Scribe: Cryptography and Network Security (Lecture 34)

Kuheli Pratihar

11-Nov-2020

1 Elliptic Curve [2]

An Elliptic Curve over a field K is a non-singular cubic curve in two variables, f(x,y) = 0 with a rational point (which maybe a point at infinity). The equation is quadratic w.r.t. y and cubic w.r.t. x

$$y^2 = x^3 + ax + b; (a, b) \in K$$

The field K is usually taken to be the complex numbers, reals, rationals, algebraic extensions of rationals, or a finite field. Elliptic curve groups for cryptography are examined with the underlying fields of F_p (where p¿3 and is a prime) and F_2^m (a binary representation with 2^m elements)

1.1 Elliptic Curve on a Finite Set of Integers

Let us consider an example of an EC over a finite field. $(x, y) \in \mathbb{Z}_5 \times \mathbb{Z}_5$, which means there are 25 possible points. If y = r is a solution then 5-r is also a solution. Consider $y^2 = x^3 + 2x + 3 (mod\, 5)$

$$x = 0 \Rightarrow y^2 = 3 \Rightarrow \text{no solution } (mod\, 5)$$

$$x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow 1, 4 (mod\, 5)$$

$$x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow 0 (mod\, 5)$$

$$x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow 1, 4 (mod\, 5)$$

$$x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow 0 (mod\, 5)$$

Then the points on the elliptic curve are

$$(1, 1); (1, 4); (2, 0); (3, 1); (3, 4); (4, 0) \text{ and the point at infinity}$$

1.2 General from of Elliptic Curve

An elliptic curve over the field K is a plane curve defined by the equation of the form $y^2 = x^3 + ax + b; (a, b) \in K$.

1.2.1 Weierstrass Equation

Generalized Weierstrass Equation of elliptic curve is given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Here x and y are constants which belong to a field of rational numbers, complex numbers, finite field(F_p) or Galois Field ($GF(2^n)$). A two variable equation F(x,y) = 0, forms a curve in the plane and we use geometric arithmetic methods to find the solutions. If the characteristic field is not 2 :

$$(y + \frac{a_1x}{2} + \frac{a_2}{2})^2 = x^3 + (a_2 + \frac{a_1^2}{4})x^2 + a_4x + (\frac{a_3}{4} + a_6)$$
$$\Rightarrow y_1^2 = x^3 + a_2x^2 + a_4x + a_6$$

If the characteristic field is neither 2 or 3 (substituting $x_1 = x + \frac{a_2}{3}$):

$$\Rightarrow y_1^2 = x_1^3 + Ax_1 + B$$

2 Elliptic Curve Properties

2.1 The Abelian Group

Given two points P, Q in $E(F_p)$, there is a third point denoted by $P + Q$ on $E(F_p)$ and the following realtions hold for all P, Q, R in $E(F_p)$.

- $P + Q = Q + P$ (communtativity)
- $(P + Q) + R = P + (Q + R)$ (associativity)
- $(P + 0) = (0 + P) = P$ (existence of identity element)
- There exists $-P$ such that $-P + P = P + (-P) = 0$ (existence of inverse)

For cryptography, the points on the elliptic curve are chosen from a large finite field. The set of points on the elliptic curve form a group under the addition rule. The point at infinity, denoted by O, is the identity element of the group. The operations on the elliptic curve, i.e., the group operations are point addition, point doubling and point inverse.

3 Point Addition and Point Doubling

Let us consider the curve $y^2 = x^3 + Ax + B$
Point Addition: Let P and Q be two points on the curve with coordinates (x_1, y_1) and (x_2, y_2). Also, let $P \neq Q$, then adding the two points result in a third point $R = (P + Q)$. The addition is performed by drawing a line through P and Q as shown in Figure 1(a). The point at which the line intersects the curve is $(P + Q)$. The inverse of this is $R = (P + Q)$. The slope of the line is given by $m = (y_2 - y_1)/(x_2 - x_1)$. Let the coordinates of R be (x_3, y_3), then the equations for x_3 and y_3 is given by

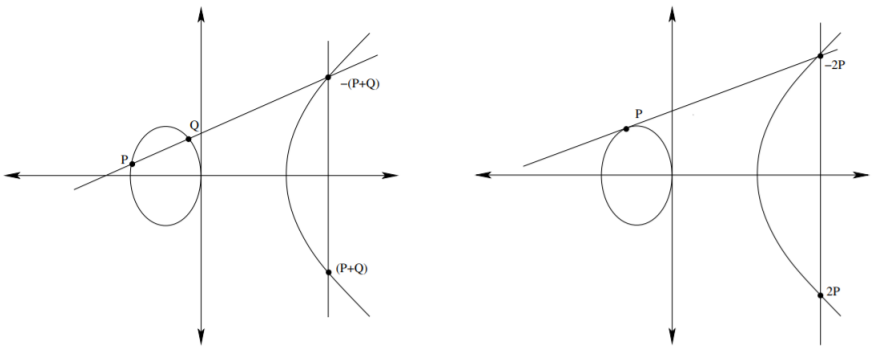

Figure 1: Point Addition (a) and Point Doubling (b)[1]

$$\begin{aligned} \Rightarrow (m(x - x_1) + y_1)^2 &= x^3 + Ax + B \\ \Rightarrow 0 &= x^3 + m^2x^2 + \cdots \\ \Rightarrow x_3 &= m^2 - x_1 - x_2 \\ \Rightarrow y_3 &= m(x_1 - x_2) - y_1 \end{aligned}$$

Point Doubling: Let P be a point on the curve with coordinates (x_1, y_1) and $P \neq P$. The double of P is the point $2P = (x_3, y_3)$ obtained by drawing a tangent to the curve through P. The inverse of the point at which the tangent intersects the curve is the double of P shown in Figure 1(b). The slope of the tangent is found using the derivative of the ellipse curve.

$$2y\frac{dy}{dx} = 3x^2 + A \Rightarrow m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

If $y_1 \neq 0$ (since $P_1 + P_2 = \infty$)

$$\begin{aligned} \therefore 0 &= x^3 - m^2x^2 + \cdots \\ \Rightarrow x_3 &= m^2 - 2x_1 \\ \Rightarrow y_3 &= m(x_1 - x_3) - y_1 \end{aligned}$$

4 Algorithm for Scalar Multiplication

The fundamental algorithm for ECC is the scalar multiplication, which can be obtained using the basic double and add computations as shown in the Algorithm in Figure 2. The input to the algorithm is a basepoint P and a m bit scalar k. The result is the scalar product kP, which is equivalent to adding the point P k times.

Algorithm : Double and Add algorithm for scalar multiplication

Input: Basepoint $P = (x, y)$ and Scalar $k = (k_{m-1}, k_{m-2} \cdots k_0)_2$, where $k_{m-1} = 1$
Output: Point on the curve $Q = kP$

```
1 Q = P
2 for i = m − 2 to 0 do
3     Q = 2 · Q
4     if k_i = 1 then
5         Q = Q + P
6     end
7 end
8 return Q
```

Figure 2: Algorithm for ECC Scalar Multiplication [1]

5 Conclusion

In this lecture, we successfully covered the Elliptic Curves, Elliptic Curve on a finite set of integers, Weierstrass Equation, the Abelian Group, Point Addition and Point Doubling along with the algorithm for Elliptic Curve Scalar Multiplication. **Note:** No homework questions were provided in the class.

References

[1] Rajat Subhra Chakraborty Debdeep Mukhopadhyay. *Hardware Security, Design, Threats & Safeguards, Chapter 2*. CRC Press, 2014.

[2] Douglas Robert Stinson and Maura Paterson. *Cryptography: theory and practice*. CRC press, 2018.