ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 5, November 2015

Various attacks over the Elliptic Curve-based Cryptosystems

Anurag Singh, Ram Govind Singh
Department of CSE, UIT Allahabad

***Abstract*— The aim of this paper is to survey and determine various types of attacks in the field of elliptic curve cryptography. an overview of different type of attacks on ECC has presented and an analysis of time complexity has been performed.. The efficiency of elliptic curve cryptographic scheme is to find the rational points over the finite field in less time and less effort as compare to RSA cryptographic algorithm. It will also show how computation time will affects on attacks using various techniques.**

***Index Terms*— elliptic curve cryptography, cryptographic attacks, discrete logarithm problem.**

I. INTRODUCTION

In today's world security is very necessary, in which legal transmission of data, integrity, authentication is being so important. One way to secure the transmission is cryptography. Miller and Koblitz[1] has first proposed the concept of Elliptic curve cryptography in 1985.idea of ECC is based on Elliptic Curve Discrete Logarithm Problem(ECCDLP). It is a new concept used for security purpose where complexity and hardness level is similar to algorithm RSA using smaller key size. Let E be an elliptic curve this define over a finite field E_q, with q number of elements. Discrete logarithm problem states that for given P,Q $\in$ $E(F_q)$.Compute an integer number such that Q = zP in the given group $E(F_q)$.Generating and standardizing elliptic curve which can be used for a specific context is a hard task. It has some distrust on these generalise standard curve and give a need to modify it, so that a new general definition of curve can be propose in this paper, we study a set of possible attack that has been arise an general definition of elliptic curve cryptography. We first discuss the methods of attacks and then its complexity

II. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve depends on arithmetic involving the points of the curve. Their operation is crucial to efficiency and performance. Elliptic over finite field is used for secret key exchange and gives equivalent security level as RSA cryptography providing shorter key length. An elliptic curve E over a finite field K is defined by an equation

$$y^2 + a_1xy + a_3y = x^2 + a_2x^2 + a_4x + a$$

Where $a_1, a_2, a_3, a_4, a_6 \in K$, Δ is the discriminant of E, which is define as

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6$$
$$d_2 = a_1^2 + 4a_2$$
$$d_4 = 2a_4 + a_1a_3$$
$$d_6 = a_3^2 + 4a_6$$
$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$

If L is any extension field of K, then the set of L-rational points on E is

$$E(L) = \{(x,y) \in L^*L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\}$$

Where ∞ is the point at infinity.

WEIERSTRASS EQUATIONS

In elliptic curve, the curve of genus having a specified base point. Every such curve is represent as the locus in P^2 of a cubic equation with only one point, the base point, on the line at ∞. The coordinates of X & Y are scaled in elli[tic curve has equation in the form-

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

A. The Group Law in ECC

It starts with two points, or even one point on an elliptic curve, and produces another point itself.

1. Adding Points on a Elliptic Curve

So, the two points are $P_1 = (x_1y_1)$, $P_2 = (x_2,y_2)$ on an elliptic curve E, gives the equation

$y^2 = x^3 + Ax + B$ L is the line drawn through P_1 and P_2, Lintersect E in a third point P_3' across the x-axis to obtain P_3.

$$P_1 + P_2 = P_3$$

Assume that P1 ≠ P and that neither point is ∞. The line L through P_1 & P_2 give slope is

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

If $x_1 = x_2$, the line L is parallel to y-axis.
If $x_1 \neq x_2$, then L is gives: $y = m(x - x_2) + y_1$
To find the intersection with E, we get

$$(m(x-x_1) + y_1)^2 = x^3 + Ax + B$$

***Note-** For the Weierstrass equation, if P=(x,y), then, -p = (x, -y). For the generalized Weierstrass equation, if P =(x,y), then,-P = $(x_1 - a_1x - a_3 - y)$.*

B. An Elliptic Curve over C

If E is define over R, then E(R) is isomorphic in the closed unit circle which is represent as S'. The first case correspond to the cubic polynomial $x^3 + Ax + B$ which has only one real root. The second case, the cubic has three real roots. If the plane passing through the hole of circle in the middle, we obtain curve as equation $y^2 = x^3 - x$. If it does not pass through the hole, the curve has equation $y^2 = x^3 + x$.If P is a point on

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 5, November 2015

elliptic curve and k is belong to positive integer, then kP denotes P + P + --------+ P. If k<0, then kP = (-P) + (-P). To compute kP for a large inter k, it is efficient to add P to itself repeatedly. It is much faster to use successive doubling.

III. ELLIPTIC CURVE BASED CRYPTOSYSTEM

Public key cryptography was invented by Diffie and Hellman, but they were unable to give any practical idea. Practically the public key cryptosystem was proposed by Rivest, Shamir and Aldeman. The RSA cryptosystem based its security on the difficulty of factoring large number. Diffie and Hellman describe the algorithm of key exchange where security lies on the discrete log problem on finite field F_q^*. Kobliz and Miller gives his idea to replace the finite field F_q with elliptic curve E. Its gives larger security using less key size.

Algorithm Family	Crypto system	Security level (Bits)			
		80	128	192	256
Integer factorization	RSA	1024	3072	7680	15360
Discrete logarithm	DH,DSA, Elgamal	1024	3072	7680	15360
Elliptic curve	ECDH, ECDSA	160	256	384	512
Symmetric key	AES, 3DES	80	128	192	256

Table 1: Cryptosystem Algorithms and Their Security Levels

IV. ATTACKS ON DISCRETE LOGARITHM PROBLEM (ECDLP)

The security of Elliptic Curve Cryptography is based on the complexity of solving the elliptic curve discrete log problem. Discrete log problem in the elliptic curve group $E(F_q)$ might be harder to solve than discrete logarithm problem in the multiplicative group F_q^*.The ECDLP is elliptic curve E define over a finite field F_q, point P ϵ $E(F_q)$ of order n, and a point Q ϵ (P), where the integer l ϵ [0,n-1] such that Q = lP. the integer l is called discrete logarithm of Q to the base P, denote l = $\log_p Q$.There is no mathematical proof and does not exit an algorithm to solve the ECDLP. The Pohlig – Hellman and Pollard' rho algorithm and such algorithm, we survey the attempt at devising general purpose sub exponential – time attacks for the ECDLP.

A. Pohlig – Hellman Attack[1,2]

The Pohlig – Hellman algorithm efficiency use to minimise the complexity of discrete logarithm over the prime order subgroup <P>. Computation of ECDLP in its prime order subgroups is harder than ECDLP in <P>. The Pohlig – Hellman attack is use over the elliptic curve so that order n is divisible by large prime (m). Prime factorisation of n is

$n = p_1^{e1}\ p_2^{e2}\ p_3^{e3}$ ---------p_r^{er}

The Pohlig – Hellman equation gives-

$l_i = l \bmod p_i^{ei}$ where $1 \le i \le r$

$l = l_1 \pmod{p_1^{e1}}$

$l = l_2 \pmod{p_1^{e1}}$

$l = l_r \pmod{p_r^{er}}$

Its gives unique solution for $l \in [0,n-1]$. Here , l_i is reduce to the computation of e_i (discrete logarithm).

$l_i = z_0 + z_1p + z_2p^2 +$_____$z_{e-1}p^{e-1}$

where, $z_i \in [o, p-1]$. Now compute $P_0 = \left(\frac{n}{p}\right)^p$ and $Q_0 = \left(\frac{n}{p}\right)^q$ and the order of P_0 is P.

$Q_0 = \frac{n}{p}q = l\left(\frac{n}{p}p\right) = lP_0 = z_0P_0$

Hence, $z_0 = \log_{p_0} Q_0$ obtain by solving ECDLP. We compute

$Q_1 = \left(\frac{n}{p^2}\right)(Q - z_0P)$

$$Q_1 = \frac{n}{p^2}(Q - z_0P) = \frac{n}{p^2}(l - z_0)P = (l - z_0)\left(\frac{n}{p^2}P\right)$$

$$= (z_0 + z_1p - z_0)\left(\frac{n}{p^2}p\right) = z_1\left(\frac{n}{p}P\right) = z_1p_0$$

Hence,

$$z_1 = \log_{p_0} Q_1$$

If digit $z_0, z_1, \dots\dots\dots\dots\dots\dots z_{t-1}$ have been solved then, $z_t = \log_{p_0} Q_t$, where

$$Q_t = \frac{n}{p^{t+1}}(Q - z_0P - z_1pP - z_2p^2P - \cdots - z_{t-1}p^{t-1}P)$$

B. Pollars's Rho Attack[1]

The Pollard'srho is the fastest algorithm used for factoring numbers which like to generate k numbers $x_1 \dots\dots\dots\dots\dots x_k$. The basic idea of Pollard's rho algorithm is to find distinct pair (c', d') and (c'', d'') of integer modulo n such that

$$c'P + d'Q = c''P + d''Q$$

Then, $(c' - c'')P = (d'' - d')Q = (d'' - d')lP$

and so, $(c' - c'') \equiv (d'' - d')l \pmod n$

Hence,

$$l = \log_p Q$$

get by solving

$$l = (c' - c'')(d'' - d')^{-1} \bmod n$$

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 5, Issue 5, November 2015

C. Pollard's Rho Algorithm of ECDLP

INPUT:

$P \in E(F_q)$ of prime order $n, Q \in \langle P \rangle$.

Output: The discrete logarithm $l = \log_P Q$.

1. Select the number L of branches $(eg, L = 12 \text{ or } L = 24).$
2. Select the partition function H: <P> $\rightarrow \{1,2, \dots L\}.$
3. Select j from 1 to L do.
   3.1 . Select $a_j, b_j \in_R [0, n-1]$.
   3.2 . Compute $R_j = a_j P + b_j Q.$
4. Select $c', d' \in_R [0, n-1]$ and compute $X' = c'P + d'Q.$
5. Select $x'' \leftarrow x', c'' \leftarrow c', d'' \leftarrow d'.$
6. Repeate the following.
   6.1 . Set
   $x' \leftarrow x' + R_j, c' \leftarrow c' + a_j \text{mod} n, d \leftarrow d' + b_j \text{mod} n.$
   6.2 . For i from 1 to 2 do
   Complete j = H(x")
   Set
   $x'' \leftarrow x' + R_j, c'' \leftarrow c'' + a_j \text{mod} n, d'' \leftarrow d'' + b_j \text{mod} n.$
   Unit x'=x".
7. If d'-d" then return ("failure");
   Else compute $l = (c' - c'')(d'' - d')^{-1} \text{mod} n$ and return (l)

D. Baby Step, Giant Step [2]

Baby step Giant step algorithm was developed by Dishpans where it gives same complexity in time and storage memory that is $\sqrt{N}$.

This method consists of following steps.

- Take an integer m $\geq \sqrt{N}$ and compute mP where m is constant.
- Store a list of iP for $0 \leq i < m$ (Baby step).
- Compute the Giant step list of points Q-jmP for j=0,1,.....m-1 until we found the one match element from the store list.
- Resolve Q = kP with k $\equiv$ i+jm(mod$N$), if iP = Q – jmP.

E. MOV Attack [3]

The MOV attack is proposed by Menezes, Okamoto, and Vanstone. Here the point given P, xP of an elliptic curve and x is unknown which is belonging to DLP. It uses Weil pairing to convert a DLP in $E(F_q)$ to F^*_{qm}.

$e(PQ)$ and $ex(P,Q) = e(P,Q)^x$ will be computed where its belongs to finite field. P,Q are linearly independent, $e(P,Q)$ cannot be unity by the no degeneracy of the Weil Pairing.

F. The Frey-Rück Attack [7]

Frey and Rück showed that in some situations, the Tale-Lichtenbaum pairing T_n can be use for discrete log problems. Let $E(F_q)$ and P be as in lemma, and suppose Q = kP. Compute $T_\ell(P,Q) = T_\ell(P,P)^k$.

V. CONCLUSION

On the basis of above study, its seems that the elliptic curve cryptography gives highest security using less key size. The current drawback is mention that the implementation of elliptic based cryptosystem is hard to implement which required lots of mathematical theories, and its very hard for attackers to retrieve key in ECC. Now elliptic curve based cryptosystem protocol is required in various applications like in generating public key, ID based cryptosystem, authentication and access database , security in cloud computing, homomorphism encryption or generating smartcards.

REFERENCES

[1] Gabriela Moise "On the attacks over the elliptic curve-based cryptosystem" 2012 third international conference on emerging intelligent data and web technologies.

[2] Guide of elliptic curve cryptography/ Darrel Hankerson, Alfred J. Menezas, Scott Vanstone. p. cm. Springer, 2004

[3] J.H Silverman, The Arithmetic of Elliptic Curve 2nd edition, Graduate Texts in Mathematics. Springle Dordrecht Heidelberg London New York, 2009.

[4] V.S. Miller, "The Weil Pairing, and Its Efficient Calculation", Journal of cryptography.

[5] M. Zandra, "Elliptic Curve Cryptography, Improving the Pollard rho Algorithm.

[6] W. Diffie and M. E. Hellman, "New direction in cryptography", IEEE Transaction on Information Theory.

[7] Elliptic Curve, Number theory and Cryptosystem 2nd edition, Kenneth H. Rosen, Ph.D.