International Journal of Knowledge Based Computer Systems
Volume 5 Issue 2 December 2017
ISSN.: 2321-5623

Image Encryption Using Elliptic Curve Cryptography

N. Gupta
Department of Computer Science and Engineering, Govt. Engineering College, Bikaner, Rajasthan, India.
Email: 08niki@gmail.com

Abstract: Elliptic Curve Cryptography or Cryptosystem (ECC) is one of the public-key cryptosystem. The main advantage and benefit of ECC instead of RSA is that it gives equivalent security by using smaller key then in RSA; thereby it consumes less number of resource and also less amount of memory. There are various advantages of ECC over RSA such as low bandwidth usage, low computational time and small key size; it can also be used for image encryption. Through this paper image encryption with using ECC is presented. It discusses the encryption, compression and decryption of image using ECC on matlab as platform.

Keywords: Cryptography, Decryption, Elliptic curve, Encryption.

I. Introduction

There are two type of cryptosystem that most prominently defined: symmetric key cryptography and asymmetric key cryptography [6]. The symmetric key cryptography relies on shared key between communicating parties. Examples are Advanced Encryption Standard (AES) and Data Encryption Standard (DES). On the other hand, the asymmetric key cryptography use two keys for encryption and decryption processes; these keys are named as public and private keys. Common examples of asymmetric key cryptography are Rivest, Shamir, Adleman (RSA) [7] and El-Gamal cryptosystem [8]. The complication of the underlying mathematical problem represents the fundamental security of all protocols in the public-key cryptography [9]; the RSA relies on the difficulty of Integer Factorization problem (IFP), while El Gamal cryptosystem relies on Discrete Logarithm Problem (DLP) [10]. Hence, asymmetric key cryptography is slower than the symmetric key cryptography, it also requires larger memory capacity, and higher computational power for solving underlying mathematical problem than symmetric key cryptography.

Elliptical curve cryptography (ECC) is a public key encryption technique based on the elliptic curve theory that is used to create faster, smaller, and more efficient cryptographic keys for cryptography. ECC generates keys through the properties and underlying equations of the elliptic curve. It can yield a high level of security with a 164-bit key while other systems require a 1,024-bit key to achieve the goal. An elliptic curve is not just an ordinary ellipse (oval shape), but it is represented as a looping line intersecting two axes (i.e., x-axis and y-axis). ECC is based on properties of the underlying equation created from the mathematical equations derived from the points where the line intersects the axis. The principle is multiplying a point on the curve by a number will produce another point on the same curve, but the key feature is that it is very difficult to find what number was used for multiplication, even if you know the original points and the result.

For current cryptographic purposes, it is assume that an elliptic curve is a plane curve over a finite field which consists of the points satisfying the equation of elliptic curve.

$$y^2 = x^3 + ax + b$$

In beginning we assume that the distinguished points are at infinity, denoted ∞. (The coordinates are to be chosen from the fixed finite field of characteristic not equal to 2 or 3, and the curve equation should be somewhat more complicated.)

This set together with the group of operation of elliptic curves is called as Abelian group, with the points at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic relation.

$$Div^0(E) \to Pic^0(E) \cong E$$

Depending on the value of 'a' and 'b', elliptic curves may have different shapes on the plane. As it can easily seen and verified, elliptic curves are symmetric about the x-axis.

We can refine our definition of elliptic curve as follows:

$$\left\{(x,y) \in R^2 | y^2 = x^2 + ax + b, 4a^3 + 27b^2 \neq 0\right\} \cup \{0\}$$

II. Goal of Elliptic Curve Cryptography

There are three main aspects of enhancing security in elliptical curve cryptography they are confidentiality integrity and availability.

A. Confidentiality

From the ages of Technology it is important that the security of the data and information have the highest priority level. Hence confidentiality plays an important role in constitution of cryptography. Now as the name suggests it provide privacy to the user from praying Eyes it provide the feature of authorization if the user other party doesn't have authorization then they doesn't able to access the file or the data so they provide high level of confidentiality it is important that the data is encrypted by the authorized person and only in that person is able to decrypt it but it also have some threat to it these are snooping and traffic analysis.

B. Integrity

In Cryptography it is important that the message was sent by the sender and the message which is received by the receiver are exactly same integrity provide this facility in the cryptosystem integrity basically contains 2 mechanism for ensuring that the message on both side are same another free these are preventing mechanism and detector mechanism to prevent mechanism as the name suggests prevent the message from the attacker do not let that occur modified a information and data now another mechanism which is used and integrity is detective mechanism as the name suggests it is the mechanism which detect if there is any change or modification in the data which is sent by sender and receiver the receiver so and this way Cryptography provide complete integrity to the user.

C. Availability

Another important characteristic of cryptography is availability as confidentiality and integrity of the two major aspect of the Cryptography but it is of no use if the data is it available to the authorised user hands availability is the aspect and the property of the chapter system which provides the right to access of the information to the authorised user from anywhere after checking authentication and other words it provide it makes information available to the authorised user when they need it.

Hence all the three properties of cryptography play significant role in the trip to system are providing security but availability is another most important characteristic without it confidentiality and integrity doesn't hold any mean.

III. ECC Encryption and Decryption

Elliptic Curve Cryptography can be applied to encrypt plaintext message into cipher text and decrypt the cipher text back into plaintext message. The plaintext message is first mapped to a point on the curve. Underlying working algorithm is as follow:

A. Key Generation

1. Alice and Bob agree on a common curve, $y^2 \pmod p = x^3 + ax + b \pmod b$ with the generator point as $G(x_g, y_g)$.
2. Alice selects an integer as his private key and computes a point, $P_a = n_a G = (x_a, y_a)$ using the group law.
3. Alice's public key is reported as $P_a = (x_a, y_a)$
4. Bob also selects an integer $P_b = n_b G = (x_b, y_b)$ as his private key and computes a point, using the group law.
5. Bob's public key is reported as $P_b = (x_b, y_b)$

B. Encryption

Suppose that Alice is dispatching the message $P_m = (x_m, y_m)$ to Bob. His steps are given below:

1. Alice chooses a random integer k.
2. Using the group law, he computes the two points, $c_1 = kG$ and $c_2 = P_m + kP_b$
3. Alice sends the two pair of points, $C_m = (c_1, c_2)$ as ciphertext to Bob.

C. Decryption

Bob obtains the cipher text, $C_m = (c_1, c_2)$ from Alice. His reconstruction steps to recover original message are as follows:

He multiplies c_1 by his private key and subtracts it from c_2. That is, he calculates

$$\begin{aligned} c_2 - n_b c_1 &= (P_m + kP_b) - n_b(kG) \\ &= (P_m + kn_b G) - n_b\, kG = P_m \\ &= (x_m, y_m) \end{aligned}$$

IV. Elliptic Curve Cryptography Computation

A. Operation Over Elliptic Groups

There is a rule called the chord-and-tangent rule, for adding two points on an elliptic curve E(Fp) to give a third elliptic curve point. Together with this addition operation, the set points E(Fp) forms with O serving as the identity. This is the group which is used in the construction of elliptic curve cryptosystems. The addition rule is explained geometrically. Let P = (x1, y1) and Q

= (x2, y2) be two distinct points on an elliptic curve E as shown in the Fig. 1. Then the sum of P and Q, denoted by R = (x3, y3), is defined as follows:

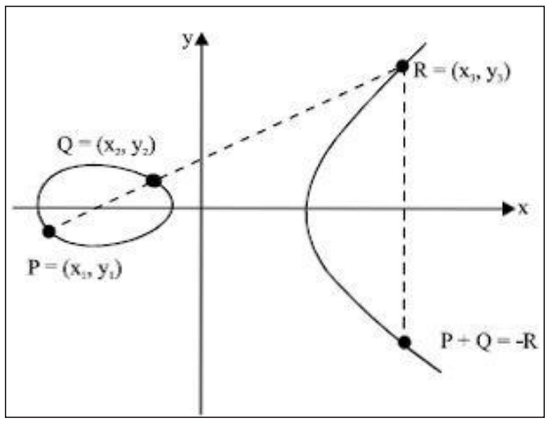

Fig. 1: Geometric Description of the Addition of Two Ditinct Elliptic Curve P+Q = R

First draw the line through the point P and Q; this line intersects the elliptic curve at the third point R. Then R is the reflection of this point in the x-axis. The elliptic curve in the Fig 1 consists of two parts, the ellipse-like figure and the infinite curve.

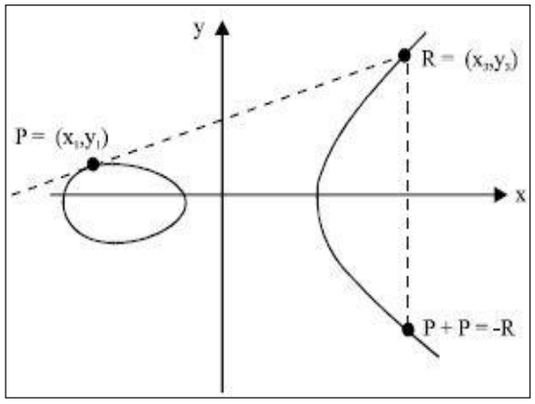

Fig. 2: Geometric Description of the Addition of Two Distinct Elliptic Curve P+P = R

If P = (x1, y1), then the double of P, denoted by R = (x3, y3), is defined as follows: First draw the tangent line to the elliptic curve at P. This line intersects the elliptic curve at the second point. Then R is the reflection of this point in the x-axis as shown in Fig 2.

The following algebraic formulae for the sum of two points and double of the point can now be derived from the geometric description in the next two sections.

B. Point Addition

To add two points P and Q, we will draw the line PQ through them (or use the tangent line at P to add it to itself), find the third point of intersection −R of that line, and reflect it over the axis of symmetry of the curve. The resulting point, R, will be the sum of P and Q.

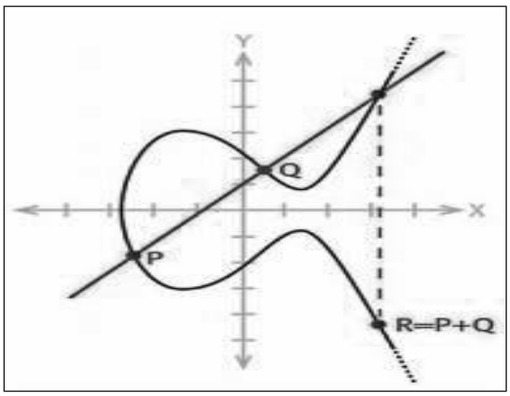

Fig. 3: Point Addition in Elliptic Curve

Theorem 1: The addition law on elliptic curve C has the following properties (where O = −O is the point at infinity, and if *P = (x0, y0), then −P = (x0, −y0))*:

- For point $P \in C$, $P + O = P$,
- For points $P, Q \in C$, $P + Q = Q + P$
- For point $P \in C$, there is some point $-P$ such that $P + (-P) = O$
- For $P, Q, R \in C$, $(P + Q) + R = P + (Q + R)$.

C. The ElGamal Elliptic Curve Cryptosystem

Suppose that we have some elliptic curve C defined over a finite field where is large (and p is prime). Suppose that C, q, and a point G ∈ C are publicly known, as is the embedding system. When Alice wants to communicate secretly with Bob, they proceed thus:

- Bob chooses a random integer, and publishes the point (while b remains secret).
- Alice chooses her own random integer and sends the pair of points to Bob (while a remains secret).
- To decrypt the message, Bob calculates from the first part of the pair, then subtracts it from the second part to obtain, and then reverses the embedding to get back the message m.
- Eve, who can only see must find from or from to make sense of Pm + a(bG), so her problem is reduced to the ECDLP, and she is thwarted.

This is a successful cryptographic system because every operation that Alice and Bob perform (addition or subtraction on the curve) is relatively easy, while the operation that Eve would have to perform to crack the system is extremely difficult.

V. Mechanics of Elliptic Curves

Elliptical is a mathematical aspect so if we define optical come over any function then we have to define it in the form of equation. Equation of elliptical curve is define on two things

1. numeric finite field and
2. Characteristic finite field.

An elliptic curve is the solution set of a cubic equation in two variables. For theoretic purposes, the equation can be brought into the Weierstraβ form, i.e., E: y2 = x3+ax+b, [9] with integer coefficients a and b, although other forms can be used as well. The solution set is relative to the field of definition, such as the field of complex numbers. The greatest interests in the rational solutions are such equations [9]. The rational points on the elliptic curve E are the points E (a, b) that satisfy the defining equation. The number of rational points on the elliptic curve is determined uniquely, if the set of parameters (a, b, p) are specified, this number is refer as the order of the elliptic curve E and is denoted by #E [8]. It is known that rational points form additive group in the addition over the elliptic curve as shown in Fig 4. But most of the theory and essentials for all the cryptographic applications lie in the solutions mod p (or, more generally, in solutions over finite fields) [10]. One of the key features of elliptic curves is that mod p is of the size of the solution set should never be too far from p. The exact theorem, proved by Hasse in 1933, is |Np-p|#2p½ where, Np is the number of solutions mod p. This ensures that for large p, there are lots of solutions over the finite field Fp [9].

But the main feature of elliptic curves, over any field, is the solution set, with an extra "point at infinity" forms a group, with a group law given by the explicit pair of rational functions [8]. The group turns out to be abelian group (hence the additive notation) and the point at infinity, usually denoted by 0, is "zero" element. In many cases, the order of the group (over function) is itself a large prime, q, or a small multiple of such a prime number [7]. When that happens, the curve is ready for use in cryptography.

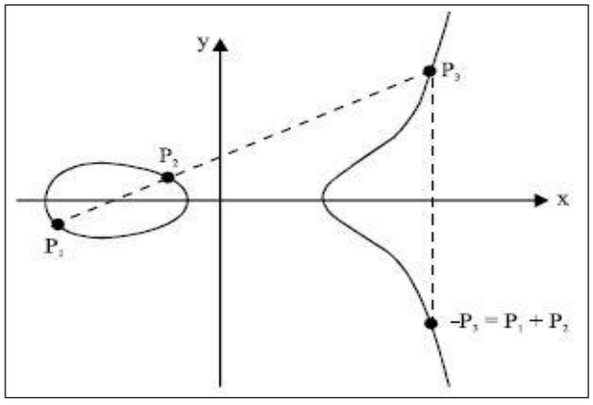

Fig 4. Addition Over Elliptical Curve

VI. Image Encryption Using Elliptic Curve Cryptography

In case of image encryption it is important that it include encryption with compression so that we can maintain the quality and size of the image. Larger size is more subjected to distortion over encryption and sending and receiving image. It basically includes the following ways to achieve it:

- First encryption then compression.
- Encryption with compression take place jointly.
- First compression and then encryption.

The encryption algorithms that work jointly with the compression algorithms are known as 'joint compression and encryption algorithms'[11], while the algorithms that work independently of compression algorithms are known as 'compression-independent encryption algorithms' [11]. In joint compression and encryption algorithms, encryption is performed during compression [11], or during quantization [12]. On the other hand, in compression-independent encryption algorithms, encryption can be done before compression [14] or after compression [15]. In this work we use ECC with joint compression to encrypt and compress image.

The operations on elliptic curve cryptography are defined over the elliptic curve equation.

$$y^2 = x^3 + ax + b \bmod N$$

Where (a, b) are the coefficients that define the curve, and x and y are the coordinate values of point P. The public key is a point in the curve; while the private key is a secret random number generated by the owner entity [21]. The public key is achieved by multiplying the private key with the generator point G on the curve, and this operation is known as point or scalar multiplication [21]. In point multiplication the chosen point from the curve is multiplied by a scalar integer, which is achieved using two operations named as point addition and point doubling.

$$\lambda = \begin{cases} \left(\frac{y_2 - y_1}{x_2 - x_1}\right) mod N \text{ if } P \neq Q(\text{point addition}) \\ \left(\frac{3x_1^2 + a}{2y_1}\right) mod N \text{ if } P = Q(\text{point doubling}) \end{cases}$$

Basically in ECC we don't encrypt or decrypt the message. In ECC the message is embedded in the point on the curve and then this point is encrypted using point multiplication and sends with receiver public key and sender public key to the receiver and then the receiver decrypt the message using his own private key.

To encrypt and compress an image, it first takes an image from the user and converts each pixel into a binary and produce a binary image so that the quality and color of image shouldn't be affected. After this there is another step of quantization. Quantization is performed where the higher spatial frequency coefficients whose amplitudes are below a certain threshold are set to zeros while the coefficients with lower spatial frequency are preserved [19]. Distortion in image frequency can't be visible by human eyes but whenever compression and encryption take place on any image there is distortion occur in the frequency of the image and which further lead to the degrade quality of the image. Now after that each point is then encrypted using ECC. And then this point is send to the receiver.

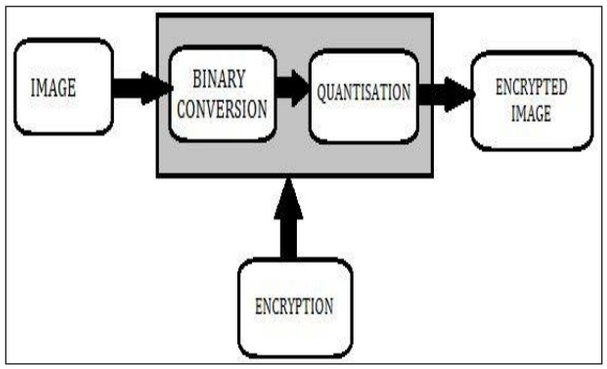

Fig. 5: Flowchart of Image Encryption

Decryption includes the same steps but in reverse order. So that receiver gets the right result using his private key.

VII. Discussion And Result

In this section result of color image encryption using ECC is presented. Result include image during binary conversion and image during the process of quantization is presented. It also includes the decryption result.

Fig. 5 represents the original image of candy then the encrypted and compressed image and the 3rd or final image is resultant image or the decrypted image.

Fig. 6: ECC Encryption and Decryption of Image

Fig. 6 represents the binary image of original image then encrypted image and the final decrypted binary image.

Fig. 7: Binary Image of Encryption and Decryption

Fig. 7 represents the process of quantization that is frequency of the original image, encrypted/compressed image and the final output resultant image i.e. decrypted image.

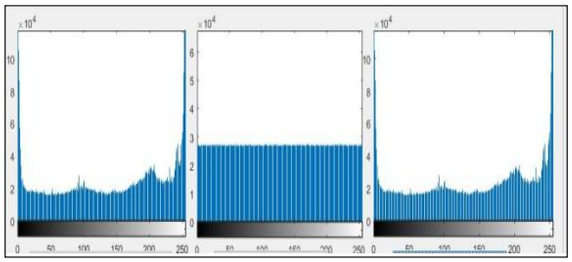

Fig. 8: Frequency Histogram of Encryption and Decryption

This is how the image encryption takes place using the ECC and the respective results. Now another thing related to ECC is related to level of security. So in case of ECC, it works on the DLP in which it is very difficult for the hacker/third person to extract the key which gives the first point of cipher pair (kG) and the generator point G. Even a small key provide high level of security.

VIII. Conclusion and Future Work

This paper presents the concept of image encryption using elliptic curve cryptography. Result show that the ECC fulfill the entire requirement to not even encrypt image but also provide high level of security. It also maintains the quality and color of the image. It concludes that ECC can further use for the transferring multimedia providing high security with less memory usage. Even it has potential for multimedia steganography.

Acknowledgement

I would like to express my sincere thanks to Asst. Prof. Rishiraj Vyas for his advice during my research work. As my supervisor, he has constantly encouraged me to remain focused on achieving my goal. I must acknowledge the academic resources that I have got from Govt. Engineering College, Bikaner. I would

like to thank administrative and technical staff members of the Department who have been kind enough to advise and help in their respective roles.

REFERENCES

[1] R. Soram, and E. S. Meitei, *International Symposium on Advanced Computing and Communication (ISACC),* 2015.

[2] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," *IEEE Wireless Communications*, vol. 11, no. 1.

[3] G. Vennila, M. Manikandan, and S. Aswathi, "Performance analysis of point multiplication algorithms in ECDH for an end-to-end VoIP network," *INDICON*, 2015.

[4] P. Mathew, P. Jilna, and P. P. Deepthi, "Efficient implementation of EC based key management scheme on FPGA for WSN," *International Conference on Telecommunication Systems Services and Applications (TSSA),* 2015.

[5] X. Fang, and Y. Wu "Investigation into the elliptic curve cryptography," *3rd International Conference on Information Management (ICIM),* 2017.

[6] S. R. Singh, A. K. Khan, and S. R. Singh, "Performance evaluation of RSA and elliptic curve cryptography," *2nd International Conference on Contemporary Computing and Informatics (IC3I),* 2016.

[7] R. V. Rijswijk-Deij, K. Hageman, A. Sperotto, and A. Pras "The performance impact of elliptic curve cryptography on DNSSEC validation," *IEEE/ACM Transactions on Networking,* 2017.

[8] S. R. Singh, A. K. Khan, T. S. Singh, "A critical review on Elliptic Curve Cryptography," *International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),* 2016.

[9] K. Jiang, B. Zhao, W. Shan, L. Wang, and J. Liu, "Profiling attack on modular multiplication of elliptic curve cryptography," *12th International Conference on Computational Intelligence and Security (CIS),* 2016.

[10] F. Akhter, "A novel elliptic curve cryptography scheme using random sequence,".

[11] 2015 International Conference on Computer and Information Engineering (ICCIE).

[12] M. S. Salah, A. Maizate, and M. Ouzzif, "Security approaches based on elliptic curve cryptography in wireless sensor networks," 27th International Conference on Microelectronics (ICM), 2015

[13] P. Chandrakar, and H. Om, "A secure two-factor mutual authentication and session key agreement protocol using Elliptic curve cryptography," *IEEE International Conference on Computer Graphics, Vision and Information Security (CGVIS),* 2015.

[14] N. Alimi, Y. Lahbib, M. Machhout, and R. Tourki, "Elliptic curve cryptography implementations and evaluation," *2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP),* 2016.

[15] D. He, H. Wang, M. K. Khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications,* vol. 10, no. 14, pp. 1795-1802, Sep. 2016.

[16] L. Deligiannidis, "Elliptic curve cryptography in Java," *IEEE International Conference on Intelligence and Security Informatics (ISI),* 2015.

[17] J. H. Silverman, "Elliptic curve," Springer International Edition, 2010.

[18] L. C. Washington, "Elliptic curves: Number theory and cryptography," 2nd ed., 2008.

[19] I. F. Blake, G. Seroussi, and N. P. Smart, "Elliptic curves in cryptography," Cambridge University Press,1999.

[20] D. B. Johnson, A. J. Menezes, "Elliptic curve DSA (ECDSA): An enhanced DSA," 2012.

[21] K. Lauter, The Advantages of Elliptic Curve Cryptography for Wireless Security, Microsoft Corporation.