7. Eliptik Eğri Kripto Sistemler

7.1. Eliptik Eğri ElGamal Kripto Sistemi (ECELG)

$E(\mathbb{F}_q)$, $\mathbb{F}_q$ cismi üzerinde tanımlı eliptik eğri olsun. H, $\alpha \in E(\mathbb{F}_q)$ noktası tarafından üretilen $E(\mathbb{F}_q)$ eliptik eğrisinin bir alt grubu olsun öyle ki H alt grubunda ECDLP makul zamanda hesaplanamasın. α noktasına kripto sistemin taban noktası denir.

$\mathcal{P} := E(\mathbb{F}_q)$, $\mathcal{C} := E(\mathbb{F}_q) \times E(\mathbb{F}_q)$, $\mathcal{K} := \{(E(\mathbb{F}_q), \alpha, a, \beta) : \beta = a\alpha\}$

olarak tanımlansın öyle ki α ve β herkes tarafından bilinirken a gizlidir.

$K = (E(\mathbb{F}_q), \alpha, a, \beta)$ ve rasgele seçilen $k \in \mathbb{Z}_{|H|}$ için kapama fonksiyonu (k gizli) :

$$y_1 := k\alpha \quad \text{ve} \quad y_2 := x + k\beta \quad \text{olmak üzere}$$

$$e_K(x, k) := (y_1, y_2) \qquad \text{dir.}$$

$y = (y_1, y_2)$ için açma fonksiyonu :

$$d_K(y) := y_2 - ay_1 \text{ dir.}$$

B şahsının yukarıdaki işlemleri yapıp bir a sayısı seçtiğini ve gizli tutuğunu düşünelim.

A şahsı, B şahsına bir x açık yazısını göndermek için öncelikle rasgele bir k sayısı seçer. α ve β herkes tarafından bilindiğinden $y_1 := k\alpha$ ve $y_2 := x + k\beta$ ifadelerini hesaplar ve sonra $y = (y_1, y_2)$ kapalı yazısını B şahsına gönderir.

B şahsı kendisine gelen y kapalı yazısına açma fonksiyonunu uygularsa :

$$\begin{aligned} d_K(y) &= y_2 - ay_1 \\ &= (x + k\beta) - a(k\alpha) \\ &= (x + k(a\alpha) - a(k\alpha)) \\ &= x \end{aligned}$$

x açık yazısını elde eder. B şahsı a sayısını gizli tuttuğundan x açık yazısını sadece kendisi hesaplayabilir. α ve β bilinirken $\beta = a\alpha$ ifadesinden a sayısını hesaplamak bir ECDLP dir. Sonuç olarak, eliptik eğri ElGamal kripto sistemi ECDLP ye dayanır. Eliptik eğri ve taban noktası güvenlik için ECDLP nin makul bir zamanda hesaplanamayacağı şekilde uygun seçilmelidir.

Örnek 7.1.1. $p = 11$ olmak üzere $E(\mathbb{Z}_{11})$ eliptik eğrisinin denklemi $y^2 = x^3 + x + 6$ olsun. Bölüm 5.5 den $|E(\mathbb{Z}_{11})| = 13$ dür. 13 asal sayı olduğundan $E(\mathbb{Z}_{11})$ devirli bir gruptur. Yani, sonsuzdaki nokta hariç eliptik eğri üzerindeki her nokta bir üreteçtir. Taban noktası olarak $\alpha = (2, 7)$ seçilmiş olsun.

B şahsı $a = 7$ gizli sayısını seçmiş ise

$$\begin{aligned} \beta &= 7\alpha \\ &= (7, 2) \text{ dir.} \end{aligned}$$

α ve β herkes tarafından bilinirken, a sayısını yalnızca B şahsı bilir.

A şahsı, B şahsına $x = (10, 9)$ açık yazısını göndermek istesin. A şahsı rasgele $k = 3$ sayısını seçmiş olsun. α ve β herkes tarafından bilindiğinden, $y_1 = 3(2, 7) = (8, 3)$ ve $y_2 = (10, 9) + 3(7, 2) = (10, 2)$ ifadelerini kapama fonksiyonunu kullanarak hesaplar ve $y = (y_1, y_2)$ kapalı yazısını B şahsına gönderir.

B şahsı kendisine gelen $y = (y_1, y_2)$ kapalı yazısına açma fonksiyonunu uygularsa,

$$\begin{aligned} d_k(y_1, y_2) &= y_2 - 7y_1 \\ x &= (10, 2) - 7(8, 3) \\ &= (10, 2) - (3, 5) \\ &= (10, 2) + (3, 6) \\ &= (10, 9) \end{aligned}$$

x açık yazısını elde etmiş olur.

7.2. Eliptik Eğri Diffie-Hellman Anahtar Alış Verişi (ECDH)

A ve B şahısları aralarında gizli bir anahtar belirlemek istesinler. A ve B şahısları öncelikle bir p asalı ve $q = p^r$ olacak şekilde $\mathbb{F}_q$ cismi, $\mathbb{F}_q$ cismi üzerinde tanımlı $E(\mathbb{F}_q)$ eliptik eğrisi ve rasgele bir $\alpha \in E(\mathbb{F}_q)$ taban noktası belirlerler (α Algoritma 6.2.3 kullanılarak belirlenebilir).

Not : α noktası Diffie-hellman anahtar alış verişindeki g noktasına karşılık gelir. α, $E(\mathbb{F}_q)$ eliptik eğrisinin üreteci olmak zorunda değildir. Fakat, güvenlik için α tarafından üretilen alt grupda ECDLP nin makul bir zamanda hesaplanamaması gerekir.

A şahsı rasgele bir a tamsayısı seçip, $a\alpha$ noktasını hesaplar ve B şahsına gönderir. Aynı şekilde B şahsı da bir b tamsayısı seçip, $b\alpha$ noktasını hesaplar ve A şahsına gönderir. A şahsı $b\alpha$ ve gizli tuttuğu a sayısından $P = ab\alpha$ noktasını hesaplar. B şahsı da $a\alpha$ ve b den $P = ab\alpha$ noktasını hesaplar. Sonuç olarak A ve B şahsı P gizli anahtarını belirlemiş olurlar.

Bir başka şahsın P yi bulabilmesi için a ve b sayılarını hesaplaması gerekir. Fakat, $\alpha, a\alpha$ ve $b\alpha$ bilinirken a veya b tamsayılarının hesaplanması ECDLP dir. Yani, sistemin güvenliği ECDLP ye dayanır.

7.3. Eliptik Eğri ve Taban Noktasının Seçilişi

$char\,(\mathbb{F}_q) > 3$ olsun. T taban noktasını göstersin. $\mathbb{F}_q$ üzerinde tanımlı olan E eliptik eğrisinin denkleminin $y^2 = x^3 + ax + b$ olduğunu biliyoruz.

(a) (E, T) nin rasgele seçilişi

İlk olarak q büyük olacak şekilde bir $\mathbb{F}_q$ sonlu cismi seçilir. $\mathbb{F}_q$ cisminden rasgele $\overline{x}, \overline{y}$ ve a elemanları seçilir ve $b := \overline{y}^2 - (\overline{x}^3 + a\overline{x})$ olarak tanımlanır.

Eğer $4a^3 + 27b^2 \neq 0$ ise $T := (\overline{x}, \overline{y})$ yi taban noktası ve E eliptik eğrisinin denklemini

$y^2 = x^3 + ax + b$ olarak tanımlayalım. Böylece (E, T) rasgele belirlenmiş olur. $4a^3 + 27b^2 = 0$ durumunda ise $\mathbb{F}_q$ cisminden yeniden üç eleman seçilir ve işlemler tekrar edilir.

ECDH ve ECELG için $|E|$ yi bilmeye gerek yoktur. Fakat, taban noktasının oluşturduğu alt grubun yeterli güvenliği sağlayabildiğinden emin olmak için $|E|$ nin bilinmesi faydalıdır. Güvenlik için $|E|$ yeterince büyük bir asal bölene sahip olmalıdır. Eğer $|E|$ küçük asal bölenlere sahipse PSH (Pohlig, Silver ve Hellman) algoritması ECDLP yi makul bir zamanda çözebilir. PSH algoritması DLP için tanımlanmış bir algoritma olmasına rağmen ECDLP ye de uyarlanabilir. DLP yi

hesaplayan bir başka algoritma index-calculus algoritması ise ECDLP ye uyarlanamamaktadır. Bundan dolayı ECDLP nin DLP den daha zor bir problem olduğu söylenebilir.

(b) (E, T) **nin global seçilişi**

E, $\mathbb{Q}$ cismi üzerinde tanımlanmış bir eliptik eğri ve T, E üzerinde sonsuz mertebeli bir nokta olsun. Öncelikle büyük bir p asalı seçilir ve sonra E eliptik eğrisinin katsayılarını $\bmod p$ ye indirgeyerek $\mathbb{F}_p$ sonlu cismi üzerinde $y^2 = x^3 + ax + b$ denklemli bir eliptik eğri bulunur (p asalı büyük olduğundan $\mathbb{F}_p$ üzerinde doğru bir eliptik eğri elde ederiz). $\mathbb{F}_p$ sonlu cismi üzerinde elde edilen $y^2 = x^3 + ax + b$ denklemli eliptik eğri bir kaç küçük p asalı haricinde $\Delta(f) \neq 0$ dır. $\mathbb{F}_p$ üzerindeki eliptik eğrinin taban noktasını da elde etmek için T noktası $\bmod p$ ye indirgenir. E ve T sabit tutulup farklı p değerleri için farklı eliptik eğri ve taban noktaları elde edilebilir.

(c) T **noktasının mertebesi**

ECDH ve ECELG sistemlerinin güvenliği için taban noktası tarafından üretilen alt grupta ECDLP probleminin makul bir zamanda hesaplanamaması gerekiyordu. Eğer T noktasının mertebesinin büyük bir asal böleni (yaklaşık olarak $|E|$ büyüklüğünde) varsa ECDLP problemi T tarafından üretilen alt grupta makul bir zamanda hesaplanamaz. Böyle bir nokta elde etmenin bir yolu seçilecek olan E eliptik eğrisinin eleman sayısının asal olmasıdır. Bu durumda, sonsuzdaki nokta hariç E üzerindeki her nokta bir üreteçtir. Yani, eliptik eğri üzerinde herhangi

bir noktanın mertebesi $|E|$ dir. Böylece, herhangi bir nokta taban noktası olarak seçilebilir.

$|E|$ asal oluncaya kadar **(a)** ve **(b)** metotları uygulanıp E eliptik eğrisi ve T taban noktası seçilebilir. Fakat bu işlemin ne kadar zaman aldığı hala tam olarak cevaplanmış değildir.