**Lecture 6: An Elliptic Curves over F2***m*

**LEARNING OUTCOME**

**By the end of the lesson the student will be able to:**

1. understand a concept of irreducible polynomial in an Elliptic Curves over F2*m*.
2. compute a double point along an elliptic curve over F2*m*.
3. compute a point addition along an elliptic curve over F2*m*.

The field **F2*m***, for instance *m*=256, called a characteristic two finite field or a binary finite field, can be viewed as a vector space of dimension *m* over the field **F2*m*** which consists of the two elements 0 and 1. In this lecture, we take an easy case *m* = 8. An Elliptic Curve Cryptosystem over finite field **F2*m*** is the preferred ECC due to its efficient computation without any carry.

An elliptic curve E over F[2*m*] is given by

*y*2 + *xy* = *x*3 + *ax*2 +*b* modulo *M*(*t*).

1. Choose the base point P1(*x*1, *y*1).
2. **Double Point**

From a basic Point, compute P2(*x*2, *y*2) = 2 ⊗ P1(*x*1, *y*1)

Let us choose an irreducible polynomial 283 =256 +16+8+2+1 =*M*(*t*) = *t*8 + *t*4 +*t*3 + *t* +1.

Let (*x*1, *y*1) be a point on an elliptic curve E(F2*m*), and (*x*1, *y*1) ≠ (*x*2, –*y*2)

then let (*x*2, *y*2) = 2 ⊗ (*x*1, *y*1) such that



1. **Add Point**

Compute P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2)

Let (*x*1, *y*1) and (*x*2, *y*2) are two points on an elliptic curve E(Fp), and

(*x*1, *y*1) ≠ (*x*2, ± *y*2)

then let (*x*3, *y*3) = (*x*1, *y*1) ⊕ (*x*2, *y*2) such that



Let the slope

of the line connecting (*x*1, *y*1) and (*x*2, *y*2)

then

*x*3 = *m*2 + *m* – (*x*1 + *x*2) + *a* and *y*3 = *m*⋅(*x*1 – *x*3 ) – ( *x*3 + *y*1.)

**Tutorial 6a**: Let us take *x*1=2, *y*1=100+*i*, where *i* is the last 2 digits of your matrix number. Take *a*=3, compute *b*. We will always compute in a ring modulo *m*=283.

Step 1: Double point

Step 2: Add point

Note: Refer to an inverse table modulo *m*(*x*).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *a*-1 |  | **0** |  | **1** |  | **2** |  | **3** |  | **4** |  | **5** |  | **6** |  | **7** |  | **8** |  | **9** |  | **A** |  | **B** |  | **C** |  | **D** |  | **E** |  | **F** |
| **0** | 0 | 0 | 0 | 1 | 8 | D | F | 6 | C | B | 5 | 2 | 7 | B | D | 1 | E | 8 | 4 | F | 2 | 9 | C | 0 | B | 0 | E | 1 | E | 5 | C | 7 |
| **1** | 7 | 4 | B | 4 | A | A | 4 | B | 9 | 9 | 2 | B | 6 | 0 | 5 | F | 5 | 8 | 3 | F | F | D | C | C | F | F | 4 | 0 | E | E | B | 2 |
| **2** | 3 | A | 6 | E | 5 | A | F | 1 | 5 | 5 | 4 | D | A | 8 | C | 9 | C | 1 | 0 | A | 9 | 8 | 1 | 5 | 3 | 0 | 4 | 4 | A | 2 | C | 2 |
| **3** | 2 | C | 4 | 5 | 9 | 2 | 6 | C | F | 3 | 3 | 9 | 6 | 6 | 4 | 2 | F | 2 | 3 | 5 | 2 | 0 | 6 | F | 7 | 7 | B | B | 5 | 9 | 1 | 9 |
| **4** | 1 | D | F | E | 3 | 7 | 6 | 7 | 2 | D | 3 | 1 | F | 5 | 6 | 9 | A | 7 | 6 | 4 | A | B | 1 | 3 | 5 | 4 | 2 | 5 | E | 9 | 0 | 9 |
| **5** | E | D | 5 | C | 0 | 5 | C | A | 4 | C | 2 | 4 | 8 | 7 | B | F | 1 | 8 | 3 | E | 2 | 2 | F | 0 | 5 | 1 | E | C | 6 | 1 | 1 | 7 |
| **6** | 1 | 6 | 5 | E | A | F | D | 3 | 4 | 9 | A | 6 | 3 | 6 | 4 | 3 | F | 4 | 4 | 7 | 9 | 1 | D | F | 3 | 3 | 9 | 3 | 2 | 1 | 3 | B |
| **7** | 7 | 9 | B | 7 | 9 | 7 | 8 | 5 | 1 | 0 | B | 5 | B | A | 3 | C | B | 6 | 7 | 0 | D | 0 | 0 | 6 | A | 1 | F | A | 8 | 1 | 8 | 2 |
| **8** | 8 | 3 | 7 | E | 7 | F | 8 | 0 | 9 | 6 | 7 | 3 | B | E | 5 | 6 | 9 | B | 9 | E | 9 | 5 | D | 9 | F | 7 | 0 | 2 | B | 9 | A | 4 |
| **9** | D | E | 6 | A | 3 | 2 | 6 | D | D | 8 | 8 | A | 8 | 4 | 7 | 2 | 2 | A | 1 | 4 | 9 | F | 8 | 8 | F | 9 | D | C | 8 | 9 | 9 | A |
| **A** | F | B | 7 | C | 2 | E | C | 3 | 8 | F | B | 8 | 6 | 5 | 4 | 8 | 2 | 6 | C | 8 | 1 | 2 | 4 | A | C | E | E | 7 | D | 2 | 6 | 2 |
| **B** | 0 | C | E | 0 | 1 | F | E | F | 1 | 1 | 7 | 5 | 7 | 8 | 7 | 1 | A | 5 | 8 | E | 7 | 6 | 3 | D | B | D | B | C | 8 | 6 | 5 | 7 |
| **C** | 0 | B | 2 | 8 | 2 | F | A | 3 | D | A | D | 4 | E | 4 | 0 | F | A | 9 | 2 | 7 | 5 | 3 | 0 | 4 | 1 | B | F | C | A | C | E | 6 |
| **D** | 7 | A | 0 | 7 | A | E | 6 | 3 | C | 5 | D | B | E | 2 | E | A | 9 | 4 | 8 | B | C | 4 | D | 5 | 9 | D | F | 8 | 9 | 0 | 6 | B |
| **E** | B | 1 | 0 | D | D | 6 | E | B | C | 6 | 0 | E | C | F | A | D | 0 | 8 | 4 | E | D | 7 | E | 3 | 5 | D | 5 | 0 | 1 | E | B | 3 |
| **F** | 5 | B | 2 | 3 | 3 | 8 | 3 | 4 | 6 | 8 | 4 | 6 | 0 | 3 | 8 | C | D | D | 9 | C | 7 | D | A | 0 | C | D | 1 | A | 4 | 1 | 1 | C |

Table 3.2 An inverse table of *a*(*x*) mod *m*(*x*) = *x*8+*x*4+*x*3+*x*+1.

Sample Case:

*y*2 + *xy* = *x*3 + *ax*2 + *b*, take *a*=3, *b*=254.

Let us see a graph of an elliptic curve looks like. Next let us draw *y*2 + *xy* = *x*3 + *ax*2 +*b*,

Figure 1. An elliptic curve of *y*2 + *xy* = *x*3 + 3*x*2 + 254*.*

Let us take another example:

Step 0: Choose a simple base point on the curve,

*y*2 + *xy* ≡ *x*3 + *ax*2 +*b* modulo *M*(*t*).

Preferably, we choose a base point without modulo *M*.

Let us take *x*1=2, *y*1=200. Take *a*=3, compute *b*. We will always compute in a ring modulo *m*=283.

From the LHS, *y*1 = 200 = 110010002 = C816.

*y*12 = 11001000⋅11001000

11001000

11001000

11001000000

= 101000001000000

100011011

= 1011010000000

100011011

= 11100110000

100011011

= 1101011100

100011011

= 101101010

100011011

= 1110001= 7116.

*y*2 + *xy* = *x*3 + *ax*2 +*b* modulo *M*(*t*).

Next we need to compute *xy* = 10⋅110010002.

= 110010000.

100011011

= 10001011 = 8B16.

We move to the RHS, we need to compute *x*3,

*x*2 = 10⋅10

100 = 416.

*x*3 = *x* ⋅ *x*2

10⋅100

= 1000 = 816.

Let us move on to *ax*2  = 11⋅100

= 100

100

= 1100 = C16.

Finally, we can compute *b*, from *y*2 + *xy* = *x*3 + *ax*2 +*b*,

*b* = *y*2 + *xy* − (*x*3 + *ax*2 )

= 1110001+10001011-(1000+1100)

= 1110001

10001011

1000

1100

= 11111110 = FE16.

Let us move to Double Point operation on P1(*x*1, *y*1) = (2, 200)

**Double Point**

From a basic Point, compute P2(*x*2, *y*2) = 2 ⊗ P1(*x*1, *y*1)

Let (*x*1, *y*1) be a point on an elliptic curve E(F2*m*), and (*x*1, *y*1) ≠ (*x*2, –*y*2)

then let (*x*2, *y*2) = 2 ⊗ (*x*1, *y*1) such that



From *x*12 = 410 = 0416, we can look up an inverse table mod 283,

*x*1−2 = CB = 11001011

we can compute *b*⋅ *x*1−2 = FE⋅CB = 11111110⋅11001011

= CB⋅FE

= 11001011⋅11111110

= 11111110

11111110

11111110

11111110

11111110

= 100011001110010

100011011

= 10110010 = B2

Now we can compute *x*2 = *x*12 + *b* ⋅ *x*1−2 = 04 +B2

= 100 + 10110010

= 10110010

100

= 10110110 = B6.

Let us move to the right *y*1 ⋅ *x*1−1 = C8⋅8D

= 11001000⋅10001101

= 10001101

10001101

10001101000

= 110000110101000

100011011

= 10011101101000

100011011

= 10000001000

100011011

= 1100100 = 6416.

From the RHS, 1 + *x*1 + *y*1 ⋅ *x*1−1 = 1 + 10 + 1100100

= 1100100

10

1

= 1100111 = 6716.

Now, we take (1 + *x*1 + *y*1 ⋅ *x*1−1)⋅*x*2 = 67⋅B6.

=1100111⋅10110110

=10110110

10110110

10110110

10110110

10110110

=11100001000010

100011011

= 1101100100010

100011011

= 101010010010

100011011

= 1001001010

100011011

= 1111100 = 7C.

Finally,

*y*2 = *x*12 + (1 + *x*1 + *y*1 ⋅ *x*1−1)⋅*x*2

= 04 + 7C

= 1111100

+ 100

= 1111000 = 7816.

Let us move on to a Point Addition (02, C8) + (B6, 78)

Compute P3(*x*3, *y*3) = P1(*x*1, *y*1) ⊕ P2(*x*2, *y*2)

Let (*x*1, *y*1) and (*x*2, *y*2) are two points on an elliptic curve E(F2*n*), and

(*x*1, *y*1) ≠ (*x*2, ± *y*2)

then let (*x*3, *y*3) = (*x*1, *y*1) ⊕ (*x*2, *y*2) such that



Let the slope

of the line connecting (*x*1, *y*1) and (*x*2, *y*2)

then

*x*3 = *m*2 + *m* – (*x*1 + *x*2) + *a* and *y*3 = *m*(*x*1 – *x*3 ) –( *x*3 + *y*1.)

Adding Point P1(02, C8) + P2(B6, 78)

Take a denominator *x*2 − *x*1 = B6 – 02,

= 10110110

10

= 10110100 = B4

Based on an inverse table, we look up for an inverse of B4, we get 1116.

Take a numerator *y*2 − *y*1 = 78 – C8

= 1111000

11001000

=10110000 = B0

Take a slope between two points P1 and P2, *m* = (*y*2 − *y*1)⋅( *x*2 − *x*1)−1

= 10110000⋅10001

= 10001⋅10110000

= 10110000

10110000

= 101110110000

100011011

= 1101101000

100011011

= 101011110

100011011

= 1000101 = 45.

On the LHS, *x*3 = *m*2 + *m* – (*x*1 + *x*2) + *a*, we start from computing

*m*2 = 1000101⋅1000101

= 1000101

1000101 1000101

= 1000000010001

100011011

= 110100001

100011011

= 10111010 = BA.

Now we are ready to compute *x*3 = *m*2 + *m* – (*x*1 + *x*2) + *a*,

= BA + 45 – B4 + 03

=10111010

1000101

10110100

11

= 1001000 = 48.

Since *y*3 = *m*(*x*1 – *x*3) – (*x*3 + *y*1), First let us compute,

(*x*1 – *x*3) = 02 – 48

= 1001000

10

= 1001010 = 4A.

*m*(*x*1 – *x*3) = 45⋅4A

=1000101⋅1001010

=1001010

1001010

1001010

=1001111100010

100011011

= 1001010010

100011011

= 1100100 = 6416.

We are ready to compute *y*3 = *m*(*x*1 – *x*3) – (*x*3 + *y*1),

= 64 – (48 + C8)

= 1100100

+ 1001000

+ 11001000

= 11100100 = E416.

A sample answer is in this case P2(B616, 7816) = 2⊗P1(0216, C816)

and P3(4816, E416) = P1(0216, C816) ⊕ P2(B6, 78).