An Approach for Security of Images over Elliptical Curve Cryptography and Digital Signature

Toradmalle Dhanashree
Department of Information Technology
Shah and Anchor Kutchhi Engineering College,
Chembur, India.

Sonigara Varsha Rakesh
UG Student, Information Technology
Shah and Anchor Kutchhi Engineering College,
Chembur, India.

Singh Kiran Premnath
UG Student, Information Technology
Shah and Anchor Kutchhi Engineering College,
Chembur, India.

Kakade Omkar Shashikant
UG Student, Information Technology
Shah and Anchor Kutchhi Engineering College,
Chembur, India.

Panigrahy Krishnachandra Gourishankar
UG Student, Information Technology
Shah and Anchor Kutchhi Engineering College,
Chembur, India.

ABSTRACT
Nowadays, the need of transferring data over a network has increased. Some of these data is confidential and requires to be transferred securely. The type of data can be a Text, Image or any other multimedia. It is essential to provide security to the data that one wants to share over a network. The goals of security are Confidentiality, Integrity and Authentication. Cryptography plays a major role in providing security to the data. Cryptography is the study of techniques for secure communication in the presence of third parties called adversaries. The most popular asymmetric cryptography techniques are RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). RSA is based on Factorization Problem and ECC is based on Elliptic Curve arithmetic and Discrete Logarithm Problem. ECC provides same level of security or comparatively better security with smaller key size (bit lengths) than traditional cryptosystems like RSA, thereby requiring less storage and processing time.

Keywords
Elliptic Curve Cryptography; Image Security

1. INTRODUCTION
The security system that had been in use so far mainly uses cryptographic techniques like RSA, Diffie-Hellman and other asymmetric techniques. But one of the main disadvantages of using RSA is its increase bit length. To overcome this disadvantage of RSA, Elliptical Curve Cryptography (ECC) can be used. Elliptical curve cryptography was introduced by Neal Koblitz and Victor S. Miller [1]. It makes use of the structure of elliptical curves over finite fields. ECC has the advantage of smaller key size over the earlier public key cryptosystems in turn demanding lesser storage requirements. Theoretically the strength of elliptical curves can be attributed to ease of finding a resultant point on the curve by multiplying a given point by random number but deciphering the number even after knowing given and resultant point is a herculean task.

2. REVIEW OF LITERATURE
2.1 Elliptical Curve Cryptography
ECC is an asymmetric key cryptography which requires public key and private key to perform encryption and decryption. It makes use of structure of elliptic curves over finite fields. Many cryptosystems often require use of algebraic groups. Elliptical curve may be used to form elliptical curve groups. A group is set of elements with custom defined arithmetic operation on those elements. For elliptical curve groups, these specific operations are defined geometrically. Computationally intensive hard problems lead to a stronger cryptographic system, which means that elliptic curve cryptosystems are harder to break than RSA and Diffie-Hellman. Although initially these algorithms were not used much but now these algorithms are gaining popularity.

General equation of an elliptic curve is:

$$y2=x3+ax+b \text{ over } R \qquad [1]$$

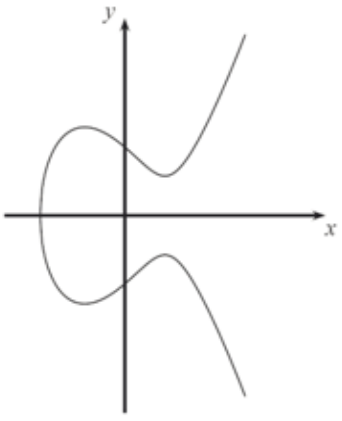

Figure 1: General Elliptic Curve

In Elliptical Curve Cryptography operations are performed on the co-ordinate points of an elliptic curve. Different operations of ECC are as follows:

a)Point Addition: If a line is drawn through points P and Q on the elliptical curve then this line intersects the elliptical curve at a third point R'. The reflection of this point R=P+Q will give a resultant point R' which will be addition of points P and Q.

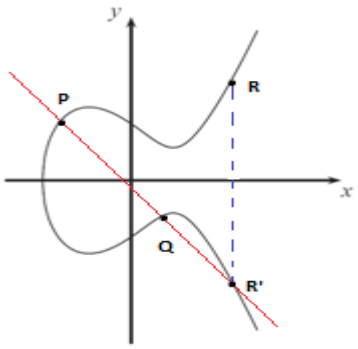

Figure 2: Point Addition

b)Point Doubling: Point doubling is addition of point P on Elliptical curve to itself so as to obtain another point R on the same elliptic curve.

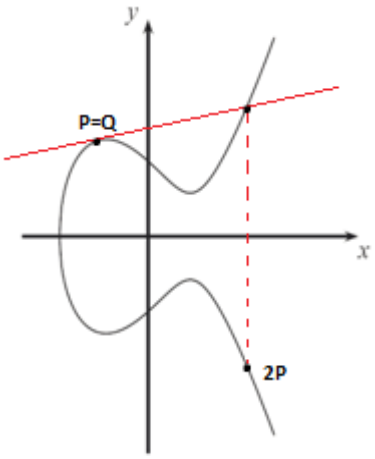

Figure 3 Point Doubling

2.2 Images and Elliptical Curve Cryptography

Images are made up of pixels. To encrypt an image one needs to work on pixel level. In [2], the author uses OpenCV as a matrix container, where the matrix is divided into n parts. The decision of n parts is based on the random number generated. For each of this part, Koblitz encoding [1] is used to generate points on the elliptic curve. For images for larger pixel sizes, this method proved to be very much time consuming and also it requires a static mapping table for decryption part. In [3], the author talks about the pixel grouping method which reduces the number of pixels to be encrypted and solves the static mapping problem. The approach followed used Mathematica [6] tool for pixel grouping operation. This method proved to save the computational time for encryption as compared to traditional method proposed.

2.3 Digital Signature and Elliptical Curve Cryptography

Defining a mathematical scheme, a digital signature is used to demonstrate the authenticity of any digital message. Digital signature provides authenticity to the message which is been sent from authenticated user and the sender can't denied to it, keeping in consideration that the message sent is not been altered throughout the transmission.

Elliptical Curve Digital Signature Algorithm (ECDSA) is a variant of the digital signature algorithm which operates on elliptic curve groups. The elliptic curve variant provides smaller key sizes for the same security levels with the same execution time and signature size is also the same. This traditional ECDSA uses inversion operation for signature signing and verification algorithms. The author in [4] talks about improved versions of Digital Signature Schemes based on ECC. These improvements removed the inversion operations by some modifications in the algorithms, which reduced the time complexity. Also in [5], the author talked about the variants of Digital Signature Algorithm and also compared them.

3. COMPARISION OF ECC WITH OTHER ALGORITHMS

3.1 Key Size

Key size comparison of ECC over other security algorithms is as shown below:

Table 1. Key Comparison [2]

Symmetric Key Size	RSA and Diffi-Hellman Key Size	ECC Key Size
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

3.2 Papers Comparison

The following table below shows the comparison between methods that authors in [2] and [3] used for performing ECC function on the images. The table clearly shows the work done in terms of parameters used, use of digital signature and so on.

Table 2. Paper Comparison

Papers	Static Mapping Table	Standard Used	Parameter Value	Digital Signature	Processed On
Individual pixel mapping [2]	Required	P192,P224, P256,P384, P521 NIST	Parameter are kept confidential	Not applied	Individual pixels
Pixel grouping method [3]	Not required	512 NIST	Parameters values a, b are given	Applied	Group of pixels

4. CONCLUSION

This paper initially focuses on study about individual pixel mapping for ECC encryption and decryption. But the time computation for individual pixel mapping is more, and requires a static pixel mapping table for it. To overcome this

disadvantage pixel grouping operation can be used. The grouping of pixels takes less computational time as compared to individual pixel mapping. The variants of Digital Signature are better in comparison with traditional Digital Signature Algorithm in terms of time complexity. Thus, one can conclude that by using the pixel grouping and DS variants, a better approach for security of images can be achieved. The future scope of improvement can be looking forward to encrypt videos by extracting each frame and encrypting the images simultaneously. Since, videos have sound so encrypting frames and sound simultaneously.

5. REFERENCES

[1] GUIDE TO ELLIPTIC CURVE CRYPTOGRAPHY, Darrel Hankerson, Alfrared Menzes, Scott Vanstone, Springer

[2] ELLIPTIC CURVE CRYPTOGRAPHY FOR CIPHERING IMAGES, Nikita Gupta, Vikas Kundu, Neha Kurra, Shivani Sharma, Bhagyashree Pal, Department of Computer Engineering

[3] IMAGE ENCRYPTION USING ELLIPTIC CURVE CRYPTOGRAPHY, Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Eleventh International Multi-conference Information Processing.

[4] TWO IMPROVEMENTS TO DIGITAL SIGNATURE SCHEME BASED ON ELLIPTIC CURVE CRYPTOSYSTEM, Tao LONG, Xiaoxia LIU School of Information Science and Technology, Northwest University

[5] A SURVEY ON ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM AND ITS VARIENTS, Greeshma Sarath, Devesh C Jinwala and Sankita Patel, Department of Computer Engineering SVNIT, Surat.

[6] https://www.wolfram.com/mathematica