Performance Analysis of Elliptic Curve Cryptosystem Compared to RSA

Muhammad Fareed Uddin[1], Syed Shams-ul-Haq[2]
Karachi, Pakistan

Abstract: *The field of cryptography can broadly be categorized in symmetric cryptography and asymmetric cryptography. RSA, in terms of its adaption and ubiquity, is by far the most popular asymmetric key cryptographic algorithm used now-a-days. The foremost drawback of RSA algorithm is its key size: it must be over 1024-bits (128-bytes) to be considered secure. As a consequence of the large key size, RSA requires more computation resources, space and time. Elliptic Curve Cryptography (ECC) is a promising and emerging asymmetric key cryptosystem for devices with limited amount of processing power, memory and network connectivity. Elliptic Curve Cryptosystem operates over points on an elliptic curve. This paper illustrates the basic operations behind ECC and compares its performance with its counterpart, RSA.*

Keywords: *Elliptic Curve Cryptography, RSA, Fields, Security, Public Key Cryptography*

1. INTRODUCTION

RSA, in terms of its adaption and ubiquity, is by far the most popular asymmetric key cryptographic algorithm used now-a-days. RSA is widely used in network applications, web sites, smart cards and plethora of other areas where security is a major concern. RSA stands for Rivest, Shamir and Adleman, the names of the designers who designed this algorithm. Despite its wide use and high acceptance, the major drawback of RSA algorithm is its key size: it must be over 1024-bits (128-bytes) to be considered secure. As a consequence of the large key size, RSA requires more computation resources, space and time.

As the market trend is moving more towards the use of compact gadgets like personal digital assistants, smart phones and smart cards, the need for a faster and secure cryptographic algorithm is essential. Also, many devices, such as smart cards have built-in cryptographic co-processor hardwired within the device for performing encryption and decryption operations using different industry-standard cryptographic algorithms. The processing power and memory of such devices are limited, and larger key size increases the processing time. Also, some of such devices don't have a direct power connection, and rely on batteries for that purpose. Excessive processing quickly consumes the battery power.

Elliptic Curve Cryptography (ECC) is a promising and emerging asymmetric key cryptosystem for devices with limited amount of processing power, memory and network connectivity. While RSA and other conventional cryptographic algorithms operate on large integer numbers, Elliptic Curve Cryptosystem operates over points on an elliptic curve. This paper illustrates the basic operations behind ECC and explains the ECC's Discrete Log Problem that makes ECC added efficient as well as in some cases, more secure as compared its counterpart RSA.

2. ELLIPTIC CURVE CRYPTOGRAPHY

The major asymmetric key algorithm used today in SSL and digital signatures is RSA, but Elliptic Curve Cryptosystem is rising as a striking alternate. Elliptic Curve Cryptosystem was designed by Miller and Koblitz in the year 1985 and since then, it has evolved into an established public-key technology.

All cryptographic algorithms have a common technique which they imply to secure data: a difficult mathematical problem which is almost impossible to track back and solve without prior knowledge of some secret value. This mathematical technique is used to encrypt and decrypt messages. For instance, in case of RSA, the mathematical problem is factoring large prime numbers. The strength of the cryptographic algorithm relies on the complexity of cracking that mathematical difficulty. The more difficult the problem, the more secure the algorithm.

The best known brute force algorithm to assault ECC runs more slowly that for the RSA, ECC offers almost equal security but with smaller key size. Reduced key size contributes to high performance. A significantly greater security is offered by ECC for a given key size. Implementation on compact and smaller systems, having limited amount of memory and processing power, is also possible and much easier given the smaller key size of ECC for digital signature generation, verification, etc. This implies faster and so-to-speak, more portable operations on smaller devices and less heat generation due to less power consumption.

2.1 Elliptic Curves

The idea from central Elliptic Curve Cryptography is that a rule can be defined as adding two points which get a third point.[9] This rule is the key to perform encryption and decryption operations. This rule of addition confirms to normal properties of addition and addition low form a finite Abelian group. To add two points, an extra point, called the zero point or the infinity, which doesn't fulfill the equation

of the curve, is used and is considered hypothetically to be a point of the arc.
Elliptic curve certainly is not an ellipse, however, it is named elliptic curve because cubic equations, similar to that of ellipse, are used to describe it.

In general, the cubic equations for elliptic curves take the form. [12]

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

Where a and b are elements of a finite field. And the ordered pairs (x,y) is the set of points on the curve. To fully understand who elliptic curves are used to perform encryption/decryption in ECC cryptosystem, we first need to understand the concepts of point addition and point multiplication.

2.2 Point Addition

Point addition is the addition of two points A and B on an elliptic curve to obtain another point C. [13] Suppose there are two points on the curve: $A(X_1,Y_l)$ and $B(X_2,Y_2)$ and if - $X_1 \neq X_2$, (they are not inverse), then, a third point can be obtained by point addition as $C(X_3,Y_3)=A+B$. When $A \neq B$, a line which intersects the elliptic curve at point A and B must also intersect at the third point $-C$. [9][3][4]

2.3 Point Multiplication

In point multiplication, a point A on the elliptic curve is multiplied by scalar k to obtain point B i.e. $kA = B$. Point multiplication is achieved by two basic elliptic curve operations. Below are the two ways in which point multiplication can be done:
1. Piont addition: Adding two points A and B to obtain another point C i.e. $C = A + B$ (as stated above). This technique requires two points.
2. Point doubling: Its obtained by adding a point to itself to obtain a different point B i.e. $B = 2A$. This technique does not require two points as the point is doubled. [13]

3. ELLIPTIC CUVRE DOMAIN PARAMETERS

There are two familiar categories of elliptic curves domain parameters used widely in cryptographic applications: prime curves defined over F_p and binary curves constructed over $F(^{2m})$ [14]

3.1 Elliptic Curve Domain Parameters over Fp

Elliptic curve domain parameters over F_p are:

$$T = (p, a, b, G, n, h) \quad (2)$$

Comprising of p: an integer value which specifies the F_p. Two components a and b belonging to F_p identify an elliptic curve which is defined by the equation:

$$E: y^2 \equiv x^3 + ax + b \ (mod\ p) \quad (3)$$

A base point $G = (x_G;y_G)$ on $E(F_p)$, a prime n which is the order of G, and h: co-factor. The domain parameters specify the base point and the elliptic curve.

3.2 Elliptic Curve Domain Parameters over F2m

Elliptic curve domain parameters over F^{2m} are a septuple:

$$T = (m, (f(x), a, b, G, n, h) \quad (4)$$

Comprising of m that describes the field F^{2m}. $f(x)$: a polynomial having degree m. Elements a and b belonging to $2m$ specifying the $E(F^{2m})$:

$$y^2 + xy = x^3 + ax^2 + b \ in \ F^{2m} \quad (5)$$

A base point $G = (x_G;y_G)$ on $E(F_p)$, a prime n which is the order of G, and h: cofactor. The domain parameters specify the base point and the elliptic curve.

4. ECC ENCRYPTION/DECRYPTION

Elliptic Curve Cryptography is an asymmetric key cryptographic algorithm founded on the structure of the elliptic curves. ECC is not a new cryptographic algorithm; rather it's an implementation of existing algorithms public key algorithms, but using Elliptic Curves. It is understood for ECC that it is infeasible and very difficult to find the discrete logarithm of an elliptic curve element. The level of security provided by ECC is determined by the size of the elliptic curve. Same level of security as that of RSA can be obtained by using smaller groups. Storage, processing, power and transmission requirements are thus reduced by using smaller groups.

As with any cryptosystem, the main object of ECC is to take a plain text message, and convert it into some unreadable form by using cryptographic techniques and a secret key. The first step in the ECC cryptosystem is to encrypt plain message (m) and encode it as point $P_m(x,y)$ so that it is scrambled and is ready to be transmitted over an insecure channel. This point P_m is the cipher text and will be decrypted on the other end of the channel. As part of the key exchange mechanism, this scheme needs G and group $E_q(a,b)$ as input. The secret key comprises of n_A. Public part of the key is $P_A = n_A \times G$. If user A wishes to send an encrypted message P_m to user B, then he selects a random positive number k and generates the cipher message C_m:

$$C_m = \{kG, P_m + kP_B\} \quad (6)$$

Note that A has used B's public key P_B. To retrieve the original message, user B decrypts the cipher text by multiplying the first point in the pair by B's secret key and the result is subtracted from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_B G) - n_B(kG) = P_m \quad (7)$$

The original message P_m has been scrambled by user *A* by the addition of kP_B. Even though P_b of user *B* is declared publically, nobody else can unscramble the mask kP_B from the message except the user *B* himself. [5]

5. TEST SETUP

As mentioned earlier in the paper, the purpose and the main objective of conducting this research was to elucidate whether the ECC cryptosystem is more efficient and better suited for public-key encryption and digital signature generation/verification than the contemporary RSA algorithm. For that purpose, implementation of ECC and RSA was done on Java programming language and test results were extracted using the jProfiler tool.

6. TEST RESULTS

Table 1. RSA Encryption/Decryption Results

RSA Key Size	Encryption (ms)	Decryption (ms)
1024-bit	48.8±2.9	5045.9±5.2
2048-bit	125.0±10.2	6239.1±260.8

Table 2. ECC Encryption/Decryption Results

ECC Key Size	Encryption (ms)	Decryption (ms)
163-bit	4027.4±4.5	1952.8±3.8
193-bit	6705.4±2.1	3301.1±0.3

7. CONCLUSION

The goal of this research study was to elucidate that whether the new ECC cryptosystem provides better encryption/decryption mechanism in terms of speed and memory than the RSA. Key size has been used as a performance criterion to compare the two cryptosystems. The test results clearly show that the ECC outperforms RSA in decryption. From the performance point of view, ECC cryptosystem is quicker than RSA for decryption and digital signing messages.

8. REFERENCES

[1] Vivek Kapoor, Vivek Sonny Abraham and Singh, Elliptic Curve Cryptography Issue 20.

[2] Ganesh Ananthanarayanan, Ramarathnam Venkatesan,Prasad Naldurg, Sean and Adithya Hemakumar, SPACE: Secure Protocol for Address-Book based Connection Establishment, Fifth Workshop on Hot Topics in Networks (HotNets-V) (Nov 29 & 30, 2006, in Irvine, California).

[3] William Stallings, Cryptography and Network Security, Principles and Practices, Third Edition.

[4] Hansmann, Nicklous, Shaeck, Schneider and Seliger, Smartcard Application Development using Java, Second Edition.

[5] Dr.R.Shanmugalakshmi and M.Prabu
Assistant Professor, Department of CSE, Research Issues on Elliptic Curve Cryptography and Its applications, Government College of Technology, Coimbatore, India, Research Scholar, Anna University- Coimbatore, Tamil Nadu, India. VOL.9 No.6, June 2009

[6] Sutikno, Surya, Effendi, "An Implementation of ElGamal Elliptic Curves Cryptosystems",1998.Integrated System Laboratory,Bandung Institute of Technology.

[7] Qiu and Xiong, "Research On Elliptic Curve cryptography" Wuhan University of Technology, 2003.

[8] W. Stallings, "networks security and cryptography,fourth edition,2001

[9] Yacine Rebahi,Jprdi Jaen Pallares,Gergely Kovacs,Dorgham Sisalem "Performance Analysis of Identity management in the session Initiation Protocol"IEEE Journal. 2002.

[10] Elliptic Curve Cryptography, An Implementation Tutorial by Anoop MS, Tata Exlsi Ltd, India

[11] G.J. Simmons - The Science of Information Integrity Contemporary Cryptology, 1992.

[12] Henna Pietilainen, Elliptic Curve Cryptography on Smart Cards, Helsinki University of Technology, Oct 30, 2003.

[13] Kristin Lauter, The advantages of Elliptic Curve Cryptography for Wireless Security.[14] Werner Schindler.