An Extensive Review on Elliptic Curve Cryptography for Ciphering Images

Priyangi Trivedi[1] & Rishi Sharma[2]
[1]M-Tech Research Scholar, [2] Research Guide
Department of Electronics & Communication Engineering, OIST, Bhopal

Abstract: It is generally accepted that data encryption is the key role in current and future technologies. Many public key cryptography schemes were presented and divided into different classes, depending on a specific mathematical problem. Cryptography plays an important task in accomplishing information security. It is used for encrypting or signing data at the source before transmission, and then decrypting or validating the signature of the received message at the destination. Since the introduction of the public-key cryptography by Diffie and Hellman in 1976, the potential for using the discrete logarithm problem in public-key cryptosystems has been recognized. There are several public key cryptography, such as RSA, El-Gamal and Elliptic curve cryptography.

Keywords : Encryption, Elliptic Curve Cryptography

I. INTRODUCTION

Message Encryption

Encryption is the process of encoding messages that only authorized users can access it. In an encryption scheme, the message or information, known as plaintext, is encoding using an encryption algorithm, converted it into an unreadable ciphertext. This is generally done with the use of an key along with encryption algorithm. So, any adversary can't be able to settle anything about the original message. An authorized user, however, is capable of decode the ciphertext by using a decryption algorithm, that normally requires a secret decryption key, that adversaries do not have access to it. Cryptography has two way of an encryption process called symmetric key encryption and asymmetric key encryption or public key encryption is given below.

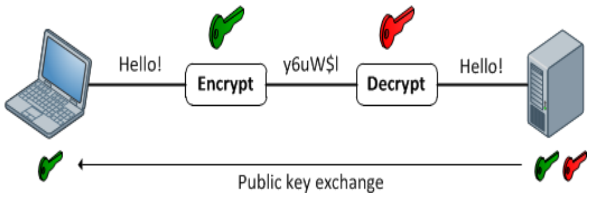

Fig. 1: Symmetric Key Encryption Process

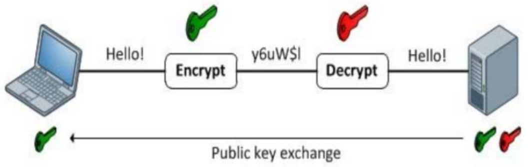

Fig. 2: Asymmetric Key Encryption Process

Digital Signature

Digital signatures rely on certain types of encryption to ensure authentication of sender. The signature process intended to receiver that the message was sent by sender and nothing modified at the time of transmission. Digital signatures are generally made in a two - step .The first step is to use a secure hashing algorithm on the data. Thus, when a signature is verified by the public key, it decrypts to a hash matching the message. That hash can only be deciphered by using the public key if it were encrypted with the private signing key.

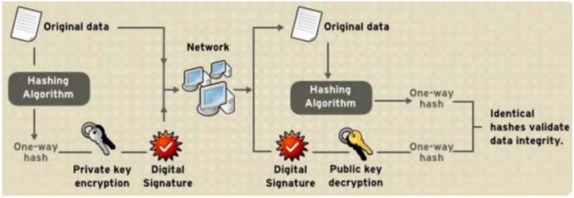

Fig. 3: Digital Signature

Cryptography is based on hard mathematical problems like prime number factorization, Elliptic curve discrete logarithm problem and discrete logarithm problem. The idea behind these problems is the computation can be easily done in one direction, but it is very difficult in the opposite direction. It is not difficult to find the result of multiplying two numbers, but it is extremely challenging to find prime factors of a number. Thus, cryptography is concerned with the design and the analysis of mathematical techniques which can offer secure communications in the presence of malicious adversaries. It is an area which is concerned with the transformation of data for security reasons.

Before moving further, these are a number of terms which are commonly associated with cryptography:

- **Plaintext:** The message which is transmitted to the recipient.
- **Encryption:** The procedure of changing the content of a message in a way that it conceals the real message.
- **Ciphertext:** The output which is produced after encrypting the plaintext.
- **Decryption:** The reverse function of encryption. It is the process of retrieving the plaintext from the ciphertext.

Security Requirements

There must be some security services to secure the communications, to prevent some security issues such as eavesdropping.

Cryptography provides the following security services:

1. *Confidentiality:* A service which keeps information accessible only to those who are authorized to access this information. The service contains both protection of all user data which are being transmitted between points and likewise, the protection of the traffic flow analysis.

2. *Integrity:* A service which ensures that only authorized users who are capable of writing, deleting of the transmitted information.

3. *Authentication:* A service which a receiver determines its source to confirm the sender‟s identity by using something that you have or you know. Normally, it is done by using the sender public key. It is the same integrity provided by digital signature.

4. *Non-repudiation:* It ensures the sender and receiver from denying the sending or receiving of a message and the authenticity of their signature. Typically, it is provided by digital signature.

Types of cryptography

There are two main types of mathematical cryptography

• Symmetric or secret key

• Asymmetric or public key

Symmetric Key

Symmetric key is a relatively easy concept to understand. Essentially one party (the encryptor) uses a secret key to a mathematical function which encrypts the plaintext message to a secure form. The message is passed to the decrypted that uses the same key to apply an inverse mathematical function which decrypts the message returning it to its original plaintext. The principal issue in symmetric cryptography is the secure transport of the key between the parties. Examples include DES, IDEA, & AES.

Asymmetric Key

Asymmetric key cryptography is a more complex concept to grasp but is generally more useful for application level security. The key is broken up into two parts known as the public key and the private key. The public key is used to encrypt the message and the private key to decrypt. Asymmetric is popularly known as public key cryptography.

II. LITERATURE SURVEY

N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal, [1] The growing dire need for more and more secure systems has led researchers worldwide to discover and implement newer ways of encryption. Public key cryptography techniques are gaining worldwide popularity for their ease and better strength. With the rapid developments of the communication and applications of multimedia techniques in recent years lead the researchers to focuses on the security of digital data over the internet. In this paper authors have discussed the use of Elliptical Curve Cryptography for ciphering color images. ECC has been proved to score over RSA on the basis of its strength and speed. In this paper authors have used NIST Curves for ciphering color image.

L. Chen, X. Chen and Z. Peng, [2] in this paper, a novel public key encryption scheme for large image is presented based on elliptic curve. As a public key encryption scheme, it does not need to exchange and distribute secret keys. Based on elliptic curve discrete logarithm problem (ECDLP), the scheme has high security. The simulation results show that the presented scheme is computationally less complex than ECC (Elliptic Curve Cryptography) and suitable for large image encryption.

S. Sowmya and S. V. Sathyanarayana, [3] Until recently, Cryptography has been of interest primarily to the military and diplomatic communities. But the dawning of the information age has revealed an urgent need for cryptography in the private sector too. Cryptography is the study of techniques for ensuring the secrecy and authentication of the information. In this paper, cyclic elliptic curve of the form $y^2 = x^3 + ax + b$, a, b $\in$ GF(p) with order M is considered and key Sequences are derived from random sequence of cyclic elliptic Curve points. Elliptic Curve is a cubic equation in two variables, x and y, with coefficients from a field satisfying certain conditions. For cryptographic applications the coefficients are chosen from finite fields. A point on the Elliptic curve is a pair of (x, y) which satisfies the Elliptic curve equation. The total number of points (x, y) which satisfy the elliptic curve equation along with x=∞, y=∞ is called the Order of the curve `M'. The least integer N for which NP is equal to point at infinity O is called order of the point P. Elliptic curves for which there exists a point P having the same order N, as that of the curve M are called cyclic elliptic curves

Table : Summary of Literature Review

SR. NO.	TITLE	AUTHORS	YEAR	METHODOLOGY
1	Elliptic Curve Cryptography for ciphering images	N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal	2015	Discussed the use of Elliptical Curve Cryptography for ciphering color images. ECC has been proved to score over RSA on the basis of its strength and speed.
2	A Novel Public Key Encryption Scheme for Large Image	L. Chen, X. Chen and Z. Peng	2014	a novel public key encryption scheme for large image is presented based on elliptic curve.
3	Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)	S. Sowmya and S. V. Sathyanarayana	2014	Cyclic elliptic curve of the form y2 = x3 + ax + b, a, b ∈ GF(p) with order M is considered and key Sequences are derived from random sequence of cyclic elliptic Curve points.
4	Multi image hiding using joint transform digital holography	N. Padmapriya, P. Elamathi and P. Kanimozhi	2014	Has been used multi image hiding technology
5	Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network	Baheti, L. Singh and A. U. Khan	2014	Introduces an efficient symmetric encryption scheme based on a cyclic elliptic curve and chaotic system that can overcome these disadvantages.
6	Robust and Secure Image Steganography Based on Elliptic Curve Cryptography	D. E. M. Ahmed and O. O. Khalifa	2014	The issue of secure and robust image data hiding is proposed through using (LSB) technique and Elliptic curve cryptography (ECC).
7	Elliptic curve based key generation for symmetric encryption	S. Maria Celestin Vigila and K. Muneeswaran	2011	Presents the implementation of stream cipher, where the key stream is generated based on the properties of Linear Feedback Shift Register and cyclic Elliptic Curve over a finite prime field.
8	An Ethical Way of Image Encryption Using ECC	K. Gupta, S. Silakari, R. Gupta and S. A. Khan	2009	Proposed image encryption method using elliptic curve cryptography (ECC). RSA is too slow compared to ECC because ECC required smaller key size.
9	Secure electronic passport certification using re-water marking	V. Mehan, R. Dhir and Y. S. Brar	2013	A novel re-watermarking system is proposed for authenticating electronic passport by using Elliptic Curve Cryptography (ECC) applied in dual domain.
10	Image Encryption for mobile devices	T. N. Shankar, G. Sahoo and S. Niranjan	2010	Introduce an algorithm 'Elliptic Curve Cryptography for Image Encryption'.

A pseudorandom sequence generator based on chaotic function and Elliptic Curve arithmetic over GF (p) is proposed here. The logistic Map is used as a chaotic function which generates a random sequence of real numbers. This random real sequence is converted to binary which drives an Elliptic Curve arithmetic module generating a random sequence of Elliptic Curve points. The sequence of points {P, 2P... NP} is calculated from a base point P, and stored in a file. Every element in this sequence is a point on the cyclic elliptic curve. The Chaotic binary sequence selects x or y-coordinates of elliptic curve points, pre-computed and stored. This forms a random integer sequence. The randomness properties of this sequence have been tested using various techniques like, auto correlation distribution, cross correlation distribution and first return map. It is observed that the sequence generated satisfies the required randomness properties. These sequences find applications in Stream Cipher Systems. An additive Stream Cipher system is designed using this sequence as the key sequence to encrypt images. Results of image encryption and decryption for a medical image is discussed and analyzed in this paper. The results are also compared with the scheme proposed by Lap-Piu Lee and Kwok-Wo Wong [1]. The security analysis of the proposed system is also discussed. It is interesting to observe that, proposed algorithm is superior compared to Lap-Piu Lee scheme [1].

N. Padmapriya, P. Elamathi and P. Kanimozhi, [4] In the world of internet and digital technology, even with the most advanced technology protecting information from unauthorized distribution is still a challenging problem. Hence authors can protect a data from unauthorized access through multi image hiding technology. This multi image hiding uses joint transform correlate architecture adopting two-step phase-shifting digital holography. The multi image is encrypted by using ECC algorithm. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The encrypted of multi image is recombined and embeds into the host image. The experimental result shows that the proposed system multi image hiding is more efficient than others.

Baheti, L. Singh and A. U. Khan, [5] as multimedia applications are used increasingly; security becomes an important issue of security of images. The combination of chaotic theory and cryptography forms an important field of information security. In the past decade, chaos based image encryption is given much attention in the research of information security and a lot of image encryption algorithms based on chaotic maps have been proposed. But, most of them delay the system performance, security, and suffer from the small key space problem. This paper introduces an efficient symmetric encryption scheme based on a cyclic elliptic curve and chaotic system that can overcome these disadvantages. The cipher encrypts 256-bit of plain image to 256-bit of cipher image within eight 32-bit registers. The scheme generates pseudorandom bit sequences for round keys based on a piecewise nonlinear chaotic map. Then, the generated sequences are mixed with the key sequences derived from the cyclic elliptic curve points. The proposed algorithm has good encryption effect, large key space, high sensitivity to small change in secret keys and fast compared to other competitive algorithms.

D. E. M. Ahmed and O. O. Khalifa, [6] With the ease of editing and perfect reproduction in digital multimedia, the protection of ownership and the prevention of unauthorized tampering of multimedia data (audio, image, video, and document) become important concerns. Steganography is one of these schemes that entails the opportunity of hide any secret information into images. Recently there are many techniques used for robust and secure image steganography that can trade off between the capacity, payload, security, minimizing distortions of the image and high robustness. All these are challenges that need to implement a suitable technique that verify the most of these challenges. However developing a robust and secure image steganographic technique against detect ability need to combined cryptography and steganography. In this paper the issue of secure and robust image data hiding is proposed through using (LSB) technique and Elliptic curve cryptography (ECC). The proposed scheme allow the sender to select a suitable cover and secret message that decidable to transmit through unsecure channel and then encrypt the message using (ECC) and embed it by (LSB) into selected cover.

S. Maria Celestin Vigila and K. Muneeswaran, [7] With the explosion of networks and the huge amount of data transmitted along, securing data content is becoming more and more important. Data encryption is widely used to ensure security in open networks such as the internet. This paper presents the implementation of stream cipher, where the key stream is generated based on the properties of Linear Feedback Shift Register and cyclic Elliptic Curve over a finite prime field. In this paper authors illustrate the process of encryption/decryption of an image in spatial domain and also encrypt key file parameters needed for generating the key stream to other parties using Elliptic Curve Cryptography. Therefore the encrypted key file parameters are only transmitted and not the entire full length key. Since Elliptic Curve Cryptography is replacing RSA for key exchange and Elliptic Curve based stream cipher offers a good choice for encryption in real time application. The strength of the proposed cipher lies in the generation of random sequence using Linear Feedback Shift Register over GF(p), difficulty of Elliptic Curve Discrete Logarithmic Problem and the entire key need not be transmitted in the encryption process. This paper also discusses the security aspects of the proposed cipher which is secure against all kinds of attacks.

K. Gupta, S. Silakari, R. Gupta and S. A. Khan, [8] in the development of 3G devices, all element of multimedia (text image audio and video) are used. To use this information, a channel of high bandwidth and more secured system is required. In this era, network security has become an issue of importance, on which lot of research is going on. Authors have proposed image encryption method using elliptic curve cryptography (ECC). RSA is too slow compared to ECC because ECC required smaller key size.

In this method, every pixel of the original image is transformed into the elliptic curve point (Xm,Ym), these elliptic curve point convert into cipher image pixel. The resulting system gives comparatively small block size, high speed and high security.

V. Mehan, R. Dhir and Y. S. Brar, [9] A novel re-watermarking system is proposed for authenticating electronic passport by using Elliptic Curve Cryptography (ECC) applied in dual domain. The scheme splits the cover passport image into twin segments (S). Likewise the passport particulars are fragmented into two parts (P). P_1 statistics are attached with the image data in S_1 to create a multipart message. The message formed is digitally signed using Elliptic Curve Digital Signature Algorithm (ECDSA). The generated signature is inserted spatially by exploiting the Human Visual System (HVS) characteristics of S_1. Implanting signature safeguards passport authentication and shields image veracity. P_2 facts are encoded by means of Advanced Encryption Standard (AES) with key generated over Elliptic Curve Diffie Hellman Protocol (ECDHP). The encoded data is inserted using double Discrete Cosine Transform (DCT). Applying double DCT allows for an extended watermarking implanting capacity. Experimental outcomes ascertain high imperceptibility and true authenticity of passport against any alteration applied to the watermarked image. Smearing re-watermarking order marks for execution of divergent secure algorithms for a successive implanting system.

T. N. Shankar, G. Sahoo and S. Niranjan, [10] Encryption is used to transmit data in open networks with security. Each type of image has its own features, therefore different techniques can be adopted to protect the image from unauthorized access. Most of the available encryption algorithms are mainly used for large devices. There is no such image encryption algorithm with smallest key for smaller devices like cell phone, smart card etc. In this paper, authors introduce an algorithm 'Elliptic Curve Cryptography for Image Encryption'. This algorithm has been applied as an efficient technique to resolve issues involving image encryption. The original image, represented as a set of two dimensional picture elements on a coordinate system can be encrypted using ECC.

Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang and Mengmeng Wang, [11] A new image encryption algorithm based on pixels is proposed in this paper. All the strategies, programs, parameters, encryption and decryption steps and other key technologies are given in detail. First, scrambling the image pixels, then through the method of watermark increasing the difficulty of its decoded. At last, choose a camouflaged image to vision or the pixels of the true image, getting the final encryption image. The key parameters are encrypted by Elliptic Curve Cryptography (ECC). Authors verify and analyze the algorithm security, reliability and efficiency with an experiment. The experiment results and algorithm analyses indicate that the new algorithm possesses a large key space and high level security and the time needed for encrypting the interactive image tends to $+\infty$. It provides a new access to satisfy high level security of interactive information requirements in the fields of aerospace, military, confidential, financial and economic, national security.

III. PROBLEM IDENTIFICATION

Elliptic Curve Cryptography is such an excellent choice for doing asymmetric cryptography in portable, necessarily constrained devices right now, mainly because of the level of security offered for smaller key sizes. A popular, recommended RSA key size for most applications is 2,048 bits. For equivalent security using Elliptic Curve Cryptography, you need a key size of 224 bits. The difference becomes more and more pronounced as security levels increase (and, as a corollary, as hardware gets faster, and the recommended key sizes must be increased). A 384 -bit Elliptic Curve Cryptography key matches a 7680-bit RSA key for security.

IV. CONCLUSION

A Literature review has been exhibit with Elliptic curve cryptography (ECC) that has been introduced as a public-key cryptosystem, which offers smaller key sizes than the other known public-key systems at equivalent security level. The key size advantage of ECC provides faster computations, less memory consumption, less processing power and efficient bandwidth usage. These properties make ECC attractive especially for the next generation public-key cryptosystems. The elliptic curve point multiplication operation, which has a great influence on the performance of ECC protocols.

REFERENCES

[1] N. Gupta, V. Kundu, N. Kurra, S. Sharma and B. Pal, "Elliptic Curve Cryptography for ciphering images," Electrical, Electronics, Signals, Communication and Optimization (EESCO), 2015 International Conference on, Visakhapatnam, 2015, pp. 1-4.

[2] L. Chen, X. Chen and Z. Peng, "A Novel Public Key Encryption Scheme for Large Image," 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, 2014, pp. 955-960.

[3] S. Sowmya and S. V. Sathyanarayana, "Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)," Contemporary Computing and Informatics (IC3I), 2014 International Conference on, Mysore, 2014, pp. 1345-1350.

[4] N. Padmapriya, P. Elamathi and P. Kanimozhi, "Multi image hiding using joint transform digital holography," Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on, Ramanathapuram, 2014, pp. 1497-1501.

[5] Baheti, L. Singh and A. U. Khan, "Proposed Method for Multimedia Data Security Using Cyclic Elliptic Curve, Chaotic System, and Authentication Using Neural Network," Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on, Bhopal, 2014, pp. 664-668.

[6] D. E. M. Ahmed and O. O. Khalifa, "Robust and Secure Image Steganography Based on Elliptic Curve Cryptography," Computer and Communication Engineering (ICCCE), 2014 International Conference on, Kuala Lumpur, 2014, pp. 288-291.

[7] S. Maria Celestin Vigila and K. Muneeswaran, "Elliptic curve based key generation for symmetric encryption," Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on, Thuckafay, 2011, pp. 824-829.

[8] K. Gupta, S. Silakari, R. Gupta and S. A. Khan, "An Ethical Way of Image Encryption Using ECC," Computational Intelligence, Communication Systems and Networks, 2009. CICSYN '09. First International Conference on, Indore, 2009, pp. 342-345.

[9] V. Mehan, R. Dhir and Y. S. Brar, "Secure electronic passport certification using re-water marking," Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), Noida, 2013, pp. 371-375.

[10] T. N. Shankar, G. Sahoo and S. Niranjan, "Image Encryption for mobile devices," Communication Control and Computing Technologies (ICCCCT), 2010 IEEE International Conference on, Ramanathapuram, 2010, pp. 612-616.

[11] Guiliang Zhu, Weiping Wang, Xiaoqiang Zhang and Mengmeng Wang, "Digital image encryption algorithm based on pixels," Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on, Xiamen, 2010, pp. 769-772.