A Study of Elliptic Curve Cryptography and Its Application

M Prabu
Research Scholar
Anna University Coimbatore
Tamil Nadu, India
+91 99422 71899
prabu_pdas@yahoo.co.in

R Shanmugalakshmi
Assistant Professor/CSE
Government College of Technology
Tamil Nadu, India
+91 422 2432221
shanmuga_lakshmi@yahoo.co.in

ABSTRACT
Now a day, there are so many drawbacks in recent encryption techniques respectively. In security, performance in real-time etc., .Many developing cryptography researchers to instigate and to increase the security developments, developed many cryptographic algorithms. Among them, ECC uses smaller key to provide high security and performance in real time as same level to other cryptographic algorithms. In this paper, we have discussed many mathematical performance of ECC, applications of ECC.ECC uses with smaller keys to provide high security and high speed in a low bandwidth.

Categories and Subject Descriptors
C.2.Computer Communication Networks- *Security and protection*

General Terms
Experimentation, Legal Aspects Performance, Security, Standardization.

Key Words
Cryptographic Algorithms, ECC, High Security, High Speed, Low Bandwidth

1. INTRODUCTION
ECC is a kind of public key cryptosystem like RSA. But it differs from RSA in its quicker evolving capacity and by providing attractive and alternative way to researchers of cryptographic algorithm. The security level which is given by RSA can be provided even by smaller keys of ECC. For example, the 1024 bit security strength of RSA could be offered by 163 bit security strength of ECC. Other than this, ECC is particularly well suited for wireless communications, like mobile phones, PDAs, smart cards and sensor networks[9].EC point of multiplication operation is found to be computationally more efficient than RSA exponentiation.

ICWET'10, February 26–27, 2010, Mumbai, Maharashtra, India.

2. AN ELLIPTIC CURVE
Elliptic Curve Cryptography (ECC), which was initially proposed by Victor Miller and Neal Koblitz in 1985, is becoming widely known and accepted. The way that the elliptic curve operations are defined is what gives ECC its higher security at smaller key sizes. [10][11]. The elliptic curve is used to define the members of the set over which the group is calculated, as well as the operations between them which define how math works in the group[6][9].

3. MATHEMATICAL FORMS
The elliptic curve certainly is not in ellipse shape, they are so named because they are described by cubic equations, similar to those used for calculating the circumferences of an ellipse. In general and cubic equations for elliptic curves take the form [9] [12]

$$y^2+axy+by=x^3+cx^2+dx+e$$

Where a, b, c, d and e are real numbers and x and y take on values in the real numbers. An Elliptic curve E is often expressed as the weierstrass equation:

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

Where x, y, a, b $\in F(2^m)$ $b\neq 0$.There are two operations to describe the abelian group

3.1. Point Addition
If $P(X_1,Y_1)$ and $Q(X_2,Y_2)$ are points on the elliptic curve and if $-X_1 \neq X_2$ (equally $P \neq -Q$),then, $R(X_3,Y_3)=P+Q$ can be defined geometrically, in the case of $P\neq Q$, a line intersecting the curve at points P and Q must also intersect the curve at the third point -R, and $R(X_3, Y_3)$ is the answer, if P=Q,the tangent line is used[3][4][9]

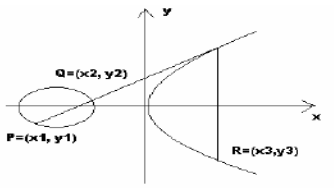

Figure 1 Point Addition

3.2. Scalar Multiplication (Point Multiplication)
Point Multiplication (also called scalar multiplication) is defined by repeated addition. Q=kP=P+P+....+P.(k times addition) Elliptic curve discrete logarithm problem (ECDLP), is based on ECC's security and is described as follows. Given an elliptic and a point on it, to determine k from Q=kP, where Q and P are points on the curve and kP means P added itself k times. It is easy to get Q from k and P, especially for the big numbers. [6][7]

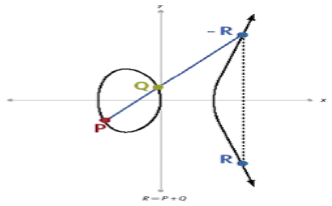

Figure 2.Point Multiplication

Group law for E/F : $y^2 = x^3 + ax + b$,
char(F) $\neq$ 2, 3
Point Addition. Let P = $(x_1, y_1) \in E(F)$ and Q = $(x_2, y_2) \in E(F)$, where $P \neq \pm Q$. Then P + Q = (x_3, y_3), where
$x_3 = ((y_2 - y_1)/(x_2 - x_1))^2 - x_1 - x_2$
and $y_3 = ((y_2 - y_1)/(x_2 - x_1))(x_1 - x_3) - y_1$.
Point Doubling. Let P = $(x_1, y_1) \in E(F)$, where $P \neq -P$. Then 2P = (x_3, y_3), where
$x_3 = ((3x_1^2 + a)/2y_1) - 2x_1$
and $y_3 = ((3x_1^2 + a)/2y_1))(x_1 - x_3) - y_1$[1][9].

Group law for E/F: $y^2 + xy = x^3 + ax^2 + b$,
char(F) = 2
Point Addition. Let P = $(x_1, y_1) \in E(F)$ and Q = $(x_2, y_2) \in E(F)$, where $P \neq \pm Q$. Then P + Q = (x_3, y_3), where $\lambda = (y_1 + y_2)/(x_1 + x_2)$
$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$, and
$y_3 = \lambda(x1 + x3) + x3 + y1$.
Point Doubling. Let P = $(x_1, y_1) \in E(F)$, where $P \neq -P$. Then 2P = (x_3, y_3), where
$x_3 = (x_1 + y_1/x_1)^2 + (x_1 + y_1/x_1) + a$
and $y_3 = x_1^2 + (x_1 + y_1/x_1)\, x_3 + x_3$[1][9.

3.3. Pros of Elliptic Curve Cryptography (ECC)

ECC offers considerably greater security for a given key size. The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software. This means less heat production and less power consumption. There are extremely efficient, compact hardware implementations available for ECC exponentiation operations, offering potential reductions in implementation footprint even beyond those due to the smaller key length alone.

3.4. Performance of ECC

Its inverse operation gets harder, faster, against increasing key length than do the inverse operations in Diffie Hellman and RSA.As security requirements become more stringent, and as processing power gets cheaper and more available, ECC becomes the more practical system for use. And as security requirements become more demanding, and processors become more powerful. This keeps ECC implementations smaller and more efficient than other implementations. ECC can use a considerably shorter key and offer the same level of security as other asymmetric algorithms using much larger ones. Moreover, the gulf between ECC and its competitors in terms of key size required for a given level of security becomes dramatically more pronounced, at higher levels of security.

3.5. Security and Future Enhancement of ECC

First, the fact that the security and practicality of a given asymmetric relies upon the difference in difficulty between cryptosystems

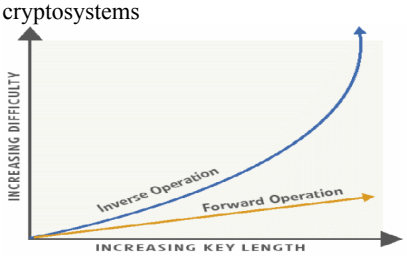

Figure.3.Level of Security

Second, the fact that the difference in difficulty between the forward and the inverse operation in a given system is a function of the key length in use, due to the fact that the difficulty of the forward and the inverse operations increase as very different functions of the key length, the inverse operations get harder faster.
Third, the fact that as you are forced to use longer key lengths to adjust to the greater processing power now available to attack the cryptosystem, even the 'legitimate' forward operations get harder[8][10].

4. COMPARISON

4.1. Key sizes

Comparison between the two asymmetric cryptographic algorithms such as RSA and ECC, same level of security data sizes, encrypted message sizes and computational power. But ECC have smaller keys than other cryptographic algorithms (RSA) [2] [4]. ECC offers equal security for a far smaller key size, there by reducing processing overhead the best known algorithm for solving hard the elliptic curve discrete logarithm problem
(ECDLP).It takes full exponential time.

Table 1. Key sizes for ECC and RSA

ECC Key Size (bits)	RSA Key Size (bits)	Key Size ratio
160	1024	1:6
224	2048	1:9
256	3072	1:12
384	7680	1:20
512	15360	1:30

This means that significantly smaller parameters can be used in ECC than in other systems such as RSA and DSA, but with equivalent levels of security. ECC takes full-exponential time and RSA takes sub-exponential time. For example, RSA with key size of n,1024 bit takes 3*10n MIPS years with best known attack ECC with 160 bit key size takes 9.6*10n MIPS years. ECC offers same level of security with smaller keys. [9]

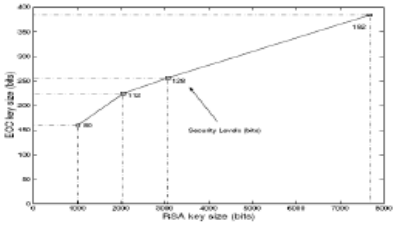

Figure 4.RSA vs. ECC key sizes

5. APPLICATION OF ECC

5.1. Elliptic Curve Digital Signature Algorithm (ECDSA)

In the context of this paper, the Elliptic Curve Cryptography is a means for generating signatures. As a consequence, the Elliptic Curve Digital Signature Algorithm (ECDSA) will be used. First an elliptic curve *E* is defined over GF (p) or GF (2^k) with large group of order *n* and a point *P* of large order is selected and made public to all users[5]. Then, the following key generation primitive is used by each party to generate the individual public and private key pairs. Furthermore, for each transaction the signature and verification primitives are used. We briefly outline the Elliptic Curve Digital Signature Algorithm (ECDSA) below, details of which can be found in [11].

5.1. ECDSA Key Generation

The user *A* follows three steps

1. Select a random integer d Є [2, n − 2]
2. Compute Q = d.P
3. The public and private keys of the user A are (E, P, n, Q) and d, respectively

5.2. ECDSA Signature Generation

The user A signs the message m using three steps:

1. Select a random integer k Є [2, n − 2]
2. Compute k.d = (x1, y1) and r = x1 mod n.

If x1 Є GF (2k), it is assumed that x1 is represented as a binary number.

If r = 0 then go to step 1

3. Compute k−1 mod n
4. Compute s = k−1(H(m) − dr) mod n.

Here H is the secure hash algorithm SHA.

If s = 0, go to step 1.

5. The signature for the message m is the pair of integers(r, s).[12]

5.3. ECDSA Signature Verification

The user B verifies A's signature (r, s) on the message m by applying the following steps:

1. Compute c = s−1 mod n and H(m)
2. Compute u1 = H(m)c mod n and u2 = rc mod n
3. Compute u1.P + u2.Q = (x0, y0) and v = x0 mod n
4. Accept the signature if v = r

6. CONCLUSION

The paper focused mainly on ECC, and mathematical functions and it applications. Group law is also an important law in many other areas of cryptography. It gives a clear view of a comparative study between ECC and RSA. A detailed study of ECDSA is done for our verification. Thus, it is proved that, there is a computational advantage too in using ECC with a shorter key length, comparatively with RSA. The performance, security and future enhancement of ECC is clearly projected.

7. REFERENCES

[1] Abhishek Parakh, "Oblivious Transfer using Elliptic Curves" Department of Electrical and Computer Engineering",2006,ICC.

[2] A.Nithin V.S,Deepthi P.P, Dhanaraj K.J,Sathidevi P.S "Stream ciphers Based on the Elliptic Curves" national Institute of Technolgy,Calicut,ICCIMA 2007

[3]. Eugen Petac "About a method for Distribution keys of a computer netwrok using elliptic curves"Department of mathematics and Computer Science,1997

[4]. Guicheng shen,Xuefeng Zheng, "Research on Implementation of Elliptic Curve Cryptosystem in E-Commerce", International Symposium on Electronic Commerce and Security,2008

[5] G.V.S.Raju and Rehan Akbani,2003, "Elliptic Curve Cryptosystem and its Applications",2003,The University of Texas at san Atonio.

[6] Hans Eberle,Nils Gura,Scheduling Chang-Shantz "A Cryptographic Processor for Arbitary Elliptic Curves Over GF(2^m)",2003 proceedings of the Application-Specific System Architectures, and processors(ASAP'03).

[7] jia Xiangya, Wang Chao. "The Application of Elliptic Curve Cryptosystem in Wireless Communication", 2005 IEEE International Symposium on Microwave, Antenna, Propagation and EMC Technologies for Wireless Communication, 2005

[8] Kristin Lauter,Microsoft Corporation,2004, "The Advantage of Elliptic Curve Cryptography For Wireless Security",IEEE Wireless Communications.

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

[10] Qizhi Qiu and Qianxing Xiong,2003, "Research On Elliptic Curve cryptography"Wuhan University

[11] W.stallings, "Cryptocgraphy and Network Security and,ourth edition,2001

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