# Elliptic Curve Digital Signature Algorithm Challenges and Development Stages

**Wageda El Sobky, Sara Hamdy, Mustafa Hussien Mohamed**

***Abstract:** This paper try to introduce the advantages and disadvantages of the Elliptical Curve Digital Signature Algorithm that could be put in consideration for future usage through applications and future scalability depending on improvement levels of elliptical curve Digital Signature Algorithm starting from The elliptical Curve Cryptography that it was extracted from till showing, elliptical curve Digital Signature Algorithm's security power, performance quality, memory usage rate, applications, challenges, and last improvement. To help in the future in evading some problems like forgery, worse usage of memory because of big sized keys that cause the need for high processing power that reduces the performance quality, and considering it as a level in a new algorithm to reduce the tries of attacking and hacking specific messages between specific parties, after explaining the Elliptical Curve Cryptography and how the scientists reached from the Elliptical Curve Cryptography to the Elliptical Curve Digital Signature Algorithm and why they developed Elliptical Curve Digital Signature Algorithm, the paper will explain its advantages and disadvantages of the Elliptical Curve Digital Signature Algorithm, then the paper will explain what is the differences happen in a new type of the Elliptical Curve Digital Signature Algorithm called Multiple Elliptical Curve Digital Signature Algorithm, trying to show what is the improvement stages was happened in the Elliptical Curve Digital Signature Algorithm, how that affected the nowadays applications, and how that participated in improving the security performance and increasing the security strength, there fore what was included in the paper could be used as a nucleus for more and more improving of the Elliptical Curve Digital Signature Algorithm, and evading its defects.*

***Keyword:** Cryptography of the Elliptical Curve(ECC ), Algorithm of Digital Signature with Elliptical Curve (ECDSA),Algorithm of Digital Signature with Multiple elliptical curves (MECDSA), Signature Digitalized(DS), Algorithm of Signature Digitalized (DSA), Rivest–Shamir–Adleman Digital Signature(RSADS), Rivest–Shamir–Adleman(RSA).*

## I. INTRODUCTION

An elliptical curve is represented by the form y2 = p(x), where p(x) is a mix of cubic parameters and polynomial also with different roots. elliptical curve appeared for the first time in the second century after date of birth. Neal [3], In 1985 with Victor Miller [4] independently benefited from ECC to develop public-key cryptography systems. In the late 1990s,ANSI, IEEE, ISO, NIST are examples of where ECC was standardized[ 5,6,7,8,9,10], then it began to receive commercial conformance. Today, it is prevailed, as it is being used in different fields such as wireless networks fields, and mobile networks fields.it is a direction that old public-key cryptography rules are gradually replaced with ECC rules. Daniel V. Bailey in Sep'2000 with Paar[11] produced mathematical infinite or prime field extensions with implementation in ECC. there many of researches that depend on the elliptical curve Digital Signature Algorithm as MECDSA that try to decrease the size of the signature and avoid secp256k1 [14], The relative to standards implicate requirements that break the least requirement for PDF signatures. With more of these requirements, signature investigation algorithms can easily be performed to thwart attacks that would otherwise go unnoticed through normal PDF or online signature investigation processes [15]; advanced electronic signatures must fulfil specific requirements that ensure their authenticity to be considered useful. The signature must identify and be unique to its signatory [16], Modifications of ECDSA [18].

The paper is divided to the ten sections (sec. One: talk about Introduction, sec. Two:talk about ECC, sec. Three: talk about Signatures, sec. Four: talk about DS, sec. Five: talk about ECDSA, sec. Six: talk about ECDSA Applications, sec. Seven: talk about ECDSA Features, sec. Eight: talk about ECDSA Challenges, sec. Nine: Latest research in ECDSA, sec. Ten: Comparison between ECDSA and MECDSA).

## II. ELLIPTICAL CURVE CRYPTOGRAPHY

This section aims to survey the basic theory for ECDSA applications.

Def. An elliptical curve E is the method to solve a Weierstrass form.

Eq$^{n}$:

$$\mathbf{Y^2 = X^3 + const1X + const2} \tag{1}$$

Manuscript received on August 14, 2021.
Revised Manuscript received on August 21, 2021.
Manuscript published on August 30, 2021.
* Correspondence Author

**Mustafa Hussien Mohamed***, Computer Department, MTC, Cairo, Egypt. Email: mostafahosen042@gmail.com

**Wageda I. El Sobky**, Math Department, Benha University, Benha, Egypt. Email: wageda.alsobky@bhit.bu.edu.eg

**Sara Hamdy**, Electric Department, Benha University, Benha, Egypt. Email: sara.hamdy@bhit.bu.edu.eg

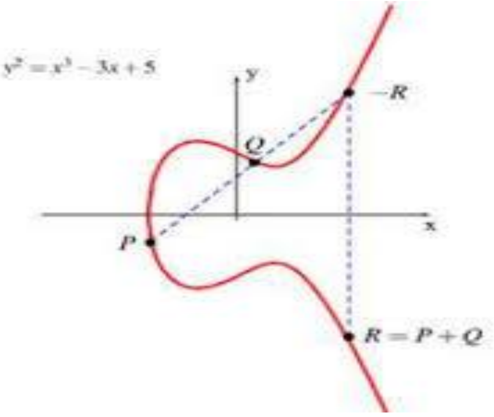

**Figure 1 Elliptic Curve**

Point L, where the constants const1 and const2 must satisfy.

The addition rule on the equation is defined like:

p1 and p2 be two points on elliptic curve ec.

C = (x, y), the summation of p1 and p2 is defined to be the reflection = (x, −y) of C on the X-axis.

This sum is denoted by p1 ⊕ p2, or simply by p1 + p2. Further, if p1 = (x, y), the reflected point given by

#p1 = (x, −y), or by −p1; and p2 - p1 (or p1 − p2) to be p1 ⊕ (-p2). AS, multiplication of a point by an integer the repeated addition is represented ,
K Point = Point + Point + Point + · · · + Point .

$$\lambda = \frac{(3x^3+A)}{2y} \tag{2}$$

If p1 = p2

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \tag{3}$$

If p1 ≠ p2

$$y_3 = \lambda_1 - x_3 - y_1 \tag{4}$$

Therefore

$$p_1 + p_2 = (x_3, y_3) \tag{5}$$

## III. SIGNATURES

It is a mark that leads someone to know the thing that carries that mark is owned specifically by somebody.

Like DNA, Fingerprint, Eye print, The Wet Signature, Click Wrap Signatures, Electronic Signature (E-Signature), The Digital Signature (D.S.). Each type of them has its own definition [27]:

1. The Wet Signature: Is any corporal mark on documents produced by a human. In most times, it's writing your personal name on a paper, document, or contract, often with primitives on each page indicating the extent of what is being signed.

**Figure 2 Wet Signature**

2. Click Wrap Signatures: Which is used for most online purchases, where a simple press in a box is an acceptance of the terms and conditions the page has referred to somewhere on the website. A user must click the box before the services can be delivered.

**Figure 3 Click Wrap Signatures**

3. The Electronic Signature (E-Signature): The a digital type of a wet signature, where different countries defined the legacy and description of the usage of electronic signatures. These are the most common shape of signatures used by Institutions globally.

**Figure 4 Electronic Signature**

4. The Digital Signature: This authentication method enables a code to be implemented as a signature. It is required for certain specific agreements and issued through a certification agency.

**Figure 5 Digital Signature**

So, this paper will depend on digital signature as nowadays because of scientific progress In the context of digital transformation, and everything is turning to become digital. Most of our dealings are digital, like websites security authentication, banking transaction, visa card usage through the internet.

### A. Digital Signature

The History of Digital Signatures in 1976 and 1977 Diffie described the idea of the RSADS with Hellman where it was created and began to be used in 1989 when The first advertised software of the DS, Lotus Notes 1.0, was launched. Goldwasser, Micali is the first one defined the security conditions of DS in 1999, 2000, and 2002 with help of Rivest where PDF format adds possibility to embed digital signatures into documents electronic signature Act produces legally online signatures is founded and became the most broadly used digital signature software depending on cloud-based. In 2008 Digital signatures considered as the most secure method to get documents signed online Digital signatures contained in standardization for PDFS established by the International Institution for Standardization Resources "New Directions in Cryptography" "A Method for Implementing Digital Signatures and Public-Key Cryptosystems" by RSA in (1978).

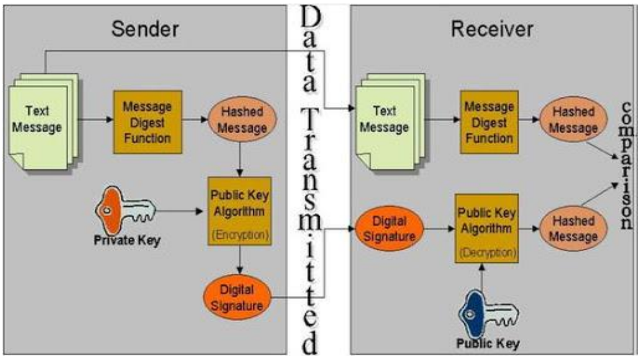

**Figure 6 How digital signature algorithm work**

### B. Digital Signature Standard

NIST published the Standard of treatment of Information FIPS 186. The DSS used the SHA and presents a new digital signature protocol, the DSA.[1]

From Cryptography techniques that use DSS the elliptical curve Cryptography and the paper will explain in the next paragraphs why the elliptical curve technique specifically.

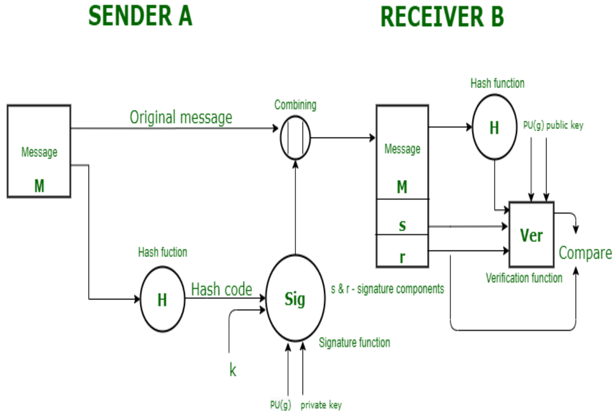

**Figure 7 DSS [48]**

### C. Digital Signature Approach

The DSS utilizes the algorithm which developed for providing just the digital signature form. In contrast with RSA, it couldn't be used for encryption or key exchange. However, it is a public-key technique.[1]

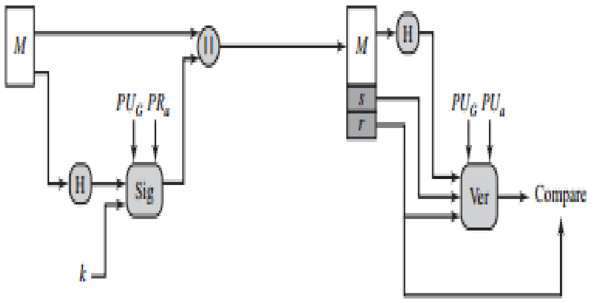

**Figure 8 DSS Approach [28]**

## IV. ELLIPTICAL CURVE DIGITAL SIGNATURE ALGORITHM

The first appearance the DS idea was in seminal paper that developed by diffie with aid of hellman , “new directions in cryptography” [13]. one side was wanted to publish a "public key" but saving the "secret key". in their design the message “m” side a’s signature is a value that based on the secret key of “m and a's”, as a's public key could be used for assurance the possibility of the signature of a using. So some many protocols and applications depend on the elliptical curve from that application ECDSA, the ECDSA is a type of the DSA. It was recognized in 1999 as a standard of ANSI and was recognized in 2000 as standard of IEEE and standard of NIST. It was also recognized in 1998 as an standard of ISO and is under the regard of containing other different standards of ISO. On oppisite to the normal discrete logarithm design and the integer factorization design, no algorithm with exponentially time distribution utilized for the EC discrete logarithm rule. So, the force-per-key-bit is mainly better for an design that utilizes ECs. Descriping the ECDSA of ANSI X9.62 and studies related to security. The DSA was specified in a U.S.A FIPS called the DSS [29]. Its security depended on the computational int.

Although knowing one side's key that is public is enough to permit one to validate signatures of A, it does not permit one to create the signatures that sides easily. They also suggested a way of doing signatures depended on "functions of trap-door ".

To utilize ECDSA, as descriped in the standard of ANSI[5,6] and others, one created EC ec with limited field Ffinite whose degree is equal to a prime num times a small cofactor n, i.e.

#ec(Ffinite) = n · num. Also, a base point P ∈ ec(Ffinite) is chosen of order num. Note that, however users can choose their base points, it is discussed that some main authority should set them. All users have two keys where one is private and the other is public. With more features, the Blockchain has created ability to be applicable in other divisions as well and not only cryptocurrency.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication
© Copyright: All rights reserved.

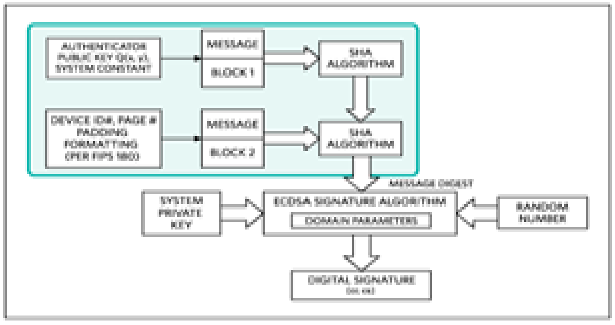

**Figure 9  ECDSA**

## V. ELLIPTICAL CURVE DIGITAL SIGNATURE ALGORITHM APPLICATIONS

DS schemes are used in providing the following services of basic cryptographic:

1. data integrity (to assure that no one show the data or used it with unauthorized ways).
2. authentication of data origin(to assure that the original data is similar to the shown).
3. non-repudiation (is that where an entity not able to deny previous actions, commitments, and commands).
4. DS schemes are commonly used as basic protocols of cryptography that produce some services containing authentication of entity [37].
5. ECDSA is used in different security systems.
6. messaging security apps, and is the base of the security of Bitcoin.
7. ECDSA utilized differently as Security of Transport Layer for Sockets Layer Security, by website browsers and the web application connections encryption. That is clarified by the shape of the shutter in the website browser, is developed by ECDSA signed certificates.
8. An excellent property of ECDSA with respect to RSA, which is producing a higher security level and shorter lengths of key. What help to increase the ROI more as ECDSA computer power use is less than RSA.

## VI. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM FEATURES

What make any cryptography algorithm difference about the other its effect what is due to its features like security power, performance quality, memory usage rate.

**Table- I ECDSA Feature**

| Feature | Value |
|---|---|
| security power | Very strong, as it contain three types of security because it depends on hash function, discrete logarithm problem and elliptic curve, therefore it is at least have security power higher than any one from the three cryptography sections that were mentioned, in addition to dependability on mathematical problem solving.[47] |
| performance quality | Due to its power of security it has a good performance from the point of view of difficulty and safety, but due to the difficulty of that mathematical problem solving that may make its performance some how worst. [47] |
| memory usage rate | Due to the difficulty of its mathematical equation problem solving, it has a high memory usage rate and high processing power consumption.[47] |

## VII. ELLIPTICAL CURVE DIGITAL SIGNATURE ALGORITHM CHALLENGES

Most of the systems like cryptocurrency or blockchain technology nowadays uses the ECDSA on the Curve secp256k1, which will be defected by back doors wrongly done by the curve creator (secp256k1).

Digital signatures[38,39] were applied to detect unauthorized attacks on data and authenticate the signer's identity. The reception side of the message with signature can utilize a DS as a guide to pretend to a hidden side that the known signer produced the signature. Digital signatures use a mixture of hash 256 and cryptography of public-key. where, the message “m” hashed. Creating the signature by encrypting “m” using the private key of signer. Everyone may use the public key of the signer and the hash created before to verify the received signature. Until now, most of systems depend on cryptocurrency[40,41] or systems built by blockchain technology [42,43] have used ECDSA [44,45], which is depending on secp256k1. It was as not common before Bitcoin popularity, unlike now it’s used a lot due to several beneficial properties. The most-common curves own a irregular structure, however it was developed in a unique, regular way that permits for excellent computation. Therefore, it is about faster by 30% more than the other ones if the performance is enough improved. However, it cannot stop the Curve's developer from creating any back doors to the created Curve.

## VIII. THE LATEST DEVELOPMENT IN ECDSA

Algorithm for Blockchain it’s a paper published in 2018 trying to avoid the back doors in ECDSA like that a MECDSA (multiple ECDSA), that is better in security and evading any defects. In the MECDSA design, the user can select how many of ECs due to requirements of practical security and modify the Curve by editing its parameters. The MECDSA renders four purposes. At first, the signature specifies who is the private key holder by involvement the funds holder, who has authorized the finances spending. Second, the proof of authorization couldn't be denied. Third, the signature assure that if the transaction has been signed, therefore it cannot be edited by anyone. Fourth, the signature design can evade any back doors in the ECDSA curve.

## IX. COMPARISON BETWEEN ECDSA & MECDSA

In this section the paper will compare between the ECDSA and the last modification was developed for it, the MECDSA.

### A. ECDSA Generation And Verification

An elliptical curve over a finite prime field is defined by ec:

$$Y^2 = X^3 + AX + B \qquad (6)$$

*Retrieval Number: 100.1/ijitee.J943308101021*
*DOI: 10.35940/ijitee.J9433.08101021*
*Journal Website: www.ijitee.org*

*Published By:*
*Blue Eyes Intelligence Engineering*
*and Sciences Publication*

**Table-II ECDSA Generation and Verification**

| Generate | Verify |
|---|---|
| **$k$ ∈ [1, n−1], $d$∈ [1, $n$]**<br>**Where d is the private key and Q=dP(The public key).** | ($r$, s) ∈ [1, $n$-1]. |
| **$k$P= ($x$, y).** | $e = H(m)$. |
| **$e$=H($m$).** | $w = s^{-1}(modn)$. |
| **$r$=x($modn$).**<br>**If r =0 reselect k** | $u = ew(modn)$, $v = rw(modn)$. |
| **$s$=$k^{-1}$($e$+$dr$)($modn$).**<br>**If s=0 reselect k** | $R = uP + vQ = (x, y)$. |
| **Then the signature on the message m is the pair ($r$, s).** | $r = x(modn)$. |

ECDSA Generation :

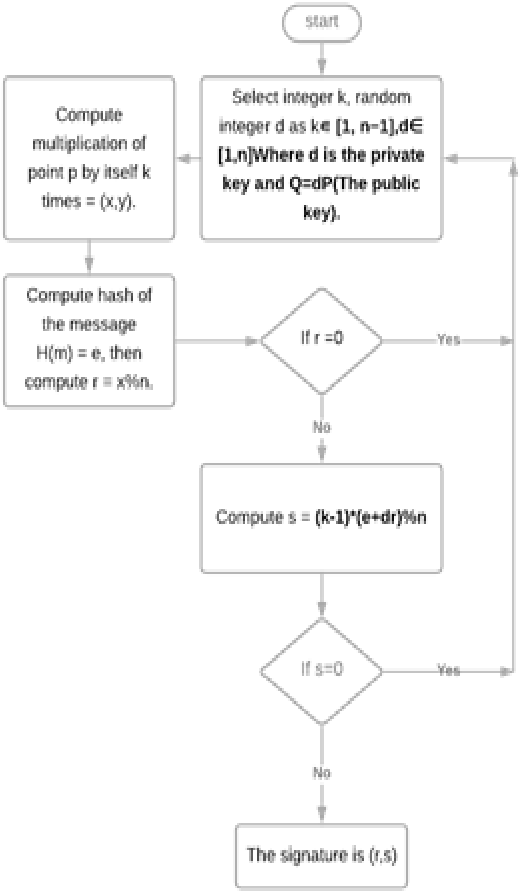
start
Select integer k, random integer d as k∊ [1, n−1],d∈ [1,n]Where d is the private key and Q=dP(The public key).
Compute multiplication of point p by itself k times = (x,y).
Compute hash of the message H(m) = e, then compute r = x%n.
If r =0
Yes
No
Compute s = (k-1)*(e+dr)%n
If s=0
Yes
No
The signature is (r,s)

**Figure 10 ECDSA Generation flowchart**

ECDSA Verification:

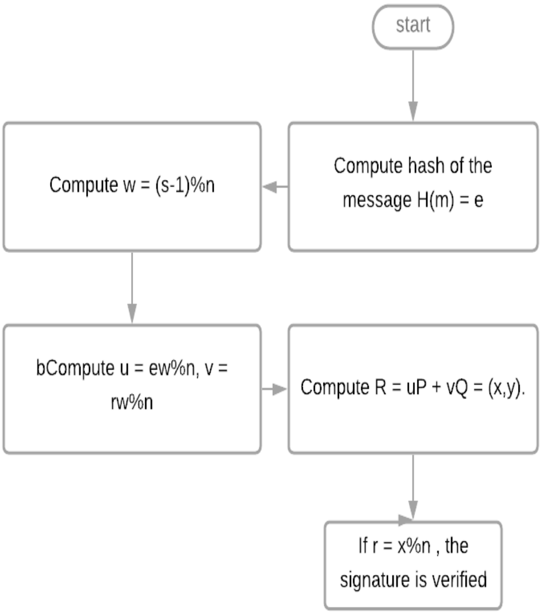
start
Compute hash of the message H(m) = e
Compute w = (s-1)%n
bCompute u = ew%n, v = rw%n
Compute R = uP + vQ = (x,y).
If r = x%n , the signature is verified

**Figure 11 ECDSA Verification flowchart**

## B. MECDSA Generation And Verification

It depends on more than one elliptic curve so For ith elliptical curves, the paper will show the generation and verification of MECDSA.

**Table-III MECDSA Generation and Verification**

| Generate | Verify |
|---|---|
| **$k_i$ ∊ [1, $n_i$−1], $d$∈ [1, $n$], Q= dP.** | **($r$, s) ∈ [1, $n$-1].** |
| **$k_i$ $P_i$= ($x_i$ , $y_i$ ).** | **$e = H(m)$.** |
| **$e$=H($m$).** | **$w_i = s_i^{-1}(modn)$.** |
| **$r_i$ =$x_i$ ($modn_i$ ).**<br>**If $r_i$ =0 reselect $k_i$**<br>**R=$r_{i1}$+$r_{i2}$+…** | **$u_i = ew_i(modn_i)$, $v = rw_i(modn_i)$.** |
| **$s_i$ =$k_i^{-1}$($e$+$d_i$ R)($modn$).**<br>**If $s_i$ =0 reselect k** | **$R_i = u_i P_i + v_i Q_i = (x_i, y_i)$.** |
| **Then the signature on the message m is the pair ($r$, $s_i$).** | ri = xi (modni).<br>If R=ri1+ri2+…<br>accept the signature |

MECDSA Generation:

Retrieval Number: 100.1/ijitee.J943308101021
DOI: 10.35940/ijitee.J9433.08101021
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication

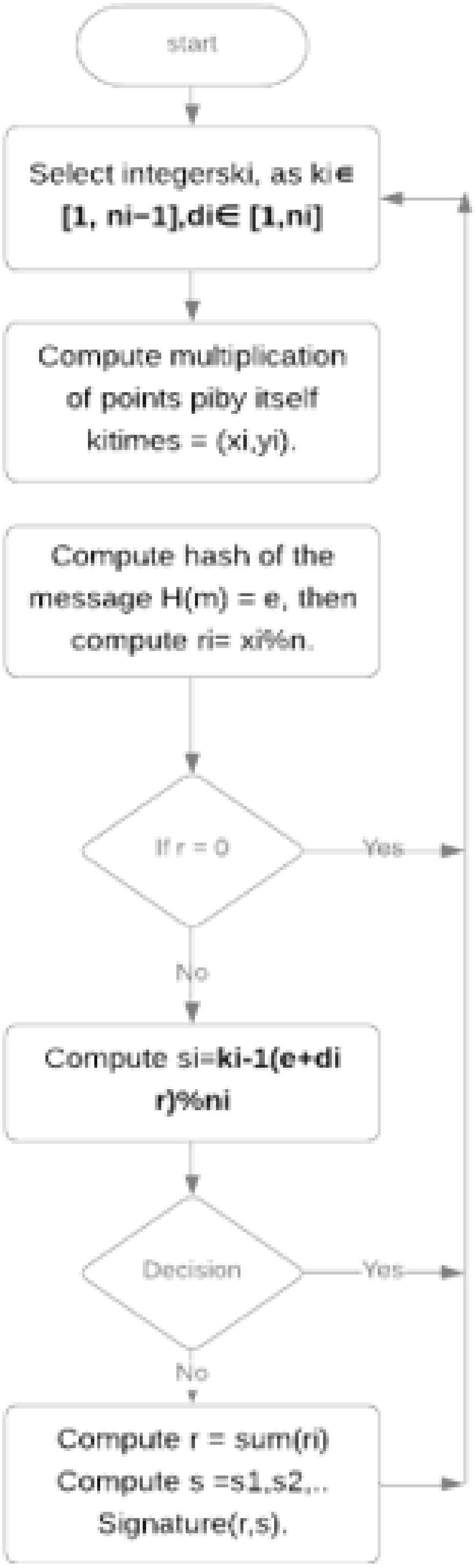
start
Select integerski, as ki∈ [1, ni−1],di∈ [1,ni]
Compute multiplication of points piby itself kitimes = (xi,yi).
Compute hash of the message H(m) = e, then compute ri= xi%n.
If r = 0
Yes
No
Compute si=ki-1(e+di r)%ni
Decision
Yes
No
Compute r = sum(ri)
Compute s =s1,s2,..
Signature(r,s).

**Figure 12 MECDSA Generation flowchart**

MECDSA Verification:

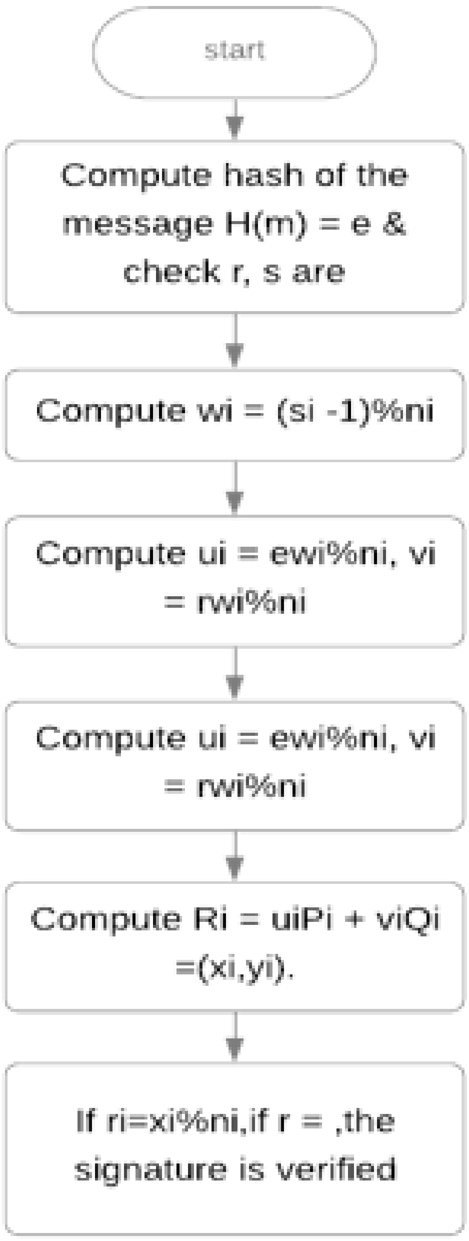
start
Compute hash of the message H(m) = e & check r, s are
Compute wi = (si -1)%ni
Compute ui = ewi%ni, vi = rwi%ni
Compute ui = ewi%ni, vi = rwi%ni
Compute Ri = uiPi + viQi =(xi,yi).
If ri=xi%ni,if r = ,the signature is verified

**Figure 13 MECDSA Verification flowchart**

## X. CONCLUSION

The ECDSA is one from the most effective algorithms in cryptography that has a high applicability in the nowadays applications, it has a good features and bad ones, many researches are trying to modify it to avoid its bad features and also for improving its good one, that paper showed its features and cleared the last modification for it and how the wok for improving good features and avoiding bad features is flowing.

## REFERENCES

1. Sklavos, Nicolas. "Book Review: Stallings, W. Cryptography and Network Security: Principles and Practice: Upper Saddle River, NJ: Prentice Hall, 2013, 752p., $142.40. ISBN: 13: 978-0133354690." (2014): 49-50, p308.

2. Hoffstein, Jeffrey, et al. An introduction to mathematical cryptography. Vol. 1. New York: Springer, 2008, p301.
3. Koblitz, Neal. "elliptical curve cryptosystems." Mathematics of computation 48.177 (1987): 203-209.
4. Miller, Victor S. "Use of elliptical curves in cryptography." Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1985 ,p417.
5. ANSI, X9. "62: public key cryptography for the financial services industry: the elliptical curve digital signature algorithm (ecdsa)." Am. Nat'l Standards Inst (1999).
6. Gajbhiye, Samta, Monisha Sharma, and Samir Dashputre. "A survey report on elliptical curve cryptography." International Journal of Electrical and Computer Engineering 1.2 (2011): 195.
7. Jonsson, Jakob, and Burt Kaliski. Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1. RFC 3447, February, 2003.
8. Koblitz, Neal. "elliptical curve cryptosystems." Mathematics of computation 48.177 (1987): 204.
9. Koblitz, Neal. "elliptical curve cryptosystems." Mathematics of computation 48.177 (1987): 205.
10. Hankerson, Darrel, Julio López Hernandez, and Alfred Menezes. "Software implementation of elliptical curve cryptography over binary fields." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2000.
11. Bailey, Daniel V., and Christof Paar. "Efficient arithmetic in finite field extensions with application in elliptical curve cryptography." Journal of cryptology 14.3 (2001): 153-176.
12. Bednara, Marcus, et al. "Tradeoff analysis of FPGA based elliptical curve cryptography." 2002 IEEE International Symposium on Circuits and Systems. Proceedings (Cat. No. 02CH37353). Vol. 5. IEEE, 2002.
13. Diffie, Whitfield, and Martin Hellman. "New directions in cryptography." IEEE transactions on Information Theory 22.6 (1976): 644-654.
14. Bi, Wei, Xiaoyun Jia, and Maolin Zheng. "A secure multiple elliptical curves digital signature algorithm for blockchain." arXiv preprint arXiv:1808.02988 (2018).
15. Foresti, Sara, and Javier Lopez. Information Security Theory and Practice. Springer International Pu, 2016.
16. https://scholarship.richmond.edu/jolt.
17. Malone-Lee, John, and Nigel P. Smart. "Modifications of ECDSA." International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2002.
18. Conti, Mauro, et al. "A survey on security and privacy issues of bitcoin." IEEE Communications Surveys & Tutorials 20.4 (2018): 3416-3452.
19. Paar, Christof, Peter Fleischmann, and Peter Roelse. "Efficient multiplier architectures for Galois fields G.F. (2/sup 4n/)." IEEE Transactions on Computers 47.2 (1998): 162-170.
20. Orlando, Gerardo, and Christof Paar. "A super-serial Galois fields multiplier for FPGAs and its application to public-key algorithms." Seventh Annual IEEE Symposium on Field-Programmable Custom Computing Machines (Cat. No. PR00375). IEEE, 1999.
21. Greenan, Kevin M., Ethan L. Miller, and Thomas JE Schwarz SJ. "Optimizing Galois Field arithmetic for diverse processor architectures and applications." 2008 IEEE International Symposium on Modeling, Analysis and Simulation of Computers and Telecommunication Systems. IEEE, 2008.
22. Paar, Christof. "A new architecture for a parallel finite field multiplier with low complexity based on composite fields." IEEE Transactions on Computers 45.7 (1996): 856-861.
23. Lesavich, Stephen, and Zachary C. Lesavich. "Method and system for storage and retrieval of blockchain blocks using galois fields." U.S. Patent No. 9,569,771. 14 Feb. 2017.
24. Koblitz, Neal. "elliptical curve cryptosystems." Mathematics of computation 48.177 (1987): 208.
25. Hoffstein, Jeffrey, et al. An introduction to mathematical cryptography. Vol. 1. New York: Springer, 2008, pp.487.
26. Hoffstein, Jeffrey, et al. An introduction to mathematical cryptography. Vol. 1. New York: Springer, 2008, pp.97.
27. https://realyst.com/digital-transaction-management/different-types-of-signatures.
28. Sklavos, Nicolas. "Book Review: Stallings, W. Cryptography and Network Security: Principles and Practice: Upper Saddle River, NJ: Prentice Hall, 2013, 752p., $142.40. ISBN: 13: 978-0133354690." (2014): 49-50, p431..
29. FIPS, PUB. "186 National Institute of Standards and Technology." FIPS PUB 186: Digital Signature Standard (1994).
30. Alsobky, Wageda, Hala Saeed, and Ali N. Elwakeil. "Different Types of Attacks on Block Ciphers."
31. El Sobky, Wageda I., et al. "Enhancing Hierocrypt-3 Performance by Modifying Its S-Box and Modes of Operations." Journal of Communications 15.12 (2020).
32. Mansour, Medhat, Ayman Hasan Wageeda Elsobky, and Wagdy Anis. "Appraisal of Multiple AES Modes Behavior using Traditional and Enhanced Substitution Boxes." no 5 (2020): 530-539.
33. Abdel-Hafez, Ahmed A., and Wageda_Hafez Reda-Elbarkouky. "Algebraic Cryptanalysis of AES using Gröbner Basis."
34. Abdel-Hafez, Ahmed A., and Wageda_ Hafez Reda-Elbarkouky. "Comparative Study of Algebraic Attacks."
35. Afify, Eslam & El, Wageda & Khalil, Abeer & Alez, Reda & Alsobky, Wageda. (2020). Algebraic Construction of Powerful Substitution Box. International Journal of Recent Technology and Engineering. 8. 10.35940/ijrte.D8279.038620.
36. Afify, Eslam & Khalil, Abeer & El, Wageda & Alez, Reda & Alsobky, Wageda. (2020). Performance Analysis of Advanced Encryption Standard (AES) S-boxes. 2277-3878. 10.35940/ijrte.F9712.059120.
37. Johnson, Don, Alfred Menezes, and Scott 1.
38. Douglas R. Stinson. Cryptography: Theory and Practice. Third Edition, 2006.
39. Ian F. Blake, Gadiel Seroussi, Nigel P. Smart Advances in elliptical curve Cryptography.
London Mathematical Lecture Note Series, 317, 2005, pp. 3-20.
40. Ujan Mukhopadhyay, Anthony Skjellum, Oluwakemi Hambolu, Jon Oakley, Lu Yu, Richard Brooks. A Brief Survey of Cryptocurrency Systems. 14th Annual Conference on Privacy, Securiy and Trust, 2016, pp. 745-752.
41. Dejan Vujičić, Dijana Jagodić, Siniša Ranđić. Blockchain Technology, Bitcoin, and
Ethereum: a Brief Overview. 17th International Symposium INFOTEH-JAHORINA, 2018,
pp. 1-6.
42. Olivier Alphand, Michele Amoretti, Timothy Claeys. IoTChain: a Block Security Architecture for the Internet of Things. IEEE Wireless Communications and Networking Conference, 2018, pp. 1-6.
43. Emre Yavuz, Ali Kaan Koc, Umut Can Cabuk, Gokhan Dalkilic. Towards Secure E-Voting Using Ethereum Blockchain. 6th International Symposium on Digital Forensic and Security, 2018, P.P. 1-7.
44. N. Koblitz. elliptical curve Cryptosystems. Mathematics of Computation, 48, 1987, pp. 203-209.
45. W. J. Caelli, E. P. Dawson, S. A. Rea. PKI, elliptical curve Cryptography, and digital signature. Computers & Security, 18, 1999, pp. 47-66.
46. Barsagade, Minal Wankhede, and Suchitra Meshram. "Overview of history of elliptical curves and its use in cryptography." International Journal of Scientific & Engineering Research 5.4 (2014): 467-471.
47. Doerner, J., Kondi, Y., Lee, E., & Shelat, A. (2018, May). Secure two-party threshold ECDSA from ECDSA assumptions. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 980-997).
48. https://www.geeksforgeeks.org/digital-signature-standard-dss/

## AUTHORS PROFILE

**Mustafa Hussien Mohamed,** was born in Egypt in 1994. He received a B.Sc. degree in computers from Military Technical College of engineering in 2017. He is currently a demonstrator at Benha Faculty of Engineering, Benha University, Egypt.

**Wageda Ibrahim El Sobky,** was born in Egypt in 1981. She received a B.Sc. degree in communications and computers from Benha faculty of engineering in 2003. She received a B.Sc. degree in science from Benha faculty of science in 2008. She received the M.Sc. in applied mathematics from Benha University, Cairo, Egypt, in 2012 and the Ph.D. degree in cryptography from Ain Shams University, Cairo, Egypt, in 2017. She is currently a doctor in basic engineering sciences at Benha Faculty of Engineering, Benha University, Egypt. Her current research interests include data security and cryptography.

**Sara Hamdy**, was born in Al Taif, Saudi Arabia in 1987. She received the B.S. and M.S. degrees in Electrical Engineering Technology from the University of Benha, Benha Faculty of Engineering, in 2014 and the Ph.D. degree in Philosophy in Engineering Sciences in Electrical Engineering from Benha University, Benha Faculty of Engineering, in 2020. From 2010 to 2014, she was a Demonstrator with the Electrical Engineering. From 2015 to 2091, she was an Assistant Lecturer in Electrical Engineering. She is currently an Assistant Professor, Electrical Department, Benha Faculty of Engineering, Benha University. Her current research interests include Video Processing.