IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 19, Issue 4 Ser. 1 (July. – August. 2023), PP 01-07
www.iosrjournals.org

Mathematical Model of Digital Signature based on ECDSA and Rabin encryption technique

Bhavadip Mogharіya[1], Ravi Gor[2]
[1]*Research Scholar, Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University*
[2]*Department of Applied Mathematical Science, Actuarial Science and Analytics, Gujarat University*
[1]*bhavadipmogharіya@gujaratuniversity.ac.in*

ABSTRACT: *In recent years, the internet plays a vital role in education, business and other industries. Tons of data are transferred using the internet. This results in a number of concerns, including data confidentiality, user authenticity, non-repudiation and so on. To address this issue, more research on digital signatures should be conducted in order to increase the data security and authenticity of transferred data. Digital Signature is an electronic signature that can be used to authenticate the identity of the sender. It ensures that the content of the message or document that has been sent is unchanged. In this study, a new digital signature method is mathematically modelled using the Elliptic Curve Digital Signature Algorithm (ECDSA) and Rabin encryption technique. It provides features like confidentiality, non-repudiation and authenticity.*

Keywords: *Digital Signature, ECDSA, Rabin encryption technique.*

Date of Submission: 20-06-2023 Date of Acceptance: 02-07-2023

I. INTRODUCTION

Data Storage and Data Transmission is a very crucial part in the virtualisation. For users who wish to access data stored on the cloud, data security and authenticity are essential. So, various techniques and algorithms of cryptography have been used to make data secure.

Cryptography is a powerful tool for securely transmitting data over the internet. During transmission, some algorithm converts data into a different form. As a result, no one can access the data. This process is known as "encryption". After receiving the data, the receiver converts it into readable form, which is known as "decryption".

There are different types of algorithms based on,

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

Cryptography also includes Digital Signatures, which provide various benefits during data transfer over an open network. A digital signature is merely a number generated by several algorithmic operations. A digital signature provides evidence of the owner's identity and ensures that they cannot deny their signature. If signature is not verified by receiver, there are some possibilities of forgery in shared data.
Different kinds of digital signature algorithms are used to create and validate the signature. Some well-known signature algorithms are RSA Digital Signature Algorithm, ElGamal Digital Signature Algorithm, and Elliptic Curve Digital Signature Algorithm (ECDSA).

Digital Signature algorithm have mainly three steps:
(1) Key Generation (2) Signature Generation (3) Signature Verification

Currently, ECDSA is widely used in different applications. ECDSA has a very high level of computational complexity when compared to other algorithms, which offers great security against various forms of attacks. ECDSA is based on Elliptic Curve Cryptography, which requires some different algebraic operations.

Mathematical Model of ECDSA:

An Elliptic Curve E is defined over a field $K = F_p$. Which is the set of points satisfying an equation

$$y^2 = x^3 + ax + b, \quad \text{where } a, b \in K \text{ and } 4a^3 + 27b^2 \neq 0 \pmod p,$$

Here, characteristic of $K = F_p$ is neither 2 nor 3.

Different values of a and b gives different elliptic curves. These elliptic curves also contain a special point O, called the point at infinity.

Set of points on Elliptic Curve form a group under a specific binary operation. This binary operation is 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

Consider two distinct points P and Q on an elliptic curve as shown in Figure 1. If $Q \neq -P$ 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 addition of points P and Q. Thus, on an elliptic curve, $P + Q = R$. If $Q = -P$, the line through this point does not intersect to Elliptic Curve at any point. So, it is considered that line intersects a point at infinity O. Hence, $P + (-P) = O$. Negative of a point is the reflection of that point with respect to $X-$ axis.

(2) Point doubling

Point doubling is the addition of a point P on the elliptic curve to itself. It obtains 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 nonzero, then the tangent line at P will intersect the elliptic curve at exactly one more point say $(-R)$. 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 a point at infinity O. Hence, $2P = O$ when $y_j = 0$.

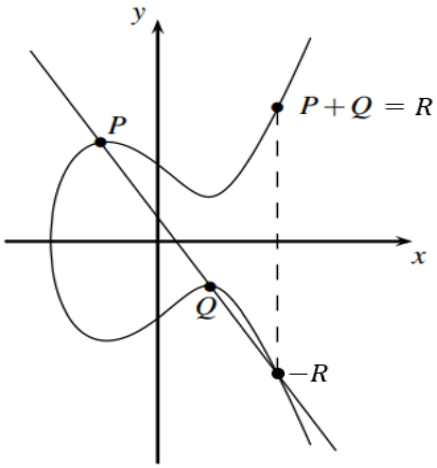

Figure 1 (Point addition)

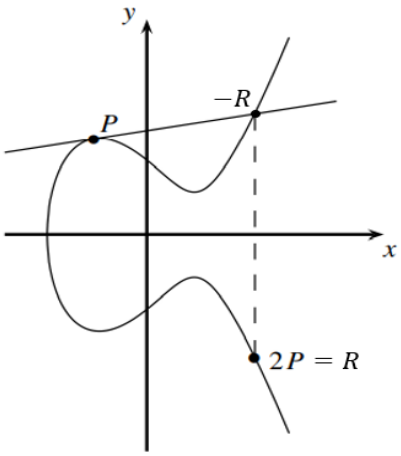

Figure 2 (Point doubling)

Algebraically, addition can be defined as follows:

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

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

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

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

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

ECDSA is a Digital signature algorithm based on Elliptic Curve Cryptography. It is much better than RSA encryption and signature algorithm. In compare to RSA, it uses smaller key and have same security level because of its complex operations.

Let an entity A wants to send a message to B then the steps are as follows:
Before the key generation, signer choose some parameters, prime numbers p, a and b. These parameters are used to define a specific elliptic curve. A point P on curve $y^2 = x^3 + ax + b$ is a base point. P generates a group of prime order n.

(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 and 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 $r = x_1 \bmod n$ (where x_1 is regarded as an integer between 0 and $q - 1$). If $r = 0$, then reselect k
c) Compute $t = k^{-1}$
d) Compute, $s = k^{-1}(H(m) + dr) \pmod n$ where $H(m)$ is the hash value compute by secure hash algorithm. If $s = 0$, then reselect k
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 the integers r and s are in the interval $[1, n - 1]$
c) Compute $w = s^{-1} \pmod n$ and $H(m)$
d) Compute $u_1 = H(m)w \pmod n$ and $u_2 = rw \pmod n$
e) Compute $u_1P + u_2Q = (x_0, y_0)$ and $v = x_0 \pmod n$
f) Accept the signature if and only if $v = r$

Rabin encryption technique
Rabin algorithm introduced by Michael O. Rabin in 1979. It is based on factorization of a large number as prime numbers.
Rabin encryption technique also has three steps:
(1) Key Generation (2) Encryption (3) Decryption
(1) Key Generation
a) Choose two distinct large prime numbers p and q such that $2^k < p, q < 2^{k+1}$ and $p, q \equiv 3 \pmod 4$
b) Calculate $n = pq$
c) Public key is n and private keys are p and q
(2) Encryption
a) Represent the message by integer m in the interval $[1, n - 1]$
b) Compute $C = m^2 \pmod n$
c) Cipher text is C and send it to the receiver
(3) Decryption
a) Compute two integers r and s such that $rp + sq = 1$
b) Compute $m_p \equiv C^{\frac{p+1}{4}} \pmod p$
c) Compute $m_q \equiv C^{\frac{q+1}{4}} \pmod q$
d) Compute $m_1 \equiv rpm_q + sqm_p \pmod n$
e) Compute $m_2 \equiv rpm_q - sqm_p \pmod n$
f) Compute $m_3 \equiv -m_2 \pmod n$
g) Compute $m_4 \equiv -m_1 \pmod n$
h) Convert these four values m_1, m_2, m_3 and m_4 in the binary representation.
i) One of these four binary representations contains same doubled representation which will be plain text

II. LITERATURE REVIEW

Rabin [16] (1979) introduced a public key function. It included a number as a product of two primes. The function was based on the difficulty to find the square root modulo of a composite number. Computation time for this function was very low then the RSA scheme. The function in RSA scheme was one-one but this function was four to one. So, it needs bit of modification for the applications.

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

Hieu and Tuan [7] (2012) proposed two Multi-signature schemes based on the discrete logarithm problem and the difficulty of finding the k^{th} roots of number with modulo of prime p. In this Multi-signature scheme, signature was generated by multiple entity with multiple private keys.

Hashim [6] (2014) presented a H-Rabin cryptosystem which was modified version of original Rabin encryption algorithm. The new algorithm was defined by considering three primes as private keys. Public key was composition of these three primes.

Budiman et al. [4] (2019) analysed cryptanalysis of the public key for Rabin encryption technique using Fermat factorization method to obtain p and q. Additionally, it was determined whether both of the factors were compatible with the Rabin private key or not. It was concluded that the value of n does not always correlate with the factoring time.

Asbullah and Ariffin [1] (2016) proposed a cryptosystem which was similar to Rabin cryptosystem but without use of Jacobi symbol. This proposed cryptosystem namely Rabin-p cryptosystem which only uses a single prime p as the decryption key. Also, procedure required only one modular exponentiation during the decryption process which reduces the computational effort.

Asbullah and Ariffin [2] (2016) examined the Rabin-p cryptosystem. It was analysed that the prime factors of its public key can be found amongst the list of the continued fraction expansion of the ciphertext c and the modulus in polynomial time. For the second analysis, by using the Coppersmith's theorems they showed that the message m can be retrieved in polynomial time provided some condition on the message length. They also proposed a countermeasure to avoid both analyses.

Mahad et al. [12] (2017) offered two distinct methods using the modulus of the type $N = p^2q$ coupled with the restriction on the plaintext space M. In the first method, the plaintext space was limited to $M \in \mathbb{Z}_{pq}$. For the second method, they restrict the plaintext in the range of $M \in (0, 2^{2n-2})$. They proved that the decryption output of the proposed methods was unique and without decryption failure. The results in this work indicate that the decryption problem of Rabin cryptosystem was overcome.

Zhang et al. [18] (2011) proposed the improved digital signature algorithm based on the elliptic curve cryptography and enhance the security of the digital signature. This proposed method increased one step that encrypt signature with signer's private key and then sent the encrypted result to the verifier. Verifier verifies the encrypted result before verifying the signature.

Kavin and Ganapathy [11] (2021) proposed an Enhanced Digital Signature Algorithm (EDSA) for verifying the data integrity while storing the data in cloud database. Proposed EDSA had been developed according to the Elliptic Curve Square points that were generated by using an upgraded equation and these points were used as public key. A new base formula was also introduced for signing and verification process. This work introduced a new compression technique which had been used for reducing the bit size of the signature.

III. PROPOSED METHOD

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

Step 1: Firstly, Bob chooses parameters to use ECDSA algorithm. Similarly, Alice also chooses parameters to use Rabin encryption technique.

Step 2: Using above parameters Bob generates a key for signing and Alice generates a key for encryption and share this key to Bob.

Step 3: Using the key shared by Alice, Bob encrypts the message by Rabin encryption technique.

Step 4: Now, Bob generates signature for this encrypted message by ECDSA.

Step 5: Then Bob sends this signature to Alice along with encrypted message and key which are required for signature verification.

Step 6: Lastly, Alice verifies the signature by ECDSA.

Step 7: If signature is verified, Alice decrypts the cipher text by Rabin encryption technique to read the original message. If it is not verified, then it means someone has forged the original data.

IV. NUMERICAL EXAMPLE OF THE PROPOSED METHOD

Let Bob wants to send a message '$m = 51$' to Alice. Then Bob and Alice will follow the following phases and steps.

Phase I: Selection of Parameters

Step 1: Bob chooses following parameters for ECDSA: prime $p = 41$, $a = 3, b = 12$.
So, elliptic curve becomes $y^2 = x^3 + 3x + 12$. Select generator point $P = (1,4)$.

Then order of group generated by P is $n = 17$ which is prime.

Step 2: Alice chooses security parameter $k = 6$ for Rabin encryption technique.

Phase II: Key Generation

Step 1: Bob chooses $d = 11$, where $1 \leq d \leq 16$ and calculate $Q = dP = 11(1,4) = (24,3)$.
So, private key $d = 11$ and public key $Q = (24,3)$ for ECDSA.

Step 2: Alice chooses prime $\alpha = 83 \equiv 3 \pmod 4$ and $q = 107 \equiv 3 \pmod 4$.
Also $2^6 < \alpha, \beta < 2^7$.
Calculate $N = \alpha\beta = 83 * 107 = 8881$.
Private key is $\alpha = 83, \beta = 107$ and public key is $N = 8881$.
Alice shares this public key to Bob for encryption.

Phase III: Signature Generation

Step 1: For ECDSA Bob chooses $k_E = 9$, where $1 \leq k_E \leq 16$.
Calculate $k_E P = (x_1, y_1) = 9(1,4) = (22,36)$. So, $r = x_1 = 22 = 5 \pmod{17}$.

Step 2: To encrypt the message by Rabin encryption technique,
Bob converts message '$m = 51$' to binary digit $m = 51 = (110011)_2$.
Append this binary number with same value. So, new value is $(110011 \mid 110011)_2$.
Converting this binary value to decimal value, the new modified message is $M = 3315$.
Encrypt the message $m = 51$, by calculating $e = M^2 \pmod N$

$$= (3315)^2 \pmod{8881}$$

$$e = 3428$$

So, encrypted message is $e = 3428$.

Step 3: Compute the Hash value of encrypted message,

$$H(e) = H(3428) = (4500e4037738e13c0c18db508e18d483)_{16}$$
$$= (917213563731307950087858200849715580 19)_{10}.$$

Compute $s = k^{-1}(H(e) + d * r) \pmod n$
$= 2 * (917213563731307950087858200849715580 19 + 11 * 5) \pmod{17}$
$= 3 \pmod{17}$
So, signature is $(r, s) = (5,3)$.

Bob shares encrypted message $e = 3428$ and signature $(r, s) = (5,3)$ along with public key $Q = (24,3), P = (1,4)$ and parameters $a = 3, b = 12, p = 41, n = 17$.

Phase IV: Signature Verification and Decryption of Cipher text

Signature Verification

Step 1: Alice verifies that $r = 5$ and $s = 3$ lies in the interval $[1,16]$ $(= [1, n-1])$.
Find the hash value of encrypted message $e = 3428$.
which is,

$$H(3428) = (4500e4037738e13c0c18db508e18d483)_{16}$$
$$= (917213563731307950087858200849715580 19)_{10}$$

Step 2: Now, calculate $w = s^{-1} = 3^{-1} = 6 \pmod{17}$.

Step 3: Calculate $u_1 = H(e) * w$
$= 917213563731307950087858200849715580 19 * 6 \pmod{17}$
$= 2 \pmod{17}$.
Also, $u_2 = r * w = 5 * 6 \pmod{17} = 13 \pmod{17}$.

Step 4: Find $(x, y) = u_1 P + u_2 Q = 2(1,4) + 13(24,3) = (22,36)$.
So, $x = 22 = 5 \pmod{17}$.

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

Decryption of Message

Step 6: If Signature is verified, decrypt the cipher text by Rabin algorithm to read the original text.
Compute $y_\alpha * \alpha + y_\beta * \beta = y_\alpha * 83 + y_\beta * 107 = 1 = GCD(\alpha, \beta)$.
Hence, $y_\alpha = 49$ and $y_\beta = -38$.

Step 7: Calculate $m_\alpha = e^{\frac{\alpha+1}{4}} \pmod \alpha = (3428)^{21} \pmod{83} = 78 \pmod{83}$.

$$m_\beta = e^{\frac{\beta+1}{4}} \pmod{\beta} = (3428)^{27} \pmod{107} = 105 \pmod{107}.$$

Step 8: Compute $m_1 = y_\alpha * \alpha * m_\beta + y_\beta * \beta * m_\alpha \pmod{N}$

$$= 49 * 83 * 105 + (-38) * 107 * 78 \pmod{8881}$$

$$m_1 = 3315 \pmod{8881}$$

$$m_2 = y_\alpha * \alpha * m_\beta - y_\beta * \beta * m_\alpha \pmod{N}$$

$$= 49 * 83 * 105 - (-38) * 107 * 78 \pmod{8881}$$

$$m_2 = 7060 \pmod{8881}$$

Now, $m_3 = -m_1 \pmod{N} = -3315 \pmod{8881} = 5566 \pmod{8881}$

Similarly, $m_4 = -m_2 \pmod{N} = -7060 \pmod{8881} = 1821 \pmod{8881}$

Thus, $m_1 = 3315$, $m_2 = 7060$, $m_3 = 5566$ and $m_4 = 1821$

Step 9: Convert these four values in binary form.

$m_1 = (3315)_{10} = (110011110011)_2$

$m_2 = (7060)_{10} = (1101110010100)_2$

$m_3 = (5566)_{10} = (1010110111110)_2$

$m_4 = (1821)_{10} = (11100011101)_2$

Here, m_1 has same binary representation from middle to left and right. Therefore, m_1 is the plain text. Considering one half of this representation and convert it into decimal to read the message.

So, original message is $m = (110011)_2 = 51$.

Alice got the unforged and signed message sent by Bob.

V. CONCLUSION

The method proposed in this paper uses features of Elliptic Curve Digital Signature Algorithm (ECDSA) and Rabin encryption technique. The suggested digital signature method prevents the forging of shared data, and the receiver can also detect any forgery in shared data. Since the data is encrypted in the suggested manner, a third party cannot access it. The decryption procedure gives four outputs, only one will be plaintext among these four. So, one cannot determine plaintext easily. Moreover, this method also features authenticity and non-repudiation. Proposed method provides strong security as there is no plaintext in calculation of algorithm as well as in the sharing.

REFERENCES

[1]. Asbullah, M. A., Ariffin, M. R. K. (2016). "Algebraic Analysis of a Rabin-Like Cryptosystem and Its Countermeasures". Indian Journal of Science and Technology, 9(1), 1-5.

[2]. Asbullah, M. A., & Ariffin, M. R. K. (2016). "Design of Rabin-like cryptosystem without decryption failure". Malaysian Journal of Mathematical Sciences, 10, 1-18.

[3]. 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.

[4]. Budiman, M. A., Rachmawati, D., & Utami, R. (2019, June). "The cryptanalysis of the Rabin public key algorithm using the Fermat factorization method". In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012084). IOP Publishing.

[5]. 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.

[6]. Hashim, H. R. (2014). "H-Rabin cryptosystem". Journal of Mathematics and Statistics, Volume 10, Issue 3, pp.304-308, ISSN 1549-3644(online).

[7]. Hieu, M. N., & Tuan, H. D. (2012, October). "New multisignature schemes with distinguished signing authorities". In The 2012 International Conference on Advanced Technologies for Communications (pp. 283-288). IEEE.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Kavin, B. P., & Ganapathy, S. (2021). "A new digital signature algorithm for ensuring the data integrity in cloud using elliptic curves". The International Arab Journal of Information Technology, 18(2), 180-190.

[12]. Mahad, Z., Asbullah, M. A., & Ariffin, M. R. K. (2017). Efficient methods to overcome Rabin cryptosystem decryption failure. Malaysian Journal of Mathematical Sciences, 11, 9-20.

[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]. Rabin, M. O. (1979). "Digitalized signatures and public-key functions as intractable as factorization". Massachusetts Inst of Tech Cambridge Lab for Computer Science.

[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]. Zhang, Q., Li, Z., & Song, C. (2011, August). "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) (pp. 1689-1691). IEEE.