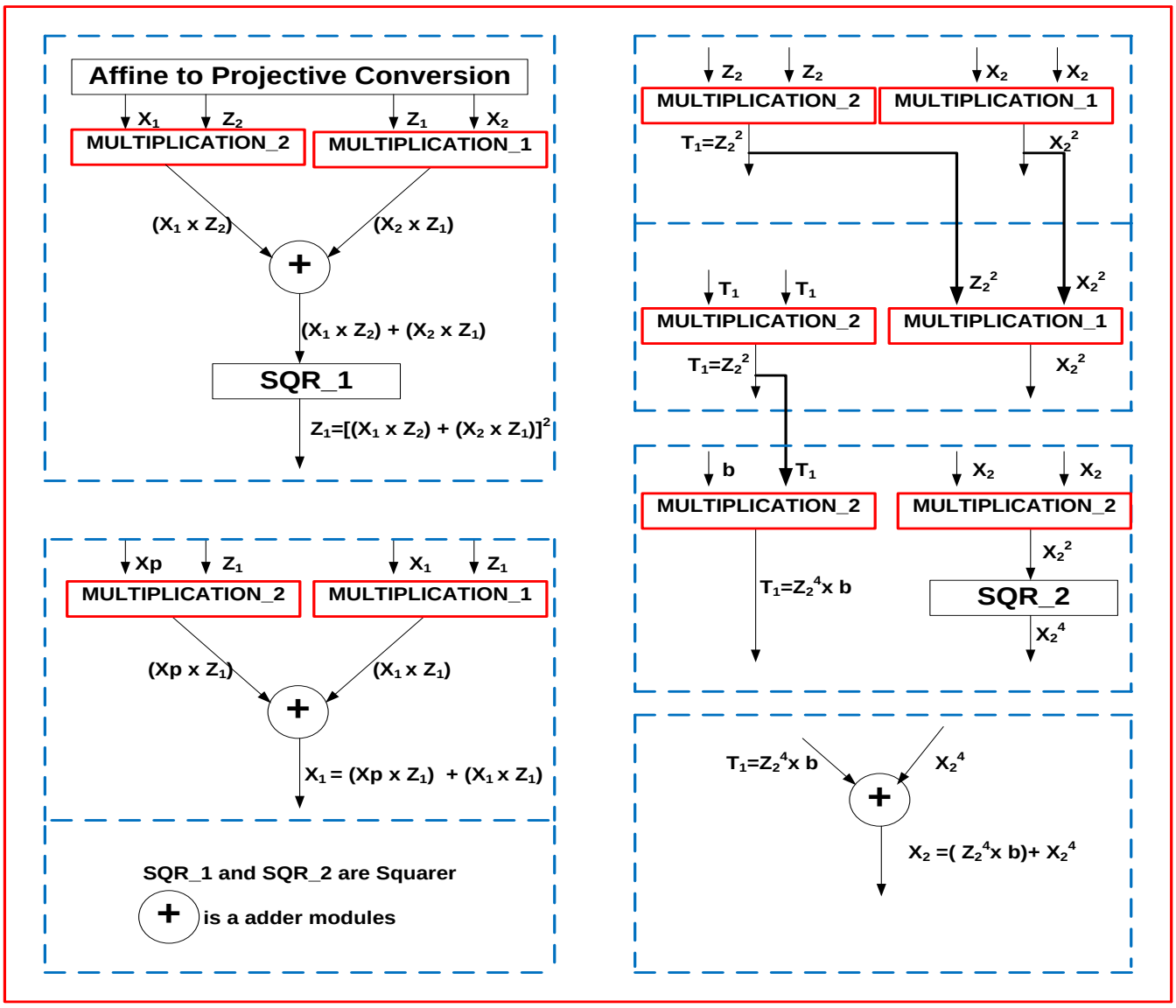

Fig. 3 Architecture of PA and PD Group Operations

The performance of the ECC system depends on the different modules such as modular multiplication, point addition/subtraction, scalar multiplication and key generation module. Each module plays a key role in deciding the ECC system's performance. The design and simulation of each module have been performed with a unique concept.

4. Simulation and Results of ECC System

Implemented ECC architecture on Zynq 7000 using HW/SW co-design concept to accelerate the encryption and decryption process. The design and simulation of the proposed design are carried out on the Xilinx Vivado software. Zed board development kit containing the FPGA as well as processor. The Xilinx Zynq-7000 is Programmable SoC, providing an ideal platform to impart intelligence into today's embedded applications. It's All Programmable, which means that you can add intelligence to a system with software and use programmable hardware to do real-time data processing and decisions and programmable I/O to optimize and evolve system interfaces. All of this knowledge can be combined with inexpensive design costs and a lot of flexibility in terms of flexibility or upgrading the design in the field. We have used the HW/SW co-design concept to boost cryptographic operations. All the cryptography operations are executed in programmable logic (PL) and processing system (PS). PL modules contain point addition, point doubling, Scalar multiplication, Modular multiplication, Encryption, and Decryption. PS (Processing System) controls the private key generation module. Elliptic curve base point selection, Curve base effective random number selection, Data control through AXI interface.

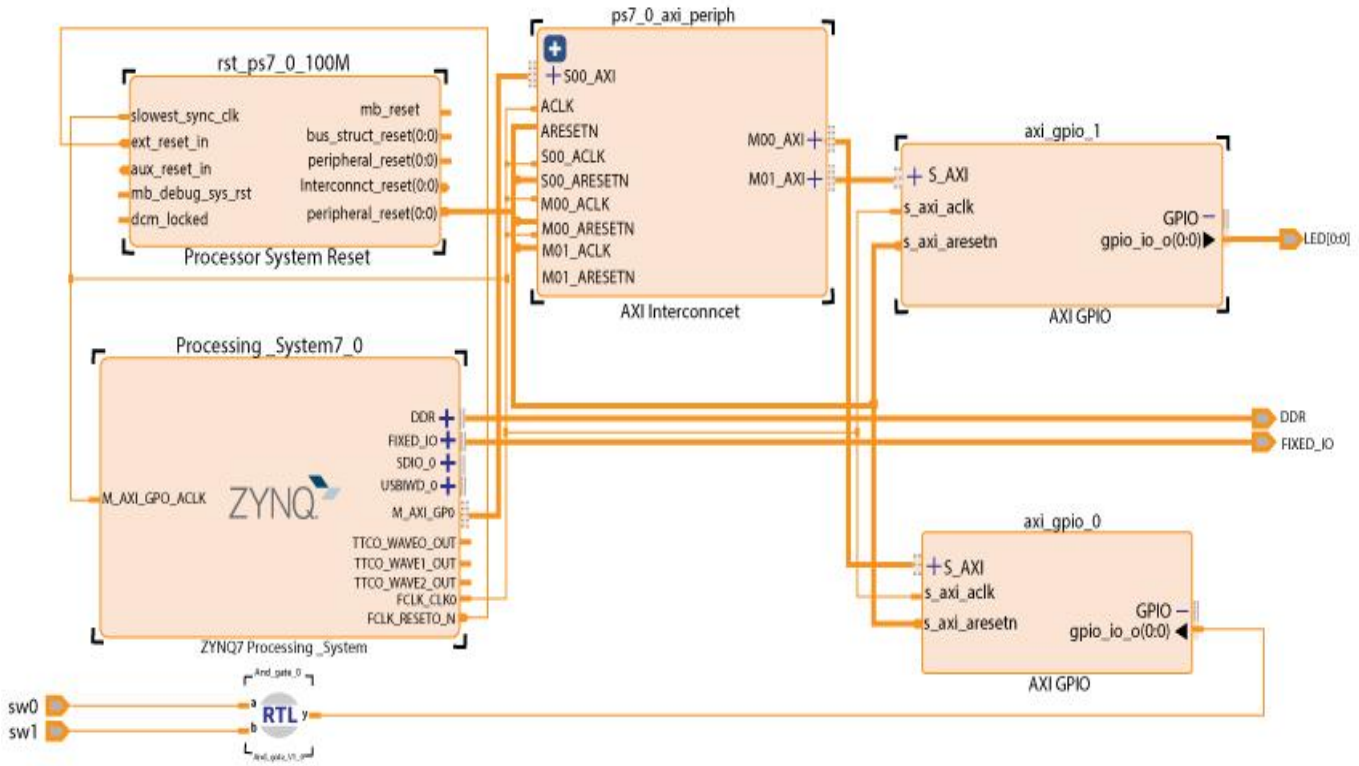

Fig. 4 ECC Accelerator on Xilinx Zynq7000

4.1. Performance Comparison of Proposed Point Addition and Point Doubling

The utilization of the ECC core takes advantage of hardware acceleration. It allows the MPU to conduct other tasks. At the same time, the ECC core executes the scalar-point multiplication function of cryptography, enhancing the system's overall performance for generating securely encrypted data transfers in a parallel manner.

The second layer of the ECC architecture hierarchy is the point addition and point doubling operation. The simulation results of the proposed design of PA and PD modules are shown in table 1 for the NIST recommended bits and compared with the previous literature research article.

Table 1. Performance Comparison of Point Addition and Point Doubling operation

Reference Work	Clock cycles	Field size	Frequency (MHz)	Area (LUTs)	Time (μ s)	Area xTime (LUTs x μ s)	Algorithm
[20]	50	256	40.1	23977	0.80	9.2	Radix-4 interleaved
[21]	98	192	101.3	3020	0.97	2.9	Radix-4 booth encoded
	114	224	98.2	3427	1.16	4.0	
	130	256	95.2	3877	1.36	5.3	
[22]	131	256	166	6300	0.79	5.0	Radix-4 interleaved
[23]	97	192	92	11152	1.1	12.3	Radix-4 booth encoded interleaved
	129	256	86.6	18520	1.49	7.6	
	257	512	76.25	29916	3.37	10.8	
[24] (Design-1)	48	192	101	3100	0.94	2.9	Radix-4 serial interleaved
	56	224	99	3400	1.13	3.8	
	64	256	96	3900	1.30	2.1	
[24] (Design-2)	48	192	171	4200	0.56	2.4	Radix-4 parallel interleaved
	56	224	167	4900	0.67	3.3	
	64	256	166	5300	0.77	4.1	

	308	521	270.5	1988	1.14	2.26	
	366	571	260.8	2130	1.40	2.99	
Proposed Design	123	256	370.5	1676	0.48	1.68	HW/SW co-design

Z. Razali et al. [19] have used Radix-4 interleaved algorithm and achieved a 9.2 LUTs x µs product. K. Javeed et al. [23] proposed two designs. Design-1 has used the Radix-4 serial interleaved algorithm, and design-2 has used the Radix-4 parallel interleaved algorithm. Design-1 and design-2 have achieved 2.1 and 4.1 LUTs x µs product, respectively, for the 256-bit Galois Field.

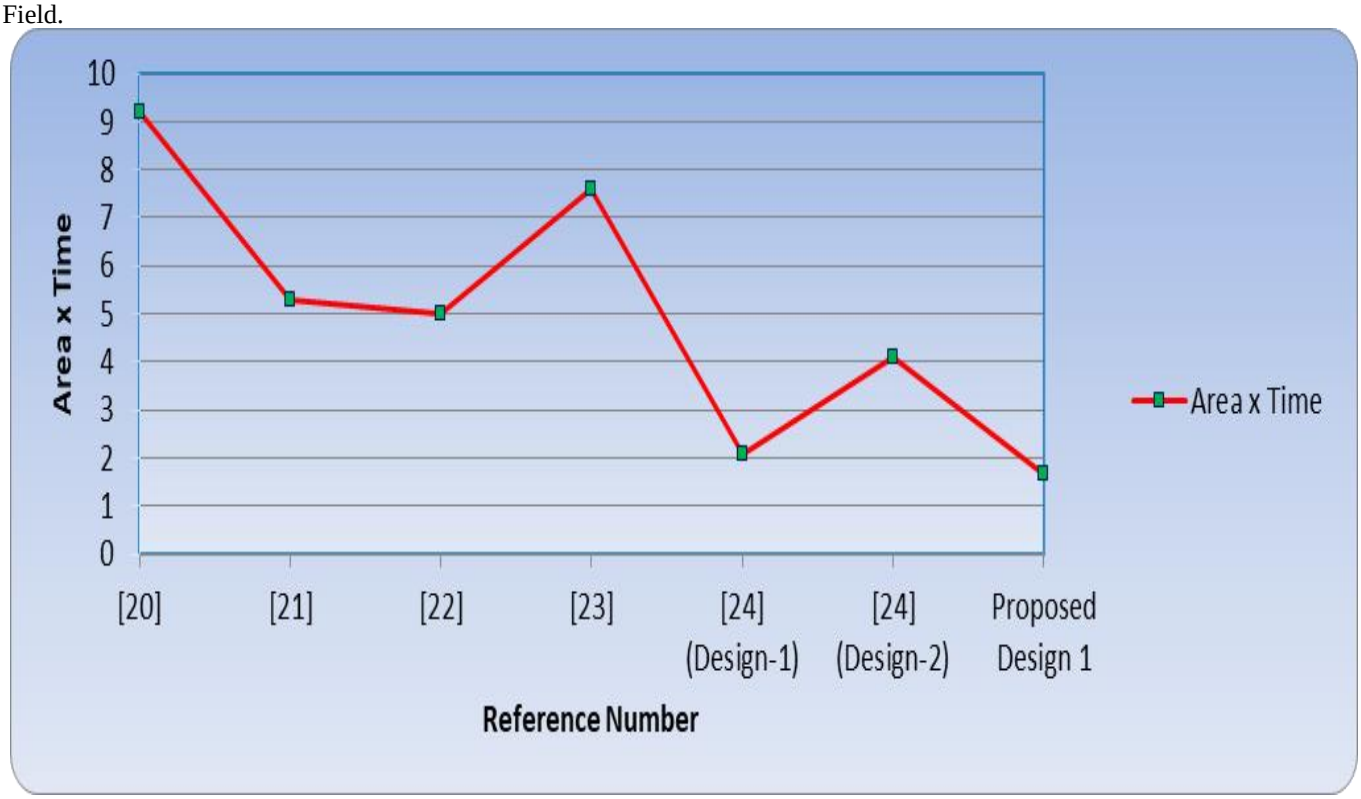

Fig. 5 Performance Parameter Comparison of Point Group Operation

Our proposed HW/SW co-design achieved 1.68 LUTs x µs product. The comparison of the proposed design is present in fig. 5 for Galois field 256bits. The comparison chart is present in terms of area–time product with the previous design and shows that the proposed design uses less area–time product compared to the other design.

4.2. Comparison of Point Operation Design for GF(256)

The proposed design is implemented using HW/SW co-design concept on Xilinx zynq7000 device. The comparison results with previous literature are shown in table 2. The Cryptosystem based on the residue number system was proposed in [25] and achieved 71.63 area-time product. Redundant signed digit-based elliptic curve cryptographic system architecture has been proposed, improving the performance system. [27] RSD-based elliptic curve cryptographic system proposed and implemented on Zynq 7000 device and achieved 12.88 area-time product.[28]

Table 2. Performance parameters comparison of ECC system

Reference Work	Platform	Clock Frequency (MHz)	GF	Clock Cycles	Number of Slices (K)	Time (ms)	Area X Time	Remarks
Proposed Design	Zynq7000	105.4	256	130	5.2	1.21	6.29	Design using HW/SW Co-design concept
[25]	Artix-7	72.9	256	215.	24.2	2.96	71.63	Cryptosystem based on residue number system
[26]	Kintex-7	121.5	256	397	11.3	3.27	36.95	ECC over NIST prime field

[27]	Virtex-6	327	256	153	65.6	1.47	47.87	Redundant signed digit-based elliptic curve cryptographic system
[28]	Zynq7000	160	256	361	5.7	2.26	12.88	RSD-based elliptic curve cryptographic system
[29]	Zynq7000	66.7	256	442	10.2	6.63	67.63	NIST 256 prime bit ECC processor
[30]	Virtex-7	104.39	256	198	7.5	1.4	25.50	Unified point addition on twisted Edwards curve
[29]	Virtex-6	93.23	256	198	9.6	2.13	20.45	Unified point addition on twisted Edwards curve

4.3. Comparison of ECC system design

The comparison chart shown in fig. 6 suggests that our proposed design consumed less LUT and achieved a higher speed than other proposed designs. The implemented design supports up to 105.4 Mhz frequency and uses a 6.29 area–time product.

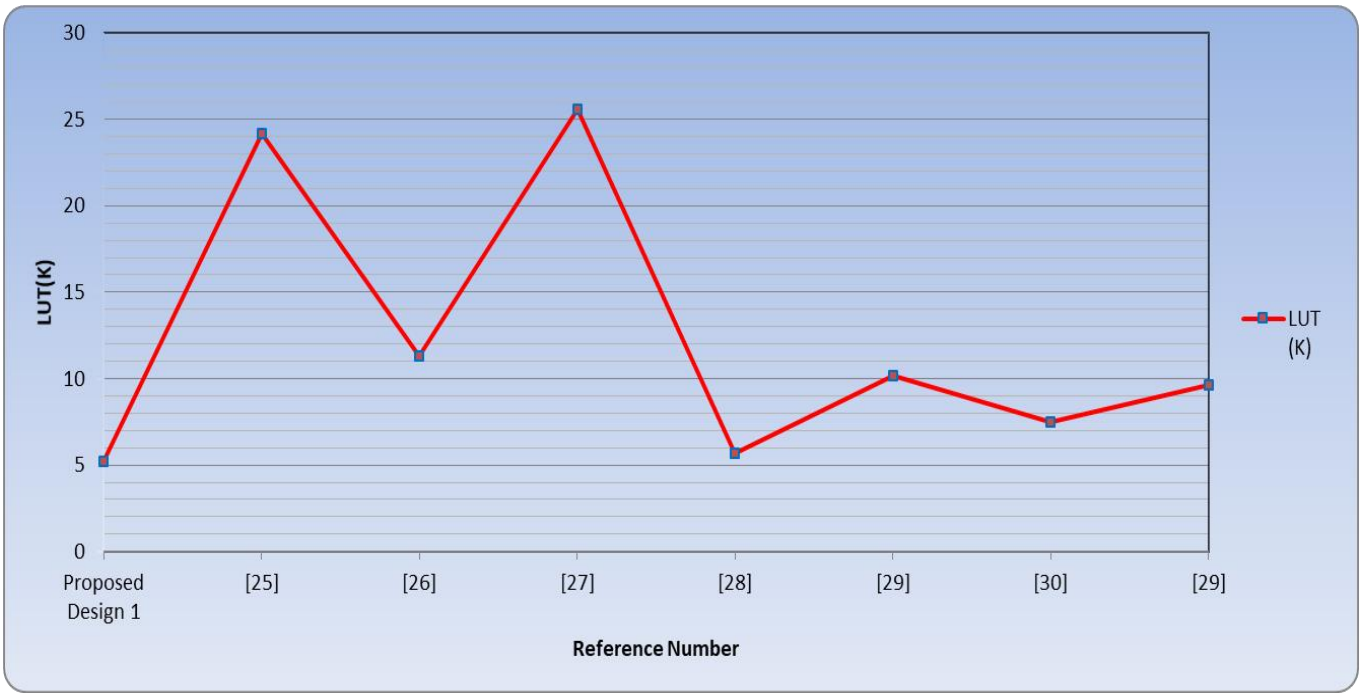

Fig. 6 Performance Parameter Comparison of ECC System

5. Conclusion

Our paper presents the design and implementation of ECC on Xilinx Zynq-7000. The proposed design has used HW/SW co-design concept-based programmable SoC and accelerator ECC operations. The paper proposed restructuring ECC's point addition, point doubling operation, and the Twisted Edwards curve for elliptic cryptographic operations. The result shows that the proposed design achieves better speed with fewer FPGA resources than the literature study. It is an intelligence ECC system with software and programmable hardware to do real-time data processing and effective decisions in the embedded system. The proposed design gives scalability and flexibility with the advantage of reconfigurability features of FGPA. The proposed design performs the best trade-off between speed, area, cost, and security.

References

[1] M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal, and Y. M. Jang, "Design and Implementation of High-Performance ECC Processor with Unified Point Addition on Twisted Edwards Curve," *Sensors* Switzerland, vol. 20, no. 18, pp. 1-19, 2020.

[2] M. Kashif and İ. ÇiÇek, "Field-Programmable Gate Array (FPGA) Hardware Design and Implementation of a New Area Efficient Elliptic Curve Crypto-Processor," *Turkish J. Electr. Eng. Comput. Sci.*, vol. 29, no. 4, pp. 2127, 2021.

[3] J. Li, W. Wang, J. Zhang, Y. Luo, and S. Ren, "Innovative Dual-Binary-Field Architecture for Point Multiplication of Elliptic Curve Cryptography," *IEEE Access*, vol. 9, pp. 12405–12419, 2021.

[4] K. V. Patel and M. V. Shah, "Analysis of Efficient Implementation of Elliptic Curve Cryptography Architecture for Resource Constraint Application," *Int. J. Innov. Technol. Explor. Eng.*, vol. 10, no. 12, pp. 28-35, 2021.

[5] K. V Patel and M. V Shah, "Implementation of Generic and Efficient Architecture of Elliptic Curve Cryptography over Various GF(p) for Higher Data Security," *AJET*, vol. 9, no. 2, pp. 1-7, 2020.

[6] Md. Mainul Islam, Md. Selim Hossain, Moh. Khalid Hasan, Md. Shahjalal , Yeong Min Jang, "Design and Implementation of High-PerformanceECC Processor with Unified Point addition on Twisted Edwards Curve," *Sensors*, vol. 20, pp. 5148, 2020. Doi:10.3390/s20185148.

[7] Kalaiarasi, M., Venkatasubramani, V.R., Vinoth Thyagarajan, V. et al., "A Parallel Elliptic Curve Crypto-Processor Architecture with Reduced Clock Cycle for FPGA Platforms," *J Supercomput*, 2022. C*rossref*, https://doi.org/10.1007/s11227-022-04442-2

[8] B. Panjwani, "Scalable and Parameterized Hardware Implementation of Elliptic Curve Digital Signature Algorithm Over Prime Fields," in Proc. *Int. Conf. Adv. Comput., Commun. Informat, (ICACCI)*, pp. 211–218, 2017.

[9] Dennis Agyemanh Nana Gookyi and Kwangki Ryoo, "A Lightweight System-on-Chip Based Cryptographic Core for Low-Cost Devices," *Sensors*, vol. 22, pp. 3004, 2022. https://doi.org/10.3390/s22083004.

[10] Ahmed A.H. Abd-Elkader et al., "Efficient Implementation of Montgomery Modular Multiplier on FPGA," *Elsevier Computer and Electric Engineering*, vol. 97, pp. 107585, 2022.

[11] Luis Parrilla, José A. Álvarez-Bermejo, Encarnación Castillo, Juan A, López-Ramos, Diego P, Morales-Santos, Antonio García, "Elliptic Curve Cryptography Hardware Accelerator for High-Performance Secure Servers," *Springer*, 2018. C*rossref*, https://doi.org/10.1007/s11227-018-2317-6

[12] Mojtaba Bisheh-Niasar , Reza Azarderakhsh , Mehran Mozaffari-Kermani, "Cryptographic Accelerators for Digital Signature Based on Ed 25519," *IEEE Transaction On Very Large Scale Integration (VLSI) Systems*, pp. 1063-8210.

[13] Pradeep Kumar Goud Nadikuda, Lakshmi Boppana, "An Area-Time Efficient Point-Multiplication Architecture for ECC Over GF(2m) using Polynomial Basis," *Microprocessors and Microsystems*, vol. 91, 2022.

[14] Luis Parrilla, Ahmed Mohamed Bellemouy, Antonio Garc´ıa, Encarnaci´on Castillo, "Efficient Elliptic Curve Cryptoprocessor for enabling TLS Protocol in Low-Cost Reconfigurable Socs," *IEEE*, 2019. 978-1-7281-5458-9.

[15] Philipp Koppermann, Fabrizio De Santis, Johann Heyszl and Georg Sig, "X25519 Hardware Implementation for Low-Latency Applications," *IEEE Euromicro Conference on Digital System Design*. DOI 10.1109/DSD.2016.65

[16] J. Li, W. Wang, J. Zhang, Y. Luo, and S. Ren, "Innovative Dual-Binary-Field Architecture for Point Multiplication of Elliptic Curve Cryptography," *IEEE Access*, vol. 9, pp. 12405–12419, 2021.

[17] J. Wen, N. Wu, F. Ge, and L. K. Zhao, "A Length-Scalable Modular Multiplier Implemented with Multi-bit Scanning," *IEEE 4th Int. Conf. Electron. Technol. ICET*, vol. 978, no, 1, pp. 109-113, 2021.

[18] X. Zhao, B. Li, L. Zhang, Y. Wang, Y. Zhang, and R. Chen, "FPGA Implementation of High-Efficiency ECC Point Multiplication Circuit," *Electron*, vol. 10, no. 11, pp. 1-22, 2021.

[19] Z. Razali, N. Muslim, S. Kahar, F. Yunos and K. Mohamed, "Improved Point 5P Formula for Twisted Edwards Curve in Projective Coordinate Over Prime Field," *International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 498-502, 2022. Doi: 10.1109/DASA54658.2022.9765062.

[20] Y. Yang, C. Wu, Z. Li, and J. Yang, "Efficient FPGA Implementation of Modular Multiplication Based on Montgomery Algorithm," *Microprocess and Microsystem*, vol. 47, pp. 209-215, 2016.

[21] K. Javeed, X. Wang, and M. Scott, "High Performance Hardware Support for Elliptic Curve Cryptography over General Prime Field," *Microprocess And Microsystem*, vol. 51, pp. 331-342, 2017.

[22] A. El Aroudi, E. Rodriguez, and M. Orabi, "Modelling of Switching Frequency Instabilities in Buck- based DC – AC H-bridge Inverters," *Int. J. Circuit Theory Appl*, pp. 2295, 2020.

[23] K. Javeed and X. Wang, "Radix-4 and Radix-8 Booth Encoded Interleaved Modular Multipliers over General FP," Conf. Dig. - 24th Int. *Conf. F. Program. Log. Appl. FPL*, pp. 6927452, 2014.

[24] K. Javeed, X. Wang, and M. Scott, "Serial and Parallel Interleaved Modular Multipliers on FPGA Platform," 25th Int. *Conf. F. Program. Log. Appl. FPL*, pp. 2-5, 2015.

[25] S. Asif, M. S. Hossain, Y. Kong, and W. Abdul, "A Fully RNS based ECC Processor," *Integration VLSI journal ELSEVIER*, vol. 61, pp. 138-149, 2018.

[26] P. M. Matutino, J. Araujo, L. Sousa, and R. Chaves, "Pipelined FPGA co-processor for Elliptic Curve Cryptography Based on Residue Number System," *Proc. - 17th Int. Conf. Embed. Comput. Syst. Archit. Model. Simulation*, vol. 2018, no. 3, pp. 261-268, 2018.

[27] R. Items, W. Rose, W. Rose, T. If, and W. Rose, "Throughput / Area Efficient ECC Processor on FPGA," *IEEE Transactions on Circuits and Systems*, vol. 2, pp. 1078-1082, 2015.

[28] C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight Elliptic Curve Cryptography Accelerator for Internet of Things Applications," *Ad Hoc Networks*, vol. 103, pp. 102159, 2020.

[29] S. Asif, M. S. Hossain, and Y. Kong, "High-throughput Multi-Key Elliptic Curve Cryptosystem Based on Residue Number System," *IET Comput. Digit. Tech.* vol. 11, no. 5, pp. 165-172, 2017.

[30] Narmatha.K, Sujay.S, Arjitvijey. J *" Internet of Things Security By Elliptic Curve Cryptography"* International Journal of Computer Trends and Technology 68.6 (2020):37-40.

[31] Vanajeswari Imandi, Nagalakshmi Harisha A, "Performance Comparison Between Ultra Low Power Alu With Cmos And Gdi Techniques," *SSRG International Journal of VLSI & Signal Processing*, vol. 7, no. 2, pp. 43-46, 2020. *Crossref*, https://doi.org/10.14445/23942584/IJVSP-V7I2P107