A New Attacking Method to Solve the Discrete Logarithm Problem on Elliptic Curves

Ammar Ali Neamah Alrammahi

Faculty of Mathematics and Computer Science Mathematical Department

Kufa University

[*]*Corresponding author:Ammar22@mu.edu.iq*

Received:3/1/2016, accepted:18/3/2016,published:12/9/2016

Abstract In this paper, we provides two propositions that give a direct computing of the Elliptic Curve Discrete Logarithm problem (ECDLP) and propose a method for the computation of discrete logarithms in the Elliptic Curve (EC) defined over finite fields F_p .This propositions and propose method provides a new approach to the field of attacking methods of the Elliptic Curve Cryptosystems. In addition, we give a program to implement the proposed method by using MATLAB.

Introduction

Several researches were available about ECDLP related to them. For good survey one can turn to[4]. The security of modren public key cryptosystems is based in the difficulty for solving efficiently some kind of mathematical problems. Since the invention of the public key cryptography by Diffie and Hellman in 1976[1], many public key crypto sysytems have been proposed, of these some have been broken and others have been demonstrated to be impractical. Tody, only three type of systems are considered enough secure and efficient. Such systems are based in one of the following mathematical problems:

Integer factorization problem (IFP).

Discrete logarithm problem (DLP).

Elliptic Curve Discrete Logarithm problem (ECDLP).

Although non of these problems have been proved to be intractable, are considered as intractable because years of study has failed to yield efficient algorithms to solve them. The Elliptic Curve Discrete Logarithm problem can be defined as followes: Given an elliptic curve E defined over a finite field F_p, a point P of order n on E, and a point Q a point in the group generated by P, determine the integer k is called the discrete logarithm of Q to the base P, denoted $k = \log_P Q$, between 0 andn–1 such that Q =[k]P, provided that such an integer exists.Based on the statement above we define Qto be the public key and kthe private one.Based on intractabilityof this problem, Neal Koblitz [3] and Victor Miller [5] independently proposed using the group of points on an elliptic curve defined over a finite field to implement the various discrete logarithm cryptosystems. Elliptic curves have been applied to modify public key cryptosystem, such as the DSA [6].

Background on Elliptic Curves

An elliptic curve Eover field F_p is defined by an equation of the form

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

where a, b $\in F_p$, such that $4a^3 + 27b^2 \neq 0$ in F_p. The set E (F_p) consists in all points (x, y) $\in F_p \times F_p$ which satisfy equation (1), together with a special pointO_∞, called the point at the infinity. **E**(F_p) forms an abelian group with the addition operation defined as follow:

$\mathbf{O}_\infty \oplus \mathbf{O}_\infty = \mathbf{O}_\infty$

(x, y) $\oplus \mathbf{O}_\infty$ = (x, y), $\mathbf{O}_\infty$ is the identity

(x, y) $\oplus$(x,– y) = $\mathbf{O}_\infty$. The inverse of one element is obtained changing the sign of the second component.

To add two different elements, which are not one inverse of the other, we apply the following rule :

$(x_1, y_1) \oplus (x_2, y_2) = (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1$

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

To add a point with itself, we apply the rule :

$2(x_1, y_1) = (x_3, y_3)$

$x_3 = \lambda^2 - 2x_1, \qquad y_3 = \lambda(x_1 - x_3) - y_1$

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

The last two operations have a straight geometric interpretation. As shown inFigure(1), if P=(x_1, y_1) and Q=(x_2, y_2) are two distinct points over the elliptic curve, then the sum of P, Q, denoted as R=(x_3, y_3),defined as follows: First draw a line through P and Q. This line intersects the EC at the third point R′. Tacking the reflection of this point about the x-axis. We obtain the point R.

To add a point P =(x_1, y_1) to itself, a tangent line to the curve is drawn at the point P. If $y_1 \neq 0$then the tangent line intersects the curve at a second point, R′. R′ is reflected to the x-axis to R. This operation is called doubling the point P as shown in Figure (2).

If a point P is such that y_1=0, then the tangent line to the EC at P is vertical and does intersect the EC at any other point. By part(5),[2] P=$\boldsymbol{O}_\infty$ for such a point P as shown in Figure (3).

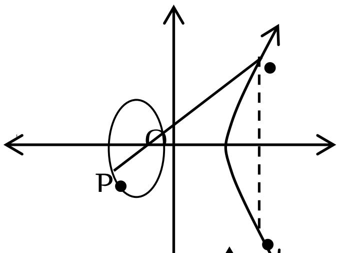

Figure 1: Geometric Addition of Elliptic Curve Points.

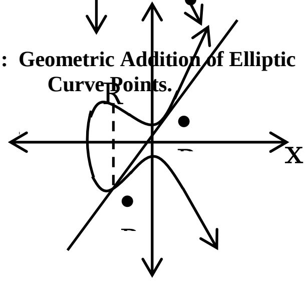

Figure 2: Geometric Doubling of Elliptic Curve Points. when $v_1 \neq 0$.

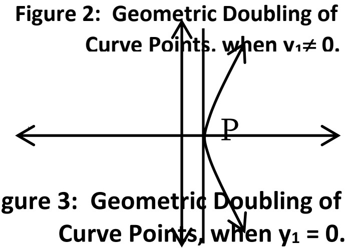

Figure 3: Geometric Doubling of Elliptic Curve Points, when $y_1 = 0$.

If P $\in$ **E** (F_p) then we denoted as [k]P the result of adding k times with himself; $\underbrace{P \oplus P \oplus \cdot\cdot\cdot \oplus P}_{k \text{ times}}$ and the order of P is the smallest positive integer n such that [n]P = O∞. We denote the order of P byord (P) [2].

Inventions for Solving ECDLP

This section provides two proposition that give a direct computing of the ECDLP and anew attacking methodto slove ECDLP.

Proposition (1)

Let **E** be an EC defined over the finite field F_p, and P, Q $\in$**E** (F_p) and **ord** (P)=n, compute R=[A]P $\oplus$ Q where A $\in$[2, n – 1] then

If R=$\boldsymbol{O}_\infty$then $\log_P Q$=(n – A) mod n.

If R=P then $\log_P Q$=(1 – A) mod n.

If R=$\ominus$ P then $\log_P Q$=(–1 – A) mod n.

Proof:

Since R = [A]P $\oplus$ Q then R = [A + k]P and since **ord** (P) = n$\Rightarrow$[n]P = $\boldsymbol{O}_\infty$. So if R = $\boldsymbol{O}_\infty$ then [A + k]P = $\boldsymbol{O}_\infty \Rightarrow$ A + k = n

$\Rightarrow$ A + k = n (mod n)
$\Rightarrow$ k = $\log_P Q$ = (n – A) mod n.

Since R = [A]P ⊕ Q then R = [A + k]P and since**ord** (P)=n$\Rightarrow$[n]P = $\boldsymbol{O}_\infty$. So if R = P then [A + k]P =P$\Rightarrow$ A+k =1
$\Rightarrow$ A + k=1 (mod n)
$\Rightarrow$ k= $\log_P Q$=(1 – A) mod n.

3) Since R = [A]P ⊕ Q then R = [A + k]P and since **ord** (P) = n$\Rightarrow$[n]P = $\boldsymbol{O}_\infty$. So if R=⊖ P then[A+k]P= ⊖ P
$\Rightarrow$ A + k = – 1
$\Rightarrow$ A + k = – 1 (mod n)
$\Rightarrow$ k = $\log_P Q$ = (– 1 – A) mod n.

Example (1)
Consider the elliptic curve E defined over F_{131} by the equation:
E : $y^2 = x^3 + 102\,x + 35$.
Let P = (100, 15) ∈E (F_{131}).We wish to determine the discrete logarithm of point Q = (75, 50) to the base P.

Solution:
The order of P is n = 142.
1) Choose A ∈ [2, n – 1], let A = 93 and then compute Z = [A]P ⊕ Q =[93](100, 15) ⊕ (75, 50)=(75, 81) ⊕ (75, 50) = O_∞, hence by Proposition (1.1) then k≡(n–A) mod n=(142–93) mod142 = 49 mod 142 = 49. Then the discrete logarithm of Q to the base P is 49.

2) Choose A ∈ [2, n – 1], let A=94 and then compute Z=[16]P⊕Q=[94](100,15)⊕ (75,50)=(99,40)⊕ (75,50)=(100,15)=P, hence by Proposition (1.1) then k ≡ (1 – A) mod n = (1–94) mod 142 = – 93 mod 142 = 49. Then the discrete logarithm of Q to the base P is 49.
3) Choose A ∈ [2, n – 1], let A = 92 and then compute Z=[192]P ⊕ Q= [92](100, 15)⊕(75, 50)= (68, 86)⊕ (75, 50) = (100, 116) =⊖P, hence by Proposition (1.3) then k ≡ (– 1 – A) mod n = (– 1 – 92) mod 142 = – 93 mod 142 = 49. Then the discrete logarithm of Q to the base P is 49.

Proposition (2)
Let E be an EC defined over the finite field F_P, and P, Q ∈ E (F_P) and or d (P)= n, compute R=P ⊕ [B]Q where B∈[2, n – 1] then

If R=O∞ and gcd (B, n)=1 then $\log_P Q = \frac{n-1}{B}$ mod n.

If R=Q and gcd (1–B, n)=1 then $\log_P Q = \frac{1}{1-B}$ mod n.

If R=⊖ Q and gcd (–1–B, n)=1 then $\log_P Q = \frac{1}{-1-B}$ mod n.

Proof:
Since R=P⊕[B]Q then R=[1+ B·k]P and since ord (P)=n$\Rightarrow$[n]P=O∞. So if R=O∞ then [1+B · k]P =O∞$\Rightarrow$ 1+B·k=n
$\Rightarrow$ 1+B · k =n (mod n)
$\Rightarrow$ k= $\log_P Q = \frac{n-1}{B}$ mod n.

Since R=P⊕ [B]Q then R=[1 + B·k]P and since ord (P)=n $\Rightarrow$[n]P=O∞. So if R=Q then [1+B · k] P=Q $\Rightarrow$ [1+B · k] P=[k]P
$\Rightarrow$ 1 + B · k = k
$\Rightarrow$ 1 + B · k = k (mod n)
$\Rightarrow$ 1 = k – B · k (mod n)
$\Rightarrow$ 1= k · (1 – B) (mod n)
$\Rightarrow$ k= $\log_P Q = \frac{1}{1-B}$ mod n.
Since R=P ⊕ [B]Q then R=[1+B ·k]P and since or d (P)=n $\Rightarrow$[n]P=O∞. So if R=⊖ Qthen[1+B·k]P=⊖Q$\Rightarrow$[1+B·k]P =⊖[k]P
$\Rightarrow$ 1 + B · k = – k
$\Rightarrow$ 1 + B · k = – k (mod n)
$\Rightarrow$ 1 = – k – B · k (mod n)
$\Rightarrow$ 1 = k · (– 1 – B) (mod n)
$\Rightarrow$ k=$\log_P Q = \frac{1}{-1-B}$ mod n.

Proposed Method

Let $E(F_p)$ be an elliptic curve with generator P. Suppose that P has order n, and let $Q \in E(F_p)$ Suppose that we want find k such that Q=[k]P. Calculate $R=P \oplus Q$. Then calculate [d] Q for $1 \le d \le n-1$ and check these points until found a match with point R. When a match is found we have solved the ECDLP as following:

[d]Q=R hence,

$[d]Q=P \oplus Q$

$[d]Q \ominus Q = P$

$[d-1]Q = P$

$Q = \left[\frac{1}{d-1}\right] P.$

Therefore, if gcd (d–1, n)=1, we get that

$\log_P Q = k = \frac{1}{d-1} \bmod n.$

Example 3

Consider the elliptic curve E defined over F_{641} by the equation:

E :y2 = x3 +3x + 44.

Let P=(401, 245)$\in$E (F_{641}).We wish to determine the discrete logarithm of point Q=(584, 405) to the base P.

Solution:

The order of P is n=647. Firstly calculate $R=P \oplus Q=(401, 245) \oplus (584, 405)=(260, 162)$

Now, calculate [d]Q for$1 \le d \le 647$ until we find a match with point R as following:

[1]Q=[1](584, 405)=(584, 405)

[2]Q=[2](584, 405)=(25, 436)

[3]Q=[3](584, 405)=(180, 240)

[4]Q=[4](584, 405)=(332, 398)

⋮

[163]Q=[163](584,405)=(250, 360)

[164]Q=[164](584, 405)=(260,162)

At this point we have a match. Hence we find that $k \equiv \frac{1}{d-1} \bmod n$

Also, a new proposed method for solving the ECDLP were suggested. It can be considered as a new approach to tackle the problem of attacking the ECDLP. That is provides a reduction to mathematical operations. This leads to main conclusion that the new proposed method is batter than the Exhaustive Search in the reduction cost can be offered for complexity of calculation.

Appendix

The Program for computing the discrete logarithm k of point Q=(x2, y2) to the base P=(x1, y1) from Q=[k]P, where P, Q ∈ E :y2 = x3 + ax + b defined over F_p.

```
% program to find secret key k
p = input ('enter prime no. p =');
a= input('enter integer no.a=');
b = input('enter integer no.b=');
x1 = input ('enter integer no. x1=');
y1 = input ('enter integer no. y1=');
x2 = input ('enter integer no. x2 =');
y2 = input ('enter integer no. y2 =');
m1=mod(y2-y1,p);
m2=mod(x2-x1,p);
for z=1:p-1
w=mod(m2*z,p);
if w==1;[z];
m=mod(m1*z,p);
end,end
xR=mod(m^2-x1-x2,p);
yR=mod(m*(x1-xR)-y1,p);
R=[xR yR];
for k=1:2*p
r=dec2bin(k);
[row,col]=size(r);
xk=x1;
yk=y1;
for i=2:col
m1=mod(3*xk^2+a,p);
m2=mod(2*yk,p);
for z=1:p-1
w=mod(m2*z,p);
if w==1;[z];m=mod(m1*z,p);
end,end
x3=mod(m^2-2*xk,p);
y3=mod(m*(xk-x3)-yk,p);
s=[x3 y3];
xk=s(1);
yk=s(2);
if r(i)==49
m1=mod(yk-y1,p);
m2=mod(xk-x1,p);
for z=1:p-1
```

```
w=mod(m2*z,p);
  if w==1;[z];mm=mod(m1*z,p);
  end,end
 x4=mod(mm^2-x1-xk,p);
y4=mod(mm*(x1-x4)-y1,p);
z=[x4 y4] ;
xk=z(1);
yk=z(2);
  end,end
  if xk==x1 & yk~=y1
n=[k+1];break
  end
R=[xk,yk];
  end
  for d=1:n-1
r=dec2bin(d);
[row,col]=size(r);
xd=x2;
yd=y2;
  for i=2:col
m1=mod(3*xd^2+a,p);
m2=mod(2*yd,p);
  for z=1:p-1
w=mod(m2*z,p);
  if w==1;[z];m=mod(m1*z,p);
  end,end
x3=mod(m^2-2*xd,p);
y3=mod(m*(xd-x3)-yd,p);
s=[x3 y3];
xd=s(1);
 yd=s(2);
  if r(i)==49
m1=mod(yd-y2,p);
 m2=mod(xd-x2,p);
  for z=1:p-1
w=mod(m2*z,p);
  if w==1;[z];mm=mod(m1*z,p);
  end,end
x4=mod(mm^2-x2-xd,p);
y4=mod(mm*(x2-x4)-y2,p);
z=[x4 y4] ;
xd=z(1);
yd=z(2);
  end,end
[xd,yd];
  if [xd,yd]==[xR,yR]
di=d;
  break
  end,end
d; r=d-1;
  for z=1:n-1
w=mod(r*z,n);
  if w==1; [z]; r=1*z; inversrer=r;
  end,end
k = mod (inversrer,n);
secretkey = k
```

Example (2)

Consider the elliptic curve E defined over F_{131} by the equation:

$E:y^2 = x^3 +102\, x + 35.$

Let P=(100,15)$\in$E(F_{131}). We wish to determine the discrete logarithm of point Q=(75, 50) to the base P.

Solution:

The order of P is n=142.

Choose B $\in$[2, n–1], let B =113 and then compute Z=P⊕[B]Q=(100,15)⊕ [113] (75, 50)=(100, 15)⊕(100,116)=O_∞, hence by Proposition (2.1) then k≡$\frac{n-1}{B}$ mod n= $\frac{142-1}{113}$ mod142=$\frac{141}{113}$ mod 142=$141\cdot 113^{-1}$ mod 142=141·93 mod 142=13113 mod 142=49. Then the discrete logarithm of Q to the base P is 49.

Choose B$\in$[2, n –1], let B=114 and then compute Z=P⊕[B]Q=(100,15)⊕[114] (75, 50)=(100, 15)⊕(99, 91)=(75, 50)=Q, hence by Proposition (2.2) then

k ≡$\frac{1}{1-B}$ mod n=$\frac{1}{1-114}$ mod 142=$\frac{1}{-113}$ mod 142 =$\frac{1}{29}$ mod 142=$1\cdot 29^{-1}$ mod 142 =1·49 mod 142=49. Then the discrete logarithm of Q to the base P is 31.

Choose B $\in$[2, n – 1], let B=112 and then compute Z=P⊕[16]Q=(100,15)⊕[112] (75,50)=(100,15)⊕ (68, 86)=(75,81)=⊖ Q, hence by Proposition (2.3) then k≡$\frac{1}{-1-B}$ mod

$n=\dfrac{1}{-1-112}$ mod $142=\dfrac{1}{-113}$ mod $142=\dfrac{1}{29}$ mod $142=1\cdot 29^{-1}$ mod $142=1{\cdot}49$ mod $142=49$. Then the discrete logarithm of Q to the base P is 49.

$=\dfrac{1}{164-1}$ mod $647=\dfrac{1}{163}$ mod $647=$ $(1{\cdot}163^{-1})$ mod 647=(1·389) mod 647=389

Thus $k=\log_P Q=389$.

Algorithm 1

A proposed method algorithm for computing ECDLP.

```
INPUT: a generator P of a cyclic group $E(F_p)$, of order n and an point Q $\in E(F_p)$.
OUTPUT: the discrete logarithm $k=\log_P Q$.
1. Calculate $R=P \oplus Q$.
2. For d from 1 to n–1 do the following :
2.1 If R=[d]Q then do the following:
        Set r =d –1
        If gcd(r , n)=1
k= $r^{-1}$ mod n and return k
```

Conclusions

In this paper, we get two propositions that compute $\log_P Q$ in E over the finite field F_p without method but with some condition. The first proposition that starts with initial point R=[A]P ⊕ Q where A∈[2, n–1] such that discrete logarithm of Q to the base P in E over the finite field F_p as follows:

$$\log_P Q=\begin{cases}(n-A) \bmod n & \text{if } R=O_\infty\\ (1-A) \bmod n & \text{if } R=P\\ (1-A) \bmod n & \text{if } R=\ominus P\end{cases}$$

The second proposition that starts with initial point R=P ⊕ [B]Q where B∈ [2, n–1] such that discrete logarithm of Q to the base P in E over the finite field F_p as follows:

$$\log_P Q=\begin{cases}\dfrac{n-1}{B} \bmod n & \text{if } R=O_\infty\\ \dfrac{1}{1-B} \bmod n & \text{if } R=Q\\ \dfrac{1}{-1-B} \bmod n & \text{if } R=\ominus Q\end{cases}$$

References

[1] W. Diffie and M. Hellman, “New Directions in cryptography”, IEEE Transactions on Information Theory, volume 22, pages 644-654, 1976.

[2] D. Hankerson, A. Menezes, and S. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer Professional Computing, Springer-Verlag, Berlin, 2004.

[3] N. Koblitz, “Elliptic curve cryptosystems”, Mathematics of Computation, 48 (1987), 203-209.

[4] A. Menezes, “Evaluation of Security Level of Cryptography: The Elliptic Curve Discrete Logarithm Problem (ECDLP)”, 2001.

[5] V. Miller, “Uses of elliptic curves in cryptography”, Advances in Cryptology–Crypto ’85,Lecture Notes in Computer Science, 218 (1986), Springer-Verlag, 417-426.

[6] H. C. Williams, “A modification of the RSA public-key encryption procedure”, IEEE Transactions on Information Theory, volume 26, pages 726-729, 1980.