International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Comparative Analysis of Elliptic Curve Cryptography Methods and Survey of Its Applications

**KM Abirami[1], Dr. R. Srikanth [2], Dr. R. Kavitha*[3]**

**Submitted:** 24/05/2023 **Revised:** 17/07/2023 **Accepted:** 28/07/2023

**Abstract:** Cyber security is a key priority in today's highly technological generation; by employing modern technologies, many security ways have been produced as of now; nevertheless, the gap to breach that security is also expanding, thus there is a need for improved security techniques. Elliptic Curve Cryptography (ECC) is the finest among all other earlier technologies by its uniquenature of untrace ability, compressibility and most importantly for its finite condition.This research looks into ECC and its improved variant, Hyperelliptic Curve Cryptography (HECC), as well as a survey of real-world applications of ECC and HECC are also detailed.

***Keywords:*** *ECC, Hyperelliptic curve, Encryption, Decryption, Application analysis.*

## 1. Introduction

In our day-to-day lives, cybersecurity is imperative. For instance, we want to ensure the information on our laptops and smartphones, which are personal technological devices. To use messaging apps like Skype, WhatsApp, and others to conduct confidential interactions over the unreliable internet. To safeguard our data while using cloud storage services like Google Drive,Onedrive, pCloud and others, or when using online banking and bill-paying features, or when making purchases online and taking use of e-commerce features like those provided by Amazon, Flipkart, eBay, and many more. Cybersecurity's implementation and advancement make all of those feasible. In order to establish cybersecurity for the aforementioned items, the discipline of cryptography can offer essential security.

In the field of cryptography engineering, we are aiming for greater security strength, quicker implementation, and reduced power consumption. These conditions can already be met by a large number of cryptographic methods. The new communication devices, however, are compact in size and have minimal processing and storage capacity. The RSA key size [8] is rather big, therefore tiny device implementations of RSA need a lot of processing time and power. The Discrete Logarithm Problem (DLP) over the multiplicative group of elliptic curves specified in the finite fields and other lower key size cryptosystems are therefore preferred in practice.

### 1.1. Related Works

ECC was pioneered by Koblitz [1] in 1987. Its foundation is the DLP over the curve's abelian group of points. The computation is quick and simple by virtue of the group law over the curve. Elliptic Curve Discrete Logarithm Problem (ECDLP) sub-exponential techniques are not available, which is another benefit of utilizing ECC over RSA.At a significantly lower key size, ECC may offer the same degree of safety as RSA or DLP-based systems like the ElGamal public key cryptosystem and Diffie Hellman Key Exchange (DHKE). On the other hand, elliptic curves' mathematical complexity is greater than that of RSA and DLP-based systems. DHKE, RSA, ElGamal, and ECC are the four well-known public-key algorithms. HECC is a more recent addition to the group[5], [6], [7], [9].

The DLP on hyper elliptic curves (HEC) and the cryptography built on the Jacobian of HEC were both proposed by Koblitz [2] in 1989. Be aware that elliptic curves of genus 2 can also be thought of as hyper elliptic curves. Even when compared to ECC, the benefit of utilizing HECC is the reduced key size for the same magnitude of safety. Additionally, it lacks sub exponential techniques, like those for ECC, to solve the HEC DLP. HEC are a viable option for the low weight cryptosystems due to a shrinking size of the base field.

Theoretically more secure than any existing public key cryptosystem is HECC [4]. This is because ECC with equal key lengths have a lower level of mathematical complexity than this. This paper examines the

*1 Ph.D Student, SASTRA Deemed University, Thanjavur – 613401, India*
*abirami@maths.sastra.ac.in*
*2 Professor, SASTRA Deemed University, Thanjavur – 613401, India*
*ORCID ID : 0000-0002-8872-1384*
*srikanth@maths.sastra.ac.in*
*3 Department of Mathematics, Assistant Professor* SASTRA Deemed University, Thanjavur – 613401, India*
*ORCID ID : 0000-3343-7165-777X*
** Corresponding Author Email: kavitha_r@cse.sastra.ac.in*

mathematical foundations of ECC and HECC in detail and looks at effective group operation techniques.

The Jacobian of the curve's addition and doubling are part of the group law of the HECC.Cantor provided the algorithm for the group operation [3]. After then, there have been significant advancements in the computing of group operations that are more efficient, and HECC research has also been quite active. Harley [10] achieved one of the initial attempts in order to create an effective algorithm for group operation for HECC. Numerous academic later studies (see [11–14]) offered more effective algorithms for carrying out group operations of HECC. To improve the security system for stored data in cloud [15] followed the HECC.

HECC [16] is perfectly suited for devices with minimal storage and computing power developed by XX. Recently XX [17] showed that high level secure mechanism of HEC helps to transfer the medical data. Several applications have been developed for HECC due ti its portable nature and ability to withstand cryptographic attacks (see [18-20])

## 2. On Elliptic and Hyperelliptic curve

### 2.1. Formulation of elliptic curves by Weierstrass

Turn on by explaining how a Weierstrass equation may be used to define elliptic and hyperelliptic curve.

Recall the general Weierstrass equation:

$$W: y^2 + \underbrace{(a_1X + a_3)}_{k(x)}\, y = \underbrace{X^3 + a_2X^2 + a_4X + a_6}_{l(x)}$$

Where, $deg(l) = 2g + 1\ and\ deg(k) \leq g$

Where, $g =$ Genus of curve

If $g = 1$, is called Elliptic Curve

If $g \geq 1$, is called Hyperelliptic Curve

### 2.2. Elliptic Curve (EC)

Consider specific finite fields and specific equations over which curves are defined in cryptography. The curve's points form a commutative group. Due to the computationally complexity nature of the DLP in elliptic curve groups, elliptic curves offer great potential for cryptography applications. Additionally, it is "more difficult" than in groups, which was previously taken into consideration, allowing for reduced key lengths.

The reducedWeierstrass form of an EC, $W_{EC_{(ab)}}$ formed over a prime field M (with $M > 3$) isexpressed as:

$$\boldsymbol{W_{EC_{(ab)}}: y^2 = x^3 + ax + b;\ a, b \in M}$$

#### 2.2.1. Graphical representation of EC over real field

Let $\{W_{EC} = (x, y) \in \mathbb{Z}_M \times \mathbb{Z}_M;$ satisfies the condition, $y^2 \equiv x^3 + ax + b\ (mod\ M); a, b \in \mathbb{Z}_M$. Such that $4a^3 + 27b^2 \equiv 0(mod\ M) \cup \{O\}\}$ be an Elliptic curve over $\mathbb{Z}_M$

Where O is the Point of Infinity

Since $\mathbb{Z}_M$is a finite field, it is possible to find all the possible points that lie on an Elliptic Curve over $\mathbb{Z}_M$.

**Steps to find all possible points:**

Consider the equation for Elliptic Curves over Prime Fields $\mathbb{Z}_M$

$$y^2 \equiv x^3 + ax + b\ (mod\ M)$$

1. Take the values of $x$ from $0\ to\ M - 1$ inclusive.
2. For each $x$ value, compute the right side of the equation $x^3 + ax + b\ (mod\ M)$
3. If the right-hand side is a perfect square modulo M, then let y be the square root of the right-hand side modulo M. Note that there are two possible square roots modulo M, so we can choose either one.
4. $(x, y)$ is a point on the EC, and$(x, -y)$ (which is the mirroring of $(x, y)$ across the $x$-axis).

**Point generation**

Consider the elliptic curve,

$$W_{EC}: y^2 \equiv x^3 - x + 6\ (mod\ 13)$$

| $x$ | $x^3 - x + 6\ (mod\ 13)$ | $y$ |
|---|---|---|
| 0 | 6 | n/a |
| 1 | 6 | n/a |
| 2 | 12 | n/a |
| 3 | 4 | 2 |
| 4 | 1 | 1 |
| 5 | 9 | 3 |
| 6 | 8 | n/a |
| 7 | 4 | 2 |
| 8 | 3 | n/a |
| 9 | 11 | n/a |
| 10 | 8 | n/a |
| 11 | 0 | 0 |
| 12 | 6 | n/a |

Legitimate points:

| | |
|---|---|
| (3,2) | (5, 10) |
| (3, 11) | (7, 2) |
| (4, 1) | (7, 11) |
| (4, 12) | (11, 0) |
| (5, 3) | |

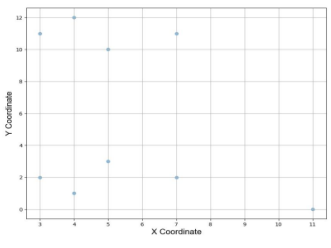


**Fig. 1.** Elliptic curve equation $y^2 = x^3 - x + 6$

In this manner, we have all the legitimate points of the curve,

For the curve with the equation,$y^2 = x^3 - x + 6$ has 9legitimate points.

### 2.3. Hyperelliptic Curve (HEC)

Let $M$ be a field and $\overline{M}$be its algebraic closure. The genus$g(g \geq 1)$of hyperelliptic curve,$W_{HEC}$over $M$ is an equation of the type,

$$\boldsymbol{W_{HEC}: y^2 + k(x)y = l(x)}$$

Where $k(x),\ l(x)\ \in M\ [x]$ and $k(x)$ is a polynomial of $\deg\ (k) \leq g$ and a monic polynomial$l(x)$ of $\deg(l) = 2g + 1$.

#### 2.3.1. Graphical representation of HEC over real field

$W_{HEC}$:$y^2 \equiv x(x-3)(x-2)(x+3)(x+2)\ (mod\ 11)$

We now need to know the $W_{HEC}$ curve's valid points. In order to achieve it, Python's power and mod functions can be used for this.

In this manner, we have all ofthe legitimate points of the curve:

$W_{HEC}$: $\{(x,y): y^2 \equiv x(x-3)(x-2)(x+3)(x+2)\ (mod\ 11)\} \cup \{O\}$

$W_{HEC} = \{(0,0), (2,0), (3,0), (6,5), (6,6), (7,4), (7,7), (8,0), (9,0), (10,3), (10,8)\}$

For the curve with the equation,$y^2 \equiv x(x-3)(x-2)(x+3)(x+2)(mod\ 11)$has 11legitimate points.

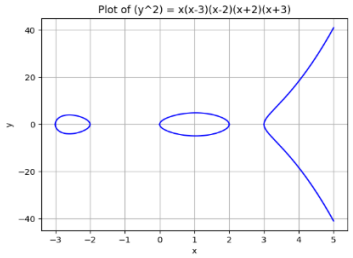


**Fig. 2.** HEC$y^2 \equiv x(x-3)(x-2)(x+3)(x+2)\ (mod\ 11)$

## 3. Cryptography based on ECC and HEC

### 3.1. Process of Key Generation

Consider two users A and B.

1. Users select a suitable elliptic curve $EC$, and prime number $q$.
2. Users choose a generator $G$, which is a point on the EC.
3. User A selects a private key: $(a)$ which is an integer. Then User A calculates the public key: $(a * G)$, where $G$ indicate the generator point on the EC. The calculated value is also a point on the EC.
4. User B follows the same method as User A and generates their private key: $(b)$ and public key: $(b * G)$.
5. User A and User B exchange their public keys.
6. Users then multiply the received public key by their private key to generate the secret shared key: $(a * b * G)$ which is also a point on the curve EC.

### 3.2. Process of Encryption and Decryption

Consider the following scenario:

User A owns the private key: $(a)$ and a public key $P_A = a * G$

User B owns the private key: $(b)$ and a public key $P_B = b * G$

They carry out a DHKEand createa shared secret key:

$$S = a * b * G$$

Now, User A wants to send a message $P_m$by utilizingthe point on an EC to User B.

The steps User A would take to encrypt the communication are as follows: $\boldsymbol{P_m}$:

1. User A would choose arbitrary positive integer $v$
2. User A would then generate the cipher text $C_m$which includes a pair of points$C_1$and$C_2$.

$$C_m = \{C_1,\ C_2\}$$

Where,$C_1 = vG$ and $C_2 = P_m + vP_B$

To decrypt the encrypted text, User B would do the following actions. $\boldsymbol{C_m}$:

1. User B would find the following value$b * C_1$
2. User B would then subtract the above value with $C_2$ which would give the original message,

$$P_m = C_2 - (b * C_1)$$

Because,

$$\begin{aligned} C_2 - (b * C_1) &= P_m + vP_B - b(vG) \\ &= P_m + v(bG) - b(vG) \\ &= P_m \end{aligned}$$

## 4. Comparative analysis and Results

In this section, we compare the EC and HEC in the same field$M_{197}$.

Elliptic curve:$W_{EC}$: $y^2 \equiv x^3 - 16x\ (mod\ 197)$

Hyperelliptic curve:$W_{HEC}$: $y^2 \equiv x(x-3)(x-2)(x+3)(x+2)\ (mod\ 197)$

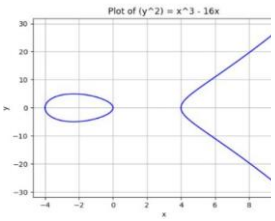


**Fig. 3.** EC $y^2 \equiv x^3 - 16x$

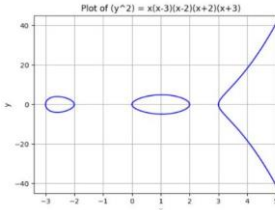


**Fig. 4.** HEC $y^2 \equiv x(x-3)(x-2)(x+$

By comparing the curves' valid points (figures 3 and 4). In comparison to the Elliptic curve, hyperelliptic curves have a greater number of valid points. The curve $W_{EC}$ has 196 legitimatepoints for $M_{197}$, but the curve $W_{HEC}$ has 206 legitimate points for $M_{197}$. We may literally say that $W_{HEC}$ has more than 10 legitimate points than$W_{EC}$ .

## 5. Application on ECC and HECC

### 5.1. On ECC

There are many traditional applications for ECC here we concentrate some of the developing applications of ECC.

G. Sahebi et al. created a system that uses ECC for its quick tempo, fewer keys and for increased safety in E-health services like sensors and devices [21]. S. Vishnubhatla created an ECC-based hashing technique for optic pattern detection. Pictures from the UBIRIS database were fed into the system as test input. Python and the OpenCV package were employed to hash grayscale photos.After reviewing the results, it was discovered that the EC hashing method surpassed the usual hashing algorithms [22]. Vehicular communicationis currently utilized for situations of emergency and location secrecy. False signals can be broadcast via unsecured wireless connection, leading cars to be misguided. A strategy for safe smart city vehicle message communication has been presented by A. Dua et al. Large key sizes used to make secure communication challenging to establish. The team was able to establish a system that can employ lower key sizes and provide equivalent or more security than earlier discussedcryptographic techniques for vehicle communication by using ECC [23].

### 5.2. On HECC

Prasanna Ganesan [24] emphasizes the use of HECC for mobile devices with limited power and compares the effectiveness of RSA and HECC, concluding that the ElGamal-based HECC provides an enhanced level of security. With the help of HECC, A.Klimm created a cryptographic processor to validate automobile access control systems. Additionally, he created both the software and hardware interface for the vehicle access control system [25].According to Deng Jian-zhi [26], the development of a HECC-based digital signature, will resolve the issue by examining the file's integrity and signature ID, is particularly suitable for online activitiesthat need identity validation.

## 6. Conclusion

From this comparison of the EC and the HEC, based on point generation, addition, and doubling for both curves, combined with a powerful encryption and decryption method, we were able to compare the results based on mathematical complexity. It unequivocally establishes that a HEC is superior to an EC.Furthermore, several significant contemporary applications that make use of ECC and HECC are also covered.

## References


[1] Koblitz, Neal. "Elliptic curve cryptosystems." Mathematics of computation. 48.177 (1987):203-209.

[2] Koblitz, Neal. "Hyperelliptic cryptosystems." Journal of cryptology 1.3 (1989): 139-150.

[3] Cantor, David G. "Computing in the Jacobian of a hyperelliptic curve."Mathematics ofcomputation 48.177 (1987): 95-101.

[4] Pelzl, Jan, et al. "Hyperelliptic curve cryptosystems: Closing the performance gap to ellipticcurves." Cryptographic Hardware and Embedded Systems-CHES 2003. Springer BerlinHeidelberg, 2003. 351-365.

[5] Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography."InformationTheory, IEEE Transactions on 22.6 (1976): 644-654.

[6] Merkle, Ralph C. "Secure communications over insecure channels."Communications of theACM 21.4 (1978): 294-299.

[7] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digitalsignatures and public-key cryptosystems." Communications of the ACM 21.2 (1978): 120-126.

[8] Paar, Christof, and Jan Pelzl. Understanding cryptography: a textbook for students andpractitioners. Springer Science & Business Media, 2009.

[9] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discretelogarithms." Advances in cryptology. Springer Berlin Heidelberg, 1984.

[10] Harley, R. "Fast arithmetic on genus two curves; 2000."

[11] Lange, Tanja. "Efficient arithmetic on hyperelliptic curves." IACR Cryptology ePrintArchive 2002 (2002): 107.

[12] Matsuo, Kazuto, Jinhui Chao, and Shigeo Tsujii. "Fast genus two hyperelliptic curvecryptosystems." Technical Report ISEC2001-23, IEICE, (2001): 89-96.

[13] Miyamoto, Yosuke, et al. "A fast addition algorithm of genus two hyperelliptic curve." The2002 Symposium on Cryptography and Information Security—SCIS 2002, IEICE Japan.2002.

[14] Takahashi, Masashi. "Improving Harley algorithms for Jacobians of genus 2 hyperellipticcurves." SCIS, IEICE Japan (2002).

[15] Dr. A. Pasumpon Pandian. “Development of Secure Cloud Based Storage Using the Elgamal HyperElliptic Curve Cryptography with Fuzzy Logic Based Integer Selection”. Journal of Soft Computing Paradigm(JSCP), (2020):2(1)24-35. DOI: https://doi.org/10.36548/jscp.2020.1.003

[16] Shamsher Ullah and Nizamud Din. “Blind signcryption scheme based on hyper elliptic

curvescryptosystem". Peer-to-Peer Networking and Applications, (2021): 14:917–932, https://doi.org/10.1007/s12083-020-01044-8

[17] B. Prasanalakshmi, et al. "Improved authentication and computation of medical datatransmission in the secure IoT using hyperelliptic curvecryptography". The Journal of Supercomputing (2022): 78, 361–378. https://doi.org/10.1007/s11227-021-03861-x

[18] AymenDiaEddineBerini et al. "HCALA: Hyperelliptic curve-based anonymous lightweightauthentication scheme for Internet of Drones". Pervasive and Mobile Computing 92 (2023): 101798. https://doi.org/10.1016/j.pmcj.2023.101798

[19] Naveed Ahmed Azam et al. "A novel image encryption scheme basedon elliptic curves and coupled map lattices". Optik, 274 (2023): 17051. https://doi.org/10.1016/j.ijleo.2023.170517

[20] Khalid Javeed et al. "EC-Crypto: Highly Efficient Area-Delay Optimized Elliptic Curve Cryptography Processor". IEEEAccess. 11, (2023):56649-56662.

[21] GolnazSahebi et al. "SEECC: A Secure and Efficient Elliptic Curve Cryptosystem for E-health Applications". In 2016 International Conference on High Performance Computing & Simulation (HPCS). IEEE, Innsbruck, 492-500. DOI: https://doi.org/10.1109/HPCSim.2016.7568375

[22] Sasank Venkata Vishnubhatla. "An Elliptic Curve Algorithm for IrisPattern Recognition". In 2015 Annual Global Online Conference on Informationand Computer Technology (GOCICT). IEEE, Louisville, KY, 51-59. DOI:https://doi.org/10.1109/GOCICT.2015.19

[23] Amit Dua et al. "Secure Message Communication Among Vehicles Using Elliptic CurveCryptography in Smart Cities". In 2016 International Conference on Computer,Information and Telecommunication Systems (CITS). IEEE, Kunming, 1-6. DOI:https://doi.org/10.1109/CITS.2016.7546385

[24] S. P. Ganesan. "An authentication Protocol For Mobile Devices using Hyper Elliptic Curve Cryptography".In the ACEEE proceeding of International Journal of Recent Trends in Engineering and Technology, 3.2 (2010).

[25] A. Klimm. "A Flexible Integrated Crypto processor for Authentication Protocols based on HyperellipticCurve Cryptography".In the IEEE proceeding of International Symposium on System on Chip (SoC), 1(2010), 35-42.

[26] D. Jian-zhi, C. Xiao-hui and G. Qiong, "Design of Hyper Elliptic Curve Digital Signature".In the IEEEproceeding of International Conference on Information Technology and Computer Science, 2(2009):45-47.

[27] Revathy, S. ., & Priya, S. S. . (2023). Enhancing the Efficiency of Attack Detection System Using Feature selection and Feature Discretization Methods. International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 156–160. https://doi.org/10.17762/ijritcc.v11i4s.6322

[28] Mark White, Thomas Wood, Carlos Rodríguez, Pekka Koskinen, Jónsson Ólafur. Machine Learning for Adaptive Assessment and Feedback. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/169