International Conference on Recent Innovations in Science, Engineering & Management
R.R. INSTITUTE OF TECHNOLOGY, Bengaluru (India)
10th - 11th May 2019 www.conferenceworld.in ISBN : 978-93-87793-87-3

Elliptical Curve Cryptography Digital Signature Algorithm (ECDSA)

Manasa H.R, Krishna R.Kulkarni, Keerthana B

Manasa H.R,Department of Information science & Engineering,SKIT College

Krishna R.Kukarni,SKIT College

Keerthana B,SKIT College

Abstract- *Data encryption is used widely to ensure high security in open networks such as the internet. The fast development of cryptography research and computer technology, capabilities of cryptosystems such as RSA and Diffie-Hellman are inadequate due the requirement of large number of bits. The cryptosystem based on Elliptic Curve Cryptography (ECC) is becoming the recent trend of public key cryptography.In recent years, Elliptic Curve Cryptography (ECC) has grabbed the attention of researchers and product developers because of its robust mathematical structure and highest security in comparison to other existing algorithms like RSA (RivestAdleman and Shameer Public key Algorithm) and ELGAMAL algorithm. Elliptic Curve Digital signature represents one of the most widely used security technologies for ensuring un-forge-ability and non-repudiation of digital data. Its performance depends on an operation called point multiplication. The ECCDSA involves point addition and point doubling operations. It is found to be more secure in contrast to existing RSA and ELGAMAL algorithms.*

Keywords— ECDSA, ECC, Point multiplication, Point Addition,Signature generation, Signature verification.

INTRODUCTION.

Elliptic curve cryptography (ECC) is an public-key cryptography method, based on the algebraic structure of elliptic curves over finite fields. An elliptic curve cryptographic of the corresponding RSA schemes. Speed and efficient use of power, bandwidth, and storage are some of the significant merits of utilizing smaller keys.

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document, as analogous to a physical signature on paper. Authentication can be defined as a process by which one corroborates that someone is who they claim they are [2]. The purpose of digital signature is to provide a means for an entity to bind its identity to a piece of information. The process of signing entails renovating the message and some secretinformation held by an entity into a tag called signature. Digital signature represents one of the most widely used security technologies for ensuring un-forge-ability and nonrepudiation of digital data.

The Elliptic Curve Digital Signature Algorithm is the Elliptic Curve analogue to the more widely used Digital Signature Algorithm (DSA). It is the application of ECC to digital signature generation and verification. Its security is based on the elliptic curve discrete logarithm problem [3] (ECDLP).

I.EXISTING METHODOLOGY

RivestAldeman and Shameer Algorithm (RSA):

It is a cryptosystem for public key encryption, and it is widely used for securing sensitive data,particularly when being sent over an insecure network such as the internet.The algorithm of RSA is shown in the fig 1.

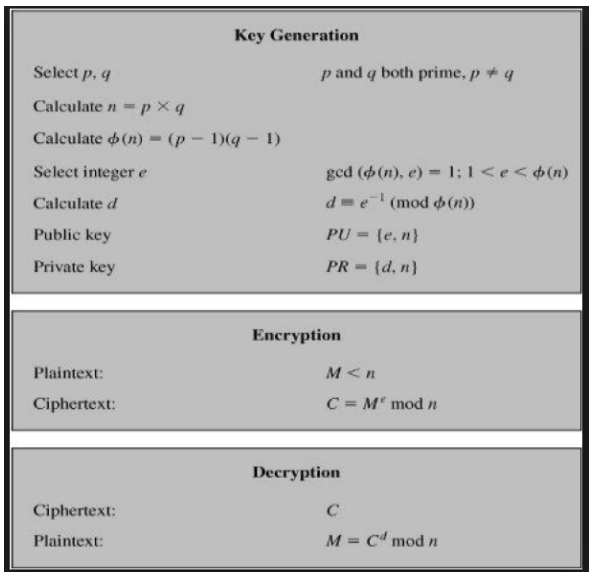

Fig 1. RSA algorithm

Elgamal Algorithm:

The ELGAMAL cryptosystem is used in some form in a number of standards including the digital signature standard. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm of ELGAMAL is shown in the fig 2.

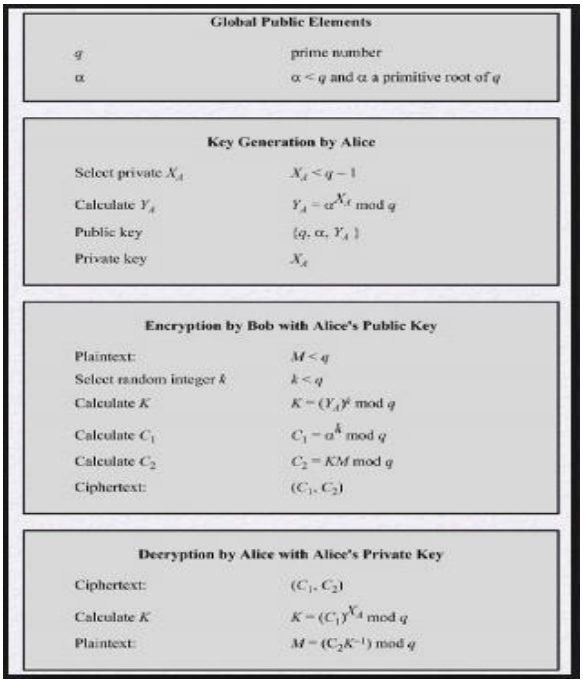

Fig 2.ELGAMAL algorithm

II. METHODOLOGY

Elliptic curves are Cubic curves. These may be defined as a set of discrete points on the co-ordinate plane, satisfying the equation of the form, $y^2 [+xy] = x^3 + ax^2 + b \pmod p$ [6].

The square bracket means that the term is optional. x and y are variables, a and b are constants. Each value of 'a' and 'b' gives a different elliptic curve. An elliptic curve in its"standard form" is illustrated by $y^2 = x^3 + a \times x + b$ for some fixed values of parameters 'a' and 'b'. This equation is also referred as Weierstrass equation of characteristic 0. The block diagram of ECC process is shown in the fig 3. Where the information at sender side is in the

form of plaintext which is then converted into cipher text using public key by an encryption process, then the received cipher text is converted back to plaintext using the private key by decryption process .

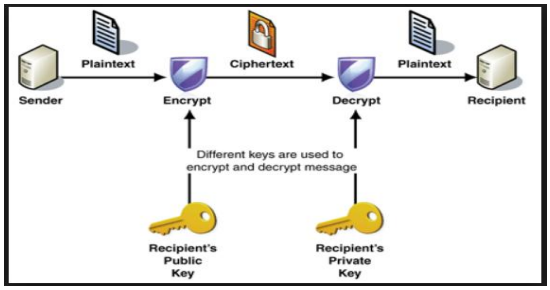

Fig 3.ECC process

Elliptic Curve Group*:* When the point addition operation is considered as a group operation, an additive group that consists of the set of solutions of the elliptic curve equation and a special point O called point-at-infinity is formed. It is well known that E/ F q with a binary operation, called addition of points and denoted by +, is an Abelian group with O∞ as the identity element. The group is denoted by E(F q).

Generating Point*:* The base points or generating points are used in elliptic curve cryptography for public key generation and private key generation. Base points are the points which can generate all the coordinates of an elliptic curve. The order of all base points must be equal to n where n is the total number of points for a particular elliptic curve.

Suppose the point P is in E(F q), and suppose P has a prime order n, then, the cyclic additive subgroup of E(F q) generated by P is P = {O, P, 2P, 3P... (n -1) P}.

Point Addition **:** It is possible to obtain a third point R on the curve given two points P and Q with the aid of a set of rules. Such a possibility is termed as elliptic curve point addition. The symbol ` + ' represents the elliptic curve addition P3 = P1 + P2. Point addition should not to be confused with scalar addition.

Point Multiplication **:** e× P denotes the multiplication of an elliptic curve point P by an integer e. This is analogous to the addition of P to itself 'e' times and this results in another point on the curve.

In Elliptic curves addition of points on a curve in the following manner: In order to find the sum of two points P and Q on elliptic curve E, draw a line connecting P and Q.

This line will intersect E at exactly one other point, which will denote P × Q. P + Q will be defined as the reflection of P × Q across the x-axis.

There are certain cases for which this definition will not suffice. One such case is where P and Q are the same point. In this case, draw the tangent line to E at P and find the second point where this line intersects E. Call this point P × P. Again, reflection of this point over the x-axis is P + P. Another case is where the line connecting P and Q is vertical.

In this case, P + Q is defined to be O, the point at infinity since the line connecting any point and Owill be a vertical line, and reflection of O about the x-axis results in O [7].

Consider a point P (x_p, y_p) on elliptic curve E. To determine 2P, P is doubled. This should be an affine point on EC. Equation of the tangent at point P is:

$S = [(3x_p^2 + a)/2y_p] \pmod p$

Then 2P has affine coordinates (x_r, y_r) given by:

$x_r = (S^2 - 2x_p) \bmod p$ and $y_r = [S(x_p - x_r) - y_p] \pmod p$

Now 3Pcan be determined by point addition of points P and 2P, treating 2P=Q. P has coordinates

(xp,yp) and Q=2P has coordinates (xq,yq). Now the slope is:

$$S = [(y_q - y_p) / (x_q - x_p)] \bmod p$$
$$P+Q = -R$$
$$x_r = (S^2 - x_p - x_q) \bmod p$$
$$y_r = (S (x_p - x_r) - y_p) \bmod p$$

Thus k× P can be calculated by a series of point-

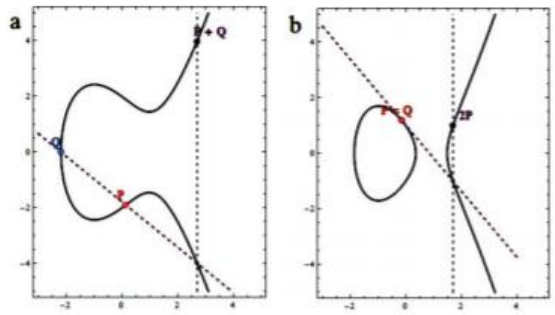

Fig a&b: Point addition and Point doubling

III.ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

The steps involved in ECDSA are formation of key-pair, signature-generation and signature-verification [4]. The digital signature is typically created using the hash function. The transmitter sends the encrypted data along with signature to the receiver. The receiver in possession of sender's public key and domain parameters can authenticate the signature.

The prime q of the finite field Fq, the equation of the elliptic curve E, the point P on the curve and its order n, are the public domain parameters. Furthermore, a randomly selected integer d from the interval [1, n-1] forms a private key. Multiplying P by the private key d, which is called scalar multiplication, will generate the corresponding public key Q.

The pair (Q, d) forms the ECC public-private key pair with Q is the public key and d is the private key. The generating point G, the curve parameter 'a' and 'b', together with few more constants constitute the domain parameters of ECC.

The public key is a point on the curve and the private key is a random number selected by signer. The public key is obtained by multiplying the private key with the generating point on the curve [5].

Key-Pair generation: Using generating point G and random integer d, public key Q is computed through following steps:

1) Select a random integer d in the interval [0, n-1].

2) Compute Q = d× G, obtained by point Multiplication. Q, G are points on the elliptic curve.

3) Now key-pair is (G, Q) where G is the Private Key and Q is the Public key.

The block diagram of key pair generation is shown in fig 4.

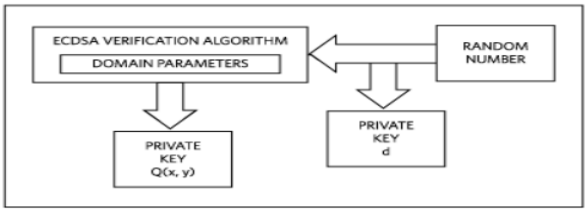

Fig 4.Key Pair generation

Signature Generation*:* Signer utilizes parameters q, a, b, p, n, d and private key G, to sign a message M where a, b, p and q are constants in elliptic curve equation. To sign a message signer does the following:

1) Chooses a random integer k with $1 \leq k \leq n-1$.

2) Compute k×G = (x1, y1).

3) Compute hash value z of mess: M, $z=h^{-1}(M)^2$.

4) Compute $s = (z \times d) \times k^{-1} \bmod n$.

If s = 0 then return to step 1.

5) Signature for the message M is (s, x1).

The block diagram of signature generation is shown in fig 5.

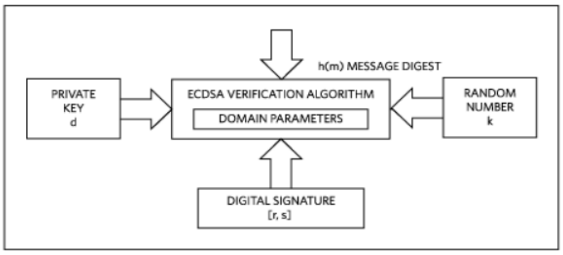

Fig 5.Signature Generation

Signature Verification **:** Authenticity of the received message can be verified by receiver exploiting the following steps:

1) First verify that s is integer in the interval [1, n −1].

2) Calculate hash z of the message/document M

3) Calculate the numbe $w = s^{-1} z \pmod n$

4) Using this number compute the point (x, y) = w× Q on the curve, and, finally, authenticate the signature by checking whether the equivalence x=x1 holds. The block diagram of signature verification is shown in fig 6.

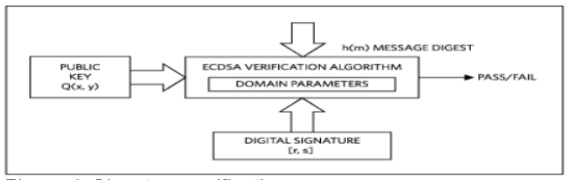

Fig 6.Signature Verification

Correctness of Algorithm**:** If the signature (s, x) on the message M was indeed generated by $s = (z\times d) \times k^{-1} \pmod n$.

Using this information correctness of algorithm can be proved through following methods: For signature verification receiver compute

$(x, y) = s^{-1}zQ$
$= s^{-1}zdG$ as $Q=d\times G$, step 2 of key pair generation
$= (z \times d)^{-1}(z\times d) k\times G$
$= k\times G$

As $(x_1, y_1) = k\times G$
Thus $(x_1, y_1) = (x, y)$

IV.ADVANTAGES OF ECDSA

The proposed ECDSA treats generating point as private key, which ultimately revolutionize the whole algorithm and improves the security and execution speed of the algorithm. The key advantages of proposed ECDSA are as follow:

1) Less complex algorithm: Unlike existing ECDSA, the signature generation using proposed ECDSA consists of computing the value of parameter ‘s’ only. Integer ‘r’ is not calculated in this algorithm. Also signature verification consists of one point multiplication operation whereas existing algorithm have two point multiplication and one point addition operation.

2) Provide more security: As only two points are shared publically and generating point is private, this algorithm is more secure against intruders.

3) Less number of curve points provided publically.

4) Reduces number of point multiplication in signature verification.

5) Reduced point addition operation in signature verification method.

6) Reduces number of parameters made public. No need to share curve parameters ‘a’, ‘b’, ‘q’ and ‘n’ with everyone.

7) Remove the overhead to calculating ‘r’.

8) When utilized in Key Exchange algorithm to authenticate the message sent by both parties, remove the Man-in-theMiddle attack.

CONCLUSION

ECDSA is less complex algorithm to calculate digital signature. This algorithm consists of less number of point-addition, point multiplication and point doubling processes which enhances its execution time.

The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates.

ACKNOWLEDGEMENT

We thank Head of our Department for giving us this opportunity and his guidance through this endeavour.

REFERENCES

[1]WilliamStallings, "Cryptography and Network Security", ISBN 81-7758- 011-6, PearsonEducation, Third Edition, pages 42-62,121-144,253-297.

[2] Ms. P. G. Rajeshwari and Dr. K. Thilagavathi, "An Efficient Authentication Protocol Based on Elliptic Curve Cryptography for Mobile Network," IJCSNS, vol 9, feb 2009.

[3] Mrs. Megha Kolhekar and Mrs. Anita Jadhav," Implementation of Eliptic Curve Cryptography on Text and Image," International Journal of Enterprise Computing and Business System," vol 1, issue 2, july 2011.

[4] Liu Yongliang, WEn Gao, Hongxun Yao and Xinghua Yu, "Elliptic curve Cryptography Based Wireless Authentication Protocol," International Journal of Network Security, vol. 5, pp. 327–337, Nov. 2007.

[5] Elhadiyoussef Wajih, Benhadiyoussef Noura, Machhout Mohsen and Tourki Rached," Low Power Elliptic Curve Digital Signature Design for Constraned Devices," International Journal of Computer Science and Security, vol 1, issue 3, 2012.

[6] M. Ashkar Mohammed and Dr. S. Suresh Babu," Realization of Elliptic Curve Cryptography Based on ECDSA," Current Trends in Technology and Sciences, vol 1, issue 2, sept. 2012

[7] Dipti Aglawe and Samta Gajbhiye," Software Implementation of Cyclic Abelian Elliptic Curve using MATLAB," International Journal of Computer Applicatios, vol 42, no. 6, march 2012.