ESKİŞEHİR
ANADOLU ÜNİVERSİTESİ

BİLECİK
ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Ana Bilim Dalı

ELİPTİK EĞRİLERİN FARKLI MODELLERİ ÜZERİNE

Bayram YAŞAR
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2019
Ref.No: 10309582

ESKİŞEHİR
ANADOLU ÜNİVERSİTESİ

BİLECİK
ŞEYH EDEBALİ ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü
Matematik Ana Bilim Dalı

ELİPTİK EĞRİLERİN FARKLI MODELLERİ ÜZERİNE

Bayram YAŞAR
Yüksek Lisans

Tez Danışmanı
Doç. Dr. İlker İNAM

BİLECİK, 2019

ESKISEHIR
ANADOLU UNİVERSİTY

BILECIK
SEYH EDEBALI UNİVERSİTY

Graduate School of Sciences
Department of Mathematics

ON DIFFERENT MODELS OF ELLIPTIC CURVES

Bayram YAŞAR
Master's Thesis

Thesis Advisor
Assoc. Prof. Dr. Ilker INAM

BILECIK, 2019

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

BİLECİK ŞEYH EDEBALİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS

JÜRİ ONAY FORMU

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun 05.11.2019 tarih ve 67-2 sayılı kararıyla oluşturulan jüri tarafından 20.11.2019 tarihinde tez savunma sınavı yapılan Bayram Yaşar'ın "Eliptik Eğrilerin Farklı Modelleri Üzerine" başlıklı tez çalışması Matematik Anabilim Dalında YÜKSEK LİSANS tezi olarak oy birliği/ ~~oy çokluğu~~ ile kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) : Doç. Dr. İlker İNAM

ÜYE : Prof. Dr. Nülifer ÖZDEMİR

ÜYE : Dr. Öğr. Üyesi Bilal DEMİR

ONAY

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulunun …./…./…..... tarih ve ……/…… sayılı kararı.

İMZA/ MÜHÜR

TEŞEKKÜR

Bu çalışmanın yürütülmesi sırasında desteğini esirgemeyen danışmanım Doç.Dr.İlker İnam'a, yoğun çalışmalarım sırasında sabır gösterdiği ve bana katlandığı için biricik eşim Sebahat'e, motivasyon desteği ve ümit verici konuşmaları ile beni rahatlatan annem, babam, kardeşlerim ve sevgili zümrem Mustafa Dinç'e, yazım sırasında ve oluşan aksaklıklarda destek veren ve işleri yoluna koymaya gayret gösteren Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü personeline ve çalışmam sırasında küçük veya büyük yardımını esirgemeyen başta Dr. Hüseyin Hışıl olmak üzere herkese teşekkür ederim.

BEYANNAME

Bilecik Şeyh Edebali Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kılavuzu'na uygun olarak hazırladığım bu tez çalışmasında, tez içindeki tüm verileri akademik kurallar çerçevesinde elde ettiğimi, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun olarak sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu Üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

…../…./ 2019

Bayram YAŞAR

ELİPTİK EĞRİLERİN FARKLI MODELLERİ ÜZERİNE

ÖZET

Eliptik eğriler matematiğin son yıllarda oldukça geniş bir bilim insanı topluluğu tarafından çalışılan önemli bir konusudur. Kriptoloji uygulamaları oldukça dikkat çekicidir. Bu alandaki ihtiyaç nedeniyle çeşitli kriptosistemler söz konusu olup, 7 bölümden oluşan bu çalışmada eliptik eğrilerin farklı modelleri incelenmiştir. İlk bölümde eliptik eğri kriptolojisi tanıtılmış olup, ikinci bölümde Edwards eğrileri ve üçüncü bölümde twisted Edwards eğrileri incelenmiştir. Dördüncü bölümde ise eliptik eğriler için verilen dört seviye bir theta modeli tanıtılmıştır. Beşinci bölümde ise yine eliptik eğriler için verilen yeni bir theta modeli ele alınmıştır. Altıncı bölümde bu modellerin maliyet analizi yapılmış olup son bölümde ise bazı modellerin maliyet karşılaştırılması ile sonuç ve tartışma yapılmıştır. Çalışma derleme niteliğindedir.

Anahtar Kelimeler: Eliptik Eğriler; Edwards Eğrileri; Theta Modeli

ON DIFFERENT MODELS OF ELLIPTIC CURVES

ABSTRACT

Elliptic curves are an important topic of mathematics that has been studied in recent years by a very large group of scientists. Cryptology applications are quite striking. Due to the need in this field, various cryptosystems are involved, and in this seven-part study, different models of elliptic curves are examined. In the first part elliptic curve cryptography is introduced and in the second part Edwards curves and in the third part twisted Edwards curves are examined. In the fourth chapter, a four-level theta model for elliptic curves is introduced. In the fifth chapter, a new theta model for elliptic curves is discussed. In the sixth section, the cost analysis of these models is made and in the last section the cost comparison of some models and conclusion and discussion is made. The study is compilation.

Keywords: Elliptic Curves; Edwards Curves; Theta Model

İÇİNDEKİLER

Sayfa No

TEŞEKKÜR .....

BEYANNAME .....

ÖZET ..... **I**

ABSTRACT ..... **II**

ŞEKİLLER DİZİNİ ..... **IV**

ÇİZELGELER DİZİNİ ..... **V**

SİMGELER ve KISALTMALAR DİZİNİ ..... **VI**

1. ELİPTİK EĞRİ KRİPTOLOJİSİ **1**

1.1. Giriş 1

1.2. Kamusal Anahtar Şifreleme Prensibi 2

1.3. EEK'nın Kapaklı Kapı Fonksiyonu 3

2. EDWARDS EĞRİLERİ **5**

3. TWISTED EDWARDS EĞRİLERİ **10**

4. ELİPTİK EĞRİLER İÇİN DÖRT SEVİYE BİR THETA MODELİ **14**

5. ELİPTİK EĞRİLER İÇİN YENİ BİR THETA MODELİ **18**

5.1. Eliptik Eğrilerin Yeni Modeli İçin Bir Eşitlik 18

5.2. Weierstrass Modelleri ile Bir Rasyonel Denklik 22

5.3. Yeni Theta Modeli Üzerinde Nokta Toplamı Formülleri 22

6. YENİ MODELDE TOPLAM FORMÜLLERİN HESAPLAMA MALİYETLERİ **24**

6.1. Projektif Koordinatlardaki Hesaplamalar 25

6.1.1. Nokta Toplamı 25

6.1.2. Bir Noktanın İki Katını Alma 26

7. MALİYET KARŞILAŞTIRMALARI İLE SONUÇ VE TARTIŞMA **27**

KAYNAKLAR **29**

ÖZGEÇMİŞ .....

ŞEKİLLER DİZİNİ

Sayfa No

Şekil 1.1. Kamusal Anahtar Şifrelemesi 1
Şekil 1.2. Eliptik Eğri Üzerindeki Nokta Toplamı 4
Şekil 2.1. Bir Edwards Eğrisi Örneği 5
Şekil 2.2. Çeşitli Edwards Eğrileri 6
Şekil 3.1. Twisted Edwards Eğrisi Örneği 11
Şekil 5.1. Bir Yeni Theta Modeli Örneği 20

ÇİZELGELER DİZİNİ

Sayfa No

Çizelge 4.1. Algoritma Ve Nokta Toplama Maliyeti 16

Çizelge 4.2. Algoritma Ve İki Katını Alma Maliyeti 16

Çizelge 4.3. İkili Cisimlerde Nokta Toplamı Algoritması Ve Maliyeti 17

Çizelge 4.4. İkili Cisimlerde İki Katını Alma Algoritması Ve Maliyeti 17

Çizelge 7.1. Çeşitli Modellerin Maliyet Karşılaştırmaları 27

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler

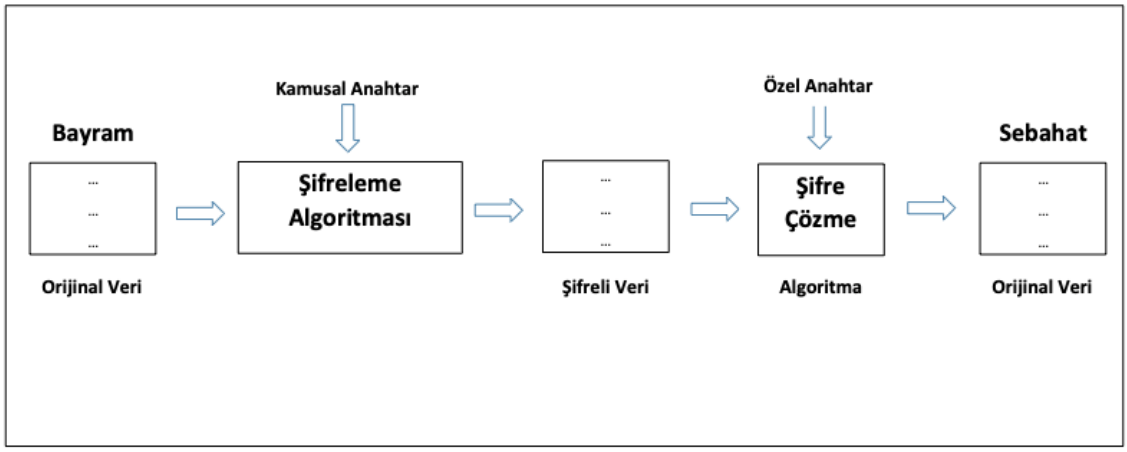
$\mathbb{R}$	: Reel Sayılar
$\mathbb{Z}$	: Tam Sayılar
$\mathbb{C}$	: Kompleks Sayılar

1. ELİPTİK EĞRİ KRİPTOLOJİSİ

1.1. Giriş

Eliptik Eğri Kriptolojisi (EEK) veriyi şifrelemenin öyle bir yoludur ki sadece uzman kişiler bu şifreyi çözebilirler. Günümüz bilişim çağındaki en önemli konulardan birisi veri güvenliğidir. EEK'nin gerçek hayat uygulamalarının yanı sıra en çok kullanıldığı yer internet veri trafiğindeki şifrelemedir. Örneğin bir e-postanın sadece muhatabı tarafından okunması için şifrelenmesinde EEK kullanılır.

Kamusal anahtar şifrelemenin birçok metodu vardır. EEK bunlardan yalnızca biridir. (Cohen ve Frey 2006)'den de takip edilebileceği üzere kamusal anahtar şifrelemelerde RSA, Diffie-Helman vb. başka algoritmalar da kullanılır. Aşağıdaki şemada kamusal anahtar şifrelemesi gösterilmiştir.



Şekil 1.1. Kamusal Anahtar Şifrelemesi

Dikkat edilirse Şekil 1.1'de iki anahtar vardır: kamusal anahtar ve özel anahtar. Bu iki anahtar sırasıyla veriyi şifrelemede ve veri üzerindeki şifreyi çözmede kullanılır. Öyle ki veri aktarılırken Dünya üzerindeki herhangi bir kişi şifreli veriyi görebilirken gönderen ve alıcı dışında kimse mesajı okuyamaz.

Örnek 1.1.1. Bayram yeni ispatladığı teoremi Sebahat'e göndermek istiyor. Ancak bu önemli teoremin ispatını kimsenin görmesini istemiyor. Kamusal anahtar şifrelemesi yardımıyla Bayram aşağıdaki adımları takip ederek bu mesajı güvenli bir şekilde Sebahat'e iletebilir.

1) Bayram, Sebahat'e gizli bir mesaj yollamak istediğini belirtir.

2) Sebahat , Bayram'a kendine ait olan kamusal anahtar yollar.

3) Bayram mesajını bu anahtar ile şifreler.

Teorem + Kamusal anahtar = 3d4k7lj79hghsgfd6656vhv

4) Bayram, Sebahat'e şifrelenmiş mesajı gönderir.

5) Sebahat, mesajın şifresini çözebilmek için özel anahtarı kullanır.

3d4k7lj79hghsgfd6656vhv + özel anahtar = Teorem

Böylece Bayram, Sebahat'e teoremin ispatını güvenli bir şekilde ulaştırmış olur.

Uyarı 1.1.2. Kamusal anahtar herkes ile paylaşılabilir. Özel anahtar iyi saklanmalıdır. Çünkü bu anahtar ele geçirilirse mesaj kolayca okunabilir. Bilgisayar yardımıyla şifreleme ve şifre çözme hızlıca yapılabilir. Bir bilgisayarın özel anahtara sahip olmadan şifreli mesajı çözebilmek için belki de milyonlarca yıl gereklidir.

1.2. Kamusal Anahtar Şifreleme Çalışma Prensibi

Bu şifreleme çeşidinin çalışma prensibi tek yönlü olarak açılabilen bir "kapaklı kapı fonksiyonu" olarak isimlendirilebilir. Gerçekten de bu fonksiyon "tek yönlü" hesaplanabilen bir fonksiyon olmalıdır. Her bir şifreleme çeşidi bir tek "kapaklı kapı fonksiyonu"na sahiptir. Doğal olarak modern bilgisayarların teorik olarak özel anahtara sahip olmadan şifreyi çözebilme olasılığını da düşünerek "kapaklı kapı fonksiyonu"nu en azından bir tarafı kolayca hesaplanan bir fonksiyondur denilebilir.

$A + B = C$ bir kapaklı kapı fonksiyonu olamaz. Bu fonksiyon için eğer A ve B verilirse C hesaplanabilir. Burada B ve C verilirse A kolayca hesaplanır. O halde bu fonksiyon bir kapaklı kapı fonksiyonu olamaz. Örnek 1.1.1'e dönecek olursak "Teorem" ve kamusal anahtar verilirse "3d4k7lj79hghsgfd6656vhv" elde edilebilir. Ancak "3d4k7lj79hghsgfd6656vhv" ve kamusal anahtar verilirse "Teorem" mesajı elde edilemez.

En popüler şifreleme algoritması olan RSA'da kapaklı kapı fonksiyonunun güvenilirliği büyük bir tam sayının asal çarpanlarına hangi zorlukla ayrıldığına bağlıdır. Örneğin;

Kamusal anahtar 944.871.836.856.449.473 ve özel anahtar 961.748.941 ve 982.451.653 olsun. Bu örnekte kamusal anahtar çok büyük bir tam sayı olup özel anahtar kamusal anahtarın iki asal çarpanıdır. Dikkat edilirse bu iki anahtar da kapaklı kapı fonksiyonunun amacına oldukça uygundur.

Uyarı 1.2.1 (a) Gerçek hayat kriptolojisinde bir özel anahtarın güvenilir sayılabilmesi için en az 200 haneli olması gerekir.

(b) EEK ile RSA karşılaştırılacak olursa EEK şu yönleriyle ön plana çıkar. EEK'de tıpkı RSA'daki gibi hem kamusal hem de özel anahtar üretilir. Ancak güvenlik düzeylerine bakıldığında EEK' de üretilen 256 bit uzunluğundaki bir anahtar RSA'da üretilen 3072 bit'lik bir anahtar ile aynı güvenliğe sahiptir. Böylece EEK bilgisayarlar, akıllı telefonlar gibi yerlerde %10 oranında daha az bant genişliği ve hard diskte yere ihtiyaç duyarlar.

1.3. EEK'nin Kapaklı Kapı Fonksiyonu

İlk olarak eliptik eğri kavramı tanıtmakla işe başlayalım. **F** karakteristiği 2 veya 3 olmayan bir cisim olsun. Bu takdirde $a_1, a_2, a_3, a_4, a_6 \in \mathbf{F}$ olmak üzere

$$E(\mathbf{F}) = \{(x, y) \in F^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\} \quad (1.1)$$

şeklinde tanımlanan kümeye **F** üzerinde tanımlı bir eliptik eğri denir (Silverman 2016). Bir eliptik eğri farklı şekillerde ifade edilebilir. Buna eliptik eğrilerin formları adı verilir. (1.1) eşitliğindeki formuna *Weierstrass formu* denir.

(1.1) eşitliğinde (Silverman 2016) sayfa 46'da yer alan uygun bir değişken değişimi yardımıyla eliptik eğrinin *kısa Weierstrass formu* $a, b \in \mathbb{Z}$ ve $\Delta = -16(4a^3 + 27b^2) \neq 0$ olmak üzere

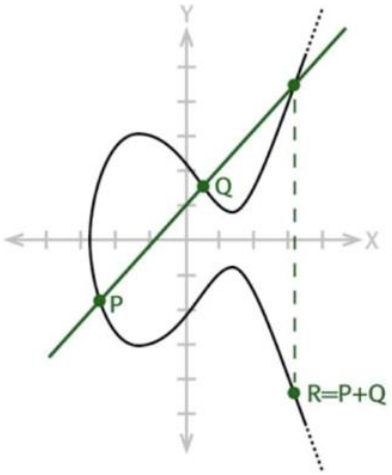
$$y^2 = x^3 + ax + b$$

eşitliğiyle verilir. Bir eliptik eğrinin Montgomery formu ise

$$BY^2 = X^3 + AX^2 + X$$

olarak tanımlanır.

Eliptik eğriler üzerinde tanımlanan ilginç nokta toplamı yardımıyla bir abelyen grup oluştururlar (Silverman 2016). Buna göre P ve Q noktaları $E(\mathbf{F})$ eliptik eğrisi üzerinde iki nokta olsun. P ve Q noktalarından geçen doğru verilen eliptik eğri üçüncü dereceden bir denklem olduğu için eğriyi bir üçüncü noktada keser. $P + Q$ noktası eğriyi kesen üçüncü noktanın x-eksenine göre simetriği olarak tanımlanır (Silverman 2016). Bir noktayı kendisiyle toplarken ilgili doğru olarak teğet doğrusu alınır. Teğet doğrusunun varlığını $\Delta \neq 0$ koşulu garantiler. Aşağıdaki şekilde eliptik eğri üzerindeki nokta toplamı geometrik olarak tanıtılmıştır.



Şekil 1.2. Eliptik Eğri Üzerinde Nokta Toplamı

Bir E eliptik eğrisi ve bu eğri üzerinde bir A noktasını göz önüne alalım. Bu noktayı keyfi bir B noktası ile toplayalım. Yani

$A + B = C$ olsun.

Devamında $A + C = D$ noktası elde edilsin. Son olarak da $A + D = E$ noktasına ulaşalım. Dikkat edilirse toplam 3 tane toplama işlemi yapılmış olur. O halde

Kamusal anahtar: Başlangıç noktası A ve bitiş noktası E

Özel anahtar: Yapılan toplama işlemi sayısı olur.

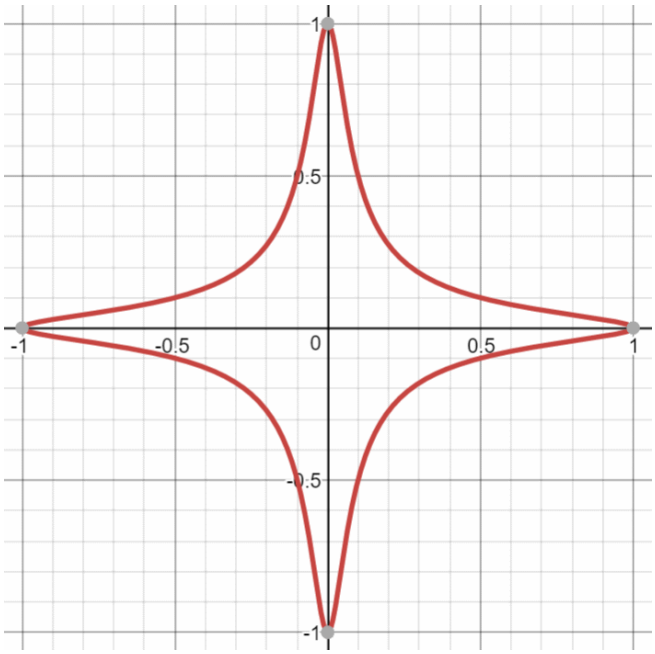
Böylece oldukça başarılı bir kapaklı kapı fonksiyonu elde edilmiş olur. Özel anahtar bilindiği takdirde A'dan E'ye ulaşmak oldukça kolaydır. Ancak A noktası verildiğinde kaç adımda E noktasına ulaşıldığını bulabilmek imkansıza yakındır. Burada ilk akla gelen soru B noktasının nasıl seçildiğidir. Genellikle $B = A$ yani bir noktanın iki katı alınır.

2. EDWARDS EĞRİLERİ

Harol Edwards, 2007'de eliptik eğrilerin bir yeni formunu tanımlamıştır. Bilim insanları bu ilgi çekici eğrilere Edwards eğrileri ismini vermiştir. Eliptik eğrilerin bu yeni formunun bu çapta bir kabul görmesinin sebebinin oldukça hızlı, şık ve basit bir nokta toplama işlemine sahip olması olduğu söylenebilir.

Bu bölümde Edwards eğrileri tanıtılacaktır ve grup yapısı incelenecektir. Detaylar için (Edwards 2007) kaynağı incelenebilir.

Tanım 2.1. **F** karakteristiği 2'den farklı bir cisim olsun. $d \neq 0,1$ olmak üzere $d \in \mathbf{F}$ alınsın. Bu durumda $x^2 + y^2 = 1 + dx^2y^2$ eşitliği ile tanımlanan eğriye *Edwards eğrisi* denir.



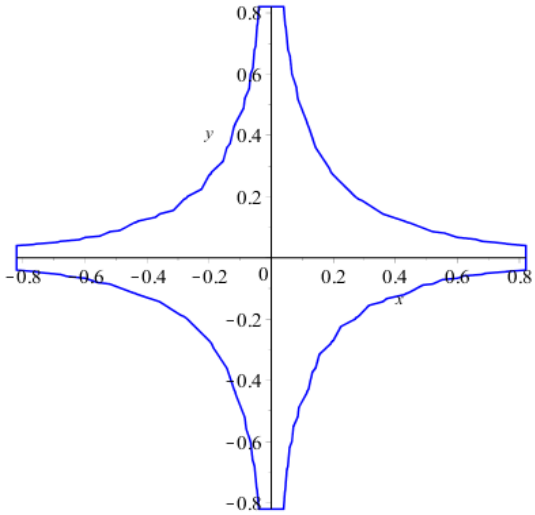
Şekil 2.1. Bir Edwards Eğrisi Modeli Örneği

Şekil 2.1'de $x^2 + y^2 = 1 + 300x^2y^2$ Edwards eğrisinin grafiği verilmiştir.

MAPLE programı yardımıyla Edwards eğrileri çizilebilir. Şekil 2.1'deki Edwards eğrisi aşağıdaki şekilde gibi çizdirilebilir.

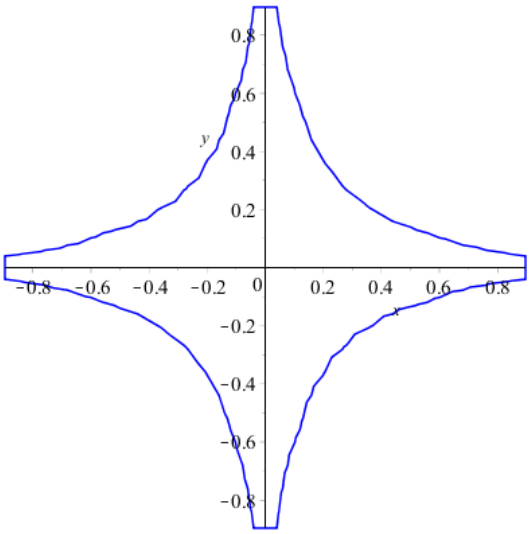
```
# d= -300 için fonksiyonun grafiği

implicitplot(x^2+y^2+300*x^2*y^2=1, x=-1..1,y=-1..1,color=blue);
```




```
# d= -150 için fonksiyonun grafiği

implicitplot(x^2+y^2+150*x^2*y^2=1, x=-1..1,y=-1..1,color=blue);
```



Şekil 2.2. Çeşitli Edwards Eğrileri

Tanım 2.2. Ed(**F**) = { $(x, y) \in$ **F**x**F** l $x^2 + y^2 = 1 + dx^2y^2$} kümesine *Edwards eğrisi üzerindeki noktaların kümesi* adı verilir.

Tanım 2.3. d sayısı **F** cismi üzerinde bir tam kare olmamak üzere (x_1, y_1), $(x_2, y_2) \in$ Ed(**F**) için Edwards eğrisi üzerinde toplama işlemi aşağıdaki şekilde tanımlanır:

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ olsun.

Bu durumda

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} \quad \text{ve} \quad y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} \tag{2.1}$$

Teorem 2.4 (Edwards 2007). Ed(**F**) yukarıda tanımlanan toplama işlemine göre bir grup olur.

İspat. Ed(**F**)'nın elemanı olan sıralı ikililer **F** cisminin elemanları olması ve $d \neq 0,1$ olmak üzere $d \in$ **F** olması koşulu nedeniyle verilen işlemin kapalılık özelliğini sağladığı kolayca görülür. *d* sayısı bir tam kare olmadıkça nokta toplamı formülündeki paydanın sıfır olma olasılığı yoktur. Birleşme özelliği doğrudan hesapla, oldukça karmaşık işlemlerle görülebilir. Öte yandan (0,1) noktasının bu işlemin etkisiz elemanı olduğu açıktır. Gerçekten de

(x_1, y_1) +(0,1) = $x_3 = \frac{x_1}{1}$ ve $y_3 = \frac{y_1}{1}$ olur.

(x_1, y_1) in bu işleme göre tersi $(-x_1, y_1)$'dir. Gerçekten de

$$(x_1, y_1) + (-x_1, y_1) = x_3 = \frac{x_1y_1 - x_1y_1}{1 - dx_1x_1y_1y_1} = 0 \quad \text{ve}$$

$$y_3 = \frac{y_1y_1 + x_1x_1}{1 + dx_1x_1y_1y_1} = \frac{1 + dx_1x_1y_1y_1}{1 + dx_1x_1y_1y_1} = 1$$

$= (0,1)$ olur.

Değişme özelliği görmek için (x_1, y_1), $(x_2, y_2) \in$ Ed(**F**) olmak üzere

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right) = (x_3, y_3) \text{ olsun.}$$

$$(x_2, y_2) + (x_1, y_1) = \left(\frac{x_2y_1 + y_2x_1}{1 + dx_1x_2y_1y_2}, \frac{y_2y_1 - x_2x_1}{1 - dx_1x_2y_1y_2}\right) = (x_3, y_3) \text{ olduğundan}$$

aşikar olarak $(x_1, y_1) + (x_2, y_2) = (x_2, y_2) + (x_1, y_1)$ olduğu görülür. O halde değişme özelliği vardır.

Böylece Ed(**F**) yukarıda tanımlanan toplama işlemine göre değişmeli bir grup olur.

Uyarı 2.5. Edwards eğrileri üzerindeki nokta toplamının geometrik yorumu şu şekilde açıklanabilir. Birim çember üzerinde aslında bir nokta toplamı tanımlanabilir. Öyle ki $x^2 + y^2 = 1$ ve $i = 1,2$ için $x_i = \sin\ (\alpha_i)$, $y_i = \cos\ (\alpha_i)$ olduğu kabul edilsin. Birim çember üzerinde (x_1, y_1) ve (x_2, y_2) noktalarının toplamı (x_3, y_3) olmak üzere bu iki noktanın toplamı

$$x_3 = \sin\ (\alpha_1 + \alpha_2) \quad \text{ve} \quad y_3 = \cos\ (\alpha_1 + \alpha_2)$$

Olarak tanımlayalım

$$x_3 = \sin\ (\alpha_1 + \alpha_2)$$

$$= \sin\ (\alpha_1).\cos\ (\alpha_2) + \cos\ (\alpha_1).\sin\ (\alpha_2)$$

$$y_3 = \cos\ (\alpha_1 + \alpha_2)$$

$$= \cos\ (\alpha_1).\cos\ (\alpha_2) - \sin\ (\alpha_1).\sin\ (\alpha_2)$$

olur. Böylece açıların toplamı etkisiz elemanı $(0,1)$ olan değişmeli bir grup tanımlar. Edwards eğrisi üzerindeki toplam buradan hareketle tanımlanmıştır. Birim çember üzerindeki bu toplama işlemiyle noktaların katları hızlıca hesaplanabilir ancak güvenlik düzeyi oldukça düşüktür. Ancak Edwards eğrisine bu nokta toplamının uyarlanması ile oldukça popüler bir kriptosistem elde edilmiştir.

Bir grupta sonlu mertebeli noktalar büyük önem taşır. Bu nedenle belirli mertebeye sahip tüm elemanları belirlemek oldukça önemlidir. Aşağıdaki teoremde Edwards eğrileri üzerindeki 2 ve 4. mertebeden tüm noktalar belirlenmiştir.

Teorem 2.6 (Edwards 2007). Bir Edwards eğrisi üzerindeki $(0,-1)$ noktasının mertebesi 2, $(1,0)$ ve $(-1,0)$ noktalarının mertebeleri ise 4'tür.

İspat. Doğrudan hesaplama yardımıyla $(0,-1) + (0,-1)$ işlemi yapıldığında $x_3 = 0$ $y_3 = \frac{1}{1} = 1$ olduğu görülür. Etkisiz eleman elde edildiği için $(0,-1)$ noktasının mertebesi 2'dir. Benzer şekilde hareket edilerek $(1,0)$ ve $(-1,0)$ noktalarının mertebeleri ise 4 olduğu görülür.

Aşağıdaki teoremde bir Edwards eğrisi üzerinde alınan bir *P* noktasını iki katına götüren formül verilmiştir. Bu tarz "yalın" formüller kriptosistemlerin hem pratikliği hem de güvenilirliği adına kritik rol oynar.

Teorem 2.7 (Edwards 2007). $P = (x_1, y_1) \in$ Ed(**F**) için $2P = \left(\frac{2x_1y_1}{x_1{}^2y_1{}^2}, \frac{y_1{}^2 - x_1{}^2}{2-(x_1{}^2+y_1{}^2)}\right)$olur.

İspat. Nokta toplamı formülü dikkate alınırsa $P = (x_1, y_1) \in$ Ed(**F**) için

$(x_1, y_1) + (x_1, y_1) = (x_3, y_3)$ olup burada

$$x_3 = \frac{2x_1y_1}{1+d\,x_1{}^2+y_1{}^2} \qquad y_3 = \frac{y_1{}^2-x_1{}^2}{1-d\,x_1{}^2+y_1{}^2}$$

olarak bulunur, bu da ispatı bitirir.

Teorem 2.8 (Edwards 2007). **F** karakteristiği 2'den farklı olan bir cisim ve *E* eliptik eğrisi **F** cismi üzerinde tanımlı ve en az bir tane 4. mertebeden noktaya sahip eliptik eğri olsun. Bu durumda *E* eliptik eğrisi ya **F** üzerinde ya da **F**' nin uygun bir cisim genişlemesi üzerinde tanımlı bir Edwards eğrisine dönüştürülebilir.

Uyarı 2.9. Edwards eğrisi üzerinde nokta toplamı işlemine bakıldığında paydanın sıfır olma riski göze çarpar. Eğer *d* tam kare değilse paydanın sıfır olamayacağı kolayca gösterilebilir.

Uyarı 2.10. Teorem 2.8 sayesinde eliptik eğrilerle Edwards eğrileri arasındaki ilişki kurulmuş olur. Bu ise Edwards eğrilerinin teori içindeki önemini gösterir.

3. TWISTED EDWARDS EĞRİLERİ

Bu bölümde daha genel bir Edwards eğrisi olan twisted Edwards eğrisine kısaca değinilecektir. Bu eğrilere ihtiyaç duyulmasının sebebi şu şekilde açıklanabilir. Teorem 2.7 gereği bir eliptik eğrinin daha "hızlı" bir kriptosistem olan Edwards eğrisine dönüştürebilmesi için 4. mertebeden bir noktaya sahip olması gerekliydi. Bu önemli bir kısıttır. Bu ise bir çok eliptik eğrinin Edwards eğrisine dönüştürülmesini engeller. Bunu aşabilmek için Edwards eğrilerini de kapsayan bir genelleştirilmeye gidilmiştir. Bu sayede daha hızlı bir nokta toplamına kavuşulmuş olup, çok daha fazla sayıda eliptik eğri kullanılabilmiştir. Bazı Edwards eğrilerinin twistleri alınarak daha hızlı kriptosistemler elde edilir. Twisted Edwards eğrilerinin bir diğer avantajı ise tüm Montgomery eğrilerinin twisted Edwards eğrisi cinsinden yazılabilmesidir.

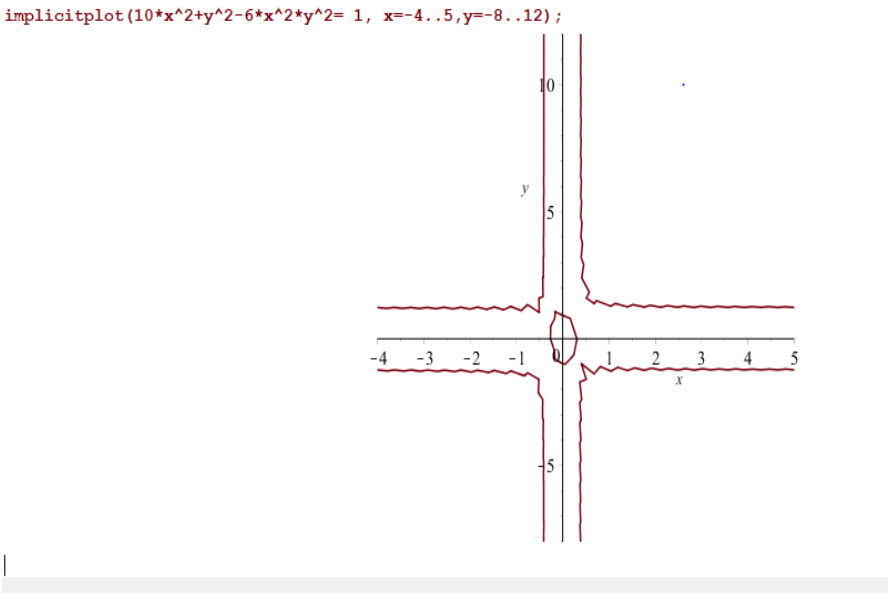
Tanım 3.1. (Bernstein vd. 2008) **F** karakteristiği 2'den farklı bir cisim ve $a, d \in \mathbf{F}$ 0'dan farklı iki eleman olsun. Bu durumda a ve d katsayılarına sahip *Twisted Edwards eğrisi* $\mathrm{Ed}_{a,d}$ ile gösterilir ve

$$\mathrm{Ed}_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

olarak tanımlanır.

Uyarı 3.2. Dikkat edilirse $a = 1$ alınması halinde klasik Edwards eğrisi elde edilir.

Örnek 3.3. $10x^2 + y^2 = 1 + 6x^2y^2$ eşitliğiyle tanımlanan eğrisi bir twisted Edwards eğrisi olup grafiği aşağıdaki gibidir.



Şekil 3.1. Twisted Edwards Eğrisi Örneği

Tanım 3.4 (Bernstein ve Lange 2007). Ed $_{a,d}$(**F**) twisted Edwards eğrisi üzerindeki nokta toplamı her $(x_1, y_1), (x_2, y_2) \in$ Ed $_{a,d}$(**F**) için

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

olarak tanımlanır.

Tanım 3.5. C_1 ve C_2, $\bar{F}^2$ üzerinde tanımlı iki eğri olsun. C_1 eğrisinden C_2 eğrisine **F** üzerinde bir rasyonel dönüşüm φ ile gösterilir ve

$$\varphi: C_1 \rightarrow C_2 \quad \varphi = (f, g)$$

olarak tanımlanır.

Burada f ve g **F** cismi üzerinde f ve g'nin tanımlı olduğu her $p \in C_1$ noktası için $\varphi(p) = (f(p), g(p)) \in C_2$ özelliğindedir.

Örnek 3.6. C eğrisi F_{13} üzerinde $v^2 = u^3 + 6u^2 + u$ eşitliğiyle tanımlansın.

$$f(u, v) = \frac{-2u}{v} \text{ ve } g(u, v) = -\frac{1+u}{1-u}$$

olarak tanımlansın. Bu takdirde f ve g sonlu sayıda nokta hariç (ki bu noktalara istisnai noktalar denir) tanımlıdır. Tam olarak istisnai noktalar $v = 0$ veya $u = 1$ şeklindedir.

Bu noktalar hesaplanırsa

1) Eğer $v = 0$ ise $u = 0$ veya $u^2 + 6u + 1 = 0$ olur. $u^2 + 6u + 1 = 0$ ın F_{13} te kökü yoktur. Böylece buradan bir tek istisnai nokta gelir o da $(0,0)$ noktasıdır.

2) Eğer $u = 1$ ise $v^2 = 8$ olur ki 8 F_{13} te ikinci dereceden kalan değildir. Bu yüzden buradan istisnai nokta gelmez.

O halde g her yerde tanımıdır. f için dikkat edilirse $\frac{u}{v} = \frac{v}{u^2+6u+1}$ olur ki $f(0,0) = 0$ elde edilir. Yani f c'nin tamamına genişletilebilir.

Örnek 3.7. Örnekte $v^2 = u^3 + 6u^2 + u$ eliptik eğrisi üzerinde

$$\frac{4u^2}{v^2} + \left(\frac{1+u}{1-u}\right)^2 = 1 + \frac{8u^2}{v^2} + \left(\frac{1+u}{1-u}\right)^2$$

özdeşliği yardımıyla $f^2 + g^2 = 1 + 2f^2g^2$ olduğu görülür.

O halde $\varphi = (f, g)$, $C: v^2 = u^3 + 6u^2 + u$ eliptik eğrisinden F_{13} üzerinde tanımlı $x^2 + y^2 = 1 + 2x^2y^2$ Edwards eğrisine bir rasyonel dönüşüm olur.

φ dönüşümünün C eliptik eğrisinin etkisiz elemanı $\infty' a$ verdiği resmi hesaplayalım. Öncelikle C'nin projektif koordinatlardaki denklemi

$C: v^2z = u^3 + 6u^2z + uz^2$ şeklindedir. ∞ noktasu $(0:1:0)$ olur (Silverman 2006). φ rasyonel dönüşümü $u = \frac{u}{z}$ ve $v = \frac{v}{z}$ dönüşümleri yardımıyla

$$\varphi\,(u:v:z) = \left(\frac{-2u}{v}, \frac{u+z}{u-z}\right) = \left(\frac{-2u}{v}, \frac{1+z/u}{1-z/u}\right)$$

olur. $\frac{z}{u} = \frac{u^2+6uz+z^2}{v^2}$ ve $(0:1:0)$'da sıfır olduğundan $\varphi(\infty) = (0,1)$ olur. Yani bu dönüşüm eliptik eğrinin etkisiz elemanını Edwards eğrisinin etkisiz elemanına resmeder.

Tanım 3.8 (Cohen ve Frey 2006). $\varphi : c_1 \to c_2$ bir rasyonel dönüşüm olsun. Eğer $\sigma o \varphi = id_{c1}$ ve $\varphi o \sigma = id_{c2}$ olacak şekilde bir $\sigma: c_2 \to c_1$ dönüşümü bulunabiliyorsa

φ'ye birasyonel dönüşüm denir ve bu durumda c_1 ve c_2 eğrilerine birasyonel olarak denk eğriler denir.

Örnek 3.9. Örnek 3.7 ile devam edelim $\alpha = (u, v)$ dönüşümü

$Ed: x^2 + y^2 = 1 + 2x^2y^2$ edwards eğrisi üzerinde her $(x, y) \in F_{13}\backslash\{0,1\}$ için

$$u = \frac{1+y}{1-y} \quad \text{ve} \quad v = \frac{2(1+y)}{x(1-y)}$$

ile tanımlansın.

$\sigma(0,1) = \infty \in C(F_{13})$ olur. O halde bu bir rasyonel dönüşüm olur. Dikkat edilirse bu φ ile birlikte σ dönüşümü E ile C arasında birasyonel denklik tanımlar.

Teorem 3.10 (Bernstein vd. 2008). Her bir Twisted Edwards eğrisi Montgomery formundaki bir eliptik eğriye dönüştürebilir. Tersi de doğrudur.

İspat. $Bv^2 = u^3 + Au^2 + u$ eşitliğiyle verilen Montgomery eğrisi $a = (A + 2)/B$ ve $d = (A - 2)/B$ olmak üzere $\text{Ed}_{a,d}(\mathbf{F})$: $ax^2 + y^2 = 1 + dx^2y^2$ twisted Edwards eğrisine birasyonel olarak denktir. Burada $(u, v) \mapsto (x, y) = (\frac{u}{v}, \frac{u-1}{u+1})$ şeklindeki dönüşüm istenilen özellikteki dönüşüm olur.

Bu çalışmanın temel amacı eliptik eğrilerin farklı formlarını incelemek ve derleme niteliğinde bir çalışma yapmak olduğu için Edwards ve twisted Edwards eğrileri hakkında derinlemesine bir inceleme yapılmamıştır, Edwards eğrileri hakkında yapılmış bir çalışma için (Muş 2009) kaynağına bakılabilir.

4. ELİPTİK EĞRİLER İÇİN DÖRT SEVİYE BİR THETA MODELİ

Bu bölümde eliptik eğriler için verilen dört seviyeli bir theta modeli ele alınacaktır. Bu modelin bu şekilde adlandırılmasının nedeni theta fonksiyonlarının Riemann ile ilişkilerinden gelmektedir. Daha kesin olarak theta fonksiyonlarının Riemann ilişkileri $\mathbb{C}$ üzerinde tanımlı bir eliptik eğriyi parametrize eder. (Silverman 2006)'ya göre $\mathbb{C}$ üzerinde tanımlı bir eliptik eğri $\mathbb{C}/\Lambda_\omega$ toruna izomorftur. Burada $\Lambda_\omega \coloneqq \omega\mathbb{Z} + \mathbb{Z}$ kafesini göstermektedir. Bu izomorfizm ise $\mathbb{P}^3$ projektif uzayına bir gömme tanımlar. Eliptik eğrilerin bu modeli 4 parametre ile tanımlandığı ve de theta fonksiyonun Riemann ilişkileri yardımıyla tanımlandığı için "Dört seviye theta modeli" olarak adlandırılmıştır. Bu bölümle ilgili detaylı bilgi (Diao ve Fouotsa 2015) ve (Fouotsa ve Diao 2017)'da bulunabilir.

Tanım 4.1. p bir asal sayı ve belirli bir r pozitif tamsayısı olmak üzere $q = p^r$ olsun ve F_q sonlu cismini ele alalım. Bu durumda *4 seviyeli theta modeli* (Mumford 1966), sayfa 352'ye göre

$\lambda = {c_0}^2 + 4{c_2}^2$ olmak üzere

$$E_\lambda = \left\{ \begin{matrix} {X_0}^2 + {X_2}^2 = \lambda X_1 X_3 \\ {X_1}^2 + {X_3}^2 = \lambda X_0 X_2 \end{matrix} \right\}$$

eşitliklerinin kesişimi olarak tanımlanır.

Etkisiz eleman $[c_0, 1, 2\,c_2, 1]$'dır. Diğer yandan $c_0, c_2 \in F_q$ katsayıları verilen eliptik eğrinin katsayılarına bağlı olarak tanımlanmıştır (Mumford 1966) ve üstelik $c_0\,c_2\,({c_0}^2 + 4{c_2}^2) = 1$ eşitliğini sağlarlar. $\lambda\,(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$ koşulu E_λ dört seviyeli theta modelinin singüler olmadığının kanıtıdır.

Aşağıdaki teorem dört seviye theta modeli üzerinde tanımlanmış birleşik toplam formüllerini verir. Bu formüller hem 2 farklı noktanın toplamı ve bir noktanın kendisiyle toplamı içinde kullanılabilir. Bu formüllerin bir diğer özelliği ise bu formüllerin yalnızca karakteristiği tek sayı olan cisimler üzerinde değil aynı zamanda ikili cisimler üzerinde geçerli olmasıdır.

Teorem 4.2 (Fouotsa ve Diao 2015). $P_1 = [X_0, X_1, X_2, X_3]$ ve $P_2 = [Y_0, Y_1, Y_2, Y_3]$ noktaları F_q sonlu cisim ve tanımlı E_λ eliptik eğri üzerinde iki nokta olsun. Bu durumda $P_1 + P_2 = P_3$ özelliğindeki P_3 noktasının $[Z_0, Z_1, Z_2, Z_3]$ koordinatları aşağıdaki gibi yazılabilir.

$$Z_0 = (X_0^{\,2} Y_0^{\,2} + X_2^{\,2} Y_2^{\,2}) - 4(\frac{c_2}{c_0}) X_1 X_3 Y_1 Y_3$$

$$Z_1 = a_0(X_0 X_1 Y_0 Y_1 + X_2 X_3 Y_2 Y_3) - 2\, c_2(X_2 X_3 Y_0 Y_1 + X_0 X_1 Y_2 Y_3)$$

$$Z_2 = (X_1^{\,2} Y_1^{\,2} + X_3^{\,2} Y_3^{\,2}) - 4(\frac{c_2}{c_0}) X_0 X_2 Y_0 Y_2$$

$$Z_3 = a_0(X_0 X_3 Y_0 Y_3 + X_1 X_2 Y_1 Y_2) - 2\, c_2(X_0 X_3 Y_1 Y_2 + X_1 X_2 Y_0 Y_3)$$

Herhangi bir sonlu cisim üzerinde $P = [X_0, X_1, X_2, X_3]$ noktasının tersi $-P$ ile gösterilir. $-P = [X_0, X_3, X_2, X_1]$ olarak bulunur.

Etkisiz eleman ise $o_0 = [c_0, 1, 2c_2, 1]$ dir.

Aşağıdaki teoremde eliptik eğrilerin dört seviye bir theta modelinin önemli bir özelliği verilmiştir.

Teorem 4.3 (Diao ve Fouotsa 2015). E_λ , $\mathbb{F}_q$ sonlu cismi üzerinde tanımlı bir eliptik eğrinin bir dört seviye theta modeli olsun. Bu takdirde E_λ dört mertebeli bir rasyonel noktaya sahiptir.

Aşağıdaki tablolarda nokta toplamı ve bir noktanın iki katını almayla ilgili algoritmalar verilmiştir. Bu tablolarda M, S ve m sırasıyla bir çarpma, kare alma ve bir sabit ile çarpmayı göstermektedir.

İşlemler	Maliyet
$\mathrm{A} := X_0.Y_0;\ \mathrm{B} := X_1.Y_1;\ \mathrm{C} := X_2.Y_2;\ \mathrm{D} := X_3.Y_3;\ \mathrm{E} := A^2;\ \mathrm{F} := B^2;$	$4M + 2S$
$\mathrm{G} := C^2;\ \mathrm{H} := D^2;\ Z_0 := E + G + (2c_2/c_0)((\mathrm{B} - \mathrm{D})^2 - F - H);$	$3S + 1m$
$Z_2 := F + H + (2c_2/c_0)((\mathrm{A} - \mathrm{C})^2 - E - G);\ I = 1/2((\mathrm{A} + \mathrm{B})^2 - E - F);$	$2S + 1m$
$J = 1/2((\mathrm{C} + \mathrm{D})^2 - G - H);\ \mathrm{K} := (U_1 + V_1)(U_2 + V_2) - I - J;$	$1M + 1S$
$\mathrm{L} := (A + C)(B + D) - I - J;\ Z_1 := a_0(I + J) - 2c_2K;$	$1M + 2m$
$\mathrm{E} := (X_0 + X_2)(X_3 + X_1) - U_1 - V_1;\ \mathrm{E} := (Y_0 + Y_2)(Y_3 + Y_1) - U_2 - V_2;$	$2M$
$G := EF - L;\ Z_3 := c_0L - 2c_2G;\ U_3 := Z_0\ Z_1\ ;\ V_3 := Z_2\ Z_3.$	$3M + 2m$
Toplam maliyet: $11M + 8S + 6m$	

Çizelge 4.1. Algoritma ve Nokta Toplama Maliyeti

İşlemler	Maliyet
$\mathrm{A} := X_0X_2;\ \ \mathrm{B} := X_1X_3;\ \ \mathrm{C} := A^2;\ \mathrm{D} := B^2;\ \ \ Z_0 := ({\lambda_1}^2 - 4{c_2}^2\lambda_1)D - 2C;$	$2M + 2S + 1m$
$Z_2 := ({\lambda_1}^2 - 4{c_2}^2\lambda_1)C - 2D;\ \mathrm{E} := U_1V_1);\ \mathrm{F} := (U_1 + V_1)^2 - 2E;$	$1M + 1S + 1m$
$Z_1 := c_0F - 2E;\ U_3 := Z_0\ Z_1\ ;$	$1M + 1m$
$Z_3 := c_0\big(\ ((X_0 + X_1)(X_3 + X_2) - A - B)^2 - 2E\big) - 4c_2E;\ V_3 := Z_2\ Z_3.$	$2M + 1S + 1m$
Toplam maliyet: $6M + 4S + 3m$	

Çizelge 4.2. Algoritma ve iki katını alma maliyeti

İşlemler	Maliyet
$\mathrm{A} := X_0.Y_0;\ \mathrm{B} := X_1.Y_1;\ \mathrm{C} := X_2.Y_2; \mathrm{D} := X_3.Y_3;\ Z_0 := (\mathrm{A}+\mathrm{C})^2;$	$4M + 1S$
$Z_2 := (\mathrm{B}+\mathrm{D})^2; Z_1 := c_0(AB+CD); Z_3 := c_0(A+C)(B+D) - Z_1$	$3M + 1S + 2m$
Toplam maliyet: $7M + 2S + 2m$	

Çizelge 4.3. İkili cisimlerde nokta toplamı algoritması ve maliyeti

İşlemler	Maliyet
$\mathrm{A} := {X_0}^2; \mathrm{B} := {X_1}^2; \mathrm{C} := {X_2}^2; \mathrm{D} := {X_3}^2; Z_0 := (\mathrm{A}+\mathrm{C})^2; Z_2 := (\mathrm{B}+\mathrm{D})^2;$	$6S$
$Z_1 := c_0(AB+CD);\ Z_3 := c_0(A+C)(B+D) - Z_1$	$3M + 2m$
Toplam maliyet: $3M + 6S + 2m$	

Çizelge 4.4. İkili cisimlerde iki katını alma algoritması ve maliyeti

5. ELİPTİK EĞRİLER İÇİN YENİ BİR THETA MODELİ

Bu bölümde eliptik eğrinin dört seviye theta modelinden herhangi bir sonlu cisim üzerinde tanımlı ve yeni bir theta modeli adını vereceğimiz yeni bir model tanımlayacağız. Ayrıca bu model ile ikili olmayan cisimler üzerinde tanımlı Edwards modeli arasında bir rasyonel denklik vereceğiz.

5.1. Eliptik Eğrilerin Yeni Modeli İçin Bir Eşitlik

Bu kısımda ileride tanımlanacak eliptik eğrilerin yeni modeli için gerekli olan hazırlıklar yapılacaktır. Buna göre ilk olarak eliptik eğriler arasında tanımlanabilen özel bir dönüşüm olan "isogeni" kavramı verilecektir.

Tanım 5.1.1. (Silverman 2016). E_1 ve E_2, K cismi üzerinde tanımlı iki eliptik eğri olsun. Eğer $f: E_1 \to E_2$ sabit olmayan bir morfizm ise yani O_{E_1} ve O_{E_2} sırasıyla E_1 ve E_2 eliptik eğrilerinin etkisiz elemanını göstermek üzere, eğer f dönüşümü $f(O_{E_!}) = O_{E_2}$ olacak şekilde katsayıları K cisminden olan rasyonel fonksiyonlar yardımıyla verilen bir morfizm ve f'ye E_1 'den E_2'ye K üzerinde bir isogeni adı verilir.

Eğer $f: E_1 \to E_2$ olacak şekilde bir isogeni bulunabiliyorsa E_1 ve E_2'ye isogenik eliptik eğriler denir.

İsogeni dönüşümünün bir grup homomorfizma olduğu kolayca görülebilir. İsogeni dönüşümünün çekirdeğinin eleman sayısına isogenin derecesi denir.

Çekirdeğinde iki eleman bulunan isogeniye 2-isogeni denir.

Teorem 5.1.2 (Fouotsa ve Diao 2017). F_q sonlu cisim üzerinde tanımlı E_λ 4 seviye theta modeli olsun. Bu takdirde, $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$ ve etkisiz eleman $o_0=\left(\frac{2c_2}{c_0}, 1\right)$ olmak üzere E_λ 4 seviye theta modeli

$$\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$$

eşitliğiyle verilen eliptik eğriye 2-isogenidir.

İspat. φ= $E_\lambda \to \varepsilon_\lambda$

$[X_0,\ X_1,\ X_2,\ X_3] \mapsto (x,y) = (\frac{X_2}{X_0}, \frac{X_3}{X_1})$ dönüşümünü ele alalım. Bu durumda kolayca görülebilir ki;

$$1 + x^2 = \lambda \frac{X_1 X_3}{X_0^2} \text{ ve } 1 + y^2 = \lambda \frac{X_0 X_2}{X_1^2}$$

olur.

Yukarıdaki iki eşitlik çarpılarak $(1 + x^2).(1 + y^2) = \lambda^2 xy$ elde edilir. Böylece $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ elde edilir. Bu yüzden φ bir rasyonel dönüşümdür. Üstelik $\varphi_{(P)} = (0,0)$ olması E_λ üzerinde olmayan $P = (0,0,0,0)$ noktası olmasını gerektirdiğinden φ düzgün bir dönüşümdür. Buna ilave olarak o_0=$[c_0, 1, 2c_2, 1]$ etkisiz elemanı φ dönüşümü altında o_0=$\left(\frac{2c_2}{c_0}, 1\right)$ noktasına resmeder ki buradan φ'nin 1-isogeni olduğu açıkça görülür. Direkt hesaplama yardımıyla bu isogeninin derecesi $ker\ \varphi = \{o_0, [-c_0, 1, -2c_2, 1]\}$ olduğundan 2 olarak bulunur.

O halde bu dönüşüm bir 2-isogeni dönüşümü olur. Bu ise ispatı bitirir.

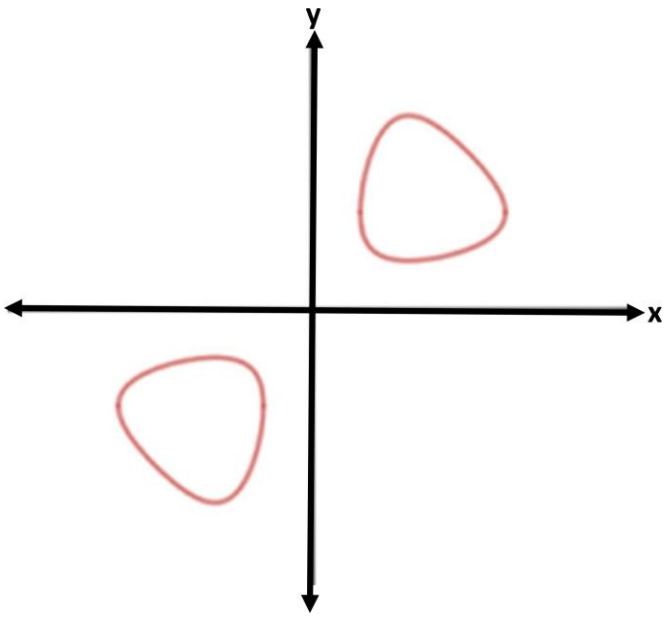
Uyarı 5.1.3. $\frac{2c_2}{c_0}$ değerine λ diyeceğiz.

Tanım 5.1.4. Bir F_q sonlu cismi üzerinde tanımlı eliptik eğrilerin theta modeli etkisiz eleman o_0=$\left(\frac{2c_2}{c_0}, 1\right)$ ve $\lambda = c_0^2 + 4c_2^2$ eşitliği $\lambda(\lambda^2 - 4)(\lambda^2 + 1) \neq 0$ özelliğini sağlamak üzere

$$\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$$

yardımıyla tanımlanır.

Aşağıdaki şekilde bir yeni theta modelinin grafik temsili yer almaktadır. Burada eğrinin reel sayıların bir alt kümesi olarak tanımlandığı kabul edilmiştir.



Şekil 5.1. Bir Yeni Theta Modeli Örneği

Uyarı 5.1.5. ε_λ eliptik eğrisi tıpkı Edwards modelindeki gibi önemli bir simetri özelliğine sahiptir. Öyle ki eğer (x, y) noktası ε_λ nın bir elemanıysa (y, x) noktasında ε_λ eğrisinin bir elemanıdır.

Teorem 5.1.6 (Fouotsa ve Diao 2017). $o_0=\left(\frac{2c_2}{c_0}, 1\right)$ özdeşlik elemanı olmak üzere ikili olmayan cisim üzerinde tanımlı ε_λ eliptik eğrisi bir rasyonel olarak

$$E_c: x^2 + y^2 = c^2(1 + x^2 + y^2)$$

Edwards modeline denktir.

İspat. $\varphi = \varepsilon_\lambda \to E_c$ dönüşümü

$$(x, y) \mapsto \left(\frac{x+1}{x-1}, \frac{1+y}{1-y}\right)$$

$$\left(\frac{2c_2}{c_0}, 1\right) \mapsto (0,1)$$

$$\left(1, \frac{2c_2}{c_0}\right) \mapsto (1,0)$$

olarak tanımlansın.

φ dönüşümü $c = \frac{c_0 - 2c_2}{c_0 + 2c_2}$ olmak üzere ε_λ eğrisini $E_c: x^2 + y^2 = c^2(1 + x^2y^2)$ Edwards modeline resmeder.

o_0=$\left(\frac{2c_2}{c_0}, 1\right)$ etkisiz elemanı dışında $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda xy$ eliptik eğrisi 3 tane 2-torsiyon rasyonel noktaya sahiptir. Ve bunlar $\lambda = \frac{2c_2}{c_0}$ olmak üzere $P_2 = (\frac{1}{\lambda}, 1)$ $P_3 = (-\lambda, -1)$ ve $P_4 = (-\frac{1}{\lambda}, -1)$ noktalarıdır.

Bunun yanı sıra ε_λ eliptik eğrisi F_q üzerinde rasyonel olan $\mathrm{Q}_1 = (1, \lambda)$, $\mathrm{Q}_2 = (1, \frac{1}{\lambda})$ $\mathrm{Q}_3 = (-1, -\lambda)$ ve $\mathrm{Q}_4 = (-1, -\frac{1}{\lambda})$ gibi 4 tane 4-torsiyon noktasına sahiptir. 2 mertebeli ve 4 mertebeli rasyonel mertebelerin etkileri

$$(x, y) + Q_0 = (x, y)$$

$$(x, y) + P_3 = (-x, -y)$$

$$(x, y) + Q_1 = (\frac{1}{y}, x)$$

$$(x, y) + Q_3 = (-\frac{1}{y}, -x)$$

$$(x, y) + P_2 = (\frac{1}{x}, \frac{1}{y})$$

$$(x, y) + P_4 = (-\frac{1}{x}, -\frac{1}{y})$$

$$(x, y) + Q_2 = (y, \frac{1}{x})$$

$$(x, y) + Q_4 = (-y, -\frac{1}{x})$$

şeklindedir.

Uyarı 5.1.7. Eğer F_q bir ikili cisimse bu durumda $P_3 = o_0$, $P_4 = P_2$, $Q_3 = Q_1$ ve $Q_4 = Q_2$ 'dir. Üstelik ε_λ eliptik eğrisi üzerindeki rasyonel noktaların sayısı 4 ile bölünebilir.

5.2. Weierstrass Modelleri ile Bir Rasyonel Denklik

Teorem 5.2.1 (Fouotsa ve Diao 2017). $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ eliptik eğrisi karakteristiği $p \geq 0$ olan bir F_q sonlu cismi üzerinde tanımlı bir eliptik eğri olsun.

1.) $p \neq 2$ ise bu durumda ε_λ bir kübik Weierstrass modele bir rasyonel olarak denktir.

2.) $p = 2$ ise bu durumda ε_λ eliptik eğrisi bir rasyonel olarak $v^2 + uv = u^3 + 1/\lambda^4$ Weierstrass modeline denktir.

Karakteristiği 2 olan cisimler için ε_λ modeliyle Weierstrass modeli arasındaki bir rasyonel dönüşüm ve bunun tersi aşağıdaki gibi verilmiştir.

Sonuç 5.2.2 (Fouotsa ve Diao 2017). $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ eliptik eğrisi ikili olmayan bir F_q cismi üzerinde tanımlanmış olsun. Bu durumda ε_λ j –invaryantı

$$j = \frac{((c_0{}^4 - 4\ c_0{}^3 c_2 + 8\ c_0{}^2\ c_2{}^2 + 16 c_0\ c_2{}^3 + 16\ c_2{}^4)(\ c_0{}^4 + 4\ c_0{}^3\ c_2 + 8\ c_0{}^3\ c_2{}^2 - 16 c_0\ c_2{}^3 + 16\ c_2{}^4))^3}{(c_2\ c_0(\ c_0 - 2\ c_2)(\ c_0 + 2\ c_2)(\ c_0{}^2 + 4\ c_2{}^2))^4}$$

olur.

5.3. Yeni Theta Modeli Üzerinde Nokta Toplamı Formülleri

Bu kısımda $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ eliptik eğrisi üzerinde nokta toplamı formüllerini elde edebilmek için seviye dört theta modeli üzerinde toplama formüllerini kullanacağız.

Teorem 5.3.1. (x_1, y_1) ve (x_2, y_2) ε_λ üzerinde iki nokta olsun. Bu durumda $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ olacak şekilde (x_3, y_3) noktasının koordinatları aşağıdaki gibi verilir.

$$(x_3, y_3) = \left(\frac{c_0(x_1 + y_1x_2y_2) - 2c_2(y_1 + x_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)}, \frac{c_0(x_1x_2 + y_1y_2) - 2c_2(x_1y_2 + y_1x_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)} \right)$$

(x_1, y_1) noktasının tersi ise $-(x_1, y_1) = (x_1, \frac{1}{y_1})$ 'dir.

Karakteristiği 2 olan cisimler üzerinde 2 noktanın toplamı için koordinatları mod 2'deki indirgeme yardımıyla elde edilir.

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1+y_1x_2y_2}{y_2+x_1y_1x_2}, \frac{x_1x_2+y_1y_2}{1+x_1y_1x_2y_2}\right) \tag{5.1}$$

Uyarı 5.3.2. Yukarıda verilen nokta toplamı formülleri herhangi bir cisim üzerinde birleştirilebilir. Yani toplam formülleri bir noktanın iki katını hesaplamak için de geçerlidir. x_2, x_1 üzerinde ve y_2, y_1 ile değiştirilerek verilen bir (x_1, y_1) noktasının iki katı aşağıdaki gibi bulunur.

$$2(x_1, y_1) = \left(\frac{c_0x_1(1 + {y_1}^2) - 2c_2y_1(1 + {x_1}^2)}{c_0y_1(1 + {x_1}^2) - 2c_2x_1(1 + {y_1}^2)}, \frac{c_0({x_1}^2 + {y_1}^2) - 4c_2x_1y_1}{c_0(1 + {x_1}^2{y_1}^2) - 4c_2x_1y_1}\right) \tag{5.2}$$

ikili cisimlerde (5.1) ve (5.2) formülleri yardımıyla (x_1, y_1) noktasının iki katı

$$2(x_1, y_1) = \left(\frac{x_1(1 + y_1)^2}{y_2(1 + x_1)^2}, \frac{(x_1 + y_1)^2}{(1 + x_1y_1)^2}\right)$$

olarak bulunabilir.

6. YENİ MODELDE TOPLAM FORMÜLLERİN HESAPLAMA MALİYETLERİ

Bu bölümde sonlu cisim üzerinde tanımlı yeni model için hem afin hem de projektif koordinatlardaki toplam formüllerinin maliyetlerini bulacağız. Burada önceki bölümdeki işlemlere ilaveten I ile tersinme gösterilmektedir. Afin koordinatlarda (x_1, y_1) ve (x_2, y_2) F_q cismi üzerinde tanımlı $\varepsilon_\lambda : 1 + x^2 + y^2 + x^2y^2 = \lambda^2 xy$ eliptik eğrisi iki nokta olsun. Aşağıdaki formüller $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ özelliğindeki (x_3, y_3) noktasını hesaplamaya yarar.

$$A = x_1.y_1\,; \quad B = x_2.y_2\,; \quad C = x_1 + y_1.B\,; \quad D = y_1 + x_1.B;$$

$$E = y_2 + x_2.A\,; F = x_1 + y_1.A\,; \qquad G = A + B\,;$$

$$H = (x_1 + y_2).(x_2 + y_1) - G\,; I = (x_1 + y_1).(x_2 + y_2) - H\,;$$

$$J = 1 + A.B\,;$$

$$x_3 = (c_0.C - 2c_2.D)/(c_0.E - 2c_2.F)\,;$$

$$y_3 = (c_0.H - 2c_2.I)/(c_0.J - 2c_2.G)$$

Bu formüller ikili olmayan cisimler üzerinde $2I + 9M + 8m$ maliyete sahiptir. İkili cisimler üzerinde ise maliyet $2I + 5m$ şeklindedir. Bir noktanın tersini almanın bir tersinme maliyetindedir, bu ise oldukça pahalı bir işlemdir. Bununla beraber (x_1, y_1) ve (x_2, y_2) gibi iki noktanın toplamı ve farkı aynı maliyete sahiptir. Gerçekten de bu iki noktanın farkını (x_4, y_4) ile gösterirsek $(x_4, y_4) = (x_1, y_1) - (x_2, y_2)$ noktası aşağıdaki formül yardımıyla hesaplanır.

$$(x_4, y_4)$$
$$= \left(\frac{c_0(x_1y_2 + y_1x_2) - 2c_2(x_1x_2 + y_1y_2)}{c_0(1 + x_1y_1x_2y_2) - 2c_2(x_1y_1 + x_2y_2)}, \frac{c_0(y_1 + x_1x_2y_2) - 2c_2(x_1 + y_1x_2y_2)}{c_0(y_2 + x_1y_1x_2) - 2c_2(x_2 + x_1y_1y_2)} \right)$$

Nokta toplamını hesaplamada kullanılan 8 polinomu tekrar ele alalım.

$$F_1 = x_1 + y_1x_2y_2\,, \quad F_2 = y_1 + x_1x_2y_2\,, \quad F_3 = y_2 + x_1y_1x_2,$$

$$F_4 = x_2 + x_1y_1y_2\,, \quad F_5 = x_1x_2 + y_1y_2\,, \quad F_6 = x_1y_2 + y_1x_2,$$

$$F_7 = 1 + x_1y_1x_2y_2\,, \quad F_8 = x_1y_1 + x_2y_2$$

o halde yukarıda verilen formüller aşağıdaki gibi tekrar yazılabilir:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{c_0F_1 - 2c_2F_2}{c_0F_3 - 2c_2F_4}, \frac{c_0F_5 - 2c_2F_6}{c_0F_7 - 2c_2F_8}\right),$$

$$(x_1, y_1) - (x_2, y_2) = \left(\frac{c_0F_6 - 2c_2F_5}{c_0F_7 - 2c_2F_8}, \frac{c_0F_2 - 2c_2F_1}{c_0F_3 - 2c_2F_4}\right).$$

6.1. Projektif Koordinatlarda Hesaplamalar

$t = xy$ gibi yeni bir koordinat tanımlayarak ε_λ eliptik eğrisi $\mathbb{P}^2$ projektif uzayına gömeriz. Daha etkili hesaplama yapabilmek için bir noktanın iki katını alma ve iki noktanın toplamını hesaplamada Hisil ve arkadaşlarının (2009) yaklaşımını kullanacağız. Öyle ki burada $z \neq 0$ ve $x = X/Z$, $y = Y/Z$, $t = T/Z$, $T = X.Y/Z$ olmak üzere $[X, Y, Z, T] \in \mathbb{P}^3$ genişletilmiş projektif koordinatlarını bulalım. $\mathbb{P}^3$'teki tanımlı bir eğrinin projektif kapanımı

$$Z^2 + X^2 + Y^2 + T^2 = \lambda^2.T.Z$$

olur.

6.1.1. Nokta Toplamı

$[X_3, Y_3, T_3, Z_3] = [X_1, Y_1, T_1, Z_1] + [X_2, Y_2, T_2, Z_2]$ noktasının koordinatları

$$X_3 = (X_1.Z_2 + Y_1.T_2).(Z_1.Z_2 + T_1.T_2)$$

$$Y_3 = (X_1.X_2 + Y_1.Y_2).(Z_1.Y_2 + X_2.T_1)$$

$$Z_3 = (Z_1.Z_2 + T_1.T_2).(Z_1.Y_2 + X_2.T_1)$$

$$T_3 = (X_2.Z_2 + Y_1.T_2).(X_1.X_2 + Y_1.Y_2)$$

X_3'ü hesaplamanın maliyeti $5M$'dir. Gerçekten de $X_1.Z_2, Y_1.T_2, Z_1.Z_2, T_1.T_2$ ve ara çarpımdır. Benzer gerekçe Y_3 noktası içinde geçerlidir. Z_3'ü ve T_3'ü hesaplamanın maliyeti $1M$ olup X_3 ve Y_3 hesaplanırken bu çarpımlar zaten hesaplandığından toplam maliyet $12M$ çıkar.

6.1.2. Bir Noktanın İki Katını Alma

$[X_3, Y_3, T_3, Z_3] = 2.[X_1, Y_1, T_1, Z_1]$ noktasının koordinatları:

$$X_3 = (X_1.Z_1 + Y_1.T_1).(Z_1 + T_1)^2$$

$$Y_3 = (Y_1.Z_1 + X_1.T_1).(X_1 + Y_1)^2$$

$$Z_3 = (Y_1.Z_1 + X_1.T_1).(Z_1 + T_1)^2$$

$$T_3 = (X_1.Z_1 + Y_1.T_1).(X_1 + Y_1)^2$$

olarak elde edilir.

X_3'ün hesaplanmasının maliyeti $3M + 1S$'dir. Gerçekten de $X_1.Z_1$, $T_1.Y_1$, $(X_1 + Y_1)^2$ 'dir. Benzer işlemler Y_3 için de geçerlidir. Z_3 ve T_3'ün hesaplanmasının her biri $1M$ maliyetine sahiptir ve bu çarpımlar X_3 ve Y_3'ün hesaplanmasında zaten kullanılmıştır. O halde bir noktanın iki katının almanın toplam maliyeti $8M + 2S$'dir.

7. MALİYET KARŞILAŞTIRMALARI İLE SONUÇ VE TARTIŞMA

Bu bölümde ikili cisimler üzerinde toplam formüllerini karşılaştıracağız. Aşağıdaki çizelge (Fouotsa ve Diao 2017)'de yer almaktadır.

Modeller	**İki Katını Alma**	**Toplama**
Weierstrass	7M + 3S	14M + 1S
Yeni theta modeli	8M + 2S	12M
4 seviyeli theta modeli	3M + 6S + 2m	7M + 2S + 2m
İkili Edwards	2M + 5S + 2m	16M + 1S + 4m

Çizelge 7.1. Çeşitli modellerin maliyet karşılaştırmaları

Yeni kriptosistemlerin oluşturulması için gerekli motivasyon daha hızlı ve daha güvenli şifreleme istenmesinden sağlanmaktadır. Bu nedenle literatürde sürekli yeni çalışmalar eklenmekte olup örneğin ikili cisimler üzerindeki en güncel çalışmalar (Kohel 2012) ve (Kohel 2017) olmuştur.

Çizelge 7.1 ikili sayı cisimleri üzerindeki sistemleri karşılaştırmaktadır. Çeşitli modellerle ilgili karşılaştırmalar için (Hışıl 2010), (Fouotsa ve Diao 2017), (Diao ve Fouotsa 2015) ve (Cohen ve Frey 2006) kaynakları incelenebilir. Modeller arasında karşılaştırma yaparken doğal olarak tek kriter maliyet hesapları değildir, başka faktörler de göz önünde bulundurulmalıdır. (Foutosa ve Diao 2017) çalışmasındaki temel amaç theta fonksiyonları ile eliptik eğriler arasındaki ilişkiyi grup yapısını koruyarak vermek olduğu için maliyet hesapları ikinci planda kalmıştır, bu nedenle yeni theta modelinin toplamada 4 seviyeli theta modelinden biraz daha yavaş olması bu nedene bağlanabilir. Çizelge 7.1 kare alma işlemi olan S'nin çarpma işlemi olan M'ye göre çok daha az maliyetli bir işlem olduğu dikkate alınarak incelenmelidir.

Sadece ikili cisimler değil, karakteristiği tek sayı olan cisimler üzerinde tanımlı eliptik eğriler, grup yapısı ve etkili hesaplamayla ilgili olarak geniş kapsamlı bir çalışma

(Hışıl 2010) doktora tezi olup ilgili tezin 112. sayfada eliptik eğrilerin farklı modellerinin maliyet karşılaştırılmaları yapılmıştır.

KAYNAKLAR

Bernstein, D., Lange, T., (2007) Faster Addition and Doubling on Elliptic Curves, ASI-ACRYPT, 29-50.

Bernstein, D. J., Lange, T., Farashahi, R., Binary Edwards curves. In: Cryptographic Hardware and Embedded Systems—CHES.(2008), 10th International Workshop, Washington, D.C., USA, August 10-13, (2008). *Proceedings, Lecture Notes in Computer Science*, pp. 244–265. *Springer.*

Kohel, D., (2012) Efficient Arithmetic in Elliptic Curves in Characteristic 2, INDOCRYPT 2012.

Kohel, D., (2017) Twisted $\mu 4$ Normal Form for Elliptic Curves, EUROCRYPT 2017.

Cohen, H., Frey, G., (2006) Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman&Hall/CRC.

Diao, O., Fouotsa, E., (2015) Arithmetic of the Level Four Theta Model of Elliptic Curves, *Afr. Math.* 26:283-301.

Edwards, H., (2007) A Normal Form for Elliptic Curves, *Bulletin of the American Mathematical Society*. 44(3): 393-422.

Fouotsa, E., Diao, O.,(2017) A Theta Model for Elliptic Curves. *Mediterr. J. Math.,* 14:65, DOI: 10.1007/s00009-017-0840-y1660-5446/17/020001-16.

Hısıl, H., Koon-Ho, W., Carter, K., Dawson, G., Eds (2009) Jacobi Quartic Curves Revisited, Information Security and Privacy, 14th Australasian Conference, ACISP 2009, Brisbane-Avustralya, Springer, *Proceedings, Lecture Notes in Computer Science*, 452-468.

Hışıl, H., Elliptic Curves, Group Law and Efficient Computation. Quennsland University of Technology, Avustralya, Doktora Tezi.

Mumford, D., (1966) On the Equations Defining Abelian Varieties-I, *Inventiones Math.*, 1, 287-354

Muş, K., (2009) Eliptik Eğri Kriptolojisi için Alternatif bir Eliptik Eğri Formu: Edwards Eğrileri. Orta Doğu Teknik Üniversitesi, Yüksek Lisans Tezi.

Smart, N. P., (2001).The Hessian form of an elliptic curve. In: Cryptographic Hardware and Embedded Systems—CHES (2001), Third International Workshop, Paris, France, May 14–16, , *Proceedings, Lecture Notes in Computer Science*, 118–125. *Springer.*

Silverman, J., (2016) The Arithmetic of Elliptic Curves, *Springer*.

ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Bayram Yaşar

Doğum Yeri ve Tarihi : Kırşehir / 1989

Eğitim Durumu

Lisans Öğrenimi : Adıyaman Üniversitesi, Matematik

Bildiği Yabancı Diller : İngilizce

İş Deneyimi

Çalıştığı Kurumlar : Özel İstanbul Temel Lisesi

Kavram Koleji

İstanbul Kurs Merkezi

İletişim:

Adres : Osmangazi/Bursa

E-posta Adresi : bayrammatematik40@gmail.com

Tarih: 20/11/.2019