6. Sonlu Cisimler Üzerindeki Eliptik Eğriler

6.1. Eliptik Diskrete Logaritma Problemi

Tanım 6.1.1.

$q = p^r$, p asal ve $r \in \mathbb{Z}^+$ olacak şekilde $\mathbb{F}_q$ sonlu bir cisim olsun. $p > 3$ olmak üzere $a, b \in \mathbb{F}_q$, $\Delta(f) \not\equiv 0 \pmod{p}$ ise

$$y^2 \equiv (x^3 + ax + b) \pmod{p}$$

kongrüansının $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ çözümleri ve sonsuzdaki noktanın oluşturduğu kümeye $\mathbb{F}_q$ üzerindeki eliptik eğri denir ve $E(\mathbb{F}_q)$ ile gösterilir.

Şimdi, $E(\mathbb{F}_q)$ üzerinde bir toplama işlemi tanımlayalım.

$P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ eliptik eğri üzerindeki herhangi iki nokta olsun:

(1) Eğer $y_1 \equiv 0 \pmod{p}$ ise $P := -P$ ve $P + P := \vartheta$

(2) Eğer $x_2 \equiv x_1 \pmod{p}$ ve $y_2 \equiv -y_1 \pmod{p}$ ise $P + Q := \vartheta$

(3) Diğer durumlarda, $P + Q = (x_3, y_3)$ olsun.

Eğer $P = Q$ ise

$$m := (y_2 - y_1)(x_2 - x_1)^{-1} \pmod{p}$$

aksi halde;

$$m := (3x_1^2 + a)(2y_1)^{-1} \pmod{p}$$

olmak üzere

$$x_3 := (m^2 - x_1 - x_2) \pmod{p} \qquad \text{ve} \qquad y_3 := (m(x_1 - x_3) - y_1) \pmod{p} \text{ dir.}$$

$E(\mathbb{F}_q)$ kümesi tanımlanan toplama işlemi altında değişmeli bir gruptur. $E(\mathbb{F}_q)$ sonlu bir cisim üzerinde tanımlı olduğundan $E(\mathbb{F}_q)$ üzerinde sonlu sayıda nokta bulunur. Kriptografi için gerekli bir özellik grubun sonlu sayıda eleman içermesidir.

$|E(\mathbb{F}_q)|$ üzerindeki nokta sayısını göstersin. Eliptik eğri $\mathbb{F}_q$ üzerinde olduğundan eliptik eğri üzerindeki noktaların x koordinatları q tane olası değer alabilir. Her bir x koordinatına karşılık y koordinatı iki farklı değer alabilir. Yani, eliptik eğri üzerindeki (x, y) noktaları sayısı en fazla $2q$ tanedir. Sonsuzdaki noktayla birlikte $|E(\mathbb{F}_q)|$ için bir üst sınır $2q + 1$ dir.

$r = 1$ için $E(\mathbb{F}_q) = E(\mathbb{Z}_p)$ dir. Şimdi, $E(\mathbb{Z}_p)$ eliptik eğrisi üzerindeki nokta sayısını Legendre sembolünü kullanarak hesaplayan bir formül verelim. Eliptik eğrinin denklemini $y^2 = f(x)$ şeklinde gösterelim. mod p kalan sistemindeki herhangi bir x_0 için:

Eğer $\left(\dfrac{f(x_0)}{p}\right) = 1$ ise $y^2 \equiv f(x) \pmod{p}$ kongrüansının bir y_0 çözümü vardır. Yani, (x_0, y_0) ve $(x_0, -y_0)$ noktaları eliptik eğri üzerindedir.

Eğer $\left(\dfrac{f(x_0)}{p}\right) = -1$ ise eliptik eğri üzerinde x koordinatı x_0 olan bir nokta yoktur.

Eğer $\left(\dfrac{f(x_0)}{p}\right) = 0$ ise $p \mid f(x_0)$ dır. Bu durumda $(x_0, 0)$ eliptik eğri üzerinde bir noktadır. Bu üç durumu birleştirirsek, eliptik eğri üzerinde x koordinatı x_0 olan nokta sayısı :

$$1 + \left(\frac{f(x_0)}{p}\right) \text{ dir.}$$

Sonuç olarak, sonsuzdaki noktayla birlikte $\mathbb{Z}_p$ üzerindeki nokta sayısı :

$$|E(\mathbb{Z}_p)| = 1 \ + \sum_{x=0}^{p-1}(1 + \left(\tfrac{f(x)}{p}\right)) = p + 1 \ + \sum_{x=0}^{p-1}\left(\tfrac{f(x)}{p}\right) \quad \text{dir.}$$

$E(\mathbb{Z}_p)$ sonlu bir grup olduğundan grup teorideki bir çok sonuç $E(\mathbb{Z}_p)$ için kullanılabilir. Mesela, $E(\mathbb{Z}_p)$ üzerindeki her P noktası için $|E(\mathbb{Z}_p)|\, P = \vartheta$ dır. $r \neq 1$ için de $E\left(\mathbb{F}_q\right)$ eliptik eğrisinde de nokta sayısını hesaplamak mümkündür.

Örnek 6.1.1 $E(\mathbb{Z}_p)$ eliptik eğrisinin denklemi $y^2 = x^3 + 1$ olsun. $p = 5$ asalı için $|E(\mathbb{Z}_p)| = 6$ dir. $P = (2, 3)$ noktası E_p üzerindedir. P noktasının katlarını hesaplayalım :

$P = (2, 3) \qquad 2P = (0, 1) \qquad 3P = (4, 0)$

$4P = (0, -1) \quad 5P = (2, -3) \quad 6P = \vartheta$

E_p nin tüm noktalarını P noktasınının katlarıyla hesapladık. Yani, P noktası E_p nin bir üretecidir ve E_p devirli bir gruptur.

Tanım 6.1.2. P, $E(\mathbb{F}_q)$ üzerinde mertebesi n olan bir nokta ve $Q \in E(\mathbb{F}_q)$ olsun. P,Q ve $E(\mathbb{F}_q)$ bilinirken $Q = lP$ ifadesinden $0 \leqslant l \leqslant n-1$ olacak şekildeki l sayısını (varsa) hesaplama problemine *eliptik eğri diskrete logaritma problemi* denir ve ECDLP ile gösterilir.

ECDLP nin çarpanlara ayırma problemi ve DLP den daha zor bir problem olduğu kabul edilmektedir. Genel olarak, bu üç problem için de yapılan algoritmalar tamamen üstel zamanlı algoritmalardır. Fakat, bazı özel durumlarda DLP ve çarpanlara ayırma problemi için etkili algoritmalar mevcuttur. Eliptik eğrilerin küçük bir sınıfı olan supersingular eliptik eğriler için de etkili algoritmalar mevcuttur fakat eliptik eğrinin supersingular olup olmadığını kontrol etmek kolaydır.

$\mathbb{F}_q$, eliptik eğrinin üzerinde tanımlı olduğu sonlu cisim olsun. En çok bilinen supersingular eğriler,

$$char(\mathbb{F}_q) = p \equiv 3 \pmod 4 \text{ olmak üzere } y^2 = x^3 + ax$$

veya

$$char(\mathbb{F}_q) = p \equiv 2 \pmod 3 \text{ olmak üzere } y^2 = x^3 + b$$

formundadır.

Not : Eliptik eğrilerin büyük çoğunluğu supersingular değildir.

ECDLP ye dayanan kripto sistemleri kırmak diğer açık anahtar kripto sistemleri kırmaktan daha çok zaman alır. Dolayısıyla, eliptik eğri kripto sistemlerin en önemli özelliği RSA ve DLP ye dayalı kripto sistemlere göre daha küçük anahtar uzunluğu ile aynı güvenliğin sağlanabilmesidir.

6.2. Algoritmalar

Bu bölümde, $E(\mathbb{Z}_p)$ üzerinde skaler çarpma, toplama, rasgele bir nokta bulma ve $\bmod p$ de karakök bulma gibi faydalı algoritmalar verilecek. Aşağıdaki algoritmalar $(y^2 \equiv x^3 + ax + b) \pmod p$ denklemli $E(\mathbb{Z}_p)$ eliptik eğrisi içindir ($p > 3$ ve p asal).

Algoritma 6.2.1 (Toplama)

Bu algoritma, $E(\mathbb{Z}_p)$ eliptik eğrisi üzerinde verilen $P = (x_1, y_1)$ ve $Q = (x_2, y_2)$ noktalarının toplamını hesaplar. P ve Q noktalarının toplamını $R := (x_3, y_3)$ olarak gösterelim.

1. Eğer $P = \vartheta$ ise $R := Q$ ve Bitir.

2. Eğer $Q = \vartheta$ ise $R := P$ ve Bitir.

3. Eğer $x_1 \neq x_2$ ise

a) $m := (y_1 - y_2)(x_1 - x_2)^{-1} \pmod p$

b) Git adım 7

4. Eğer $y_1 \neq y_2$ ise $R := \vartheta$ ve Bitir.

5. Eğer $y_1 = 0$ ise $R := \vartheta$ ve Bitir.

6. $m := (3x_2^2 + a)(2y_2)^{-1} \pmod p$

7. $x_3 := m^2 - x_1 - x_2 \pmod p$

8. $y_3 := (x_2 - x_3)m - y_1 \pmod p$

9. $R := (x_3, y_3)$

10. Bitir.

Adım 3.a ve 6. da Euclidean algoritması kullanarak $\bmod p$ de ters alma işlemi makul bir zamanda hesaplanabilir (Bakınız Bölüm 3).

Algoritma 6.2.2 (Skaler Çarpma)

Bu algoritma verilen bir n tamsayısı ve eliptik eğri üzerindeki bir P_1 noktası için $S := nP_1$ yi hesaplar. $P_1 := (x, y)$ olsun.

1. $P_2 := \vartheta$

2. Eğer $n = 0$ ise $S := P_2$ ve Bitir.

3. Eğer $n \pmod 2 = 1$ ise $P_2 := P_2 + P_1$, $n := n - 1$ ve Git Adım 2

4. Eğer $n \pmod 2 = 0$ ise $P_1 = 2P_1$, $n = n/2$ ve Git Adım 2

Adım 3. ve 4. de Algoritma-1 kullanılarak toplama işlemi yapılır.

Algoritma 6.2.3 (Eliptik Eğri Üzerinde Rasgele bir Nokta Bulma)

Sonsuzdaki noktadan farklı rasgele bulunacak noktayı P ile gösterelim.

1. $0 \leqslant x < p$ olacak şekilde rasgele bir x seç
2. $\tau := x^3 + ax + b \,(\mathrm{mod}\, p)$
3. Eğer $\tau = 0$ ise $P := (x, 0)$ ve Bitir.
4. Algoritma 6.2.4 ü kullanarak varsa τ nun $\mathrm{mod}\, p$ deki karekökünü bul
5. Eğer Adım 4. te karekök yoksa Git Adım 1, aksi halde $\sigma^2 := \tau \,(\mathrm{mod}\, p)$
6. Rasgele bir β biti üret (0 veya 1) ve $y := (-1)^{\beta}\sigma$
7. $P := (x, y)$
8. Bitir.

Algoritma 6.2.4 ($\mathrm{mod}\, p$ de Karekök Bulma)

Bu algoritma, $0 < g < p$ olacak şekilde verilen bir g tamsayısının $\mathrm{mod}\, p$ de varsa karekökünü bulur. Eğer g tamsayısının varsa $\mathrm{mod}\, p$ deki karekökünü z ile gösterelim.

1. Eğer $p \equiv 3 \,(\mathrm{mod}\, 4)$ ise

a) $k := (p-3)/4$

b) $z := g^{k+1} \,(\mathrm{mod}\, p)$ ve Bitir.

2. Eğer $p \equiv 5 \,(\mathrm{mod}\, 8)$ ise

a) $k := (p-5)/8$

b) $\gamma := (2g)^k \pmod p$

c) $i := 2g\gamma^2 \pmod p$

d) $z := g\gamma(i-1) \pmod p$ ve Bitir.

3. Eğer $p \equiv 1 \pmod 4$ ise

a) $k := (p-1)/4$

b) $Q := g$

c) $0 < P < p$ olacak şekilde rasgele bir P sayısı üret

d) Lucas dizisinin elemanlarını hesapla (Tanım 6.2.1.).

$$U := U_{2k+1} \pmod p \ , \ V := V_{2k+1} \pmod p$$

e) Eğer $U = 0$ ise $z := V/2 \pmod p$ ve Bitir.

f) Eğer $V = 0$ ise Yaz " Karekök yok " ve Bitir.

g) Git Adım 3.c

Tanım 6.2.1. P ve Q sıfırdan farklı tamsayılar olsun. P ve Q için Lucas dizileri U_k ve V_k ,

$$U_0 := 0,\ U_1 := 1 \text{ ve } \forall k \geqslant 2 \text{ için } U_k := PU_{k-1} - QU_{k-2}$$
$$V_0 := 2,\ V_1 := P \text{ ve } \forall k \geqslant 2 \text{ için } V_k := PV_{k-1} - QV_{k-2}$$

olarak tanımlanır.

6.3. Açık Yazıyı Eliptik Eğri Noktalarına Gömme

Bu bölümde, açık yazıyı $E(\mathbb{F}_q)$ eliptik eğrisi üzerindeki noktalar olarak kodlayan bir algoritma verilecek. m açık yazısı $0 \leqslant m \leqslant M$ olacak şekilde kodlanmış bir tamsayı olsun (M, açık yazı için üst sınırı gösteren tamsayı). Algoritma, m açık yazısına karşılık gelen eliptik eğri üzerindeki P_m noktasını ve P_m noktasından da m açık yazısını kolayca hesaplayabilmelidir. k , $30 \leqslant k \leqslant 50$ olacak şekilde bir tamsayı olsun. Burada incelenecek olan algortimanın başarısızlık olasılığı $\frac{1}{2^k}$ dır. $\mathbb{F}_q$ cismi ($q = p^r$, p asal, $p > 3$) $q > Mk$ olacak şekilde seçilsin. 1 ile Mk arasındaki tamsayıları $mk + j$, $1 \leqslant j \leqslant k$ formunda yazabiliriz. Bu tamsayılarla $\mathbb{F}_q$ cisminin bir alt kümesi arasında 1-1 ve örten bir eşleme yapabiliriz.

Bir m açık yazısından eliptik eğri üzerindeki P_m noktası şu şekilde bulunur :

$j = 1, 2, ..30$ değerleri için

$mk + j$ tamsayısına karşılık gelen $\alpha \in \mathbb{F}_q$ elemanı bulunur. $y^2 = x^3 + ax + b$ denklemli $E(\mathbb{F}_q)$ eliptik eğrisinde x yerine α yazılırsa $y^2 = f(\alpha)$ elde edilir. Algoritma 6.2.4 kullanılarak varsa y koordinatı bulunur. Böylece m noktasına

karşılık gelen $P_m := (x, y)$ noktası hesaplanmış olur. $y^2 = f(\alpha)$ kareköke sahip değilse bir sonraki j değeri için aynı işlemler yapılır.

Not : $j > k$ olduğunda P_m noktası bulunabilir fakat m açık yazısını P_m noktasından elde edemeyiz.

Şimdi, m açık yazısını P_m noktasından elde edelim.

$\overline{x}$, P_m noktasının x koordinatı olmak üzere eliptik eğri üzerindeki P_m noktasından

$$m = \left\lfloor \frac{\overline{x}-1}{k} \right\rfloor$$

formülü kullanılarak m açık yazısı kolayca hesaplanabilir.

Örnek 6.3.1. $p = 4177$ ve $E(\mathbb{Z}_p)$ eliptik eğrisinin denklemi $y^2 = x^3 + 3x$ olsun. $k = 30$ olarak seçilsin. $m = 2174$ açık yazısının P_m karşılığını bulalım. Pratikte $p > 30m$ seçilmelidir.

$A := \{30 \times 2174 + j : j = 1, 2, ..30\}$ ve $\alpha \in A$ olsun. α, $y^2 = \alpha^3 + 3\alpha$ ifadesinin $\bmod p$ de y çözümü bulununcaya kadar j nin artan değerleri için hesaplanır.

$j = 15$ olduğunda,

$$\begin{aligned}
\alpha &= 30 \times 2174 + 15 \\
&= 65235 \\
\alpha^3 + 3\alpha &= (30 \times 2174 + 15)^3 + 3 \times (30 \times 2174 + 15) \\
&= 277614407048580 \\
&\equiv 1444 \,(\bmod 4177) \\
&\equiv 38^2
\end{aligned}$$

$m = 2174$ açık yazısı için eliptik eğri üzerinde $P_m = (65235, 38)$ noktası karşılık gelir.

Tersine, P_m noktasından m açık yazısı

$$m = \left\lfloor \frac{65235}{30} \right\rfloor = \lfloor 2174.5 \rfloor = 2174$$

olarak elde edilir.