IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 24, Issue 3, Ser. III (May. –June. 2022), PP 20-25
www.iosrjournals.org

Mathematical Model of Digital Signature based on ECDSA and ElGamal encryption techniques

Bhavadip Mogharіya[1], Ravi Gor[2]
[1]*Research Scholar, Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University, India*
[2]*Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University, India*

Abstract: *Today digitalization plays an important role in day-to-day life. Many things become easy by digitalization. In this digitalization, lots of data is shared over the open network. In case of sensitive data, security of this data is very important. Main security goals are confidentiality of data, authenticity of sender and non-repudiation. This paper proposes Digital Signature algorithm using Elliptic Curve Digital Signature Algorithm (ECDSA) and ElGamal encryption techniques.*

Key Word*: Digital Signature; ECDSA; ElGamal encryption scheme.*

Date of Submission: 06-06-2022 Date of Acceptance: 21-06-2022

I. Introduction

Now days lot of information go through the internet using different means. Some of the information are highly confidential and we cannot compromise with its security. So, we use lot of different techniques and algorithms to make our data as much secure as possible. And these techniques and algorithms are collectively called as Cryptography.

In Cryptography, for the communication, a sender gives some code to his massage. This process is called "encryption". After getting that code, receiver decodes it. This is known as "decryption".

One can find various algorithms according to the types of cryptography. In general, there are three types of Cryptography:

1. Symmetric Key Cryptography (Secret Key Cryptography)
2. Asymmetric Key Cryptography (Public Key Cryptography)
3. Hash function

Like secure exchange of messages, the exchange of documents requires special security measures to safeguard the information from unauthorized access. For that cryptography gives solutions in form of 'Digital Signature'.

Digital signature schemes are designed to provide the digital counterpart to handwritten signatures.

A digital signature is a number dependent on some secret, known only to the signer (the signer's private key) and additionally on the contents of the message being signed.

Signatures must be verifiable — if a dispute arises as to whether an entity signed a document, an unbiased third party should be able to resolve the matter equitably, without requiring access to the signer's private key.

Disputes may arise when a signer tries to repudiate a signature it did create, or when a forger makes a fraudulent claim.

There are mainly three stages in Digital signature as follows:

(1) Key Generation (2) Signature Generation (3) Signature Verification

Suppose there is a Sender A and a Receiver B: -

Sender (A) end: -

- Sender A inputs hash function, it generates a fixed binary value to a signature.
- Signature is formed with the help of private key encryption.
- Signature along with the original message is sent to the Receiver B.

Receiver (B) end: -

- When B receives the message from A Signature is decrypted with public key.

When the received message from the decryption is matched with the original message and results to be same, we can say that the message has been properly received from source to destination without losing its

contents and provides all internet security requirements i.e., integrity, confidentiality, non-repudiation, and authentication etc.

Mathematical Model of ECDSA:

An Elliptic Curve E defined over a field $K = F_p$ is the set of points satisfying equation $y^2 = x^3 + ax + b$ Where $a, b \in K$ and $4a^3 + 27b^2 \neq 0 \ (mod\ p)$, where characteristic of K is neither 2 nor 3.

This elliptic curve also contains a special point O, called the point at infinity.

Each value of a and b gives a different elliptic curve.

Elliptic curve operations are defined over finite fields. The main operation, Point multiplication is achieved by two basic elliptic curve operations.

(1) Point addition (2) Point doubling

(1) Point addition:

Point addition is the addition of two points P and Q on an elliptic curve to obtain another point R on the same elliptic curve. i.e., $R = P + Q$.

Consider two points P and Q on an elliptic curve as shown in Figure 1. If $P \neq -Q$ then a line drawn through the points P and Q will intersect the elliptic curve at exactly one more point $-R$ (negative of R).

The reflection of the point $-R$ with respect to $X - axis$ gives the point R, which is the result of addition of points P and Q.

Thus, on an elliptic curve $R = P + Q$. If $Q = -P$ the line through this point intersects at a point at infinity O.

Hence $P + (-P) = O$. A negative of a point is the reflection of that point with respect to $X - axis$.

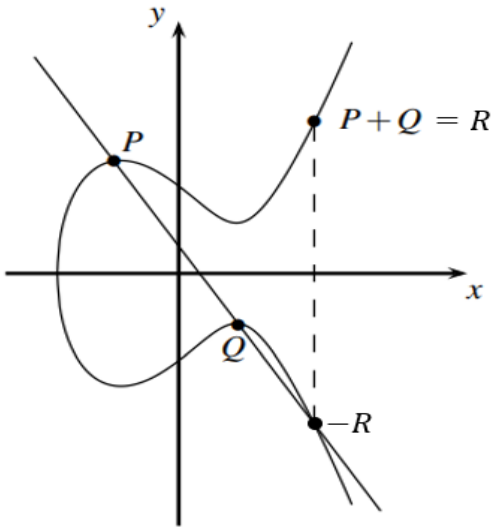

Figure 1 (Point Addition)

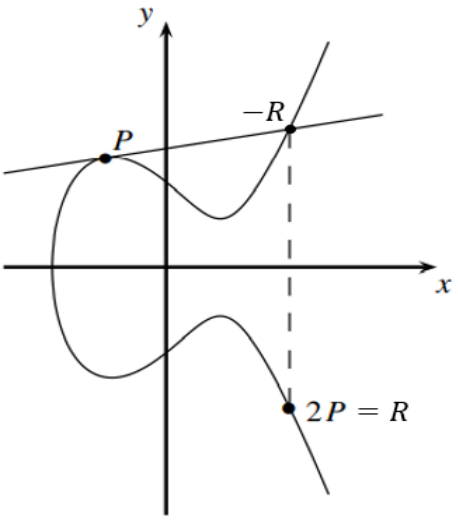

Figure 2 (Point Doubling)

(2) Point doubling:

Point doubling: adding a point P to itself to obtain another point R. i.e., $R = 2P$.

Point doubling is the addition of a point P on the elliptic curve to itself to obtain another point R on the same elliptic curve. i.e., $R = 2P$.

Consider a point P on an elliptic curve as shown in Figure 2. If y coordinate of the point P is not zero, then the tangent line at P will intersect the elliptic curve at exactly one more point $-R$.

The reflection of the point $-R$ with respect to $X - axis$ gives the point R, which is the result of doubling the point P. i.e., $R = 2P$.

If y coordinate of the point P is zero, then the tangent at this point intersects at a point at infinity O. Hence $2P = O$ when $y_j = 0$. Figure 2 shows point doubling.

Algebraically, let $P(x_1, y_1)$ and Q(x_2, y_2) are two points on the elliptic curve then

$$R = P + Q = \begin{cases} 0 & if\ x_1 = x_2 \\ Q & if\ P = 0 \\ (x_3, y_3) & otherwise \end{cases}$$

Where $x_3 = \begin{cases} \lambda^2 - x_1 - x_2\,, & if\ P \neq Q\ (Point\ addition) \\ \lambda^2 - x_1\,, & if\ P = Q\ (Point\ doubling) \end{cases}$

and $y_3 = \lambda(x_1 - x_3) - y_1$

Where $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}\,, & if\ P \neq Q\ (Point\ addition) \\ \frac{3x^2 + a}{2y_1}\,, & if\ P = Q\ (Point\ addition) \end{cases}$

ECDSA [15] is a Digital signature algorithm based on Elliptic Curve Cryptography. There are mainly three steps:

(1) Key Generation (2) Signature Generation (3) Signature Verification

Let an entity A want to send a message to B then the steps are as follows:

Before the Key Generation Signer choose some parameters, prime number p, a and b. Using these parameters define a particular elliptic curve.

A Point P on curve $y^2 = x^3 + ax + b$ is a Base Point which generate a Group, integer n is order of group generated by P.

(1) Key Generation:

a) Select a random integer d in the interval [1, n - 1]
b) Compute Q = dP
c) A's public key is Q: A's private key is d

(2) Signature Generation:

a) Select a random integer k in the interval [1, $n - 1$]
b) Compute $kP = (x_1, y_1)$ and $r = x_1\ mod\ n$ (where x_1 is regarded as an integer between 0 and $q - 1$). If $r = 0$ then go back to step 1
c) Compute $t = k^{-1}$
d) Compute, $s = k^{-1}(H(m) + dr)\ (mod\ n)$ where h is the Secure Hash Algorithm. If $s = 0$, then go back to step 1
e) The signature for the message m is the pair of integers (r, s)

(3) Signature Verification:

a) Obtain an authenticated copy of Sender's Public key Q
b) Verify that r and s are integers in the interval $[1, n - 2]$
c) Compute $w = s^{-1}\ (mod\ n)$ and $H(m)$
d) Compute $u_1 = H(m)w\ (mod\ n)$ and $u_2 = rw\ (mod\ n)$
e) compute $u_1P + u_2Q = (x_0, y_0)$ and $v = x_0\ (mod\ n)$
f) Accept the signature if and only if $v = r$

ElGamal Encryption Technique [15]:

Just like the ECDSA, ElGamal algorithm has three steps:

(1) Key Generation (2) Encryption (3) Decryption

(1) Key Generation:

a) Select large prime number p
b) Select primitive element $\alpha \in \mathbb{Z}_p^*$
c) Select $K_{pr} = d \in \{2,3, \dots, p - 2\}$ as the private key
d) Calculate $K_{pub} = \beta = \alpha^d\ mod\ p$ as the public key
e) Then p, α and β are published as public key while d should be kept secret as a private key

(2) Encryption:

a) The receiver's public key (p, α, β) is obtained
b) Select random integer number i
c) Calculate ephemeral key $K_E = \alpha^i\ mod\ p$
d) Calculate masking key $K_M = \beta^i\ mod\ p$
e) Calculate cipher text as $C = m \cdot K_M\ mod\ p$ Where, m is the secret message which is to be encrypted
f) The Cipher text C and K_E sent to the receiver

(3) Decryption:

a) Calculate masking key $K_M = K_E^d\ mod\ p$
b) Recover the secret message m by using the formula: $m = C(K_M)^{-1}\ mod\ p$

II. Literature Review

ElGamal [5] (1985) discussed a new signature scheme with an implementation of the Diffie-Hellman key distribution scheme that achieves a public key cryptosystem. Security of this scheme relies on the difficulty of computing discrete logarithms over finite fields.

Neal [13] (1985) introduced Elliptic Curve Cryptography. This Elliptic Curve Cryptosystem is more secure because of the analog of the discrete logarithm problem. This paper discussed Elliptic Curves and different operations of points over finite field.

Neal [14] et. al. (2000) in their paper surveyed the development of elliptic curve cryptosystems from their inception in 1985.

Kefa [10] (2005) concluded that The DSA is based on the ElGamal signature algorithm. However, this ElGamal signature is not same as Elagaml encryption and decryption schemes.

Jarusombat [6] et. al. (2006) provided a digital signature technique on mobile devices based on location. This technique works on those devices that have low computational capability and low battery time period by using GPS technology and also by applying geo-encryption and mobility model in process of digital signature generation.

Markus [11] (2015) in their work compared the security levels of RSA and ECC. He presented the ECDSA and its applications. Furthermore, implementation failures like in the case of the ECDSA based code authentication of the PlayStation 3 in 2010 was analyzed.

Kadek [9] et. al. (2017) designed a digital signature algorithm by combining MAC address with AES-128. First of all, SHA-256 is used to generate hash code and further this hash value is encrypted using encryption technique generated by combining features of MAC address and AES algorithm.

Bharathi [2] (2018) proposed improved ElGamal encryption technique for elliptic curve cryptography. By the analysis it has been concluded that proposed scheme in this paper outperforms the standard ElGamal encryption technique.

Mishall [12] et. al. (2019) in their work they discussed detailed and comprehensive survey of an update of the ECDSA algorithm in terms of performance, security and applications.

Thakkar and Gor [20] (2021) represented a review of literature concerned with cryptographic algorithms and mathematical transformations. The review of RSA and ElGamal algorithms aids readers in better understanding the differences between the two asymmetric key cryptographic algorithms.

III. Proposed Method

A Sender Bob wants to send a message to a Receiver Alice. Then the model work as given below.

- Firstly, Bob chooses parameters to use ECDSA algorithm. Similarly, Alice also chooses parameters to use ElGamal encryption technique.
- Using above parameters Bob generates a key for signing and Alice generates a key for encryption and share this key to Bob.
- Using the key shared by Alice, Bob encrypts the message by ElGamal encryption technique.
- Now Bob generates signature for this encrypted message by ECDSA.
- Then Bob sends this signature to Alice along with encrypted message and key which are required for signature verification.
- Lastly, Alice verifies the signature by ECDSA.
- If signature is verified then Alice decrypts the cipher text by ElGamal encryption technique to read the original message. If it is not verified then it means someone has forged the original data.

IV. Algorithm of the Mathematical Model

Let Bob want to send a message m=26 to Alice. Then Bob and Alice follow the following phases and steps.

Phase I: Selection of Parameters

Step 1: Bob chooses following parameters for ECDSA: prime $p = 17$, $a = 2, b = 2$.
So, Elliptic curve becomes $y^2 = x^3 + 2x + 2$. Select Generator point $P = (5,1)$.
Then order of group generated by P is $n = 19$.

Step 2: Alice chooses following parameters for ElGamal encryption technique: prime $q = 29$ and a primitive element $\alpha = 2$.

Phase II: Key Generation

Step 1: Bob chooses $d = 7$, where $1 \leq d \leq 18$ and calculate $Q = dP = 7(5,1) = (0,6)$.

So, private key $d = 7$ and public key $Q = (0,6)$ for ECDSA.

Step 2: Alice chooses $\lambda = 12$, where $2 \leq \lambda \leq 27$.
Calculate $\beta = 2^{12} \ (mod\ 29) = 7 \ (mod\ 29)$. So, private key $\lambda = 12$ and public key $\beta = 7$ for ElGamal encryption technique.
Alice shares this public key to Bob.

Phase III: Signature Generation

Step 1: For ECDSA Bob chooses $k = 10$, where $1 \leq k \leq 18$.
Calculate $kP = (x_1, y_1) = 10(5,1) = (7,11)$. So, $r = x_1 = 7 \ (mod\ 19)$.

Step 2: To encrypt the message by ElGamal encryption technique,
Bob chooses $i = 5, 1 \leq i \leq 28$. Calculate $K_E = \alpha^i = 2^5 = 3 \ (mod\ 29)$.
Also calculate $K_M = \beta^i = 7^5 = 16 \ (mod\ 29)$.
Encrypt the message m, Cipher text $e = m * K_M = 26 * 16 \ (mod\ 29)$
$= 416 \ (mod\ 29) = 10 \ (mod\ 29)$.
So, Encrypted message $e = 10$.

Step 3: Compute Hash value of encrypted message, $H(e) = H(10) = 26$.
Compute $s = k^{-1}(H(e) + d * r)(mod\ n) = 2(26 + 7 * 7) \ (mod\ 19)$
$= 17 \ (mod\ 19)$.
So, Signature is $(r, s) = (7,17)$.

Bob shares encrypted message $e = 10$ and signature $(r, s) = (7,17)$ along with $Q = (0,6), K_E = 3, a = 2, b = 2, p = 17, n = 19, P = (5,1)$.

Phase IV: Signature Verification

Step 1: Alice verifies that r and s are between 1 and 17 $(= n - 2)$.
Finds Hash value of encrypted message $e = 10$ which is $H(10) = 26$.

Step 2: Now calculate $w = s^{-1} = 17^{-1} = 9 \ (mod\ 19)$.

Step 3: Calculate $u_1 = H(e) * w = 26 * 9 \ (mod\ 19) = 6 \ (mod\ 19)$.
Also $u_2 = r * w = 7 * 9 \ (mod\ 19) = 6 \ (mod\ 19)$.

Step 4: Now find $(x, y) = u_1 P + u_2 Q = 6(5,1) + 6(0,6) = (7,11)$.
So, $x = 7 \ (mod\ 19)$.

Step 5: Verify $r = x$ or not. Here $r = 7 = x$.
So, Signature is verified.
If signature is not verified, then someone has forged the shared data.

Step 6: If Signature is verified then decrypt the cipher text to read the original text.
Calculate $K_M = (K_E)^{\lambda} \ (mod\ q) = (3)^{12} \ (mod\ 29) = 16 \ (mod\ 29)$.

Step 7: Calculate $m = e * (K_M)^{-1} (mod\ p) = 10 * (16)^{-1} \ (mod\ 29) = 26 \ (mod\ 29)$.
So, Alice got original message $m = 26$ sent by Bob.

V. Conclusion

Proposed method of digital signature avoids forgery of shared data. Moreover, this method also features authenticity and non-repudiation. Such type of algorithm provides strong security as there is no plain text in calculation of algorithm as well as in the sharing. Provided algorithm shares message but in hidden form which increase the security as well as authenticity because of ECDSA algorithm.

References

[1]. Benjamin K. (2017). "Elliptic Curve Digital Signatures and Their Application in the Bitcoin Crypto-currency Transactions", International Journal of Scientific and Research Publications (IJSRP), Volume 7, Issue 11, ISSN 2250-3153.education (8)

[2]. C.R. Bharathi (2018). "Improved ElGamal encryption for Elliptic curve cryptography", Volume 118, Issue 17, ISSN-1311-8080(Printed Version).

[3]. Dindayal M. and Dilip Kumar Y. (2017). "RSA and ECC: A Comparative Analysis", International Journal of Applied Engineering Research, Volume 12, ISSN 0973-4562.

[4]. Don J., Alfred M., Scott V. (2001). "The elliptic curve digital signature algorithm (ECDSA)", International journal of information security 1, no. 1, pp.36-63.

[5]. ElGamal T. (1985). "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm", IEEE Transaction on Information Theory, volume IT-31, No.4, July 1985, pp.10-18.

[6]. Jarusombat, Santi, and Surin Kittitornkun (2006). "Digital signature on mobile devices based on location." In 2006 International Symposium on Communications and Information Technologies, IEEE, pp. 866-870.

[7]. Jayabhaskar M. and Prof. Bachala S. (2012). "Implementation of Elliptic Curve Digital Signature Algorithm Using Variable Text Based Message Encryption", International Journal of Engineering Research (IJCER), Volume 2, Issue 5, ISSN 2250-3005.

[8]. Joselin J., S. J. Brintha, V. Magesh (2015). "Role of Digital Signature in Network Security and Cryptography", International Journal of Computer Science and Information Technologies (IJCSIT), Volume 6(1), ISSN 0975-9646.

[9]. Kadek D., M. Rizqia, Leonardus I., Guruh F. (2017). "Digital Signature using MAC address based AES128 and SHA-2 256-bit", International Seminar on Appliction for Technology of Information and Communication (iSemantic), IEEE.
[10]. Kefa R. (2005). Elliptic Curve ElGamal Encryption and Signature Schemes", Information Technology Journal., 4(3), ISSN 1812-5638, page 299-306
[11]. Markus S. (2015). "ECDSA-Application and Implementation Failure".
[12]. Mishall Al Z., Zhongwei Z., Ji Z. (2019). Efficient and Secure ECDSA Algorithm and its Applications: A Surveyor.
[13]. Neal K. (1985). "Elliptic Curve Cryptosystems", Mathematics of Computation, Volume 48, Number 177, Pages 203-209.
[14]. Neal K., Alfred M., Scott V. (2000). "The State of Elliptic Curve Cryptography", Designs, Codes and Cryptography, 19, pp.173-193.
[15]. Paar C. and Pelzl J. (2009). "Understanding cryptography: a textbook for students and practitioners", Springer Science & Business Media.
[16]. Payel S. (2016). "A comprehensive study on digital signature for internet security", ACCENTS Transactions on Information Security, Volume1(1), ISSN(Online) 2455-7196.
[17]. Rahat A. and S. C. Mehrotra (2011). "A Review on Elliptic Curve Cryptography for Embedded Systems", International Journal of Computer Science & Information Technology (IJCSIT), Volume3(3).
[18]. R. Rivest, A. Shamir, L. Adleman (1978). "A Method for Obtaining Digital Signature and Public key Cryptosystems", Communication of the ACM, Vol. 21, No. 2, pp.120-126.
[19]. Shivendra S., Md. Safaraz I., Arunima J. (2015). "Survey on Techniques Developed using Digital Signature: Public key Cryptography", International Journal of Computer Applications, Volume 117, ISSN 0975-8887.
[20]. Thakkar A. and Gor R. (2021). "A Review paper on Cryptographic Algorithms and Mathematical Transformations", Proceeding of International Conference on Mathematical Modelling and Simulation in Physical Sciences (MMSPS), Excellent Publishers, ISBN: 978-81-928100-1-0, 324-331.
[21]. William Stallings. "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition.
[22]. Zhang, Qiuxia, Zhan Li, Chao Song. (2011). "The Improvement of digital signature algorithm based on elliptic curve cryptography", In 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), IEEE, pp. 1689-1691.

Bhavadip Mogharіya, et. al. "Mathematical Model of Digital Signature based on ECDSA and ElGamal encryption techniques." *IOSR Journal of Computer Engineering (IOSR-JCE),* 24(3), 2022, pp. 20-25.