International Journal of Students Research in Technology & Management
Vol 1(2), April 2013, pg 115-117

IMAGE ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY

Ashutosh Shukla[1], Jay Shah[2], Nikhil Prabhu[3]
Electronics & Telecommunication Engineering Department,
[1,2]Thakur College of Engineering and Technology, Kandivali(E) , Mumbai-400101
[3] St Francis Institute of Technology Borivali (W), Mumbai - 400103

Abstract

This paper deals with encryption of image using Elliptic curve cryptography (ECC).Elliptic curve cryptography (ECC) is an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields. Basic ElGamal elliptic curve encryption is used for encryption of the image. It brings about confidential, authentication and integrity in the exchange of data. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements.

Keywords: ECC, domain parameter generation, key pair generation, ElGamal encryption algorithm.

I. Introduction

The way to secure distributed multimedia applications is to encrypt multimedia data using public key cryptography algorithms. Cryptography means protecting private information against unauthorized access in that situation where it is difficult to provide physical security [1]. It is science of using mathematics to encrypt and decrypt data. The basic idea behind the cryptography is that "If it is not possible to prevent copying of information, it is better to prevent compression."

II. Elliptic Curve Cryptography(ECC)

Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible [2]. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

For current cryptographic purposes and elliptic curve is a plane curve which consists of the points satisfying the equation (1)

$$y^2 = x^3 + ax + b \qquad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

along with a distinguished point at infinity, denoted "∞". (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve will be somewhat more complicated)[3].

A. **ECC Domain Parameters**

The public key cryptographic systems involve arithmetic operations on Elliptic curve over finite fields which are determined by elliptic curve domain parameters.

The ECC domain parameters over Fq is defined as D = (q, FR, a, b, G, n, h), where

• q: prime power, that is q = p or q = 2m, where p is a prime

• FR: field representation of the method used for representing field elements ∈ Fq

• a, b: field elements, they specify the equation of the elliptic curve E over Fq, $y^2 = x^3 + ax + b$

• G: A base point represented by G= (xg, yg) on E(Fq) • n: Order of point G , that is n is the smallest positive integer such that nG = O

• h: cofactor, and is equal to the ratio #E(Fq)/n, where #E(Fq) is the curve[4].

B. **Key Generation**

Alice's (or Bob's) public and private keys are associated with a particular set of elliptic key domain parameters (q, FR, a, b, G, n, h).

Alice generates the public and private keys as follows

1. Select a random number d, d ∈ [1, n – 1]
2. Compare Q = dG.
3. Alice's public key is Q and private key is d.

It should be noted that the public key generated needs to be validated to ensure that it satisfies the arithmetic requirement of elliptic curve public key.[4]

a. ElGamal Elliptic Curve Encryption

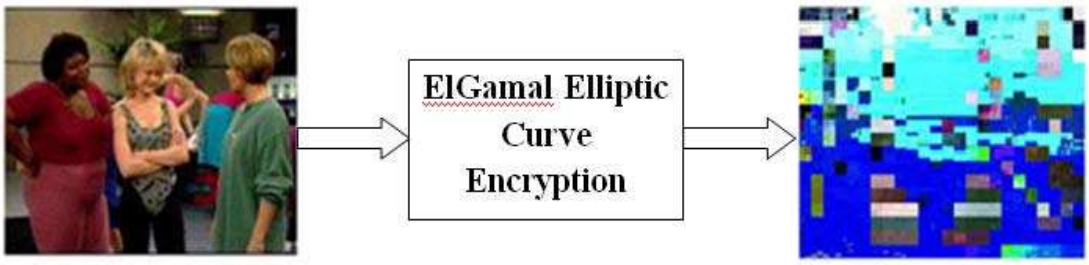
Elliptic curve cryptography can be used to encrypt an image, M, into cipher text. The image M is encoded into a point PM form the finite set of points in the elliptic group, Eq(a,b). The first step consists in choosing a generator point G ∈ Eq(a,b),such that the smallest value of n such that n G=O is a very large prime number. The elliptic group Eq(a,b) and the generator point G are made public.

Each user select a private key, nA <n and compute the public key PA = nA *G*A . To encrypt the point PM for Bob, Alice chooses a random integer k and computes the cipher text pair of points P*C* using Bob's public key PB : P*C* =[(kG),(PM+kPB)] [5].

III. Results and Conclusions

In this paper, we have presented an application of ECC with Generator G in image encryption. ECC points convert into cipher image pixels at sender side and decryption algorithm is used to get original image within a very short time with a high level of security at the receiver side. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the image encryption, which are beneficial to systems where real time performance is a critical factor ECC can be used into a

security system such as video compression, face recognition, voice recognition, thumb impression, sensor network, industry and institutions.



References

1. William Stallings, Cryptography and Network Security, Prentice Hall, 4th Edition, 2006.
2. V. Miller, "Uses of elliptic curves in cryptography", Advances in Cryptology, Springer-Verlog New York,1986
3. Jeffrey L. Vagle, "A Gentle Introduction to Elliptic Curve Cryptography",BBN Technology,Nov21,2010.
4. D.Hankerson, A.Menezes, and S.A. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2004.
5. ElGamal, T., "A public key cryptosystem and a Signature scheme based on discrete logarithm," IEEE Trans. Informn, Theory, IT-31, no.4, pp 469-472, July 1985.