Analysis of Elliptic Curve Cryptography

LUCKY GARG, HIMANSHU GUPTA

Abstract: ECC Cryptosystem is an efficient public key cryptosystem which is more suitable for limited environments. The Performance of ECC is depending on a key Size and its operation. The paper represents the comparative study of the entire public key cryptosystem key size i.e. RSA, DSA. In this paper we have explained that the smaller key size is more efficient than the other key size, as it reduces the size of the operation. How Elliptic Curve Arithmetic works with the Curve Equation. This paper also discusses the implementation of ECC.

Keywords: ECC, RSA, DSA, Elliptic Curves, Elliptic Equations

———————————— ◆ ————————————

1. Introduction

Elliptic curve cryptography was come into consideration by Victor Miller and Neal Koblitz in 1985. Elliptic curve cryptography is famous due to the determination that is based on a harder mathematical problem than other Public key Cryptosystems. It is gaining wide acceptance as an alternative to the conventional other public key cryptosystem such as RSA, DSA.

ECC is a discrete Logarithm problem, it offers same level of security as other public key Cryptosystem provides but with more efficient way as well as it reduces the size of operation and their key sizes as it leads to the better performance in limited Environments.
In Elliptic Curve nothing is based upon ellipse, it's all about the plane curve. There doesn't exist any continuous element. These are used to verify the key agreement, signing, digital signatures generation and verification.

Implementation of ECC is defined on mathematical operation over elliptic curves i.e. **y2 = x3 + ax + b** where x is not a continuous element, a and b is a different elliptic curve.

2. Comparison of Public Key Cryptosystem

In RSA and DSA, for authentication it requires both phases as compared above because RSA provides fast verification and DSA provides fast signature.

Table1. Differences between RSA, DSA and ECC

	RSA	DSA	ECC
Invented Year	1977	1991	2004, Elliptic Curves in 1985.
Used for	Public key Encryption and Digital Signature	Digital Signatures only	Digital Signatures and Key Agreement.
Security	Difficulty of Factoring large numbers.	Difficulty of solving certain types of Discrete Logarithm	Size of Elliptic Curves.
Encryption Method	Out of the box	EIGAMEL	Algebraic structure of Elliptic Curve over Finite Fields.
Protocols	SSL and TLS (Secure Socket Layer & Transport Layer Security)	SSH Protocol 2	Elliptic Curve Diffie Hellman (ECDH) Version 1 & 2.
Advantage	Faster in Encryption	Faster in Signature	Faster than RSA in

- *Lucky Garg is currently pursuing Master of Computer Application from Amity University, Noida-201301, India, Ph-No. 8527563240, Email: lckgarg5@gmail.com.*
- *Himanshu Gupta is senior Faculty member in Amity University, Noida-201301, India. Ph-No.9911987390, Email: hgupta5@gmail.com.*

	& validation but slower in Signature & Decryption.	generation & Decryption but slower in verifying, validation & encryption.	Signature & Decryption but slower with DSA in Signature. Faster than DSA in Encryption but slower than RSA.
Function	Faster in Multiple Function	Faster in Single Function	Doesn’t Depend upon Function. It saves memory, energy and bandwidth.

DSA used for authentication only while RSA for authenticate & Encryption of a message. SSH used authentication key, again used together.

3. Elliptic Curve Arithmetic

Point Addition: It is an Addition of two points through Elliptic Curves**,** Consider two Different points i.e. P1 & P2, Draw a Straight Line from P1 to P2, then it will intersect an Elliptic Curve i.e. gives 3rd point and the reflection of the 3rd point on the X-axis is the addition of the two points.

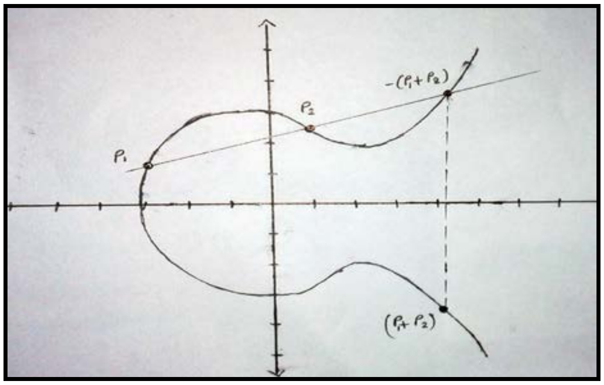

Fig.1 Curve for Point Addition

If ($p1 \neq p2$). Slope of the line at y axis $Y=MX+C$ where $m=Y2-Y1/X2-X1$ then $Y=M(X-X1)+Y1$. Elliptic Curve Equation $Y^2=a^3+AX+B$ putting the value of Y in Equation. $X1+X2+X=M^2 \Rightarrow X=M^2-(X1+X2)$

Point Doubling: If points are equal or same (p1 = p2) then it is called as point Doubling because then the nature of the slope of the line has been changed, for the value of M we have to do the calculation through Differentiation.

$Y^2=X^2+AX+B$ then $2Ydy/dx = 3X^2+A$
$M \neq dy/dx|_{(x1,y1)} = 3X1+A/2Y1$ then $M=3X1+A/2Y1$

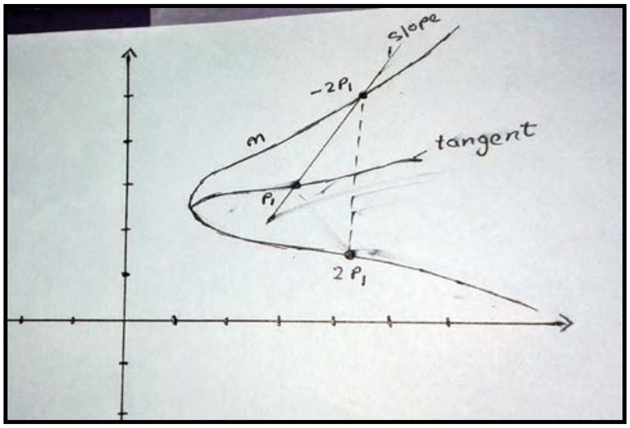

Fig.2 Curve for Point Doubling

Inverse: when point is equivalent to Infinity i.e. p1= ∞ then p1=p1+O = p1, here O is identity.

In any elliptic curve inverse of the point p1 is p1′ and addition of the point p1+O is the reflection of the p1′ i.e. p1.

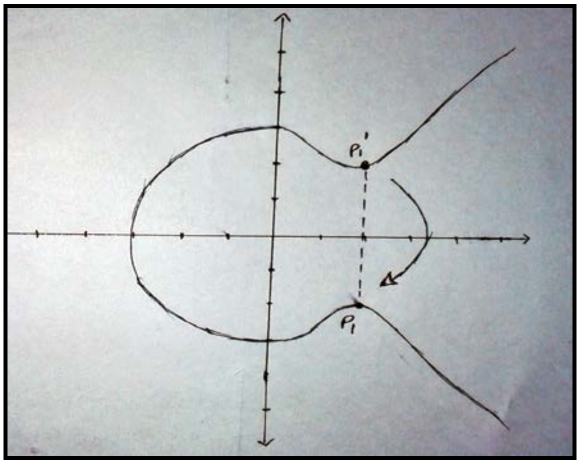

Fig.3. Curve for Inverse

4. Implementation of ECC

Implementation of ECC requires 3 levels to implement in which it has

1. Point Multiplication

2. Group Operation i.e. Point Addition and Doubling
3. Finite Field Arithmetic i.e. Addition , Multiplication, Inverse, Square

For Point Multiplication we have **Scalar Multiplication on the Basis of MSD and LSD**

In **MSD** it has only 1 register that is Q, so, it takes more time, cost and lot of steps required.
$k= (k_{m-1}, k_{m-2,.....} k_0)_2$, $k_m = 1$ where $Q = kP$, $Q = P$ for $i = m - 2$ to 0, $Q = 2Q$

If $K_i = 1$ then $Q = Q + P$. Its sequential Algorithm requires m point doubling & (m-1) / 2 point addition on the average.

Illustration1:
If it is 11P = 11 = (1011) in Binary
Q = P, when its 1 then double + add Q if its 0 then only double the value of Q

It starts from the left side of values.
Q = P , its 1 = P
0 = 2P
1 = 4P + P
1 =2(4p + P) + P

In **LSD** it has 2 Register i.e. Q and R because of two register additions and doubling done simultaneously that require less time, cost and fewer steps incurred.

$k= (k_{m-1}, k_{m-2,.....} k_0)_2$, $Q = kP$ where $Q = 0$ and $R = P$
For $i = 0$ to $m - 1$, If $K_i = 1$ then $Q = Q + R$ and $R = 2R$.

Illustration 2:
11P = 11 = (1011) in Binary
It has 2 Register i.e. Q = 0 and R = P
If it is 1 then Double the Value of R and for Q = Q+R
It start from right most.

So.. values are : 1 = Q = 0 + P = P and R = 2P

1 = Q = 2P + P = 3P and R = 4P
0 = Q = 3P and R = 8P
1 = Q = 3P + 8P = 11P and 16P

For Group Operations i.e. Point Addition and Doubling we have **Weierstrass Point Addition**
$Y^2 +XY = X^3 + AX^2 + B$, (X,Y) i.e. belongs $GF(2^m) * GF (2^m)$
$P = (X_1,Y_1)$ be point on curve, $-P = (X_1,X_1+Y_1)$,
$R = R + Q = (X_3,Y_3)$

X_3 $((Y_1 + Y_2) / (X_1 + X_2))^2 + (Y_1 + Y_2) / (X_1 + X_2) + X_1 + X_2 + A : P \neq Q$
$X_1{}^2+B/X_1{}^2 :P=Q$

Y3 $((Y_1+Y_2)/(X_1+X_2))^2(X_1+X_3)+X_3+Y_1: P \neq Q$
$X_1{}^2+(X_1+Y_1/X_1)X_3+X_3: P=Q$

For Finite Field Arithmetic it has Point Addition and Doubling each **require 1 Inversion and 2 Multiplication**, Neglect the cost of **Squaring and Addition**.

Montgomery's method to perform Scalar Multiplication
$K > 0$, P and $Q = kP$
Set $k < (k_{i-1},...... k_1,k_0)_2$, $P_1= P$,$P_2= 2P$
For i from l - 2 to 0 if $k_i = 1$ then $P_1 = P_1+ P_2$, $P_2 = 2P_2$ else $P_2 = P_2 + P_1$, $P_1 = 2P_1$ THEN $Q = P_1$ i.e. Invariant Property $P = P_2 - P_1$

Illustration 3:
11P =11 = (1011) in Binary
In this, if it is 1 then $P_1 = P_1 + P_2$ and $P_2 = 2P_2$
If it is 0 then $p1 = 2P_1$ and $P_2 = P_1 + P_2$
In Stating it is 1 then $P_1 = P$ and $P_2 = 2P$
$0 = P_1 = 2P$ and $P_2 = 3P$
$1 = P_1 = 5P$ and $P_2= 6P$
$1 = P_1 = 11P$ and $P_2 = 12P$

Algorithm

```
Input : $k > 0 m$ ,  $P = (x,y)$ Output : $Q = kP$
If $k = 0$ or $x = 0$ then Output (0,0)
Set $k = (k_{i-1},k_{i-2},....k_0)_2$ , $x_1 = x$ , $x_2 = x^2 + b / x^2$
For i from I - 2 to 0
    Set $t = x_1 / (x_1+x_2)$
    If $k_i =1$ then $x_1 = x + t^2 + t$ ,  $x_2 = x_2{}^2 + b / x_2{}^2$
    Else $x_2 = x + t^2 + t$ , $x_2 = x_1{}^2 + b / x_1{}^2$
$R_1 = x_1 + x$ ,  $R_2 = x_2 + x$
$Y = R_1(R_1R_2 + X_2 + Y) (X + Y)$
RETURN $Q = (X_1,Y_1)$
```

Motivation is replace inversion by the multiplication operations and then perform one inversion at the end to obtain back the affine coordinates.

In Projective Coordinates
$P_1 = P_2$, $X_3 = X_1{}^4 + B2_1{}^4$, $Z_3 = Z_1{}^2X_1{}^2$
$P_1 \neq P_2$, $Z_3 = (X_1Z_2 + X_2Z_1)^2$
$X_3 = XZ_3 + (X_1Z_2)(X_2Z_1)$

5. Advantage and Disadvantage of ECC

ECC algorithm has various advantages over other existing cryptographic algorithm. These advantages are described below.

1. It has Short Encryption key that value has to be fed from encryption Algorithm and later to be decrypted an encrypted message.
2. It is faster & requires less computation power and less time consuming.
3. It is more important in wireless devices, where computing power, memory and battery life are limited.
4. It increases the size of the encrypted message.

ECC algorithm has some disadvantages also, which can be illustrated as:

1. ECC Algorithm is more complex and more difficult to implement.
2. Due to complexity of the Algorithm, it increases the implementation errors and by that it reduces the security of the Algorithm.

5. Conclusion

Elliptic Curve Cryptography is most secure and powerful Cryptosystem in all Public key Cryptography. ECC is stronger Cryptosystem then other cryptosystem as compared to RSA and DSA.

As ECC require Short key sizes as compared, ECC require only 224 bits where RSA and DSA require 2048 bits, in this paper we have overview about ECC as well as describe the Implementation of ECC, we discussed about its point arithmetic as well as Elliptic Equations, As we mention ECC with Projective Coordinates rather than Affine Coordinates because it is more secure and fast.

REFERENCES

[1] N. Koblitz, Elliptic Curve Cryptosystem, Mathematics of Computation 48 (1987) 203-209.

[2] R.L.Rivest, A.Shamir, L.M.Adleman , A Method for obtaining digital signatures and public key cryptosystem, communications of the ACM 21 (1978) 120-126.

[3] Anoop MS, “Elliptic Curve Cryptography”, available at http://security.ittoolbox.com/research/ elliptic-curve-cryptography, 5 jan 2007.

[4] Koblitz N., Menezes A.J., and Vanstone S.A. The state of elliptic curve cryptography, Design, codes and cryptography, vol 19, issue 2-3, 2000, 173-193.

[5] Tarun Narayan Shankar, G.Sahoo Cryptography with Elliptic Curves in Vol.2, No.1 2-3, 2009.

[6] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithm, IEEE Trans. Inform, theory, IT-31, no.4, pp469-472,july 1985.

[7] Darrel Hankerson, Julio Lopez Hermandez, Software Implementation of Elliptic Curve Cryptography over Binary Fields, 2000.

[8] WWW.stratus.com/blog/openvos/?p=1513.

[9] en.wikipedia.org/wiki/digital-signatures-algorithm.

[10] Arun Kumar, Dr. S.S. Tyagi, Manisha Rana, Neha Agarwal , Pawan Bhadana A comparative Study of Public Key Cryptosystem based on ECC and RSA in Vol.3 No. 5 May 2011.