International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-10 Issue-12, October 2021

Analysis of Efficient Implementation of Elliptic Curve Cryptography Architecture for Resource Constraint Application

Kirit V. Patel, Mihir V. Shah

Abstract: ***Elliptic Curve Cryptography is gaining attraction in providing a high security level in data transmission with low cost, small key size and smaller hardware realization. High-speed implementation is a significant factor in ECC applications such as smart cards, network servers, wireless sensor based networks, Internet of Things and Radio Frequency Identification. These applications require low-cost and lightweight implementations. In the resource constrain application, lightweight cryptography has emerged as the desired one because of limited energy in devices and the scarce computational resources. Design options and a wide range of parameters affect the overall implementation of the ECC system. Implementation target device, coordinate system, underlying finite fields and modular arithmetic algorithms are key design parameters that impact the overall implementation outcome. A statistical study is conducted on a large collection of published work based on the design parameters. The basic question that arises is how to select the appropriate flexibility-efficiency tradeoff. The subjects of generator, versatile, reconfigurable, dedicated and general purpose scalar multipliers are addressed. A review of various algorithms to perform scalar multiplication on prime and binary fields has been done more effectively. The results of ECC implementation on different FPGA platform is compared and analyzed with the various performance parameters. Besides, a classification of the previous works in terms of flexibility, performance, scalability and cost effectiveness is presented.***

Keywords: Elliptic Curve Cryptography (ECC), Galois Field (GF), Discrete Logarithm Problem (DLP), Scalar multiplication, Public Key Cryptography (PKC), Field Programmable Gate Array (FPGA), Elliptic Curve Cryptography Processor (EECP), Elliptic Curve Scalar Multiplication (ECSM).

I. INTRODUCTION

In recent times, confidential information transmission over the internet is increased and recommended for higher data security. Cryptography serves as a renowned method to provide sensitive data transmission with a high degree of confidentiality. There are two widely accepted PKC (Public key cryptography) algorithms for cryptographic applications are Rivest-Shamir-Adleman (RSA) and elliptic curve cryptography (ECC) [1].

Manuscript received on March 24, 2021.
Revised Manuscript received on October 18, 2021.
Manuscript published on October 30, 2021.
* Correspondence Author
Kirit Patel*, Department of Electronics and Communication, L.D. College of Engineering, Gujarat Technological University, Ahmedabad (Gujarat), India. Email: kirit@ldce.ac.in
Mihir Shah, Department of Electronics and Communication, L.D. College of Engineering, Gujarat Technological University, Ahmedabad (Gujarat), India. Email: mihirec@gmail.com

RSA is based on integer factorization, whose encryption strength depends on the key sizes. ECC is relevant to both the discrete logarithm algorithm and integer factorization families which were first introduced by Koblitz [2] and Miller [3]. ECC has the main features of Discrete Logarithm Problem (DLP) over various points on the elliptic curve which provides complex security. ECC requires a shorter key length than RSA to provide the same level of security. This smaller key size feature makes ECC the best suited for resource-constrained IoT devices as well as high-speed cryptographic processors [4]. ECC offers strong security per bit and provides an efficient hardware implementation in terms of power consumption and speed than other PKC algorithms[5]. In order to implement the ECC algorithm, there are three choices: software, ASIC and FPGA. FPGA is a perfect hardware implementation platform for a prototype design, considering cost, time consumption, and hardware development facility. Our literature review consists of four segments. First, we place the design options and discuss design flow and its impact on ECC implementation. Second, we compile different approaches and algorithms used in the literature for implementing scalar multiplication. Third, we review and analyze best practices in the literature to implement ECC architectures in the different reconfigurable platforms. Fourth, we summarize the performance enhancement parameters for ECC. Besides, this paper provides a comparison of the different design parameters and hardware platform implementations of ECC.

II. DESIGN FLOW OF ECC

The Various options in the implementation of ECC architecture are shown in the representation of flowchart in figure 1 which is useful to optimize the finite field operations for ECC architecture to reduce area and power consumption. The design flow level is shown with the various options such as the selection of curve, scalar multiplication, prime field, coordinate, point operation, and field operations. In the initial step, the designer has the basic selection options such as the elliptic curve type. The selected curve will define the characteristics and performance of the complete cryptography system. There is a choice of point multiplication algorithm based on the elliptic curve in the next phase, and this algorithm affects the performance parameter like speed, area, and power consumption. The finite field size, the type of finite field and other properties are selected for implementation. Two related fields are prime field Fp and binary field $F2^m$. The various research works for flexibility are

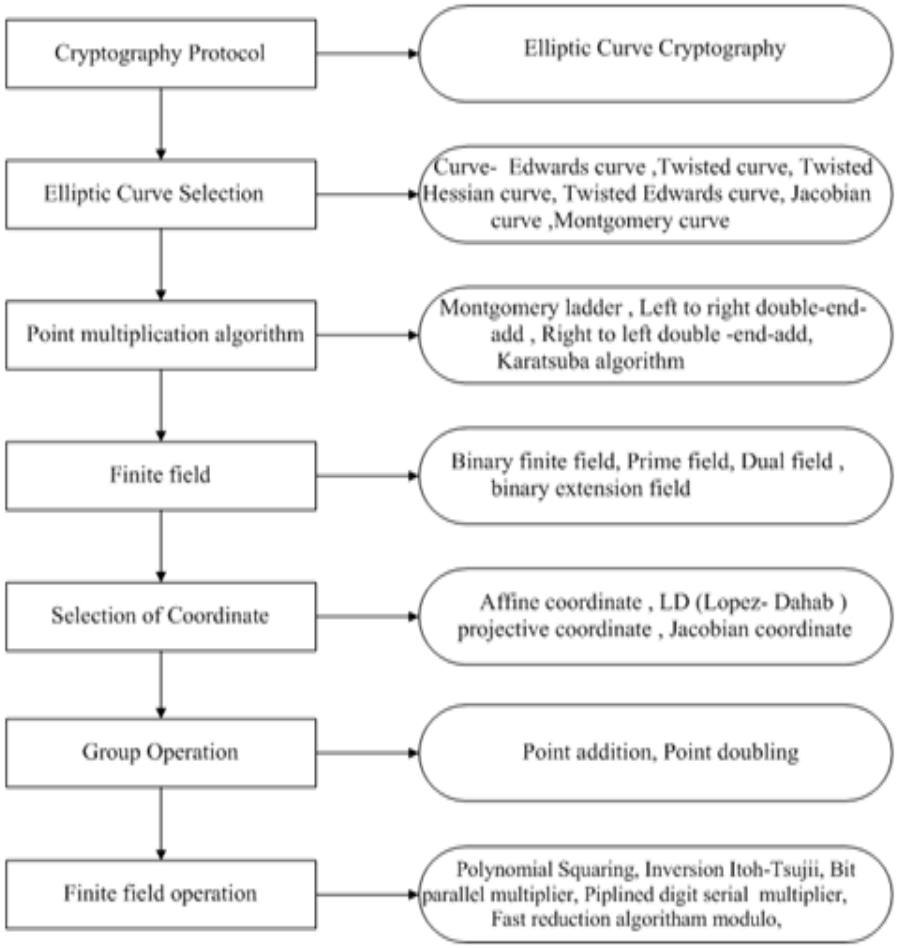

Fig 1. various options in the implementation of ECC

implemented based on two fields that are called a dual-field implementation system. In the next step, point operation and finite field operations are the selection option. There are multiple effective algorithms available for finite field operation used to design effective ECC system as per application requirements [6]. The ECC application's feasibility depends on scalar multiplication or point multiplication (PM) based on group and finite field (FF) activities [7]. ECC is recommended for hardware cryptosystem processor synthesis for the required small key size, low area, lower memory requirements, faster encryption and decryption, less power consumption, and lower bandwidth requirements [8].

2.1 Scalar Multiplication

The ECC's basic operation is point scalar multiplication, where a point on the curve is multiplied by a scalar. A point scalar multiplication is measured by calculating a series of point doublings and point additions. Points are added or doubled by their geometrical properties by a series of subtractions, additions, divisions and multiplications of their respective coordinates Various ECC processors are discussed in the literature that either target prime fields or dual field operations of binary extension fields. Many ECC device parameters influence the hardware ECC architecture from the upper layer of the elliptic curve down to the underlying finite field. Variation of device parameters offers a barrier to formalizing a hardware ECC implementation design framework. There are four types of well established ECC processor architecture presented in [9]: Dedicated, generator, versatile and general purpose. In ECC, modular multiplication is a key arithmetic operation. The efficiency of the modular multiplication algorithm determines the efficiency of an elliptic curve cryptosystem. The efficiency of the area and the processor's maximum achievable frequency depend entirely on the modular multiplier adopted by it. Without compromising the speed, it is a key challenge in prime field ECC to build a low-area modular multiplier for lightweight cryptography. Therefore, a key demand is to improve the modular multiplication algorithm [10]. Many authors have implemented hardware architecture for ECSM in prime fields GF(p) or binary fields GF(2^n) or dual field where "p" and "n" represent the number of bits in a specific field, respectively. The ECSM calculations can be implemented using projective coordinates or affine coordinates, or mixed coordinates systems. Hossain et al. proposed an ECC processor over GF(p) in both application-specific integrated circuit (ASIC) and FPGA design[11]. The proposed design implementation has a feature of parallel processing of radix-2. It is based on an interleaved modular multiplier. It also used a binary inversion algorithm to execute ECSM operation in mixed projective coordinates and affine coordinates without using any hardware accelerators. Javeed [12]

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

proposed a double-and-add always (DAA) algorithm to execute ECSM operation on reconfigurable platforms like Xilinx Virtex-6 FPGA over GF(p) [13].
Secure algorithms are required to map the best options for lightweight asymmetric and symmetric algorithms so that minimum energy requirements with less execution time can be achieved and all security resources such as confidentiality of authenticity and integrity can be confirmed [14].

2.2 Resource Constrained Application

A constrained environment is defined as a computational system of multiple heterogeneous modules, where the underlying computational module has limited capabilities. The limitations are related to the storage memory, the size of the device, the processing power, bandwidth and the energy availability of the devices. The Internet of Things (IoT) nodes and the Wireless Sensor Network (WSN) motes are considered as a Resource Constrained Application. It is a great challenge to provide higher security for resource constrained based new generation network. The security algorithms can be constrained by severe restrictions on processing time, bandwidth, hardware, and energy supply. These systems need at least the same security resources, even though fewer computing capacity than the traditional network. In aggressive conditions, restricted devices can be installed and an attacker may have physical access to the network. For fixing these vulnerabilities, additional protection measures, such as side channel countermeasures, should be addressed [15]. The significant module in the design of IoT systems is to achieve savings in computing power, area, storage capacity, power, and bandwidth of the restricted devices. The proposed method for offering security services under restricted structures in lightweight cryptography. PKC helps the realizing of encryption, authentication and key establishment for networked environments. ECC is the most powerful public-key option for offering security services to constrained environments applications [16]. Cryptographic implementations, in real-time applications, are facing challenges as it has to ensure fast and effective performance but still provide a higher security level comparable to traditional systems [17].The desired low area, small key size, lower memory requirements, faster encryption and decryption process, low power consumption, and lower bandwidth necessities recommend ECC for hardware cryptosystem processor synthesizes. Implementing an efficient ECCP with a fully pipelined, parallel, special scalar multiplier and self-controlled architecture can be achieved. It intends to enhance the ECCP hardware design targeted for resource constrained application like IoT [8]. The Internet of Things (IoT) is a heterogeneous network where millions of modules are connected through the Internet and communicate confidential data with each other. Since most of these modules have limited resources like power, area and time. Usually, data are stored in the cloud where people can continuously download and upload data from anywhere through the Internet [18]. The end user has no control over the data management in the cloud-computing environment, which requires a high security level in data transmission. The limited resources of IoT devices and the requirement of higher data security encourage the researcher to develop lightweight cryptographic systems that can justify low memory, higher security and low power requirements of the IoT applications [10].

2.3 Edwards Curves

Cryptography researchers get much interest in using Edwards curves in cryptographic applications because of closed group operations [19] and high protection to side-channel attacks (SCAs) [20]. Edwards curves can recommend strongly unified addition [21] formulas that can be used for both point doubling and point addition, ensuring side-channel security. A cryptographic architecture based on Edwards curve can be developed with low power consumption and low area utilization, providing high computational speed with a high security level [22]. The implementation of ECC on a hardware platform with resource constrained is a highly challenging task because low module uses lead to low computational speed. Edwards curve is more effective than the traditional elliptic curve because its implementation provides high security and high computational speed with fewer hardware resources. Most of the ECC implementation on the hardware platform proposed in the literature is based on elliptic curves. It offers area-efficient hardware architecture for digital signature verification with its reconfigurable platform implementation.[4] Due to high resistance to SCAs and simplicity, the Edwards curve is gaining enormous interest among security researchers [23]. ECPM is quicker and more stable on Edwards curves than on elliptical curves in the Weierstrass form [24]. The benefit of Edwards curves is that they give highly coherent addition formulas [25], covering both PA and PD. To perform ECPM, distinct hardware architectures for PA and PD are not necessary. Moreover, through rendering the secret key identical to power tracing, the unified PA prevents possible SPA attacks [4]. Implementing the Twisted Edward curve can use the unified formula for both doubling and addition, thereby implementing side-channel security [26-27]. A range of work is carried out aimed at high speed scalar multiplication operation or high-throughput which is the main feature of the ECC processor [17].

III. RESULTS ANALYSIS/COMPARISON OF ECC IMPLEMENTATION

Various researchers have designed and implemented ECC on the different reconfigurable platforms. In this section, different implementations of ECC are compared and analyzed.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table 1. Results comparison of Scalar Multiplication on a different platform

Reference Work	Publishing year	Finite field size	Platform	Clock Frequency	Number of Slices	Latency	Performance area x time	Through put	Remarks
[5]	2020	256	VIRTEX-7	125 MHz	12.71K	0.46ms	6.1	N.A.	RNS ECC point multiplication
[5]	2020	256	VIRTEX-7	125 MHz	14.01k	0.25ms	3.5	N.A.	RNS ECC point multiplication
[28]	2018	256	VIRTEX-7	86.6 MHz	N.A.	0.73ms	14.0	N.A.	RNS based ECC processor
[29]	2017	256	SPARTAN -6	147MHz	789	25.4ms	20.1	N.A.	Pipelined FPGA ECC coprocessor on RNS
[04]	2019	256	VIRTEX-7	177.7 MHz	8.9k	1.48ms	13.17	173.20 kbps	Edwards curve digital signature algorithm
[04]	2019	256	VIRTEX-6	161.1 MHz	9.2k	1.63ms	15.00	157.00 kbps	Edwards curve digital signature algorithm
[40]	2018	256	VIRTEX-6	327.0 MHz	65.6k	0.47ms	30.80	546.42 kbps	Redundant signed digit based ECC processor,
[16]	2019	251	SPARTAN -6	109 MHz	4.12 k	7.62 ms	N.A.	N.A.	Lightweight ECC accelerator
[15]	2019	251	SPARTAN -6	13.56MHz	7.25k	2.15 ms	N.A.	N.A.	Scalar multiplication with binary edwards curves
[04]	2020	256	VIRTEX-7	104.39 MHz	5.457k	1.899 ms	N.A.	134.8 kbps	ECC Processor with Unified Point Additionon Twisted Edwards Curve

IV. SCALAR MULTIPLICATION

Mohamad Ali et al.[5] proposed an RNS-based ECC core hardware implementation for the two families of elliptic curves. The proposed design includes twisted Edwards curves and short Weierstra ß. RNS is an active research field due to its inherent parallelism, faster public-key cryptography operations. Different ECC point multiplication algorithms are implemented on the Xilinx FPGA platform. The simulation results prove that fully RNS ECC point multiplication efficiency is higher than the literature's fastest ECC point multiplication hardware. For the ECC state machine, different scalar multiplication algorithms were introduced. In order to demonstrate the effect of layout process technology on speed, the design was implemented on the VIRTEX-7 and VIRTEX Ultra Scale+ families [5].

All the literature survey proved that scalar multiplication plays an essential role in deciding cryptography architecture's performance. The implementation of scalar multiplication in different reconfigurable platforms using various algorithms is

compared in table (1) considering the performance parameters. The recent works [22] and [17] are the effective time efficient implementations of the point multiplication on Edwards curves. RNS based work presented in [5] and [28] over GF(2^{256}) on Virtex-7 achieves a low latency output. Unified Point Addition on twisted Edwards Curve was implemented on GF(2^{256}) and Virtex 7 platform in[4] by achieving low latency. A lightweight ECC accelerator was implemented in [16]. Figure 2 shows a graphical representation of the latency and the number of Slices for the previous implementation. In the presentation, the results are distinguished based type of FPGA platform to have a better comparison. The work [5] has acceptable performance in latency and [29] has no. of slices.

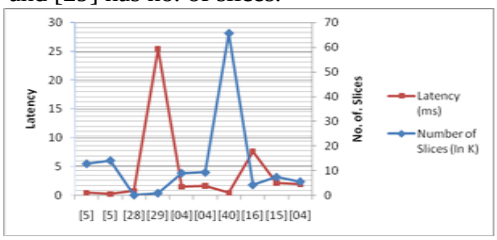

Fig 2. Analysis of no. of slice and latency for scalar multiplication

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Implementation on Edwards curves

Binary Edwards curves (BEC) [30] are considered in the implementation of scalar point architecture. Literature studies have identified merits for ECC hardware implementations when a binary is the underlying finite field [31]. BECs have the most powerful kP formulae concerning field operations cost [32] from the different alternatives of binary elliptic curves. In order to use the final architecture as an accelerator or a co-processor and to unload calculations from the main processor, a hardware realization was chosen. The architecture is motivated by two fundamental inspirations: a) to obtain a solution according to National Institute of Standards and Technology (NIST) guidelines capable of providing long-term protection b) to minimize the size of implementation to reduce IoT system manufacturing costs [16]. The different curve of a family of elliptic curves and coordination systems provides a diversity of design options. The Twisted Edward curve is one of the recently trending curves used to develop elliptic curves. It's strong immunity to side-channel attacks have gained much interest in developing cryptographic system. The Edward curve cryptography (EdCC) processor's efficiency ensures the desired security by combining the high intractability and the efficient point operation design feature of the cryptographic curve. The most recently proposed design of twisted Edward curve for performing point operation is presented in [17]. A novel unified point operation architecture has been developed field that can perform Edward curve point addition and point doubling in Jacobian coordinates over GF(256). The architecture implanted on Virtex-5. The proposed hardware architecture enhances the use of the slices available area and reduces the time required for GF(256) Twisted Edward Curve in Jacobian coordinates [17].

Implementation on Reconfigurable Platform

An appropriate pipelined ECC core architecture is used to execute the proposed design over the binary (2^n) NIST suggested curves. An improved Montgomery ladder algorithm is used for the point scalar multiplication by introducing pipelined registers in ideal locations. *The* proposed architecture has been developed on Xilinx Virtex, Kintex, and Artix FPGA board. it can perform a single scalar multiplication in 226 clock cycles within 0.63 µs. A scalar multiplication can be computed in GF (2^{233}) and GF (2^{571}) within 1.05 µs and 2.32 µs in 327 and 674 clock cycles, respectively. The proposed reconfigurable architecture reduces the number of clock cycles required and operates with competitive high working frequencies that require lesser FPGA resources. The proposed architecture is well designed in low-powered resource-constrained real-time cryptography systems such as banking platforms, wearable smart devices and network-attached storage. An effective Montgomery ladder scalar point method has been developed to perform scalar multiplications (kP). The algorithms of Karatsuba-Ofman and Itoh-Tsuji were used to perform finite field operations for inversion and multiplication [33]. Proposed a novel architecture for elliptic curve point-multiplication based on modified Lopez-Dahab-Montgomery in [34] to improve hardware complexity and time utilization. The proposed architectural data-path is organized and pipelined to realize finite-field operations like square operations and multiplication parallel to reduce the critical-path delay. The FF-operations are designed to execute each iteration of point addition and point doubling without data-dependency. The elliptic curve-point multiplication (ECPM) implementation over the NIST recommended binary curve GF(2^{163}) confirms that the design achieves an improvement of area-time efficiency. The data path is designed to reduce critical path delay and to execute parallel FF operations. To increase the operating frequency and minimize the LUTs required, the Hybrid Karatsuba multiplier was used. Over Galois Fields GF (2^{163}) and GF (2^{409}) on Xilinx Integrated Synthesizes Environment (ISE) Virtex 6 FPGA, the developed ECCP method is designed [34]. Shaimaa et al. presented an effective ECCP architecture for security in embedded devices and IoT. A finite field polynomial multiplier uses most of the implementation effort of an ECCP because it consumes most area and time for an operation. So, the main objective is to implement the main operation of Point Multiplication (PM) using FPGA.

Table 2. Analysis of ECC Implementation on reconfigurable platform

Reference Work	GF (2^n)	Platform	Clock Frequency	LUT	Number of Slices	Time	Efficiency	Throughput	Power Consumption	Remarks
[33]	233	Virtex-7	310 MHz	16,003	4,762	1.05 us	46385.32	N.A.	1.014 watt	Pipeline architecture and improved Montgomery ladder Algorithm for the scalar multiplication
[33]	571	Virtex-7	290 MHz	71,180	18,178	2.32 us	13515.38	N.A.	1.434	
[33]	233	Artix-7	209 MHz	15,236	3,977	1.56 us	37445.44	N.A.	1.583	
[33]	233	Kintex-7	311 MHz	15,221	4,915	1.06 us	44796.41	N.A.	0.609	
[33]	233	Virtex-6	239 MHz	14,402	4,143	1.451us	38759.1	N.A.	N.A.	
[41]	163	Virtex-7	397 MHz	4,721	1,476	10.51 us	N.A.	64.47	N.A.	Montgomery point multiplication

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

[34]	283	Virtex-7	313 MHz	19225	N.A.	7.69 us	N.A.	147.84	N.A.	Modified Lopez-Dahab-Montgomery (LDM) point-multiplication algorithm
[42]	283	Virtex-7	337 MHz	20202	N.A.	20.32 us	N.A.	410.5	N.A.	Optimized pipelined architecture
[34]	233	Virtex-7	340 MHz	14391	N.A.	5.9 us	N.A.	84.94	N.A.	Modified Lopez-Dahab-Montgomery point multiplication algorithm
[42]	233	Virtex-7	370 MHz	7895	N.A.	16.01 us	N.A.	126.39	N.A.	Montgomery point multiplication
[34]	163	Virtex-7	389 MHZ	8529	N.A.	3.71 us	N.A.	31.72	N.A.	Modified Lopez-Dahab-Montgomery(LDM) point-multiplication algorithm
[38]	163	Virtex-7	800 MHz	3806	N.A.	65 us	N.A.	247.39	N.A.	Lopez-Dahab scalar point multiplication and left-to-right algorithms
[22]	256	Virtex-7	104.39 MHz	N.A.	6.5k	1.9 ms	N.A.	134.49	N.A.	Unified Point Addition on Twisted Edwards Curve
[22]	256	Virtex-6	93.23 MHz	N.A.	6.6k	2.13 ms	N.A.	120.12	N.A.	Unified Point Addition onTwisted Edwards Curve
[28]	256	Virtex-7	72.9 MHz	N.A.	24.2k	2.96 ms	N.A.	1816.2	N.A.	Cryptosystem based on residue number system
[10]	256	Kintex-7	121.5 MHz	N.A.	11.3k	3.27 ms	N.A.	78.28	N.A.	ECC over NIST prime field

The developed ECCP design is implemented over Galois Fields GF (2^{163}) and GF (2^{409}) on Xilinx Integrated Synthesizes Environment (ISE) Virtex 6 FPGA. Implementing algorithms such as Montgomery [35], Itoh-Tsujii [36], and Karatsuba [37] for optimizing finite field operations to improve throughput, speed and computation time [8]. Md. Mainul et al. proposed a low-area, high speed, simple power analysis resistant implementation of ECC processor with unified point addition on a twisted Edwards curve on FPGA platform. Proposed efficient hardware architectures for modular inversion, modular multiplication, unified point addition, and elliptic curve point multiplication. The ECPM scheme is developed in projective coordinates instead of affine coordinates to reduce the computational complexity. The proposed ECC processor executed 256-bit point multiplication over a prime field and implemented on the Xilinx Virtex-7 FPGA platform. It supports high speed public-key generation using fewer hardware resources without compromising the security level which is the main IoT application requirement. To execute high-speed modular multiplication, an efficient radix-4 interleaved modular multiplier was proposed. It is well suited for resource-constrained IoT devices because of its less hardware resource requirements and high computation speed [4]. The performance parameter like clock frequency, latency, no. of a slice, prime field and FPGA platform decide the cryptography system's effectiveness. So based on the different parameter of ECC implementation is analyzed in table (2). This comparison is effective in deciding the algorithm and FPGA platform for the customized application. In recent work of [38], Pipeline architecture and improved Montgomery ladder Algorithm for the scalar multiplication were used and presented Virtex-7, Artix-7 and Kintex-7 platform results. Implemented Unified Point Addition on Twisted Edwards in [4] and presented results of Virtex-7 and Virtex-6. Implemented ECC over NIST prime field in [39] with effective performance.

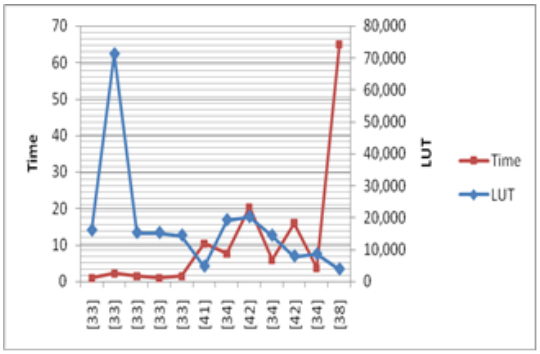

Fig 3. Analysis of LUT and Time for ECC system

A graphical representation of the LUT and time for the previous ECC structures shown in Figure 3. There is a tradeoff between LUT and time for the different reconfigurable platforms, so as per the application requirements, ECC can select the specific algorithm

V. CONCLUSIONS

A survey and analysis discussion has been done on cryptographic architecture and its implementation on the reconfigurable hardware platform in this paper. This survey determined the criteria that make lightweight ECC based solutions and feasible for use in resource constrained applications. We also discussed the open challenges which are facing by cryptographic systems. Our analysis would enable designers to choose the right ECC implementation based on a design target.

A review of various algorithms to perform scalar multiplication on both prime and binary fields was more effectively done. In this paper, a comprehensive study of hardware implementations of elliptic curve cryptography is presented. For fair comparison and better analysis, the implementations are categorized and presented based on finite used field, type of elliptic curves, representation basis and implementation platforms. Various elliptic curves, scalar point multiplication algorithms, finite field arithmetic algorithm and their effect on implementations are defined and discussed. The implementations are compared in terms of hardware utilization and execution time which is essential for many applications that required a high speed execution process.

REFERENCES

1. MD. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography. New York, NY, USA: Springer-Verlag, 2004.
2. N. Koblitz, ``Elliptic curve cryptosystems," Math. Comput., vol. 48, no. 177, pp. 203_209, 1987.
3. V. S. Miller, ``Uses of elliptic curves in cryptography," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 218. New York, NY
4. 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, doi: 10.3390/s20185148.
5. M. Mehrabi, C. Doche, and A. Jolfaei, "Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module," IEEE Trans. Comput., vol. 9340, no. c, pp. 1–12, 2020, doi: 10.1109/TC.2020.3013266.
6. B. Rashidi, "A Survey on Hardware Implementations of Elliptic Curve Cryptosystems," arXiv, no. December, pp. 1–61, 2017.
7. R. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curve Cryptography, Chapter 3 "Elliptic Curve Arithmetic", New York: Springer Professional Computing, 2004.
8. S. Abu Khadra, S. E. S. E. Abdulrahman, and N. A. Ismail, "Towards Efficient FPGA Implementation of Elliptic Curve Crypto-Processor for Security in IoT and Embedded Devices," Menoufia J. Electron. Eng. Res., vol. 29, no. 2, pp. 106–118, 2020, doi: 10.21608/mjeer.2020.103280.
9. H. Marzouqi, M. Al-Qutayri, and K. Salah, "Review of Elliptic Curve Cryptography processor designs," Microprocess. Microsyst., vol. 39, no. 2, pp. 97–112, 2015, doi: 10.1016/j.micpro.2015.02.003.
10. M. M. Islam, M. S. Hossain, M. D. Shahjalal, M. K. Hasan, and Y. M. Jang, "Area-Time Efficient Hardware Implementation of Modular Multiplication for Elliptic Curve Cryptography," IEEE Access, vol. 8, pp. 73898–73906, 2020, doi: 10.1109/ACCESS.2020.2988379.
11. Hossain MS, Kong Y, Saeedi E, Vayalil NC. High-performance elliptic curve cryptography processor over NIST prime fields. IET Comput & Digit Tech. 2016;11(1):33-42.
12. Javeed K,Wang X. Low latency flexible FPGA implementation of point multiplication on elliptic curves over GF (p). Int J Circ theory appl. 2017;45(2):214-228.
13. T. Kudithi and R. Sakthivel, "An efficient hardware implementation of the elliptic curve cryptographic processor over prime field, Fp," Int. J. Circuit Theory Appl., vol. 48, no. 8, pp. 1256–1273, 2020, doi: 10.1002/cta.2759.
14. S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," Int. Conf. Adv. Sustain. Eng. Appl. ICASEA 2018 - Proc., pp. 105–108, 2018, doi: 10.1109/ICASEA.2018.8370965.
15. C. A. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Elliptic Curve Lightweight Cryptography: A Survey," IEEE Access, vol. 6, pp. 72514–72550, 2018, doi: 10.1109/ACCESS.2018.2881444.
16. 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, p. 102159, 2020, doi: 10.1016/j.adhoc.2020.102159.
17. M. R. Hossain, M. S. Hossain, and Y. Kong, "Efficient FPGA Implementation of Unified Point Operation for Twisted Edward Curve Cryptography," 5th Int. Conf. Comput. Commun. Chem. Mater. Electron. Eng. IC4ME2 2019, pp. 1–4, 2019, doi: 10.1109/IC4ME247184.2019.9036635
18. Ding, S.; Li, C. ; Li, H. A novel efficient pairing-free CP-ABE based on elliptic curve cryptography for IoT. IEEE Access **2018**, 6, 27336–27345.
19. D. J. Bernstein and T. Lange, ``Faster addition and doubling on elliptic curves," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 4833. Heidelberg, Germany: Springer-Verlag, 2007, pp. 29_50.
20. E. Brier and M. Joye, ``Weierstraÿ elliptic curves and side-channel attacks," in Public Key Cryptography (Lecture Notes in Computer Science), vol. 2274. Heidelberg, Germany: Springer-Verlag, 2002, pp. 335_345.
21. H. Hisil, K. K. H. Wong, G. Carter, and E. Dawson, ``Twisted Edwards curves revisited," in Advances in Cryptology (Lecture Notes in Computer Science), vol. 4833. Heidelberg, Germany: Springer-Verlag, 2008, pp. 29_50.
22. M. M. Islam, M. S. Hossain, M. K. Hasan, M. Shahjalal, and Y. M. Jang, "FPGA Implementation of High-Speed Area-Efficient Processor for Elliptic Curve Point Multiplication over Prime Field," IEEE Access, vol. 7, pp. 178811–178826, 2019, doi: 10.1109/ACCESS.2019.2958491.
23. Edward, H.M. A normal form for elliptic curves. Bull. Am. Math. Soc. 2007, 44, 393–422.
24. Bernstein, D.J.; Lange, T. Faster addition and doubling on elliptic curves. In Proceedings of the Advances in Cryptology (LNCS); Springer: Heidelberg, Germany, 2007; Volume 4833, pp. 29–50.
25. Hisil, H.; Wong, K.K.H.; Carter G.; Dawson, E. Twisted edwards curves revisited. In Proceedings of the Advances in Cryptology (LNCS); Springer: Heidelberg, Germany, 2008; Volume 5350, pp. 326–343.
26. N. Koblitz, "Elliptic curve cryptosystems," Math. Comput., vol. 48, pp. 203–209, 1987.
27. Brian Baldwin, Richard Moloney, Andrew Byrne, Gary McGuire, and William P. Marnane-"A Hardware Analysis of Twisted Edward Curves for an Elliptic Curve Cryptosystem", A version of this paper appears in ARC 2009, the 5th International Workshop on Applied Reconfigurable Computing.
28. S. Asif, M. Hossain, Y. Kong, and W. Abdul, "A fully rns based ecc processor," Integration, the VLSI Journal, vol. 61, pp. 138–149, 3 2018.
29. P. M. Matutino, J. Ara´ujo, L. Sousa, and R. Chaves, "Pipelined fpga coprocessor for elliptic curve cryptography based on residue number system," in 2017 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS), 2017, pp. 261–268.
30. D.J. Bernstein, T. Lange, R.R. Farashahi, Binary Edwards Curves, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008, pp. 244–265, doi: 10.1007/ 978- 3- 540- 85053- 3 _ 16 .
31. E. Wenger, M. Hutter, Exploring the design space of prime field vs. binary field ECC-hardware implementations, in: Proceedings of the 16th Nordic Conference on Information Security Technology for Applications, NordSec'11, Springer- Verlag, Berlin, Heidelberg, 2012, pp. 256–271, doi: 10.1007/978- 3- 642- 29615- 4 _ 18 .
32. B. Koziel, R. Azarderakhsh, M. Mozaffari-Kermani, Low-resource and fast binary edwards curves cryptography, in: Springer International Publishing, Cham, 2015, pp. 347–369, doi: 10.1007/978- 3- 319- 26617- 6 _ 19 .
33. Salah Harb, M. Omair Ahmad and M. N. S. Swamy, "A Reconfigurable Implementation of Elliptic Curve Cryptography over GF (2n) ", ICETE 2019, CCIS 1247, pp. 87–107, 2020.
34. N. P. Kumar and C. Shirisha, "An area-efficient ECC architecture over GF(2m) for resource-constrained applications," AEU - Int. J. Electron. Commun., vol. 125, p. 153383, 2020, doi: 10.1016/j.aeue.2020.153383.
35. P. L. Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization," Math. Computing, Vol. 48 - pp. 243–264, 1987.
36. Rashidi B., Farashahi R. R. and Sayedi S. M., "High-Performance and High-Speed Implementation of Polynomial Basis Itoh-Tsujii Inversion Algorithm over GF(2m)," IET Information Security, Vol. 11, Iss. 2, pp. 66-77, 2017.
37. A. B. El-Sisi, S. M. M Shohdy, and N. Ismail, "Reconfigurable Implementation of Karatsuba Multiplier for Galois Field Elliptic Curves," Tarek Sobh, Khalid Ellithy, and Ausif Mahmood (Editors), Novel Algorithms and Techniques in Telecommunications and Networking, Springer Nature America, pp 87-92 Inc, 2010.
38. Nguyen TT, Lee H. Efficient algorithm and architecture for elliptic curve cryptographic processor. Journal of Semiconductor Technology and Science 2016; 16 (1): 118-25. doi: 10.5573/JSTS.2016.16.1.118
39. Hossain, M.S.; Kong, Y.; Saeedi, E.; Vayalil, N. High-performance elliptic curve cryptography processor over NIST prime fields. IET Comput. Digit. Tech. **2016**, 11, 33–42.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

40. A. Shah, K. Javeed, S. Azmat, and X. Wang, ``Redundant signed digit based high-speed elliptic curve cryptographic processor," J. Circuits Syst. Comput., vol. 28, no. 5, 2018, Art. no. 1950081.
41. Khan, Z.U., Benaissa, M," Throughput/area-efficient ECC processor using montgomery point multiplication on FPGA." IEEE Trans. Circuits Syst. II: Express Briefs **62**(11), 1078–1082 (2015)
42. Imran M, Rashid M, Jafri AR, Kashif M. Throughput/area optimised pipelined architecture for elliptic curve crypto processor. IET Computers & Digital Techniques. 2019 Feb 26;13(5):361-8.

AUTHORS PROFILE

Kirit V. Patel, He is currently working as an assistant professor in the Electronics and Communication (EC) department at L. D. College of Engineering, Gujarat, India. He is pursuing a Ph.D. degree from Gujarat Technological University. He has received MTech. degree in EC with a specialization in VLSI Design from the Institute of Technology, Nirma University in 2009. He has received BE degree from VNSGU, Gujarat in 2006. He has more than 12 years of teaching experience and published 10 research papers in International /National journals/conferences. His main area of research is cryptography and VLSI Front End design.

Dr. Mihir V. Shah, He is currently working as a professor and Head in the Electronics and Communication (EC) department at L. D. College of Engineering, Gujarat, India. He is awarded a Ph.D. degree from MSU, Baroda, Gujarat in 2009. He has received M.E. degree in EC from Malaviya Regional Engineering College Jaipur, Rajasthan in 2001. He has 4 years of industry experience and more than 24 years of teaching experience. He has published more than 30 research papers in International/National Journal / Conference. His main area of research is VLSI Front End design and CMOS analog design.