Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 739–758
DOI : 10.47974/JDMSC-1749

Pragmatic analysis of ECC based security models from an empirical perspective

Neha Purohit *
School of Computer Science
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

and

G H Raisoni College of Engineering
Nagpur
Maharashtra
India

Shubhalaxmi Joshi †
Milind Pande §
Dr. Vishwanath Karad MIT World Peace University
Pune
Maharashtra
India

Susan Lincke ‡
Director MSCIS Program
University of Wisconsin-Parkside
U.S.A.

* *E-mail:* **neha.purohit@raisoni.net (Corresponding Author)**
† *E-mail:* **shubhalaxmi.joshi@mitwpu.edu.in**
§ *E-mail:* **milind.pande@mitwpu.edu.in**
‡ *E-mail:* **lincke@uwp.edu**

Abstract

This paper provides a detailed discussion about currently proposed Elliptic Curve Cryptography (ECC) models focusing on performance parameters such as Security, Complexity, Scalability, and cost of deployment. It was observed that Machine Learning optimizations including bio inspired computing, deep learning, and transformation models outperform other techniques. This discussion is extended via an empirical estimation of these models related to the performance metrics under different application scenarios. This paper also proposes the calculation of an ECC Performance Metric (EPM), which combines the evaluated parameter sets to identify ECC Models that can perform better under multiple operating scenarios.

Subject Classification: *11G05, 11G07, 11G16, 11G20.*

Keywords: *ECC, Security, Curves, Scalability, Complexity, Delay, Cost, Performance, Scenarios.*

1. Introduction

Miller and Koblitz developed the concept that would eventually be known as Elliptic Curve Cryptography (ECC) in 1986 and 1987, respectively. Despite having substantially smaller key sizes [5], it is an asymmetric cryptographic system that offers security comparable to that offered by the well-known RSA [3] system. Elliptic curves are used to provide public-key encryption, which is based on the algebraic structure and function of a curve over a finite graph. This is accomplished by the use of a function called a trapdoor. In public-key cryptography, trapdoor functions are used to design a system in which travelling from point A to point B is straightforward yet impractical. This is achieved by making use of a particular mathematical puzzle. Numerous ECC optimization strategies have been put out in the literature, focusing either on binary extension fields, prime fields or dual field operations and bidirectional extension. The vast variety of potential values for the system parameters makes it difficult to build a design framework for ECC optimization method implementations and compare and assess the many ECC optimizers that have been suggested in the relevant literature. [12] Illustrates an accepted classification of ECC processor designs by many metrics to distinguish between the various ECC improvement approaches, including speed, scalability, and security. The four architectures they developed are as follows: Dedicated, Generator, Versatile and General Purpose [13–19]. Researchers conduct a literature review on ECC optimization approaches in this work and provide a resource for models that are used in successful ECC implementations. Researchers also provide a summary of the

research on ECC optimization. Their literature review is developed in the context of a procedural environment utilizing a bottom-up methodology. The survey begins by establishing a number of requirements, design considerations, and the impact those requirements, considerations, and influences have on a variety of distinct system components along with the many approaches and methods that may be employed to put machine learning to use. This article provides a thorough and well-organized examination of several ECC optimization algorithms that may be used in a range of application scenarios. In this paper, researchers assessed a variety of models based on the various values of the optimization parameters and other ECC optimization models that are relevant to the current issue and comes up to different conclusions.

2. Existing ECC optimization techniques – A survey

Researchers advocate a variety of ECC-based models, each of which has a unique set of internal operational characteristics. Researchers provide an attribute-based blind signature approach that uses ECC and show that it is secured despite the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) [1]. Their approach demands a significant reduction in computing and storage resources compared to attribute-based blind signature systems.

According to [2], the author done a rapid arithmetics on elliptic curves over finite fields using Residue Number Systems (RNS) for an Internet of things (IoT) applications and recommend an ECC core based on random number generators for concave Edwards curves and compact Weierstrass curves.

The elliptic curve scalar multiplication by the parameter k is particularly efficient, according to cyber security specialists [3]. In the suggested technique, the reseacher used the binary string k which is recoded and the multiplication operation is evaluated on the fly.

Security professionals from [4] suggested a new symmetric cryptosystem for uncompressed image encryption. In this case, an author uses BMP images from prying eyes and the outcomes of the performance study provide evidence for the suggested ABE system's effectiveness.

According to [6], have created image encryption that is resistant to chosen- ciphertext and chosen-plain text attacks using the dynamic S-box and discovered that the suggested method of image encryption is more secure than the most recent alternatives. The suggested approach is capable of 60 MB/s of encryption performance.

An image encryption method based on isomorphic elliptic curves that was developed by cryptography experts [7] . The suggested technique uses Kobltiz to convert common images into points on an elliptic curve, and leads to the cipher text becoming disordered.

As per [8], for the protection of sensitive data, they construct a reconfigurable cryptosystem that makes use of ECC on FPGA to safeguard data streams by multiplying and adding points on a Koblitz Elliptic Curve (KEC) to achieve ElGamal public-key encryption.

The author [9] describe a theft attempt against ECC. Elliptic Curve Digital Signature Algorithm (ECDSA), Elliptic Curve Integrated Encryption System, Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE), ElGamal Encryption and Elliptic Curve Qu-Vanstone implicit certificate technique backdoor insertion are all highlighted in depth by researchers. Researchers changed the Edwards-backdoor curve's methodology, and using a cryptographic technique for digital signatures hides backdoors to compare the execution durations and malicious programs in order to find a backdoor.

According to [10], researchers created random numbers for ECC using fuzzy logic, which enhances encryption and authentication in IoT devices. As per [11], The author has led to the creation of a simple and flexible authentication technique for use in automotive data transmission. The proposed protocol uses a variety of lightweight operations, including Concatenation, XOR, and Hashing (CRH). AVISPA does a security study of this approach. An experimental assessment results in a solution time of 7.96 seconds and an 834-bit data transmission rate.

According to [12], the author presents a 6CC-6CC (clock cycle) dual-field PM design as well as a 6CC-4CC dual-field PM design in order to provide parallel processing and a more effective use of resources. Both designs rely on the processing capability of Xilinx Virtex-5 and Virtex-7 FPGAs. Applications in the actual world demonstrate that the suggested designs work well and are adaptable enough to be employed in ECC setups.

An Elliptic curve-based paradigm for the secure storage and transmission of colour and grayscale images was proposed by the author [13]. With an average entropy of 7.9993 for grayscale and 7.99925 for colour, this model's ECDH and ElGamal session key generates good cypher pictures. For both colour and black-and-white images, the model shows a good NPCR (99.6%) and a low correlation, and it uses less processing power and resources by limiting the number of point multiplication operations.

As per [14] presented a novel hybrid methodology for isogeny-based cryptosystems based on Edwards Curves (EDC) . He utilized Montgomery curves to extract curve coefficients, while Edwards curves are employed for a number of different functions and drawn to the conclusion that their approach is much faster than the hybrid one.

An ECC processor designed to safeguard the IoT while utilizing little power is purportedly examined by security researchers in [15], to minimize power and energy use. In order to decrease both storage and power needs, the suggested ECPM approach uses the Signed Binary Representation (SBR) in combination with the m-ary strategy which results in less wasted space and power.

Due to its shorter key and improved security, elliptic curve cryptosystem is well-liked and used in wireless sensor networks. According to [16] develop k for scalar multiplication kP, which accelerates the scalar multiplication technique, using the triple-based chain foundation of 2,3,7. Using Co Z in the Septuple Elliptic Curve (CZ SEC) formula results in a save of 8.3%. The approach is resistant to side channel assaults because of the inherent resilience of the triple-based chain.

The pros and cons of using Huff curves in isogeny-based encryption are discussed in [17]. To retrieve the curve coefficient from a particular Huff curve point for SIDH, the author provide a novel formula by using Edwards curves to get the image curve coefficient and Huff curves to apply the Square-root Vélu (SV) formula. Although the outcomes of Huff-SIDH and Montgomery-SIDH are equivalent, Huff-CSIDH is 6 percentage points faster.

According to [18] suggest a Block-Based Elliptic Curve (BBEC) public key encryption is used as the initial encryption phase in the strategy to tackle the symmetric key distribution and management issue and conclude that the suggested strategy is quicker and safer than other alternatives. The features include resistance to statistical, differential, and noise assaults, a wide key space, altering pixel values depending on the key, and low correlation.

According to [19], a reseacher provides a hybrid method to exchange secret keys and cloak communications between a sender and reciever by introducing a complex chaotic 2D map with strong positive Lyapunov Exponents (LE) and combining the chaotic pseudo-orbits of the proposed map with elliptic curves in public key cryptography which results resilience against attacks.

Work carried out by [20] a hardware implementation of modular multiplication over five NIST-recommended prime fields for lightweight

ECC is provided. Conducting interleaved modular multiplication takes less time if you use the Modified Radix-2 Interleaved Method (MRIM). Implementations on Virtex-6, Virtex-5, and Virtex-4 FPGAs demonstrate that the proposed design significantly outperforms past techniques of modular multiplication in terms of hardware resource usage and area-delay product.

The ECC-based Ant Colony Optimisation Adhoc was recommended by research by [21]. When messages are distributed across the Internet of Vehicles (IoV), the On-demand Distance Vector (ACO-AODV) routing protocol helps drivers avoid questionable vehicles. An ACO-AODV-based secure route selection that stays clear of hostile vehicles and is based on the goal of communications. A trust level calculated from status message exchanges underlies the Malicious Vehicle (MV) detection technique. Their process is comprised of these three parts. Experiments demonstrate that the proposed approach outperforms state-of-the-art methods.

According to [22], The authors of this article propose a novel authentication approach by using Burrows-Abadi-Needham (BAN) logic, the suggested method's mutual authentication in order to ensure the secrecy of communications and increase their effectiveness. The proposed approach uses just point-additive ECC for communication signature and verification. Their suggested solution has less computational cost than prior ones as it does not use ECC-based point multiplication.

The author [23], discusses digital data encryption and makes use of an underlying substitution-permutation network by using a pair of Bijective Maps (BiM) form the basis of the method. This approach uses elliptic curves to provide safe containers for cryptographic data. The most perplexing image data has been replaced with created replacement boxes to eliminate any ambiguity. The suggested method uses little CPU resources and could be able to encrypt images in real time.

As per [24], Researchers look into group extensions of a popular key exchange protocol, the elliptic curve variation of the Diffie-Hellman protocol, using the NIST-standardized elliptic curve and Four Q curve. Automotive-grade ARM and Infineon processors are used to build and test protocols. Researchers employ CAN and CAN-FD as their communication platform in this cutting-edge study. When dealing with elliptic curves, processing time matters more than bandwidth.

The researchers created [25] Certificateless Elliptic Curve Aggregate Signcryption (CL-ECASC) for the IoT to increase authentication efficiency, safeguard private data from prying eyes, and do away with time-consuming processes like certificate maintenance and key escrow. On

elliptic curves, CL-ECASC offers protection against computational Diffie-Hellman difficulties and discrete logarithm problems which results into quicker calculation efficiency and cheaper transmission costs.

According to [26], In this paper, researchers rediscover the Montgomery reduction for NIST primes and offer a new modular reduction strategy by providing an effective ECC coprocessor over NIST prime fields using this novel modular reduction mechanism and other optimization methods. In compared to earlier investigations, the recommended coprocessor is relatively quick, with a 194.7 k gate count and a multiplicative time of 0.055 milliseconds for elliptic curve points.

Using the Symmetric Cryptosystem of the Elliptic Curve (SCEC), encrypted integers may withstand up to 40% of damage, according to [27]. SCEC uses chaos to build a nonlinear 88 S-box to fight against linear attacks by adding a random permutation step before encryption for security. Occlusion noise, Gaussian noise, additive noise, and multiplicative noise were all applied to encrypted images for assessment. The testing outcomes show the superior calibre of SCEC's cryptographic features but provide extra noise protection for encrypted images.

The author [28], in this paper provides an RFID authentication technique that is based on the hyperelliptic curve Signcryption (RFID-AS). The RFID-AS offers protection against system flaws and assaults and validated the security of RFID-AS using the Automated Validation of Internet Security Protocols and Applications (AVISPA) and Real-Or-Random (ROR) paradigm. The efficiency of their method's compute overhead is 70%, its communication overhead is 42.7 percent, and its storage overhead is 57.3 percent.

According to [29] research, to deploy a large field-size ECC is more challenging. The authors of this paper provide a novel PM strategy for enhancing signal throughput and resource productivity. The results demonstrate the large field-size ECC processor's suitability for use in a variety of high-security activities.

According to [30], the authors have developed DPF-ECC, a broad framework for speeding ECC algorithms across the prime field by using DPF processing capability, to solve the drawbacks of integer-based approaches. Researchers created the well-known ECC schemes Curve25519/448 and Edwards25519/448, which are used in TLS 1.3, SSH, and other protocols, to assess the proposed DPF-ECC framework in reality. The DPF-ECC framework is a strong contender for ECC implementation in practical reality since it just requires the widely used IEEE 754 floating point standard.

The Researchers [31] provide a cryptographic-based ECC-enabled RFID mutual authentication method for IoV. The proposed protocol consists of three steps: setup, tagging, and the server. The suggested protocol consider costs of compute, communication, and storage and provides high performance metrics . To dramatically strengthen network security for the IoV, a Blockchain-based RFID-enabled IoV security architecture has been developed.

In order to decrease the processing time required for scalar multiplication, kP, a high-performance S-ECIES crypto processor is proposed in [32]. A Montgomery Ladder Scalar Multiplier (MLSM) was built in the crypto processor using Gaussian normal bases and random curves over GF (2163) and GF (3163), (2233). For GF (2 163) and GF (2 233), decryption takes 8.10 and 11.9 seconds, but encryption takes 20.70 and 30.90 seconds.

Work carried out by [33] claimed that, a Wireless Body Area Network (WBAN) system called Technology for Medical Information Systems (TMIS) may help with remote healthcare delivery and entails the open exchange of private patient data. The author suggest merging biometric and ECC mutual authentication by using a three-factor mutual authentication system for TMIS that is based on ECC. Compared to other protocols of a similar kind now in use, theirs is more secure and has reduced communication costs.

The researchers [34] provide a deep learning-based technique for high-capacity image steganography, to make the secret image more difficult to decipher, by using DCT and then encrypted with ECC. The results of the experiments demonstrate that the technique can successfully assign each pixel, resulting in a steganographic capacity of 1. The steganography image's PSNR and SSIM values, 40 dB and 0.96 dB, are much greater than the baseline.

Researchers [35] provides a conditional, low-overhead authentication mechanism for Vehicular Ad hoc Networks (VANET) that protects privacy. The proposed approach, which is based on ECC, substitutes an initial public parameter and key into each RSU for the on-border unit TPD. The effectiveness of the suggested technique has been assessed, and the results demonstrate that it is more efficient than traditional ways in terms of calculation and communication time and cost.

Reduces computational complexity and improves hardware implementations are two benefits of Binary Ring -LWE (BRLWE) [36]. In this study, two effective designs for Inverted Binary Ring -LWE (INV BRLWE)-based encryption are proposed, with a particular focus on the

operation of AB+C over the polynomial ring Zq/(xn+1). Experimental findings demonstrate that the provided topologies greatly reduce area-delay product by 71.23 percent when compared to traditional techniques. Both solutions are suited for use in low-weight software since they are both time and space economical.

The article develops a safe ECDSA [37] , which may be impervious to the weak randomness attack used by ECDSA against Bitcoin and may be integrated into blockchain-based digital currency trading platforms, that eliminates the need for the inverse procedure of signature and verification. ECDSA is 51% slower than the other existing techniques.

According to study [38], the ECC point multiplication algorithm is provides a high-performance design for ECC over Curve448 uses a Karatsuba formula for an asymmetric digit multiplier that works well with asymmetric DSP primitives.It decreases the number of necessary DSPs while preserving performance by using pipelining and parallelization. In terms of Area Time, the suggested plan is 63% more efficient. The study ends with a number of side-channel defenses, such as continuous randomization, base-point randomization, and scalar blindness.

According to [39] research, a Flying Ad-hoc Network (FANET) consists of Unmanned Aerial Vehicles (UAVs) responsible for multi-hop ad-hoc communication. The authors of this work provide instructions for building a CL-KESC that uses Hyperelliptic Curve Encryption (HECC) and the key size is 80 bits as opposed to an elliptic curve's 160 bits. The suggested solution was shown to be more secure and to perform better overall in performance studies comparing it to current options.

According to [40], Researchers provide a technique for encrypting chaotic images that accelerates the production of chaotic sequences by taking use of pixel-level parallelism over points on an elliptic curve are used to produce a chaotic sequence with discrete structure. The suggested solution performs better than EC-based image encryption methods in terms of efficiency. Through tests on a quad-core CPU, the suggested strategy has been demonstrated to increase the efficiency of parallelization, producing a 3.93 speedup.

In order to address the issues with the Evolved Packet System Authentication and Key Agreement Protocol (EPS-AKA) that plague LTE networks, the author proposes [41] a Group Security Authentication and Key Agreement Protocol Built by ECDHKE (GSAKA-ECDHKE). To generate and disperse secret EC keys for encrypting and securing routing authentication parameters, GSAKA-ECDHKE makes use of ECDHKE

and a hash function. The proposed technique requires less time for communication.

When calculating point addition and doubling on an elliptic curve, the unified point addition rule prevents information leakage through a side channel, as stated in [42]. The paradigm of Binary Huff Curves (BHC) provides a consistent point-addition elliptic curve framework. With this new unified BHC method, researchers have improved side-channel security by adding new unified point addition methods with higher clock frequencies and throughput.

The literature presents several security strategies for IoT, some of which are multi-factor authentication systems. This paper provides the first independent evaluation of Kumari et al. ESEAP [43] system's security. To further strengthen security, researchers propose the RESEAP protocol in the second phase.When compared to ESEAP, RESEAP is far more secure and effective.

The use of Chaotic Maps (CM) for multiple-image encryption was proposed by experts [44]. The outcomes of the experiments demonstrate the effectiveness, security, and speed of the proposed method. The proposed method is more reliable and productive than alternatives.

Accoding to study, Researchers [45] developed a safe ECC (SECC) based authentication technique for Internet-of-Drones (IoD) over FANET. The efficiency and effectiveness of the proposed security mechanism is shown by a comparison with state-of-the-art methodologies, demonstrating that the work presented in this paper is suitable for application in the IoD.

This study [46] fills a knowledge vacuum by introducing parking recommendation systems based on LDP and ECC. Researchers proposed HMAC as an alternative to ECC for providing privacy and security in online interactions. Their research demonstrates that their proposed method requires very little more space for storage, calculation, or transmission.

In some approaches, the public key of the utility supplier is used to encrypt data on energy use, which the utility supplier can then decrypt if it obtains the encrypted data. A Modular Elliptic-Based (MECC) multidimensional data aggregation method was recommended by researchers for the smart grid [47]. A different key is given to the metre if the electrical company is unable to decrypt the meter's readings. Meters may now provide multiple types of data simultaneously due to the proposed method's scalability.

A researchers [48] proposed a system for secure and fast authentication for cloud-assisted SMS using ECC for Common Services and Entities Framework (CSEF). The ECC and hash function used by CSEF allow for

secure two-way authentication between healthcare providers and the cloud. The CSEF is more effective in both computing and communication than its competitors.

According to [49] studies, in order to protect the IoT, researchers develop the idea of One-Time Passwords (OTPs) and provide an OTP generating technique that utilizes ECC and isogeny. The author evaluate their method against two others, one based on a hash message authentication code and another on the passage of time. Proof of the safety and effectiveness of their method is shown by its performance outcomes.

Work carried out by [50] focuses on four main metrics: mistake rate, throughput, categorization accuracy, and security. As a result, it is clear that researchers have proposed a wide range of ECC models, each of which differs in terms of its internal operating characteristics. To choose the best ECC models for particular security deployments, the next section compares the models' encryption and decryption delays, computational complexity, deployment cost, security level, and scalability levels.

According to [51] , in order to maintain confidentiality and authentication of data for military use, the idea of ECC and Identity Based Public Key Cryptography, this author suggests a certificate less asymmetric key based cryptographic technique. By doing away with the necessity for a digital signature or certificate, the suggested solution improves efficiency in terms of decreasing the time required for encryption and decryption.

For the military heterogeneous wireless sensor network (MHTWSN), a researcher [52] suggested a unique secure multipath routing protocol (NSRP) to ensure secure data transfer. To identify trusted neighbour nodes in the MHTWSN and create secure multiple paths for dependable data transmission, NSRP uses ECC. The protocol offers a reliable key management system that improves security and network performance. Compared to previous key management systems, NSRP has reduced communication overhead, memory requirements, and energy consumption.

To lessen the complexity at the client side, a researcher [54] introduces a lightweight authentication protocol solution for WBAN based on ECC. Researchers have enhanced mutual authentication, session key security, forward security, and computational and storage costs with this new, unified approach.Security study has shown that the real protocol is secure under the Dolev-Yao attack scenario using game-based evidence and AVISPA.

Results analysis and comparison

To help readers choose the best models for their application-specific use cases, the reviewed models are compared in terms of various empirical characteristics, such as encryption and decryption delays (EDD), computational complexity (CC), cost of deployment (CD), security level (Se), and scalability (Sc) levels. The measurements' values were transformed into fuzzy performance level ranges of Very High (VH), High (H), Medium (M), and Low (L). The performance of the reviewed models is summarised in table 1 using this method as follows:

Based on this performance evaluation, it can be observed that BBEC [18], LE ECC [19], BiM ECC [23], and QECC [24] showcase low computational complexity levels. Thus, they can be used for application use cases that require low complexity operations. It can also be observed that BP ECC [5], SV ECC [17], BiM ECC [23], and HECC [28] showcase lower deployment cost, thereby making them highly useful for low-cost network deployment use cases.

It was also observed that CRH [11], SETUP [9], SV ECC [17], LE ECC [19], BiM ECC [23], and SCEC [27] showcase lower encryption & decryption delays, thus making them useful for high-speed network application scenarios. In terms of security levels, Kobltiz ECC [7], CRH [11], MRIM ECC [20], BAN ECC [22], BiM ECC [23], QECC [24], RLWE ECC [36], and GS AKA ECDH KE [41] showcase better performance, thus can be used for high-security application deployments. While, in terms of scalability levels, CRH [11], ACM [13], BiM ECC [23], NIST ECC [26], SCEC [27], ECDLP [37], and CSEF ECC [48] are capable of achieving better performance, thus can be used for large-scale deployments. These metrics were combined to form an ECC Performance Metric (EPM), which was evaluated via equation 1,

$$EPM = \frac{1}{CC} + \frac{1}{CD} + \frac{1}{EDD} + \frac{Se+Sc}{5} \quad ...(1)$$

Based on this evaluation, it can be observed that BiM ECC [23], CRH [11], QECC [24], SCEC [27], BP ECC [5], SV ECC [17], LE ECC [19], RLWE ECC [36], HECC [28], Kobltiz ECC [7], and ECDLP [37] showcase lower complexity, lower cost, lower delay, with high security and high scalability, thereby making them useful for a wide variety of real-time use cases

Table 1
Performance analysis of different ECC Models

Sr. No.	ECC Model	CC	CD	EDD	Se	Sc	Sr. No.	ECC Model	CC	CD	EDD	Se	Sc
1	ECDLP [1]	H	M	H	H	M	23	MLSM ECC [32]	VH	M	H	H	L
2	ECPT [2]	H	M	H	H	M	24	DCT ECC [34]	H	H	VH	H	H
3	RK FND [3]	VH	H	VH	H	H	25	RLWE ECC [36]	M	H	H	VH	H
4	CDE [4]	H	H	VH	H	L	26	ECDLP [37]	H	M	VH	H	VH
5	BP ECC [5]	M	L	H	H	H	27	MLS ECC [38]	H	M	H	H	H
6	HM ECC [6]	M	H	H	H	H	28	CL PKC [39]	M	H	VH	H	M
7	KobltizECC [7]	H	M	VH	VH	H	29	GSAKA ECDH KE [41]	H	H	VH	VH	H
8	KEC [8]	H	VH	H	H	M	30	BHC ECC [42]	H	H	VH	H	H
9	SETUP [9]	H	H	M	H	H	31	RES EAP [43]	M	H	H	H	M
10	ADFTECC [10]	H	H	H	M	H	32	CM ECC [44]	H	M	VH	H	H
11	CRH [11]	M	M	L	VH	VH	33	SECC [45]	H	H	VH	H	H
12	ACM [13]	H	H	H	H	VH	34	LDP ECC [46]	M	H	VH	H	M
13	EdC [14]	H	H	H	H	H	35	MECC [47]	H	M	VH	H	H
14	SPA ECC [15]	M	VH	H	H	M	36	CSEF ECC [48]	H	H	H	H	VH
15	CZ SEC [16]	H	M	H	H	L	37	LEC DS [50]	M	H	VH	H	H
16	SV ECC [17]	H	L	M	H	H	38	QECC [24]	L	H	H	VH	H
17	BBEC [18]	L	H	H	H	M	39	CLEC ASC [25]	H	H	H	H	H
18	LE ECC [19]	L	H	M	H	H	40	NIST ECC [26]	H	H	H	H	VH
19	MRIMECC [20]	M	H	VH	VH	M	41	SCEC [27]	H	M	M	H	VH
20	ACOECC [21]	H	M	VH	H	H	42	HECC [28]	H	L	H	H	H
21	BANECC [22]	H	H	VH	VH	H	43	MPM ECC [29]	H	M	H	H	M
22	BiMECC [23]	L	L	M	VH	VH	44	DPF ECC [30]	H	H	VH	H	H

3. Conclusion and Future scope

This study analyses and contrasts a wide range of ECC models with regard to the internal working characteristics of the models under a number of different conditions. This paper provides a comparison of various ECC models in terms of their encryption and decryption delays, computational complexity, cost of deployment, level of security, and scalability levels

to assist in the selection of optimal ECC models for various security deployments. The result yields that BBEC, LE ECC, BiM ECC, and QECC all exhibit low levels of computational complexity and thus are suitable for usage in application use cases that call for processes of modest complexity. Due to their low costs of deployment, BP ECC, SV ECC, BiM ECC, and HECC are well-suited for use cases that include the development of low-cost networks. Also, it was found that CRH, SETUP, SV ECC, LE ECC, BiM ECC, and SCEC had shorter times required for encryption and decryption, which makes them suitable for usage in situations involving high-speed network application scenarios. Performance-wise, Kobltiz ECC, CRH, MRIM ECC, BAN ECC, BiM ECC, QECC, RLWE ECC, and GS AKA ECDH KE are superior to Kobltiz ECC, MRIM ECC, BAN ECC, and BiM ECC and thus they find place in high-security application deployments. Based on the comparison, it is realized that BiM ECC, CRH, QECC, SCEC, BP ECC, SV ECC, LE ECC, RLWE ECC, HECC, Kobltiz ECC, and ECDLP showcase lower complexity, lower cost, and lower delay, along with high security and high scalability, which makes them useful for a wide variety of real-time use cases. In future, these models will need to be evaluated on a variety of application scenarios, and can be expanded with the use of machine learning optimizations for different ECC curves. This performance can also be optimized by using pattern-learning deep nets, which will help in selecting the ideal parameter section for deployment use cases that are context-specific under different application sets.

References

[1] R. Ma and L. Du, "Attribute-Based Blind Signature Scheme Based on Elliptic Curve Cryptography," in *IEEE Access*, Vol. 10, pp. 34221-34227 (2022), doi: 10.1109/ACCESS.2022.3162231.

[2] M. A. Mehrabi, C. Doche and A. Jolfaei, "Elliptic Curve Cryptography Point Multiplication Core for Hardware Security Module," in *IEEE Transactions on Computers*, Vol. 69, No. 11, pp. 1707-1718 (1 Nov. 2020), doi: 10.1109/TC.2020.3013266.

[3] A. K. Oudjida and A. Liacha, "Radix-2w Arithmetic for Scalar Multiplication in Elliptic Curve Cryptography," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 68, No. 5, pp. 1979-1989, (May 2021), doi: 10.1109/TCSI.2021.3054781.

[4] E. A. Hernández Díaz, H. M. Pérez Meana and V. M. Silva García, "Encryption of RGB Images by Means of a Novel Cryptosystem using

Elliptic Curves and Chaos," in *IEEE Latin America Transactions*, Vol. 18, no. 08, pp. 1407-1415 (August 2020), doi: 10.1109/TLA.2020.9111676.

[5] K. Sowjanya, M. Dasgupta, S. Ray and M. S. Obaidat, "An Efficient Elliptic Curve Cryptography-Based Without Pairing KPABE for Internet of Things," in *IEEE Systems Journal*, Vol. 14, No. 2, pp. 2154-2163 (June 2020), doi: 10.1109/JSYST.2019.2944240.

[6] S. Ibrahim and A. Alharbi, "Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography," in *IEEE Access*, Vol. 8, pp. 194289-194302 (2020), doi: 10.1109/ACCESS.2020.3032403.

[7] I. Khalid, S. S. Jamal, T. Shah, D. Shah and M. M. Hazzazi, "A Novel Scheme of Image Encryption Based on Elliptic Curves Isomorphism and Substitution Boxes," in *IEEE Access*, Vol. 9, pp. 77798-77810 (2021), doi: 10.1109/ACCESS.2021.3083151.

[8] 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.

[9] A. Sajjad, M. Afzal, M. M. W. Iqbal, H. Abbas, R. Latif and R. A. Raza, "Kleptographic Attack on Elliptic Curve Based Cryptographic Protocols," in *IEEE Access*, Vol. 8, pp. 139903-139917 (2020), doi: 10.1109/ACCESS.2020.3012823.

[10] A. Abdaoui, A. Erbad, A. K. Al-Ali, A. Mohamed and M. Guizani, "Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things," in *IEEE Internet of Things Journal*, Vol. 9, No. 12, pp. 9987-9998 (15 June15, 2022) doi: 10.1109/JIOT.2021.3121350.

[11] S. Velliangiri et al., "An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography," in *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 9, pp. 6494-6502 (Sept. 2022), doi: 10.1109/TII.2021.3139609.

[12] J. Li, W. Wang, J. Zhang, Y. Luo and S. Ren, "Innovative Dual-Binary-Field Architecture for Point Multiplication of Elliptic Curve Cryptography," in (IEEE Access), Vol. 9, pp. 12405-12419 (2021), doi: 10.1109/ACCESS.2021.3051282.

[13] P. Parida, C. Pradhan, X. -Z. Gao, D. S. Roy and R. K. Barik, "Image Encryption and Authentication With Elliptic Curve Cryptography

and Multidimensional Chaotic Maps," in *IEEE Access*, Vol. 9, pp. 76191-76204 (2021), doi: 10.1109/ACCESS.2021.3072075.

[14] S. Kim, K. Yoon, J. Kwon, Y. -H. Park and S. Hong, "New Hybrid Method for Isogeny-Based Cryptosystems Using Edwards Curves," in *IEEE Transactions on Information Theory*, Vol. 66, No. 3, pp. 1934-1943 (March 2020), doi: 10.1109/TIT.2019.2938984.

[15] L. -Y. Yeh, P. -J. Chen, C. -C. Pai and T. -T. Liu, "An Energy-Efficient Dual-Field Elliptic Curve Cryptography Processor for Internet of Things Applications," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 67, No. 9, pp. 1614-1618 (Sept. 2020), doi: 10.1109/TCSII.2020.3012448.

[16] S. Liu and L. Zhang, "Efficient Septuple Formula for Elliptic Curve and Efficient Scalar Multiplication Using a Triple-Base Chain Representation," in *IEEE Access*, Vol. 9, pp. 129512-129520 (2021), doi: 10.1109/ACCESS.2021.3113792.

[17] S. Kim, "Complete Analysis of Implementing Isogeny-Based Cryptography Using Huff Form of Elliptic Curves," in *IEEE Access*, Vol. 9, pp. 154500-154512 (2021), doi: 10.1109/ACCESS.2021.3128515.

[18] R. I. Abdelfatah, "Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography," in *IEEE Access*, Vol. 8, pp. 3875-3890 (2020), doi: 10.1109/ACCESS.2019.2958336.

[19] A. Al-Khedhairi, A. Elsonbaty, A. A. Elsadany and E. A. A. Hagras, "Hybrid Cryptosystem Based on Pseudo Chaos of Novel Fractional Order Map and Elliptic Curves," in *IEEE Access*, Vol. 8, pp. 57733-57748 (2020), doi: 10.1109/ACCESS.2020.2982567.

[20] M. M. Islam, M. S. Hossain, M. Shahjalal, M. K. Hasan and Y. M. Jang, "Area-Time Efficient Hardware Implementation of Modular Multiplication for Elliptic Curve Cryptography," in *IEEE Access*, Vol. 8, pp. 73898-73906 (2020), doi: 10.1109/ACCESS.2020.2988379.

[21] S. Safavat and D. B. Rawat, "On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities," in *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 8, pp. 5050-5059 (Aug. 2021), doi: 10.1109/TITS.2020.3008361.

[22] J. S. Alshudukhi, B. A. Mohammed and Z. G. Al-Mekhlafi, "Conditional Privacy-Preserving Authentication Scheme Without Using Point Multiplication Operations Based on Elliptic Curve

Cryptography (ECC)," in *IEEE Access*, Vol. 8, pp. 222032-222040 (2020), doi: 10.1109/ACCESS.2020.3044961.

[23] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi and A. R. Alharbi, "Construction of S-Boxes Using Different Maps Over Elliptic Curves for Image Encryption," in *IEEE Access*, Vol. 9, pp. 157106-157123 (2021), doi: 10.1109/ACCESS.2021.3128177.

[24] A. Musuroi, B. Groza, L. Popa and P. -S. Murvay, "Fast and Efficient Group Key Exchange in Controller Area Networks (CAN)," in *IEEE Transactions on Vehicular Technology*, Vol. 70, No. 9, pp. 9385-9399 (Sept. 2021), doi: 10.1109/TVT.2021.3098546.

[25] H. Yu and R. Ren, "Certificateless Elliptic Curve Aggregate Signcryption Scheme," in *IEEE Systems Journal*, Vol. 16, No. 2, pp. 2347-2354 (June 2022), doi: 10.1109/JSYST.2021.3096531.

[26] P. Choi, M. -K. Lee and D. K. Kim, "ECC Coprocessor Over a NIST Prime Field Using Fast Partial Montgomery Reduction," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 68, No. 3, pp. 1206-1216 (March 2021), doi: 10.1109/TCSI.2020.3039753.

[27] V. M. Silva-García, R. Flores-Carapia, M. D. González-Ramírez, E. Vega-Alvarado and M. G. Villarreal-Cervantes, "Cryptosystem Based on the Elliptic Curve With a High Degree of Resistance to Damage on the Encrypted Images," in *IEEE Access*, Vol. 8, pp. 218777-218792 (2020), doi: 10.1109/ACCESS.2020.3042475.

[28] U. Ali et al., "RFID Authentication Scheme Based on Hyperelliptic Curve Signcryption," in *IEEE Access*, Vol. 9, pp. 49942-49959 (2021), doi: 10.1109/ACCESS.2021.3069429.

[29] C. -Y. Lee, M. Zeghid, A. Sghaier, H. Y. Ahmed and J. Xie, "Efficient Hardware Implementation of Large Field-Size Elliptic Curve Cryptographic Processor," in *IEEE Access*, Vol. 10, pp. 7926-7936 (2022), doi: 10.1109/ACCESS.2022.3141104.

[30] L. Gao et al., "DPF-ECC: A Framework for Efficient ECC With Double Precision Floating-Point Computing Power," in *IEEE Transactions on Information Forensics and Security*, Vol. 16, pp. 3988-4002 (2021), doi: 10.1109/TIFS.2021.3098987.

[31] S. Sharma, B. Kaushik, M. K. I. Rahmani and M. E. Ahmed, "Cryptographic Solution-Based Secure Elliptic Curve Cryptography Enabled Radio Frequency Identification Mutual Authentication

Protocol for Internet of Vehicles," in *IEEE Access*, Vol. 9, pp. 147114-147128 (2021), doi: 10.1109/ACCESS.2021.3124209.

[32] P. Realpe-Muñoz, J. Velasco-Medina and G. Adolfo-David, "Design of an S-ECIES Cryptoprocessor Using Gaussian Normal Bases Over GF(2m)," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 29, No. 4, pp. 657-666 (April 2021), doi: 10.1109/TVLSI.2021.3057985.

[33] J. Ryu et al., "Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System," in *IEEE Access*, Vol. 10, pp. 11511-11526 (2022), doi: 10.1109/ACCESS.2022.3145959.

[34] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, "A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," in *IEEE Access,* Vol. 8, pp. 25777-25788 (2020), doi: 10.1109/ACCESS.2020.2971528.

[35] J. S. Alshudukhi, Z. G. Al-Mekhlafi and B. A. Mohammed, "A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography," in *IEEE Access*, Vol. 9, pp. 15633-15642 (2021), doi: 10.1109/ACCESS.2021.3053043.

[36] J. L. Imaña, P. He, T. Bao, Y. Tu and J. Xie, "Efficient Hardware Arithmetic for Inverted Binary Ring-LWE Based Post-Quantum Cryptography," in *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 69, No. 8, pp. 3297-3307 (Aug. 2022), doi: 10.1109/TCSI.2022.3169471.

[37] S. -G. Liu, W. -Q. Chen and J. -L. Liu, "An Efficient Double Parameter Elliptic Curve Digital Signature Algorithm for Blockchain," in *IEEE Access*, Vol. 9, pp. 77058-77066 (2021), doi: 10.1109/ACCESS.2021.3082704.

[38] A. M. Awaludin, J. Park, R. W. Wardhani and H. Kim, "A High-Performance ECC Processor Over Curve448 Based on a Novel Variant of the Karatsuba Formula for Asymmetric Digit Multiplier," in *IEEE Access*, Vol. 10, pp. 67470-67481 (2022), doi: 10.1109/ACCESS.2022.3184786.

[39] M. A. Khan et al., "An Efficient and Provably Secure Certificateless Key-Encapsulated Signcryption Scheme for Flying Ad-hoc Network," in *IEEE Access*, Vol. 8, pp. 36807-36828 (2020), doi: 10.1109/ACCESS.2020.2974381.

[40] A. M. Abbas, A. A. Alharbi and S. Ibrahim, "A Novel Parallelizable Chaotic Image Encryption Scheme Based on Elliptic Curves," in *IEEE Access*, Vol. 9, pp. 54978-54991 (2021), doi: 10.1109/ACCESS.2021.3068931.

[41] K. H. Moussa, A. H. El-Sakka, S. Shaaban and H. N. Kheirallah, "Group Security Authentication and Key Agreement Protocol Built by Elliptic Curve Diffie Hellman Key Exchange for LTE Military Grade Communication," in *IEEE Access*, Vol. 10, pp. 80352-80364 (2022), doi: 10.1109/ACCESS.2022.3195304.

[42] M. Rashid, M. Imran, M. Kashif and A. Sajid, "An Optimized Architecture for Binary Huff Curves With Improved Security," in *IEEE Access*, Vol. 9, pp. 88498-88511 (2021), doi: 10.1109/ACCESS.2021.3090216.

[43] M. Safkhani, N. Bagheri, S. Kumari, H. Tavakoli, S. Kumar and J. Chen, "RESEAP: An ECC-Based Authentication and Key Agreement Scheme for IoT Applications," in *IEEE Access*, Vol. 8, pp. 200851-200862 (2020), doi: 10.1109/ACCESS.2020.3034447.

[44] D. S. Laiphrakpam, R. Thingbaijam, K. M. Singh and M. Al Awida, "Encrypting Multiple Images With an Enhanced Chaotic Map," in *IEEE Access*, Vol. 10, pp. 87844-87859 (2022), doi: 10.1109/ACCESS.2022.3199738.

[45] S. U. Jan, I. A. Abbasi, F. Algarni and A. S. Khan, "A Verifiably Secure ECC Based Authentication Scheme for Securing IoD Using FANET," in *IEEE Access*, Vol. 10, pp. 95321-95343 (2022), doi: 10.1109/ACCESS.2022.3204271.

[46] A. A. Khaliq, A. Anjum, A. B. Ajmal, J. L. Webber, A. Mehbodniya and S. Khan, "A Secure and Privacy Preserved Parking Recommender System Using Elliptic Curve Cryptography and Local Differential Privacy," in *IEEE Access*, Vol. 10, pp. 56410-56426 (2022), doi: 10.1109/ACCESS.2022.3175829.

[47] Y. Chen, J. -F. Martínez-Ortega, P. Castillejo and L. López, "An Elliptic Curve-Based Scalable Data Aggregation Scheme for Smart Grid," in *IEEE Systems Journal*, Vol. 14, No. 2, pp. 2066-2077 (June 2020), doi: 10.1109/JSYST.2019.2954080.

[48] A. Kumari, V. Kumar, M. Y. Abbasi, S. Kumari, P. Chaudhary and C. -M. Chen, "CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC," in *IEEE Access*, Vol. 8, pp. 107838-107852 (2020), doi: 10.1109/ACCESS.2020.3001152.

[49] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally and Y. Begriche, "A Lightweight ECC-Based Authentication Scheme for Internet of Things (IoT)," in *IEEE Systems Journal*, Vol. 14, No. 3, pp. 3440-3450 (Sept. 2020), doi: 10.1109/JSYST.2020.2970167.

[50] B. Sowmiya, E. Poovammal, K. Ramana, S. Singh and B. Yoon, "Linear Elliptical Curve Digital Signature (LECDS) With Blockchain Approach for Enhanced Security on Cloud Server," in *IEEE Access*, Vol. 9, pp. 138245-138253 (2021), doi: 10.1109/ACCESS.2021.3115238.

[51] Suhag, Deepika, Shailendra Singh Gaur, and A. K. Mohapatra. "A proposed scheme to achieve node authentication in military applications of wireless sensor network." *Journal of Statistics and Management Systems* 22.2 : 347-362 (2019).

[52] Kumar, Kakelli Anil, Addepalli VN Krishna, and K. Shahu Chatrapati. "New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks." *Journal of Information and Optimization Sciences* 38.2 : 341-365 (2017).

[53] Mehta, Ekta, and Arun Solanki. "Minimization of mean square error for improved euler elliptic curve secure hash cryptography for textual data." *Journal of Information and Optimization Sciences* 38.6 : 813-826 (2017).

[54] Joshi, Ashish, and Amar Kumar Mohapatra. "A novel lightweight authentication protocol for body area networks based on elliptic-curve cryptography." *Journal of Information and Optimization Sciences* 41.7 : 1645-1672 (2020).