Grenze International Journal of Engineering and Technology, July 2017

Improved Scheme of ECC and as Intrusion Detector

Mr. Sangamkumar G H[1], Mr. Shreenivas P Gudi [2]
[1] Don Bosco Institute of Technology,
Department Of Electronics and Communictaion, Bengaluru
Email: hgsangami@gmail.com
[2-] Don Bosco Institute of Technology
Email: shrinivasgudi@gmail.com

***Abstract*— This paper explains the Improved Version of ECC and its Application as Intrusion detector. ECC works well for secure encryption methods. It is faster than the RSA because ECC uses smaller key sizes for equivalent security. For the design of ECC, the message encoding is done before modifying or hiding data. ECC can modify a point but not the data. The data to coordinate and coordinate to data are main functions in ECC. The paper defines Koblitz's, Menezes-Vanstone Encryption/Decryption method to represent a message to a coordiantor and vice-versa. The paper also describes and implementation of proposed protocol using Koblitz's and Menezes-Vanstone Encryption/Decryption Schemes and Application as Intrusion Detector for data saving.**

***Index Terms*— ECC; Intrusion Detection; Hash Function.**

I. INTRODUCTION

ECC is asymmetry Cryptography. ECC suites for mobile phones and cards as these applications need high-term security requirements. Every user in public key cryptography will use a pair of keys. Only theindividual user knows the security key whereas the keys which are shared to all users called as public key ECC on elliptic curves needs mathematical background to understand. Curves are not ellipses. The general representation of elliptic curves is $y^2 + axy + by = x^3 + cx^2 + dx + e$. But for ECC it is restricted $y^2 = x^3 + ax + b$. Say EP(a,b) represents curve satisfy the above equation together with element at infinity O. The complexity of ECC is discrete logarithm problem, i.e "it should be very difficult to find a value k such that Q=kP where P and Q are known'. But 'it should be easy to find Q where k and P are known' [6] P,Q are points on the elliptic curve.

For ECC, we are concerned over a finite field. This is defined as follows. Choose two non negative integers, a and b, less than p that satisfy:

$$4a^3 + 27b^2 (\text{mod p}) \neq 0.$$

II. KEY EXCHANGE

A ECC key exchange between two users can be explained as follows Figure 1:

- A selects an random number nA.it should be less than n. its A's private key. A then generates a public key PA = nA * G; even public key is one of a coordinate in Eq(a, b).
- B similarly selects a random key nB its private keyand generate a public key PB of user B.

Grenze ID: 01.GIJET.3.3.180

- A generates the intermediate key K = nA * PB. And B generates the secret key K = nB * PA.Your goal is to simulate the usual appearance of papers in a Conference Proceedings or Journal Publications. We are requesting that you follow these guidelines as closely as possible.

Global Public Elements
Eq(a,b) elliptic curve with parameter a,b and q, where q is a prime or an integer of the form 2^m

G point on elliptic curve whose order is large value n

User A Key Generation
Select private nA nA<n
Calculate public PB PA=nA*G

User B Key Generation
Select private nB nB<n
Calculate public PB PB=nB*G

Calculation of Secret Key by User A
K=nA*PB

Calculation of Secret Key by User B
K=nB*Pa

Figure 1: Diffie-Hellman Key Exchange.

Note that Diffe-Hellman algorithm is used just to generate secret keys [6].

III. ECC ENCRYPTION/DECRYPTION

Several approaches are defined using Elliptic Curve. And have been analyzed in literatures. In this paper we look at three tasks. The first task is to convert the message (M) to an (x, y) point Pm in E(F) that we encrypt as ciphertext and subsequently decrypt. Note that we can not simply encode the M as an coordinates of a point,[5] because not all such coordinates are in E(F). The second task is not to need to encode the M to be sent as an (x, y) point in E(F), that is enough in representation M as any random pair number. The third task is proposed scheme these tasks are applied in the following encryption/decryption schemes.

IV. ELGAMAL ENCRYPTION/DECRYPTION SCHEMES

The encryption/decryption of ElGamal scheme require a point B of an group E (F). The user Bob selects a private key d and generate a public key Q=dB.
Alice to encrypt message Pm and send to Bob, select a random positive integer e and produce the cipher text Cm consisting of the pair of points:

$$Cm =\{ C, eB\}$$

Where

$$C =Pm + eQ$$

Note that: Alice has used Bob's public key Q.
To decrypt the cipher text, Bob multiplies the second point in the pair by his secret key and subtracts the result from the first point:

$$C- d(eB) = Pm + eQ - d(eB) = Pm + e(dB) - d(eB)= Pm.$$

V. MENEZES-VANSTONE ENCRYPTION/DECRYPTION SCHEMES

This system that is not need to encode the plaintext message as a point in the curve E, is called Menezes-Vanstone ECC (MVECC). It is a Modified ElGamal cryptosystem.
The encryption/decryption of MVECC schemes require a point B of an ECC E(F). The user Bob selects a key d and generate a public key Q=dB.
Alice to modify and send a to Bob .select a random integer e and produce the text Cm consisting of the pair:

$$Cm =\{C, eB\}.$$

$$c1= m1 * k1 \bmod p.$$

$$c2= m2 * k2 \bmod p.$$

Where C = (c1, c2) (k1, k2) = eQ (m1, m2) = M.
Note that: Alice has used Bob's public key Q.
To decrypt the cipher text, Bob multiplies the second point in the pair by his secret key and compute M as follows:

$$m1= c1 * k1^{-1} \bmod p. \qquad m2= c2 *k2^{-1} \bmod p.$$

VI. PROPOSED SCHEME

The proposed protocol make use advantage of both the schemes Elgamal Encryption/Decryption Schemes and Menezes-Vanstone Encryption/Decryption Schemes.

- Advantage of Menezes-Vanstone Encryption/Decryption Schemes i.e. No not need to encode the plaintext message in the elliptic curve make it more efficient than the original ElGamal scheme.
- Advantage of Elgamal Encryption/Decryption scheme. i.e. Never need to calculate the inverse operation of key in the decryption method.

Suppose user 1 wants to send a message M to user 2. Let d denote user 2 secret key and Q = dB denote user 2 public key. user selects a random integer e and sends Cm

$$Cm = \{C, eB\}.$$

Where C = (c1, c2), (k1, k2) = eQ.

$$c1= m1+k1 \bmod p.$$

$$c2= m2+k2 \bmod p.$$

To decrypt the cipher text user 2 computes

$$(k1, k2) = d (eB).$$

$$m1= c1 –k1 \bmod p.$$

$$m2= c2 – k2 \bmod p.$$

VII. IMPLEMENTATION AND ANALYSIS OF PROPOSED PROTOCOL

Let us suppose a text file has to be used, A user can encrypt the ASCII code of each and every printable character on the keyboard , Figure 2 defines the steps of proposed protocol

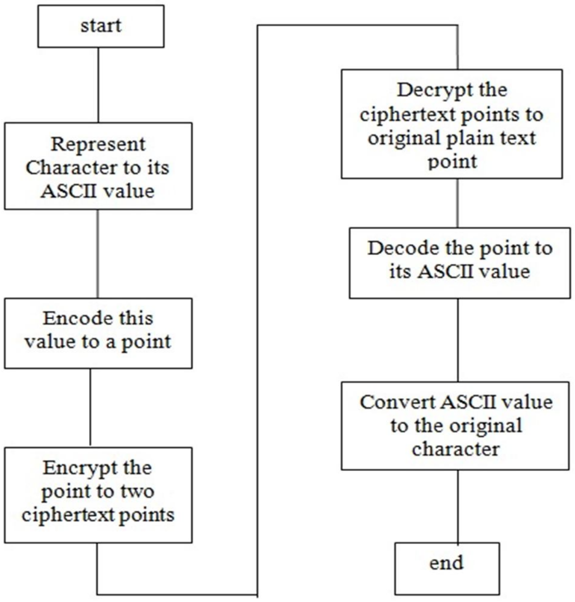
start
Represent Character to its ASCII value
Encode this value to a point
Encrypt the point to two ciphertext points
Decrypt the ciphertext points to original plain text point
Decode the point to its ASCII value
Convert ASCII value to the original character
end

Figure 2: Steps followed in Proposed Protocol.

Example for proposed protocol

Step 1: Pick an elliptic curve Ep (a, b)
Say that the parameters of curve are P (151),a(1),b(13).
Step 2: Say we have to send character ‘A’.
Step 3: ‘A’ is first encoded to its ASCII value i.e. 65
Step 4: Now choose an auxiliary base parameter, for example k (20). (Both parties should agree upon this)
Step 5: Encode the message i.e. ‘A’ to a point using any Mathematical relation. For example x1=ASCII-k, y1=x1-k.For 65 the point will be (45, 25) with respect to above curve the point (x1,y1) = (45,25) does not lie.
Step 6: Now the point (45,25) is encrypted and decrypted as a message.
Step 7: To decode just compute (y1+2k) i.e. 65
Step 8: The number 65 is decoded to character ‘A’.

Advantages of Proposed scheme over RSA

- Smaller key size for equivalent security
- Higher security per bit
- Leads to faster implementations i.e. higher security for the same amount of computation
- ECC device require less storage, less power, less memory, and ofen less bandwidth than any other public key systems.

Thought to be more secure (largest ECC and RSA systems broken to date are 108b & 512b respectively) largest effort ever expended in a public key cryptography challenge for solving 108b ECC. Amount of efforts was about 50 times of 512b RSA.

vIII. Application As Intrusion Detector

Intrusion detection is defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource. By applying a message digest to a files and then checking the hash hasn’t altered a degree of assurance is maintained. On detecting a change an alert will be triggered.

A. Basic Block Diagram for Intrusion Detection

A prepares a plaintext message M and then provides this as input to a function F that produces an hash. The hash is appended to M and the entire block is then encrypted. At the destination, B decrypts the incoming block and treats the results as a message with an appended hash. B applies the same function F to attempt to reproduce the hash. If the calculated hash is equal to the incoming hash, then the message is considered authentic. It is unlikely that any random sequence of bits would exhibit the desired relationship.

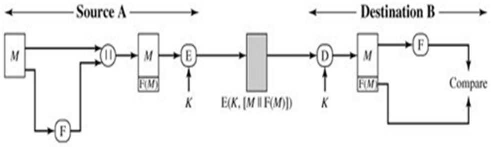

Figure 3: Block Diagram for Intrusion Detection.

Example for Intusion Detection

Step 1: Pick an elliptic curve Ep (a, b)
Say that the parameters of curve are P (151),a(1),b(13).
Step 2: Say User A has to send message 'CRYPTO'.
Step 3: 'CRYPTO' is encoded to its ASCII value i.e. 67, 82,89,80,84 &79.
Step 4: Now choose an auxiliary base parameter, for example k (20). (Both parties should agree upon this)
Step 5: Encode the message i.e. 'CRYPTO' to a point using any Mathematical relation. For example x1=ASCII-k,y1=x1-k.For 67 the point will be (47, 27) with respect to above curve the point (x1,y1) = (47,27) does not lie.
Step 6: Now the point (47,27) is encrypted and Decrypted as a message. For "CRYPTO" the points are (47,27),(62,42),(69,49),(60,40),(64,44) & (59,39).Steps from 3 to 6 as performed to Hash values too.
Step 7: With the help of ECC key Exchange generate the Public and Private key of User B. For example consider 77 as Private key then the Public key will be (28,20).
Step 8: With the User B Public Key encrypt the points of Message and Hash and transmit encrypted values to User B.
For example Message= "CRYPTO" & Public key=(28,20)
The encrypted message will be ((3,63),96,84,117,30,6,35,84,7,150,53,143,71)
Step 9: User B GETS the message using Private key 77 in this case. Decrypted message will be in points.
Step 10: To decode just compute (y1+2k) .
Step 11: Compare the CIPHER Hash value and Message Hash value to detect the Intrusion.

IX. CONCLUSION

Elgamal scheme AND Menezes-Vanstone scheme though simple has a hole. Here, we have proposed a improved scheme of ECC and its application as intrusion detector i.e. authenticating the message so that message tampering and message forging kind of attack is detected and hence discouraged.

REFERENCES

[1] Baris Coskun, Nasir Memon, "Confusion/Diffusion Capabilities of Some Robust Hash Functions " IEEE 2006.
[2] Chuanhua Zhou, Baohua Zhao, "Study of One-way Hash Function to Digital Signature Technology" IEEE 2006.
[3] Hans Vandierendonck, Member and Koen De Bosschere, "XOR-Based Hash Functions "IEEE 2009.
[4] Vhclav Skala, Martin KuchaP, "The Hash Function and the Principle of Duality" IEEE 2004
[5] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes,
[6] *" Software Implementation of Elliptic Curve Cryptography over Binary Fields".*
[7] W. Stallings," Cryptography and Network Security", Prentice Hall, Second Edition,1998.
[8] Darrel Hankerson,Alfred Menezes,Scott Vanstone, "Guide to Elliptic Curve Cryptography".
[9] Man Young Rhee, "Cryptographic Principle,Algorithms and Protocol",Wiley.
[10] Request for Command Rfc 4270 "Attacks on Cryptographic Hashes in Internet Protocols".
[11] Request for Command Rfc 3174 "Secure Hash Algorithm 1".