Multimedia Data Transmission Using Elliptic Curve Cryptography

Sonal Sharad Pawar[1], Prof.R.H.Goudar[2]

Abstract

As multimedia application are used in daily life, security has become most important issuse. So using ECC sending of multimedia data (text, image, audio, video) is described . ECC is mainly used for security and it uses smaller key compared to other algorithm such as RSA, Diffie Hellman. In this paper we have presented the architecture for security of multimedia data, text and image encryption and decryption is done using Koblitz method, video encryption and decryption is done using ECC and RC5, audio encryption and decryption is done using ECC. ECC is also used for various application such as phone, PDAs, Pagers, Smart cards etc.

Index Terms : Elliptic curve cryptography (ECC), Encryption, Decryption.

I. Introduction

Cryptography is art of hiding information or keeping the information secret from external environment [1]. Cryptography is process of protecting data by converting it into scribbled format. There are two types of cryptography: symmetric key cryptography and asymmetric key cryptography (or public key cryptography) [1].

In symmetric key cryptography there is only one key called secret key (shared) between the source and destination. In asymmetric key cryptography involves two key, public key and private key. Public key is public to all, any user can access public key where as private key is not shared, it is kept secret. Basic terms in cryptography

1. Plain text: original message to be transmitted.
2. Cipher text: Encrypted or coded message.
3. Encryption: converts message into cipher text
4. Decryption: converts cipher text into Message

Victor S. Miller (IBM) and Neal Koblitz's (University of Washington) in the year 1985 introduced Elliptic curve cryptography [2][13]. The U. S. National Security Agency has approved ECC including it in the recommended cryptographic algorithms.

Elliptic curve cryptography (ECC) is based on mathematical equation of elliptic curve (EC) over field and is a public key cryptography approach [2][3]. General equation form of elliptic curve is

$$Y2=x3+ax+b \qquad (1)$$

Where $4a3 + b \neq 0$ and 'a' and 'b' gives different EC depending. The point (x, y) satisfies the equation

[1] *Department of Computer Networks*
VTU PG Centre, Belgaum, India. sonal.spawar@gmail.com

[2] *Department of Computer Networks*
VTU PG Centre, Belgaum, India. rhgoudar@gmail.com

and infinity point lies on the EC. Elliptic curve has a public key as point on curve and random number is private key. The domain parameter of ECC is the point generator G and curve parameter ‘a’ and ‘b’ and Fig 1 shows the general form of the elliptic curv

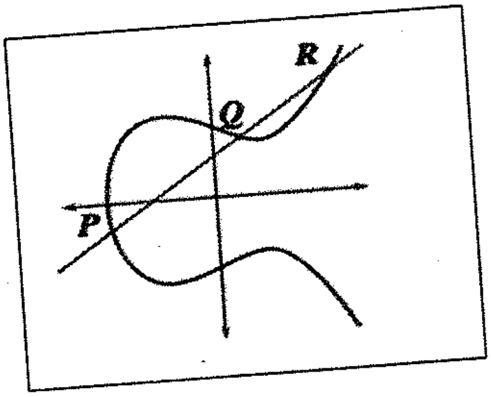


Figure 1 $y2 = x3 + ax + b$

The main advantage of ECC is it has smaller key size, reduces storage capacity and tranmission requirments.

A.Application of ECC [4]

1.Application requiring public-key operations such as web servers that needs to handle more than one encryptions session (many encryption).

2.Application with limited power,speed transfer,memory storage,bandwidth and computational power such as wireless communcation and PDAs.

3.Apllications rigid constraints on processing power and code space such as smart cards and tokens

B.Comaparison of ECC with RSA

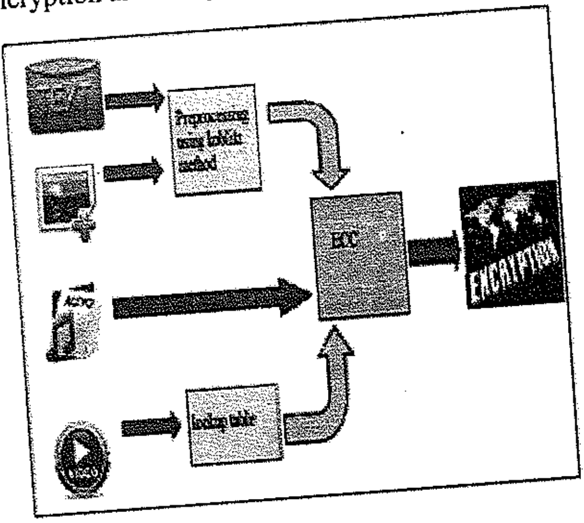
Table 1 describes the differences between ECC and RSA

Table 1:Difference between ECC and RSA

ECC	RSA
Smaller key,ciphertext and signature. so very fast key genertion	Bigger key size so slow key generation
Fast encryption and decryption	Slow encryption and decryption,which is difficult to implement securley
Difficult to implement	Easier to implement
Faster computation and need less storage space	Slower computation and needs more storage space
Based on binary curve and are fast in hardware	Based on the integer factorization problem
Security relies on smaller key size	Security relies on the factoring in slow and multiplication is fast.

II. Archietecture

As multimedia application are used in daily life, security has become most important issuse. So using ECC sending of multimedia data (text, image, audio, video) is described by the fig 1 and fig 2 ie shows the flow diagram of encryption and decryption resp. In this text and image encryption and decryption is done using Koblitz method, video encryption and decryption is done using ECC and RC5, audio encryption and decryption is done using ECC.



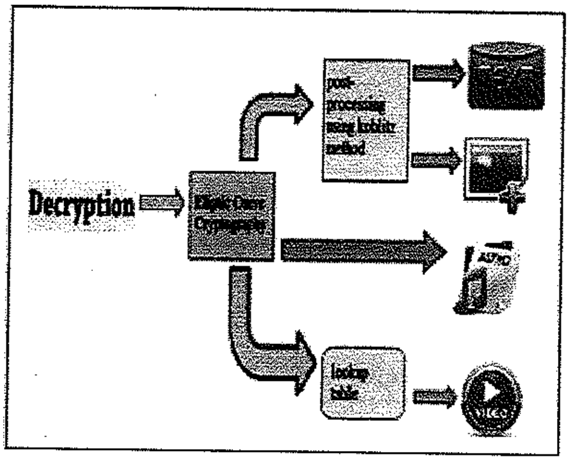


Figure 3 Flow Diagram of Decryption

A. Text Encryption and Decryption

Suppose a message or text file has to encrypt then user first has to convert plain text (message) into ASCII value. After this select a curve, so that each point is fixed on the curve to an ASCII value [5].

ECC encoding and decoding can encrypt and decrypt a fix points on the elliptic curve and not the messages. For example "CAT" has to be written in ASCII value and the sequence of ASCII character '67' '65' '84. Now this value has to fix point on the curve. The sequence of the steps using Koblitz's method is as shown in the figure 3

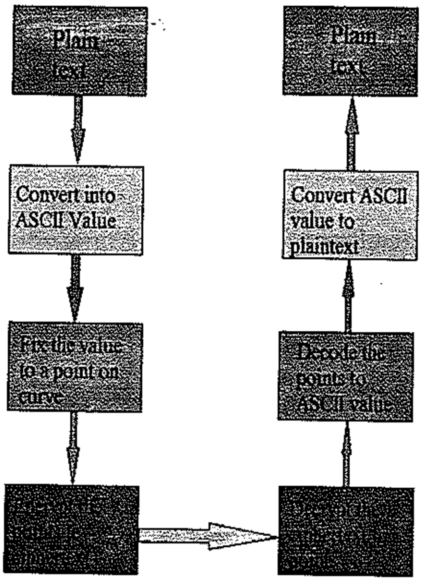

Plain text
Convert into ASCII Value
Fix the value to a point on curve
Plain text
Convert ASCII value to plaintext
Decode the points to ASCII value

Fig 3 Flow Diagram of Text encryption and Decryption

Algorithm

Koblitz's method for encoding and decoding plaintext

Step 1: select E (a, b) as elliptic curve (EC).

Step 2: let Elliptic curve has N points on it.

Step 3: Convert the message or plaintext into ASCII values.

Step 4: Choose an Auxiliary base parameter (both parties' i.e. sender and receiver should agree) say k.

Step 5: For each number or integer mk, take x=mk+1 and calculate the value for y (m is ASCII value of character).

Step 6: If you don't get the answer for x=mk+1 then go on increasing value like x=mk+2,x=mk+3 so on till you get the value for y.

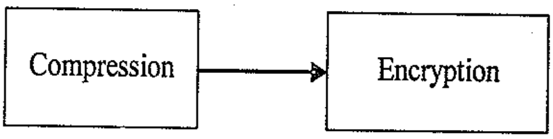
Step 7: Take points (x, y) and convert this value m into point on EC. This way you get complete message is converted into points.

Step 8: For decryption take points (x, y) and select m such that value m should be larger integer and compute (x-1)/k. this number is converting to character. Repeat this step for decryption of entire message.

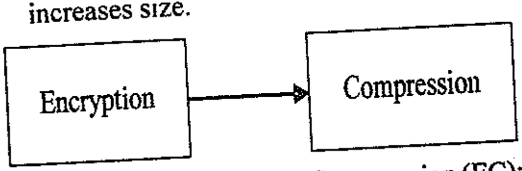
A. Image Encryption and Decryption

There are different ways for encryption and compression as shown in the below [6]

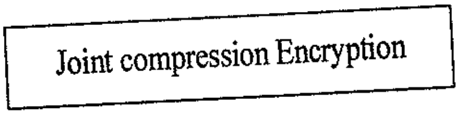
- Compression followed by Encryption (CE): In this first compression of image is done and



after that encryption is performed. Encryption increases size.



- Encryption followed by Compression (EC): In this first encryption of image is done after that compression is performed on image. Encryption does not increase size.
- Joint compression and encryption (JCE): compression algorithm which works with encryption algorithms is called Joint Compression-Encryption algorithm. This is faster than the above methods.



- Koblitz's method for image encryption and decryption [7].

Fig 4 shows steps for ECC encryption and decryption using JPEG compression

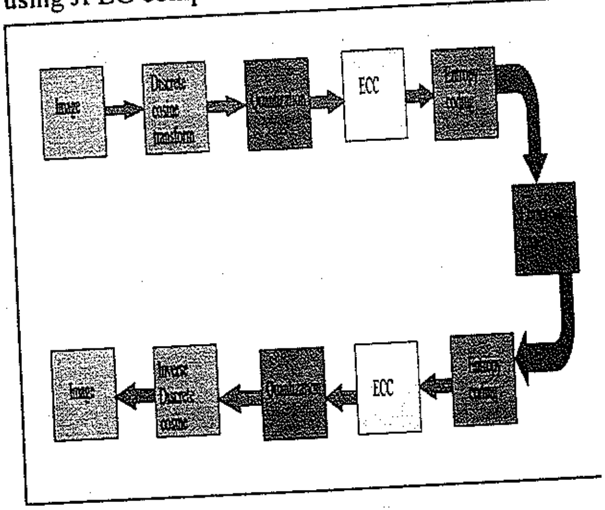


Fig ure 5 combination of ECC and Jpeg Compression

For performing JPEG compression of image, divide image first into 8*8 blocks (pixels). Now DCT (discrete cosine transforms) is use to convert each block into spatial frequency domain, so that it can eliminate higher frequency components which cannot be detected by the eyes. The output of DCT consists of 64 DCT coefficients as a set, where the value with zero coefficients is called as DC coefficients and all other remaining is called as AC coefficients [8].

After applying DCT, quantization is performed. Quantizer is one which represents the original signal with minimum loss or distortion. Amplitude with lower threshold are stored in higher spatial frequency, are set to zero and lower spatial frequency are preserved. E(953822980,31357327) is used for encryption for DC coefficient. Entropy coding is used for compression of image.

A. Audio Encryption and Decryption[9]

Step 1: Select the audio file as input x.

Step 2: Each value of audio is called as message m. Convert this into the coordinates (x, y), x and y are point on the elliptic curve (EC).

X=m*k+j where j=0, 1, 2.................

$$y = \sqrt{(x3 + ax + b)}$$

Where k is random number and p=prime integer.

Step 3: Encryption and Decryption require a base point G and EC E(a, b). User Alice chooses a secret integer s and computes Q=s*G. User Bob consists of public Key which has E(x, y), G, Q and s is private. To encrypt the message, Alice send Pm (plain text) to Bob by choosing a k (random integer) and produce Cm (cipher text) consists of pair of points.

$$Cm = (kG, Pm + kQ)$$

Step 4: decryption of cipher text

$$(Pm + kQ - s(kG) = Pm + k(s.G) - s(kG)$$

$$= Pm$$

A. Video Encryption and Decryption

In general, video data/information is a huge (i.e. frame consists of bit and there may be 25 to 30 frames per second) [
ity videos can be encrypted using algorithms like DES, AES, RC etc.

RC5 is used for encryption of DCT coefficients. RC5 has some of characteristics such as varying block cipher, varying key size and number of round (variable). Fig 6 shows the steps or block diagram for encryption process [11]

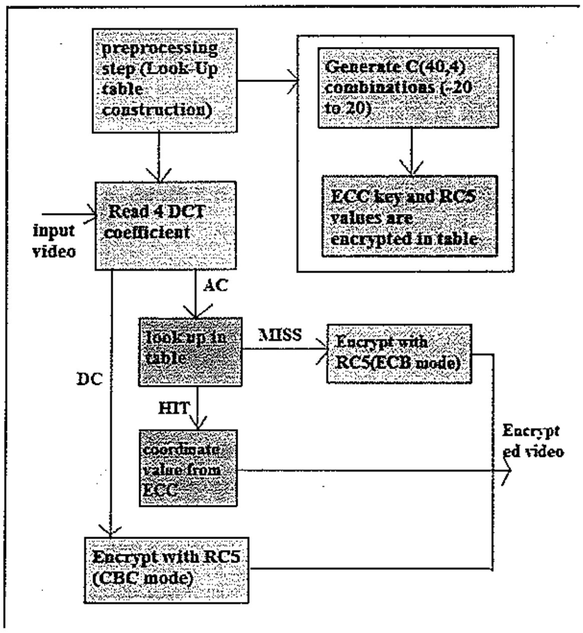

preprocessing step (Look-Up table construction)
Generate C(40,4) combinations (-20 to 20)
ECC key and RC5 values are encrypted in table
input video
Read 4 DCT coefficient
AC
DC
look up in table
MISS
Encrypt with RC5(ECB mode)
HIT
coordinate value from ECC
Encrypt ed video
Encrypt with RC5 (CBC mode)

Figure 6 Encryption of video

Algorithm1 : Lookup table construction (preprocessing step)

Step 1: Generate from -20 to 20 as quadruples or fourfold for all combinations.

Step 2: using ECB (Electronic Code Book) of RC5 encryption encrypt quadruple.

Step 3: list of coefficients and encoded values are stored in lookup table and are used for encryption of AC coefficients

Algorithm 2

Step 1: For each block of frame.

Step 2: consider 4 consecutive ACs (AC1, AC2, AC3 and AC4).

Step 3: Compare all this coefficients with lookup table for miss and hit. Replace the 4 AC coefficients if hit is present then apply the algorithm of ECB mode with RC5 and ECC. Otherwise take input as DCs coefficients.

Step 4: Consider DC coefficients, collect all DC coefficients values and use CBC mode and RC5 algorithms to encrypt these values.

For decryption, the receiver generates a lookup table and encrypts the quadruples. The columns in lookup table are interchanged and to see the pair values are arranged in correct order or not. For getting DC coefficients, we have to use RC5 decryption followed by CBC mode. Similarly the same table can be used for AC coefficients.

III. Conclusion

We conclude that, ECC provides security for transmissions of multimedia data .We have also Compared ECC with other standard algorithm RSA. Because of smaller key size ECC provides reliable encryption and decryption and hence it is faster. Applying ECC based algorithms shows that ECC is better choice for multimedia data; it can also be used for real time applications.

References

[1] Komal Agrawal, Anju Gera “Elliptic curve Cryptography with Hill generation for Secure text cryptosystem” International Journal of Computer Application (0975-8887) vol 106-No.1, November pp-18.

[2] N.koblitz, “Elliptic curve cryptography, mathematics of computation”, vol 48 1987,pp 203-209 1987.

[3] Anoop MS, "Elliptic curve cryptography-An implementation Tutorial".

[4] Vivek Katiyar, Kamlesh Dutta, Syona Gupta "A survey on Elliptic curve cryptography for Pervasive computing environment" International Journal of Computer Application (0975-8887) vol 11-No. 10, December 2010.

[5] Padma Bh, D. Chandravathi, P. Prapoorna Roja "Encoding and Decoding of Message in the Implementation of Elliptic curve cryptography using Koblitz's Mehod" International Journal of Computer Science and Engineering vol 02, No. 05, 2010, 1904-1907.

[6] Abdul Razzaque, Dr. Nileshsignh V. Thakur "Image Compression and Encryption: An overview" International Journal of Engineering Research and Technology (IJERT) ISSN 2278, vol 1 Issues, july 2012.

[7] Saeid Bhahtiari, Subhariah Ibrahim, Mazleena Salleh, Majid Bhahtiari "JPEG Image Encryption with Elliptic curve cryptography" 2014 International Symposium on Biometrics and Security Technologies (ISBAST).

[8] Wu Zhen, Xu Zhe, Zhang Rui-nian, Li shao-Mei "SIFT Feature Extraction Algorithm for Image In DCT Domain" procreeding of the 2nd International Symposium on Computer , Communication Control and Automation(ISSCCCA-13), 2013

[9] Rahul Singh, Ritu Chauhan, Vinit Kumar Gunjan, Pooja Singh "Implementation of Elliptic curve cryptography for audio Based Application" International Journal of Engineering Research and Technology (IJERT) ISSN 2278-0181, vol 13Issues-1, janauary 2014.

[10] C. Narsimha Raju, Ganugulu Umdevi, Kannan Srinath and C. V. Jawahar "Fast and Secure Real-Time Video Encryption" Sixth International Conference on Computer Vision, Graphics and Image Processing.

[11] Lekha Bhandari, Mr. Avinash Wadhe "Speeding Up Video Encryption Using Elliptic Curve Cryptography (ECC)" International Research in Management and Technology, ISSN: 2278-9859 (volume 2, Issue 3), march 2013.

[12] W. Stallings," Cryptography and Network Security",Prentice Hall, Second Edition,1998.

[13] V.S. Miller," Use of Elliptic Curves in Cryptography ",Advances in Cryptology-Proceedings of CRYPTO'85, Springer Verlag Lecture Notes in Computer Science 218, pages 417-426, 1986.

Authors Biography

Sonal Sharad Pawar have completed Master of Technology in Computer Networks and Bachelor Of Engineering in Computer science from Visveswaraya Technological University Belgaum. Her area of interests are networks, image processing and android.