IMAGE ENCRYPTION AND DECRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

Dr. ParmaNand Astya[1], Ms. Bhairvee Singh[2], Mr. Divyanshu Chauhan[3]

[1] *Department of CSE, Galgotia University, Greater Noida, Uttar Pradesh, (India)*

[2]*Department of CSE& IT, SET, Sharda University, Greater Noida, Uttar Pradesh, (India)*

[3]*Department of CSE, ASET, Amity University, Noida, Uttar Pradesh, (India)*

ABSTRACT

In today's world image plays an important role in everyone's life. The, security of image is required while transferring them across the network. Various encryption and decryption algorithms are available to protect the image from unauthorized user. RSA and Diffie-hellman key exchange provide a good level of security but the size of encryption key in these two is a big problem. ECC is a better alternative for public key encryption. It provides equal security with smaller key size. In this paper the image which is considered to be in the form of a grid, is first transformed on an elliptic curve. These points or coordinates are then encrypted and send to the recipient. At the receiver end decryption algorithm is used to convert the encrypted image into the original image. Brute force attack is infeasible for ECC because of the discrete logarithmic nature of elliptic curves. This paper presents the technique to encrypt and decrypt the digital image(BMP) from Elliptic Curve Cryptography.

Keywords: Elliptic Curve Cryptography (ECC), Discrete Logarithm Elliptic Curve (EC), Public Key Cryptography.

I INTRODUCTION

Elliptic curve cryptography was introduced by Koblitz and Miller in 1985, and since then enormous amount of research has been done in this field. Elliptic curves are not ellipses; they are named so because they are described by cubic equations. Generally the cubic equations can be represented as:

$$y^2 + axy + by = x^3 + cx^2 + dx + e \quad (1)$$

But here for this paper following equation can be used:

$$y^2 = x^3 + ax + b \quad (2)$$

In ECC we normally start with the base point (G). Base point has the smallest (x,y) coordinates, which satisfy the equation of elliptic curve. By using different x and y coordinates all the points of elliptic curve can be identified along with 0 which is known as point of infinity.

Here the image file is considered as a stream of bits and constructed as various grids. Every grid of this image tells the intensity of the pixel. These intensity values are first mapped into point of elliptic curve by using this as multiplier of P_m , where P_m is a point on elliptic curve. This operation can be performed by repeated addition and doubling technique.

Now this point is encrypted using elliptic curve cryptography, and sent to the recipient. Recipient uses the decryption algorithm and recover theP_{mi}. The next step is to get the value of I fromP_{mi}. This can be evaluated because of the discrete logarithmic concept of elliptic curve. The keys are shared between two parties in a secure way. This logarithmic concept provides the ECC maximum security against the hacker and intruders.

II RELATED WORKS

In the past, many researchers have tried to exploit the features of ECC field for security applications. We have stated highlights of some of the relevant work in this section. Ray C., [4] in his work explained the design of a generator, which automatically produces customized ECC hardware that meets user-defined requirements. Alessandro Cilardo et al illustrates the engineering of ECC as a complex interdisciplinary research field encompassing such fields as computer science and electrical engineering [5].M.Aydos et al [2] has presented a working of ECC over the field GF(p) on a 80 MHz, 32 bit RAM microprocessor along with the results. Kristin Lauter has provided an overview of ECC for wireless security [3]. It emphasizes on the performance advantages in the wireless environment by using ECC instead of the traditional RSA cryptosystem. C. J. McIvor et.al [6] introduces a novel hardware architecture for ECC over GF(p). The work presented by Gang Chen explains a high performance EC cryptographic process for general curves over GF(p) [7]. The standard specifications for public key cryptography is defined in[8] .

A simple tutorial of ECC concept is very well documented and illustrated in the text authored by Williams Stallings et.al [9]. The paper which was presented by Kevin M. An efficient and new approach of a scalar point multiplication method than existing double and add by applying redundant recoding, which originates from radix-4 Booths algorithm was proposed by SangookMoon[II].Finnigin et al outlines a brute-force attack on ECC implemented on UC Berkley's Tiny OS operating system for wireless sensor networks [10]. The attack utilize the short period of the pseudorandom number generators used by cryptosystem to generate private keys. In the paper as proposed by Jaewon Lee [12] presents 3 algorithms to perform scalar multiplication on EC defined over higher characteristic finite fields such as OEA (Optimal Extension Field). Liu Yongliang [13] showed that Aydoset al.' s protocol is susceptible to man-in the-middle attack from any attacker but not restricted on the inside attacker. They proposed a new ECC based wireless authentication protocol. A comprehensive coverage of EC field with the in-depth mathematical treatment is given in [14]. Owing to these prevailing works on ECC and its popularity, it is proposed to implement the crypto system based on ECC for text based application. The proposed work can be extended to XML based application since the future middleware technologies are in the control of XML based documents which is purely based on text.

III DETAIL METHODOLOGY

As the general elliptic curve is represented by following equation:

$Y^2=x^3 + ax + b$ (3)

Where x and y are the points on the elliptic curve and a, b are the coefficients satisfying the following equation:

$4a3+ 27\ b2\neq 0 \pmod p$ (4)

Here p is a modular prime integer. So we can say that an elliptic curve consists of all the points satisfying the elliptic curve equation and along with the point at infinity.

3.1 Elliptic curve arithmetic

The important EC operations are point addition and point doubling. To compute a value kP, where P is some point on elliptic curve, we need to perform a series of addition and doubling operations.

Let's start with a point P(xp, yp) which is a valid point on Elliptic curve. Now to determine the value of 2P, doubling operation will be used. Newly evaluated point will also exist on the EC. Following equation will be used to find the point

$S = [(3Xp^2 + a)/2Yp] \bmod p$ (5)

Now the 2P can be expresserd as (X_R, Y_R) given by:

$X_R = (S2- 2\ Xp) \bmod p$ (6)

$Y_R = [S\ (Xp - X_R) - Yp] \bmod p$ (7)

To determine 3P, addition operation will be used. So addition will be performed when P≠Q. here P is (X_P, Y_P) and Q is 2P =(X_Q, Y_Q). now the slope S is given as

$S = [(Y_Q - Yp) /(X_Q - Xp)] \bmod p$ (8)

P+Q= -R

$X_R = (S^2 - Xp - X_Q) \bmod p$ (9)

$Y_R = [S\ (Xp - X_R) -Yp] \bmod p$ (10)

In this manner if we want to calculate kP, where k=15 then the following operations of addition and doubling will be performed

P	2P	3P	6P	7P	14P	15P
	Doubling	Addition	Doubling	Addition	Doubling	Addition

Every point will be calculated in similar way, till it reaches to the point at infinity.

3.2Proposed Algorithm

This algorithm first converts an image into binary and then map the

1. A square grid of required size is constructed by taking the binary data from source file. We are considering a grid of 32 X 32, padding with 0 if necessary.
2. As the image is now seen as a grid of 32 X 32, every pixel of this is first mapped on the elliptic curve by applying the genpoint(a, b, p).
3. Next the pixels are encrypted using ECC.

Genpoint(a,b,p)

{

For x=0;

While(x<=p)

{

$Y^2=(x^3+ax+b)\bmod p$

If y2 is a perfect square in GF(p)

Output(x,sqrt(y)), (x-sqrt(y))

x++;

}

Algorithm EC

{

// ***Key*** **Distribution**

// *Let* U_A and U_B be legitimate users

U_A= {P_A, n_A} // *Key* pair for UA

U_B= {P_B, n_B} // *Key* pair for UB

// *Send* the Public key of U_B, to U_A

Send(P_B,U_A);

// *Send* the Public key of U_A to U_B

Send (P_A, U_B);

// **Encryption at A**

PmI=aPm

// a: Intensity value from the image grid

// Pm: random point on EC

$P_B=n_B * G$

// *G* is the base point of EC

// n_B is the private key

CipherText={kG,PmI+k*P_B}

// **Decryption at B**

Let kG be the first point and

PmI + k*P_B be the second point

n_BkG = n_B * first point;

Calculate PmI = PmI + kP_B- n_BkG;

Calculate the Pm value from PmI using discrete logarithm.

3.3Implementation of Proposed Algorithm:

To map an image on the Elliptic Curve following steps are executed:

1. Assume the following elliptic curve

   $y^2= x^3-x+188$ mod 751

   That is: a=-1, b=188 and p=751. The elliptic curve group generated by the above elliptic curve is represented by Ep (a,b) =E_{751}(-1, 188).

   Let the generator point G=(0, 376). Then the multiples kG of the generator point are (for (1<=k<=751)

   G=(0,376) 2G=(1,376) 3G=(750,375) 4G(2,373)

   5G=(188, 657) 6G=(6, 390) 7G=(667,571) 8G=(121, 39)

   9G=(582, 736) 10G=(57, 332)…..

   762G=(328, 569) 763G=(677, 185) 764 G=(196,681) 765G=(417,320)

   766G=(3, 370) 767G=(1,377) 768G=(0,375) 769G=O (point at infinity)

   Encryption at sender side

   1. PmI=aPm, Where a is the intensity value of the pixels in the grid. PmI is the transformed value of the pixel on Elliptic Curve. Pm is the random point on the Elliptic Curve.
   2. G is the base point. Here I consider G as (0,376).
   3. Now generate the public key P_B

      P_B= n_B X G

      Where n_B is the secret key generated secretly by sender.
   4. Encrypted image pixel= {kG, PmI + kP_B}
   5. In the similar manner all the pixels will be first mapped on the elliptic curve and then converted into encrypted file.

Decryption at receiver side

1. To Decrypt the cipher image file, B multiplies the first point in the pair by B's secret key and subtract the result from the second point.
2. $PmI + kP_B - n_BkG = PmI + k(n_BG) - n_BkG = PmI$
3. PmI gives us the image vales converted or mapped on the Elliptic Curve.
4. Now from this We can easily recover Pm. As Pm= I * Pm
5. Above process will be repeated for every pixel of image and we will get the original image.

IV RESULT

In this paper an image is first transformed on EC and then encrypted using ECC. The work has been implemented in C language. The decryption algorithm perfectly recovers the original image.

Fig.1 Original Image

Fig. 2 Encrypted Image

Fig. 3 Decrypted Image

V CONCLUSION

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.

The proposedtechnique is implemented for BMP images of different sizes in C language. Here, the intensity of each pixel is transformed into the elliptic curve and encrypted using ECC. At the receiver size original image is recovered by using decryption algorithm different files and their encryption/decryption times are given in the table. It has been observed that the original image is recovered from the encrypted image.

Table 1 Image Encryption time Using ECC

File Name	Encryption using ECC	Decryption using ECC
Woman_darkhair.bmp	79.000000 ms	525.000000ms
Woman_blonde.bmp	436.000000 ms	73.000000 ms

Walkbridge.bmp	72.000000 ms	72.000000 ms
Pirate.bmp	655.000000 ms	712.000000 ms
Peppers_gray.bmp	701.000000 ms	993.000000 ms
Livingroom.bmp	281.000000 ms	978. 000000 ms
Lena_gray256.bmp	421.000000 ms	342. 000000 ms
Lake.bmp	32.000000 ms	946. 000000 ms
Jetplane.bmp	686.000000 ms	57. 000000 ms

It can be easily seen that ECC encrypts the images so well, that nobody can recover the image until he or she has possession of keys. Because of the logarithmic nature of elliptic curves they provide comparatively same level of security as of RSA but for smaller key size. In future the same technique can be applied on different image extensions and audio, video files.

REFERENCES

[1] N.Koblitz, Elliptic Curve Cryptosystems, *Mathematics ofComputation,* volA8, 1987, pp.203 -209.

[2] M.Aydos, T.Yanik and C.K.Kog, "High-speed implementation of an ECC based wireless authentication protocol on an ARM microprocessor," *lEEProcCommun.,Vol.* 148, No.5, pp. 273-279, October 2001.

[3] Kristin Lauter, "The Advantages of Elliptic Cryptography for Wireless Security", *IEEE Wireless Communications,* pp. 62- 67, Feb. 2006.

[4] Ray C. C. Cheng, Nicolas Jean-baptiste, Wayne Luk, and Peter Y. K Cheung,"Customizable Elliptic Curve Cryptosystems" , *IEEE Trans. On VLSI*

Systems, vol. 13, no. 9, pp. 1048-1059, Sep. 2005.

[5] Alessandro Cilardo, Luigi Coppolino, Nicola Mazzocca, and Luigi Romano,"Elliptic Curve Cryptography Engineering", *Proceedings of the*

IEEE, Vol. 94, no. 2, pp. 395 - 406, Feb. 2006.

[6] C. 1. McIvor, M. McLoone, and 1. V. McCanny, "Hardware elliptic curve cryptographic processor over GF(p)," *IEEE Trans. Circuits Syst.l*Reg.

Papers, vol. 53, no. 9, pp. 1946-1957, Sep. 2006.

[7] Gang Chen, GuoqiangBai, and Hongyi Chen, " A High-Performance Elliptic Curve Cryptographic Processor for General Curves Over GF(p) Based on a Systolic Arithmetic Unit" , *IEEE Trans. Circuits Syst. - 11:* Express Briefs, vol. 54, no. 5, pp. 412- 416, May. 2007.

[8] Standard specifications for public key cryptography, *IEEE standard,* pI363,2000.

[9] Williams Stallings, Cryptography and Network Security, *Prentice Hall,* 4th Edition, 2006.

[10] Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines, Henry B.Potoczny, "Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks," *Internationaljournalofsecurity and networks,* Vol. 2, No. 3/4, pp. 260- 271,2006.

[11] Sangook Moon, "A Binary Redundant Scalar Point Multiplication In Secure Elliptic Curve Cryptosystems," *International journal of networksecurity,* Vol.3, No.2, PP.132-137, Sept. 2006.

[12] Jaewon Lee, Heeyoul Kim, Younho Lee, Seong-Min Hong, and Hyunsoo Yoon, "Parallelized Scalar Multiplication on Elliptic Curves Defined over Optimal Extension Field," *International journal of networksecurity*, VolA, No.1, PP.99-106, Jan. 2007.

[13] Liu Yongliang, Wen Gao, Hongxun Yao, and Xinghua Yu , "Elliptic Curve Cryptography Based Wireless Authentication Protocol," *Internationaljournal ofnetwork security*, VolA, No.1, PP.99-106, Jan. 2007.

[14] R.V.Kurja, Kirti Joshi, N.Mohan Kumar, Kapil H Raranape, A.Ramanathan, T.N.Shorey, R.R.Simha, and V.Srinivas, Elliptic Curves, *International Distribution by American Mathematical Society*, 2006