Combining Multimedia Building Blocks In Image Analysis

P. Shanmugam[1], Dr. C. Loganathan[2]

[1] Associate Professor, Department of Mathematics, Kongu Engineering College,
Perundurai – 638052, India [2] Principal, Maharaja Arts and Science College, Coimbatore – 641407, India

Abstract

Messages are given as text needs to be coded to avoid loss of secrecy in any transaction. This has been atempted through any media requires tough crypto analysis and can be handled through known ciphers. This job gets better results while combining the text message along with other building blocks of multimedia. In this paper a noval approach to insert a message on an image and both of them are passed in a media using elliptic curve crypto systems. Caution is made in maintaining the quality of the vehicle image carrying the text. We have presented the algorithm and illustrated through standard images used in image analysis.

Key Words: Elliptic curve cryptography, Encryption, Image analysis, Multimedia, Text conversion.

1. Introduction

The idea of information security lead to the evolution of Cryptography. In other words, Cryptography is the science of keeping information secure. It involves encryption and decryption of messages. Encryption is the process of converting a plain text into ciphertext and decryption is the process of getting back the original message from the encrypted text. Cryptography, in addition to providing confidentiality, also provides Authentication, Integrity and Non-repudiation

The use of elliptic curves in public key cryptography was independently proposed by Koblitz and Miller in 1985[1] and since then, an enormous amount of work has been done on elliptic curve cryptography. Public key cryptography[2] does not require any shared secret key between the communicating parties. Elliptic Curve Cryptography[3] is emerging as an attractive public key cryptosystem. The attractiveness of using elliptic curves arises from the fact that similar lever of security can be achieved with considerably shorter keys than in methods based on the difficulties of solving discrete logarithms over integers or integer factorizations. Elliptic Curve Cryptography[4] provides an excellent solution not only for the data encryption but also for the secure key transport between two communicating parties. Understanding ECC needs full mathematical background on elliptic curves.[5]

2. Elliptic Curve Cryptography

Elliptic curve cryptography starts with generating points of a curve. Using the real numbers[6] for cryptography will cause a problem because it is very hard to store them precisely in computer memory and to predict how much storage will need for them. Also calculations over the real numbers are slow and inaccurate due to round-off error and the implementation of these calculations into cryptographic schemes require fast and precise arithmetic; thus elliptic curve groups over finite fields F_p and F_2m are used.

2.1 Construction of Elliptic Curve Group

Consider the elliptic curve E: $y^2 = x^3 + ax + b$ mod p defined over F_p where p is prime number and $4a^3 + 27b^2 \mod p$ is not 0. Then the set of (p – 1)/2 quadratic residues Q_p is obtained from the reduced set of residues Z_p = {1, 2, 3, ……, p – 1}. Now, for $0 \le x < p$, compute $y^2 = x^3 + ax + b$ mod p and determine whether the value of y^2 is in the set of quadratic residues Q_p. If so then there are two values in the elliptic group and if not so then the point is not in the elliptic group $E_p(a, b)$.[7]

Example: Consider the elliptic curve $E_{23}(1,1)$: $y^2 = x^3 + x + 1$ mod 23 defined over the prime number p = 23 and a = 1, b = 1 for which $4a^3 + 27b^2 \mod p$ is not 0. For the reduced set of residues E_{23} = {1, 2, 3, ……, 21, 22} the quadratic residues Q_{23} is obtained as follows.

Table-1: Quadratic residues Q_{23}

$x^2 \bmod 23$	$(p-x)^2 \bmod 23$	Q_{23}
$1^2 \bmod 23$	$22^2 \bmod 23$	1
$2^2 \bmod 23$	$21^2 \bmod 23$	4
$3^2 \bmod 23$	$20^2 \bmod 23$	9
$4^2 \bmod 23$	$19^2 \bmod 23$	16
$5^2 \bmod 23$	$18^2 \bmod 23$	2
$6^2 \bmod 23$	$17^2 \bmod 23$	13
$7^2 \bmod 23$	$16^2 \bmod 23$	3
$8^2 \bmod 23$	$15^2 \bmod 23$	18
$9^2 \bmod 23$	$14^2 \bmod 23$	12
$10^2 \bmod 23$	$13^2 \bmod 23$	8
$11^2 \bmod 23$	$12^2 \bmod 23$	6

The set of (23–1)/2 = 11 quadratic residues Q_{23} = {1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18} For $0 \le x < 11$,

Table-2: Generation of Elliptic Curve Points

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
y^2	1	3	11	8	0	16	16	6	15	3	22	9	16	3	22	10	19	9	9	2	17	14	22
$y^2 \in Q_{23}$	y	y	n	y	n	y	y	y	n	y	n	y	y	y	n	n	n	y	y	y	n	n	n
y_1	1	7		10	0	4	4	11		7		3	4	7				3	3	5			
y_2	22	16		13		19	19	12		16		20	19	16				20	20	18			

The points on the elliptic curve are

$$E_{23}(1,1) = \begin{Bmatrix} (0,1), (0,22), (1,7), (1,16), (3,10), (3,13), (4,0), (5,4), (5,19), (6,4), (6,19), (7,11), (7,12), (9,7), (9,16), (11,3), (11,20), \\ (12,4), (12,19), (13,7), (13,16), (17,3), (17,20), (18,3), (18,20), (19,5), (19,18) \end{Bmatrix}$$

2.2 Arithmetic in an Elliptic Curve Group

The negative of the point at infinity is – ∞ and is equal to ∞ and the negative of a point $P = (x, y)$ is defined to be $-P = (x, -y \bmod p)$.

Adding distinct points: If $P(x_P, y_P)$ and $Q(x_Q, y_Q)$ are distinct pints on $E_p(a,b)$ such that $P \ne -Q$ then their sum P + Q = R is given by

$x_R = [\lambda^2 - x_P - x_Q] \bmod p$ and

$y_R = [\lambda(x_P - x_R) - y_P] \bmod p$ where

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \bmod p .$$

Doubling the point: If the y coordinate of P is zero, modulo p, then P = – P. Doubling of the point $P = (x_P, y_P)$ with $y_P \ne 0 \bmod p$, is defined as $2P = P + P = R$ and is given by

$x_R = [\lambda^2 - x_P - x_Q] \bmod p$ and

$y_R = [\lambda(x_P - x_R) - y_P] \bmod p$ where

$$\lambda = \frac{3x_P^2 + a}{2y_P} \bmod p .$$

2.3 Elliptic Curve Encryption

Elliptic curve cryptography can be used to encrypt plaintext message M into ciphertext. The plaintext message M is encoded into a point P_M from the finite set of points in the elliptic group, $E_p(a,b)$ by multiplying the corresponding ASCII value with the generator point G. The first step consists in choosing the generator point, G $\in$ $E_p(a,b)$, such that the smallest value of for which nG = O is a very large prime number. The elliptic curve group $E_p(a,b)$ and the generator G are made public.

Suppose that A wants to encrypt and transmit plaintext message M to B. Each A and B selects a private key and uses it to compute their public key. A selects a random integer $n_A < n$ as his private key and computes his public key $P_A = n_A G$ and makes it publicly available. Similarly B selects a random integer $n_B < n$ as his private key and computes his public key $P_B = n_B G$ and makes it publicly available. To encrypt the message point P_M corresponding to the message M, A chooses his private key n_A and B's public key P_B to compute the ciphertext pair of points $C_M = [(n_A G), (P_M + n_A P_B)]$.

2.4 Elliptic Curve Decryption

After receiving the ciphertext pair of points C_M, B decrypts it to retrieve the plaintext message point P_M as follows:

First point, $n_A G$ is multiplied with his private key n_B to obtain $n_A n_B G$ and it is subtracted from the second point $P_M + n_A P_B$ = $P_M + n_A n_B G$, the plaintext point P_M corresponding to the plain text message M is retrieved.

Example: Consider the Elliptic curve $E_{281}(1,4)$. Let the generator point G = (0, 2). Then multiple of are 2G = (123, 178), 3G = (194, 239), etc and 311G = O - Point at infinity.
If A wants to encrypt the plaintext 'ENCRYPT' in which the first character is 'E'.
The ASCII value of the character is 101. Then $P_M = 101(0, 2)$ = (95, 173).
Let the private key of A be $n_A = 100$ then its public key is $P_A = n_A G$ = 100G = (254, 244).
Let the private key of B be $n_B = 200$ then its public key is $P_B = n_B G$ = 200G = (29, 265).
Then the ciphertext pair of points is

$$C_M = [(n_A G), (P_M + n_A P_B)]$$
$$C_M = [(254,244), ((95,173) + 100(29,265))]$$
$$C_M = [(254,244), ((95,173) + (31,151))]$$
$$C_M = [(254,244), (269,136)]$$

Upon receiving the ciphertext pair of points $C_M = [(254,244), (269,136)]$, B decrypt is as follows:

$P_M + n_A P_B - n_B(n_A G)$ = (269, 136) – 200 × (254, 244)
$P_M + n_A P_B - n_B(n_A G)$ = (269, 136) – (31, 151)
$P_M + n_A P_B - n_B(n_A G)$ = (269, 136) + (31, 130) since – (31, 151) = (31, –151) = (31, 130)
$P_M + n_A P_B - n_B(n_A G)$ = (95, 173) = P_M
Thus (95, 173) = (ASCII value of the character) × G.
Applying discrete logarithm concept to get back the ASCII value of the character from which the character is retrieved.

3. Inserting Text In An Image

To hide the text inside the image, the ASCII value of the text and the pixel value of the image are converted into streams of 8-bit binary. Two pixel pairs of the image in two adjacent rows are used to hide one character of the text. The four least significant bits of the selected pixel value in two adjacent rows are replaced respectively by the four least significant bits and four upper significant bits of one character of the text. The modified 8-bit binary numbers are converted to decimal number which gives the pixel value of the image, after hiding the text. To hide each character of secret message, two pixels are needed. So the number of characters that can be hidden in (n × n) image is given by the equation: Number of characters ≤ (n · n) ÷ 2 – n. In this equation, n pixels are subtracted because the secret text is not set in the first row of the cover image[8]. So start setting data from the second row of the cover image. The first row of the covered image is used to store specific data, like the position of last pixel in the covered image that contains secret data. Reconstruction of the secret text message is performed by reversing the process used to insert the secret message in the container image.

4. Image Encryption Using Elliptic Curve Cryptography

Elliptic Curve Cryptography, with proper choice of curve parameters, is used to encrypt images. The pixel value at each point of the image is used in place of ASCII value and encoded into pixel point. The same encryption and decryption method is adopted to compute the encrypted pair of points corresponding to the pixel value and to retrieve the pixel value from the encrypted pair of points.

5. RESULT

Cameraman image is taken and the text 'image' in inserted in the image by using the method explained in section 3.

Cameraman Original

Text inserted

157	157	157	157	157	…
158	158	158	158	158	…
159	159	159	159	159	…
158	158	158	158	158	…
156	156	156	156	156	…
…	…	…	…	…	…

Pixel value of Text inserted image

To encrypt the text inserted image, consider the elliptic curve $y^2 = (x^3 + x + 4) \bmod 281$; that is a = 1, b = 4 and p = 281. Let the generator point G = (0, 2) and note that 311G = O, the point at infinity.

If A wants to encrypt the Text inserted image, A selects his private key $n_A < n$ and generate the public key $P_A = n_A \times G$ and produces the ciphertext pair of points $C_M = \{n_A G, P_M + n_A P_B\}$. After receiving the ciphertext pair of points C_M, B multiplies the first point, $n_A G$ with his private key n_B and the subtract this from the second point $(P_M + n_A P_B)$. Thus $(P_M + n_A P_B) - n_B(n_A G) = P_M$. The pixel value M of the image at the position (1, 1) is 157 and therefore $P_M = 157G = 157 \times (0,2) = (243,156)$.

Let A chooses his private key $n_A = 100$ randomly and the private key of B is $n_B = 200$ and so

$P_B = n_B G = 200 \times (0,2) = (29,265)$.

Hence

$C_M = \{100 \times (0,2), (243,156) + (100 \times (29,265))\}$

$C_M = \{(254,244), (243,156) + (31,151)\}$

$C_M = \{(254,244), (23,162)\}$

All the Pixel values of the image are encrypted and the corresponding ciphertext pair of points are computed for the entire image.

After receiving the ciphertext pair of points $C_M = \{(254,244), (23,162)\}$, B computes

$P_M + n_A P_B - n_B(n_A G) = (23,162) - [200 \times (254,244)]$

$P_M + n_A P_B - n_B(n_A G) = (23,162) - (31,151)$

$P_M + n_A P_B - n_B(n_A G) = (23,162) + (31,-151)$

$P_M + n_A P_B - n_B(n_A G) = (23,162) + (31, 130)$, since – 151mod 281 = 130

$P_M + n_A P_B - n_B(n_A G) = (243,156) = P_M$

Applying discrete logarithm concept to get back, the pixel value of the image is retrieved. After retrieving all the pixel values, the text inserted image can be regenerated. From this reconstruction of the secret text message is performed by reversing the process used to insert the secret message in the container image.

6. Conclusion

In this paper, a novel idea has been developed from Elliptic Curve Cryptography. Instead of sending the encrypted ciphertext pair of points, of a plaintext message, from entity A to B, the plaintext is hidden within the image as described in section 4 and the pixel value at each point of the image is encrypted to a pair of points as described in section 5 and can be send from A to B with added security.

References

1. Koblitz. K, Elliptic Curve Cryptosystems, Mathematics of Computation, 48: 203-209, 1987.

2. Anoop. M S., Elliptic curve cryptography, an Implementation Guide

3. Prof. Jagdale. B. N., Prof Bedi. R. K., and Sharmishta Desai, “Securing MMS with High Performance Elliptic Curve Cryptography”, International Journal of Computer Applications, 8(7): 2010.

4. Suneetha. Ch., Sravana Kumar. D and Chandrasekhar. A., “Secure key transport in symmetric cryptographic protocols using elliptic curves over finite fields”, International Journal of Computer Applications, 36(1): 2011

5. Padma Bh, Chandravathi. D, Prapoorna Roja. P, “Encoding and Decoding of a Message in the Implementation of Elliptic Curve Cryptography using Koblitz’s Method”, International Journal on Computer Science and Engineering, 2(5): 1904-1907, 2010.

6. Kaabneh. K, Al-Bdour. H, “Key Exchange Protocol in Elliptic Curve Cryptography with no Public Point” American Journal of Applied Sciences, 2(8): 1232-1235, 2005.

7. Kefa Rabah, “Implementation of Elliptic curve Diffe-Hellman and EC Encryption Scheme” Information Technology Journal 4(2): 132-139, 2005,

8. Habes. A, “Information Hiding in BMP image Implementation, Analysis and Evaluation”, Information Transmission in Computer Networks 6(1): 1-10, 2006.

9. Stallings. W, “Cryptography and Network Security”, 4th edition, Prentice Hall, 2005