MARMARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

LATİSLER ÜZERİNDE KRİPTOLOJİ VE NTRU KRİPTOSİSTEMİ

MEHMET SEVER

720916001

DOKTORA TEZİ
Matematik Anabilim Dalı

Matematik Programı

DANIŞMAN

Prof. Dr. Ahmet Şükrü ÖZDEMİR

İSTANBUL, 2020

MARMARA UNIVERSITY

INSTITUTE FOR GRADUATE STUDIES IN PURE AND APPLIED SCIENCES

CRYPTOLOGY ON LATTICES AND NTRU CRYPTOSYSTEM

MEHMET SEVER

Ph.D. THESIS

Department of Mathematics

Thesis Supervisor

Prof. Dr. Ahmet Şükrü ÖZDEMİR

ISTANBUL, 2020

ÖNSÖZ

Yaşadığımız çağa verilen yaygın isimlerden birisi de “dijital çağ”dır. Çağımızın bu isimle anılmasının temel etkeni bilgisayar ve yazılımlardır. İyi bilinmelidir ki her bilgisayar yazılımının en alt katmanında mutlaka bir matematiksel modelleme veya formülasyon yatmaktadır. Açıktır ki birbirini olumlu anlamda etkileyen bu iki disiplin (bilgisayar ve matematik) geleceği birlikte inşa edeceklerdir. Bir bilgisayar yazılımının veya uygulamasının güvenliği, altında yatan matematik modele ve cebirsel denkleme dayanmaktadır. Buradan hareketle, bilgisayarın gelişimi ve büyüyen soyut matematik evreni ile birlikte sanal gerçeklik hayatımızda daha fazla yer alacaktır denebilir.

Bu mütevazı eser de gelecekte var olmayı hedefleyip dijital dünyaya bir katkı sunmayı hedeflemektedir.

Kasım 2020 **Mehmet SEVER**

İÇİNDEKİLER

ÖNSÖZ i

İÇİNDEKİLER ii

ÖZET viii

ABSTRACT ix

YENİLİK BEYANI x

TEŞEKKÜR xi

ŞEKİLLER xii

TABLO LİSTESİ xiii

1. GİRİŞ 1

1.1 İlkçağda Şifreleme 4

1.2 Orta çağda Şifreleme 6

1.2.1 Vigenere cipher 6

1.3 Etimolojik Kriptoloji 6

1.4 Modern Kriptolojinin Temelleri 7

1.5 Kriptolojik Modelleme 8

1.5.1 Karakterler 8

1.5.2 Temel bir senaryo: kriptosistem 9

1.6 Bir Kriptosistemi Kırmak 11

1.7 Mükemmel-Gizli Şifreleme (Perfectly-Secret Encryption) 12

1.8 Açık Anahtar Kriptosistemler 14

1.8.1 Açık anahtar kriptosistemlerin matematiksel modellemesi 14

1.9 Kriptografi ile Modern Kriptografi Karşılaştırması 15

1.10 Şifrelerin Matematiği 16

1.10.1 Afin şifreleme 17

1.10.2 Blok şifreleme ve Hill şifrelemesi.....19

1.10.3 Üstel şifreleme 22

1.11 Rivest-Shamir-Adleman (RSA) Kriptosistemi 24

1.11.1 Şifreleme-deşifreleme prosedürü 25
1.11.2 Sistemin temelini oluşturan matematik 25
1.11.3 RSA sistemine saldırı 28
1.11.4 RSA sisteminin etkinliği ve hızı 28
1.12 Elgamal Kriptosistemi 29
1.12.1 $m \in G$ yi şifreleme safhası 29
1.12.2 Deşifreleme safhası 29
1.13 Dijital İmza 31
1.14 Knapsack (Sırt Çantası) Tabanlı Kriptosistemler 31
1.14.1 Altküme toplamı 31
1.14.2 Şifreleme 32
1.14.3 Deşifreleme 33
1.14.4 Deşifreleme neden doğru çalışır? 33
1.15 Tezin Amacı ve Vizyonu 34
1.16 Tezin İçeriği ve Kapsamı 35
2. MATEMATİKSEL ALTYAPI.....37
2.1 Polinom Halkaları 42
2.2 Halkaların Yapısı ve Özellikleri 43
2.3 Cisimlerin Yapısı ve Özellikleri 44
2.4 Halkalar Üzerinde Polinomlar 44
2.5 Cisimler Üzerinde Polinomlar 45
2.6 İndirgenemez Çarpanlar Bulmak 47
2.7 İndirgenemez Çarpanlara Ayrışımın Yegane Olmadığı Bazı Halklar 47
2.8 Galois Halkaları ve Cisimleri 48
2.9 Sonlu Cisimlerin Yapısı ve İnşası 48
2.10 Döngüsel Polinomlar ve Birimin Kökleri 51
3 KOD BAZLI KRİPTOSİSTEMLER 53
3.1 Kod Teorisi 53

3.1.1 Kodlama teorisinin temel amacı 53
3.2 Blok Kodlar ve Üreteç Matrisleri 55
3.3 Devirli Kodlar 56
3.4 McEliece Kriptosisteminin Matematiği 59
3.4.1 Dekodlama nasıl çalışır? 59
3.4.2 McEliece kriptosisteminin ayırt edici özellikleri 60
3.5 Kriptolojik Bir Sistemde Kullanılmaya Uygun Olan Kodların Özellikleri 60
3.5.1 Halkalar üzerinde devirli kodlar 60
3.5.2 Birimin kökleri ve kodlama teorisindeki önemi 63
4 LATİSLER ÜZERİNDE KRİPTOLOJİ VE NTRU KRİPTOSİSTEMİ 64
4.1 Latislere Giriş 64
4.2 Latis Problemleri 64
4.3 Latis Tabanlı Sistemler 65
4.3.1 Ajtai-Dwark kriptosistemi 65
4.3.2 Goldwasser-Goldreich-Halevi kriptosistemi 65
4.4 İlk Önerilen Latis Tabanlı Kriptosistem: GGH Kriptosistemi 66
4.4.1 Anahtar üretimi 66
4.4.2 Şifreleme 66
4.4.3 Deşifreleme 66
4.5 İdeal Latisler 67
4.5.1 İdeal latislerin inşası 67
4.6 Döngüsel Latisler 68
4.7 Latis Tabanlı Sistemden NTRU' ya Geçiş 68
4.8 $x^n - 1$ Polinom Parçalanışı ve NTRU Sistemine Etkisi 70
4.9 NTRU Kriptosistemi 70
4.10 NTRU' nun Cebirsel Altyapısı 72
4.10.1 Tanımlar ve notasyon 72
4.10.2 NTRU kriptosisteminin parametreleri ve kullanılacak notasyonlar 74

4.11 Anahtar Üretimi 75
4.11.1 Şifreleme 75
4.11.2 Deşifreleme 76
4.11.3 Deşifreleme neden doğru çalışır? 76
4.12 Hata Polinomu r nin Seçimleri 78
4.13 Parametreler N, p, q ve d_f, d_g seçimleri 78
4.14 f ve g Anahtarlarının Seçimi 79
4.15 m Mesaj Polinomunun Seçimine Dair 80
4.16 Özel anahtar f Polinomlarının Bulunması 82
4.17 Latisler ve NTRU Kriptosistemi Arasındaki Bağlantı 85
4.18 NTRU Kriptosistemine Yapılabilecek Kriptolojik Saldırı Türleri 85
4.18.1 CVP metoduyla saldırı 85
4.18.2 Çoklu gönderim saldırısı 86
4.18.3 Kaba güç (Brute force) atağı 87
4.18.4 Ortada buluşma atağı 87
4.18.5 Latis saldırısı 88
4.19 NTRU Türevi ve Çalışmalar 88
4.19.1 Terslenebilir olmayan polinomlar ile NTRU 89
4.20 MATRU Kriptosistemi 90
4.20.1 Sistem nasıl çalışır? 90
4.20.2 Sistemin analizi 91
4.21 QTRU Kriptosistemi 91
4.22 Gaussyen Tam Sayılı Girdili Matrislerle NTRU 91
5 TEZİN İÇERİSİNDE CEVAP ARANAN SORULAR VE AÇIK PROBLEMLER 92
6 GALOİS HALKALARI ÜZERİNDE NTRU 94
6.1 Galois Halkalarının Cebirsel Yapısı 94
6.2 Önerilen Kriptosistem 95
6.2.1 Önerilen sistemin parametreler seçimi 95

6.3 Galois Halkaları Üzerinde NTRU 97

6.3.1 Özet ve sonuçlar 101

6.4 NTRU' ya İki Anahtar Eklenmesi ile Yeni Bir Yaklaşım 103

6.4.1 Deşifreleme safhası 104

6.4.2 Çalışmanın özeti 114

7 NTRU KRİPTOSİSTEMİNİN BAZI GENELLEMELERİ VE ELDE EDİLEBİLECEK DİJİTAL İMZALAR 116

7.1 Yeni Sistemin Parametreler Seçimi 116

7.2 Yeni Sistemde Kullanılacak Notasyonlar 116

7.3 Toplamsal Genelleme Sistemi Nasıl Çalışır? 116

7.4 Çarpımsal Genelleme 119

7.4.1 Sistemi nasıl çalışır? 119

7.5 Koordinat Genellemesi ve Boyut Yükseltme 121

7.5.1 Sistemi nasıl çalışır? 123

7.5.2 Sistemin avantajları 123

7.5.3 Sistemin dezavantajları 123

7.6 Genelleştirmelerden Elde Edilebilecek NTRU Dijital İmzaları 123

8 SONUÇLAR, TEZİN ÇIKTILARI VE SENTEZ 125

9 TARTIŞMA 128

10 ARAŞTIRMACILAR İÇİN GELECEK PERSPEKTİFİ VE ÖNERİLER 131

11 KODLAR 132

11.1 NTRU Kriptosisteminin İşleyişine Dair Algoritmik Bir Örnek 132

11.2 NTRU Kriptosisteminde Modül Parametresinin Büyütülmesine Dair Algoritmik Bir Örnek.....135

11.3 NTRU Kriptosisteminde Mesaj Polinomuna Rotasyon Uygulanışına Dair Algoritmik Bir Örnek 140

11.4 NTRU Kriptosisteminde Mesaj Polinomuna Rotasyon ve İzomorfizma Etkisinin Birlikte İşleyişine Dair Algoritmik Bir Örnek 146

11.5 NTRU Kriptosisteminin Galois Hlakları Üzerindeki İşleyişine Dair Algoritmik Bir Örnek 151

11.6 NTRU Kriptosisteminde m Mesaj Polinomuna Bir İzomorfizma Etkisi ve İşleyişine Dair Algoritmik Bir Örnek 156

11.7 NTRU Kriptosisteminde Modüllerin Polinom Olarak Seçilmesine Dair Algoritmik Bir Örnek 162

11.8 NTRU Kriptosisteminde Modüllerin Polinom Olarak Seçilmesine Dair Algoritmik Bir Örnek 169

KAYNAKLAR 176

ÖZGEÇMİŞ 184

ÖZET

LATİSLER ÜZERİNDE KRİPTOL0Jİ VE NTRU KRİPTOSİSTEMİ

1996 yılında, J. Hoffstein, J. Pipher ve diğerleri tarafından ilk kez sunulan bir açık anahtar kriptoloji sistemi olan NTRU' ya cebirsel ve algoritmik yönden sistemin güvenlik düzeyini geliştirmeye yönelik katkı sağlanması amaçlanan bu tez çalışmasında aşağıdaki bulgular elde edilmiştir.

1. Mevcut kriptosistem, Galois halkaları üzerinde ele alınarak daha fazla sayıda parametre ve anahtar ilave edilmiştir.
2. NTRU polinom halkasına bir modül olarak yaklaşılıp bu cebirsel yapının kriptosisteme sağlayacağı avantajlar incelenmiştir.
3. Kriptolojik sistem toplamsal, çarpımsal ve boyut olarak n. güvenlik düzeyine yükseltilerek yeni bir dijital imza türü elde edilmiştir.
4. NTRU kriptosisteminin uygun seçilen bir parametre ilavesi ile diğer popüler açık anahtar bir sistem olan RSA' nın sisteme dahil edilerek sistemin güvenlik düzeyi daha da artırılmıştır.

Kasım 2020 **Mehmet SEVER**

ABSTRACT

CRYPTOLOGY ON LATTICES AND NTRU CRYPTOSYSTEM

The following results are obtained in this thesis which is aimed to contribute to the public-key cryptosystem NTRU being originally presented by J. Hoffstein, J. Pipher et al in 1996, towards improving the security level of the system in terms of algebraic and algorithmic.

1. More parameters and keys are added by analyzed available cryptosistem on Galois rings.
2. The polynomial ring NTRU is approached as a modulo and the provided advantages to the algebraic cryptosystem are researched.
3. A new type of a digital signature is obtained by enhancing the cryptologic system to the nth security level as summative, multiplicative and dimension
4. The security level of the system is increased by incorporating in the system the another popular public-key system RSA with the addition of a properly chosen parameter of the NTRU cryptosystem.

November 2020 **Mehmet SEVER**

YENİLİK BEYANI

Bu tezin içerisindeki hiçbir çalışma daha önce bir yükseköğretim kurumunda veya enstitülerde sunulmamıştır. Atıf vermeksizin, bire bir bilgi, bulgu ve yorum alınmamştır. Diğer tüm ifadeler, önermeler ve bulgular tarafımdan ve bilimsel etiğe ve metodolojiye uygun olarak işlenmiştir. Bu bağlamda tezden ikisi uluslararası alan indeksli(mathscinet) ve birisi de sci indeksli toplam üç adet yayın türetilmiştir.

Mehmet SEVER

10.11.2020

TEŞEKKÜR

Bu tezin ortaya çıkmasında, ilk aşamasından son safhaya kadar destek, bilgi ve tecrübelerini esirgemeyen değerli danışmanım Prof. Dr. Ahmet Şükrü ÖZDEMİR hocama en içten teşekkürlerimi sunmayı bir borç bilirim. Kendilerinin gösterdiği hedef ve çalışma teşvikleri, gayretlendirmeleri, cesaretlendirmeleri olmasaydı bu eser ortaya çıkamazdı. Bir teşekkür de bölüm hocalarım olan Prof. Dr. Ünsal TEKİR' e, Prof. Dr. Uğur ŞENGÜL' e ve tez izleme jürimde bulunan hocam Prof. Dr. Bayram Ali Ersoy'a etmek isterim. Aldığım derslerden, sunduğum tez raporları sürecinin sonuna kadar manevi desteklerini hep yanımda hissetim. Ve elbette hususi bir teşekkürü de aileme sunmak zorundayım. Maddi ve manevi desteklerinden ötürü…

Mehmet SEVER

M. Talha’ma ithafen…

ŞEKİL

Şekil 1.1 Şifreleme Türleri …… 8

Şekil 1.2 Alice ve Bob bir kriptosistem kullanıyorlar …….... 9

Şekil 1.3 Alice ile Bob simetrik bir kriptosistem kullanıyorlar ……. 9

Şekil 1.4 Alice ile Bob açık anahtar kriptosistem kullanıyorlar ...…….... 10

Şekil 1.5 Eve şifreli metin saldırısı yapıyor ……. 10

Şekil 1.6 Eve bilinen metin atağı düzenliyor ……... 11

Şekil 1.7 Eve seçilmiş düz metin atağı yapıyor ……... 11

Şekil 1.8 ……..…… 12

Şekil 1.9 ……..... 13

Şekil 6.1 ……..... 107

Şekil 6.2 ……..... 110

TABLO LİSTESİ

Tablo 1.1 …… 2

Tablo 1.2 …… 5

Tablo 1.3 ……..... 6

Tablo 1.4 $C \equiv 7P + 10\ (mod\ 26)$ kuralına göre yeni alfabe ……. 18

Tablo 1.5 İngiliz alfabesinde harflerin kullanım sıklığı ……... 19

Tablo 1.6 Harflerin ikilik dijital gösterimleri ……..... 22

Tablo 6.1 Önerilen NYTU şeması ……..... 102

Tablo 6.2 ……..... 107

1. GİRİŞ

Kriptografi, gizli mesajları, belirlenmiş bir alıcı dışındaki hiç kimsenin görememesini sağlayan bir şifreleme ve deşifreleme çalışmaları metodolojisidir. Kriptanaliz ise izni olmadığı halde mesajı almayı ve deşifre etmeyi, kodu kırmayı esas alan çalışmaları kapsar. Kriptografide alıcıya bir anahtar verilirken kriptanalizde kod kırıcı bu anahtar olmadan bilgiyi elde etmeyi amaçlar. Anahtar, mesajın hangi özel şartlar altında şifrelendiğinin ve nasıl deşifre edileceğinin ipuçlarını vermeye yarar. Kriptoloji çalışmaları ise hem kriptografi hem de kriptanaliz metodlarını kapsar **[1].**

Oxford İngilizce Sözlüğü kriptografiyi şu şekilde tanımlar:

> "Harfleri veya karakterleri alışılagelmişin dışında kullanarak yazmak, sadece zeki insanların kullanabildiği bir yöntem, genel olarak şifre yazma ve kırma sanatıdır."

Kriptografi her ne kadar antik bir sanat dalı olsa da son otuz yılda yapılan çalışmalarla sadece bir şifre yazmanın ve onu kırmanın etkinliği olmadığını yani yukarıdaki tanımı boşa çıkaran onlarca gelişmeye sahne olmuştur. Örneğin, kişisel web sayfasına girip değişiklikler yapmanın ilk şartı sayfa yöneticisi olduğunuzun güvenlik adımları sonucunda ispatı gerekmektedir ki bu da kriptografik protokoller sürecidir.

Bilgisayarın icadı ve hızla yayılmasından itibaren bilginin hızlı ve güvenliği kavramları da lügatimize girmiştir. Sadece kişilerin kullandığı bu cihazlar devlet kurumları ve güvenlik ajansları gibi çok önemli kurumlarda da kullanıldığından kriptografi bir bilim dalı olarak kendisini kabul ettirmiş ve hızla gelişmesine devam etmektedir. Matematik altyapısını matematikçilerin kurduğu kriptografik protokoller, bilgisayar bilimciler tarafından da ataklarla sınanıp güvenlik düzeylerinin kontrol edilmesiyle kendi alt bilim dallarını dahi oluşturmuştur **[2].**

Temel olarak iki tür kriptografik mesaj gönderme yöntemi vardır. Birisi transposition (yerini değiştirme) yöntemi denilen mesajdaki karakterlerin yerini, belirlenmiş bir kurala göre yine aynı karakterlerle değiştirir. Bir diğeri ise substitution (ikame etme) yöntemidir ki mesajdaki her bir karakteri bir başka karakter sistemiyle belirli bir kurala göre dönüştürür **[1].**

Bu tezde de daha ziyade ikame etme yöntemi kullanılacaktır. Bu yöntemin etkin kullanılabilmesi için cebirsel teorem ve konuların sık kullanılacağı aşikârdır. Bu sebeple

bazı cebirsel yapı, tanım ve teoremleri okuyucuya aşina kılmak adına araştırma bulguları kısmından hemen önce verilecektir.

Yerini değiştirme metotlarında temel prensip alfabe harflerinin seçildiği kümenin bir permütasyonu olan bir f belirleyip bu f permütasyonu ile her bir x harfini alıp $f(x)$ ile belirtmektir. Bu şekilde belirlenen f permütasyonuna anahtar (key) denmektedir. Misal olarak, varsayalım ki

$$ALGEBRA\ IS\ GREAT\ FUN$$

mesajını arkadaşımıza göndereceğiz. Mesajı sadece arkadaşımızın görmesini istediğimizden ayırt edici bir anahtar seçmemiz gerekir. Bu f yi şu şekilde belirlediğimizi varsayalım;

Tablo 1.1.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	F	P	R	K	S	C	E	L	A	J	Q	G	T	B	I	M	D	H	O	X	Z	V	Y	U	W

yani f yukarıdaki harfleri aşağıdakine dönüştürüyor olsun. Mesajımızı bu f kuralına göre yazarsak,

$$NQCKFDNLHCDKNOSXT$$

olur. Biz bu şifreli mesajı arkadaşımıza f gizli anahtarı ile gönderdiğimizden o da $f^{-1}(y) = x$ kuralına göre deşifreleme yaparak açık metne ulaşır. Bir atak niyetinde olan yetkilendirilmemiş bir katılımcı bir mesaja ancak muhtemelen tüm permütasyonları deneyerek ulaşacaktır. Fakat İngiliz alfabesindeki harflerin permütasyonlarının sayısı

$$26! = 403291461126605635584000000 \approx 4.10^{26}$$

dır. Bu sayının ne kadar büyük olduğunu izaha gerek yoktur. Eğer saldırgan her bir permütasyonu bir saniyede deniyor olsa bile 10^{19} yıl sonra ancak doğru permütasyonu bulabilecektir. Buradan hareketle noktalama işaretleri, büyük-küçük harf, numaralar vesaire kullanılması durumunda düzenlenecek olan atağın çaresizliği hayli derecede artacaktır **[1]**.

Şimdi terminolojiden bahsedilecek olursa, mesajın ilk orijinal haline plain text (düz metin) denir. Gönderilmiş mesaja ciphertext (şifreli metin) denir. Düz metni şifreli metne dönüştürme süreçlerine encryption (şifreleme) denir. Ulaşılmış şifreli metni revize ederek düz metne ulaşmaya ise decryption (deşifreleme) denir. Tüm bunları içinde barındıran özel bir şifreleme işlemine cryptosystem (kripto sistem) denir. Düz metni yazarken kullanılan karakterlere alfabe denir. Bu bir dil alfabesi olabileceği gibi bir sayı sistemi vesaire de olabilir. Bu bağlamda şifre alfabesi ile düz metin alfabesi aynı olmak zorunda değildir. Mesela düz metin alfabesi $A, B. \dots, Z$ olup şifreli metin alfabesi $1, 2, \dots, 26$ olabilir. Şimdi $\mathcal{A}$ ve $\mathcal{B}$ sırasıyla düz metin alfabesini ve şifreli metin alfabesini göstersinler. Bir $f: \mathcal{A} \to \mathcal{B}$ içine dönüşüm olsun ($\mathcal{A}$ ile $\mathcal{B}$ aynı sayıda eleman içeren kümeler ise f üzerinedir). Eğer düz metindeki her bir x karakteri $f(x)$ ile şifreli metne dönüşüyorsa f ye şifreleme anahtarı ya da sadece anahtar (key) denir. f birebir olduğundan bir $g: Imf \subset \mathcal{B} \to \mathcal{A}$ vardır öyle ki $g\big(f(x)\big) = x,\ \forall x \in \mathcal{A}$ böyle bir g dönüşümüne de deşifreleme anahtarı denir. Şifreli metindeki her bir y karakteri $g(y)$ ile değiştirilirse düz metin kurtarılmış olur. Böyle bir şifreleme prosedürüne yerine ikame etme (simple substitution cipher) şifrelemesi denir. Bu tarzdaki şifrelemelerin bir dezavantajı da şudur; örneğin İngiliz alfabesinde hangi harflerin ne sıklıkta kullanıldığı veya hangi harflerin hangi harflerle bir araya gelerek anlamlı sözcükler oluşturduğu istatiksel analiz yöntemleriyle belirlenmiştir. Şayet yeteri kadar uzun bir metin şifrelenip gönderilmişse deşifreleme safhasında metni bulmak kolay olacaktır. Bu sebepten şayet bu yöntem kullanıldıysa ya anahtarlar fazla sayıda seçilmelidir ya da sürekli güncellenmelidir. Her seçilen yeni anahtar alıcıya gönderilmelidir. Tek anahtarlı şifreleme algoritmalarında risk daha fazla olduğundan çok sayıda anahtar kullanılmalıdır. Bu şekilde muhtemel tüm anahtarlar kümesine anahtar uzayı (key space) denir **[1]**. Eğer anahtar uzayı yeteri kadar büyük seçilmez ise kod kırıcılar tarafından kırılmaları kolay olacaktır. Böyle bir güçlü şifreleme algoritmasını üretmek için güçlü cebirsel yapılardan esinlenilebilir. Örnek olarak halka, cisim, modül ve benzeri yapılar üzerine komplike cebir teoremleri ile daha güçlü algoritmalar yazılabilir.

Bu bilimler askeri haberleşmeler için hep önemli olagelmiştir. Bugün ise hem finansal yöntemlerde hem de kişisel bilgilerimizin korunmasında bilgisayar çağının getirdiği dijitalleşme sebebiyle daha da önemli bir durumdadır. Örneğin, telefon sim kartlarında kişiye özel belirlenen Personal Identity Number (PIN) sadece yetkili kurum ve kullanıcı kişi arasında kalması gereken bir sayıdır. Ya da sesten kişiyi ayırt eden aygıtların her kişinin sesini uygun bir kod ile gizlemesi örneği de verilebilir. Ayrıca pratik olmasından

ötürü hemen her kalabalık cadde ve avmlerde bulunan ATM cihazları sadece hesap sahibinin erişebileceği bir şifre ile çalışmaktadır. Aksi halde kişinin kendi parasını başkaları da alıp kullanabilirdi. Devletlerin vergi veri tabanları da halklarının zamanı geldiğinde vergi borçlarını verip vermediklerini kayıt altına alan bir sistemdir. Vatandaşlarının özlük haklarını ve kişisel bilgilerini güvence altına almak isteyen devlet kurumları güçlü altyapılara sahip kriptosistemler kullanmaktadırlar. Bir başka kriptografi kullanılan merci ise bahis ve loto şirketleridir. Kazanan kişinin ve şanslı numaranın haklarının zayi olmaması, bir başka numaraya verilmemesi ya da şanslı kişinin hile yapıp iki defa talepte bulunmaması gibi sebeplerle kriptografi bu alanlarda da kullanılmaktadır.

Tam da bu noktada kriptografiyi amaçları üzerinden tekrar tanımlamak gerekirse, şu dört temel özellik kriptografik bir sistemin olmazsa olmazıdır:

1. Tutarlılık; paylaşılan bilginin sadece izin verilmiş alıcıların ulaşmasının sağlanması durumu,
2. Bilgi bütünlüğü; paylaşılan bilginin herhangi bir kanaldan değiştirilmediği veya eksiltilmediği şartı,
3. Yetkilendirme; bilginin, sisteme sadece tanımlı veya izin verilmiş bir kullanıcı tarafından girilmesi şartı,
4. Tekrarsızlık; özellikle finans alanlarında kullanılan ödeme sistemlerinin tekrarlı harcamalara izin vermemesi ilkesi.

Peki bunca sır, gizem, yalanlar ve aldatılmalar karşısında gerçekten nasıl emin olabiliriz? Göndermek istediğimiz bilginin, sırrın ve mesajın nasıl olur da sadece almasını istediğimiz alıcının aldığından emin olabiliriz? Ya da elimize ulaşan bilginin gerçek olduğuna, kaynağının doğru olduğuna ve bilginin bütünüyle bize ulaştığına kesin derecede nasıl ikna olabiliriz? İşte tüm bu kuşkular artarak devam etmiştir ki insanlık gizliliğe ve güvenliğe hiç olmadığı kadar önem atfetmektedir. Öyle görünüyor ki kriptografi cazibesini artırarak büyümeye devam edecektir.

1.1. İlkçağda Şifreleme

Güçlü cebirsel yapılar üzerine kurulu şifreleme türlerine geçmeden evvel, tarihteki ilk ve yüksek cebir bilgisi gerektirmeyen bir şifreleme yöntemini anlatalım. Tarihsel süreci bakımından da ilginç olan bu yöntem, adını antik çağlarda yaşamış Roma imparatoru Julius Caesar' dan alır. Çünkü yöntemi ilk kullanan O' dur. Hayal edelim ki alfabenin

harfleri bir daire etrafına dizilmiş olsunlar. Eğer her bir harfi k adım sonrasına ötelersek yeni oluşan dizilime k uzunluğundaki devirsel öteleme ya da sadece k −ötelemesi (k −shift) denir. İşte bu şekilde yapılan şifrelemelere öteleme şifrelemesi (shift cipher) ya da Sezar şifrelemesi denir. Sezar' ın ilk uyguladığı bu yöntemde $k = 3$ alınmıştı. Yani bu durumda A harfi D ye, B harfi E ye, C harfi de F ye ve benzeri öteleniyordu. Aşağıdaki tablo $k = 3$ Sezar şifrelemesinde harflerin permütasyonunu göstermektedir.

Tablo 1.2.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Örnek vermek adına; $k = 3$ için aşağıdaki mesaj yukarıdaki tabloya göre şifrelensin.

$$ROMAYI\ YAKIN$$

Yukarıdaki tablodan ve boşluklar da yok sayılarak

$$URPDBLBDNLQ$$

şeklinde bir şifreli metne ulaşılır. Ayrıca aşağıdaki metin deşifre edilirken yukarıdaki tabloya göre $k = 3$ için her harf üç öncesine taşınır;

$$URPD\ BLNLOGL$$

$$ROMA\ YIKILDI$$

Sezar' ın şifresini kırmak açıktır ki basit olmasına rağmen kendi zamanında hiç kimse bunu başaramamıştır. Muhtemelen nasıl şifrelendiğini tahmin edemediklerinden anahtarı da bulamadılar. Öteleme tipi şifrelemede key (anahtar) detaylı bir anahtar kümesi analiziyle elde edilip mesaja ulaşılabilir **[3].**

Örnek 1.1 Aşağıdaki metin öteleme yöntemiyle şifrelenmiştir. Uygun anahtarı elde ederek deşifre etmeye çalışınız.

$$UIBPMUIBQKAQAMIAG$$

Şayet öteleme tipi bir şifreleme yapılmış ise $k = 1, 2, ...$ için anlamlı sözcükler elde edene kadar anahtar araştırması yaparak $k = 8$ için

$$MATHEMATICS\ IS\ EASY$$

sonucu elde edilir.

1.2. Orta Çağda Şifreleme

1.2.1. Vigenere cipher

Tarihler 16. yüzyılı gösterdiğinde Fransız kriptolojist Claise de Vigenere yerini değiştirme şifrelemesinin bir kompozisyonu olan periyodik öteleme şifrelemesi yöntemini tanıttı. Bu yönteme göre periyodu P olan bir anahtara $(k_1, k_2, \dots, k_P)$ dersek şifelenmek istenen metin P uzunluğuna bölünür ve P liler halinde şifrelenir. Bu yöntemde anahtar genelde bir sözcük alınır. Anahtar sözcüğe göre alfabe yeniden sıralanır ve oluşan tabloya göre şifreleme işlemi tamamlanır. Örneğin aşağıdaki tablo PARIS anahtar sözcüğüne göre Vigenere şifresini belirtir.

Tablo 1.3.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R

Bu tabloya göre $SEND\ MORE\ MONEY$ mesajını şifrelersek periyodu 5 olarak verildiğinden metni 5 li öbeklere ayırıp yeni oluşan permüte sıralamaya göre şifreleyelim. Sırasıyla $SENDM \rightarrow HEELE$ ardından $OREMO \rightarrow DRVUG$ ye ve son üç harf $NEY \rightarrow CEP$ ye dönüşür. Böylece şifreli metin $HEELEDRVUGCEP$ olur **[4]**.

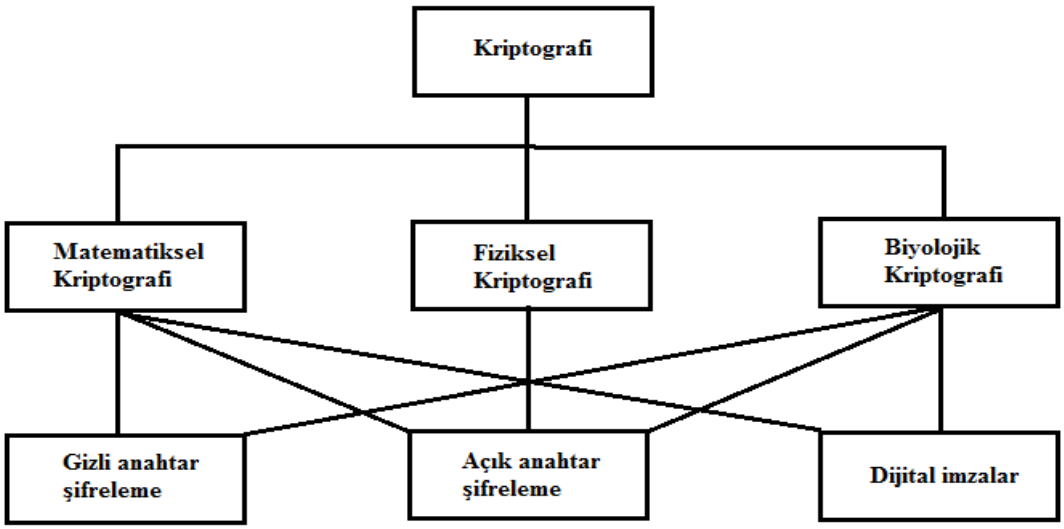
1.3. Etimolojik Kriptoloji

Kriptoloji (cryptology) sözcüğü, Yunanca gizli anlamına gelen kryptos ve kelime anlamına gelen logos sözcüklerinden oluşur. Terim ilk defa 1645 yılında James Howell tarafından kullanılmıştır. Buna karşın John Wilkins (1614-1672) "Mercury, or the Secret and Swift Messenger" adlı kitabında cryptologia ve secrecy sözcüklerini kullanmıştır. Tarihler 1967 yılını gösterdiğinde ise "The Codebreakers" adıyla yayınlanan ansiklopedik kitapta cryptology ve cryptanalysis sözcükleri kullanılan anlamları ile literatüre girmiştir.

Tarihte kayıt altına alınmış ilk kriptografi tekniği yaklaşık 4000 yıl önce Khnumhotep adında bir Mısırlı yazıcı (çizici) tarafından bir kaya yüzeyine uygulanmıştır. Kullandığı yöntem, o günün harfleri yerine hiyeroglif sembollerle metni herkesin anlayamayacağı bir forma sokmaktı. Tekniğin uygulandığı kaya bir mezar taşı olarak zamanın Mısır Firavunu II. Amenemhet' in mezarını süslemiştir. Ölen firavunun amacı elbette gizlilik değildi. Sadece asillik ve soyluluk gösterisinde bulunmak idi. Anlaşıldığı üzere modern kriptolojinin temel amacı olan gizlilik yerine soyluluk amaçlanarak tasarlanmış bir yöntemdir **[5].**

1.4. Modern Kriptografinin Temelleri

Bahsedildiği üzere kabaca 5000 yıllık bir geçmişi olan kriptografiyi 1970' lerden itibaren baz alırsak modern kriptografik yöntemleri kastediyor olacağız. Aslında modern kriptografi, büyük oranda ileri ve sofistike matematiksel temellere dayanır. Bu sebeple matematiksel kriptografi tabirini bile kullanabiliriz. Yine de kuantum fiziğine dayalı kuantum kriptografi ve moleküler biyolojiye dayanan biyolojik kriptografi (DNA) modelleri de mevcuttur. Modern kriptografinin temel karakteristik özelliği ise e, d gibi iki anahtarın simetrik anahtar yöntemlerinde olduğunun aksine birbirlerinden polinom-zamanlı hesap edilememeleridir. Yani simetrik anahtar da $e = 1/d$ olması hasebiyle bir anahtarın diğerinden elde edilebilmesi hesaplama yollarıyla polinom-zamanda mümkün iken açık anahtar (asimetrik) yönteminde ancak eksponensiyal-zamanda mümkün olacaktır. Açık anahtar şifrelemeler sadece bir kriptoloji yöntemi değil ayrıca dijital imza ve dijital para alanlarında da uygulanmaktadır. Modern kriptografiyi anlatan aşağıdaki Şekil 1.1 bu durumu modellemektedir **[6].**



Şekil 1.1. Şifreleme türleri.

1.5. Kriptografik Modelleme

Kriptografik bir protokol denildiğinde akla soyut bir denklem ve algoritmalar silsilesi gelir. Reel dünyadan bir örnekleme yapabilmek için bazı özel görevler yüklenmiş karakterler ve bu karakterler arası süreci model kurarak anlatalım.

1.5.1. Karakterler

Alice ve Bob esas karakterlerdir. Genelde Alice Bob' a gizli bir mesaj göndermek istiyordur. Ayrıca Bob gelen bu mesajı dijital olarak imzalamak ve kaydetmek isteyebilir. Çünkü daha sonra Alice' in asıl gönderdiği mesajın ne olduğu veya hangi tarihte gönderildiği gibi bilgiler hususunda kuşkuya yer bırakmak istemeyebilir. Genellikle Alice ve Bob iyi niyetlidir ama bu garanti altında da değildir. Çünkü bir telefon kulübesinde sahte jeton kullanmak isteyen iki kişi de olabilirler.

Eve iyi niyetli bir gözlemcidir. Gönderilen mesajın ele geçirilip geçirilmeyeceğini, hangi zaman ve ölçüde doğru olarak ulaşabileceğini ölçen ve hatta müdahale edebilen yine iyi niyetli bir karakterdir.

Fred, Alice' in Bob' a göndereceği mesajı engellemek ister veya değiştirmek ister.

Mallory bir saldırgandır. Bilgiyi ele geçirmek ister. Ele geçirdiği bilginin yanı sıra Alice ve Bob' a vereceği zarar bununla da sınırlı değildir. Daha kötüsü mesajı değiştirip gönderebilir. Kriptografideki atnımıyla "man in the middle"dır **[7].**

1.5.2. Temel bir senaryo: kriptosistem

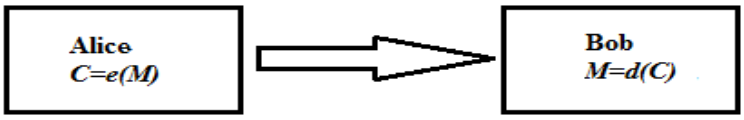
Alice Bob' a gizli bir yoldan bir şifreli mesaj göndermek istemektedir. Kullandıkları temel kriptografik sisteme şifre diyelim. Alice' in göndermek istediği mesaj veya düzmetine M dersek, bir $e(\cdot)$ şifreleme fonksiyonu ile gönderecektir. Bu süreç bir

$$C = e(M)$$

şifreli metni üretecektir. Bob ise bunu bir $d(\cdot)$ fonksiyonu ile deşifre edip

$$d(C) = d\big(e(M)\big) = M$$

sonucunu elde edecektir. Bu süre zarfında Alice ve Bob mesajın doğru aktarıldığından veya ele geçirilmediğinden emin değillerdir.

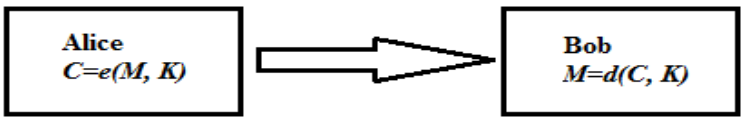


Şekil 1.2. Alice ve Bob bir kriptosistem kullanıyorlar.

Eğer Alice ile Bob sadece bir gizli anahtar belirlemiş iseler simetrik şifreleme yöntemini kullanmışlardır. Bu noktada hemen simetrik şifrelemenin temel bir tanımını verelim.

Tanım 1.1 (Simetrik Anahtar Şifrelemesi) [7] Bir kriptosistem, herhangi iki anahtar ikilisi olarak verilen (k_1, k_2) için şayet biri diğerinden temel cebir yöntemleri ile elde edilebiliyorsa, yani birini biliyorken diğerini de bulmak kolaysa simetrik anahtar kriptosistemi adını alır.

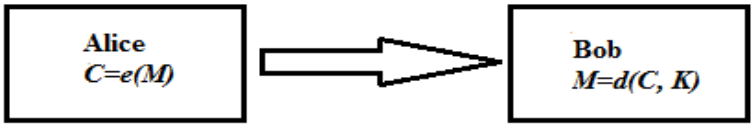
Klasik kriptosistemlerde aslında $k_1 = k_2$ seçilmekteydi. Bir anahtarın ele geçirilmesi sonucunda tüm sistemin çökebileceği bu yöntem bugün pek rağbet görmemektedir.



Şekil 1.3. Alice ile Bob simetrik bir kriptosistem kullanıyorlar.

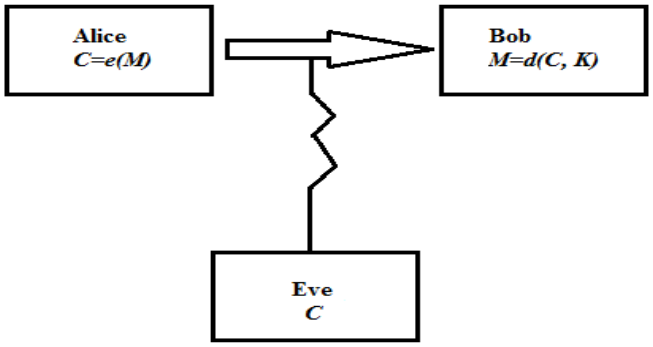
Alice ile Bob' un bu süreçte iletişimini Eve takip ediyor olup tüm bilgiye erişebilir.

Alice ile Bob birden çok gizli anahtar üzerinde anlaşabilirler. Ya da bazen Alice mesajının mutlaka anlaşılmasını istediğinden Bob' un başarısız olma durumunda mutlaka Eve' nin devreye girip mesajı iletmesi adına bir de açık anahtar kullanabilirler. Buna da asimetrik kriptosistem adı verilir.



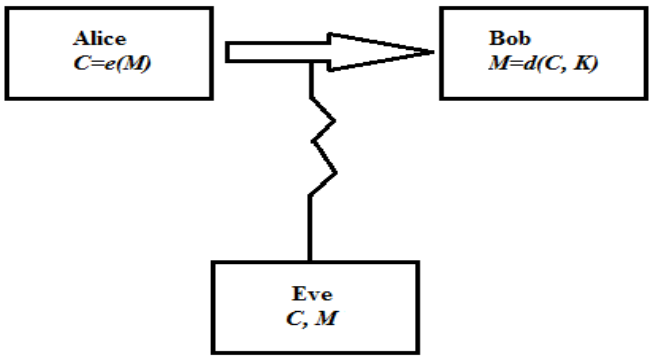
Şekil 1.4. Alice ve Bob açık anahtar kriptosistem kullanıyorlar.

Peki, Eve Bob' un sahip olduğu lakin kendisinde olmayan gizli anahtar sebebiyle mesajı okuyamayacak mıdır? Eve' nin bazı girişimleri olacaktır elbette. Misal olarak elinde C şifreli metni zaten var. Bu metin üzerinden bir atak gerçekleştirebilir. Bu tip ataklara "ciphertext only" atakları denir.



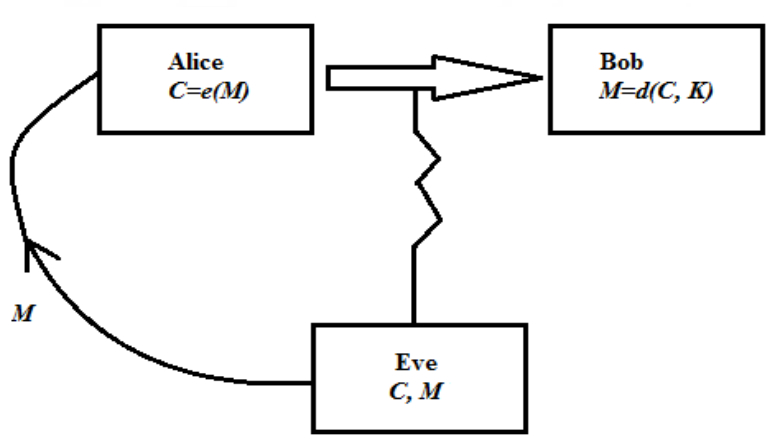
Şekil 1.5. Eve şifreli metin saldırısı yapıyor.

Eve' nin tüm yapacakları bununla da sınırlı değildir. Eve olası bir düz metin seçerek yeni bir atakta bulunabilir. Bu tip ataklara da "known plain text attack" denir.



Şekil 1.6. Eve bilinen metin atağı düzenliyor.

Eve' nin sahip yapabileceği en tehlikeli saldırı asıl metni değiştirmektir. İletişime müdahalede bulunur ve Alice' in yerine metin belirler.



Şekil 1.7. Eve seçilmiş düz metin atağı yapıyor.

Eğer yeteri kadar hesap yapma imkanı ve hızı varsa saldırgan kolayca mesaja ulaşabilir. Açıktır ki gelecekte daha etkili ve kapsamlı saldırı yöntemleri düzenlenebilecektir. Buradan hareketle, modern kriptografi, hesaplama yoluyla kolayca kırılamayan, soyut matematiksel modeller ve yapılar üzerine inşa edilmiş, anahtar uzayı geniş çaplı, komplike ve varyasyonlara açık yeni ve güncel sistemler kurma peşinde denilebilir. görmemektedir.

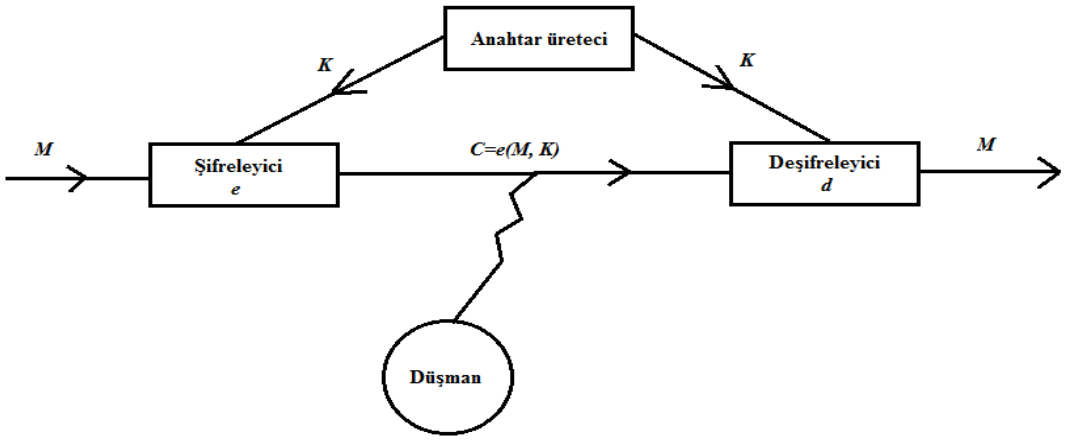
1.6. Bir Kriptosistemi Kırmak

Bir şifreli metni çözmek veya bir kriptosistemi kırmak denilince ne anlaşılır? Bir kriptanalist ya da aslında düşman şifreyi ele geçirmek için bazı bilgilere zaten sahiptir. Örneğin c şifreli metin, hatta e şifreleme dönüşümü bile ele geçirilmiş olabilir. Ayrıca

metnin yazıldığı dil alfabesinin istatiksel analizlerini biliyor olabilir. Ayrıca şanslı ise $\mathcal{K}$ anahtar uzayından bir k anahtarı bile ele geçirmiş olabilir. Ele geçirilen bu k anahtarı d deşifreleme fonksiyonu hakkında bilgi de verebilir. Tüm bu elde etmiş olabileceği bilgiler ışığında bir kriptanalist şu üç yöntemle sistemi kırabilir **[8].**

a) **Şifreli metin-parça saldırısı (ciphertext-only attack):** Bu saldırıda düşman elinde sadece şifrelenmiş metnin bir kısmı vardır. Yani ya gönderici parçalar halinde göndermiştir ya da kod kırıcı sadece bir kısmını çözümleyebilmiştir. En zayıf saldırı yöntemidir.
b) **Bilinen düz metin saldırısı (known plain text attack):** Bu saldırıyı yapabilen düşmanın elinde hem düz metnin bir kısmı hem de karşılık gelen şifrenin bir kısmı bulunmaktadır. Bu yöntemin a) dan daha etkili olduğu aşikardır.
c) **Seçili düz metin saldırısı (chosen-plain text attack):** Bu yöntemde düşman bir çok düz metin ve karşılık gelen şifreli metin çiftini ele geçirmiştir. Elinde bulunan onlarca (M, C) ikilisinden sistemin anahtarını elde etmesi zor olmayacaktır.

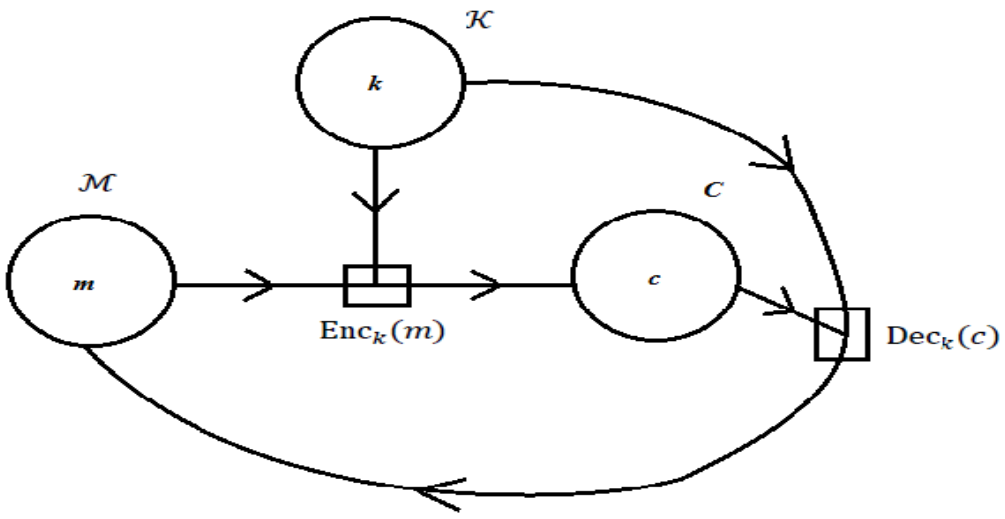
Fark edileceği üzere en saldırgan yöntem c) dir. Klasik şifreleme yöntemlerinin hiçbiri c) saldırısından sağ kurtulamaz. Bu sebeple daha güçlü bir altyapıya oturmuş cebirsel kriptoloji sistemi geliştirilmiştir. Şimdi yukarıda anlatılanları görsel bir sunum halinde Şekil 1.8 de verelim.



Şekil 1.8. Düşman deşifreleyiciden önce mesaja ulaşmak için bildiği tüm verileri kullanarak saldırı düzenliyor.

1.7. Mükemmel-Gizli Şifreleme (Perfectly-Secret Encryption)

Yöntemi tanıtmadan evvel bazı terimlerin açıklanması önemlidir. Bu yöntemde üç algoritma ve bir de özel olarak belirlenmiş bir $\mathcal{M}$ mesaj uzayı vardır. Algoritmalar sırasıyla anahtar üretme algoritması (Gen) ki bir kurala göre dağınık anahtar kümesinden uygun anahtarlar seçer. Anahtarlar kümesine $\mathcal{K}$ denirse $\mathcal{K}$ sonludur ve Gen, $\mathcal{K}$ içerisinden keyfi bir anahtar seçebilir. Diğer bir algoritma da şifreleme algoritmasıdır. Enc şifreleme algoritması bir $k \in \mathcal{K}$ ve $m \in \mathcal{M}$ yi girdi olarak alıp bir C şifreli metnini çıktı olarak verir. Bunu $\text{Enc}_k(m)$ ile gösterelim. Hemen not edelim ki $|m| > 1$ olmalıdır. Aksi takdirde sadece bir mesajı şifreleyip gönderir ve işlem biter, yani algoritma diyalog veya iletişim üretemez. Enc algoritmaları bazen olasılıklarla çalışabilir. Yani farklı zamanlarda farklı şifreli metinler üretebilir. Bu duruma sebebiyet veren temel şey farklı $k \in \mathcal{K}$ lar farklı $c \in C$ ler üretecektir. Bu gibi durumlarda $c \leftarrow \text{Enc}_k(m)$ notasyonu kullanılır. Şayet Enc algoritması kesin belirli ise $c = \text{Enc}_k(m)$ notasyonu kullanılır. Dec algoritması ise bir $c \in C$ ile bir $k \in \mathcal{K}$ yı alıp bir $m \in \mathcal{M}$ üretir. $\text{Dec}_k(c) = m$ olabilmesi için Dec algoritmasının 1 olasılıkla çalışması gerekir. Bazı kompleks yapılı kriptografik algoritmaların olasılıklı sonuçlar üretmesi sebebiyle böyle iyi belirlenmiş $\text{Dec}_k(c) = m$ algoritmalarına mükemmel deşifreleme algoritmaları denir. Mükemmel şifreleme algoritmalarında $|\mathcal{K}| = |\mathcal{M}|$ olması gerekir. $|\mathcal{K}| < |\mathcal{M}|$ durumunda anahtarlar birden çok kere kullanılabileceğinden güvenlik açığı yaşanabilir. $|\mathcal{K}| > |\mathcal{M}|$ durumlarında ise Dec algoritmaları bir $m \in \mathcal{M}$ sonucunu her daim bir $c \in C$ girdisi için net olarak vermeyebilir. Şekil 1.9 bu durumu daha açık ifade etmektedir.



Şekil 1.9. Mükemmel çalışan bir kriptosistem.

Dec algoritmaları $|C| < |\mathcal{M}|$ durumlarında kolay çalışır. Çünkü bir çok mesaj aynı $c \in C$ ile eşleştiğinden bir $c \to m$ çözümlemesinde bir çok açık metine de aynı anda ulaşılabilir. $|C| = |\mathcal{M}|$ durumlarında ise mükemmel deşifreleme yöntemi kullanılmıştır denir. $|C| > |\mathcal{M}|$ durumu için ise karmaşık bir sonuç elde edilir. Olasılıkların arttığı, komplike bir algoritma kullanılmıştır denir **[9].**

Yukarıda da bahsedildiği üzere birden çok anahtar barındıran sistemlere gereksinim doğmuştur. Bu yeni gereksinim ve süreçler açık anahtar şifreleme yöntemlerini doğurmuştur. Şimdi kısaca bu yöntem tanıtılacaktır.

1.8. Açık Anahtar Kriptosistemler

Herhangi bir kriptolojik sistemin temel sorunlarından biri de anahtar dağıtım problemidir. Bu problem alıcı ile gönderici arasında yeni ve gizli bir kanalın daha kurulması gerekliliğini ortaya çıkarmıştır. Güvenlik riski göz ardı edilse dahi anahtar gönderiminin hızlı ve maliyeti düşük bir yöntemde olması gerekmektedir. Örneğin elektronik mail sistemleri, bankalar arası havale-eft işlemleri ve benzeri zira sürekli yeni kullanıcılar ve yeni işlemler yapan eski kullanıcıların ihtiyacına binaen üretilen anahtarlar hızlı ve kolay üretilebilmelidir fakat bu hızlılık ve pratiklik güvenlik açıkları da doğurmamalıdır. İşte açık anahtar kriptosistemlerini temel olarak bu düşünceye oturtabiliriz; hızlı, pratik, düşük maliyetli ve güvenli.

1.8.1. Açık anahtar kriptosistemlerin matematiksel modellemesi

Evvela, sistemi kullanmak ve birbirleri ile iletişim kurmak isteyen kullanıcıların aynı şifreleme algoritması e yi ve aynı deşifreleme algoritması d yi kullanmaları gerekliliği mühimdir. K_i; açık anahtarlardan bir anahtarı, L_i; gizli anahtarlardan bir gizli anahtarı ve U_i de sistemdeki belirli bir kullanıcıyı göstersin. O halde sistem aşağıdaki eşitlik üzerine kuruludur;

$$d(e(M, K_i), L_i) = M.$$

K_i sistem içerisinde açık bir kaynakta tutulabilir ama L_i gizli tutulmalıdır. Sistem içerisinde iletişim şu şekildedir;

a) U_j kullanıcısı şayet U_i ile bağlantıya geçmek istiyor ise U_i nin kullandığı K_i açık anahtarını açık dosyadan bakıp öğrenmelidir.

b) Bu aşamadan sonra U_j kullanıcısı

$$C = e(M, K_i)$$

şifreli metnini açık bir kaynaktan iletmelidir.

Sistemin güvenliği ise e ve d fonksiyonlarının şu tarz özelliği taşıyıp taşımamasına göre değişkenlik gösterir;

1) M ve K belirli iken, $C = e(M, K)$ yı hesaplama işlemi kolaylık arzetmelidir.
2) Sadece C şifresi elde ediliyorsa buradan M yi hesap etmek pek uygun ve kolay olmamalıdır.
3) C şifresi L_i ile elde edildiğinde M yi hesap etmek kolay olmalıdır.

Bir başka deyişle 1) ve 2) nolu özellikler sadece gizlemeyi esas alan yani şifrelemeyi yapan fakat sonrasını koruyan algoritmaların özelliğidir. Aslında bu tür fonksiyonlara bir-yol fonksiyonu (one-way fucntion) denir. 3) özelliği ise net bir şekilde deşifre sistemini de çalıştıran algoritmalarda bulunur. Yani tersi olan bir bir-yol fonksiyonunu (ki buna da trapdoor fonksiyonu denir) ters anahtar (gizli anahtarın ters işlemi) olarak kullanıp M yi elde ederler. Tüm bu özelliklerin yanı sıra pratik bir sistem arzu ediliyorsa şu dördüncü özellik de bulunmalıdır.

4) Herhangi keyfi iki (K_i, L_i) anahtar ikilisini üretmek kolay olmalıdır. Bu pratiklik ayrıca ekstra güvenlik demektir zira düşman bazı anahtarları ele geçirmiş olsa bile başka anahtarlar yedek olarak bulunabilmelidir **[10].**

1.9. Kriptografi ile Modern Kriptografi Karşılaştırması

Kriptografi ilk zamanlarda güvenli iletişim üzerine odaklanmıştır. Oysa görünürde "kod (code)" sözcüğünü duymayan hemen hiç kimse kalmamıştır. Kod, kısaca "özelikle iletişim ve iletilen mesajlarda kesin güvenirliği sağlamaya yarayan düzenlenmiş sinyaller algoritmasıdır". 20. yüzyıla gelene kadar kriptografiye bir sanat dalı olarak bakılıyordu. Güzel bir şifre üretmek, var olan bir şifreyi kırmak gibi kişisel üretkenlik özelliklerinin sergilenme arenası olarak görülüyordu. Ayrıca güzel şifre veya kodlar yazmak ise tamamen izafidir. 20. yüzyılın sonlarına gelindiğinde, kriptografinin resmi temelden değişerek radikal yeniliklere sahne olmuştur. Zengin ve güçlü matematiksel yapılar ve

algoritmik modellerle artık tamamen bir bilim dalı olarak kabul edilmektedir. Aslında kriptografi de şu sıralar sadece gizli iletişim ile ilgilenmiyor. Zaten dijital imza, elektronik seçimler, dijital paralar, gizli anahtarlar üretme ve değiştirme algoritmaları (banka, atm vb) bunlardan birkaçıdır. Gerçekte kriptografinin modern bir tanımı şu olsa gerek: "Dağıtık bilgiler ve dağınık veri tabanları üzerine içerden veya dışardan oluşabilecek bir saldırıyı önleme ve data güvenliğini sağlama bilimidir".

Bir başka kıyaslama noktası ise kriptografiyi kimin kullandığıdır. 1980 lere kadar kriptografi zeka yarışmalarında ve askeri güvenlik konularında kullanılırdı. Bugün ise her yerde! Bilgisayarda girdiğin her güvenli site bir kriptografik eserdir. Kaybolan laptopunuzu bulmaya yarar, alışveriş sitesinde iki kez kartınızın para ödemesini engeller vb.

Kısacası modern kriptografi, bir sanat eseri olarak görülürken, bugünlerde sıradan insanın dünyaya açılıp bilgiye ulaşmasını ve yaymasını sağlayan bir bilim dalıdır.

Bir başka farklılık oluşan nokta ise anahtar üretimi protokolüdür. Eski kriptoloji daha öncede bahsettiğimiz gibi sadece bir gizli anahtar kullanıp bunu da mesajın içerisine değil de ayrı bir yoldan gönderiyordu. Mesaj güvenliğini sağlayan hususlardan biri de güvenli fiziki buluşma noktaları ve güvenilir fiziksel gerçel kişilerdi. Oysa günümüzde bu pek mümkün ve pratik görünmemektedir. Modern kriptografi artık mesajın yanına anahtarları da gizli veya açık fark etmez koymak zorundadır. Modern kriptografi hedef kitle olarak sadece mesaj iletmek istediğimiz kişiyi değil bütün dünyayı seçebileceğimiz bir skala sunduğundan mesajımızın anlaşılması için açık anahtarları artırmak, geç olsa da asıl kişilerin görmesi için ise gizli anahtarları artırmak gibi seçenekler sunmaktadır.

1.10. Şifrelerin Matematiği

Buraya kadar kriptolojinin tarihini, tanımını, gelişimini ve önemini anlatan bölümler verildi. Bu bölümde ise şifreleme türlerinin matematik altyapıları verilecektir. Kriptolojik sistemin önemini örneklerle ve uygulama alanlarıyla belirttiğimiz önceki kısımlara karşılık bu bölümden itibaren tüm yorum ve çıkarsamalar matematik idealarıyla belirtilecektir. Okuyucunun gerekli Matematik altyapısına haiz olduğu varsayılmıştır. İhtiyaç duyulması halinde bir sonraki ana başlık altında verilen altyapıyı ve materyali oluşturan tanım, ifade ve teoremlere göz atılabilir. Verilen şifreleme türlerinin sıralaması genellikle tarihsel

sıralamaya göre olacaktır. Şimdi afin dönüşüm de denilen şifreleme türünden bahsedilerek bu bölüme giriş yapılacaktır.

1.10.1. Afin şifreleme

Sezar şifresinin matematiksel ifadesi; P düz metni C de şifreli metni göstermek üzere

$$C \equiv P + 3 \ (mod\ 26), \qquad 0 \leq C \leq 25 \tag{1}$$

kuralı altında P deki her bir harfi (1) denklemine göre dönüştürmekten ibarettir. Daha sonra adına öteleme dönüşümü denilen

$$C \equiv P + k \ (mod\ 26), \qquad 0 \leq C \leq 25, \qquad 0 \leq k \leq 25$$

denklemine dönüşerek Sezar şifrelemesinin biraz daha genel hali olarak uygulanmıştır. En son ve genel hali ise adına afin dönüşüm denilen

$$C \equiv aP + b \ (mod\ 26), \qquad 0 \leq C \leq 25$$

kuralı altında şifreleme yapmaktır. Burada a ve b tam sayıları için tek kıstas $(a, 26) = 1$ olmasıdır. Sebebi ise, P ve C nin $mod\ 26$ daki rezidü sistemini tam oluşturabilmeleridir. Aşikardır ki $a = 1$ olması durumunda öteleme şifrelemesine dönüşecektir. a nın $\phi(26) = 12$ farklı ve b nin de 26 farklı seçimi olacağından $12.26 = 312$ adet farklı afin şifrelemesi uygulanabilir. Afin dönüşümün tersi ise;

$$P \equiv a^{-1}(C - b) \ (mod\ 26), \qquad 0 \leq P \leq 25$$

kuralı ile belirlenir, burada a^{-1} sayısı a nın $mod\ 26$ daki tersidir [12].

Örnek 1.2 $a = 7$ ve $b = 10$ seçerek, $PLEASE\ SEND\ MONEY$ metni afin şifreleme kuralıyla şifrelensin.

$$C \equiv 7P + 10 \ (mod\ 26)$$

kuralının ters dönüşümü $P \equiv 15(C - 10) \equiv 15C + 6 \ (mod\ 26)$ dır. Çünkü 15 ve 7 birbirlerinin $mod\ 26$ tersleridir. Bu kural altında alfabenin yeni dizilimi Tablo 1.4 de verilmiştir.

Tablo 1.4. $C \equiv 7P + 10\ (mod\ 26)$ kuralına göre yeni alfabe.

Düz metin								Şifreli metin							
A	0	H	7	O	14	V	21	10	K	7	H	4	E	1	B
B	1	I	8	P	15	W	22	17	R	14	O	11	L	8	I
C	2	J	9	Q	16	X	23	24	Y	21	U	18	S	15	P
D	3	K	10	R	17	Y	24	5	F	2	C	25	Z	22	W
E	4	L	11	S	18	Z	25	12	M	9	J	6	G	3	D
F	5	M	12	T	19			19	T	16	Q	13	N		
G	6	N	13	U	20			0	A	23	X	20	V		

Bu şifrelemenin nasıl yapıldığını açıklayacak olursak, örneğin düz metindeki L harfi 11 sayısına karşılık geldiğinden $7.11 + 10 \equiv 87 \equiv 9\ (mod\ 26)$ olduğunda ve 9 sayısı şifreli metinde J harfine karşılık geldiğinden L harfi J ile dönüşecektir.

Bu kural altında

$$PLEASE\ SEND\ MONEY$$

metni aşağıdaki

$$LJMKG\ MGXFQ\ EXMW$$

metnine dönüşür.

Monografik şifreleme denilen bu yöntem deşifre edilmeye müsait olduğundan yerini ikili harflerin şifrelemesine dayanan blok şifrelemeye bırakmıştır. Tablo 1.5 bu durumu açıklamaktadır **[15]**.

Tablo 1.5. İngiliz alfabesinde harflerin kullanım sıklığı.

Harfler	Sıklık % si	Harfler	Sıklık % si	Harfler	Sıklık % si	Harfler	Sıklık % si	Harfler	Sıklık % si	Harfler	Sıklık % si	Harfler	Sıklık % si
A	7	E	13	I	8	M	3	Q	<1	U	3	Y	2
B	1	F	3	J	<1	N	8	R	8	V	1	Z	<1
C	3	G	2	K	<1	O	7	S	6	W	1		
D	4	H	3	L	4	P	3	T	9	X	<1		

Bu tabloya göre en çok kullanılan harfler sırayla E, T, N, O ve A dır. Bu bilgi ışığında bir şifreli metin en çok hangi harfi barındırıyorsa onu E ile daha sonrakini sırayla T ile dönüştürerek deşifre edilebiliyordu. Bu zayıflığa bir çözüm olarak blok şifreleme geliştirilmiştir.

1.10.2. Blok şifreleme ve Hill şifrelemesi

Harflerin ikişerli bloklar halinde seçilip şifrelendiği bu yöntem önceleri blok şifreleme daha sonra ise 1930 larda fikir babası olan Lester Hill' in adı verilerek Hill şifreleme olarak anılmıştır.

Bu yöntem düz metindeki harfleri ikişerli öbeklere ayırıp (eğer son durumda tek bir harf buluyorsa herhangi bir harf ekleyip çifte tamamlamak koşuluyla) ikişerli denklem sistemini $mod\ 26$ da çözmekten ibaretti. Bir örnek yardımıyla anlatılacak olursa;

$$THE\ GOLD\ IS\ BURIED\ IN\ ORONO$$

metni önce ikişerli öbeklere parçalanıp

$$TH\ EG\ OL\ \ DI\ SB\ UR\ IE\ DI\ NO\ RO\ NO$$

haline getirilir. Sonra da karşılık gelen numaralar ile kodlanıp (daha önce yapıldığı gibi)

19 7 4 6 14 11 3 8 18 1 20 17 8 4 3 8 13 14 17 14 13 14

şekline dönüşür.

P_1P_2 gibi ikili bir düz metin ikilisi C_1C_2 gibi iki şifreli metin ikilisine şu kural atında dönüştürülsün;

$$C_1 \equiv 5P_1 + 17P_2 \ (mod\ 26)$$

$$C_2 \equiv 4P_1 + 15P_2 \ (mod\ 26).$$

Örneğin 19 7 ikilisi 6 25 ikilisine dönüşür çünkü

$$C_1 \equiv 5.19 + 17.7 \equiv 6 \ (mod\ 26)$$

$$C_2 \equiv 4.19 + 15.7 \equiv 25 \ (mod\ 26).$$

Bu işlemler altında tüm mesaj şu şifreli ikililere dönüşür

6 25 18 2 23 13 21 2 3 9 25 23 4 14 21 2 17 2 11 18 17 2.

Karşılık gelen şifreli metin ise

$$GZ\ SC\ XN\ VC\ DJ\ ZX\ EO\ VC\ RC\ LS\ \ RC$$

olur. Tekrar bu metni deşifre etmek için ise

$$P_1 \equiv 17C_1 + 5C_2 \ (mod\ 26)$$

$$P_2 \equiv 18C_1 + 23C_2 \ (mod\ 26)$$

kuralı altında dönüşüm yapılır. Bu yöntem matrislerle anlatılacak olursa

$$\begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \end{bmatrix} \ (mod\ 26)$$

şeklinde gösterilir. Deşifrelemek için dönüşümün ilkesi olan

$$\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix}$$

matrisinin tersi bulunur. Fark edileceği üzere dönüşümün ilkesini belirten matrislerin tersi de mevcut olmalıdır. Ters matris uygun hesaplamalar sonucunda

$$\begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix}$$

olarak elde edilir ve deşifrelemenin ilkesini veren bu matris;

$$\begin{bmatrix} P_1 \\ P_2 \end{bmatrix} = \begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \ (mod\ 26)$$

denklem çözümünden P_1P_2 açık metnini verir. Şimdi bu mantığın genellemesi olan Hill şifrelemesinden kısaca bahsedilecektir.

$P_1P_2P_3$ ... P_n açık metni n uzunluğundaki bloklar şeklinde seçilir ve regüler bir $n \times n$ tipinde A matrisi yardımıyla C_1C_2 ... C_n şeklinde n uzunluğundaki şifreli metne aşağıdaki gibi dönüştürülür;

$$C \equiv AP\ (mod\ 26),$$

A $n \times n$ tipinde matrisi ve $(\det A, 26) = 1$,

$$C = \begin{bmatrix} C_1 \\ C_2 \\ \vdots \\ C_n \end{bmatrix}$$

ve

$$P = \begin{bmatrix} P_1 \\ P_2 \\ \vdots \\ P_n \end{bmatrix}.$$

Deşifreleme yardımıyla A regüler seçildiğinden $AA^{-1} \equiv I\ (mod\ 26)$ olacak şekilde bir A^{-1} bulunabileceğinden

$$A^{-1}C \equiv A^{-1}(AP) \equiv (A^{-1}A)P \equiv P\ (mod\ 26),$$

olur ki deşifreleme işlemi

$$P \equiv A^{-1}C\ (mod\ 26)$$

şeklinde yapılır **[13]**.

Poligrafik şifreleme denilen bu yöntemin de barındırdığı zayıflıklar neticesinde kriptolojide artık yeni bir şifreleme türü üretilmiştir:

1.10.3. Üstel şifreleme

Bu bölümde anlatılacak olan şifreleme türü, 1978 de Pohlig ve Hellman tarafından ortaya atılmış, kriptanalize karşı oldukça dirençli ve modüler üs tabanlı bir sistemdir. Bu sistemin çalışması için öncelikle mesaj metni ikili öbeklere ayrılır. Şayet çift sayıda öbek oluşuyor ise ilave bir harf ile çift öbek elde edilir. Daha sonra deşifre ederken bu son harf göz ardı edilir. Matematiksel ifadesi ile; p bir tek asal sayı, e; $(e, p-1) = 1$ olacak şekilde bir sayıdır ki şifrelemenin anahtarıdır, m harften oluşan bir metne karşılık gelen $2m$ uzunluğundaki metnin dijital gösterimi ve $2525 < p < 252525$ şartlı seçimler altında bu sistem

$$C \equiv P^e \ (mod\ p), \qquad 0 \leq C < p$$

ile çalışmaktadır. Bir örnek ile açıklamak gerekirse

Örnek 1.3 $p = 2633$ ve $e = 29$ seçimleri altında

$$THIS\ IS\ AN\ EXAMPLE\ OF\ AN\ EXPONENTIAL\ CIPHER$$

metnini şifreleyelim. Bunun için önce harflerin yeni ikili gösterimlerini Tablo 1.6 da verelim.

Tablo 1.6. Harflerin ikilik dijital gösterimleri.

Harf	Dijital gösterim	Harf	Dijital gösterim	Harf	Dijital gösterim	Harf	Dijital gösterim	Harf	Dijital gösterim
A	00	G	06	M	12	S	18	Y	24
B	01	H	07	N	13	T	19	Z	25
C	02	I	08	O	14	U	20		

D	03	J	09	P	15	V	21		
E	04	K	10	Q	16	W	22		
F	05	L	11	R	17	X	23		

Örneğimizdeki metni ikili harfler ve karşılık gelen dijital gösterimleri ile yazarsak

1907 0818 0818 0013 0423

0012 1511 0414 0500 1304

2315 1413 0413 1908 0019

0314 1302 0815 0704 1723

dir. Not edelim ki çift sayıda harf öbeği için X harfini yani karşılık gelen 23 sayısını ekledik. Şimdi her bir ikili harfin karşılık geldiği sayıyı alıp teker teker

$$C \equiv P^{29}\ (mod\ 2633), \qquad 0 \leq C < p = 2633$$

kuralı ile şifreleyelim. 1907 sayısı

$$C \equiv 1907^{29} \equiv 2199\ (mod\ 2633)$$

kuralı altında 2199 sayısına dönüşür. Bu kural altında tüm ikililer şifrelenirse

2199 1345 1745 1206 2437

2425 1729 1619 0935 0960

1072 1541 1701 1553 0735

2064 1351 1704 1841 1459

şifreli mesajı elde edilir. Deşifre etmek için ise evvela bir d anahtarı elde edilmelidir. Şöyle ki; $de \equiv 1\ (mod\ p-1)$ olacak şekilde bir d mevcuttur çünkü $(e, p-1) = 1$ alınmıştı. Bu d anahtarı C şifresine üs olarak uygulanıp $mod\ p$ de hesaplanırsa P metni elde edilir;

$$C^d \equiv (P^e)^d \equiv P^{ed} \equiv P^{k(p-1)+1} \equiv (P^{p-1})^k P \equiv P(mod\ p),$$

olur ki $de \equiv 1\ (mod\ p-1)$ olmasından ötürü $de = k(p-1)+1$ yazılıp, $P^{p-1} \equiv 1\ (mod\ p)$ Fermat özelliği yardımıyla da uygulanan doğrudan P mesajına ulaşacağı aşikardır. Bu sistemin, kendisinden önceki öteleme veya yerine koyma türü kriptolojik sistemlere karşılık üstünlüğü ise bir d sayısını $de \equiv 1\ (mod\ p-1)$ şeklinde elde etmek her ne kadar zor olsa da elde edilmesine rağmen halen $C^d\ (mod\ p)$ şeklinde kullanımının da getireceği uzun hesaplamalardır. Bu hesaplamalar lineer değil üstel bit işlemleri gerektirdiğinden kriptanalizleri kolay olmayacaktır. Örnek olarak p asalı 100 basamaklı seçilirse $mod\ p$ de çözüm yapmak yaklaşık olarak 74 yıl sürecektir. Sistemin güvenirliği ve zor kırılabilirliği için iki durumdan bahsedersek bir p asalı için şayet $p-1$ küçük tam sayıların çarpımı şeklinde ise sistem zayıflayacak ve küçük modüllerle işlem yapılacağından kriptanaliz kolaylaşacaktır. Buradan hareketle büyük asalların küçük çarpımlar içermeyenleri seçilmelidir diyebiliriz. Bunu sağlamak için ise bir q asalı için $2q+1$ şeklinde yeni ve daha büyük asallar elde etmek önerilebilir. Üstel şifreleme sistemleri sadece güçlü güvenlik düzeyleri ile değil ortak anahtarlar üretebilmek ve bunu sistem içerisindeki katılımcıların paylaşabilmeleri gibi ekstra büyük özellikler de barındırmaktadır. Şöyle ki; P büyük bir asal sayı, a P ile aralarında asal olan bir sayı ve k da $(k, p-1) = 1$ olan sistemin kullandığı ortak bir anahtar olsun. Herhangi iki katılımcıda da sırayla k_1, k_2 anahtarları bulunsun ve bunu da paylaşmak istiyor olsunlar, o halde birinci katılımcı ikinciye

$$y_1 \equiv (a^{k_1}\ mod\ p), \qquad 0 < y_1 < p,$$

sayısını gönderir. İkinci katılımcı ise ortak anahtar olan k yi şu şekilde elde eder

$$k \equiv {y_1}^{k_2} \equiv a^{k_1 k_2}\ (mod\ p), \qquad 0 < k < p.$$

Benzer şekilde ikinci katılımcı birinciye bir y_2 sayısını

$$y_2 \equiv (a^{k_2}\ mod\ p), \qquad 0 < y_2 < p,$$

şeklinde gönderir ve birinci katılımcı da yine benzer şekilde ortak anahtar k ye

$$k \equiv {y_2}^{k_1} \equiv a^{k_1 k_2}\ (mod\ p), \qquad 0 < k < p$$

hesaplaması ile ulaşır. Not edelim ki ağ dışından birinin bir ortak anahtar k yi bulması uzun $mod\ p$ işlemleri gerektirdiğinden bilgisayar zamanlı bile pek mümkün değildir.

1.11. Rivest-Shamir-Adleman (RSA) Kriptosistemi

Fikir, çok büyük iki asal sayı seçiminde ve bunların çarpımından oluşan sayıya kolayca çarpanlarına ayrılamayacağı inancı üzerine oturmaktadır. Sistemi adından da anlaşılacağı üzere Rivest, Shamir ve Adleman 1978 de kurmuşlardır **[15]** . Şimdilik şifreleme ve deşifreleme safhalarını verelim. Sonrasında detaylar ve matematiksel çıkarımlar verilecektir.

1.11.1. Şifreleme-deşifreleme prosedürü

I. İki tane p ve q gibi çok büyük asal sayı seç ve bunların çarpımını $n = pq$ olarak hesapla.

II. Keyfi ve büyük bir d sayısını $\big(d, (p-1)(q-1)\big) = 1$ olacak şekilde bul.

III. $1 \leq e \leq (p-1)(q-1)$ olacak şekildeki tek türlü bulunabilecek e sayısını

$$ed \equiv 1 \ (mod \ (p-1)(q-1))$$

formülünden elde et.

IV. e ve n tam sayı ikililerini bilinir yap, yani (e, n) açık anahtar olarak verilsin.

V. Gönderilmek istenen M mesajını, şayet çok büyük ise parçalara ayır ve $\{1, 2, \dots, n\}$ bölgesine düşür.

VI. M mesajını C şifreli metnine

$$C \equiv M^e \ (mod \ n)$$

kuralı ile dönüştür.

VII. d özel anahtarını kullanarak,

$$D \equiv C^d \ (mod \ n)$$

denkleminden bir $D \equiv M \ (mod \ n)$ elde et.

Bu yedi adımda algoritma çalışır ve hesaplamalar doğru yapılırsa deşifre edilen metin de doğru açık metin olur. Şimdi alt zemini oluşturan matematiğe biraz değinilecektir.

1.11.2. Sistemin temelini oluşturan matematik

Sistemi çalıştıran matematikten bahsedilmeden evvel iki lemma verilsin.

Lemma 1.1 Herhangi iki farklı p ve q asal sayıları ve herhangi iki (m, s) pozitif tam sayıları için eğer $m^s = m\ (mod\ p)$ ve $m^s = m\ (mod\ q)$ oluyorsa

$$m^s = m\ (mod\ pq)$$

olacaktır.

İspat $m^s - m$ hem p hem de q sayılarına bölünür. Buradan pq sayısına da bölünür ki bu da

$$m^s = m\ (mod\ pq)$$

demektir. ⊠

Lemma 1.2 $(M, p) = (M, q) = 1$ olmak üzere p ve q iki farklı asal sayı olsun. O halde

$$M^{t(p-1)(q-1)+1} = M\ (mod\ pq)$$

olur.

İspat p asal ve $M \neq 0\ (mod\ p)$ olduğundan Euler-Fermat eşitliğinden

$$M^{p-1} = 1\ (mod\ p)$$

elde edilir. Buradan bir r tam sayısı için

$$M^{p-1} = rp + 1$$

olur ki bu da

$$M^{t(p-1)(q-1)+1} = (rp+1)^{t(q-1)}.M\ (mod\ p)$$

$$= M\ (mod\ p)$$

demektir. $M = 0$ durumu için de eşitlik sağlanacağından her M için doğrudur denir. Benzer düşüncelerle

$$M^{t(p-1)(q-1)+1} = M\ (mod\ q)$$

olduğu sonucuna da ulaşılır ki bu da Lemma 1.1 den hareketle

$$M^{t(p-1)(q-1)+1} = M\ (mod\ pq)$$

anlamına gelir ve ispat biter. ⊠

Şimdi RSA nın matematik alt yapısının deşifrelemeye uygun olduğu gösterilecektir.

Teorem 1.1 Tüm kullanılan parametreler RSA algoritmasında anlatıldığı gibi seçilmek koşuluyla;

$$C = M^e \ (mod\ n) \tag{2}$$

ise

$$C^d = M \ (mod\ n) \tag{3}$$

olur.

İspat $D = C^d \ (mod\ n)$ ifadesini göz önüne alalım. $C = M^e \ (mod\ n)$ olduğundan s pozitif tam sayı olmak üzere

$$C = M^e - sn$$

diyebiliriz. Buradan

$$D = (M^e - sn)^d \ (mod\ n)$$

olur ve Binom Teoremi' nden faydalanarak

$$D = M^{ed} \ (mod\ n)$$

sonucuna ulaşırız. $ed = 1 \ (mod\ (p-1)(q-1))$ olduğundan hareketle

$$D = M^{t(p-1)(q-1)+1} \ (mod\ n)$$

dir ve Lemma 1.2 den yararlanarak

$$M^{t(p-1)(q-1)+1} = M \ (mod\ pq)$$

denkliğini ifade ediyordur.

$$D = M \ (mod\ n)$$

sonucuna ulaşırız ve ispat biter. ⊠

1.11.3. RSA sistemine saldırı

Sistemi kırmak isteyen bir yapı muhtemelen (n, e) anahtarına da sahiptir. Zira bir ikili açık anahtar olduğundan elde edilebilmiştir. Ayrıca, birçok sistem üzerinden gönderilmiş ve alınmış (M, C) ikilileri de ellerinde bulunabilir. Buradan hareketle saldırganlar sistemi iki şekilde kırabilirler:

a) n yi çarpanlarına ayırmak, çünkü n yi çarpanlarına tam olarak ayırabilen bir saldırgan $\phi(n) = (p-1)(q-1)$ sayısına da rahatlıkla ulaşabilir ve böylece özel anahtar d yi bulabilir.

b) n yi parçalamadan $\phi(n)$ sayısını bulmak, şayet $\phi(n)$ biliniyorsa d elde edilebileceğinden sistem saldırı altına girebilir **[17].**

1.11.4. RSA sisteminin etkinliği ve hızı

Sistemin pratikliğini, uygulanabilirliğini ve hızını etkileyen bazı parametre seçimleri hakkında bilgi verilecek olursa,

a) Büyük ve farklı iki asal sayı seçimi için bazı algoritmalardan faydalanılabilir.

b) $\big(d, (p-1)(q-1)\big) = 1$ olacak şekildeki gizli anahtar d seçimleri $d > maks\{p, q\}$ ve d asal şartları altında hızlanacaktır.

c) $ed = 1\ (mod\ (p-1)(q-1))$ olacak şekildeki e sayılarının seçimi için Euclid algoritması kullanılabilir. $(d, (p-1)(q-1) = \phi(n)) = 1$ olduğundan

$$ad + b\phi(n) = 1$$

olacak şekilde (a, b) ikilileri mevcuttur.

$$ad = 1\ mod\ (\phi(n))$$

olacağından $a = e$ seçilebilir.

d) RSA sisteminin çarpanlarına ayırma problemi ve zorlukları üzerine kurulduğu gerçeğinden hareketle şayet (p, q) ikilileri yüz basamaklı seçilmiş ise sistem yeteri kadar güvenli olacaktır. Ayrıca özel anahtar d seçimini zorlaştırmak adına $p-1$ ve $q-1$ sayılarının çok küçük çarpanlar içermemesine dikkat edilebilir. Zira bir çarpanı bulunduğu durumda $p.1 = ab$ gibi daha küçük iki sayıya

dönüşecektir ki a nın tüm uygun katları (veya b nin) $mod\ (p-1)$ hesaplamalarında sıfır olacağından özel anahtar elemeleri kolaylaşacaktır.

Şimdi ise açık anahtar şifrelemenin temelini oluşturan ilk metodoloji yani Elgamal kriptosistemi verilecektir.

1.12. Elgamal Kriptosistemi

Ayrık logaritmayı bulma problemine dayalı ilk açık anahtar şifreleme yöntemini Elgamal vermiştir. Sistemin algoritmik bir şekilde ifadesi;

- Bir G grubu üret.
- Mertebesi asal sayı olan $g \in G$ leri ve asal mertebe r leri bul.
- Keyfi bir a sayısını $0 < a < r$ olacak şekilde seç ve $h = g^a$ yı elde et.
- Açık anahtar (G, g, h) ve gizli anahtar a dır.
- Mesaj uzayı $M = G$ dir.
- Şifreli metin uzayı $C = G \times G$ dir.

1.12.1. $m \in G$ yi şifreleme safhası

- Açık anahtar h yi networkten sağla.
- $0 < k < r$ olacak şekilde bir k seç ve $c_1 = g^k$ al.
- $c_2 = mh^k$ yı da hesapla.
- (c_1, c_2) şifreli metnini gönder.

1.12.2. Deşifreleme safhası

- c_1, c_2 nin G nin elemanları olup olmadığını kontrol et.
- $m = c_2 c_1^{-a}$ yı hesap et ve metne ulaş.

Şimdi sistemin artıları ve eksileri şu üç durumda değerlendirilecektir.

1) Elgamal kriptosistemi şifreleme kısmında G de iki üs alma işlemi yaparken deşifreleme kısmında sadece bir defa üs almaktadır. Bu ise polinom-zaman olarak uygun iken güvenlik zafiyetine sebebiyet vermektedir. Mesela g^r elemanı şifrelenirken $c_2 = g^r h^k = g^r g^{ak} = g^{ak+r} = h^k$ olur ki mesajın şifreli hali açık anahtardır.

2) Elgamal şifrelemesi keyfiliğe açıktır. Yani aynı mesaj aynı açık anahtarlar kullanılmasına rağmen farklı şifreler oluşabilecektir. Örneğin $c_2 = mh^k$ kısmında farklı k ler için farklı c_2 ler elde edilecektir.

3) RSA nın aksine sistem kullanılan tek bir grup G ve tek bir üreteç g ye karşın $g^a = h$ açık anahtarlarını farklı a lar için farklı sayıda bulabileceklerdir **[18].**

Elgamal sisteminden de görüleceği üzere, 1980 lerden sonra kriptolojiye açık anahtar şifreleme yöntemleri kazandırıldıkça yeni problemlerde doğmuş olmaktadır. Anahtar dağıtım problemi denilen bu problem güvensiz bir kanal üzerinden (internet gibi, çünkü diğer katılımcılar sisteme sızabilir) iletişim kurmak isteyen iki kullanıcının özellikle gizli anahtarı nasıl birbirlerine gönderecekleri ve aynı tür açık anahtarı nasıl mutabık kalarak seçebilecekleri esasına dayanır. 1976 yılına gelindiğinde ise Diffie ve Hellman bu probleme bir öneri getirmişlerdir. Gizli ve açık olmak üzere iki anahtardan oluşan bu yeni sistemde kullanıcılar açık anahtarı tüm sisteme ifşa edip gizli anahtarı ise ellerinde tutup paylaşmıyorlardır. Sistem gizli anahtar gönderimi yapmadığı için biraz daha güvenli hale gelmiştir (zamanına nispeten). Bu sistemde, A_1 kullanıcısı A_2 ye mesaj ilettiğinde, A_2 kullanıcısına açık anahtarını alıp mesajı bununla gizleyip böylece gizli anahtar paylaşmadan gönderiyordu. A_2 ise elindeki gizli anahtarı kullanıp mesajı okuyabiliyordu. İçeriye dışarıdan sızmak pek mümkün değildi yani kod kırıcı dinlese bile mesaja ulaşamıyordu. Sistemin tek zaafiyeti ise herkesin A_2 ye mesaj gönderebilir olmasıdır. Çünkü açık anahtarlar sistem içerisinde sürekli paylaşıldığından ele geçirilip yeni ve yanıltıcı mesajlar sisteme akıtılabilir.

Tekrar Elgamal sistemine dönülecek olursa, sistemin açık anahtar şifreleme sistemine katkılarından söz edebilmek adına şimdi, altyapısındaki matematik model verilecektir.

Bir G grubu (tercihen devirli) üzerinde bir A_1 kullanıcısı bir t gizli anahtarına sahip olsun. Açık anahtar olarak da $\alpha^t \equiv \beta \ (mod\ p)$ olmak üzere (p, α, β) kullanılsın. Burada p, α elemanının gruptaki mertebesidir. Bir $m \in G$ mesajını A_1 kullanıcısı bir $0 < K \leq p - 1$ parametresi yardımıyla

$$e_K(m) = (y_1, y_2) = (\alpha^K, m\beta^K)\ mod\ p$$

şeklinde şifreler ve gönderir. G grubunun tercihen devirli olması, seçilen $\alpha \in G$ yi üreteç kılabilir ki bu da $|\langle\alpha\rangle| = |G| = p$ sayısını büyüteceğinden büyük denklik sınıfları üretecektir. Şifreleme operatörü e yerine e_K notasyonu kullanıldı. Zira K seçimleri aynı mesajı aynı anahtarlar kullanılsa dahi farklı C şifrelerine götürecektir. Bu farklılığı

sağlayan K seçimlerine sistemin güvenlik parametresi denir. Bu parametreler yardımıyla aslında aynı mesajı farklı zamanlarda iletmek farklı K seçimleri yardımıyla farklı C şifreleri elde edilebilir. Bu ise hesaplanabilir bir karmaşıklık olduğundan, sistem; gününün en güçlü kriptolojik sistemi haline gelmiştir. Deşifreleme aşamasında ise A_2 alıcısı

$$d_K(y_1, y_2) = y_2(y_1^t)^{-1} \, mod \, p$$

hesaplamaları yaparak m mesajına ulaşacaktır **[19].**

Elgamal kriptolojik sisteminin oturduğu G gruplarına Z_p^* olarak yaklaşılırsa ve p yeterince büyük seçilirse sistem güvenlik düzeyi istenildiği kadar güçlendirilebilecektir.

1.13. Dijital İmza

Dijital imzada temel mantık, alınan mesajın gerçekten gelmesini beklediğimiz bir göndericiden gelip gelmediğini kontrol etme prosedürüdür. Bu işleme iki veya daha çok adımlı doğrulama da denir. Temel mantık, bir mesaj aldığında göndericiden sistemin açık anahtarını da göndermesini istemek üzerine kuruludur. Bir diğer emin olma adımı ise farklı gizli veya açık anahtar seçimleri ile şifrelenmiş bir mesajı okuyabiliyorsa o halde gönderen sistemin içinden birisidir denilebilir. Örnek olarak RSA sisteminde gizli anahtar olan e kuvveti $\big(e, (p-1)(q-1)\big) = 1$ şeklinde olmalı idi. Bu ise $ed \equiv 1 \; (mod \; (p-1)(q-1))$ demektir. Buradan hareketle bir e gizli anahtarının yanı sıra d de bizim için gizli anahtar görevi görebilir. Bu d ile karşılıklı şifreli metin alışverişinde ikna olunuyorsa o halde ve dijital olarak imzalanmıştır denir **[20].**

1.14. Knapsack (Sırt çantası) Tabanlı Kriptosistemler

1978 li yıllarda Merkle ve Hellman tarafından yeni bir kriptolojik sistem tanıtıldı. Bu sistem daha sonraları sırt çantası problemi olarak anıldı. Bu isimle anılmasının sebebi, o güne kadar altküme toplamı olarak bilinen bir probleme dayanmasıdır. Altküme toplamı problemi kabaca şu şekilde özetlenebilir.

1.14.1. Altküme toplamı

Girdi: $a_1, a_2, \dots, a_n, t$ pozitif tam sayılar

Soru: $J \subseteq \{1, 2, \dots, n\}$ olmak üzere

$$\sum_{i \in J} a_i = t \quad ?$$

Literal olarak, "bir küme verildiğinde keyfi belirlediğimiz bir pozitif tam sayıyı bu kümenin elemanları toplamı olacak şekilde yeniden gösterebilir miyiz?" şeklinde kapsamı belirlenecek bu problemin, her keyfi şart altında çalışmayacağını yine Hellman kendisi şu örneği vererek ortaya koymuştur.

Örnek 1. 4 $\{14, 28, 56, 82, 90, 132, 197, 284, 341, 455\}$ kümesi verildiğinde 516 sayısının bu kümeye dayanan bir knapsack gösterimi yoktur.

Bu örnekten de görüleceği üzere sistemin detaylı şartlar taşıması gerektiği açıktır. Buradan hareketle Merkle-Hellman sistemin son halini şu şartlar altında yeniden belirlemiştir.

1.14.2. Şifreleme

1) Gönderilmek istenen mesaj ikilik sistemde bir m ye dönüştürülür.

2) Açık anahtar olarak süper artan bir $(a_1, \dots, a_n)$ n lisi seçilir. (Bir $(a_1, \dots, a_n)$ dizisi süper artandır ancak ve ancak $\forall k, 1 \leq k \leq n-1$ için $a_{k+1} > \sum_{i=1}^{k} a_i$ dir.)

3) Gönderilmek istenen m mesajı n li bloklara ayrılır.

4) $m_j = (M_1, \dots, M_n)$ olmak üzere $1 \leq j \leq t$ için

$$C_j = \sum_{i=1}^{n} M_i a_i$$

ikamesi yapılır.

5) $(C_1, \dots, C_t)$ dizisi şifrelenmiş mesaj olarak gönderilir.

Deşifreleme safhasından bahsedilmeden evvel sistemin gizli ve açık anahtarlarına kısaca değinilirse, $(e_1, e_2, \dots, e_n)$ süper artan bir dizi seçilir, w ve N gibi büyük ve aralarında asal iki pozitif tam sayı belirlenir. Belirlenen bu $(e_1, e_2, \dots, e_n)$ dizisi ile w ve N parametreleri gizli tutulur. $\{T(e_1), T(e_2), \dots, T(e_n)\}$ dizisi ise

$$T(e_i) = we_i \ (mod\ N)\ 1 \leq i \leq n$$

kuralı ile belirlenen ve açık anahtar olarak paylaşılır.

1.14.3. Deşifreleme

$(e_1, e_2, \dots, e_n)$ gizli anahtarı ve $w - N$ gizli anahtarları yardımıyla

$$C' = w^{-1}C \ (mod\ N)$$

hesaplamaları yapılarak bir C' sayısına ulaşılır. Bulunan bu C' sayıları $(e_1, e_2, \dots, e_n)$ bazında 2 lik sistemde yeniden yazılır ve m ye ulaşılır.

1.14.4. Deşifreleme neden doğru çalışır?

$M = (M_1 M_2 \dots M_n)$ ve $T(e_i) = a_i$ dersek,

$$M = M_1 a_1 + M_2 a_2 + \cdots + M_n a_n$$

olur. Fakat d_i tam sayı olmak üzere

$$a_i = we_i + d_i N \ (1 \leq i \leq N)$$

şeklinde yazılabilir. Buradan

$$C = \sum M_i a_i = \sum M_i w e_i \ (mod\ N)$$

olur ki

$$w^{-1}C = \sum M_i e_i \ (mod\ N)$$

sonucuna ulaşılır ve $w^{-1}C = C'$ sonucu gizli seçilen diziye göre yeniden ikilik sistemde çözülür. Şimdi metodun bir örnek ile izahı verilecektir.

Örnek 1.5 [21] Varsayılsın ki $(1, 3, 5, 11, 35)$ süper artan dizisi ve $w = 5$, $N = 53$ gizli anahtarları verilmiş olsun. Şu halde açık anahtarlar,

$$(5, 15, 25, 2, 16)$$

olacaktır. Göndermek istenilen mesaj,

$$M = 10011010101101101110$$

olsun. Öncelikle anahtar uzunluğu $n = 5$ olduğundan M mesajı 5 li bloklara ayrılır

$$10011 \quad 01010 \quad 11011 \quad 01110$$

ve M şu şekilde şifrelenir

$$10011 \mapsto 5 + 2 + 16 = 23$$

$$01010 \mapsto 15 + 2 = 17$$

$$11011 \mapsto 5 + 15 + 2 + 16 = 38$$

$$01110 \mapsto 15 + 25 + 2 = 42$$

ve böylece şifreli metin

$$C = (23, 17, 38, 42)$$

olacaktır. Deşifreleme için $w = 5$ in tersi hesap edilir. $w^{-1} = 32$ olduğundan her bir şifreli metin bileşeni ile çarpılır. Örneğin, 23 bileşeni

$$23 \mapsto 23.32 = 47 \ (mod\ 53)$$

$$= 35 + 11 + 1$$

$$= 10011$$

şeklinde açık metne ulaşılır.

Zamanında RSA dan daha güçlü olan ve kırılamayan bu sistemin polinom-zamanda çözülebileceği ve bazı ataklara karşı savunmasız olduğu yine sistem kurucuları tarafından deklare edilmiştir. Buradan yola çıkarak gelecekte böyle bir kriptosistemin etkin kullanılamayacağı öngörülebilir.

1.15. Tezin Amacı ve Vizyonu

Bu eserin temel amacı NTRU kriptosistemini hem cebirsel açıdan daha güçlü ve geniş bir yelpazede ele almak hem de ilgi çekici katkılarla literatürdeki yerini almaktır. Ele alınan sorular ve bu sorulara verilen cevaplar bakımından orijinal ve estetik olmayı hedeflemektedir. Tezin vizyonu ise kriptoloji ve NTRU kriptosistemini daha da ilginç hale getirerek alandaki çalışmaları artırmak ve teşvik etmektir. Bugün kullandığımız teknolojilerin temel varoluş kaynaklarından birisinin matematik ve bilgisayar olduğu muhakkaktır. Önceleri "bilgisayar matematik" kavramıyla sınırlandırdığımız bu bilgisayar

ve matematik ilişkisi günümüzde çok daha karmaşık ve büyük bir düzleme taşınmıştır. Soyut matematik dünyasında üretilen bir homeomorfizma, küme, cebirsel yapı vs kendisine rahatlıkla bilgisayar dünyasında bir izdüşüm bulmaktadır. Bu izdüşümün büyük nimetlerinden birisi ise bilgiyi korumayı ve güvenli bir şekilde paylaşmayı esas alan kriptoloji bilimidir.

Kriptoloji (şifreleme) tarih boyunca önemini artırarak günümüze kadar gelmiştir. Evvela basit bir matematik mantığına oturtulup direkt olarak reel hayatta kullanılabilen şifreleme teknikleri (örneğin $f(x) = x + 3$ Sezar ötelemesi) şimdilerde çok daha güçlü matematik modellere sahip olduğundan ilkin bilgisayar bilimciler tarafından test edilmektedir. Yeterli güvenlik düzeyine haiz ve uygulamaya elverişli olanlar reel dünyada kullanılmaktadır (örneğin RSA, finans sektöründe bir indikatör işlevi görür).

Bu kısa girizgâhın asıl amacı, tezin ana temasını oluşturan NTRU (Number Theorist Research Unit) kriptosistemine değinmektir. NTRU kriptosistemi mevcut programlanmış bilgisayar saldırılarına karşı gösterdiği direnç ile her geçen gün ilgileri üzerine çekmektedir.

Şimdi burada detay vermeden okuyucunun ilgisini canlı tutmak adına nedenselliği tezin ilgili bölümlerine havale ederek NTRU nun en güçlü ve ilgi çekici yanının kuantum sonrası kriptoloji sınıfına girmiş olduğunu ve kuantum tabanlı bilgisayar saldırılarına karşı (şimdilik) korunaklı olduğunu belirtelim. Gelecekte çok daha güçlü bilgisayarların ve saldırı yöntemlerinin üretilebileceği varsayımından hareketle bu çalışmada, NTRU kriptosistemi daha büyük bir cebirsel yapı üzerinde, daha fazla sayıda parametre ve değişkenlerle ele alınıp daha karmaşık bir matematik modele oturtulmuştur. Tezin ana motivasyonunu oluşturan ve tezin en önemli çıktısı olan "NTRU kriptosistemini daha güçlü cebirsel yapılarda uygulamak" misyon ve vizyonundan hareketle bu tezde yapılan tüm çalışmalar Cebirsel Kriptoloji disiplinine hizmet etmeyi ve katkı sunmayı hedefler.

1.16. Tezin İçeriği ve Kapsamı

Bu tezde evvela belli başlı kriptolojik kavram ve sistemler tanıtılmıştır. Her biri kendi literatürünün temel başucu kaynaklarını oluşturan eserlerden yararlanılarak geniş ve kapsamlı bir kriptoloji tarihi ve gelişimi anlatılmıştır. Daha sonra ikinci bölümde tezin iddialarını açıklamaya ve anlamaya yardımcı olacak teorik matematik altyapısı sunulmuştur. Bir sonraki bölümde ise NTRU kriptosistemi detaylı bir şekilde işlenmiş ve

yorumlanmıştır. Bulgular kısmında ise bu tezin ortaya attığı iddialar ve çözüm yolları sunulup bir sentez yapılmıştır. Sonuçlar ve öneriler verilerek çalışmanın bundan sonraki ortaya çıkacak eserlere ne gibi ilham verebileceğine değinilmiştir. En son kısımda ise ortaya atılan teorik iddiaların uygulamaları ve ifadeleri mathematica kodları ile sunulmuştur.

2. MATEMATİKSEL ALTYAPI

Teorem 2.1 (Bölme Algoritması) [22] $b > 0$ olmak üzere a ve b gibi iki tam sayı verilsin. O halde yegane q ve r tam sayıları vardır öyle ki

$$a = bq + r, \qquad 0 \leq r \leq b$$

şeklinde yazılabilir.

Teorem 2.2 [22] a ve b gibi iki tam sayı verilsin. (a, b) notasyonu a ile b sayılarının en büyük ortak bölenini göstermek üzere öyle r ve s tam sayı ikilisi bulunabilir ki

$$(a, b) = ar + bs$$

şeklinde yazılabilir. Dahası $(a, b) = d$ sayısı yeganedir lakin r, s ikilisi tek türlü değildir.

Sonuç 2.1 [22] a ve b aralarında asal iki tam sayı olmak üzere öyle r, s tam sayı ikilisi vardır ki

$$ar + bs = 1$$

yazımını mümkün kılar.

Teorem 2.3 (Aritmetiğin Temel Teoremi) [22] $n > 1$ tam sayısı verilsin. O halde öyle p_i (farklı olmaları gerekmiyor), $1 \leq i \leq k$ asalları vardır ki

$$n = p_1 p_2 \dots p_k$$

şeklinde yazılabilir. Dahası bu gösterim tek türlüdür. Yani şayet q_i, $1 \leq i \leq l$ asalları için de

$$n = q_1 q_2 \dots q_l$$

yazılabiliyorsa o halde $k = l$ dir ve q_i ler p_i lerin bir permütasyonudur.

Tanım 2.1 [23] $m > 1$ tam sayısı belirlenmiş olsun. a ve b iki tam sayısı için şayet $a \equiv b \; mod \; m$ ya da $m|a - b$ oluyorsa a ile b modül m denktir denir. Bu denkliğe göre a nın denklik sınıfı

$$\overline{a} = [a]_m = \{x \in \mathbb{Z} \mid x \equiv a \; mod \; m\}$$

$$= \{x \in \mathbb{Z} \mid x = a + km,\ k \in \mathbb{Z}\}$$

kümesidir. $\overline{a}$ kümesine a nın $mod\ m$ ye göre kalan (rezidü) sınıfı da denir.

Önerme 2.1 [23] $m > 1$ tam sayısı sabitlensin. $\equiv mod\ m$ ifadesi bir denklik bağıntısıdır. Hatta bu m sayısı

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{m-1}$$

şeklinde $\mathbb{Z}$ nin bir parçalanışını meydana getirir.

Teorem 2.4 (Çin Kalan Teoremi) [23] $m = m_1 m_2 \ldots m_r$ sayısı verilsin. m_i ler tam sayı ve $(m_i, m_j) = 1,\ 1 \leq i, j \leq r$ olmak kaydıyla ve seçilmiş bir $c_1, c_2, \ldots, c_r$ tam sayıları için

$$x \equiv c_1\ mod\ m_1$$

$$\vdots$$

$$x \equiv c_r\ mod\ m_r$$

şartlarını sağlayan x tam sayısı yeganedir. Dahası $y \in \mathbb{Z}$ de $y \equiv c_i\ mod\ m_i\ 1 \leq i \leq r$ şartlarını sağlıyor ise o halde $x \equiv y\ mod\ m$ demektir.

Teorem 2.5 (Fermat' ın Küçük Teoremi) [23] p bir asal sayı ve a da bir tam sayı olmak üzere

$$a^p \equiv a\ mod\ p$$

denkliği geçerlidir.

Teorem 2.6 [24] $\alpha = \prod {p_i}^{\vartheta_i}$ ve $\beta = \prod {p_i}^{\mu_i}$, α ve β nın kanonik gösterimleri olmak üzere $\alpha|\beta$ olması için gerek ve yeter koşul $\vartheta_i \leq \mu_i\ (i = 1, 2, \ldots)$ olmasıdır.

Teorem 2.7 [24] $m, b, c \in \mathbb{Z}, m > 0$ olmak üzere $f(x) \in \mathbb{Z}[x]$ için

$$b \equiv c\ (mod\ m) \Rightarrow f(b) \equiv f(c)(mod\ m)$$

dir.

Teorem 2.8 (Euler Teoremi) [24] $(m, a) = 1$ ve $m > 1$ olmak üzere $a^{\varphi(m)} \equiv 1\ (mod\ m)$ dir.

Tanım 2.2 [24] $(\mathbb{Z}/n\mathbb{Z})^* = \{\alpha \in \mathbb{Z}/n\mathbb{Z} : bir\ \beta \in \mathbb{Z}/n\mathbb{Z}\ için\ \alpha\beta = 1\}$ şeklinde bir küme tanımlayalım. Bu kümeye $\mathbb{Z}_n$ nin çarpımsal grubu denir.

Teorem 2.9 [24] $(\mathbb{Z}/n\mathbb{Z})^* = \{x \in \mathbb{Z}/n\mathbb{Z} : (x,n) = 1\}$ olur.

Tanım ve Teorem 2.1 [25] $(G_1,\circ_1)$ ve $(G_2,\circ_2)$ iki grup ve $G \coloneqq G_1 \times G_2$ kartezyen çarpımları olsun. G üzerinde bir $\circ$ işlemini

$$(g_1, g_2) \circ (h_1, h_2) \coloneqq (g_1 \circ_1 h_1, g_2 \circ_2 h_2)$$

şeklinde tanımlarsak $(G,\circ)$ bir grup olur ve bu gruba direkt çarpım grubu denir. $G = G_1 \times G_2$ veya ve $G = G_1 \oplus G_2$ ile gösterilir. ve $G_i\ \ (i \in I)$ sonsuz sayıda grup çarpımı için $\prod_{i\in I} G_i$, sonlu sayıda G_i için ise $\sum_{i\in I} G_i$ notasyonu kullanılır.

Sonuç 2.2 [25] Eğer G sonlu bir grupsa ve $x \in G$ ise $\deg x$ G nin eleman sayısını böler. Bir başka deyişle her $g \in G$ için $g^{|G|} = 1$ olur.

Sonuç 2.3 [25] Eleman sayısı asal olan bir grup daireseldir (devirlidir) ve birim eleman hariç her eleman tarafından üretilir.

Sonuç 2.4 [25] Birbirine asal sayıda elemanı olanı olan iki devirli grubun kartezyen çarpımı da devirlidir.

Sonuç 2.5 [25] $n > 1$ doğal sayısının asallara ayrılmış hali $n = {p_1}^{k_1} \dots {p_r}^{k_r}$ ise bu durumda

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/{p_1}^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_r}^{k_r}\mathbb{Z}$$

olur.

Teorem 2.10 [25] $\varphi: G \to H$ bir homomorfizma ve $Ker\varphi$ de φ dönüşümünün çekirdeği olmak üzere

$$G/Ker\varphi \cong \varphi(G)$$

olur.

Teorem 2.11 [25] n ve m birbirine asal iki doğal sayı olsun. O zaman

$$\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

olur. Ayrıca,

$$\varphi(\hat{x}) = (\overline{x}, \tilde{x})$$

formülüyle (doğal olarak) tanımlanmış $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ fonksiyonu bir izomorfizmadır.

Teorem 2.12 [25] G bir grup, $g \in G$ ve $\deg g = d < \infty$ olsun. O zaman $g^n = 1$ olması için $d|n$ olması gerek ve yeter koşuldur. Bunun sonucu olarak $g^k = g^l$ eşitliğinin doğru olması için gerek ve yeter koşul $d|k - l$ olmasıdır.

Teorem 2.13 [25] Eğer bir grubun bir g elemanının derecesi $d < \infty$ ise

$$\{g^n : n \in Z\} = \{1, g, g^2, \dots, g^{d-1}\}$$

olur ve bu kümenin d tane elemanı vardır. Tersine bu kümenin d tane elemanı varsa o zaman g nin derecesi d dir.

Tanım 2.3 [25] G bir grup ve $H \leq G$ olsun.

$$G/H = \{xH : x \in G\}$$

şeklinde tanımlanan kümeye bölüm kümesi adı verilir.

Teorem 2.14 [25] G bir grup ve $H \leq G$ ise $|G| = |G/H||H|$ olur. Dolayısıyla, eğer G sonluysa $|G/H| = \frac{|G|}{|H|}$ olur.

Tanım 2.4 [26] Bir R halkasında $a, b \in R$ için $a = bu$ olacak şekilde $u \in R$ birimsel elemanı bulunabiliyorsa a ile b ye ilgili elemanlar denir. Bu ilgililik elemanlar arasında bir denklik bağıntısı meydana getirir.

Tanım 2.5 [26] Bir R halkasında $a \in R$ için $a^k = 0$ olacak şekilde bir $k > 0$ tam sayısı bulunabiliyorsa a elemanına nilpotent eleman denir.

Tanım 2.6 [26] Bir R halkasında $a^2 = a$ şeklindeki tüm $a \in R$ elemanları idempotenttir.

Tanım 2.7 [26] R bir halka ve $0 \neq p \in R$ birimsel olmayan bir eleman olsun.

1) $a, b \in R$ için $p = ab$ olması, a veya b nin R de birimsel olmasını gerektirirse p ye R nin bir indirgenemez (atom) elemanı denir.

2) $a, b \in R$ için $p|ab$ olması, $p|a$ veya $p|b$ olmasını gerektirirse p ye R nin bir asal elemanı denir.

Tanım 2.8 [26] P, R halkasının kendisi olmayan (has) bir ideali olsun.

$$a, b \in R, ab \in P \Rightarrow a \in P \; veya \; b \in P$$

gerektirmesi doğru oluyorsa P ye bir asal ideal denir.

Önerme 2.2 [26] R bir halka olsun. $P \subset R$ idealinin asal olması için gerek ve yeter koşul R/P bölüm halkasının bir tamlık bölgesi olmasıdır.

Örnek 2.1 $\mathbb{Z}[x]$ halkasında (n, x) idealinin asal olması için gerek ve yeter koşul n sayısının asal olmasıdır.

Tanım 2.9 [26] M, R halkasının kendisi olmayan bir ideali olsun. R nin M yi kapsayan M den başka hiçbir has ideali yoksa M ye bir maksimal ideal denir.

Önerme 2.3 [26] R bir halka olsun. $M \subset R$ idealinin maksimal olması için gerek ve yeter koşul R/M bölüm halkasının bir cisim olmasıdır.

Sonuç 2.6 [26] Her maksimal ideal asaldır fakat her asal ideal maksimal değildir. Gerçekten $\mathbb{Z}$ tam sayılar halkasında (0) ideali asaldır fakat maksimal değildir.

Örnek 2.2 $\mathbb{Z}$ nin asal idealleri, sıfır ideali ve p asal tam sayı olmak üzere (p) temel idealleridir. Sıfır ideali maksimal değildir fakat diğerleri maksimaldir.

Önerme 2.4 [27] R bir halka ve M de bir ideali olsun. M nin maksimal olması için gerek ve yeter koşul her $x \notin M$ için $1 - rx \in M$ olacak şekilde bir $r \in R$ nin bulunabilmesidir.

Tanım 2.10 [27] R halkasında sadece bir tane maksimal ideal bulunabiliyorsa R ye bir yerel (lokal) halka denir. M bir tek maksimal ideal ise R/M ye de kalıntı (rezidü) cismi denir.

Önerme 2.5 [27] Bir R halkasında birimsel olmayan elemanlar bir ideal oluşturuyor ise bu halkaya yerel halka denir.

Örnek 2.3 $\mathbb{Z}_{p^k}$ halkaları p asal ve $k \geq 2$ için lokal halkalardır. Bir tek asal idealleri ise (p) idealidir. Buradan $\mathbb{Z}_{p^k}/p \cong \mathbb{Z}_p$ yazarak bütün sıfır bölenlerin (p) de toplandığı açıkça görülür.

Tanım 2.11 [27] *R* halkasında *I* ve *J* idealleri $I + J = R$ yi sağlıyorsa bu *I* ve *J* ideallerine aralarında maksimal idealler denir.

Teorem 2.15 (Çin Kalan Teoremi) [27] $n \geq 2$ olmak üzere $I_1, I_2, \dots, I_n$ ler *R* halkasında ikişerli olarak aralarında maksimal idealler olsunlar.

1) Verilen her $a_1, a_2, \dots, a_n \in R$ için

$$a \equiv a_j \ (mod\ I_j), \qquad 1 \leq j \leq n$$

olacak şekilde bir $a \in R$ tek türlü vardır.

2) $f(a) = (a + I_1, a + I_2, \dots, a + I_n)$ ile tanımlı

$$f: R \to R/I_1 \times R/I_2 \times \dots \times R/I_n$$

fonksiyonu örten bir homomorfizmadır.

3) $R/I_1 I_2 \dots I_n \cong R/I_1 \times R/I_2 \times \dots \times R/I_n$ birbirlerine izomorfturlar.

Örnek 2.4 $n > 0$ keyfi tam sayısı için

$$n = {p_1}^{e_1} {p_2}^{e_2} \dots {p_k}^{e_k}$$

olacak şekilde farklı asallar mevcuttur. O halde

$$\mathbb{Z}/(n) \cong \mathbb{Z}/({p_1}^{e_1}) \times \mathbb{Z}/({p_2}^{e_2}) \times \dots \times \mathbb{Z}/({p_k}^{e_k})$$

yazımı mümkündür.

2.1. Polinom Halkaları

Kriptolojide favori halkalar $\mathbb{Z}_p$ ve $\mathbb{Z}_{p^k}$, kodlama teoride ise $\mathbb{Z}_2$ ve $\mathbb{Z}_{2^k}$ dır. Dolayısıyla, polinomlar genellikle bu halka ve cisim yapıları üzerinde tanımlanarak kullanılmaktadır. Bu sebeple daha genel halka özelliklerini vererek başlayalım.

2.2. Halkaların Yapısı ve Özellikleri

Tanım 2.12 [25] Bir R halkası, $+$ işlemi altında değişmeli bir grup ve çarpma işleminin birleşmeli olup toplama işlemi üzerine soldan ve sağdan dağılmalı olduğu bir yapıdır.

Tanım 2.13 [25] Değişmeli bir R halkasında $a \neq 0 \in R$ için şayet bir $0 \neq b \in R$ varsa öyle ki $ab = 0$ olacak şekilde a ya sıfır bölen denir. Benzer şekilde b de bir sıfır bölen olacaktır.

Örnek 2.5 $\mathbb{Z}_6$ halkasında $2.3 = 0$ olur ki sıfır bölenler mevcuttur. Kodlama ve kriptolojide sıfır bölenli halkalar genel itibariyle tercih edilmezler çünkü 0 a eşit olmayan bir kod herhangi bir katı kodlanırken birden 0 a düşebilir. Bu ise hem kod çözmede hem de kod üretmede zorluklar meydana getirmektedir. $\mathbb{Z}_7$ ise iyi huylu bir halkadır. 0 bellidir ve başka bir eleman 0 rolünü oynamaz.

Tanım 2.14 [25] Değişmeli, birimli ve sıfır bölensiz bir halkaya tamlık bölgesi (integral domain) denir.

Teorem 2.16 [25] R birimli ve değişmeli bir halka olsun. Bir $u \in R$ elemanı için aşağıdaki önermeler geçerlidir.

(i) u birimseldir $\Leftrightarrow$ Her $r \in R$ için $u|r$ dir.

(ii) u birimseldir $\Leftrightarrow$ $(u) = R$ dir.

Tanım 2.15 (Karakteristik) [25] Bir R halkasının karakteristiği, her $x \in R$ için $nx = \underbrace{x + x + \cdots + x}_{n\ defa} = 0$ olacak şekilde bir en küçük $n \in \mathbb{Z}^+$ sayısıdır. Eğer böyle bir sayı yoksa R, 0 karakterlidir denir.

Lemma 2.1 [25] R bir tamlık bölgesi olsun. R nin karakteristiği ya asal bir p sayısıdır ya da 0 dır.

Lemma 2.2 [25] R karakteristiği p olan bir tamlık bölgesi olsun. O halde $\forall\, x, y \in R$ için

$$(x + y)^p = x^p + y^p$$

olur.

Tanım 2.16 [25] Boştan farklı bir $I \subset R$ kümesinin R de bir ideal olması için $(I, +)$ nın R nin toplamsal altgrubu ve $\forall r \in R, \forall a \in I$ için $ra \in I$ şartlarını sağlaması gerekir.

Tanım 2.17 [25] Bir $a \in R$ için a elemanının ürettiği ideal $\langle a \rangle$ veya (a) ile gösterilir. (a), a yı içeren en küçük idealdir. Yalnız a tarafından üretildiği için bu tür ideallere esas ideal denir.

Örnek 2.6 $\mathbb{R}[x]$, reel katsayılı x belirsizinin polinomları olsun. Bu halkada bir ideal örneği olarak

$$I = (x^3 + 1) = \{f(x)(x^3 + 1) | f(x) \in \mathbb{R}[x]\}$$

verilebilir.

2.3. Cisimlerin Yapısı ve Özellikleri

Tanım 2.18 [28] Değişmeli ve birimli bir halkada sıfırdan farklı her elemanın tersi yine halkada ise bu halka yapısına cisim denir.

Önerme 2.6 [28] Sonlu bir K cisminin çarpımsal grubu devirlidir.

Teorem 2.17 [28] Keyfi seçilen bir p asalı ve $n \in \mathbb{Z}^+$ sayısı için p^n mertebeli bir cisim mevcuttur.

Teorem 2.18 [28] Herhangi bir cisim $n \in \mathbb{Z}^+$ ve p bir asal sayı olmak üzere p^n elemanlıdır.

Lemma 2.3 [28] p^n elemanlı bir cisim, $x^{p^n} - x$ polinomunun F_p üzerindeki parçalanış cismidir.

Teorem 2.19 [28] K sonlu bir cisim olsun. O halde

1) $|K| = p^n$ olur. Burada p K cisminin karakteristiği ve n de bir pozitif tam sayıdır.
2) K, $x^{p^n} - x$ polinomunun parçalanış cismidir.
3) p^n elemanlı herhangi bir cisim K ile izomorfiktir.

2.4. Halkalar üzerinde polinomlar

Teorem 2.20 [28] R bir halka olduğunda $R[x]$ de bir halka olur.

Teorem 2.21 (Bölme Algoritması) [28] R değişmeli ve birimli bir halka olsun. $f(x), g(x) \in R[x]$ ve $g(x)$ in baş katsayısı R de birimsel eleman olsun. Bu durumda

$$f(x) = q(x)g(x) + r(x) \qquad \deg r(x) < \deg g(x)$$

olacak şekilde tek türlü belirlenebilen $q(x), r(x) \in R[x]$ polinomları vardır.

Teorem 2.22 [28] R birimli ve değişmeli bir halka, $f(x) \in R[x]$ ve $a \in R$ olsun. $(x - a)$ polinomunun $f(x)$ i bölmesi için gerek ve yeter koşul $f(a) = 0$ olmasıdır.

Teorem 2.23 [28] R bir tamlık bölgesi, $f(x) \in R[x]$, $f(x) \neq 0$ ve $\deg f(x) = n$ olsun. Bu durumda $f(x)$ in $R[x]$ de en fazla n tane kökü bulunabilir.

Teorem 2.24 [28] R birimli ve değişmeli bir halka olsun. $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ polinomunda a_0, R nin tersinir bir elemanı ve $a_1, \ldots, a_n$ ler de nilpotent elemanları olsunlar. Bu durumda $f(x)$, $R[x]$ de tersinirdir.

Tanım 2.19 (İndirgenemez Polinom) [28] $R[x]$ değişmeli ve birimli bir halka olsun. Birimsel olmayan bir $0 \neq q(x) \in R[x]$ için $q(x) = a(x)b(x)$ oluyorken mutlaka $a(x)$ veya $b(x)$ ten birinin birimsel eleman olması gerekiyorsa $q(x)$ indirgenemezdir denir.

Tanım 2.20 (Asal Polinom) [28] $R[x]$ birimli ve değişmeli bir halka $0 \neq p(x) \in R[x]$ de birimsel olmayan bir elemanı olsun. $p(x)|a(x)b(x)$ olması $p(x)|a(x)$ veya $p(x)|b(x)$ durumlarından birini gerektiriyorsa $p(x)$ $R[x]$ in bir asal elemanıdır denir.

Teorem 2.25 [28] $R[x]$ bir tamlık bölgesi olsun. $R[x]$ in asal elemanları aynı zamanda indirgenemez elemanlardır.

Teorem 2.26 [28] $R[x]$ bir tamlık bölgesi olsun. $p(x) \in R[x]$ in indirgenemez olabilmesi için gerek ve yeter koşul $p(x)$ in, $R[x]$ deki bütün öz esas idealler kümesinde maksimal ideal üretmesidir.

Tanım 2.21 [28] $R[x]$ polinom halkasında esas ideallerin

$$\big(a_1(x)\big) \subset \big(a_2(x)\big) \subset \cdots$$

şeklindeki her bir zinciri için bir $n \in \mathbb{Z}^+$ sayısı bulunabiliyorsa öyle ki her $k \geq n$ için $\big(a_n(x)\big) = \big(a_k(x)\big)$ oluyorsa $R[x]$ esas idealleri için artan zincir koşulunu sağlıyor denir.

2.5. Cisimler üzerinde polinomlar

Polinomlar, güçlü cebirsel özellikler barındırması bakımından genellikle bir F cisminin üzerinde ele alınırlar. $F[x]$ diye, bir x belirsizinin F cismi üzerindeki polinomları kastedilir.

Uyarı 2.1 Polinom ve fonksiyon genelde aynı işlevi görse de aksi durumlarda mevcuttur. Örneğin, $f(x) = x^2 + x + 1$ ve $g(x) = x^4 + x + 1$ polinomları $\mathbb{Z}_3[x]$ de göz önüne alınırlarsa ikisi de farklı polinomlar olmalarına karşın aynı işlevi gördüklerinden aynı fonksiyondurlar. Bu durum $\mathbb{Z}_3[x]$ halkasının bir karakteristik taşımasından kaynaklanır. Farklı polinomlar aynı denklik sınıfına düşebilirler. Kodlama ve kriptolojide bu tip halka ve kod polinomlarına özellikle dikkat etmek gerekir.

K bir cisim olsun. Katsayıları K den seçilen bir x değişkeninin polinomlarını $K[x]$ ile gösterelim. O halde $K[x]$ de üç çeşit eleman bulunabilir

- Birimsel (tersinir) elemanlar,
- İndirgenebilir elemanlar,
- İndirgenemez elemanlar.

Önerme 2.7 [29] K cisim ise $K[x]$ bir tamlık bölgesi olur.

Önerme 2.8 (Küçük dereceli polinomların indirgenemezliği üzerine) [29] F bir cisim, $f(x) \in F[x]$ ve $\deg f = 2$ veya $\deg f = 3$ olsun. $\exists c \in F$ için $f(c) = 0$ oluyorsa o zaman f indirgenemez değildir.

Uyarı 2.2 Önerme 2.8, kök bulunduğunda kesinlikle indirgenebilirliği garanti ederken kök bulunmaması indirgenemezlik anlamına gelmemelidir. Örneğin, $(x^2 + 1)^2 \in \mathbb{R}[x]$ polinomunun $\mathbb{R}$ de kökü yoktur fakat polinom kendisinin ikinci kuvveti olduğundan açıktır ki indirgenir.

Lemma 2.4 [29] $f \neq 0$ $K[x]$ de bir polinom olsun. f polinomunun K nın bir cebirsel genişlemesinde katlı kökünün olması için gerek ve yeter koşul f' f nin türevi olmak üzere $\deg(f, f') \geq 1$ olmasıdır.

Teorem 2.27 [29] F bir cisim ise $F[x]$ bir temel ideal bölgesidir. Yani $F[x]$ de her ideal yalnız bir elemanı tarafından üretilebilirdir.

Sonuç 2.7 [29] F bir cisim olduğunda $F[x]$ esas ideal bölgesi olur ve artan zincir koşulunu sağlar.

2.6. İndirgenemez Çarpanlar Bulmak

Şayet $u \in R$ birimsel bir eleman ise o zaman herhangi bir $x \in R$ için aşikar olarak $y = u^{-1}x$ olmak kaydıyla

$$x = uy$$

yazılabilir. Bir y elemanına x ile ilgilidir denir ancak ve ancak $x = uy$ olacak şekilde bir u terslenebilir elemanı mevcuttur. Belirtelim ki $x = yz$ nin x in bir tam faktör ayrışımı olabilmesi için ne y nin ne de z nin birimsel olmaması gerekmektedir. Tam olmayan (aşikar) durumlarda ise y veya z den birisi birimsel olur. Şayet R nin terslenebilir elemanları kümesine $U(R)$ dersek $U(R)$ çarpma işlemi altında grup oluşturacaktır. Şimdi ilgililik, birimsellik ve indirgenemezlik hakkında birkaç önerme verelim. Birbiriyle ilgili olmanın bir denklik bağıntısı oluşturacağını belirtip x ve y elemanlarının birbiriyle ilgililik notasyonu olarak $x \sim y$ kullanılsın.

Önerme 2.9 [25] Bir D bölgesinde

- **a)** x birimseldir ancak ve ancak $x|1$ dir.
- **b)** Herhangi iki birimsel eleman birbiriyle ilgilidir ve birimsel eleman ile ilgili olan herhangi bir eleman birimseldir.
- **c)** x ve y birbirleriyle ilgilidir ancak ve ancak $x|y$ ve $y|x$ dir.
- **d)** Bir x elemanı indirgenemezdir ancak ve ancak x in her böleni x ile ilgilidir veya x in her böleni bir birimsel eleman ile ilgilidir.
- **e)** Bir indirgenemez eleman ile ilgili her eleman da indirgenemezdir.

Önerme 2.10 [25] D bir bölge ve x ile y de sıfırdan farklı elemanlar olmak üzere

- **a)** $x|y \Leftrightarrow (x) \supseteq (y)$
- **b)** $x \sim y \Leftrightarrow (x) = (y)$
- **c)** x birimseldir $\Leftrightarrow (x) = D$.
- **d)** x indirgenemezdir $\Leftrightarrow (x)$, D nin öz alt idealleri arasında maksimaldir.

2.7. İndirgenemez Çarpanlara Ayrışımın Yegane Olmadığı Bazı Halkalar

Bir D bölgesinde bir $\alpha \in D$ için p_i ve q_i ler indirgenemez elemanlar olmak üzere

$$\alpha = p_1 p_2 \dots p_r = q_1 \dots q_s \qquad (4)$$

olması mutlaka $r = s$ olmasını veyahut q_j lerin p_i lerin bir permütasyonu olmasını gerektiriyorsa (4) yazımı tek türlüdür denir. Şayet her $\alpha \in D$ için (4) deki tek türlü yazım mümkün ise D ye tek türlü çarpanlara ayrılma bölgesi (TAÇ) denir. Örneğin $\mathbb{Z}$ bir TAÇ bölgesidir. $15 = 3.5 = 5.3$ olarak indirgenemez 3 ve 5 elemanlarının çarpımıdır ve bu yazım tek türlü belirlidir. Bununla birlikte aksine örnek olarak $\mathbb{Q}(\sqrt{d})$ halkaları en azından d nin -5 veya -6 değerleri için TAÇ değildir.

$$6 = 2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

örneğini vermek yeterli olacaktır.

TAÇ bölgesi, kriptolojik bir algoritma üretirken veya cebirsel bir kod kümesi seçerken büyük öneme sahiptir. Kriptolojik sistemin deşifre safhasında ve kod sözcüklerin kod çözme (decoding) kısımlarında ikilik veya karmaşıklık oluşmaması adına polinomların çarpanlarına ayrışımları tek türlü belirlenmelidir.

2.8. Galois Halkaları ve Cisimleri

p bir asal sayı ve $t \geq 1$ pozitif tam sayısı için F_{p^t} şeklinde gösterilen, karakteristiği p, eleman sayısı p^t olan sonlu cisimlere Galois cisimler denir. Benzer bir tanım halkalar için de verilebilir. $p^t = q$ için $GF(q)$ notasyonu ile gösterilir. Kolaylık açısından F_q ile gösterelim. Şimdi Galois cisimlerin temelini teşkil eden bir teorem verilecektir.

Teorem 2.28 [30] $q = p^t$, p asal olmak üzere

- **(i)** Her n pozitif sayısı için $F_q[x]$ de n. dereceden indirgenemez polinomlar mevcuttur.
- **(ii)** $F_q[x]$ de indirgenemeyen her polinomun tamamen lineer çarpanlara ayrıldığı cisim bir $n \in \mathbb{Z}^+$ için F_{q^n} dir.
- **(iii)** g, $F_q[x]$ de indirgenemeyen bir polinom olsun. $\deg g = d$ olmak üzere $g | x^{q^n} - x \Leftrightarrow d | n$ dir.
- **(iv)** İndirgenemez bir g polinomunun bir kökü $F_{q^n}[x]$ de mevcut ise o halde her kökü ve keza lineer çarpanlar şeklinde yazımı $F_{q^n}[x]$ cisminde mümkündür.
- **(v)** $x^{q^n} - x$ polinomu $F_{q^n}[x]$ deki monik ve indirgenemez ve aynı zamanda dereceleri n yi bölen tüm polinomların çarpımıdır.

2.9. Sonlu Cisimlerin Yapısı ve İnşası

Asal bir F_p cismi yardımıyla F_p yi kapsayan bir F_{p^n} cismini kurmak mümkündür. $F_p[x]$ polinom halkasında belirlenmiş her $n \in \mathbb{Z}^+$ için indirgenemez polinom elde etmek mümkündür. Buradan şayet bu bulunan indirgenemez polinoma $q(x)$ denirse, $F_p[x]/(q(x))$, F_p üzerinde n boyutlu bir vektör uzayıdır. Her vektör uzayı kendisi üzerinde bir boyutlu olduğundan aslında $F_p[x]/(q(x))$ bir cisim olur. Sonlu cisimlerin ve inşa yöntemiyle bir üst cisme geçmenin kriptolojik sistemlerde uygulamaları geniştir. Bir algoritmik şifrelemenin ya da kod halkasının daha geniş bir halkada (cisimde) nasıl davranacağını incelemek bakımından indirgenemez polinomlar ve kapsayan üst cisim bulma problemlerinin cebirsel kriptolojiye katkısı yadsınamazdır.

Teorem 2.29 p bir asal sayı ve $s \geq 1$ pozitif tam sayı olsun.

(i) $s > 1$ için $\mathbb{Z}_{p^s}$ sıfır bölenli bir halkadır.

(ii) $s \geq 1$ için $\mathbb{Z}_{p^s}/(p)$ cisimdir.

İspat

(i) $\mathbb{Z}_{p^s} = \{a + \mathbb{Z} : 0 \leq a < p^s\}$ olur ve $s > 1, p \neq 0$ için $pp^{s-1} = p^s = 0$ olduğunda sıfır bölenler mevcuttur.

(ii) $s \geq 1$ ve $a \in \mathbb{Z}_{p^s}$ alınsın. a ve p ye bölme algoritması uygulanırsa

$$a = qp + r, \qquad 0 \leq r < p$$

olur ki bu ifade $\mathbb{Z}_{p^s}$ de bir denklem olarak da değerlendirilebilir. Burada $\overline{a} = \overline{r}$ olur ve her ikisi de $\mathbb{Z}_{p^s}/(p)$ nin içine düşer. $\mathbb{Z}_{p^s}/(p) = \{\overline{0}, \overline{1}, \overline{2}, \dots, \overline{p-1}\}$ olup bir $\overline{r} \neq \overline{0}$ için

$(r, p) = 1$ olacağından öyle c, d tam sayıları bulunur ki

$$cr + dp = 1 \qquad (5)$$

yazımı mümkün olur. (5) şayet $\mathbb{Z}_{p^s}$ de bir denklem ise $mod\ p$ indirgemesi yaparsak $\overline{c}\,\overline{r} = \overline{1}$ sonucuna ulaşılır ki bu $\overline{r}$ nin bir tersi olduğu anlamına gelir. Burada $\mathbb{Z}_{p^s}/(p)$ (aslında $\mathbb{Z}_p$ ye izomorf) bir cisimdir. ⊠

Teorem 2.29, kalan sınıflar halkası teşkil edilirken seçilen modülün yapısına dair bir temel fikir öne sürmektedir. Örneğin, $\mathbb{Z}_4$ halkasında $2 \neq 0$ ve $2.2 = 0$ olması sıfır bölenli bir halka olduğu anlamına gelir. Bu modülün bir $f(x)$ polinomu olması ve halkanın da $F[x]$ olması halinde şayet $f(x) = f_1(x).f_2(x)$ ve $\deg f_1(x) < \deg f(x)$,

$\deg f_2(x) < \deg f(x)$ ise benzer düşüncelerle $f_1(x) \neq 0$ ve $f_2(x) \neq 0$ olmasına karşın $f_1(x).f_2(x) = f(x) = 0$ olması sebebiyle sıfır bölenler üretecektir. Kodlama teorideki üreteceği problem $(f_1(x))$ idealinin birçok katının direk 0 olması ve kod çözmede sorun teşkil etmesidir. Bu saiklerle modülün indirgenemez seçimi mühimdir.

Lemma 2.5 [30] $f \in F_q[x]$ indirgenemez bir polinom olsun ve bir α bir genişleme cisminde f nin bir kökü olsun. O halde $h \in F_q[x]$ için $h(\alpha) = 0$ olması için gerek ve yeter şart $f|h$ olmasıdır.

Teorem 2.30 [30] $f \in F_q[x]$ n. dereceden indirgenemez bir polinom ise f nin bir kökü olan α F_{q^n} dedir. Dahası diğer bütün kökler F_{q^n} dedir ve $\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{m-1}}$ elemanlarıdır.

Bu teorem sonlu cisimler inşa ederken asal cisimden alınan bir indirgenemez polinomun kökünü barındıran üst cisimde diğer köklerin asal cismin karakteristik kuvvetlerini almanın yeterli olduğunu ifade etmesi bakımından önemlidir.

Teorem 2.31 [30] p asal sayı ve $\pi(x)$ $F_p[x]$ de n. dereceden indirgenemez bir polinom olsun. O halde $F_p[x]/(\pi(x))$ p^n elemanlı bir cisimdir.

Teorem 2.32 [30] E ve F, $F \subset E$ olacak şekilde iki cisim, $\alpha \in E$, $P(x)$ mertebesi n olan, F üzerinde indirgenemez bir polinom ve $P(\alpha) = 0$ olsun. O halde

(i) $F \subset F[\alpha] \subset E$ olacak şekilde $F[\alpha]$ bir cisimdir.

(ii) $F[\alpha]$ nın herhangi bir elemanı

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \qquad a_i \in F$$

olacak şekilde tek türlü bir gösterime sahiptir.

(iii) $F[\alpha] \cong F[x]/(P(x))$ dir.

(iv) $F[\alpha] = F(\alpha)$ dir.

(v) F, q elemanlı sonlu bir cisim ise $|F[\alpha]| = q^n$ dir

koşulları gerçeklenir.

Önerme 2.9 [30] $x^{p^n} - x \in K_p[x]$ polinomunun tüm kökleri ayrıktır.

Lemma 2.6 [30] Her $f(x) \in F_p[x]$ için $f\left(x^{p^m}\right) = f(x)^{p^m}$, $m \geq 0$ olur.

Teorem 2.33 [30] F bir cisim ve $f(x)$ de mertebesi n olan F üzerinde bir polinom olmak üzere

$$S = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} : a_i \in F\}$$

kümesi, $f(x)$ in $F[x]$ deki kalan sınıflarının tüm kümesinin bir başka gösterimidir.

Teorem 2.34 [30] $g(x)$, F_p üzerinde indirgenemez ve $g(x)|\left(x^{p^m} - x\right)$ olsun. O zaman $\deg(g(x))$, m nin bir bölenidir.

Teorem 2.35 [30] m ve n pozitif tam sayılar olmak üzere $(m, n) = d$ olsun. Herhangi bir cisim üzerinde bir cisim üzerinde $(x^m - 1, x^n - 1) = x^d - 1$ olur.

Tanım 2.22 [30] $f(x)$, F_q üzerinde $n.$ dereceden monik bir polinom olsun. Şayet F_{q^n} in bir ilkel elemanı $f(x)$ in F_q üzerinde bir kökü oluyorsa bu durumda $f(x)$ e F_q üzerinde $n.$ dereceden ilkel polinom denir.

Teorem 2.36 [30]

- **(i)** Herhangi bir n pozitif tam sayısı için F_q üzerinde $n.$ dereceden ilkel polinom vardır.
- **(ii)** Bir ilkel polinomun tüm kökleri ilkeldir.
- **(iii)** Tüm ilkel polinomlar üzerinde tanımlı oldukları cisimde indirgenemezdirler.
- **(iv)** $n.$ dereceden indirgenemez ilkel polinomların bir F_q cismi üzerindeki toplam sayısı $\frac{\varphi(q^n-1)}{n}$ dir.

2.10. Döngüsel Polinomlar ve Birimin Kökleri

Bu bölümde, $x^n - 1$ polinomunun köklerinin ne olduğu ve nerede bulunabileceğine dair tanım ve lemmalar verilecektir.

Tanım 2.23 [31] n pozitif bir tam sayı olsun. $x^n - 1$ polinomunun tamamen köklerinin lineer çarpanlarına ayrılabildiği cisme $n.$ döngüsel cisim denir ve taban cisme K denirse $K^{(n)}$ ile gösterilir. Bu köklerin kümesi ise $E^{(n)}$ ile gösterilir.

Teorem 2.37 [31] n pozitif bir tam sayı ve K karakteristiği p olan bir cisim olmak üzere

- **(i)** $p \nmid n$ ise $E^{(n)}$ mertebesi n olan devirli bir grup olur.
- **(ii)** $p|n$ ise $n = mp^e$ olmak üzere o halde $K^{(n)} = K^{(m)}$ ve $E^{(n)} = E^{(m)}$ olur.

Tanım 2.24 [31] n pozitif bir tam sayı, K karakteristiği p olan bir cisim ve $p \nmid n$ olsun. $E^{(n)}$ devirli grubunun üreteçlerine birimin n. ilkel kökleri denir.

Tanım 2.25 [31] K karakteristiği p olan bir cisim, $n \in \mathbb{Z}^+$, $p \nmid n$ ve τ birimin n. ilkel kökü olsun. O halde

$$Q_n(x) = \prod_{\substack{s=1 \\ (s,n)=1}}^{n} (x - \tau^s)$$

şeklinde tanımlı polinoma K üzerinde n. döngüsel polinom denir.

Açıktır ki $Q_n(x)$ polinomu τ kök seçiminden bağımsızdır. $\deg(Q_n(x)) = \varphi(n)$ dir.

Teorem 2.38 [31] K karakteristiği p olan bir cisim, $n \in \mathbb{Z}^+$ ve $p \nmid n$ olmak üzere

(i) $x^n - 1 = \prod_{d|n} Q_d(x)$,

(ii) $Q_n(x)$ polinomunun katsayıları asal cisim K dadır.

Örnek 2.7 $x^n - 1 = \prod_{s=1}^{n}(x - \tau^s)$ olacağından $Q_n(x) = \frac{x^n - 1}{\prod_{d|n,\ d<n} Q_d(x)}$ olacağı açıktır.

Buradan $Q_1(x) = x - 1$ ve bir p asalı için $Q_p(x) = 1 + x + x^2 + \cdots + x^{p-1}$ olduğu görülür.

3. KOD BAZLI KRİPTOSİSTEMLER

3.1. Kod Teorisi

Kod teorisinin temeli, 1940 lı yıllarda Goloy, Hamming ve Shannon' un çalışmalarına dayandırılabilir. Daha kompleks ve güçlü matematik araçlarla kod teori gelişimini artırarak sürdürmüştür. Kod teori cebirsel geometri üzerine kurulu geometrik kodlar ve graf teorisi üzerine kurulu düşük yoğunluklu parite kontrol kodları gibi temel iki kısımda incelenebilir. Kod teorinin temel amacı ise bilgiyi gönderme, bilgiyi sıkıştırma, kaynağı gizleme ve hataları düzeltme başlıkları altında verilebilir. En yaygın ve kapsamlı kod teorisi çalışmalarını ise 1978 de McEliece yapmıştır. Bu çalışmalarda açık anahtar bir lineer kod, gizli anahtar ise bir deşifreleme algoritmasıdır. Yine bu yöntemde bir e hatası ve t genişliği ile kod sözcükleri maskeleniyordur.

McEliece sisteminin zorluğu RSA veya diğer iyi bilinen açık anahtar kriptosistemlerinin aksine çarpan bulma zorluğu veya ayrık logaritmayı hesaplayabilme güçlüğüne dayanmaz. Bu sistemin güçlüğü keyfi bir hata payını nasıl ayıklayıp açık metne ulaşılabilirliği hedefler McEliece kendisinden önce kurulmuş tüm sistemlerden daha hızlıdır. Ayrıca daha geniş anahtar uzayına haizdir. Dahası işlemci de az yer kaplar. Tüm bunlara rağmen etkinliği, hızı ve güvenliği gelecekte daha da artacaktır **[32].**

3.1.1. Kodlama teorisinin temel amacı

Kodlama çalışmaları özellikle gizli mesajlar göndermeyi değil daha çok bilginin doğru ulaştığını, alınan mesajın ne kadar gerçeğe yakın olabileceği gibi konularla ilgilenir. İlave bilgi ve açıklamaları mesaja ilintileyip alıcının muhtemel oluşacak hataları temizleyip mümkün olabildiğince mesaja net ulaşması amaçlanır.

Kod bazlı sistemler genellikle hata düzeltme kodları üzerine kurulduğu için ve bir kod bazlı sistemi çözmek ve kod kırmak NP (Non-polynomial time) bir zorluk olduğundan tüm kodlama teorileri ve özelde McEliece sistemi düz mesajın veya gönderilmiş mesajın (şifreli metin) yanına ilave tanım, bilgi, detay vs. eklemek esasına dayanır. Fakat ilave bilgi şifreli metne iliştirilirse açık anahtar, düz metne yerleştirilirse gizli anahtar açığa çıkacağından seçimin dikkatli yapılması gerekir **[32].**

Şimdi McEliece kriptosistemine geçmeden önce bilinmesi gereken bazı tanım, teorem ve kriptolojik arka plana değinilecektir.

Tanım 3.1 [32] Bir C kodu, A bir sonlu cisim olmak üzere $A^n = A \times A \times ... \times A$ (n kopya) vektör uzayının herhangi bir altkümesidir. A cismi burada C kodunun alfabesini oluşturur. n sayısı kodun uzunluğunu belirtir.

Tanım 3.1 de A nın sonlu bir cismi işaret etmesine karşılık genellikle kolaylık bakımından $A = F_2$ cismi alınır. Hatta bazı çalışmalarda A yerine bir halka alınmıştır.

Tanım 3.2 [32] $\underbrace{A \times A \times ... \times A}_{n}$ kümesinin herhangi bir elemanına sözcük denir.

Tanım 3.3 [32] Bir $c \in A^n$ şayet $c \in C$ oluyorsa o halde c bir kod sözcüğüdür.

Tanım 3.4 [32] Bir C kodu A^n nin bir altvektör uzayı oluyorsa o halde C ye A üzerinde bir lineer kod denir.

Tanım 3.5 [32] Bir C kodunun boyutu, C kodunun A üzerinde vektör uzayı olunca boyutuna eşittir.

Hemen belirtelim ki, sonlu bir F_q cismi ve bu cisim üzerinde k boyutlu bir C uzayı verilirse aslında bir k boyutlu C lineer kodunu ve $boy\ C = k$ olduğundan ve $q^k = |C|$ olacağından bu kodun sözcük sayısını elde ederiz.

Tanım 3.6 $x = (x_1, x_2, ..., x_n)$ ve $y = (y_1, y_2, ..., y_n) \in A^n$ olsunlar. x ten y ye Hamming mesafesi

$$d_{ham}(x, y) = |\{i | x_i \neq y_i\}|$$

şeklinde tanımlanır.

Lemma 3.1 [32] Hamming mesafesi A^n de bir metriktir.

Tanım 3.7 [32] Bir w sözcüğünün Hamming genişliği $d_{ham}(w, 0^n)$ dir.

Tanım 3.8 [32] Bir lineer C kodunun minimum mesafesi d ye C deki kod sözcüklerinin birbirlerine olan minimum uzaklığına denir. Matematiksel olarak

$$d = \min\{d_{ham}(x, y) | \, x, y \in C\}$$

Tanım 3.9 [33] Uzunluğu n, boyutu k ve minimum mesafesi d olan bir C lineer kodu $[n, k, d]$ şeklinde gösterilir.

Not edelim ki minimum mesafe d lineer bir kodun en temel özelliğidir. Hataları bulmada ve ayıklamada bu d sayısı karakteristik bir özellik görevi görür.

Tanım 3.10 [33] Bir x kod sözcüğünün transferi esnasında t adet harfin yeri değişmiş olsun. Bunu 0 dan farklı koordinatların yerine t adet değişmiş harften oluşan bir e hata vektörü ile temsil edelim. O halde $z = x + e$ vektörü ulaşmış olacaktır. Şayet C kodu bu e hata vektörünü ortadan kaldırıp x açık metnine ulaşabiliyorsa C kodu t adet hataya kadar düzeltme yapabilir denir.

Teorem 3.1 [33] C kodu bir $[n, k, d]$ lineer kodu olsun. O halde C, en fazla $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ adet hatayı düzeltebilir.

Hata bulma: Varsayılsın ki bir $c \in C$ kod sözcüğü bir kaynaktan gönderilmiş olsun. Bu transform esnasında $0 < t < d$ olmak üzere t tane hata oluşmuş olsun (yani bir sözcükteki t tane harf değişmiş olsun). C kodunda mesafelerin en kısası d olduğundan ve $t < d$ olduğundan alıcıya giden c' sözcüğü bir kod sözcüğü değildir. Böylece alıcı bir hata oluştuğunu fark eder. Dikkat edilsin ki $t \geq d$ durumunda alıcıya giden c' sözcüğü halen bir kod sözcüğü olacağından bir hata olabileceği anlaşılmayacaktır. Böylece düzeltilmesi gereken bir hata da olmayacaktır. Bu sebeple bir $[n, k, d]$ lineer kodu $t < d$ tane hata ayıklar denir.

Hata düzeltme: Bir önceki aşamada bir hata bulunduğunu kabul edip bunun nasıl giderileceğine dair bir yaklaşım verilecek olsun. Varsayılsın ki $t \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ adet hata oluşsun.

En yakın kod sözcüğünü bulmak amacıyla her bir kod sözcüğü etrafında $\left\lfloor \frac{d-1}{2} \right\rfloor$ yarıçaplı daireler çizilir. Kod sözcükleri arasındaki mesafe $d > 2\left\lfloor \frac{d-1}{2} \right\rfloor$ olduğundan bilinir ki bu daireler kesişmez. Bu daireler kesişmeyeceğinden her bir daire kod sözcüğüyle eşleşirse daire içinde veya dışında kod sözcükleri bulunmayacağından en yakın kod sözcüğüne ulaşmaya çalışılır.

3.2. Blok Kodlar ve Üreteç Matrisleri

Bir $[n, k, q]$ kodu göz önüne alınsın. Kod bir F_q cismi üzerinde tanımlı ise bu cisim üzerinde vektör uzayı olduğunda bir baz kümesi seçilir. $\{x_1, x_2, \dots, x_k\}$ kodun bazı olsun.

$x_i = (x_{i,1}, \dots, x_{i,n})$ olmak kaydıyla bir X, $k \times n$ matrisi x_i ler satırları oluşturacak şekilde belirlenir yani,

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{k,1} & x_{k,2} & \cdots & x_{k,n} \end{pmatrix}$$

olsun. O halde X matrisi kodun üreteç matrisi olur. Yani bir kod sözcüğü X matrisinin satırlarının bir lineer kombinasyonudur. Şayet $a = (a_1, \dots, a_k) \in F_q^k$ sözcüğü kodlanmak isteniyorsa yapılması gereken tek şey,

$$a' = aX$$

matris çarpımını yapmaktır. Not edilsin ki bir kodun üreteç matrisi tek türlü belirli değildir. Herhangi bir baz kümesinin bir lineer terkibi de baz kümesi olacağından yeni bir üreteç matrisi bulmak mümkündür. Hesaplamada kolaylık bakımından bazen üreteç matrisler eşelon forma indirgenebilirler **[34].**

3.3. Devirli Kodlar

Lineer kodlar ailesinin çok özel bir alt türü olan devirli kodlar kod teoride çok önemli bir yer tutmaktadırlar.

Tanım 3.11 [35] C, F_q cismi üzerinde bir $[n, k, d]$ kod olsun. Şayet

$$\forall s = (s_0, s_1, \dots, s_{n-1}), s \in C \Rightarrow s' = (s_{n-1}, s_0, \dots, s_{n-2}) \in C$$

oluyorsa yani bir kod sözcüğünün her sağ ötelenişi yine bir kod sözcüğü oluyorsa C bir devirli koddur denir.

Kod ailesinin önemli bir alt türü oluşu, cebirsel bazı özelliklere binaendir. Şöyle ki $F_q(x)/(x^n - 1)$ polinomlar halkasından F_q üzerinde devirli bir C koduna birebir bir

dönüşüm tanımlanabilir. C de bir $a = (a_0, a_1, \dots, a_{n-1})$ vektörünü $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ polinomu ile eşlersek a vektörünün her sağ ötelenişini halkada a polinomunun x ile çarpımı temsil eder. Polinom halkasında bir $g | x^n - 1$ polinomu için ideal mevcuttur. İşte $x^n - 1$ in her bir monik g böleninin ürettiği ideal C de bir devirli koda karşılık gelecektir. Böylece g ye devirli kodun üreteç polinomu denir.

Tanım 3.12 [35] C, F_q üzerinde bir $[n, k]$ devirli kodu olsun. Şayet $g(x)$, $F_q[x]/(x^n - 1)$

halkasının bir ideali ise $\beta = \{g(x), xg(x), \dots, x^{k-1}g(x)\}$ C için bir bazdır ve C kodunun üreteç matrisi

$$G = \begin{pmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{pmatrix}$$

olur.

Teorem 3.2 [35] Bir lineer C kodunun devirli olması için gerek ve yeter şart C nin $F_q[x]/(x^n - 1)$ de bir ideal olmasıdır.

Tanım 3.13 [35] $C = (g(x))$ bir devirli kod olsun. $g(x)$, C kodunu üretiyorsa, $h(x) = \frac{x^n - 1}{g(x)}$ polinomuna C kodunun parite kontrol polinomu denir.

Tanım 3.14 [35] C, F_q üzerinde bir lineer kod ve C nin boyutu k olsun. $x.y = \sum x_i y_i$ standart Öklid çarpımı olmak üzere

$$C^{\perp} = \{y \in F_q^n | x.y = 0 \ \ \forall x \in C\}$$

kümesi $n - k$ boyutlu bir vektör uzayıdır. Aynı zamanda bir lineer kod teşkil eder ki bu koda C nin dual kodu denir.

Tanımdan anlaşılacağı üzere C bir lineer kod iken $C^{\perp}$ yeni bir lineer kod olarak elde edilmiştir. O halde bir kodun dual kodu onun karakteristik özelliğidir denebilir. Bir C kodundan yeni bir $C^{\perp}$ kodu elde edilebileceği gibi her olan iki farklı koddan da yeni bir kod türetilebilir:

Direkt toplam kodu: F_q üzerinde iki lineer kod C_1, C_2 olmak üzere $C_1 \oplus C_2 = \{(u, v) | u \in C_1, v \in C_2\}$ direkt toplam uzayı F_q üzerinde yeni bir lineer kod belirtir. Dahası şayet G_1 ve G_2 sırasıyla C_1 ve C_2 nin üreteç matrisleri iseler

$\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$ matrisi de $C_1 \oplus C_2$ nin üreteç matrisidir.

Şimdi devirli kodların önemli bir cebirsel özelliği lemma olarak verilecektir.

Lemma 3.2 [35] n uzunluğundaki her devirli K kodu $\deg(q(x)g(x)) < n$ olacak şekildeki her $q(x)$ polinomu için

$$g(x) \in K \Rightarrow q(x)g(x) \in K$$

özelliğine haizdir.

Bu lemmanın bir yorumu da devirli kodun her elemanının ideali de devirli kodun elemanlarıdır şeklindedir.

Yine bu lemmanın önemli bir sonucu olarak; bir devirli kodun üreteç polinomunun monik olarak seçilmesi durumunda yegane olacaktır. Aynı mertebeden iki polinom şayet aynı kodu üretiyorsa o halde biri diğerinin skaler katı olmalıdır. Özellikle kodun cisim üzerinde tanımlanması durumunda her skaler kat cismin içerisinde olacağından devirli koda ait üreteç ve monik polinom tek türlü olarak bulunacaktır.

Şayet $x^n - 1$ in F_q da kökleri bulunabilirse ki bunlar birimin $n.$ kökleridir bu durumda devirli bir kod üreteç polinom vasıtasıyla değil de farklı bir yoldan belirtilmiş olur. Şöyle ki;

$$x^n - 1 = \prod \prod m_i(x)$$

olsun, eğer $m_i(x)$ polinomları indirgenemez polinomlar ise monik yapılmaları durumunda $x^n - 1$ in köklerinin minimal polinomu olurlar. Bu durumda aşağıdaki teorem yardımıyla yeni bir devirli kod sıfırlar kümesi üzerinden tanımlanabilir:

Teorem 3.3 [36] $g(x) = g_1(x)g_2(x) \dots g_t(x)$, $x^n - 1$ in indirgenemez çarpanlarının çarpımı olsun. $\{a_1, a_2, \dots, a_t\}$, g nin kökleri olsun.

$$\langle g(x) \rangle = \{f(x) \in R_n | f(a_1) = 0, \dots, f(a_t) = 0\}$$

şeklinde seçilen her $f(x)$ için yeni bir devirli kod elde edilir.

Şimdi de bir devirli kodun üreteç polinomunun nerede aranacağına dair çok önemli bir teorem verilsin.

Teorem 3.4 [35] n uzunluğundaki her devirli kodun üreteç polinomu $x^n - 1$ in bir bölenidir ve yine $x^n - 1$ in her tam böleni bir devirli kodun üreteç polinomudur.

Aşağıdaki iki lemma bir kodun gönderiminde meydana gelebilecek hata polinomunun ne olabileceği üzerine önem arz etmektedir.

Lemma 3.3 [36] Bir kod sözcüğünün iletimi esnasında meydana gelen hata e ve alıcıya ulaşan (kod sözcüğü olmayan) w sözcüğü arasında g üreteç sözcük olmak şartıyla

$$w = qg + e$$

olacak şekilde bir q sözcüğü mevcuttur.

Lemma 3.4 [35] Bir w sözcüğünün kodlanması esnasında meydana gelen hata e ise bu hatalı w sözcüğünün her devirsel ötelemesinin hatası da e nin devirsel ötelemelerdir. Yani $w(x) = q(x)g(x) + e(x)$ ise $x^k w(x) \equiv x^k e(x)\ mod\ g(x)$ olur.

Artık ilk kod tabanlı kriptosistemin detaylı incelemesi verilebilir:

3.4. McEliece Kriptosisteminin Matematiği

Bir $C,\ [n, k, q]$ lineer kodu ve karşılık gelen üreteç matrisi G verilmiş olsun. Bir M mesajını k bloklara ayırıp göndermek için yapılması gerekenler:

1) Terslenebilir (tekil olmayan) bir S matrisi ve P permütasyon matrisi seçip

$$\hat{G} = SGP$$

matrisini oluşturmak, (S, P) yi gizli anahtar olarak tutup $\hat{G}$ yi açık anahtar olarak paylaşmak,

2) k bloğa ayrılan her bir m mesajın, z, uzunluğu n ve genişliği $\leq d$ olan bir hata vektörü olmak üzere

$$C = e(m) = m\hat{G} + z$$

şeklinde kodlayarak göndermekten ibarettir.

3.4.1. Dekodlama nasıl çalışır?

Alıcının gönderilmiş kodu çözmesi için

$$\hat{c} = cP^{-1}$$

$$= (mSGP + z)P^{-1}$$

$$= mSG + zP^{-1}$$

işlemlerini yapıp özel anahtar olarak verilmiş kod çözme ve hata temizleme algoritmasını uygulayarak z nin $\leq d$ hata barındırabileceğinden hareketle mSG ye ulaşması gerekir. G üreteç matrisi olduğundan mSG bir kod sözcüğüdür. O halde $mS \rightarrow \hat{c}$ kodlaması yapılmıştır. S terslenebilir olduğundan $m \rightarrow \hat{c}S^{-1}$ işlemi ile de m ye ulaşılır. McEliece ilk (orijinal) makalesinde $n = 2^a$, $k = n - at$, $d \geq 2t + 1$ parametresini önermiştir **[34]**.

3.4.2. McEliece kriptosisteminin ayırt edici özellikleri

Sistemin ilk ayırt edici özelliği diğer açık anahtar sistemlerde olmayan hata vektörü ekleme işlemidir. Bu yönüyle kod sistemi halini alır. Fakat deşifreleme yaparken S ve P nin terslerinin kullanılması ise onu bir kriptosistem yapar.

Bir diğer farklılık keyfiliktir. Şöyle ki S ve P terslenebilir matrislerinin seçimi kodlayıcının tercihine bırakılmıştır. Bu keyfi seçilen S ve P matrislerinin $\hat{G}$ açık anahtarından elde edilmesi NP bir problemdir. Fakat güvenliğine olumlu etki eden bu özellik onu sınırlı bir aygıtta kullanılmamaya iter. Zira örneğin akıllı telefonlarda sınırlı bir hafıza ve işlem kapasitesi altında bu kadar büyük anahtar havuzunu saklamak ve işlemek sorundur **[35]**.

3.5. Kriptolojik bir sistemde kullanılmaya uygun olan kodların özellikleri

Bir kod şayet aşağıdaki şartları taşıyorsa kriptolojiye uygulanabilir:

- Etkili bir deşifreleme yapmaya müsaade eden etkili bir kod çözme algoritması bulunur.
- Kod, kod çözme ataklarına karşı dirençlidir.
- Kodun yapısı ve gizli anahtar algoritması maskelenmiş olmalıdır.
- Açık anahtar uzayının boyutu (genişliği) olabildiğince küçük olmalıdır.

Şimdi belli başlı kod türleri verilecektir **[36]**.

3.5.1. Halkalar üzerinde devirli kodlar

Kodlama teorisi genelde sonlu cisimler üzerinde çalışılmıştır. Halkaların daha genel bir yapı olması sebebiyle kodlama teorisinin halkalar üzerinde inşası yeni ve görece daha az çalışma barındırır. $F_q[x] \Big/ (x^n - 1)$ halkasında ideallere karşılık devirli kodların

bulunabileceği belirtildi. F_q cismi yerine bir R halkası seçilirse benzer düşüncelerle $R[x]/(x^n - 1)$ deki idealler devirli kodlar belirtecektir. Bu durumda $x^n - 1$

polinomunun R deki çarpanları önem arz etmektedir. Daha genel bir ifade ile devirli kodların üreteç matrisleri elde edilirken karşılık gelen üreteç polinom ve halka modülünü oluşturan polinomun kökleri bilinmelidir. Tek türlü çarpanın belirlenemediği, iki polinom çarpımı sonucununsa bir sabit olabileceği bazı halkalardan dolayı devirli kodları cisim yerine genel bir halkada çalışmak zor olduğu kadar ilginç sonuçlar da verecektir. Örnek olarak, sonlu cisimlere en yakın halka türleri sonlu zincir halkaları olmalarına rağmen $\mathbb{Z}_{p^e}[x]$ $(e > 1)$ sonlu zincir sonlu zincir halkalarında indirgenemezlerin çarpımı gösterimi tek türlü değildir. Gerçekten $\mathbb{Z}_4[x]$ halkasında $x^4 - 1$ polinomu

$$x^4 - 1 = (x + 1)(x - 1)(x^2 + 1)$$

$$= (x + 1)^2(x^2 + 2x - 1)$$

şeklinde iki farklı gösterime sahiptir. Bu durum ise $x^4 - 1$ polinomunun $\mathbb{Z}_4[x]$ de ürettiği devirli kodun üreteç polinomu olarak tek türlü bir seçimin olamayacağı anlamına gelir. Zira $x + 1$ ve $x - 1$ polinomları monik ve üreteç görevi görürler.

Bir başka karmaşıklık üreten konu, sonlu cisimlerde iki polinom çarpımının mutlaka çarpan polinom mertebelerinden daha büyük mertebeli olduğu kuralıdır ki bu da halka yapısı üzerinde ihlal edilir. Şöyle ki, $2x + 1 \in \mathbb{Z}_4[x]$ için $(2x + 1)^2 = 1$ olur ki hem çarpanların derecesi sonuçtan büyük kalmakta hem de sonlu cisimlerde indirgenemezlik kıstası olan birimsel elemanlarla ifade edilmeme kuralı ihlal olur. $1 \in \mathbb{Z}_4[x]$ birimsel olduğundan $(2x + 1)^2$ indirgenir anlamı çıkmalı iken halka yapısından kaynaklı $(2x + 1)(2x + 1)$ şeklinde aslında aşikar bir indirgenme mevcuttur. Tüm bu karmaşıklığın önüne geçmek adına temel indirgenemezlik kavramı verilmiştir **[37].**

Tanım 3.15 [38] R bir halka, M R nin maksimal ideali ve R/M de rezidü cismi olsun. R den R/M ye örten bir indirgeme homomorfizması bulunabilir. O halde $f(x) \in R[x]$

polinomunun $\overline{f}(x) \in R/M\,[x]$ indirgemesi indirgenemez bir polinom ise f ye temel

indirgenemez polinom denir.

Temel indirgenemezliğin gerekli olup yeterli olmadığını bir örnekle açıklayıp gerek ve yeter şartı ihsas eden teorem verilecektir. $x^2 \in \mathbb{Z}_{p^2}[x]$ için,

$$x^2 = x.x = (x - p)(x + p)$$

olur ki tek türlü parçalanamayacağı açıkça görülür.

Teorem 3.5 [38] $f(x)$, sonlu bir zincir halka üzerinde monik bir polinom olsun. Şayet $\overline{f}(x)$ rezidü cismine indirgenmiş polinom başka bir polinomun karesi değilse $f(x)$ temel indirgenemez ve ikili olarak aralarında asal polinomların çarpımı şeklinde tek türlü yazılır.

Not 3.1 NTRU halkasında $x^n - 1$ modülünde n sayısının $\mathbb{Z}_p$ cisminin karakteristiği p ile aralarında asal seçilme nedenlerinden biri de $(n, p) = 1$ iken $x^n - 1$ in kökleri katlı olmayacaktır. Keza bir başka polinomun karesi şeklinde yazılamayacaktır.

Aşağıda verilecek lemma rezidü cisminde çarpanlara ayırma yardımıyla esas halkada çarpanların bulunabilmesi bakımından önemlidir.

Lemma 3.5 (Hensel' s Lemma) [38] $f(x)$ bir R halkası üzerinde tanımlı polinom ve $g_1(x), \dots, g_t(x)$ rezidü cismi üzerinde aralarında asal polinomlar olmak üzere şayet

$$\overline{f}(x) = g_1(x)g_2(x) \dots g_t(x)$$

şeklinde yazılabiliyorsa o halde $\overline{f}_i(x) = g_i(x)$, $1 \leq i \leq t$ olacak şekilde R de $f_1(x), \dots, f_t(x)$ polinomları bulunabilir ve

$$f(x) = f_1(x) \dots f_t(x)$$

şeklinde çarpanlara ayrılabilir.

Özetle $x^n - 1$ polinomu herhangi bir R halkasında çarpanlanırken $x^n - 1$ $\overline{R}$ rezidü cisminde çarpanlarına ayırıp yukarıya Hensel Lemma ile taşıyıp (lifting) çarpanlar aranabilir.

Örnek 3.1 $x^7 - 1$ polinomu $\mathbb{Z}_2[x]$ de $(x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ şeklinde çarpanlanır.

Böylece örneğin ikinci çarpanı $x^3 + x + 1$ polinomu yukarıya taşınırken $x^3 + 3x + 3$ şekline gelebileceğinden her $k > 1$ için $\mathbb{Z}_{2^k}[x]$ de yeni çarpanlar bulunabilir. O halde $k = 2$ için $\mathbb{Z}_4[x]$ de $x^7 - 1 = (x - 1)(x^3 + 2x^2 + x + 3)(x^3 + 3x^2 + 2x + 3)$ şeklinde temel indirgenemezlerin çarpımı şeklinde yazılabilir. Şimdi $x^n - 1$ polinomuna daha yakından bakalım.

3.5.2. Birimin kökleri ve kodlama teorisindeki önemi

$x^n - 1$ polinomu, cebirsel kodlama teorisinde devirli kodlarla olan bağlantısı sebebiyle önemli bir yer tutmaktadır. Şimdi bu polinomun özelliklerini ve köklerini inceleyelim. İlkin varsayalım ki, bir F_q cismi üzerinde ele alınmış $x^n - 1$ polinomunda $(n, q) \neq 1$ olsun. $n > q$ olarak düşünülünce $n = mp^k$, $(m, q) = 1$ yazılabilir. O halde $x^n - 1 = x^{mp^k} - 1 = (x^m - 1)^{p^k}$ olur ki temelde yine $x^m - 1$, $(m, q) = 1$ şartları altında çalışılacaktır. O halde her zaman $(n, q) = 1$ seçimi yapılmalıdır.

Şimdi de $x^n - 1$ polinomunun parçalanış cismi F_{q^m} olsun. $(x^n - 1)' = nx^{n-1}$ ve $(n, q) = 1$ olduğundan $(x^n - 1, nx^{n-1}) = 1$ olur ki bu da $x^n - 1$ polinomunun katlı köklerinin olmaması anlamına gelir. $x^n - 1$ in tüm bu farklı köklerine F_q üzerinde birimin n. kökleri denir. Bu küme W_n ile gösterilsin. W_n nin çok özel bir cebirsel yapısının olduğunu aşağıdaki lemma belirtmektedir.

Lemma 3.6 [39] $(n, q) = 1$ ve uygun bir $m \in \mathbb{Z}$ seçimi altında W_n devirli bir grup oluşturur. Üstelik bu grup $F_{q^m}^*$ çarpımsal grubunun da devirli bir altgrubudur.

F_q üzerinde mertebesi n olan birimin n. kökü elemanı devirli grup W_n i üreteceğinden bu elemana birimin n. ilkel kökü denir. $w \in W_n$ böyle bir eleman olsun. m sayısının, n ve q yardımıyla bulunabileceğine dair bir lemma verilecektir. Zira w nin mertebesi n olduğundan

$$w \in \mathbb{Z}_{q^r} \Leftrightarrow w^{q^r} = w \Leftrightarrow w^{q^r - 1} = 1 \Leftrightarrow n | (q^r - 1)$$

olur ki bu r lerin en küçüğüne m denilebilir.

Lemma 3.7 [39] $x^n - 1$ polinomunun F_q üzerinde parçalanış cismi F_{q^m} ise o halde $n | (q^m - 1)$ olacak şekildeki sayıların en küçüğü m dir. Bir diğer ifade ile $q^m \equiv 1 \ (mod\ n)$ olacak şekildeki en küçük m için F_{q^m} parçalanış cismidir.

4. LATİSLER ÜZERİNDE KRİPTOLOJİ VE NTRU KRİPTOSİSTEMİ

Latisler hem kriptanalizde hem de kriptografide geniş uygulama alanları bulmuşlardır. Zor bir latis problemi yeni bir kriptolojik şifrelemeye imkân verebilir. Fakat daha genel kullanım alanı indirgeme, ortogonalleştirme ve belirli bir noktaya yaklaşma şeklinde genellenebilecek algoritmalarla atak düzenleme, şifre kırma ve kriptanaliz sahasıdır.

4.1. Latislere Giriş

Tanım 4.1 [40] $A = \{a_1, a_2, \dots, a_m\}$ kümesi $\mathbb{R}^n$ de lineer bağımsız bir vektörler kümesi olsun ($m \leq n$ olmak zorunda). A kümesinin tüm tam sayı lineer kombinasyonları kümesine L latisi denir. Yani

$$L = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots + \mathbb{Z}a_m$$

dir ve L latisi m boyutludur denir. A kümesine de L latisinin bir bazıdır denir.

Teorem 4.1 [40] $\mathbb{R}^n$ deki bir toplamsal altgrubun latis olması için gerek ve yeter şart ayrık (discrete) olmasıdır.

Latisler n boyutlu bir uzayda noktalarının düzenli dizilimleri sebebiyle ayrık kümelerdir. $m \geq 2$ olduğunda bir latisin sonsuz sayıda bazı bulunabilir. Baz vektörleri göreceli olarak kısa vektörlerden oluşuyor ise indirgenmiş baz denir. Bir latis ayrık olduğundan 0 olmayan vektörlerinin en kısası mevcuttur. Latis indirgeme algoritmalarının temel amacı kısa, ortogonal veya ilginç bazlar kümesi bulmaktır. Latis indirgeme teknikleri kriptanalizde etkin olarak kullanılmaktadır.

4.2. Latis Problemleri

Şimdi en çok bilinen bazı latis problemleri tanıtılacaktır.

Tanım 4.2 [40] En kısa vektör problemi (SVP), verilen bir latis baz kümesinden hareketle latisin en kısa vektörünü bulmaktır.

Tanım 4.3 [40] En yakın vektör problemi (CVP), verilen bir latis bazı yardımıyla herhangi bir $a \in \mathbb{R}^n$ vektörü seçildiğinde bu a vektörüne en yakın latis vektörünü bulmaktır.

Tanım 4.4 [40] En küçük baz problemi (SBP), bir latis bazı verildiğinde bu vektörlerin boyunu minimize etme problemidir.

Tüm bu problemlerin polinom-zamanlı algoritmalarla çözülemeyeceği bir çok çalışma ile ortaya konmuştur.

4.3. Latis Tabanlı Sistemler

Temelini, Ajtai-Dwork ve Goldwasser-Goldreich-Halevi kriptosistemlerinin oluşturduğu bu yeni model kriptosistemler bir çok latis bazlı sistemin türemesine ilham kaynağı olmuştur.

4.3.1. Ajtai-Dwork kriptosistemi

Bu sistem $\mathbb{R}^n$ de çalışır. Sistemin güvenliği SVP problemlerinin çeşitlendirilmesine dayanır. Geniş açık anahtar kümesi ve geniş seçilebilir mesaj kümesi sistemin artılarıdır. Fakat ilerleyen zamanlarda Nguyen ve Stern sistemin güvenlik açıklarını buldular. Buradan hareketle şayet sistemin geniş çaplı bir bakım ve altyapısını cebirsel veya algoritmik olarak güncelleme çalışması yapılmazsa sadece bir teorik öneri olarak kalacaktır denebilir.

4.3.2. Goldwasser-Goldreich-Halevi kriptosistemi

Bu sistem ise CVP probleminin güçlükleri üzerine kuruludur. McEliece sisteminin latis varyasyonu olduğu söylenir. Bu yöntemde şifreli metne ilave olarak bir gürültü vektörü eklenir. Buna bağlı olarak önerilen gizli anahtar özel sınırlar altında deşifreleme yaparken bu hata vektörünü kaldırmalıdır.

GGH kriptosistemi AD sistemine nazaran daha güçlü ve etkilidir. Bazı ataklar sonucu bu sistemin CVP problemlerine katkı sağladığı görülmüştür.

CVP veya diğer latis problemlerinin klasik veya kuantum bilgisayarlara karşı oldukça dirençli olduğuna inanılmakla birlikte bu direkt olarak bir kriptosisteme transfer edileceği anlamına gelmez. Çünkü bazı durumlarda kriptoloji pratikliği ve hızı esas alır (average case). Bazı durumlarda ise şifrenin en zor koşullarda dahi zor kırılması hedeflenir (worst case). Dahası bir CVP probleminde kesin sonucu bulmak oldukça zor iken yaklaşık sonuçlar bulmak mümkündür **[41].**

Buradan hareketle latis tabanlı kriptolojide her türlü amaç için özel koşullu kriptolojik sistemler önermek mümkündür denebilir. Zor olmak ve zor tahmin edilmek veya zor çözülmek daha çekici ve ilginç geldiğinden olmalı ki güçlü sistem önerileri genellikle bu yapılar üzerinde önerilir.

4.4. İlk Önerilen Latis Tabanlı Kriptosistem: GGH Kriptosistemi

GGH kriptosistemi, latisleri baz alarak kurulduğundan sistem bu alanda bir ilk olarak kabul edilir. Sistemin işleyişi genel hatlarıyla şu şekildedir **[42].**

4.4.1. Anahtar üretimi

1) İyi bir baz kümesi (genellikle ortonormal seçilir) belirle. Bu kümeye R diyelim.
2) Bu iyi R bazını daha kötü seçilen (genelde ortogonal olmayan ve uzun vektörler) bir Q bazına dönüştür. Bu dönüşümü sağlayan işlemi gizli tut.
3) Kötü Q bazını açık anahtar olarak yayınla.R yi gizli anahtar olarak saklı tut.

4.4.2. Şifreleme

1) Kötü Q bazı esas alınarak belirlenmiş bir keyfi w latis noktasını seçip düz metin olarak göndermek istenilen mesaj vektörü p ile topla.
2) $c = w + p$ vektörünü şifreli metin olarak gönder.

4.4.3. Deşifreleme

1) Gizli anahtar olarak verilen iyi baz R yi kullanarak latis içerisindeki c noktasına en yakın w noktasını bul.
2) Bulunan bu w noktasını c den çıkararak $c - w = p$ metnine ulaş.

Elbette latis tabanlı kriptolojik sistemler bu ilk halinden çok daha gelişip kompleks ve quantum kriptolojik yapılara kadar evrilmiştir. Bu evrilmede Gram-Schmidt ortogonalleştirme algoritmaları ile kötü bazdan iyi baza, Hermite normal form dönüşümüyle baz dönüşümleri yaparak latis noktalarının farklı gösterimleri ile farklı şifrelemelere imkan bulmak yepyeni, komplike ve daha güçlü sistemler önerilmesiyle devam edecektir. Fakat bu çeşitlilik ve zengin varyasyonlara imkan tanıması, onu zaman ve işlevsellik noktasında ağır, maliyet ve bellek kullanımı noktasında ise pahalı yapar. Bu sebeple her defasında yeni bir model önerilmektedir.

4.5. İdeal Latisler

İdeal latisler döngüsel latislerin genel halidir. Yani aslında aynı amaca hizmet ederler. Şöyle ki döngüsel latisleri bir L latisinde tanımlarken çok yalın bir kural belirlenir. Bu L latisindeki bir vektörü seç diğerlerinin yerine bu seçilen vektörün rotasyonlarını ekle (cyclic shift). Oysa bu seçim ve kuralın daha komplike bir yapı üzerinde ve daha güç tahmin edilebilecek bir formasyona sokulması sistemin lehinedir. Z^n den bir R halkasına transforme edilen bir döngüsel latis bu R halkasında neye tekabül etmektedir. İşte bu mantık üzerine kurulu düşünceye atfen döngüsel bir latisin daha genel hali olan ideal latislerin bir R halkasında da ideale dönüşeceğinden hareketle ideal latisler denmiştir. Şimdi matematiksel ifadelerle bu ilişki açıklanacaktır.

Tanım 4.5 (İdeal latis) [42] L, Z^n de bir latis olsun. Şayet $\phi_q(L)$, R_q halkasında ideal olacak şekilde bir q monik polinomu bulunabiliyorsa o halde L ye bir ideal latis denir. Aksine şayet I, R_q da bir ideal ise o halde ${\phi_q}^{-1}(I)$ her zaman Z^n de bir latistir.

4.5.1. İdeal latislerin inşaası

$q(x) \in Z[x]$ monik ve n. dereceden

$$q(x) = q_0 + q_1 + \cdots + q_{n-1}x^{n-1} + x^n$$

şeklinde bir polinom olsun. Bu q polinomuna göre tüm tam katsayılı polinomlar halkası ise

$$R_q = Z[x]/(q(x))$$

şeklinde tanımlansın. Z modül oluşunun yanı sıra R_q, Z^n ile q nun seçiminden bağımsız olarak izomorfiktir. Bu izomorfizm,

$$\phi_q : Z^n \to R_q$$

$$(v_0, \ldots, v_{n-1}) \mapsto v_0 + v_1 x + v_{n-1}x^{n-1} + (q(x))$$

şeklinde tanımlanır.

Bu ϕ izomorfizmi sebebiyle Z^n de birbirinden farklı çarpımlar tanımlanabilir. Zira farklı q modül polinomlarına karşılık Z^n de iki vektörün çarpımı farklı sonuçlar üretecektir.

4.6. Döngüsel Latisler

Genel latislerin bir altkümesi olan döngüsel (cyclic) latisler temel olarak bir baz vektörü ve bunun tüm uygun sağa doğru ötelenmiş (shifting) vektörlerinin kümesini baz kabul eden latislerdir. Bu şekilde seçilmiş latislere geçişin iki temel sebebi vardır. Birincisi, bilgisayar belleğine sadece bir vektörü saklamamız yeterli olacaktır. Oysa genel bir latiste seçilen baz vektörleri keyfi olduğundan bu latisler bellek ve ram kullanımını artırır. İkincisi ise, bir kurala göre düzenlenmiş bu yeni baz vektör kümesi matris çarpımı, vektörel norm gibi işlemlerde hız ve işlem kolaylığı sağlamaktadır. Tüm bunlara rağmen döngüsel latislerin daha zayıf olduğuna dair bir bulguya henüz rastlanmamıştır.

Tanım 4.6 (Döngüsel latis) [42] Seçilen q rotasyon polinomu şayet $x^n - 1$ olursa R_q daki ideallere karşılık gelen Z^n nin latislerine döngüsel (cyclic) latis denir. Burada hemen belirtelim ki $x^n - 1$ polinomu yardımıyla oluşan latislere NTRU latisleri de denmektedir.

$R_q = Z[x]/(q(x))$ halkasındaki ideallerin ideal latisler üreteceğini belirtmiştik. Bu halka üzerinde karakteristiği p asalı yapmak suretiyle bir $R_{q,p} = Z_p[x]/q(x)$ halkasına geçerek daha küçük bir halka üzerinde çalışmak amaçlanmıştır. Yine $q(x)$ modülünün indirgenebilir olup olmayışı gibi farklı durumlarda incelenmiştir. Çünkü $q(x) = q_1(x).q_2(x)$ şeklinde aşikar olmayan bir çarpan bulunabilirse o halde halkada sıfır bölenler olacaktır. Özellikle $Z[x]/(x^n + 1)$ halkasının yapısı çok ilginçtir. Bu halkanın ideallerine karşılık gelen latislere negatif döngüsel (negcyclic) latis denmektedir. Bu latislerde bir v vektörünün $n.$ rotasyonu sonucu $-v$ vektörü bulunur. Yani bir vektörün kendisini $2n$ rotasyonu sonucu tekrar bulabiliriz. Ayrıca bu halkalardan tanımlı izomorfizm dönüşümleri uzaklığı da koruduğundan izometrik dönüşümler olurlar.

4.7. Latis Tabanlı Sistemden NTRU' ya Geçiş

$A \in Z_p^{n \times m}$ matrisi keyfi seçilsin. Bir f_A fonksiyonu, $f_A: Z_p^m \to Z_p^n$

$$f_A(x) = Ax \bmod p \qquad (6)$$

şeklinde tanımlansın. Burada x vektörleri şayet $\{0,1\}^m$ kümesinden seçilirse knapsack sistemine dönülür. Görüldüğü üzere latis tabanlı kriptolojik sistemler knapsack sisteminin daha genel halidir. Tekrar (6) denklemine dönülürse şayet A bir L latisinin baz vektörlerinin matrisi ise yani aslında L latisini oluşturan ve belirleyen matris ise A

matrisine L latisi yerine kullanılan lineer dönüşüm olarak bakılabilir. O halde bir $t \in L$ için x_0 bulmak oldukça kolay olacaktır.

$$t = Ax_0 \Rightarrow A^{-1}t = x_0 \; mod \; p$$

denklemi çözülürse $x_0 \in Z_p^m$ karşılık gelen vektörü belirlenir. Yine bir $x_1 \in Z_p^m$ vektörüne mesaj vektörü olarak bakılırsa

$$f_A(x_1) = Ax_1 \; mod \; p = t_1 \tag{7}$$

olduğunu varsayalım. Bir $r \in Z_p^m$ hata (noisy) polinomu için

$$f_A(x_1 + r) = A(x_1 + r) mod \; p = [Ax_1 + Ar] mod \; p \tag{8}$$

$$= Ax_1 \; mod \; p + \underbrace{Ar \; mod \; p}_{t_2 \in L} = t_1 + t_2 \in L$$

denilirse $\|.\|$, latis üzerinde tanımlı bir norm fonksiyonu olmak üzere $\|f_A(x_1 + r) - f_A(x)\| = \|t_2\|$ olur ki seçilen r hata polinomu $\|t_2\|$ değerini minimum seviyede tutmak şeklinde seçilebilir. Örneğin, t_2 latisin en küçük (SVP) vektörü ise t_1 asıl bulunması gereken noktaya oldukça yaklaşılır.

A matrisi keyfi seçildiğinde kriptanalizin oldukça zor olduğu kabul edilip yeni çalışmalarda bir $(a_1, a_2, \dots, a_n) \in Z_p^n$ vektörü seçip bu ve bu vektörün rotasyonlarıyla üretilen

$$Rot(a) = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix}$$

matrisi A yerine kullanıldığında hesaplamaların daha kolay olduğu görüldü. A matrisinin sütunları $Z_q[\alpha]/(\alpha^n - 1)$ halkasının elemanları olarak ele alındı. Bazı çalışmalarda ise bu halkanın $Z_q[\alpha]/(P(\alpha))$ şeklinde genel bir hali önerildi **[42].** Hemen belirtelim ki $P(\alpha)$ indirgenemez olduğunda ve q asal bir modül olarak seçildiğinde $Z_q[\alpha]/P(\alpha)$ bir cisim olacaktır. Cisimde 0 ve F cismin kendisi dışında ideal olamayacağından kod üretilemeyecektir. Çünkü her bir kod evveliyatında bir idealdir. Bu sebeple, $P(\alpha)$ nın en az bir kökü içerde olacak şekilde seçilir ki bu kriptolojik sistem aynı zamanda kod üretebilsin. Bunu sağlamanın en basit yolu birimli bir halkada $\alpha^n - 1$ seçimidir. Cebirsel kodlama ve kriptolojide çok özel bir yeri olan devirli (cyclotomic) polinoma bu bölümde de kısaca değinilecektir.

4.8. $x^n - 1$ polinom parçalanışı ve NTRU sistemine etkisi

$x^n - 1$ polinomunun çarpanları devirli kodlar teorisinde olduğu gibi kriptolojide ve bilhassa latis tabanlı bir sistemde de önem arz etmektedirler. Bir F_q cismi üzerinde $(n, q) = 1$ şartları altında $x^n - 1$ in tekrarlı kökünün bulunmadığını dolayısıyla farklı minimal polinomların çarpımı şeklinde yazılabileceği verilmişti. Şimdi $a \in F_{q^m}$ bir üreteç eleman olsun yani $a^{q^m-1} = 1$ olsun. Ayrıca $w \in F_{q^m}$ de birimin n. ilkel kökü olsun. $w^n = 1$ olacağından,

$$w^n = a^{q^m-1} = 1 \Leftrightarrow w = a^{(q^m-1)/n}$$

olur ki a üreteç olduğundan her kuvveti farklıdır. Yani w bir ilkel kök ise eğer,

$$\{w, w^2, \dots, w^{n-1}, w^n = 1\}$$

kümesi $x^n - 1$ in tüm kökleridir. Ayrıca bir w^i elemanı devirsel koset sınıfı,

$$w^{iq^d} = w^i \Leftrightarrow w^{iq^d-i} = 1 \Leftrightarrow n|(iq^d - i) \Leftrightarrow iq^d \equiv i \ (mod\ n)$$

olacak şekildeki en küçük $d \in \mathbb{Z}^+$ için,

$$\{w^i, w^{iq}, \dots, w^{iq^{d-1}}\}$$

sınıfıdır. O halde w^i elemanının minimal polinomu,

$$m_i(x) = \left(x - w^i\right)\left(x - w^{iq}\right) \dots (x - w^{iq^{d-1}})$$

olur. Bu minimal polinom ve herhangi bir böleni tersinir olamayacağından özel anahtar işlevi de göremeyecektir. Bu noktadan hareketle birimin köklerini kök kabul eden polinomların ideallerinde de özel anahtar arama işlemi yapılmayacaktır.

Kompleks ve zor problemler üzerine kurulu bazı latis ve kod problemleri nasıl çözülebilirdi? Bu sorunun cevabı evvela döngüsel latisleri, sonrasında da NTRU kriptosistemini doğurmuştur.

4.9. NTRU Kriptosistemi

NTRU kriptosistemi ilk defa CRYPTO'96 kongresinde Hoffstein, Pipher ve Silverman tarafından 1996 yılında tanıtılmıştır **[45]**. Daha sonra 1998 de yazılı olarak yayınlanmıştır **[46]**. 1998 den itibaren kriptosistemin detaylı tanıtımı, analizi ve parametre seçimleri gibi

birçok konuda kurucu ekip www.ntru.com internet adresinden onlarca makale ve rapor yayınlamıştır **[47]**. NTRU bazı özel yapıdaki polinom halkaları üzerinde kurulmuştur. NTRU sistemindeki "zor problem (hard problem)" kısa vektör problemidir (SVP). NTRU sistemi kendisinden önce var olan tüm açık anahtar kriptoloji sistemlerinin tamamından daha hızlı ve daha efektiftir **[48].** NTRU kriptosisteminde sadece polinom toplamı ve öteleme (shifting) işlemleri yapıldığından sistemin karmaşıklık düzeyi kuadratik seviye olan $O(N^2)$ dir. Oysa bilindik bazı kriptosistemlerde (örneğin, RSA ve ECC) karmaşıklık düzeyi kübiktir ($O(N^3)$). Bu sebeple, NTRU, ECC sisteminden 1.5 kat daha hızlıdır **[49].** NTRU ayrıca anahtar üretim hızı bakımından 200 kat, şifreleme hızı bakımından 3 kat ve deşifreleme hızı olarak da 30 kat RSA dan daha hızlıdır **[50]**. Tüm bu etkinlik ve hızlı oluşu, sistemin mobil telefonlarda, veri sıkıştırma cihazlarında ve akıllı kartlarda kullanılması gerektiğini ortaya çıkarmıştır **[51]**. Bu hız avantajının yanı sıra şayet önerilen parametreler kullanılırsa sistem ayrıca yeterli güvenlik düzeyinde olacaktır **[52].** NTRU sadece hızlı bir açık anahtar şifreleme sistemi olmayıp ayrıca kuantum saldırılara karşı da oldukça dirençlidir. Bu direnci, sistemin, sadece latis tabanlı kriptosistemlere verilen IEEE P1363 standardına ulaşmasına imkan tanımıştır **[53]**. NTRU ayrıca bir latisin içerisindeki en küçük vektörü bulma problemine dayandığından latis tabanlı sistemler arasındadır. Sistem sadece açık anahtar kriptosistemlerinden değil ayrıca latis tabanlı kriptosistemlerden dahi hız, etkinlik ve anahtar kümesi kompaktlığı gibi birçok konuda pozitif ayrışır. Örnek verilecek olursa Ajtai-Dwork, GGH kriptosistemi gibi latis tabanlı kriptolojik sistemlere nazaran NTRU oldukça ilgi çekmektedir [10].

NTRU kriptosisteminin diğer açık anahtar sistemlerden hız, etkinlik ve konulardaki üstünlüğüne değinildi. NTRU sadece bu özelliklerde değil, güvenlik ve ataklara direnç gösterme konusunda da, RSA (Rivest ve diğeri, 1978), ECC (Koeblitz, 1985), El Gamal (El Gamal, 1989) kriptosistemlerinden daha güçlüdür. Tüm bu NTRU dışındaki açık anahtar sistemlerin zorluk problemi büyük asalları çarpanlarına ayırmak ve ayrık logaritma problemine dayanır. Oysa 1997 de Shor algoritması ile gelecekte kuantum bilgisayarların bu problemleri polinom zamanda çözebileceği gösterilmiştir. Bu aşamadan sonra kuantum sonrasına hazırlık bakımından yeni sistemlere duyulan ihtiyaç artmıştır **[54].** Tam da o günlerde NTRU sistemi tanıtılmıştır. NTRU nun kuantum saldırılara gösterdiği direnç onu günden güne ilginç ve trend bir konuma getirmiştir. Bu trend içerisinde NTRU sisteminde bazı saldırılar düzenlemiştir. Bu saldırı türlerinden bazıları, NTRU sisteminin kurucu ekibinin önerdiği **[55]** deki çalışmaya yapılan latis indirgeme algoritmaları saldırısıdır. **[56]** de yapılan çalışmada latis indirgeme algoritmaları yardımıyla NTRU kriptosisteminin en

kısa vektörünü bulmaya çalışılmıştır. Ayrıca **[57]** de farklı türden bir hibrit atak düzenlenmiştir. **[58]** deki çalışma ise birçok açık anahtar sistemine toplu düzenlenen bir saldırı idi. Tüm bu ataklara karşılık kurucu ekip www.ntru.com adresinden 15 nolu raporu yayınlayarak sistemi daha korunaklı hale getirmişlerdir **[59]**. Aynı tarihlerde düzenlenen açık metin saldırısı **[60]**, seçilmiş şifreli metin saldırısı **[61]** ve diğer bazı **[62, 63, 64]** saldırıları için 12 **[65]** ve 16 **[66]** nolu raporlar aynı web adresine konulmuştur. NTRU sistemine ilk defa yapılan **[62]** daki vb diğer saldırıların özeti için **[67]** deki çalışmaya bakmak yaralı olacaktır.

Çok daha fazla atak çalışmaları olup burada en önemli ve belli başlı olanlarına değinilmiştir. Tüm bu atak ve karşı atak çalışmaları NTRU sistemini düzlemine oturtmuştur. Buradan yola çıkarak NTRU kriptosistemini NTRU-1998 **[46]**, NTRU-2000 **[68]**, NTRU-2005 **[52]**, NTRU-2007 **[69]** ve NTRU-2008 **[70, 53]** diye ayırmak koşulu ile beş evrede inceleyebiliriz. Daha sonraki bölümde detaylarıyla açıklanacak bu evreler NTRU kriptosisteminin omurgasını oluşturup birçok akademik çalışmaya esin kaynağı olmuştur. Her defasında farklı parametre ve matematiksel altyapı zenginleştirmesi ile NTRU kriptosisteminin bir çok türevi de üretilmiştir. Bunlardan bazılarına değinmek gerekirse, 2002 yılında yapılan CTRU **[71]** çalışması ki, tam sayı halkası yerine polinom halkası üzerinde NTRU incelemesi yapar, 2005 yılında yapılan bir çalışmada **[72]** ise matris halkaları üzerinde NTRU inşa edilmiştir. 2006 yılında Gaussyen tam sayılar kullanılmıştır **[73].** 2009 yılında yapılan bir çalışmada **[74]** ise Dedekind bölgeleri üzerinde NTRU incelenmiştir. Daha kapsamlı okumalar adına **[75, 76, 77]** e bakılabilir.

4.10. NTRU' nun Cebirsel Altyapısı

4.10.1. Tanımlar ve notasyon

NTRU şifreleme operasyonları, $R = Z[x]/(x^N - 1)$ bölüm halkasında yapılır. Bu halkaya polinomların konvolüsyon halkası da denmektedir. R halkasındaki bir polinom tam sayı katsayılıdır ve en fazla $N - 1$ mertebelidir. N pozitif bir tamsayıdır ve genellikle asal seçilir. Şayet $f(x)$, R de bir polinom ise her $k \in [0, N-1]$ için f_k, x^k nın katsayısını ve $x \in \mathbb{C}$ için de $f(x)$, f nin x deki değerini gösterir olsun. f ve g, R de iki polinom olmak üzere $h = f \star g$ konvolüsyon çarpımı aşağıdaki kurala göre yapılır:

$$f = \sum_{i=0}^{N-1} f_i x^i = (f_0, f_1, \dots, f_{N-1})$$

$$g = \sum_{j=0}^{N-1} g_j x^j = (g_0, g_1, \dots, g_{N-1})$$

$$f \star g = h \text{ ise } h_k = \sum_{i+j \equiv k \,(mod\ N)} f_i g_j$$

NTRU kriptosistemini kurmak için en evvel (N, p, q) gibi üç tane pozitif tam sayı şu şekilde belirlenir:

- N asaldır,
- p ve q aralarında asaldır, yani $(p, q) = 1$ dir,
- q, p den çok daha büyük seçilir.

NTRU, $R = Z[x]/(x^N - 1)$ halkasında polinom toplamı ve polinomların "yıldız" (konvolüsyon) çarpımı işlemlerinin üzerinde inşa edilmiştir.

$\star$ işlemi, iki polinomun devirsel konvolüsyonudur. $\star$ işlemi sonunda iki polinomun devirsel konvolüsyonu hesap edilirken p ve q modüllerine göre indirgeme işlemleri de yapılmalıdır. R halkasındaki bu $\star$ işlemi birleşmeli ve değişmelidir fakat her elemanın bu işleme göre R de tersi mevcut değildir. R nin çarpımsal tersleri mevcut elemanlarının kümesini $R^\star$ ile gösterirsek bir $f \in R^\star$ elemanının tersi f_q^{-1} ile gösterilir. Hemen belirtelim ki $\star$ ve polinom toplamı olan $+$ işlemleri birbirleri üzerine dağılmalıdır.

Bir diğer gereksinim ise, özel anahtar belirlenirken yapılacak iki adet polinom tersi bulma işlemidir. Bu işlemler Genelleştirilmiş Öklid Algoritması yardımıyla hesaplanır.

NTRU kriptosistemi her ne kadar R halkası üzerinde tanımlanmış olsa bile, bazı parametre seçimleri dışındaki diğer tüm işlemler $R_p = Z_p[x]/(x^N - 1)$ ve $R_q = Z_q[x]/(x^N - 1)$ gibi iki alt halkada yapılır. Uygun parametreler seçimi ve işlem yoğunluğunun bu alt halkalara taşınmasının en büyük sebebi, kriptolojik sistemin hızının ve etkinliğinin artırılmasıdır **[43].**

NTRU yu diğer açık anahtar kriptosistemlerden ayıran temel özelliklerden birisi bu halka yapısı üzerine kuruluşudur. Ayrık logaritmayı grup yapıları üzerinde çözmeye dayalı birçok (RSA, El Gamal, vb.) açık anahtar sistemin aksine, NTRU daha geniş bir yapı olan halkalarda çalışmaktadır. Bu zengin cebirsel altyapısı, NTRU kriptosisteminin birçok

varyasyonlarının çalışılmasına ve teorik olarak yapılan her çalışmanın da kriptanaliz ve saldırı örneklerinin uygulanmasına olanak tanımaktadır.

4.10.2. NTRU kriptosisteminin parametreleri ve kullanılacak notasyonlar

NTRU şifreleme ve deşifreleme işlemlerinde ve ayrıca anahtar üretim süreçlerinde kullanılan parametreler şunlardır:

1. N: Kullanılacak polinomların maksimum derecesini belirler. N parametresi ayrıca latisin boyutunu belirtir. Bu sebeple N asal olarak seçilir ki süreç, ataklara karşı korunabilsin ve yeteri kadar büyük seçilir ki latis ataklarından korunabilsin.
2. Büyük modül q, $Z[x]/(q, x^N - 1)$ halkasını oluşturur. Büyük modüldür ve pozitif tam sayı olarak seçilir. Süreç içerisinde neyi amaçladığımızla bağlantılı olarak değerleri farklılık gösterir.
3. Küçük modül p , $Z[x]/(p, x^N - 1)$ halkasını oluşturur. Küçük modüldür ve genellikle pozitif tam sayıdır. Nadiren küçük katsayılı polinom olarak seçilmiştir.
4. f polinomu ki, $Z[x]/(x^N - 1)$ de bir polinom ve $(mod\ p)$ ve $(mod\ q)$ tersleri mevcut olmalıdır.
5. g polinomu ki terslenebilir olması gerekmez.
6. Hata polinomu r, hata polinomları kümesi L_r den şifreleme sürecinde keyfi olarak seçilen küçük katsayılı bir polinomu belirtir.
7. m mesaj polinomu, henüz şifrelenmemiş ve kodlanabilir bir polinomu belirtir.
8. df; f polinomunun katsayılarınındaki 1 lerin sayısını belirtir.
9. dg; g polinomunun katsayılarındaki 1 lerin sayısıdır.
10. dr; belirlenmiş r polinomunun katsayılarınındaki 1 lerin sayısıdır.
11. L_f, katsayıları df i sağlayan $Z[x]/(x^N - 1)$ deki polinomlardır. Yani, şifreleme için seçilen ve gizli olarak tutulacak özel anahtar polinomlarının seçildiği kümelerdir.
12. L_g, katsayıları dg yi sağlayan $Z[x]/(x^N - 1)$ deki polinomlardır.
13. L_r, katsayıları dr yi sağlayan $Z[x]/(x^N - 1)$ deki polinomlardır.
14. L_m : Düz metin kümesidir. Henüz şifrelenmemiş ve kodlanabilir polinomlar kümesini belirtir.
15. f_p, $Z[x]/(p, x^N - 1)$ de f nin $(mod\ p)$ ye göre indirgenmiş halidir (gizli anahtar).
16. f_q, $Z[x]/(q, x^N - 1)$ de katsayıları $(mod\ q)$ ya göre indirgenmiş polinomdur.
17. g, $Z[x]/(q, x^N - 1)$ de bir polinomdur (f_q ile birlikte açık anahtarı oluşturacak).
18. f_p^{-1}, f_p nin $Z[x]/(p, x^N - 1)$ halkasındaki konvolüsyon çarpımına göre tersidir.

19. f_q^{-1}, f_q nin $Z[x]/(q, x^N - 1)$ halkasındaki tersidir.

20. e şifrelenmiş mesaj , $Z[x]/(q, x^N - 1)$ de bir polinomdur.

21. $center$: Merkezileştirme metodudur. Deşifreleme safhasında $(mod\ q)$ indirgemelerinin mükemmel doğrulukta çalışacağını garanti eden algoritmadır.

NTRU ilk tanıtıldığından bu yana , $p = 3$ ve q ise 2 nin bir kuvveti olarak seçilmektedir. Hemen belirtilsin ki, q asal olmak zorunda değildir. Yani R_q genelde bir cisim yapısı oluşturmaz. L_m altkümesi de, ternary polynomials denilen ve katsayıları $\{-1,0,1\}$ kümesinden seçilen polinomlardan oluşmaktadır. $f \in L_f$ olan özel anahtarlar ise genellikle $1 + p.F$ şeklinde seçilmektedir. Bu seçim kıstasları işlem hızı ve kolaylığı amacıyla önerilmektedir. p nin polinom olarak seçilebileceğini ve parametrelerin değişkenlik gösterebileceğini zaman içinde yapılan çalışmalar göstermektedir. N, q ve p parametreleri, tercih edilen güvenlik düzeylerine göre farklı şekillerde seçilebilir. $(p, q) = 1$ durumu her zaman korunmalıdır ki (p, q) ideali tüm halkayı vermelidir **[43].**

4.11. Anahtar Üretimi

Bir NTRU kriptosisteminin özel anahtarlarını üretmek için $f \in L_f$ ve $g \in L_g$ rastgele seçilir. Bu seçimler altında f polinomu ilave olarak bir şart konmaksızın $mod\ p$ ve $mod\ q$ ya göre tersinirdir. NTRU kriptosistemi olasılıklı bir kriptoloji sistem olduğundan çok uygun parametreler seçilmesi durumunda sistem yüksek olasılıkla doğru çalışacaktır **[43].**

Yani

$$f_q^{-1} \star f \equiv 1\ (mod\ q)\ ve\ f_p^{-1} \star f \equiv 1\ (mod\ p) \tag{9}$$

olacaktır.

4.11.1. Şifreleme

$$h \equiv p f_q^{-1} \star g (mod\ q) \tag{10}$$

açık anahtar olacaktır. Sistemin bir kullanıcısı kendi açık anahtarını istediği şekilde değiştirebilmektedir.

m mesajı ise f ve f_p^{-1} gizli anahtarları ve h açık anahtarı ile

$$e \equiv r \star h + m (mod\ q) \tag{11}$$

şeklinde hesaplanarak şifrelenir.

4.11.2. Deşifreleme

Şifreli mesaj, gizli anahtarı kullanarak

$$a \equiv f \star e(mod\ q) \tag{12}$$

şeklinde deşifre edilir. Bu aşamada a nın katsayılarının $(-q/2, q/2]$ aralığında olup olmadığı kontrol edilir.

$$c \equiv\ f_p^{-1} \star a(mod\ p) \tag{13}$$

hesaplanarak işlem bitirilir. Deşifrelemenin doğru çalışması için $prg + fm$ polinomunun katsayılarının mutlak değerleri $q/2$ yi geçmemelidir. Yani büyük katsayıların seçilmiş olması sebebiyle ayrıca $mod\ q$ ya göre indirgeme yapılmayacağı varsayılabilir **[43]**.

4.11.3. Deşifreleme neden doğru çalışır?

Matematiksel olarak,

$$a \equiv f \star e(mod\ q) \equiv f \star (r \star h + m)(mod\ q)$$

$$\equiv f \star r \star h + f \star m(mod\ q) \tag{14}$$

olup, $h \equiv pf_q^{-1} \star$

g (15)

olduğundan,

$$a \equiv \left[\left(f \star r \star \left(pf_q^{-1} \star g\right)\right) + (f \star m)\right] mod\ q \tag{16}$$

olur ve $f_q^{-1} \star f \equiv 1\ (mod\ q)$ olduğundan,

$$a \equiv [(pr \star g) + (f \star m)]\ mod\ q \tag{17}$$

olur. $c \equiv f_p^{-1} \star a(mod\ p) \equiv p\left(f_q^{-1} \star r \star g\right) + \left(f_p^{-1} \star f \star m\right)(mod\ p)$
$= 0 + (1 \star m) = m(mod\ p)$ olur ki m mesajı doğru bir şekilde bulunur.

Kriptolojik süreç şayet bir de algoritma dili ile anlatılacak olursa;

Anahtar üretimi

1. $f \in L_f$ ve $g \in L_g$ yi, $f\ (mod\ p)$ ve $(mod\ q)$ da terslenebilir olmak kaydıyla keyfi olarak seç.
2. $F_q \equiv f^{-1}\ mod\ q$ ve $F_p \equiv f^{-1}\ (mod\ p)$ yaz.
3. Özel anahtar (f, F_p) dir.
4. Açık anahtar ise $H \equiv p.g \star F_q\ (mod\ q)$ dur.

Not edelim ki, g deşifreleme safhasında kullanılmaz. Bu sebepten ötürü özel anahtar olarak gönderilmez. Yani, $H \star f \equiv p.g\ (mod\ q)$ olacağından, $mod\ p$ ikamesi yapıldığında $H \star f \equiv 0\ (mod\ p)$ olur ki kullanılmayacağı anlaşılır.

Şifreleme

Şifreleme algoritmik bir dilde anlatılacak olursa;

Input: $m \in L_m$ olan bir mesaj ve açık anahtar H.

Output: bir şifreli mesaj $e \in \Upsilon(m)$

1. $r \in L_r$ yi keyfi seç
2. $e \equiv r \star H + m\ (mod\ q)$ ya dön.

$\Upsilon(m)$ kümesi ile düz metin olan m lerin şifrelenebilir olanları belirtilmektedir.

Deşifreleme

Deşifreleme safhası da algoritmik anlatılırsa, bir D algoritması e ye şöyle etki eder.

Input: bir şifreli mesaj $e \in \Upsilon(L_m)$ ve özel bir anahtar olan (f, F_p).

Output: Düz bir metin olan $D(e) = m \in L_m$.

1. $a\ (mod\ q) \equiv e \star f(\ mod\ q)$ yu hesapla.
2. Merkezileştirme işlemi yaparak $a = p.r \star g + f \star m \in R$ den bir tam katsayılı $a\ mod\ q$ polinomu elde et.
3. $m\ mod\ p \equiv a \star F_p\ (mod\ p)$
4. Düz mesaj $m \equiv \Psi m\ (mod\ p)$.

Not edilsin ki $\Psi: m \mapsto mmodp$ dönüşümüdür. Yani $\Psi: L_m \mapsto L_m\ (modp)$ işlemini yapar.

Deşifreleme işleminin hatasız çalışabilmesi yani $D(e) = m$ olabilmesi için uygun parametre seçimi önemlidir. Artık sistemin işleyişi okuyucuya aşina kılındığı için, uygun parametrelerden ne kastedildiği aşağıda biraz daha detaylandırılarak anlatılmıştır.

4.12. Hata Polinomu r nin Seçimleri

r hata polinomunun seçimleri deşifrelemede m mesaj polinomunu doğrudan etkilemektedir. Şöyle ki $Z_p[x]/(x^n - 1)$ halkasında $r \in (x - 1)$ alınırsa $r(1) = 0$ olacaktır. Bu ise,

$$c(1) \equiv p.r(1).h(1) + m(1)(mod\ q)$$

$$\equiv m(1)(mod\ q)$$

olması anlamına gelir ki r hata polinomunun köklerinin bilinmesi m mesaj polinomunu ifşa etmeye yetecektir. O halde r polinomunun R_p halkasında indirgenemez seçilmesi deşifrelemeye ve hızına olumsuz etki edip güvenliği artırıcı rol oynayacaktır.

4.13. Parametreler N, p, q ve d_f, d_g Seçimleri

İlk önerilen NTRU sisteminde N bir asal sayı olarak seçilmiştir. Hatta Sophie-Germain asalları olması gerektiği belirtilmiştir. Fakat ilerleyen yıllarda sisteme biraz da hız katmak adına N nin 2^n şeklindeki seçimlerinin de mümkün olduğu açıklanmıştır. Özellikle $x^N - 1$ in her bir $d(x)$ böleni için $R_N \to Z[x]/(d)$ ye bir halka homomorfizması bulunabilir. Bu ise SVP ve CVP problemlerinin daha küçük bir halkada aranması demektir. Gentry yaptığı çalışmada $d|N$ için $Z[x]/(x^d - 1)$ halkasında en kısa elemanı ve özel anahtarları bulmanın kolaylaşacağını ifade etmiştir. Ayrıca halkanın modül polinomu $\mathbb{Q}$ da

$$x^N - 1 = (x - 1)\phi_N = (x - 1)(x^{N-1} + \cdots + x + 1)$$

şeklinde parçalanırsa, R_N de terslenebilir elemanlar kümesinin maksimize edilmesi için ϕ_N in R_q da indirgenemez olması gerekmektedir. Zira modülün her bir böleni bir ideal üreteceğinden ve ideal içerisinde birimsel eleman olamayacağından sebeple modülün indirgenemez seçimleri ideal oluşumunu engelleyecek ve birimsel eleman kümesini

büyütecektir. O halde özellikle belirtelim ki özel anahtar aramada ilk kıstas $f(1) \equiv 0\ (mod\ q)$ şeklindeki f polinomlarıdır.

p, q seçimlerinde temel sınırlama aralarında asal ideal üretmeleridir. Yani p ve q sayı iseler $(p, q) = 1$ şartı geçerlidir. Fakat büyük çoğunlukla $p = 3$ ve $q = 2^n$ seçimlerinin hız adına yaygın olduğunu belirtelim.

p ve q açık anahtarlarının büyük seçilmesi karşılık gelen R_p ve R_q halkalarını büyüteceğinden bu değişim farklı anahtar seçimlerini mümkün kılması sebebi ile güvenliğe olumlu, lakin hız ve etkinliğe olumsuz etki edecektir. Buradan yola çıkarak amaçlanan kriptografik protokole uygun olarak parametreler seçmek mümkündür. Örneğin; banka, ödeme, e-mail işlemlerinde hız ve etkinlik ön planda olmalı iken, askeri haberleşme ve operasyonlarda güvenlik had safhada tutulmaktadır.

4.14. f ve g Anahtarlarının Seçimi

Sistemin kurucuları bir L kümesini,

$$L(d_1, d_2) = \{f \in R: f\ nin\ d_1\ katsayısı\ 1, d_2\ katsayısı - 1, kalanı\ 0\}$$

şeklinde tanımlayarak f ve g seçimlerine dair şu öneride bulunmuşlardır:

$$L_f = L\left(d_f, d_{f^{-1}}\right).$$

Yani seçilen f özel anahtarının mutlaka terslenebilir olması gerektiğinden $f(1) = 1$ şartını taşıması gerekir. Hemen hatırlansın ki seçilen polinomlar genelde küçük polinomlar olduğundan $p = 3$ için $\{-1, 0, 1\}$ kümesi üzerindeki polinomlar seçilmektedir. g seçimine gelince mutlaka $d_g < d_f$ olmak koşuluyla

$$L_g = L(d_g, d_g)$$

şartı önerilmiştir. Bu öneride amaç $g(1) = 0$ durumu altında gönderilen e polinomu yardımıyla m mesajının katsayılar toplamına ulaşmaktır. Ayrıca g nin terslenebilir olması g nin seçimlerini küçülteceğinden sistemin hız veya güvenlik kararsızlığında nasıl seçileceği şartları esnektir. f özel anahtar seçimleri ise $F = F_1 \star F_2 + F_3$ ve $d_{F_1} = d_{F_2} = d_{F_3}$ şartları altında $f = 1 + pF$ şeklinde önerilmiştir. g polinomu için de $dg = \lfloor N\ /\ 3 \rfloor$ seçimi önerilmiştir **[43].**

4.15. m Mesaj Polinomunun Seçimine Dair

Mesaj polinomlarının R_p den alınması gerektiğini belirten sistemin kurucuları m için şu kümeyi önermişlerdir:

$$L_m = \left\{ m \in R_p : m \; nin \; katsayıları \; \frac{-(p-1)}{2} \; ve \; \frac{(p-1)}{2} \; aralığındadır \right\}.$$

Buradaki kısıtlamanın temel amacı p ye göre indirgenmemiş bir mesaj polinomu katsayısının indirgendikten sonraki durum m ye eşit değil denk olacağından deşifreleme hatalarına sebebiyet vermemektir. Çalışma bulguları kısmında da değinileceği gibi L_m kümesinin büyütülmesi mesajlanabilir gönderinin seçeneğini artırıp hem etkinlik hem de güvenlik anlamında sisteme olumlu yansıyacaktır. m mesaj polinomunun genişliği, aşırı küçük veya aşırı büyük olmamalıdır. $m(1)$ değerinin $r(1)$ yardımıyla kırılabileceğini ifade etmiştik. O halde $m(1)$ in aşırı büyük değerleri mesajda fazlaca $+1$ katsayılı girdiler anlamına gelecektir. Ya da $m(1)$ in aşırı küçük değerleri sadece birkaç adet $+1$ veya -1 in fazla olacağı anlamına gelir ki açık metin saldırılarına maruz kalır.

Şimdi NTRU kriptosisteminin işleyişini bir örnek üzerinde uygulamalı olarak görelim.

Örnek 4.1 $N = 11$, $q = 32$ ve $p = 3$ parametre seçimleri ve $d_f = 4$, $d_g = 3$ sınırlamaları altında

$$f = -1 + x + x^2 - x^4 + x^6 + x^9 - x^{10}$$

$$g = -1 + x^2 + x^3 + x^5 - x^8 - x^{10}$$

şeklinde seçilsin. Gerekli işlemler sonucunda

$$f_p^{-1} = 1 + 2x + 2x^3 + 2x^4 + x^5 + 2x^7 + x^8 + 2x^9$$

$$f_q^{-1} = 5 + 9x + 6x^2 + 16x^3 + 4x^4 + 15x^6 + 22x^7 + 20x^8 + 18x^9 + 30x^{10}$$

olduğu görülür. Tüm bu f, f_p^{-1}, f_q^{-1} ve g polinomları gizli tutulur. Açık anahtar olan h polinomu $h = pf_q^{-1} \star g(mod\ q)$ kuralı ile hesap edilir. Yine uzun işlemler sonucunda

$$h = 8 + 25x + 22x^2 + 20x^3 + 12x^4 + 24x^5$$

$$+15x^6 + 19x^7 + 12x^8 + 19x^9 + 16x^{10}$$

polinomu elde edilir. Elde edilen bu h polinomu açık anahtar olarak paylaşılır. Bu aşamadan sonra bir $m \in L_m$ mesajı ve $r \in L_r$ hata polinomu seçilerek

$$e \equiv r \star h + m(mod\ q)$$

hesaplanır. Şayet $m = -1 + x^3 - x^4 - x^8 + x^9 + x^{10}$ ve $r = -1 + x^2 + x^3 + x^4 - x^5 - x^7$ olarak alınırsa

$e \equiv r \star h + m(mod\ q)$

$= (-1, 0, 1, 1, 1, -1, 0, -1, 0, 0, 0) \star (8, 25, 22, 20, 12, 24, 15, 13, 12, 19, 16) +$

$+(-1, 0, 0, 1, -1, 0, 0, 0, -1, 1, 1)$

$= 14 + 11x + 26x^2 + 24x^3 + 14x^4 + 16x^5 + 30x^6 + 7x^7 + 25x^8 + 6x^9 + 19x^{10}$

polinomu şifreli metin olarak alıcıya gönderilir. Alıcı e mesajını çözümlerken evvela

$$a \equiv f \star e(mod\ q)$$

hesaplaması yaparak $-q/2$ ile $q/2$ arasından yani $[-15,16]$ aralığından seçilen katsayılarla bir a polinomunu elde eder. Daha sonra

$$b \equiv a(mod\ p)$$

hesaplaması yapılır ki b nin katsayıları $-p/2$ ile $p/2$ arasında kalsın, bu örnekte $p = 3$ olduğundan b nin katsayıları $[-1,1]$ aralığında olmalıdır. Son adımda diğer gizli anahtar olan f_p^{-1} yardımıyla

$$c \equiv f_p^{-1} \star b(mod\ p)$$

hesap edilir ve $c = m$ olması durumunda mesaja net bir şekilde ulaşılır. $a \equiv f \star e(mod\ q)$ şeklinde bulunan a polinomu gerekli tüm hesaplamalar sonucunda

$$a = (3, -7, -10, -11, 10, 7, 6, 7, 5, -3, -7)$$

olarak elde edilir. Daha sonra $b \equiv a(mod\ 3)$ işlemi yapılır ve bu adım sonunda da

$$b = (0, -1, -1, 1, 1, 1, 1, 0, 1, -1, 0, -1)$$

olarak bulunur. Son olarak

$$c \equiv f_p^{-1} \star b(mod\ p)$$

işlemi yapılır.

Sonuç olarak $c = (-1, 0, 0, 1, -1, 0, 0, 0, -1, 1, 1) = m$ olacağından açık metne hatasız bir şekilde ulaşılmış olur.

Not 4.1 Deşifreleme adımlarının minimize edilmesi adına $q > p$ seçiminin önemi Örnek 4.1 de görülmektedir. Şayet $p > q$ olsaydı deşifrelemenin son safhasındaki

$$c \equiv f_p^{-1} \star b(mod\ p)$$

polinomu $c \equiv e\ mod\ p$ olup $p > q$ olduğundan $c = e$ olur ki m polinomuna ulaşılamamıştır.

Not 4.2 F, R de keyfi seçilen bir polinom olmak üzere

$$f = 1 + pqF$$

şeklindeki tüm f polinomları R_p ve R_q da kolaylıkla tersinir olduklarından NTRU işlemlerinde hızlı bir katkı sağlaması adına önerilebilir.

Uyarı 4.1 NTRU kriptosisteminde $(p, q) = 1$ şartı mutlaka sağlanmalıdır. Aksi durumlarda sistem güvenlik açıkları verecektir. Şöyle ki

$$e \equiv ph \star r + m(mod\ q)$$

ifadesi $mod\ q$ da bir denklem olarak değil de R de ele alınırsa

$$e - m = ph \star r + qk,\ \ k \in R$$

haline gelir. Bu denklem R_p de ele alınırsa $e - m \equiv 0\ (mod\ p)$, $(p, q) \neq 1$ olduğundan $e \equiv m\ mod\ p$ olup şifreli gönderi e polinomu hiç bir anahtar bilgisine gerek kalmadan m mesajını açığa çıkarmaktadır.

4.16. Özel Anahtar f Polinomlarının Bulunması

NTRU kriptosisteminin en kritik noktalarından birisi de sistemin üzerine kurulu olduğu cebirsel yapının terslenebilir eleman üretme kapasitesidir. Akla ilk yatkın düşünce

kümenin büyümesi ve bu neticede fazla sayıda birimsel eleman içereceğidir. Şimdi bu matematiksel öngörünün ispatına dair bazı teoremler verilsin.

Teorem 4.1 [43] q asal ise, bir $a \in Z_q[x] \,/\, (x^N - 1)$ polinomunun terslenebilir olması için gerek ve yeter şart $(a, x^N - 1) = 1$ olmasıdır.

İspat ($\Leftarrow$) q asal ise $Z_q[x] \,/\, (x^N - 1)$ bir Öklid bölgesi olacağından genişletilmiş Öklid algoritması yardımıyla $u, v, c \in R$ ve

$$a \star u + v \star (x^N - 1) = 1 + qc \tag{18}$$

olacak şekilde polinomlar bulunabilir.

(18) denklemi R yerine R_q da ele alınırsa

$$a \star u \equiv 1 mod(q, x^N - 1)$$

olur ki $a^{-1} = u$ olarak elde edilir.

($\Rightarrow$) a polinomu R_q da u elemanının tersi olsun. O halde

$$a \star u \equiv 1 mod(q, x^N - 1)$$

denklemi R_q yerine R de yazılırsa

$$a \star u = 1 + qc + + v \star (x^N - 1)$$

haline gelir ve

$$a \star u - v \star (x^N - 1) = 1 + qc$$

düzenlemesi yapılıp son ifade R_q da çözülürse

$$a \star u - v \star (x^N - 1) \equiv 1 (mod\ q)$$

olur ki iddia ispatlanır. ⊠

Şimdi ise q bir asal sayı olmak üzere $Z_q[x] \,/\, (x^N - 1)$ halkasında bir a polinomunun tersi biliniyorken $k \geq 2$ için $Z_{q^k}[x] \,/\, (x^N - 1)$ halkasında terslerin nasıl bulunacağına dair önemli bir teorem verilsin.

Teorem 4.2 [43] q asal bir sayı, $a \in R$ polinomunun R_q halkasındaki tersi u ve $k \geq 2$ ise $a \in R$ nin, R_{q^k} halkasındaki tersi, uygun seçilen bir $c \in R$ yardımıyla

$$a^{-1} = (1 + q^{2^{(s-1)}} c^{2^{(s-1)}}) \star \ldots \star (1 + q^2 c^2) \star (1 + qc) \star u$$

şeklinde bulunur.

İspat a, R_q da terslenebilir olduğundan

$$u \star a + v \star (x^N - 1) = 1 - qc \tag{19}$$

olacak şekilde $u, v, c \in R$ vardır. (19) denklemi R_{q^k} da ele alınırsa

$$u \star a \equiv 1 - qc (mod\ q^k, x^N - 1)$$

ve daha sonra ise

$$u \star a = 1 - qc$$

haline gelir.

$$(1 + qc) \star u \star a = 1 - q^2 c^2$$

$$(1 + q^2 c^2) \star (1 + qc) \star u \star a = 1 - q^4 c^4$$

$$\vdots$$

$$(1 + q^{2^{(s-1)}} c^{2^{(s-1)}}) \star \ldots \star (1 + q^2 c^2) \star (1 + qc) \star u \star a = 1 - q^{2^s} c^{2^s}$$

$2^s \geq k$ ise

$$\left(1 + q^{2^{(s-1)}} c^{2^{(s-1)}}\right) \star \ldots \star (1 + q^2 c^2) \star (1 + qc) \star u \star a \equiv 1 mod\ q^k$$

olur ve böylece

$$a^{-1} = (1 + q^{2^{(s-1)}} c^{2^{(s-1)}}) \star \ldots \star (1 + q^2 c^2) \star (1 + qc) \star u$$

olarak elde edilir.

Not 4.3 Teorem 4.2, q asal olmasa bile R_q halkalarında kullanılabilir. Şöyle ki $q = q_1 q_2$ farklı asallar çarpımı ise Çin Kalan Teoremi gereğince

$$R_q \cong R_{q_1} \times R_{q_2}$$

olup R_{q_1} halkasında terslerin nasıl bulunacağını söyleyen Teorem 4.2 yardımıyla R_q büyük halkasında da terslerin kartezyen çarpımını almak şeklinde ters elemanlara ulaşılabilir.

4.17. Latisler ve NTRU Kriptosistemi Arasındaki Bağlantı

Bir NTRU kriptosistemini (n, p, q) parametreleri, f, g özel anahtarları ve

$$h \equiv p.f^{-1} \star g \ (mod\ q) \Leftrightarrow p^{-1}.h \equiv f^{-1} \star g \ (mod\ q) \tag{20}$$

şeklinde tanımlı bir h açık anahtarı eşliğinde göz önüne alalım. $h' = p^{-1}.h$ notasyonunu kullanarak (20) denklemini

$$h' \equiv f^{-1} \star g \ (mod\ q) \Leftrightarrow f \star h' \equiv g \ (mod\ q)$$

formunda yeniden yazılsın. Bir τ tam sayılı polinomu için

$$f \star h' + q.\tau = g \tag{21}$$

yazımı mümkündür. O halde (21) denklemini matris formunda

$$(f \quad \tau)\begin{pmatrix} I & H' \\ 0 & qI \end{pmatrix} = (f \quad g) \tag{22}$$

haline getirmek mümkündür. (22) denkleminde H' matrisi h' polinomunun döngüsel matrisidir. İşte bu şartlar altında tanımlı (22) denklemindeki $\begin{pmatrix} I & H' \\ 0 & qI \end{pmatrix}_{2n \times 2n}$ matrisinin sütunlarının ürettiği latise NTRU latisi denir. Açıktır ki tanım gereği (f, g) bu latisin bir vektörüdür ve yine latisin tanımı gereği bir $t \in Z$ için (tf, tg) de bir başka özel anahtardır. (f, g) nin her katının oluşturduğu altlatisin herhangi bir vektörüne ulaşılması durumunda (f, g) ye ulaşmak oldukça kolaylaşacaktır. O halde latisin en kısa vektörünün bulunması bihassa $((f, g))$ altlatisinin en kısa vektörünün yani (f, g) nin bulunması sistemi çözecektir **[43]**.

4.18. NTRU Kriptosistemine Yapılabilecek Kriptolojik Saldırı Türleri

4.18.1. CVP metoduyla saldırı

h açık anahtarı yardımıyla Konvolüsyon Modüler Latis denilen bir L_h latisi,

$$L_h = \{(a, b) \in Z^{2N} : a \times h \equiv b \ (mod\ q)\}$$

şeklinde oluşturulur. Şifreli metin, NTRU polinom halkasında

$$e = r \star h + m$$

şeklinde bir polinom iken L_h latisinde

$$(0, e) \equiv (0, r \star h + m \ (mod\ q))$$

vektörüne dönüşecektir. Hatta latis bir ayrık abel grubu olduğundan

$$(0, e) = \big(r, r \star h \ (mod\ q)\big) + (-r, m)$$

yazımını mümkün kılar. L_h latisi h ile konvolüsyon çarpılan tüm polinomlardan (vektör) oluştuğu için $(r, r \star h)\ mod\ q$ latisin bir vektörüdür. Şu durumda $(0, e)$ vektöründen nasıl bir r seçimi altında $(r, r \star h)\ mod\ q$ vektörü çıkarılsın ki $(-r, m)$ vektörüne ve buradan da açık metne ulaşılsın? Bu sorunun cevabı CVP algoritmalarında gizlidir. Buradan hareketle hata polinomu r nin bulunması neredeyse f gizli anahtarının bulunması kadar risklidir denebilir **[40]**.

4.18.2. Çoklu gönderim saldırısı

Bu saldırının temel amacı sürekli aynı h açık anahtarını kullanmanın iyi bir fikir olmadığını belirtmesi açısından önemlidir. Gönderici aynı mesajı aynı h açık anahtarıyla ve fakat farklı hata polinomları seçerek göndermiş olsun.

$$e_i \equiv pr_i \star h + m \ (mod\ q) \qquad i = 1, 2, \dots, n$$

Saldırgan ise n tane farklı şifreli metin yardımıyla

$$\big(e_i - e_j\big) \star (ph)^{-1} \ (mod\ q) \quad 1 \leq i < j \leq n$$

ifadesini ya da denk bir ifade olan

$$r_i - r_j \ (mod\ q) \qquad 1 \leq i < j \leq n$$

ifadesini bulmaya çalışır. Şayet $d_r = \{-1, 0, 1\}$ ise $r_i - r_j$ polinomunun katsayıları $\{-2, -1, 0, 1, 2\}$ kümesinden seçilecektir. r nin muhtemel sonuçları polinom zamanda bulunabileceğinden saldırıya en açık yöntem sürekli aynı h anahtarını kullanmaktır denebilir. Bu noktadan hareketle f özel anahtarının seçim kümesinin genişliği h anahtarının seçim kümesini doğrudan etkileyeceğinden büyük bir polinom halkasında NTRU daha korunaklı bir hale gelecektir **[40]**.

4.18.3. Kaba güç (Brute force) atağı

$f \star h \equiv g \ (mod\ q)$ olacağından g nin açığa çıkması f yi direkt olarak verecektir. Üstelik $d_g < d_f$ önerisi altında L_g uzayı daha küçük olacağından f yerine g yi aramak daha pratiktir.

Saldırgan d_g parametresini bildiğinden ve f küçük bir polinom olduğundan

$g \star h^{-1}\ (mod\ q)$ sonuçlarının tüm küçük olanlarını deneyecektir. Sonuç olarak yaklaşık $\binom{N}{d_g}$ kadar işlem yapıp f yi kırmaya çalışacaktır **[40]**.

4.18.4. Ortada buluşma atağı

Sistemin kurucusu, **r** hata polinomunun bilinmesinin f ye doğrudan etki edeceğinden hareketle bazı yeni önerilerde bulunmuştur. Öncesinde saldırıyı ve metodunu kısaca verelim. Öncelikle bu saldırı N ve d_f sayılarının çift olması durumunda çalışır. Keza çift olmaması durumunda modifiye edilmesi durumunda yine bu saldırıya açık hale getirilebilir. Temel düşünce ise $f = f_1 + f_2$ şeklinde $N/2$ uzunluğunda ve $d/2$ adet 1 katsayılı iki polinom elde etmektir. En uygun seçim ise 1 li katsayıları bir yana -1 li katsayıları bir yana almaktır. Saldırının matematiği,

$$f \star h \equiv g \ (mod\ q)$$

$$f_1 \star h + f_2 \star h \equiv g \ (mod\ q)$$

i. koordinatlardaki denklik

$$(f_1 \star h)_i \equiv \{0, 1\} - (f_2 \star h)_i \ (mod\ q)$$

olacağından saldırgan, $\binom{N/2}{d/2}$ seçim sonucu f_1 i belirlemeye çalışır. g polinomunun i.

koordinatı ya 0 ya da 1 olacağından iki farklı durumda f i aramaya devam eder. Bu saldırı esnasında

$$f \star h \equiv g \ (mod\ q)$$

$$f \star x^i \star h \equiv g \star x^i \ (mod\ q) \qquad 1 \leq i \leq n$$

olacağından bir özel anahtar rotasyonuna denk geldiğinden N adet seçim sonucu saldırgan f ye ulaşacaktır **[40]**.

4.18.5. Latis saldırısı

İlk latis saldırısı 1997 yılında Coppersmith ve Shamir tarafından önerildi. Bu saldırı latisin en küçük vektörünü bulma algoritmasıyla çalışmaktadır. Aşağıdaki gibi bir $2N \times 2N$ NTRU latisindeki

$$\begin{pmatrix} \tau I & H \\ 0 & qI \end{pmatrix}$$

$\tau \in R$ şeklinde seçilen parametreye dengeleyici parametre denir, $(\tau f, g)$ noktası latise aittir. O halde (f, g) ye en yakın vektörü bulma algoritmaları özel anahtarı ele geçirebilir. Bunun için ise $\|f\| \sim \|g\|$ ve $\tau = \frac{\|f\|}{\|g\|}$ seçimleri doğrultusunda $\tau \to 1$ olur ki

saldırı öldürücü niteliğe gelecektir **[40]**.

4.19. NTRU Türevi Çalışmalar

NTRU üzerine yapılan çalışmalar ve bu çalışmaların yorumlanması üzerine aşağıda sıralı olarak verilecek NTRU çalışmaları, sistemin varyasyonları ve gelinen aşama hakkında bilgilendirici niteliktedir.

$f \in L_f$ seçimi terslenebilir olmak zorunda olduğundan çalışılan halkada yeteri kadar birimsel polinom olup olmadığı problemi doğacaktır. Bu noktada Banks ve diğerleri 2002 de bir NTRU varyasyonu yayınlayarak terslenemeyen polinom seçimlerinin etkisini incelemişlerdir**[77].**

Yine 2002 de Gabroit ve diğerleri N parametresinin seçimlerinin önemini işaret eden, LLL tabanlı saldırılara karşı daha korunaklı CTRU ismiyle N seçimlerinden fazla etkilenmeyen katsayıları da polinom olan bir metod önermişlerdir [71].

2005 yılına gelindiğinde ise Cogliansе ve diğerleri MaTRU ismiyle matris tabanlı bir NTRU türevi önerdiler. Bu yöntemde ise kriptosistemin halkası $k \times k$ matrisler ve deşifreleme safhasında değişmelilik özelliğine haiz matrisler seçilerek önerilmiştir**[72].**

2008 de ise Nayak ve diğerleri NTRU sisteminin matris formunun polinom formundan daha hızlı olduğunu gösteren bir çalışma yayınladılar**[78].**

Malekian ve diğerleri ise değişmeli olmayan cebir tabanlı (quaternion algebra) yeni bir sistemi QTRU ismiyle 2009 yılında sundular. Bu çalışmanın önemi, lineer mantık ile çalışan latis saldırılarına karşın sistemin bilineer formda olması sebebiyle QTRU nun latis ataklarına karşı oldukça dirençli bir sistem oluşudur**[76].**

2010 da Nevins ve diğerleri ETRU ismiyle yeni bir Eisenstein tam sayılar tabanlı yöntemi önerdiler. 2015 yılında ise Nanda ve diğerleri Gausyen tam sayı girdili matrisler kullanarak önerdikleri sistemin NTRU ya göre oldukça dirençli olduğunu göstermişlerdir**[75].**

Şimdi yukarıda bahsi geçen çalışmalardan birkaçının matematik sistemi verilecektir.

4.19.1. Terslenebilir olmayan polinomlar ile NTRU

2002 de Banks ve diğerlerinin önerdiği bu sistem şifreleyicinin yeteri kadar birimsel polinom bulamayabileceği varsayımı üzerine kuruludur. Klasik NTRU da $f \in L_f$ hem $mod\ p$ hem de $mod\ q$ da terslenebilir olmalı idi. Oysa bu yeni sistemde f_q^{-1} şartı aranmadan keyfi bir G polinomu şayet bu f_q^{-1} görevini üstlenecek ise bu amaçla kullanılabilmelidir. Şöyle ki tüm seçimler NTRU ile aynı olduğunda tekrara gerek kalmadığını varsayıp sadece $f \in L_f$ için $f, mod\ p$ de terslenebilir olsun şartını verip $G \in R$ için $G\ mod\ q$ da terslenebilir olsun şartını ekleyelim. $f \in L_f$, $g \in L_g$ ve $G \in R$ olsun. İlave şart olarak $f\ mod\ p$ de G ise $mod\ q$ da birimsel olsun. f_p^* ve G_q^* sırasıyla bu tersleri ifade etsin. $h = G_q^* \star g\ (mod\ q)$ ve $H = G_q^* \star f\ (mod\ q)$ şeklinde iki açık anahtar belirleyip (h, H) şeklinde yeni açık anahtar ve (f, g, G) ise özel anahtar olarak kullanılır. Şifreleme yapılırken keyfi bir $m \in L_m$ seçilip

$$e = pr \star h + H \star m\ (mod\ q)$$

şeklinde gönderilir. Deşifreleme esnasında G gizli anahtarı kullanılarak ilkin

$$a = G \star e = pr \star g + f \star m$$

elde edilir. Uygun katsayı indirgemeler hesap edilerek $mod\ p$ ye inilirse

$$f_p^* \star a = m$$

olarak açık metne ulaşılır. Sistemin avantajları ise daha esnek parametreler seçimi sonrası uygun bir R halkasında yeteri kadar G nin bulunması, G nin küçük seçimi halinde hızın yükselmesi şeklinde verilebilir.

4.20. MATRU Kriptosistemi

2005 yılında ise Coglianese ve Goi **[72]** MATRU adını verdikleri çalışmalarında NTRU yu $M_{k\times k}$ matrislerin halkası üzerinde incelediler. p ve q nun aynı kaldığı bu yeni sistemde $\star$ işleminin yerine adi matris çarpımı yapılır. Matrisin girdileri ise $R = Z[x]/x^N - 1$ halkasındaki polinomlardır.

4.20.1. Sistem nasıl çalışır?

Öncelikle A ve B gibi iki matris ve $\alpha_0, \alpha_1, \dots, \alpha_{k-1} \in R$ ve $\beta_0, \beta_1, \dots, \beta_{k-1} \in R$ gibi iki polinom kümesi "kısa" olacak şekilde seçilir. Daha sonra f ve g gibi iki matris

$$f = \sum \alpha_i A^i\ , g = \sum \beta_i B^i$$

kuralı ile inşa edilir. Parametrelerin seçimi f ve g matrisleri her iki ($mod\ p$ ve $mod\ q$) modülde de tersinir kılınmalıdır. f nin $mod\ p$ ve $mod\ q$ daki terslerini sırasıyla F_p ve F_q, g nin de benzer şekilde $mod\ p$ ve $mod\ q$ daki terslerini G_p ve G_q ile gösterirsek keyfi bir $w \in M$ için

$$h \equiv F_q \star w \star G(mod\ q)$$

şeklinde kurulan h matrisi açık anahtardır. (f, g) ikilisi ise gizli anahtar olacaktır. Bir $m \in M$ mesajı keyfi seçilen T ve S matrisleri yardımıyla

$$e \equiv p(T \star h \star S) + m(mod\ q)$$

şeklinde şifrelenerek gönderilir. Alıcı ise ilk olarak

$$a \equiv f \star e \star g mod\ q$$

ifadesini hesap edip daha sonra

$$d \equiv F_p \star a \star G_p mod\ p$$

işlemi sonucunda m mesajını elde eder.

4.20.2. Sistemin analizi

MATRU sisteminde işlemler yalnız polinomlar arasında değil, ayrıca polinom matrisleri arasında olacağından bir nebze komplike bir durum oluşacaktır. Bu hesaplamaların kolaylaşması adına kurucuları α_i ve β_i polinomlarının "kısa" olması gerektiğini ve N, NTRU parametresi ile n, k MATRU parametreleri arasında şayet $nk^2 = N$ ilişkisi bulunuyorsa ancak MATRU sisteminin aynı hızlarda çalışacağını belirtmişlerdir. $nk^2 > N$ durumunda zaten uzun zaman ve efor sarfeden konvolüsyon çarpımı üstelik matrisler arasında yapılırken daha fazla zaman alıp efor harcayacağıdan sistem yavaşlayacaktır.

4.21. QTRU Kriptosistemi

2009 da Malekian ve diğerleri **[79]** QTRU adını verdikleri çalışmalarında NTRU tabanlı yeni bir kriptosistem kurdular. Kuaterniyonlar üzerinde inşa edilen bu sistemin en ayırt edici özelliği olasılık barındırmasıdır. Bir diğer karakteristik özelliği ise yüksek boyutlu olmasıdır. Detaylarının daha geniş bir cebirsel bilgi gerektirmesi nedeniyle burada verilmeyeceği bu sistemin kriptolojiye bir diğer katkısı ise değişmeli olmayan yeni bir halka üzerinde NTRU kurulmasıyla abelyen olmayan halkaların ve işlemlerin ataklara karşı daha korunaklı olduğu sonucunu çıkarmasıdır.

4.22. Gaussyen Tam Sayılı Girdili Matrislerle NTRU

Nanda ve diğerleri **[80]** 2015 yılında NTRU kriptosistemini kompleks sayılar girdili matrisler üzerinde incelediler. Bu çalışmanın temel felsefesi, daha önceki tam katsayılı matrislerin bazı ataklara karşı daha da güçlendirilmesi adına girdileri kompleks yapmak üzerinedir. bu çalışmanın NTRU ya katkısı, $\{-1,0,1\}$ kümesindeki sayıların oluşturduğu bir matriste özel anahtar ya da açık metin saldırılarına N^3 genişliğindeki bir küme yerine $\{1+i, 1-i, -1+i, -1-i, 0, 1, -1, i, -i\}$ kümesinden alınan girdilerle oluşturulacak bir matriste sistemin klasik NTRU ya göre N^6 kez daha güvenli oluşudur.

5. TEZİN İÇERİSİNDE CEVAP ARANAN SORULAR VE AÇIK PROBLEMLER

1) Kurucu ekibin yaptığı, Optimizations for NTRU adlı çalışmada**[68]** R halkası üzerindeki bir NTRU sistemi için " R_f, R_g, R_r ve R_m kümeleri ne kadar büyük seçilebilir ve bu seçimler NTRU yu nasıl etkiler?" problemine cevaplar aranacaktır.

2) Aynı çalışmada yer alan, $p \star r \star g + m \star f$ polinomu uzunluğu en fazla q olan bir aralıkta bulunmalıdır. q nun farklı seçimleri bu polinomun bulunduğu aralığı ve R_f, R_r, R_g gibi kümeleri nasıl etkiler? Sorusuna cevaplar aranacaktır.

3) f gizli anahtar seçimlerinin kurucu ekip tarafından $f = 1 + p \star f_1$, $f_1 \in R$ şeklindeki seçimlerinden olması gerektiği ve bu gerekliliğin hesaplama kolaylığı sağladığı fakat (f_1, g) şeklinde latisin içerisinde aranacak bir vektörün ne gibi güvenlik açığı vereceği sorusuna bir cevap aranmıştır.

4) p modülü bir sayı olmasının yanı sıra şayet polinom olarak seçilirse sistemin güvenlik düzeyi ve diğer parametre nasıl seçilir? sorusuna cevap aranmıştır.

5) "Choosing parameters for NTRU" isimli çalışmada[52], $x^N - 1 = (x-1)\phi_N(x)$ indirgemesinden sonra $\phi_N(x)$ polinomunun indirgenip indirgenememesi probleminin sisteme etkisi tartışmaya açılmıştır. Bu tez içerisinde de bu soruya cevap aranmıştır.

6) NTRU kriptosistemine yapılabilecek en iyi saldırının latis indirgeme algoritmaları olacağı belirtilip[52], bu atak türünden sistemin nasıl korunabileceği sorusuna cevap aranmıştır.

7) Ayrıca literatürde yer almayan ancak cevap aranan bir diğer soru ise sistemin açık ve/veya gizli anahtar sayısının artışının sisteme cebirsel etkisi incelenmiştir.

8) NTRU kriptosisteminin latisinin;

$$L_h = \{(f, g) \in R^2 : g \equiv h \star f/p \ (mod\ q)\},$$

olduğu göz önüne alınırsa, $Boy(L_h) = 2N$ ve $Det(L_h) = q^N$ olduğundan, L_h latisinin matris gösterimi bir L güvenlik sabiti ilavesi ile

$$\begin{pmatrix} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-2} & h_{N-1} \\ 0 & \alpha & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-3} & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots & \ddots \ \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & & \cdots & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & & \cdots & q \end{pmatrix}$$

şeklindedir burada $h = (h_0, \ldots, h_{N-1})$ açık anahtar polinomu latisin en önemli karakteristik özelliğidir. Latis indirgeme saldırılarına karşılık açık anahtara bir

$\varphi: R \rightarrow R$ izomorfizması eklenerek, $\varphi(g) \equiv \varphi(h) \star \varphi(f/p)(mod\ q)$ dönüşümü yardımıyla oluşan yeni latisin güvenlik düzeyi incelenmiştir.

9) "Optimizations for NTRU" çalışmasında kurucu ekip L_f, L_g, L_r ve L_m kümelerinin büyük seçilmesi gerektiğini bir saldırı esnasında h açık anahtarından f ve g gizli anahtarlarının ayrıştırılmasının zor bir hale getirilmesinin ve e şifreli polinomdan m açık metin polinomu bulunmasının bir güvenlik açığı oluşturacağından ne gibi cebirsel katkılar sunabileceğini tartışmışlardır. Z_p yerine Z_{p^k} halkası ve m mesaj polinomu da bir rotasyon, izomorfizma ve polinom çarpımı işlemleri ile denklem daha kompleks bir yapıya oturtulacaktır.

10) Matematica programı yardımıyla NTRU kriptosistemi daha büyük parametrelerle ve daha fazla ve farklı sayıda anahtar seçimleri ile incelenmiş ve doğru bir şekilde çalışan birçok uygulama örneği elde edilmiş ve bunlar tezin son bölümünde Algoritmalar bölümünde sunulmuştur.

6. GALOİS HALKALARI ÜZERİNDE NTRU

Buraya kadar da görüleceği üzere, NTRU halkasında f ve g gibi n mertebeli iki polinomun konvolüsyon çarpımı n^2 işlem gerektireceği için polinomların katsayıları küçük ya da genellikle $\{-1,0,1\}$ kümesinden seçilir. Daha önceki çalışmalarda, terslenebilir f polinomunun seçimi F keyfi bir polinom olmak üzere, $f = 1 + pF$ şeklinde yapılmıştır çünkü $f mod\ p \equiv 1$ olacak ve tersi kolayca elde edilecektir. (16) denklemindeki ifade $mod\ q$ ya göre uygun seçilmiştir. Buradan hareketle NTRU hız ve kolay işlem yapmayı esas alır diyebiliriz. Bu ise doğal olarak güvenlik açıkları verecektir. NTRU işlemleri $Z_p\ [x]$ ve $Z_q[x]$ de yapılır. Sistemin daha büyük bir kümeye taşınması sisteme katkı sağlayacaktır. $Z_{p^k}\ [x]$ açıktır ki daha büyük bir kümedir. Aynı zamanda Galois halkalarının özel bir türüdür. Önerilen yeni parametreler ve özel anahtarlar bu halkadan seçilecektir. Bu kısımda NTRU kriptosistemi ilk defa tarafımızdan Galois halkalar üzerinde ele alınıp orijinal cebirsel katkılar kriptosisteme ilave edilecektir.

6.1. Galois Halkalarının Cebirsel Yapısı

Galois halkaları, bir halkanın Galois genişlemeleri neticesinde elde edilir. p bir asal sayı, n ve r pozitif tam sayılar olmak üzere $GR(p^n, r)$ notasyonu ile gösterilirler. Bazı aşikar örnekleri aşağıdaki gibidir:

i. $n = 1$ ise $Z_p \cong F_p$ cisminin r genişlemesi elde edilir.

$$GR(p, r) = GF(p^r) = F_{p^r}$$

ii. $r = 1$ ise $GR(p^n, 1) = Z_{p^n}$

$GR(p^n, 1)$ tipindeki Galois halkaları $Z_{p^n}[x]\ /\ (f(x))$ bölüm halkasına izomorfiktir. $f(x) \in Z_{p^n}[x]$ monik, temel indirgenemez bir polinomdur. Denk olarak $f(x) \in Z[x]$, r. mertebeden monik, $mod\ p$ ye göre indirgenemez seçilirse $GR(p^n, r) \cong Z[x]\ /\ (p^n, f(x))$ olacaktır. Bu halka lokaldir ve tek maksimal ideali $pGR(p^n, r)$ dir.

Ayrıca bu halkanın tüm idealleri esas idealdir ve $(p^i) = p^i GR(p^n, r), 0 \leq i \leq n$ formundadır **[44]**.

μ doğal homomorfizması, $Z_{p^k}[x]$ den aldığı bir polinomun katsayılarını $mod\ p$ ye göre

indirgeyerek $Z_p[x]$ de bir polinoma dönüştürsün. Aşağıdaki lemma ve önermeler sunulacak sistem için önemlidir.

Lemma 6.1 [44] $m = \prod {p_i}^{e_i}, e_i \geq 1$ ve p_i farklı asal sayılar olmak üzere

$$Z_m \cong Z_{{p_1}^{e_1}} \times Z_{{p_2}^{e_2}} \times \ldots \times Z_{{p_n}^{e_n}}$$

olur. İzomorfizmayı sağlayan dönüşüm

$\varphi: i \to (a^1, a^2, \ldots, a^s), i \in Z_m$ ve $i \equiv a^j \left(mod\ {p_j}^{e_j}\right), j = 1,2, \ldots, s$

şeklindedir.

Not 6.1 $m \neq p^n$ şeklinde bir sayı olduğunda Z_m lokal halka veya zincir halkası değildir, ancak lokal halkaların direkt çarpımı şeklinde yazıldığından yarı lokal halkadır. Not edelim ki Z_{p^n} in birimsel olmayan tüm elemanları nilpotenttir ve bu sebeple Artin halkaları sınıfına girer. $m \neq p^n$ için Z_m bu yapıda değildir.

Önerme 6.1 [44] $f(x) = a_0 + a_1 x + \cdots + a_n x^n, Z_{p^k}[x]$ de bir polinom olsun.
Aşağıdaki ifadeler denktir:

- **i.** f birimseldir.
- **ii.** $\mu(f), Z_p[x]$ de birimseldir.
- **iii.** $a_0 \in Z_{p^k}$ birimsel ve $a_1, \cdots, a_n$ nilpotenttir.

Önerme 6.2 [44] $(x) = a_0 + a_1 x + \cdots + a_n x^n, Z_{p^k}[x]$ de bir polinom olsun. Aşağıdaki ifadeler denktir:

- **i.** f nilpotenttir.
- **ii.** $\mu(f) = 0$.
- **iii.** $a_0, a_1, \cdots, a_n$ nilpotent elemanlardır.
- **iv.** f sıfır-bölendir.

6.2. Önerilen Kriptosistem

6.2.1. Önerilen sistemin parametreler seçimi

Modüllerin seçimi: Klasik NTRU işlemlerindeki p modülü yerine $p^k, k \geq 1$ tam sayısı alınırsa yine $(p^k, q) = 1$ olacaktır. Modül olarak; p^k, p asal ve $k \geq 2$ seçilirse uygun parametre seçimi neticesinde işlemler Galois halkasında yapılabilecektir. Bir $m \in Z$ için

$m = {p_1}^{a_1}{p_2}^{a_2} \dots {p_r}^{a_r}$ olacak şekilde bir gösterim tek türlü olduğundan ${p_1}^{a_1} \to p^k$ ve ${p_2}^{a_2} \dots {p_r}^{a_r} \to q$ ikamesi yapılırsa $({p_1}^{a_1}, {p_2}^{a_2}, \dots, {p_r}^{a_r}) = 1$ olacağından $Z_m \cong Z_{p^k} \times$

Z_q olur ki Z_{p^k} halkasının cebirsel yapısı üzerinde işlemler yapılabilir.

Mesaj polinomlarının seçimi: Yine klasik NTRU protokolündeki $m \in Z_p[x] \,/\, (x^n - 1)$ mesaj polinomunu, $m \in Z_{p^k}[x] \,/\, (x^n - 1)$ olarak değiştirip, $h \equiv p f_q^{-1} \star g (mod\ q)$ açık anahtarını da, $h \equiv p^k f_q^{-1} \star g (mod\ q)$ haline getirelim. $e \equiv r \star h + m (mod\ q)$ ifadesi $e \equiv r \star p^k f_q^{-1} \star g + m (mod\ q)$ olacaktır. $e \star f \equiv r \star p^k f_q^{-1} \star f \star g + f \star m (mod\ q)$ olup $e \star f \equiv r \star p^k \star g + f \star m (mod\ q)$ dir. Şayet $k \to \infty$ ise $p^k \to \infty$ olacağından k sayısı istenildiği kadar büyük seçilirse ve $f \star m (mod\ q)$ ifadesi $f \star m (mod\ p^k)$ olarak kalırsa yani $f \star m$ polinomunun katsayıları $mod\ p^k$ da tekrar indirgenmez ise,

$$e \star f \equiv f \star m (mod\ p^k)$$

$$e \star f \star f_{p^k}^{-1} \equiv m (mod\ p^k)$$

$$e = m$$

olur ki bu da mesajlanabilir halkanın büyütülmesi demektir.

Özel anahtar seçimleri: Sistemin parametrelerinden olan $(p, q) = 1$ şartını sağlayan her p, q için $(p^k, q) = 1$ olacağından $k = 1$ halinde klasik parametreye dönülebilir. Seçilen bu k sayısına karşılık gizli anahtar olan f polinomu yerine de f^k alınabilir. $(f^k)^{-1} = (f^{-1})^k$ olacağından, sistem bu durumda $h \equiv p^k \left(f_q^{-1}\right)^k \star g (mod\ q)$ olmak üzere $h \equiv \left(p f_q^{-1}\right)^k \star g (mod\ q)$ halini alır. $e \equiv r \star h + m (mod\ q)$ ifadesi ise

$$e \equiv r \star p^k \left(f_q^{-1}\right)^k \star g + m (mod\ q)$$

$$e \star f^k \equiv r \star p^k \star g + m \star f^k (mod\ q)$$

$$e \star f^k \star \left(f_{p^k}^{-1}\right)^k \equiv r \star p^k \star g \star \left(f_{p^k}^{-1}\right)^k + m (mod\ p^k)$$

$$\equiv 0 + m (mod\ p^k)$$

$$e \equiv m (mod\ p^k)$$

$$e = m$$

olup gizli anahtarın çarpımsal gruptaki mertebesi büyük seçilirse farklı bir şifreleme protokolü sunacaktır. f polinomun üreteç polinom olarak seçilmesi önerilebilir.

Bir diğer anahtar seçimi f gizli anahtarına rotasyonlar uygulayıp $f \star x^i, 1 \leq i \leq n-1$ şeklinde yeni gizli anahtarlar elde etmek olabilir. Şöyle ki;

$f \star x^n = f \star 1 = f$ olacağından bu ötelemeler $n-1$ adımda bitirilmelidir. Açık anahtar olan $h \equiv p f_q^{-1} \star g (mod\ q)$ polinomu şu halde h$\equiv p^k \left(f_q^{-1}\right)^k \star g \star x^{n-i}\ (mod\ q)$ haline gelir.

$$e \equiv r \star h + m (mod\ q)$$

$$\equiv r \star p^k \left(f_q^{-1}\right)^k \star g \star x^{n-i} + m (mod\ q)$$

$$\vdots$$

$$e \star f^k \star x^i \equiv r \star p^k \star g + f^k \star m \star x^i\ (mod\ q)$$

$$\equiv f^k \star m \star x^i\ (mod\ p^k)$$

$$e \star f^k \star \left(f_{p^k}^{-1}\right)^k \star x^i \star x^{n-i} \equiv m (mod\ p^k)$$

$$e \equiv m (mod\ p^k)$$

$$e = m$$

bulunur ki, gizli anahtarın $i.$ rotasyonları da gizli anahtar görevi görür.

Sonuç olarak, klasik anahtar protokolündeki $(p, q) = 1$ olacak şekildeki p ve q sayılarının çok küçük seçilmeyip istenildiği kadar büyütüleceği ve hesaplamaların daha büyük halkalarda yapılabileceği öngörülmüştür. Bir f polinomu tersinir olduğunda her kuvveti de tersinir olacağından üreteç polinomların NTRU ya katkı sağlayacağı öngörülmektedir. $f \star g \equiv h (mod\ q)$ ifadesi her $0 \leq i \leq n$ için $f \star g \star x^i \equiv h \star x^i\ (modq)$ ifadesi geçerli olacağından özel anahtarın çok sayıda rotasyonlarını da hesaba katmanın güvenliği artırıcı etkisi olacağı öngörülmüştür.

6.3. Galois Halkaları Üzerinde NTRU

$(n, p) = 1$ olmak üzere

$$Z_{p^k}[x] \,/\, (x^n - 1) \cong Z_{p^k}[x] \,/\, (x - 1) \times Z_{p^k}[x] \,/\, (x^{n-1} + x^{n-2} + \cdots + 1) \qquad (23)$$

olur. n yerine $(p, q) = 1$ olacak şekilde bir q asalı seçilirse $\Phi_q(x) = x^{q-1} + x^{q-2} + \cdots + 1$, q. dereceden devirsel polinomu elde edilir.

Durum 1: Herhangi dereceden bir devirsel polinom Z de indirgenmezdir ancak uygun seçilmiş bir Z_{p^k} halkasında bazı kökleri bulunabilir. Eğer $\Phi_q(x)$ polinomu Z_p de

indirgenmez ise Z_{p^k} da da indirgenmezdir.(Hansel lemma). Bu durumda $Z_{p^k}[x] \,/$

$(x^{q-1} + x^{q-2} + \cdots + 1)$ Galois halkası olur. $Z_{p^k}[x] \,/\, (x - 1) \cong Z_{p^k}[x]$ ve Z_{p^k} da

Galois halkası olduğundan $Z_{p^k}[x] \,/\, (x^n - 1)$ halkası $n = q$ asalı ve $(q, p) = 1$

durumunda Galois halkalarının direkt çarpımı şeklinde yazılır. Bu durumda bir φ izomorfizması $\varphi: Z_{p^k}[x] \,/\, (x^n - 1) \to Z_{p^k}[x] \,/\, (x - 1) \times Z_{p^k}[x] \,/\, (\Phi_q(x))$

$$\varphi(f) \longmapsto (f(1), f mod\ \Phi_q(x))$$

şeklinde tanımlanarak bulunabilir. NTRU için terslenebilir bir f aradığımızdan $f(1) \neq 0$ ve $f mod \Phi_q(x) \neq 0$ şartları sağlanmalıdır.

Durum 2: Diğer bir durum ise $\Phi_q(x) = x^{q-1} + x^{q-2} + \cdots + 1$ polinomunun bazı köklerinin bulunduğu bir Z_{p^k} halkası inşa etmektir. Bu şartları sağlayan bir $p^k \in Z$ için

$\alpha_i \in Z_{p^k}, 1 \leq i \leq q - 1$ olmak üzere

$\Phi_q(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_{q-1})$

olarak yazılabilir. $\alpha_i \neq \alpha_j$, $1 \leq i, j \leq q - 1$ olacağından $(x - \alpha_i, x - \alpha_j) = 1$ olur ve

$$Z_{p^k}[x]/(\Phi_q(x)) \cong Z_{p^k}[x]/(x - \alpha_1) \times Z_{p^k}[x]/(x - \alpha_2) \times \ldots$$

$$\times Z_{p^k}[x]/(x - \alpha_{q-1}) \qquad (24)$$

olacaktır. Şu halde

$$Z_{p^k}[x]/(x^n - 1) \cong Z_{p^k}[x]/(x - 1) \times Z_{p^k}[x]/(x - \alpha_1) \times$$

$$Z_{p^k}[x]/(x - \alpha_2) \times \ldots \times Z_{p^k}[x]/(x - \alpha_{q-1}) \qquad (25)$$

olup bir φ izomorfizması,

$$\varphi: Z_{p^k}[x]/(x^n-1) \to Z_{p^k}[x]/(x-1) \times Z_{p^k}[x]/(x-\alpha_1) \times$$

$$Z_{p^k}[x]/(x-\alpha_2) \times \ldots \times Z_{p^k}[x]/(x-\alpha_{q-1})$$

$$\varphi(f) \to (f(1), f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_{q-1}))$$

şeklinde tanımlanabilir. Şayet $\varphi(f)$ polinomları $mod\ p^k$ da hesaplanırsa, yani $\bar{\varphi}(f) \to \left(f(1), f(\alpha_1), f(\alpha_2), \ldots, f\left(\alpha_{q-1}\right)\right) mod p^k$ doğal homomorfizması altındaki görüntüler alınırsa $\bar{\varphi}(f) \in Z_{p^k}[x]$ olarak ele alınabilir.

Bir $f \in Z_{p^k}[x]/(x^n-1)$ polinomunun terslenebilir olma şartı $f = \beta + ps(x), s(x) \in Z_{p^k}[x]/(x^n-1)$ ve $(\beta, p^k) = 1$ formunda olmasıdır. Bu formda seçilmiş bir f polinomunun izomorfik görüntüsü olan $\varphi(f)$ de tersinirdir. Bir $m \in Z^+$ sayısı kanonik formda $m = \underbrace{p_1^{s_1}}_{p^k} \underbrace{p_2^{s_2} \ldots p_i^{s_i}}_{q}$ şeklinde olup,

$$Z_m[x]/(x^n-1) \cong Z_{p^k}[x]/(x^n-1) \times Z_q[x]/(x^n-1)$$

olur ki, $p^k \to \infty$ ve $q \to \infty$ için $m \to \infty$ olacağından sonsuza yakınsayan bir NTRU halkasının cebirsel yapısını Galois halkalarının direkt çarpımı şeklinde incelemek faydalı olacaktır.

Tüm bu bulgular neticesinde NTRU işlemlerine bir φ izomorfizma dönüşümü, gizli anahtar olarak mesaj polinomlarına etki edecek şekilde, gizliliği bir seviye daha artırmak amacıyla eklenebilir. Şöyle ki;

Teorem 6.1 $f \in Z_{p^k}[x]/(x^n-1), g \in Z_q[x]/(x^n-1)$ olmak üzere $h = f_q^{-1} \star g(mod\ q)$ açık anahtar olsun. $m \in Z_{p^k}[x]/(x^n-1)$ ve $r(x)$ hata polinomu keyfi seçilsin. $e \equiv p^k r \star f_q^{-1} \star g + \varphi(m)(mod\ q)$ olarak mesaj gizlenirse, yeni sistemin deşifreleme adımları doğru bir şekilde çalışıp açık metne ulaşılır.

İspat $e \equiv p^k r \star f_q^{-1} \star g + \varphi(m)(mod\ q)$ olarak gizlenmiş mesaj polinomuna ulaşmak için

$$e \star f \equiv p^k r \star g + f \star \varphi(m)(mod\ q)$$

$$\equiv f \star \varphi(m)(mod\ p^k) \text{ (uygun bir } k \text{ parametresi seçilsin).}$$

$$e \star f \star f_{p^k}^{-1} \equiv \varphi(m)(mod\ p^k)$$

$$e \equiv \varphi(m)(mod\ p^k) \quad (e \in Z_{p^k}[x]/(x^n - 1))$$

$$\varphi^{-1}(e) \equiv m(mod\ p^k)$$

olacak şekilde işlemler yapılır ve iddia ispatlanır. ⊠

Galois halkalarına taşınan NTRU sistemi için özel anahtar f polinomunun seçimini belirleyen bir teorem verelim.

Teorem 6.2 $p \geq 3$ asal sayı ve $n \in N$ olsun. Eğer $(f(x), p) = 1$ ise o zaman $f^p(x) \equiv 1\ (mod\ p^{n+1})$ olması için gerek ve yeter şart $f(x) \equiv 1(mod\ p^n)$ olmasıdır.

İspat ($\Leftarrow$) $f(x) \equiv 1(mod\ p^n)$ olsun. $p^n \mid f(x) - 1$ olur, hatta $p|f(x) - 1$ olur ki $f(x) \equiv 1(mod\ p)$ anlamına gelir. Böylece

$$f^{p-1}(x) + f^{p-2}(x) + \cdots + f(x) + 1 \equiv 1 + 1 + \cdots + 1 \equiv p \equiv 0(mod\ p)$$

olup, $p \mid f^{p-1}(x) + f^{p-2}(x) + \cdots + f(x) + 1$ demektir. Buradan

$$p^{n+1} \mid (f(x) - 1)(f^{p-1}(x) + f^{p-2}(x) + \cdots + f(x) + 1) = f^p(x) - 1$$

$$\Rightarrow f^p(x) \equiv 1(mod\ p^{n+1}).$$

($\Rightarrow$) n üzerinden tümevarımla yapalım. $n = 1$ için $f^p(x) \equiv 1(mod\ p^2)$ olduğunu varsayalım.

$$f^p(x) = f(x).f^{p-1}(x) = f(x).(1 + kp)1 + lp^2 \Rightarrow f(x) \equiv 1(mod\ p)$$

olur ve iddia gerçeklenir. Şimdi bir $n \in N$ için iddianın gerçeklendiğini kabul edelim. $f(x) \equiv 1\ (mod\ p^{n+2})$ olduğunu varsayalım. Hipotezden $f^p(x) \equiv 1(mod\ p^{n+1}) \Leftrightarrow f(x) \equiv 1(mod\ p^n)$ olacaktır. $f(x) = 1 + kp^n$ yazıp

$$f^p(x) = (1 + kp^n)^p = 1 + pkp^n + \sum_{j=2}^{p} \binom{p}{j} k^j p^{nj}$$

$$= 1 + pkp^n + lp^{2n+1} + k^p p^{np},$$

$p \mid \binom{p}{j}$ ve $2n + 1 \geq n + 2, np \geq n + 2 (p \geq 3)$ olacağından

$$1 \equiv f^p(x) \equiv 1 + kp^{n+1}(modp^{n+2})$$

$$p^{n+2} \mid (1 + kp^{n+1}) - 1 = kp^{n+1} \Rightarrow p \mid k.$$

$f(x) = 1 + kp^n$ olduğundan $f(x) \equiv 1(mod\ p^{n+1})$ olur ve tümevarımla ispat tamamlanır. ⊠

Teorem, asal cisimde terslenebilir bir polinom bulunduğunda, genişleme cisminde veya üst halkada kolay yoldan yeni bir özel anahtarın nasıl türetileceğini açıklaması bakımından önemlidir.

6.3.1. Özet ve sonuçlar

- Yapılan çalışmanın temel felsefesi literal olarak, $e \equiv p.h \star r + mmod\ q$ ifadesinin yine açık anahtar olmasından ötürü $mod\ p$ de ele alınırsa açık metnin saldırılara daha kolay maruz kalabileceği fikri üzerinedir. φ izomorfizmi teorem 6.1 de belirtildiği haliyle alınıp, şayet denklem $e \equiv p.h \star r + \varphi(m)mod\ q$ olarak şifreli metni üretirse, açıktır ki bir φ izomorfizmi bir açık metin m polinomunu başka bir polinoma dönüştüreceğinden yani $\varphi(m) \neq m$ olacağından güvenlik düzeyi açık metni korumak üzerine kesin sonuç verecektir.
- $Z_p[x]\ /\ (x^N - 1)$ halkası yerine $Z_{p^k}[x]\ /\ (x^N - 1)$ k ≥ 1 Galois halkaları seçilmesinin temel sebepleri, anahtar havuzunu büyütmek ve parametre seçimlerini kolay kılmak adına yapılmıştır. Ayrıca Galois halkaları tek maksimal ideali olan çok özel halka türleridir. Bu halkalarda maksimal idealin içinde unit (birimsel eleman) aranamayacağından M maksimal ideali göstermek koşulu ile $G \setminus M$ kümesinde özel anahtar f fonksiyonları aranabilir.
- Modülü oluşturan $x^N - 1$ polinomu halkada ne kadar indirgenebilirse o sayıda ideal oluşacağından terslenebilir (özel anahtar) polinom sayısı azalacaktır ki anahtar üretmek kolaylaşacak fakat gizli anahtara yapılan saldırılara maruz kalınacaktır.
- Z_p cismi yerine Z_{p^k} halkası alınması demek, hem daha geniş bir cebirsel yapıda hem de sıfır bölenlerin olduğu daha kompleks bir yapıda çalışmak manasına geleceğinden kriptolojinin asıl amacı olan gizlilik ve karmaşıklığa yardımcı olacağı açıktır.
- $(p, q) = 1$ açıkça $(p^k, q^k) = 1$ demek olacağından k güvenlik parametresi eski sistemi koruyup genelleyen, cismi halkaya dönüştüren bir sabittir. Tıpkı simetrik şifrelemeden asimetrik sistemlere geçişin ilk örneklerinden olan RSA kriptosisteminde olduğu gibi, büyük ve keyfi asalların herhangi kuvvetleri açıktır

ki halkanın üzerindeki kriptosistemin NP (polinom olmayan ya da üstel zamanda) kırılacak olması ihtimalini bile azaltmaktadır. Büyük kümede daha fazla işlem ve hesaplama yapılmasına olanak verecek bu sabit, güvenliği yükseltip, hızı düşürecektir.

- $\varphi: R \to R$ izomorfizminin NTRU kriptosistemine başka bir katkısı ise, NTRU latisinin

$$L_h = \{(f, g) \in R^2 : g = h \star f/p \ (mod\ q)\},$$

olduğu göz önüne alınırsa, $Boy(L_h) = 2N$ ve $Det(L_h) = q^N$ olduğundan, L_h latisinin matris gösterimi bir L güvenlik sabiti ilavesi ile

$$\begin{bmatrix} \alpha & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-2} & h_{N-1} \\ 0 & \alpha & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-3} & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \alpha & h_1 & h_2 & \cdots & h_{N-1} & h_0 \\ 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & q & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & q \end{bmatrix}$$

şeklindedir burada $h = (h_0, \dots, h_{N-1})$ açık anahtar polinomu latisin en önemli karakteristik özelliğidir. Latis indirgeme saldırılarına karşılık açık anahtara bir $\varphi: R \to R$ izomorfizması eklenerek, $\varphi(g) \equiv \varphi(h) \star \varphi(f/p)(mod\ q)$ ve $h \equiv f_q^{-1} \star g \star p(mod\ q)$ özdeşliklerinden h polinomunun değil de belirlenmiş bir φ izomorfizma dönüşümü yardımıyla, $\varphi(h)$ ın açık anahtar olarak yayınlanması neticesinde oluşan latis; $\varphi(H)$, $\varphi(h)$ polinomunun devirsel matrisi olmak üzere

$$\begin{pmatrix} I & \varphi(H) \\ 0 & qI \end{pmatrix}$$

şeklinde olacaktır. Açıktır ki bu latis daha kompleks formdadır. φ nin gizli anahtar olarak seçilmesi neticesinde düzenlenen saldırılar $\varphi(h)$ polinomunu ele verecek olsa dahi burada φ^{-1} bilinmediğinden asıl açık anahtar olan h polinomu ve H devirsel matrisi ele geçirilemeyecektir.

Seçilen terslenebilir f polinomunun kümesi, $Z_p[x] \,/\, (x^N - 1)$ yapılarak daha fazla sayıda özel anahtar üretimi amaçlanmıştır. Yine $f \star h = g$ ifadesindeki g ve f özel anahtar polinomlarının belirlenmiş bir k. kuvveti alınarak h açık anahtarı biraz daha kompleks hale getirilmiştir. $h = f_q^{-1} \star g$ yerine $h \star x^k = f_q^{-1} \star g \star x^k$ alınarak açık

anahtarın uygun bir k. rotasyonu seçilmiştir. $m = p^{\alpha}q^{\beta}$, $(p,q) = 1$ şeklindeki bir $m \in Z$ için $Z_m \cong Z_{p^{\alpha}} \times Z_{q^{\beta}}$ olacağından bir φ homomorfizması

$$\varphi: Z_m \to Z_{p^{\alpha}} \times Z_{q^{\beta}}$$

$$\varphi(f) = (f mod\ p^{\alpha}, f mod\ q^{\beta})$$

şeklinde tanımlanıp seçilen mesaj polinomuna uygulanmıştır. φ izomorfizmasının tersi gizli anahtarlar setine eklenmiştir. m mesaj polinomları $Z_p[x]\ /\ (x^n - 1)$ yerine $Z_{p^k}[x]\ /\ (x^n - 1)$ halkasından alınarak daha fazla gizlenebilir polinom kümesi elde edilmiştir. Klasik NTRU sisteminin Z_p ve Z_q cisimlerinde yapılan işlemlerin Z_{p^k} ve Z_{q^r} Galois halkalarında yapılması önerilmiştir. $\alpha \to \infty$ için $p^{\alpha} \to \infty$ ve $m \to \infty$ olacağından açık anahtarlardan p ve q modüllerinin istenildiği kadar büyük seçilebileceği öngörülmüştür.

Tablo 6.1. Önerilen NTRU şeması.

Eski		Yeni	
Açık anahtar	Gizli anahtar	Açık anahtar	Gizli anahtar
p, q, h, N	f, f_p^{-1}, g	p^k, q^t, h, N	$f, f_{p^k}^{-1}$
$p = 3$	$f = 1 + pF$	$p = 3^{37}$	g, x^k, φ^{-1}
$q = 59$		$q = 59^{23}$	$f = 88 + pF$
$N = 11$		$N = 113$	$g \to g^k$
$h = f_q^{-1} \star g$		$h = f_{q^t}^{-1} \star g^k$	

6.4. NTRU' ya İki Anahtar Eklenmesi İle Yeni Bir Yaklaşım

P ve Q mertebesi N' yi geçmeyen aralarında asal iki polinom olsun. İlave olarak P ve Q indirgenemez ve $Z_{p^k}[x]\ /\ (x^N - 1)$ den seçilsin. Klasik NTRU işlemlerindeki

$$e \equiv p.h \star g + m(mod\ q) \qquad (26)$$

denklemine, P polinomu özel anahtar ve Q polinomu da polinom modülü ve açık anahtar olarak $(Q,q) = (P,q) = (Q,p) = 1$ şartları altında şu şekilde eklensin;

$$e' \equiv [p.h \star g + P \star m(mod\ q)] mod\ Q \qquad (27)$$

Bu işlemlerde $P^{-1} mod\ p = P^{-1} mod\ q = 1$ seçilmesinin ilave şart olarak verilmesi, sistemin zorluk derecesini artıracak opsiyonel bir seçim olacağını vurgulayalım. $h = f \star g \star P$ polinomu açık anahtar olarak, (f, g, P) sistemi ise gizli anahtar olarak sisteme eklenir. Bu kısımda NTRU kriptosistemini polinom idealleri modül olarak eklenecektir. Sistem cebirsel olarak çok daha güçlü bir forma getirilecektir.

6.4.1. Deşifreleme safhası

Durum 1: $P \star m(mod\ q)$ polinomunun derecesinin Q modül polinomunun derecesinden küçük olması;

Durum 1 de işlem hızı ve hesaplama kolaylığı amacıyla, küçük dereceli polinomların seçilmesi ihtimali anlatılacaktır.

$P \star m(mod\ q)$ polinomunun $mod\ p$ ye göre katsayılarının değişmeyeceği varsayılıp, (27) denkleminde önce $mod\ p$ hesaplaması yapılırsa denklem,

$$e'' \equiv [P \star m(mod\ p)] mod\ Q \qquad (28)$$

halini alır. $(P, Q) = 1$ ve indirgenmez seçildiğinden (bu indirgenmezlik şartı P bin bazı çarpanlarının mesajın içine karışmaması gerektiğindendir) P nin $mod\ Q$ da tersi mevcuttur. Buna P^{-1} denir ve (28) denklemi P^{-1} ile çarpılırsa,

$$P^{-1} \star e''' \equiv [P \star P^{-1} \star m(mod\ p)] mod\ Q \qquad (29)$$

haline gelir ki, NTRU işlemlerinde mesaj polinomunun $mod\ p$ den etkilenmeyeceği varsayılır. Buradan hareketle (29) denklemi

$$P^{-1} \star e''' \equiv m\ mod\ Q \qquad (30)$$

olur. $P^{-1}\ mod\ p = P^{-1}\ mod\ q = 1$ seçimi altında (şart değil), (30) denklemi $e''' \equiv m\ mod\ Q$ olur. Şayet, şifrelenmek istenen m mesaj polinomunun derecesi Q polinomunun derecesinden küçük seçilmişse (30) ifadesi eşitlik haline gelir ve

$$e''' = m \tag{31}$$

olup deşifreleme safhası bitmiştir denir.

Durum 2: $P \star m(mod\ q)$ polinomunun derecesi güvenlik düzeyi sebebiyle Q polinomunun derecesinden büyük seçilmiştir. Bu durumda şifreli metin

$$e \equiv [p.h \star r + [P\ mod\ Q] \star m] mod\ q$$

şeklinde hesaplanarak gönderilir. (30) denkleminde şayet şifrelenmek istenen mesaj polinomunun da derecesi Q polinomunun derecesinden büyük seçilmiş ise aşağıda detaylı anlatılacak bir yöntem önerilmiştir.

$m \in Z_{p^k}[x] \,/\, (x^N - 1)$ mesaj polinomu, $m = a_0 + a_1x + \cdots + a_sx^s$ ve $Q = b_0 + b_1x + \cdots + b_tx^t$ olsun. $s > t$ olduğundan $s = d.t + r,\ 0 \le r < t$ olacak şekilde d, r vardır. $Z_{p^k}[x] \,/\, (x^N - 1)$, Z_{p^k} üzerinde bir modüldür. Bu modüle M diyelim. $M_1 = \{a_0 + a_1x + \cdots + a_{t-1}x^{t-1} \,|a_i \in Z_{p^k}\}$ olsun. M_1 de Z_{p^k} üzerinde modüldür.

Benzer şekilde $M_2 = \{a_tx^t + a_{t+1}x^{t+1} + \cdots + a_{2t-1}x^{2t-1} | a_i \in Z_{p^k}\}$ de modül olur. Bu iki modül üzerinde bir dış direkt toplamı, $m_1 \in M_1$ ve $m_2 \in M_2$ olmak üzere ve ayrıca $m_1 = (a_0, a_1, \cdots, a_{t-1}), m_2 = (a_t, a_{t+1}, \cdots, a_{2t-1})$ için

$$\oplus : (m_1, m_2) \mapsto (m_1 m_2)$$

şeklinde tanımlansın, yani $\oplus$ işlemi $m_1 \in M_1$ ve $m_2 \in M_2$ yi işleme aldığında yan yana yazıyor olsun. Benzer düşüncelerle, $m_{d+1} = \{a_{s-r}x^{s-r} + \cdots + a_sx^s | a_i \in Z_{p^k}\}$ olmak üzere $M \cong M_1 \oplus M_2 \oplus \ldots \oplus M_{d+1}$ olur ki mesaj polinomunun kümesine modüllerin direkt toplamı olarak bakılabilir. Böylece, $m = [a_0 + a_1x + \cdots + a_{t-1}x^{t-1}] \oplus [a_tx^t + a_{t+1}x^{t+1} + \cdots + a_{2t-1}x^{2t-1}] \oplus \ldots \oplus a_sx^s$ mesaj polinomu d tane t katsayılı polinoma ayrılır. Son kalan r tane katsayılı polinom olduğu gibi bırakılıp şimdilik rezidü olarak kabul edilir. m/Q fonksiyonunu bulmak için

$$\frac{\overbrace{[a_0 + a_1x + \cdots + a_{t-1}x^{t-1}]}^{1}}{Q} \oplus \frac{\overbrace{[a_tx^t + a_{t+1}x^{t+1} + \cdots + a_{2t-1}x^{2t-1}]}^{2}}{Q}$$

$$\oplus \ldots \oplus \frac{\overbrace{[a_{s-r}x^{s-r} + \cdots + a_sx^s]}^{d+1}}{q}$$

bölme işlemleri ayrı ayrı ele alınır. Toplamda $d+1$ adım sonunda işlem bitirilecektir. 1 nolu polinom $mod\ Q$ da yazılmıştır, olduğu gibi bırakılır. 2 nolu polinom x^{N-t} ile çarpılır. $x^{N-t}.x^t = x^N = 1$ olacağından 2 nolu polinomun derecesi $t-1$ olarak indirgenmiş olur ki $mod\ Q$ da yazılmıştır. Matematiksel olarak,

$$\frac{x^{N-t}.[a_t x^t + a_{t+1}x^{t+1} + \cdots + a_{2t-1}x^{2t-1}]}{x^{N-t}.Q} = \frac{[a_t + a_{t+1}x + \cdots + a_{2t-1}x^{t-1}]}{x^{N-t}.Q}$$

$$\equiv a_t + a_{t+1}x + \cdots + a_{2t-1}x^{t-1}\ (mod\ Q).$$

Yani, 2 nolu polinom x^{N-t} ile çarpılarak derecesi indirgenip $mod\ Q$ dan etkilenmeyecek forma sokulur. Bu safhada N yeterince büyük seçilerek x^{N-t} ile çarpımlarda Q polinomunun derece kaybı önlenmelidir yani $der(x^{N-t}.Q) > derQ$ olmalıdır. Benzer düşüncelerle devam edilip uygun bir $x^{N-z.t}$ çarpımları ile bütün parantez içi polinomlar $mod\ Q$ ya göre indirgenir. $d+1$ adım sonunda parçalara ayrılarak gönderilmiş mesaj metninin parçaları birleştirilirse;

$$m \equiv [a_0 + a_1 x + \cdots + a_{t-1}x^{t-1}] \oplus [a_t x^t + a_{t+1}x^{t+1} + \cdots + a_{2t-1}x^{2t-1}]$$

$$\oplus \ldots \oplus [a_{s-r} + a_{s-r+1}x \cdots + a_s x^r] mod\ Q$$

olur ve parantez içleri yan yana yazılıp birleştirilerek mesaj polinomu olan m elde edilir.Mesaj polinomları modülünden kod sözcüklerine uygun bir θ dönüşümü, $\theta: m = [a_0, a_1, \ldots, a_t, \ldots, a_s] \mapsto (a_0 a_1 a_2 \ldots a_s)$ şeklinde tanımlanırsa her polinoma bir kod sözcüğü gibi bakılır.

Ayrıca Durum 2 deki denklem

$$e \equiv [p.h \star r + [P\ mod\ Q] \star m] mod q$$

haline getirilirse $(P, Q) = 1$ olduğundan, $derP > derQ$ olsa bile P nin Q ya göre rezidüsü olan P' polinomu da Q ile aralarında asal olup tersi mevcuttur. Sistemin kullanıcısı, bu anahtarı da kolaylıkla elde edebilecektir. Ya da kolaylık açısından $derP < derQ$ şartı altında ve Q ile bölme işleminin yapılamaması neticesinde algoritma hızı artacaktır. Üstelik bu durumda sisteme sadece $(P, q) = 1$ şartı konması gerektiğinden P polinomu olarak bir önceki gizli anahtar olan f bile seçilebilir.

Aşağıdaki önerme, lemma ve teoremler önerilen sistemin parametreler seçimine yardımcı olacak niteliktedir. Bütün teorem, lemma, ifade ve ispatlarda Q modül polinomu, $R = Z_{p^k}[x] \,/\, (x^N - 1)$ halkasında temel indirgenemez seçilmiştir.

Lemma 6.2 Herhangi iki M_i modülü birbirine izomorftur. $0 \leq i, j \leq d$ olmak üzere $M_i \cong M_j$ olur.

İspat m_i, b_i M_i modülünde iki eleman olsun. Bir μ_t dönüşümü

$$\mu_t : M_i \to M_j$$

$$\mu_t(m_i) = x^{N-(i-1)t} \star m_i$$

şeklinde tanımlansın. μ_t bir homomorfizmadır. Çünkü

$$\mu_t(m_i + b_i) = x^{N-(i-1)t} \star (m_i + b_i)$$

$$= x^{N-(i-1)t} \star m_i + x^{N-(i-1)t} \star b_i$$

$$= \mu_t(m_i) + \mu_t(b_i).$$

Ayrıca μ_t 1-1 dir, zira

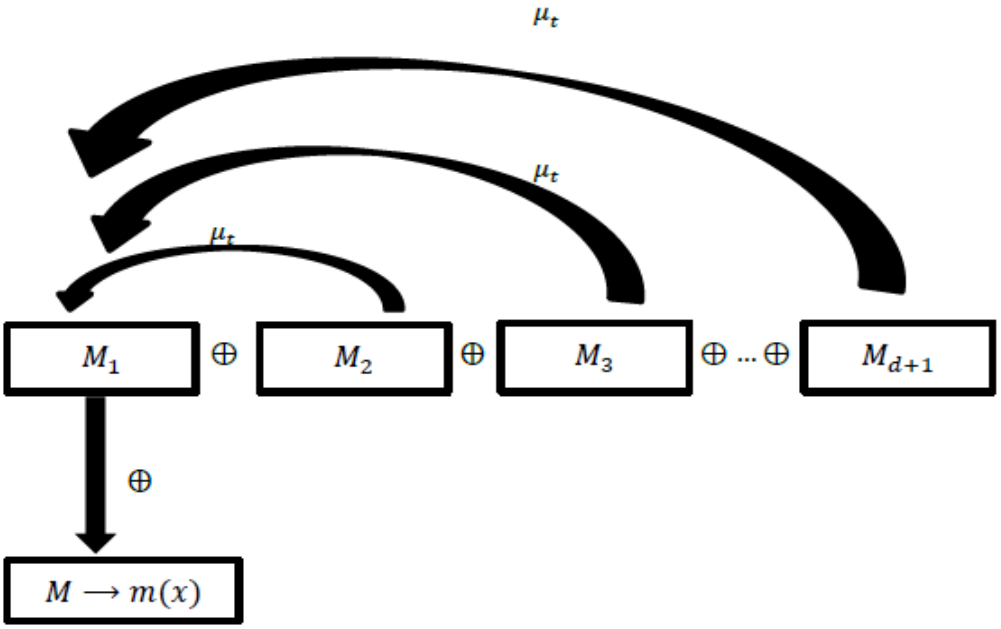
$\mu_t(m_i) = \mu_t(b_i)$ denirse

$x^{N-(i-1)t} \star m_i = x^{N-(i-1)t} \star b_i$ olup her iki yan $x^{(i-1)t}$ ile çarpılarak;

$$x^N \star m_i = x^N \star b_i$$

$$m_i = b_i$$

olarak elde edilir ki ispat biter. Rezidü modülü hariç kalmak üzere diğer bütün modüllerin birbirine izomorf olduğunu gösteren bu μ_t dönüşümüne, NTRU şifreleme safhasında mesaj polinomuna uygulanarak özel anahtar rolü verilecektir. Şimdi bu bahsedilen algoritmik deşifreleme safhalarını anlatan bir şekil verilecektir.



Şekil 6.1. Bütün mesajların ilk modüldeki izomorfik kopyalarının alınmasına dair şekil.

Tüm bu yeni modül önerilerini şekil yardımıyla açıklamak neticesinde yeni NTRU açık-gizli anahtarlarını karşılaştıran bir tablo verilsin.

Tablo 6.2. Yeni parametrelerin karşılaştırılması.

Eski NTRU		Yeni NTRU	
Açık	Gizli	Açık	Gizli
p, q, h	f_q, f_q^{-1}, g	$p^k, p^t, h, Q,$ $t, \oplus$	$f_q, f_q^{-1}, g,$ P, μ_t

Şimdi de açık metin kümesindeki her elemanın (sözcük) şifrelenebilir olmayacağını gösteren bir lemma verilsin.

Lemma 6.3 $Z_{p^k}[x]/(x^N - 1)$ halkasında şifrelenebilir mesaj polinomları kümesi

$Z_{p^k}[x]/(x^N - 1) \setminus (Q)$ dir.

İspat $Q \in Z_{p^k}[x]/(x^N - 1)$ olan indirgenemez bir polinom olup $Z_{p^k}[x]/(Q)$ halkasının modülü olacağından ve bir $S(x) \in Z_{p^k}[x]/(x^N - 1)$ için $S.Q \in (Q)$ olur ki bu da $S.Q \equiv 0 mod\ Q$ olacağından (Q) kümesindeki her mesaj çözüm olacaktır. Buradan, $(S, Q) = 1$ olmalıdır ki mesaj anlamlı olabilsin, bu da Q indirgenemez seçildiğinde $\forall S \in Z_{p^k}[x]/(x^N - 1)$ ve $S \notin (Q)$ için $(S, Q) = 1$ olacağından, şifrelemek istenen mesaj polinomları $Z_{p^k}[x]/(x^N - 1) \setminus (Q)$ kümesinden seçilmelidir demektir. ⊠

Lemma 6.4 $Z_{p^k}[x]/(Q)$ halkasındaki tüm elemanlar mesajlanabilir (şifrelenebilir)

elemanlardır.

İspat $Z_{p^k}[x]/(Q)$ halkasındaki her elemanın mertebesi Q dan küçük ve Q indirgenemez seçildiğinden $(Q) = \{0\}$ dan ibaret kalır. Diğer bir $S \in Z_{p^k}[x]/(Q)$ için $(S, Q) = 1$ olacağından tersi mevcuttur ve $mod\ Q$ da çözülebilirdir. 0 elemanı ile hiç mesaj göndermemeyi belirtelim. $Z_{p^k}[x]/(Q)$ halkasındaki her eleman mesaj polinomu olarak ele alınıp $mod\ Q$ da bir bölme işlemi yapmada dahi açığa çıkacaktır. ⊠

Şimdi, NTRU şifrelemesinde önemli bir yer tutan katsayıları toplamı "0" olan polinomlar ile ilgili bir lemma verilsin.

Lemma 6.5 $I = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1} | \sum a_i = 0, a_i \in Z_P\}$ kümesi $Z_p[x]/(x^N - 1)$ de bir ideal belirtir ve eğer $(f) = I$ olacak şekilde I idealinin bir f üreteci varsa bir $m \in I$ mesaj polinomu için $m\ mod\ Q$ ifadesi, $derQ \geq 2$ ve $m = f.s, s \in I$ olmak üzere $s\ mod\ Q$ ifadesine indirgenir.

İspat $0 \in I$ olduğundan $I \neq \emptyset$ dir. I nın bir ideal belirttiği açıktır. Şimdi üreteç polinomu olan f yi belirleyelim. $x - 1 \in I$ olup şayet $(f) = I$ ise $x - 1 = f.g$ olacak şekilde bir $g \in Z_p[x]/(x^N - 1)$ vardır. $x - 1$ polinomunun derecesi 1 olduğundan f nin derecesi 1 ya da 0 olacaktır. f nin derecesi 0 ise $f = f_0$ olup $f \in I$ olacağından $f_0 = 0$ olur ki 0 üreteç olamaz. f nin derecesi 1 ise f aslında $x - 1$ tarafından da üretilebilir. Yani $(x - 1) = (f)$ olur ki $(x - 1) = I$ olduğu ispatlanır. Mesaj polinomu $m \in I$ olacak şekilde alınırsa

$$m\ mod\ Q \equiv f.b mod\ Q, (m = f.b \in Z_p[x]/(x^N - 1))$$

$$\equiv (f mod\ Q.b mod\ Q) mod\ Q$$

$$\equiv \big(f.(b\ mod\ Q)\big) mod\ Q$$

olur ki sadece $b\ mod\ Q$ ifadesini bulmak yeterli olacaktır. ⊠

Lemma 6.6 P ve Q indirgenemez, aralarında asal ve $derP < derQ$ kabul edelim. $m\ mod\ Q$ ifadesi, bir $S \in Z_{p^k}[x]/(x^N - 1)$ olmak üzere $P.S(mod\ Q)$ ifadesine indirgenir.

İspat $(P, Q) = 1$ olduğundan $(P, Q) = Z_{p^k}[x]/(x^N - 1)$ olur. Bir $m \in Z_{p^k}[x]/(x^N - 1)$ mesaj polinomu keyfi seçilsin.

$$m = P.S + Q.bS, b \in Z_{p^k}[x]/(x^N - 1)$$

$$m\ mod\ Q \equiv (P.S + Q.b) mod\ Q$$

$$\equiv (P.S) mod\ Q$$

$$\equiv (P.(Smod\ Q)) mod\ Q$$

olur ki ispat biter. Örneğin, S polinomunun sabit olarak belirlendiği m mesajları direkt olarak $P.S$ şeklinde deşifre edilir. P ve Q parametrelerine göre katsayı olarak ele alabileceğimiz S polinomunun seçimi algoritmayı hızlandırıp yavaşlatabilecektir.

Lemma 6.7 m; $Z_{p^k}[x]/(p, Q)$ de bir mesaj polinomu, $(\alpha) = Z_{p^k}[x]/(p, Q)$ üreteç polinomu ise, $m\ mod\ Q$ ifadesi yerine $\alpha\ mod\ Q$ ifadesi hesaplanır.

İspat $Z_{p^k}[x]/(p, Q)$ bir cisim olduğundan ve her cismin çarpımsal grubu devirli olduğundan $\exists \alpha \in Z_{p^k}[x]/(p, Q)$ vardır öyle ki $(\alpha) = Z_{p^k}[x]/(p, Q)$ olur. Q polinomunun derecesi geneli bozmamak kaydıyla n seçilirse $|\alpha| = p^n - 1$ olur. Belirlenen her m mesaj polinomu için $m = \alpha^t$ olacak şekilde $0 \leq t \leq p^n - 1$ vardır. O halde deşifreleme safhasında;

$$m\ mod\ Q \equiv \alpha^t mod\ Q$$

$$\equiv [\alpha\ mod\ Q]^t$$

olur ki seçilen Q modül polinomu ile α üreteç polinomunun mertebelerinin birbirine eşit ya da yakın seçilmesi durumunda algoritma hızlanacaktır.

Teorem 6.3 $R = Z_{p^k}[x]/(x^N - 1)$ ve P, R nin bir asal ideali olmak üzere şayet bir $P \subseteq \langle a \rangle$, $a \notin P$ ve $ap_i \neq 0$, $p_i \in P$ olacak şekilde bir $a \in R$ varsa P nin bütün elemanlarının şifrelenmesi için yalnız bir elemanın şifrelenmesi yeterli olacaktır.

İ$spat$ $p \in P$ keyfi alınsın. $p \in \langle a \rangle$ olacağından, $p = ab$ olacak şekilde $b \in R$ vardır. P asal olduğundan $a \in P$ veya $b \in P$ olmalıdır ki $a \notin P$ alındığından $b \in P$ olur ki bu da $P \subset aP$ demektir. P ideal olduğundan $aP \subset P$ zaten sağlanır. Böylece $P = aP$ olur. P sonlu olduğundan aP kümesi P nin bir rotasyonudur. Yani

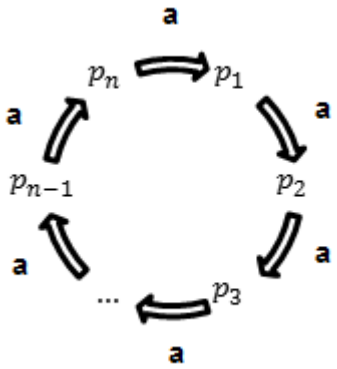
$$ap_1 = p_2$$

$$ap_2 = p_3$$

$$\vdots$$

$$ap_{n-1} = p_n$$

$$ap_n = p_1.$$



Şekil 6.2. İdealin üreteç elamanının şifrelenmesinin yetereli olacağını ifade eden şekil.

Şekil 6.2 de de açıkça görüldüğü üzere aP, P nin elemanlarının bir permütasyonudur. Bir $m \in P$ mesaj polinomunu şifrelemek için $m = p_i$ dersek ve $p_i = ap_{i-1}$, $p_{i-1} = ap_{i-2}$, …, $p_2 = ap_1$ olduğundan hareketle sadece p_1 etiketli elemanın şifrelenmesi yeterli olacaktır. Önerilen NTRU algoritmasındaki modül Q olmak kaydıyla;

$$p_2 \equiv ap_1 \; mod \; Q \equiv amodQ \; p_1 modQ$$

$$p_3 \equiv ap_2 \; mod \; Q \equiv amodQ \; p_2 mod \; Q \equiv a^2 modQ \; p_1 modQ$$

$$\vdots$$

$$p_n \equiv ap_{n-1}\, mod\ Q \equiv amodQ.p_{n-1}mod\ Q \equiv \cdots \equiv a^{n-1}modQ\ p_1 modQ$$

olur ki ispat tamamlanır. ⊠

Şimdi de bu yeni NTRU şifreleme yöntemi için bir P gizli anahtarı bulunduğunda bir yenisini P yardımıyla bulmaya yardımcı bir lemma verelim.

Lemma 6.8 $R = Z_{p^k}[x]/(x^N - 1)$ halkasından seçilen Q modül polinomu ve $(P, Q) = 1$ olan P gizli anahtar polinomu belirlenmiş olsun. Bir $t \in (Q) \subset R$ için $P - t$ polinomu da bir yeni gizli anahtardır.

İspat $(Q) \subset R$ ideali $Z_{p^k}[x]/(Q)$ da sıfır idealine dönüşür. Yani $\forall t \in (Q)$ nilpotenttir. Nilpotent elemanlar bir ideal oluşturduğundan ve bir idealde birim eleman olamayacağından bir $P \in R$ terslenebilir polinomu için $P - t$ de R de terslenebilirdir. Böylece belirli bir Q modül polinomu için birden çok gizli anahtar P elde edilebilir. ⊠

Teorem 6.4 $R = Z_{p^k}[x]/(Q)$ Galois halkasında $m = (P)$ maksimal ideal ve $R/(m)$ rezidü cismi olmak üzere şifrelenmek istenen mesaj polinomları $R/(m)[x]$ den seçilmiştir.

İspat R nin sıfır bölenlerinin kümesi (m) idealidir. Terslenebilir elemanları ise $U = R/(m)$ kümesidir. Bir t polinomu şayet $t = P^r u(x)$ şeklinde ise n, (m) idealinin nilpotentlik indeksi olmak kaydıyla $t' = P^r v(x)$ polinomu t polinomunun sıfır bölenidir. NTRU deşifreleme safhasında $t\ mod\ Q = P^r u(x) mod\ Q = 0\ mod\ p$ olacağından sıfır bölen kümesi içinden mesaj seçilemez. Bu sebeple tüm kodlanmak istenen mesaj polinomları $R/(m)[x]$ den alınmalıdır. ⊠

Teorem 6.5 $R = Z_{p^k}[x]/(Q)$ Galois halkasında (P) maksimal idealinin nilpotentlik mertebesi k olmak üzere gizli anahtar olarak seçilmek istenilen P polinomlarının sayısı en az k tanedir.

İspat $(P^k) = 0$ ve $(P^{k-1}) \neq \{0\}$ olacağından

$$\{0\} \subset (P^{k-1}) \subset (P^{k-2}) \subset \cdots \subset (P) \subset R$$

R deki ideal zinciridir. $\forall 0 < j \leq k$ için P^j nin P^{j-1} de en az iki koseti olacağından

$$|(P)| \geq 2^{k-1}$$

olacaktır. $1+(P)$ terslenebilir elemanlar olacağından en az $|(P)|$ kadar R de birimsel eleman bulunabilir. Buradan

$$|U(R)| \geq |(P)| \geq 2^{k-1} \geq k$$

olur ki bu da k sayısının büyük seçimleri gizli anahtar üretmeyi kolaylaştırır.

Teorem 6.6

- **i.** (P), $Z_{p^k}[x]$ nın bir asal ideali olarak verilsin. $(P)[x]+(x)$ de $Z_{p^k}[x]$ de bir asal idealdir.
- **ii.** Bir $m(x) \in Z_{p^k}[x] \,/\, ((P)[x]+(x))$ mesaj polinomunu NTRU da şifrelemek yerine $m \in Z_p$ karşılık gelen m sayısını şifrelemek yeterli olacaktır.

İspat

- **i.** Bir φ homomorfizmasını
$$\varphi: Z_{p^k}[x] \longrightarrow Z_{p^k}[x]/p, \qquad \varphi(f) = f(a)+(P)$$
şeklinde tanımlayalım. Açıktır ki $(P)[x]$ ve (x) $çekφ$ dedir. $çekφ$ althalka olduğundan $(P)[x]+(x)$ ideali de $çekφ$ dedir. φ örten olduğundan
$$Z_{p^k}[x]/((P)[x]+(x)) \cong Z_p$$
olur ki $(P)[x]+(x)$ asal ideal olur.
- **ii.** Şayet bir $m(x)$ mesaj polinomu şifrelenmek isteniyorsa **(i)** den bir izomorfik kopya olan m' rakamı Z_p den seçilip
$$e \equiv pf_q^{-1} \star h + m mod\ q$$
ifadesindeki her değişken polinomlar yerine rakamlarla temsil edilip işlemler $Z_{p^k}[x]$ yerine Z_p de yapılacağından ve Z_p cisim olduğundan NTRU şifreleme algoritmalarının hızlı ve kolay (ekonomik) uygulanması için bir asal ideal elde edilip bu asal ideal yardımıyla da bir cisim inşa edilirse bu yöntem etkin olarak kullanılabilecektir.

Şimdi ise bir sıfır bölen yardımıyla sisteme özel anahtar üreten bir lemma verelim.

Lemma 6.9 $R = Z_{p^k}[x]/(Q)$ Galois halkasında M maksimal ideal olmak üzere $m \in M$, $s \in R$ için

- **i.** $ms-1$ birimseldir.
- **ii.** $ms-1$ NTRU için özel anahtardır.

iii. $m \notin M$ ise $ms - 1$ özel anahtar olamaz.

İspat

i. $m \in M, s \in R$ ve $ms - 1$ birimsel olmasın. O halde $(ms - 1)$ ideali M nin öz alt idealidir. Bu ise $1 \in M$ demektir ki $M \supset R$ olmasını gerektirir. $M \subset R$ olduğundan bu mümkün değildir. O halde $ms - 1$ birimsel (terslenebilir) dir.

ii. Bir $t \in R$ mesaj polinomu için

$$P.tmod\ Q \equiv (ms - 1)tmod\ Q \equiv mstmod\ Q - tmod\ Q.$$

$m\ mod\ p = 0$ olacağından ve $Pmodp = 1$ seçildiğinden $P.tmodp\ mod\ Q = t\ mod\ Q$ olur.

iii. Şimdi $m \notin M$ seçilsin. M maksimal olduğundan $(m, M) = R$ olması gerekir. Bu ise $\exists s \in R$ ve $k \in M$ için $ms + k = 1$ olarak yazılabilir demektir. Buradan hareketle $ms - 1 = -k \in M$ olur ki $ms - 1$ birimsel olamaz. Bu ise maksimal idealin içinden seçilmeyen bir m polinomu yardımıyla $ms - 1$ şeklinde bir özel anahtar üretmenin mümkün olması demektir. ⊠

Lemma 6.10 Lemma 6.9 nin şartları altında $ms - 1$ in mesaj polinomu olarak kodlanabilmesi için gerek ve yeter şart $m \in M$ olmasıdır.

İspat $m \notin M$ iken $ms - 1$ sıfır bölen olur. $ms - 1mod\ Q$ ifadesi $mod\ p$ de sıfırlanacaktır. Keza şifre çözülemeyecektir. Bu ise R halkasında $ms - 1$ şeklindeki mesajların iletilemeyeceği anlamına gelir. ⊠

6.4.2. Çalışmanın özeti

NTRU kriptoloji sisteminde açık anahtar olan p ve q asal sayılarının modül olarak alınıp işlendiği makale sayısı oldukça fazladır. Bu çalışmada ise p ve q asal sayı modüllerinin yanı sıra P ve Q gibi iki polinom modülünün de sisteme eklenmesi ile etkileri incelendi. Q polinomu açık anahtar, P polinomu gizli anahtar olarak seçilip sistemin parametreleri ve güvenlik düzeyi daha da arttırıldı. Mesaj polinomları kümesine modül olarak bakılıp, modüllerin dış direkt toplam özelliklerinden de faydalanılarak sisteme yeni bir işlem ($\oplus$) eklenmiştir. Tüm bu adımların sistemin hızını olumsuz etkileyeceği fakat güvenlik kısmını güçlendirdiği açıktır. Şayet şifrelemek istenen m mesaj polinomunun derecesi, seçilen Q modül polinomunun derecesinden küçük ise bölme ve modül direkt toplam işlemleri yapılamayacağından sistem daha hızlı çalışacaktır. Bu sebeple hız düzeyi veya güvenlik seviyesi şifreleyicinin tercihine bırakılmıştır. Bu bölümde $f \in L_f$, $g \in L_g$ ve $P \in R$ olmak

üzere f ve g nin klasik NTRU sistemindekinin aksine terslenmesi gerekmeyen, bunlara karşılık sadece $(P, Q) = 1$ şartını sağlayan bir $P \in R$ nin bulunması gerekliliği sistemi parametre bulma konusunda esnekliğe kavuşturmuştur. $h = f \star g \star P$ polinomu açık anahtar olarak şifrelemede kullanılmıştır. m mesaj polinomu Pm şeklinde bir adım daha gizlenerek şifrelenmektedir. Deşifrelemenin son adımında $mmodQ$ ifadesi m nin Q ya bölünmesi gereken durumları ele almıştır. (h, Q) açık anahtar, (f, g, P) ise gizli anahtar olmak üzere sistemin açık veya gizli anahtarları artırılarak sistemin güvenlik düzeyi yükseltilmiştir.

7. NTRU KRİPTOSİSTEMİNİN BAZI GENELLEMELERİ VE ELDE EDİLEBİLECEK DİJİTAL İMZALAR

7.1. Yeni Sistemin Parametreler Seçimi

Önerilen genelleştirilmiş sistem birçok parametreyi aslına uygun olarak kullanmaktadır. Yani p ve q asallarının seçimleri, N sayısının seçimi, f, g, r polinomlarının seçimi vb. klasik NTRU sistemindeki gibi olacaktır. Tek farkla ki farklı açık anahtar üretimi için farklı f, g ve r polinomları seçilecektir.

7.2. Yeni Sistemde Kullanılacak Notasyonlar

Yine tüm klasik NTRU notasyonlarına bağlı kalınıp aynı şartlar ve seçimler altında aynı gösterimler kullanılacaktır. Bir tek; $f_{(n)}^{*}$, $f_{(n,j)}^{*}$ ve $f_{(n)}^{-1}$ şeklinde üç notasyonun tanıtılmasında fayda olacaktır. $f_{(n)}^{*} = f_1 \star f_2 \star \ldots \star f_n$ olacak şekildeki n tane seçilmiş tüm gizli anahtarlarının konvolüsyon çarpımından oluşur. $f_{(n,j)}^{*} = f_1 \star f_2 \star \ldots \star f_{j-1} \star f_{j+1} \star \ldots \star f_n$ ise j numaralı gizli anahtar hariç tümünün konvolüsyon çarpımından oluşmaktadır. $f_{(n)}^{-1}$ ise n tane birimsel f gizli anahtarlarının çarpımının $mod\ p$ deki tersini göstersin.

7.3. Toplamsal Genelleme Sistemi Nasıl Çalışır?

Bu genelleştirilmiş sistem bir mesajı önce n tane farklı açık anahtar ve n tane farklı hata polinomu seçerek farklı şekilde ön şifreler. Oluşan bu ön şifreli metinler toplamını ise son şifreli metin olmak üzere gönderir. n sayısını hem p hem de q ile sırasıyla aralarında asal olma zorunluluğu vardır. Fakat n sayısının modül olan p ve q sayılarından büyük ve küçük olması gibi iki farklı durum söz konusu olacaktır. Buradan hareketle bu sistemin güvenlik parametresi olarak görev yapacağından eski klasik sistem NTRU ya yeni bir parametre eklenmesine yol açacaktır.

Şimdi $n < p$, $n < q$ ve $(n, p) = 1$, $(n, q) = 1$ olan durumda sistemin nasıl çalışacağını gösterelim. Bu sistemi önce $Z_p[x]/(x^N - 1)$ ve $Z_q[x]/(x^N - 1)$ gibi klasik NTRU halkalarında ele alalım. Daha sonra halka yerine cisim alınıp tekrar incelenecektir. Bu kısımda NTRU kriptosistemi üç farklı genelleme haline getirilmiştir. Kriptosistemin RSA kripto sistemine nazaran çok daha güçlü olduğu gösterilmiştir.

Lemma 7.1 Bir m mesaj polinomunun $h_i = f_{iq}^{-1} \star g_i$ ve r_i, $1 \leq i \leq n$ açık anahtar ve

hata polinomu seçimleriyle n defa NTRU kriptosisteminin klasik yöntemine göre şifrelenip daha sonra oluşan $e_i, 1 \leq i \leq n$ şifreli metinlerin toplamının gönderilmesi halinde açık metin m ye yine ulaşılabilecektir.

İspat m mesajlarının şifrelenmiş halleri açıkça ve alt alta yazılıp toplanırsa,

$$e_1 \equiv ph_1 \star r_1 + m(mod\ q)$$

$$e_2 \equiv ph_2 \star r_2 + m(mod\ q)$$

$$\vdots \qquad\qquad \vdots$$

$$\underline{+e_n \equiv ph_n \star r_n + m(mod\ q)}$$

$$e_1 + e_2 + \cdots + e_n \equiv p[(h_1 \star r_1) + (h_2 \star r_2) + \cdots + (h_n \star r_n)] + nm(mod\ q) \qquad (32)$$

şekline gelir. Şimdi her bir f_i, $1 \leq i \leq n$ birimsel polinomlarının çarpımını (32) denklemine uygulayarak,

$$f^*_{(n)}(e_1 + e_2 + \cdots + e_n) \equiv p[(f^*_{(n,1)} \star g_1 \star r_1) + (f^*_{(n,2)} \star g_2 \star r_2) + \cdots +$$

$$(f^*_{(n,n)} \star g_n \star r_n)] + f^*_{(n)} \star nm(mod\ q). \qquad (33)$$

olur.(33) numaralı ifadede $f^*_{(n)}$, terslenebilir f gizli anahtarların çarpımından oluştuğu ve bu çarpımın da terslenebilir oluşundan hareketle, denklemin her iki yanını $f^{-1}_{(n)}$ ile çarpar ve sonra da $mod\ q$ yerine denklemi $mod\ p$ de ele alır isek ki nm mesajı bu değerlerden etkilenmemelidir.

$$e_1 + e_2 + \cdots + e_n \equiv nm(mod\ p)$$

haline gelir. Sistemin içerisindeki bir kullanıcı n güvenlik parametresini bildiğinden

$$e_1 + e_2 + \cdots + e_n \equiv m + m + \cdots + m(modp)$$

şeklindeki bir düşünce ile alınan mesajın m veya bunun n katı olan nm mesajı olduğunu bilir. Bu durum olasılıklı kriptolojiye girmektedir. Yani sistemin bir kullanıcısının bu girift durumdan çıkabileceği varsayımına dayanmaktadır. Şimdi ise kesin bir deşifreleme metodu cisimler yardımıyla verilecektir.

⊠

Lemma 7.2 p ve q asal sayılar ve M, S de sırasıyla $F_p[x]$ ve $F_q[x]$ de indirgenemeyen iki N mertebeli polinom olsunlar. O halde Lemma 7.1 de verilen sistem önerisi $F_p[x]/(M)$ ve $F_q[x]/(S)$ cisimlerinde ihtimalsiz bir şekilde çalışacaktır.

İspat Lemma 7.1 deki tüm şartlar aynı kalmak koşulu ile sadece f, g, r ve m polinomlarının $F_p[x]/(M)$ veya $F_q[x]/(S)$ den seçilebileceğini hatırlatalım. Yine benzer şekilde bir m polinomunu n farklı h açık anahtarı ve n farklı r hata polinomu ile şifreleyip toplam şifreli metni n ye bölüp gönderelim. Şöyle ki Lemma 7.1 deki (32) ifadesini n ye bölüp

$$a = \frac{e_1 + e_2 + \cdots + e_n}{n} = p.\frac{1}{n}[(h_1 \star r_1) + (h_2 \star r_2) + \cdots + (h_n \star r_n)] + m(mod\ q)$$

a yı şifreli metin olarak gönderelim. a polinomu önce $f_{(n)}^{*}$ daha sonra $f_{(n)}^{-1}$ ile çarpılırsa ve bu son ifade $mod\ p$ de hesap edilirse

$$\frac{e_1 + e_2 + \cdots + e_n}{n} = m(mod\ p)$$

olarak sistem olasılıksız bir şekilde çalışır. ⊠

Şimdi ise $q > n > p$ ve $(p, n) = 1$ durumunda sistemin nasıl çalışacağını ifade edelim.

Lemma 7.3 Lemma 7.1 deki şartlar aynı kalıp sadece ise $q > n > p$ ve $(p, n) = 1$ durumunda sistem yine küçük bir olasılık payı ile çalışacaktır.

İspat Yazım tekrarı oluşmaması adına Lemma 7.1 deki deşifreleme adımlarını geçip aşağıdaki gibi son adımı ele alalım:

$$e_1 + e_2 + \cdots + e_n = nm(mod\ p) \qquad (34)$$

$n < q$ olduğunda değişikliğe uğramadan modp ye inebiliriz. Lakin $n > p$ olduğunda $n = kp + l$ olacak şekilde $k, l \in Z$ vardır. O halde (34) denklemi

$$e_1 + e_2 + \cdots + e_n = lm(mod\ p)$$

haline gelir. Bu son durumda $l < n$ olduğundan olasılıklı bir deşifreleme yapılmalıdır. Yani alınan mesaj sadece m de olabilir lm de olabilir dahası nm dahi olabilir. Sistemdeki kullanıcı n, p, q parametresini bildiğinden $\{m, lm, nm\}$ kümesinden uygun bir metni seçer. ⊠

Önerme 7.1 $n > q > p$ durumunda Lemma 7.3 deki işlemlere ilave olarak $n = aq + b$ yazımından $b\ mod\ p$ sonucunda a ile çarpılması ihtimali de bulunacağından 4 olasılıklı olarak sistem yine çalışacaktır.

7.4. Çarpımsal Genelleme

Şimdi ise n defa şifrelenip daha sonra bu oluşan son şifreli polinomların çarpımını şifreli metin olarak gönderen bir yöntemi açıklayalım. İlk bölümde anlatılan toplamsal genelleme seçimleri ve işlemleri aynı kalıp bir m mesajını n farklı şekilde şifreleyelim. Bu defa bütün ön şifreli metinleri alt alta yazıp çarpalım. Kalan sınıflarının kompleks bir durum oluşturmaması adına p asalını yeterince büyük almanın faydalı olacağını belirtelim.

7.4.1. Sistem nasıl çalışır?

$$e_1 \equiv ph_1 \star r_1 + m(mod\ q)$$

$$e_2 \equiv ph_2 \star r_2 + m(mod\ q)$$

$$\vdots \qquad\qquad \vdots$$

$$\underline{\star\ e_n \equiv ph_n \star r_n + m(mod\ q)}$$

$$e_1 \star e_2 \star \cdots \star e_n \equiv p^n(h_1 \star h_2 \star \ldots \star h_n) \star (r_1 \star r_2 \star \ldots \star r_n) \star$$

$$p[H \star R] \star m + m^n(mod\ q) \qquad (35)$$

burada $H \star R\ h_i$ ve r_i lerin konvolüsyon çarpımının kısa bir sonucudur. Deşifreleme safhasında tersinin hesap edilmesi gerekmediğinden ve $mod\ p$ de sıfırlanacağından sadece sembolik bir sonuç yazıldı. Yine Lemma 7.1 deki gibi $f_{(n)}^{*}$ ve $f_{(n)}^{-1}$ ile sırasıyla (35) denklemi çarpılır ve sonuç $mod\ p$ de hesap edilirse

$$e_1 \star e_2 \star \cdots \star e_n \equiv m^n(mod\ p)$$

denklemine ulaşılır. $m^n(mod\ p)$ ifadesi indirgemeye gerek bırakmayacak bir şekilde seçilirse

$$e_1 \star e_2 \star \cdots \star e_n = m^n \qquad (36)$$

yazımı mümkün olur. En son aşamada gelinen bu (36) denklemi iki ihtimalli bir deşifreleme önerir:

1. Mesaj sadece m dir. Yani m^n polinomunda n güvenlik parametresi yardımıyla m açığa çıkar.
2. Ya da mesaj zaten m^n dir.

Şimdi ise sistemin olasılıksız çalışma durumu verilsin.

Lemma 7.4 Şayet tüm şartlar ve seçimler bir önceki bölümde anlatıldığı gibi yapılırsa (35) denklemi göz önüne alınsın. $e_1 \star e_2 \star \cdots \star e_n$ yerine bu polinomun n mertebeden kuvvetini alarak şifreli metin olarak gönderilmesi durumunda sistem olasılıksız çalışacaktır.

İspat (35) ifadesindeki şifreli metnin n. kuvveti alınıp

$$[e_1 \star e_2 \star \cdots \star e_n]^n$$

şeklinde gönderildiğinde tüm deşifreleme adımları uygun bir şekilde yapılırsa (36) ifadesi yerine

$$(e_1 \star e_2 \star \cdots \star e_n)^n = m^n \; mod \; p$$

denklemi oluşur ki p yeteri kadar büyük bir parametre olarak seçildiğinde

$$e_1 \star e_2 \star \cdots \star e_n = m$$

şeklinde mesaj direk olarak açığa çıkar. ⊠

Eğer "n" genelleme parametresi örneğin çarpımsal genelleme için $n = p_1 q_1$ olarak seçilirse, sistem deşifreleme adımının son basamağı RSA problemini çözmeye indirgenecektir. Bu ise önerilen genelleme sistemlerinin ne kadar güçlü bir altyapı üzerine kurulu olduğunu göstermektedir. Yani NTRU deşifreleme adımları doğru bir şekilde uygulandığında gelinen son aşama

$$e \equiv m^{p_1 q_1} \; (mod \; q)$$

olacaktır.

7.5. Koordinat Genellemesi ve Boyut Yükseltme

$R = Z[x]/(x^N - 1)$ halkasında bir NTRU kriptolama işlemi yapılırken üretilen h_1 açık anahtarından, $r_2 \in R$ gibi bir hata polinomu daha seçerek farklı bir h_2 açık anahtarı üretilebilir. Şöyle ki şayet $f, g \in R$ için $h_1 = pf_q^{-1} \star g$ ise $e_1 = h_1 \star r_1 + m(mod\ q)$ şeklinde ilk kriptolama işlemi yapılır. Keyfi seçilen $r_2 \in R$ için $h_2 = h_1 \star r_1 + r_2$ şeklinde üretilen bir diğer açık anahtar yardımıyla aynı mesaj (farklı da olabilir) $e_2 = ph_2 \star r_2 + m$ şeklinde farklı olarak gizlenebilir. Bu son durumda f ve g seçimleri klasik NTRU işlemlerindeki gibi olmak kaydıyla (h_1, h_2) açık anahtar, (e_1, e_2) şifreli metin ve (f, g) ise gizli anahtardır. Gönderilmek istenen mesaj (m, m) olabileceği gibi (m_1, m_2) de olabilir. Burada dikkat çekilmesi gereken husus tüm polinomların aynı dereceden olmalarıdır. Şayet değil iseler uygun 0 katsayılı monomial ilavesi yapılmalıdır. Bu yeni önerilen sistemin üzerine kurulduğu cebirsel yapıyı açıklamak adına öncelikle bir $a(x) = a_0 + a_1x + \cdots + a_{N-1}x^{N-1} \in R$ için

$$\theta: R = Z[x]/(x^N - 1) \to Z^N, \theta(a) = (a_0, a_1, \dots, a_{N-1})$$

şeklinde tanımlı bir dönüşümün homomorfizma olduğu açıktır. Bu θ dönüşümü yardımıyla bir μ dönüşümünü şöyle tanımlayalım. a, b, c ve $d \in R$ için $(a, b) \oplus (c, d) = (a + c, b + d), (a, b) \odot (c, d) = (a \star c, b \star d)$ işlemleri altında

$$\mu: R \times R \to Z^N \times Z^N, \mu((a, b)) = (\theta(a), \theta(b))$$

yani,

$$\mu((a, b)) = ((a_0, a_1, \dots, a_{N-1}), (b_0, b_1, \dots, b_{N-1}))$$

şeklinde tanımlayalım. $\oplus$ ve $\odot$ işlemlerinin iyi tanımlı olduğu kolayca gösterilebilir. μ bir homomorfizmadır çünkü

$$\begin{aligned}
\mu((a, b) \oplus (c, d)) &= \mu((a + c, b + d)) \\
&= (\theta(a + c), \theta(b + d)) \\
&= (\theta(a) + \theta(c), \theta(b) + \theta(d)) \\
&= (\theta(a), \theta(b)) + (\theta(c), \theta(d)) \\
&= \mu((a, b)) + \mu((c, d))
\end{aligned}$$

ve

$$\mu((a,b) \odot (c,d)) = \mu((a \star c, b \star d))$$

$$= (\theta(a \star c), \theta(b \star d))$$

$$= (\theta(a) \star \theta(c), \theta(b) \star \theta(d))$$

$$= (\theta(a), \theta(b)) \star (\theta(c), \theta(d))$$

$$= \mu((a,b)) \star \mu((c,d))$$

olur ki μ nün bir homomorfizma olduğu gösterilmiştir. Daha açık bir ifade ile $R \times R$ de işlemler $f, f', g, g' \in R$ için

$$(f,g) \oplus (f',g') = (f + f', g + g')$$

$$(f,g) \odot (f',g') = (f \star f', g \star g')$$

kuralları ile yapılacaktır. R halkası, $R \times R$ nin içine $f \mapsto (1,f)$ şeklinde gömülebileceği için $\forall f \in R$ için artık $(1,f) \in R \times R$ kullanılacaktır. O halde $(1,f)$ elemanının terslenebilir olması $f \in R$ nin terslenebilirliği ile mümkündür. Yani $f \in R$ için şayet $f \star f' \equiv 1 \; mod \; p$ ise $(1,f) \odot (1,f') = (1,1)$ olur ki $(1,1)$, $R \times R$ nin birim elemanıdır.

Tüm bu detay ve açıklamalardan sonra bu yapı üzerinde bir NTRU yu sunalım. $f, g, r_i \in R$ klasik NTRU metodolojisine göre belirlenmiş olsun. Bir $m_1, m_2 \in R$ mesaj polinomları için (m_1, m_2) mesajı gönderilmek istensin. $h_1 = p f_q^{-1} \star g$ ve $h_2 = p h_1 \star r_1 + r_2$ iki açık anahtar olmak kaydıyla

$$e_1 \equiv p f_q^{-1} \star g \star r_1 + m_1 \; (mod \; q)$$

$$e_2 \equiv p h_2 + m_2 \; (mod \; q)$$

ön şifrelemeleri ile belirlenen e_1 ve e_2 polinomlarının oluşturduğu $(e_1, e_2) \in R \times R \cong Z^{2N}$ vektörü gönderilecektir. (h_1, h_2) açık anahtar, f_p, f nin modp tersi olmak üzere (f,f) ve (f_p, f_p) gizli anahtarlar ve (r_1, r_2) de yeni önerilen sistemin hata vektörlerini temsil edecektir. g nin keyfi seçimleri bir çok gizli anahtar doğuracağından bu sistem için sadece (f,f) ve (f_p, f_p) anahtarlarının yeterli olacağını belirtiriz.

7.5.1. Sistem nasıl çalışır?

Alıcı (e_1, e_2) vektörünü gizli anahtarlar olan (f, f) ve (f_p, f_p) yardımıyla şöyle açacaktır.

$$(e_1, e_2) \odot (f, f) = (e_1 \star f, e_2 \star f)(mod\ q)$$

$$= (p \star g \star r_1 + f \star m_1, p^2 \star g \star r_1 + pr_2 \star f + f \star m_2)(mod\ q)$$

$$= (f \star m_1, f \star m_2)(mod\ p) \qquad (37)$$

olur. Buradan sonra (37) ifadesi (f_p, f_p) ile çarpılırsa, $\left(f_p, f_p\right) \odot (e_1, e_2) \odot (f, f) = (m_1, m_2)\ mod\ p$ olur ve deşifreleme sonucu direkt olarak mesaj açığa çıkar.

7.5.2. Sistemin avantajları

- Alıcı h_1 ve h_2 gibi iki açık anahtar kullanır. Dolayısıyla bir anahtar ele geçirilse dahi diğeri kolayca elde edilemeyecektir.
- Bir m mesajı yerine (m_1, m_2) gibi daha büyük bir mesaj tek seferde gönderilir.
- Kurulan bu sistem $Z^{2N} \cong Z^N \times Z^N$ üzerinde olduğundan $Z^N \cong R = Z[x]/(x^N - 1)$ halkasına göre NTRU daha korunaklıdır.
- $f \in R$ bir özel anahtar ise $(f, f) \in R \times R$ bir özel anahtar belirtir ki fazladan bir arama işlemi ve zamanına gerek kalmaz.

7.5.3. Sistemin dezavantajları

Birden çok işlemi barındırması ve birden çok açık anahtar üretmesi güvenliği artırıcı nitelikte olmasına karşın algoritmaların, zaman, bellek ve efor kapasitesinde bir gerilemeye yol açacaktır.

7.6. Genelleştirmelerden Elde Edilebilecek NTRU Dijital İmzaları

Birinci kısımda verilen toplamsal genelleme metodunda şayet e_i, $1 \leq i \leq n$ mesajları alıcıya gönderildi ve alıcı tarafından doğru bir şekilde okunduğu, sistem içerisinde bir sızma olmadığı ve bu alıcının doğru kişi olduğu şöyle anlaşılacaktır:

$e_1, e_2, \dots, e_n$ şifrelerini çözdü isen $e_1 + e_2 + \cdots + e_n$ şifresini de çöz böylece güvenilir bir kullanıcı olduğunu kanıtla! Şayet alıcı bu toplamsal şifreyi de çözerse dijital olarak imzalamış olacaktır. Benzer saiklerle çarpımsal genelleme metodu da bir dijital imza

olarak kullanılır ve son olarak anlatılan (e_1, e_2) şifrelerinin bir üst boyutta gönderilmesi yani R yerine $R \times R$ de çalışılması yeni bir dijital imza yöntemi olarak kullanılabilir. Bu yöntemde ise e_1 ve e_2 gönderilir ve alıcının son olarak (e_1, e_2) metnini çözmesi beklenir. Bunun diğer bir çözümü alıcı adına bir dijital imza görevi görecektir. Boyut büyütme kolayca $R^N = \underbrace{R \times R \times \ldots \times R}_{N}$ kümesine taşınabilir. Bu durumda ise $(e_1, e_2, \ldots, e_n)$ şifresi okununca alıcının doğru bir kullanıcı olduğu anlaşılır. Yine aynı bölümde tüm parametreler klasik NTRU kriptosisteminde tanıtıldığı gibi seçilmek üzere,

$$D^i_{NTRUEncryt}: (m, r_i, h_i) \longmapsto e_i, 1 \leq i \leq n$$

dönüşümü yardımıyla bir dijital imza

$$D^n_{NTRUSIGN}: m \longmapsto (m, \sum e_i), 1 \leq i \leq n$$

şeklinde tanımlanmış ve bu imzanın doğrulaması ise

$$D_{verification}: \sum e_i \longmapsto (m, n, n \; mod \; q)$$

şeklinde tanımlanarak yeni bir NTRU tabanlı dijital imza elde edilmiştir.

7.7. Çalışmanın Özeti ve Çıktı

Bölüm 7 de yapılan sistem genellemelerinin dijital imzalama ve doğrulama yöntemi olarak çalışabileceği gösterilmiştir. Eğer "n" genelleme parametresi örneğin çarpımsal genelleme için $n = p_1 q_1$ olarak seçilirse sistem deşifreleme adımının son basamağı RSA problemini çözmeye indirgenecektir. Bu ise önerilen genelleme sistemlerinin ne kadar güçlü bir altyapı üzerine kurulu olduğunu göstermektedir. Yani NTRU deşifreleme adımları doğru bir şekilde uygulandığında gelinen son aşama

$$e \equiv m^{p_1 q_1} \; (mod \; q)$$

olacaktır.

8. SONUÇLAR, TEZİN ÇIKTILARI VE SENTEZ

Bu başlık altında tezde matematik dili ile anlatılan iddiaların bir yorumlaması yapılacaktır. Özetle, NTRU kriptosistemi Galois halkalarında incelendi. Birçok farklı parametre ve anahtar ilavesi ile sisteme cebirsel katkılar sunuldu. Ayrıca dijital imza versiyonu olarak kullanılabilecek ve genelleme mahiyetinde bir çalışması da yapıldı. Daha kompleks ve güçlü bir latis altyapısı önerildi. Tüm bu tezlerin ve sentezlerin, araştırmalara ilham kaynağı olup kriptoloji disiplinine bir katkı da bulunması temennisi ile çıktılar aşağıdaki gibidir:

- Teorem 6.1 de yapılan çalışmanın temel felsefesi, $e \equiv p.h \star r + m \; mod \; q$ ifadesinin yine açık anahtar olmasından ötürü $mod \; p$ de ele alınırsa açık metnin saldırılara daha kolay maruz kalabileceği endişesi üzerinedir. φ izomorfizmi teorem 6.1 de belirtildiği haliyle alınıp şayet denklem $e \equiv p.h \star r + \varphi(m) \; mod \; q$ olarak şifreli metni üretirse açıktır ki bir φ izomorfizmi bir açık metin m polinomunu başka bir polinoma dönüştüreceğinden yani $\varphi(m) \neq m$ olacağından güvenlik düzeyi açık metni korumak üzerine kesin sonuç verecektir.
- $Z_p[x]/(x^N - 1)$ halkası yerine $Z_{p^k}[x]/(x^N - 1)$ $k \geq 1$ Galois halkaları seçilmesinin temel sebepleri, anahtar havuzunu büyütmek ve parametre seçimlerini kolay kılmak adına yapılmıştır. Ayrıca Galois halkaları tek maksimal ideali olan çok özel halka türleridir. Bu halkalarda maksimal idealin içinde unit (birimsel eleman) aranamayacağından M maksimal ideali göstermek koşulu ile $G \setminus M$ kümesinde özel anahtar f fonksiyonları aranmalıdır.
- Modülü oluşturan $x^N - 1$ polinomu halkada ne kadar indirgenebilirse o sayıda ideal oluşacağından terslenebilir (özel anahtar) polinom sayısı azalacaktır ki anahtar üretmek kolaylaşacak fakat gizli anahtara yapılan saldırılara maruz kalınacaktır.
- Z_p cismi yerine Z_{p^k} halkası alınması demek hem daha geniş bir cebirsel yapıda hem de sıfır bölenlerin olduğu daha kompleks bir yapıda çalışmak manasına geleceğinden kriptolojinin asıl amacı olan gizlilik ve karmaşıklığa yardımcı olacağı açıktır.
- $(p, q) = 1$ açıkça $(p^k, q^k) = 1$ demek olacağından k güvenlik parametresi eski sistemi koruyup genelleyen, cismi halkaya dönüştüren bir sabittir. Büyük kümede daha fazla işlem ve hesaplama yapılmasına olanak verecek ve güvenliği yükseltip hızı düşürecektir.

Bölüm 6.4 de yapılan çalışmaların ve bulguların yorumlanmasına gelince; amaç, $e \equiv p.h \star r + m \; mod \; q$ denklemini iki polinom ile güçlendirmektir. Yani cebirsel olarak

$$e \equiv \big[[p.h \star r + P.m] mod \; Q\big] mod \; q$$

ifadesinin daha kompleks ve güçlü olduğu aşikardır burada $(P, Q) = 1$ ve $(P, p) = (Q, q) = (Q, p) = 1$ şartları bulunmalıdır. $der(m) < der(Q)$ olması ve $der \; m > der \; Q$ durumları ayrı ayrı ele alınıp daha çok güvenlik için $der \; m > der \; Q$ daha kolay işlemler ve hız için ise $der \; m < der \; Q$ olması gerektiğini belirtelim.

- P özel anahtar ve Q da açık anahtar görevi görüp anahtar havuzu büyüdüğünden açık metin kümesinde büyük olmalıdır ki sistem düzgün bir yapıda çalışsın. Bu sebeple k güvenlik sabiti istenildiği kadar büyük seçilip Z_{p^k} üzerinde çokça açık ve gizli anahtar değişimi protokole bağlanabilir.
- Ayrıca bölüm 6.4 deki denklem

  $$e \equiv [p.h \star r + [P. mod \; Q].m] mod \; q$$

  haline getirilirse $(P, Q) = 1$ olduğunda $der \; P > der \; Q$ olsa bile P nin Q ya göre rezidüsü olan P' polinomu da Q ile aralarında asal olup tersi mevcut olacağından kolaylık açısından $der \; P < der \; Q$ şartı altında ve Q ile bölme işleminin yapılamaması neticesinde algoritma hızı artacaktır. Üstelik bu durumda sisteme sadece $(P, q) = 1$ şartı konması gerektiğinden P polinomu olarak bir önceki gizli anahtar olan f bile seçilebilir.

- $h \equiv f_q^{-1} \star g \star p \; (mod \; q)$ özdeşliğinden h polinomunun değil de belirlenmiş bir φ izomorfik dönüşümü yardımıyla $\varphi(h)$ ın açık anahtar olarak yayımlanması neticesinde oluşan latis $\varphi(H)$, $\varphi(h)$ polinomunun devirsel matrisi olmak üzere

  $$\begin{pmatrix} I & \varphi(H) \\ 0 & qI \end{pmatrix}$$

  şeklinde olacaktır. Açıktır ki bu latis daha kompleks formdadır. φ nin gizli anahtar olarak seçilmesi neticesinde düzenlenen saldırılar $\varphi(h)$ polinomunu ele verecek olsa dahi burada φ^{-1} bilinmediğinden asıl açık anahtar olan h polinomu H devirsel matrisi ele geçirilemeyecektir.

- Bölüm 7 de yapılan sistem genellemelerinin dijital imzalama ve doğrulama yöntemi olarak çalışabileceği gösterilmiştir. Eğer "n" genelleme parametresi örneğin çarpımsal genelleme için $n = p_1 q_1$ olarak seçilirse sistem deşifreleme

adımının son basamağı RSA problemini çözmeye indirgenecektir. Bu ise önerilen genelleme sistemlerinin ne kadar güçlü bir altyapı üzerine kurulu olduğunu göstermektedir. Yani NTRU deşifreleme adımları doğru bir şekilde uygulandığında gelinen son aşama

$$e \equiv m^{p_1 q_1} \ (mod\ q)$$

olacaktır.

- Yine aynı bölümde tüm parametreler klasik NTRU kriptosisteminde tanıtıldığı gibi seçilmek üzere

$$D^{i}_{NTRUEncryt}: (m, r_i, h_i) \longmapsto e_i, \qquad 1 \leq i \leq n$$

dönüşümü yardımıyla bir dijital imza

$$D^{n}_{NTRUSIGN}: m \longmapsto (m, \sum e_i), \qquad 1 \leq i \leq n$$

şeklinde tanımlanmış ve bu imzanın doğrulaması ise

$$D_{verification}: \sum e_i \longmapsto (m, n, n\ mod\ q)$$

şeklinde tanımlanarak yeni bir NTRU tabanlı dijital imza elde edilmiştir.

Bölüm 6 da $f \in L_f$, $g \in L_g$ ve $P \in R$ olmak üzere f ve g nin klasik NTRU sistemindekinin aksine terslenmesi gerekmeyen, bunlara karşılık sadece $(P, Q) = 1$ şartını sağlayan bir $P \in R$ nin bulunması gerekliliği sistemi parametre bulma konusunda esnekliğe kavuşturmuştur. $h = f \star g \star P$ polinomu açık anahtar olarak şifrelemede kullanılmıştır. m mesaj polinomu Pm şeklinde bir adım daha gizlenerek şifrelenmektedir. Deşifrelemenin son adımında $m\ mod\ Q$ ifadesi m nin Q ya bölünmesi gereken durumları ele almıştır.

(h, Q) açık anahtar, (f, g, P) ise gizli anahtar olmak üzere sistemin açık veya gizli anahtarları artırılarak sistemin güvenlik düzeyi yükseltilmiştir.

9. TARTIŞMA

Matematikte olduğu gibi sayılar teorisi de sayıların özellikleri ile ilgilenir fakat bilhassa pozitif sayıların. Tarih boyunca genel olarak, konular, problemler ve sonuçları salt matematik içerisinde çözülüp öylece kalıyordu. Örneğin, 2000 yıl önce Elemanlar adlı kitabında Euclid, sonsuz sayıda asal sayı bulunduğunu ispat ediyordu. O günün dünyasında birkaç adet asal sayı bilmenin bile ayırt edici olduğu bir tarihte Euclid matematiksel dünyada sonsuz ile ilgileniyordu. Bugünlerde çok karizmatik görünen bu eylem muhtemelen o günlerde trajik veya ironik görünüyordu. Zira sonsuzu, sonsuza ıraksayan asal sayıları ve benzeri anladığınızı ve çevrenizde hiç kimseye anlatamadığınızı veya anlaşılamadığınızı bir düşünün. Oysa bugün, iletişim ve araçlarına, bilgi ve kaynağının hatta insan nüfusu artışının da etkisiyle matematiğin reel hayata ve diğer disiplinlere uygulamaları önemli ölçüde artmaktadır.

Bir matematikçinin asıl merakını çeken konu belki, gelişen online ödeme yöntemleri, dijital imza, dijital para, güvenli iletişim kaynakları olmayabilir. Fakat bunların doğup büyümesine yardımcı olan, sayılar teorisi, ayrık logaritma problemi, grup ve halka teori, eliptik eğriler, latis ve vektör uzayı üzerine kurulu kuantum kriptografi gibi konular daha çok ilgisini çekecektir.

DNA ile ilgili çalışmaların gelip biyolojik kodlamaya dayanması, fizik çalışmalarının kuantum kriptolojisine kapı açması, finans çalışmalarının dijital ve algoritmik para kavramını tartışması hatta en beğenilen klasik müziklerin bir trigonometrik modellemesinin var oluşu… Tüm bunlar matematiğin anlaşılınca dünyanın ne kadar gelişeceği ve ilerleyeceğini gösteren örneklerdir.

Bilgisayarların daha büyük hafıza alanlarına sahip olması gereksinimi veya daha güçlü işlemciler, daha hızlı algoritmalar, programlar, uygulamalar vb olan ihtiyaç artarak devam etmektedir.

Ne ilginçtir ki, modüler aritmetik ve rezidü sistemlerin kullanıldığı bu teknolojilerde bugün daha çok hafızaya ve daha yüksek güvenliğe duyulan ihtiyaç nedeniyle rezidü kodlar, devirli kodlar ve güçlü şifreleme sistemleri kullanılmaktadır. Aşikardır ki bilgisayarlar sınırlı varlıklardır. Sınırlı uzunluktaki sayıları ve sınırlı komuttaki algoritmaları işleyip sınırlı hafızası ve sınırlı işlemci kapasitesi nedeniyle sonuçları ancak sınırlı bir formda sunacaktır. İnsan beyni ise binlerce yıl öncesinde bile sonsuzu hayal edebilecek, bu hayale ulaşacak ve onu ifade edecek donanımda yaratılmıştır.

Bilgisayarın ve doğanın bu sınırlı kaynak ve gücüne rağmen insan beyni ve matematiğin sınırsız ve sürpriz gelişmeleri ile birlikte daha hızlı ve güvenli iletişim kaynakları, daha güçlü ve korumalı banka işlemleri, daha yeni ve bakir gezegenler vb keşfetmek mümkün olabilecektir.

Açık anahtar şifreleme sistemlerini kendi içinde iki ana başlığa ayırmak gerekirse, grup bazlı ve latis-kod bazlı şeklinde bir ayrım yapmak mümkündür. İlk açık anahtar kripto sistemler ayrık logaritma problemi ve asal çarpan bulma problemlerinin zorluğu üzerine kurulmuştur. Sistem, bir grup yapısı seçilerek üzerinde inşa edilmiştir. Fakat zaman geçtikçe güçlü cebirsel ilaveler katılmasına rağmen bu sistemlerin polinom-zaman algoritmalarının da kırılabileceği görülmüştür. Kod sistemlerin aynı zamanda bir vektör uzayı teşkil etmesi, latis tabanlı sistemlerin ayrık bir vektör uzayı oluşu ve hatta yer yer halka yapısı üzerine oturtuluşu (NTRU) hasebiyle açıktır ki bu sistemler en başında zaten grup yapısı taşımaktadır. İlaveten vektör uzayının lineer özellikleri ve halka yapısının daha fazla cebirsel uygulamaya müsait oluşu sebebiyle bugün özellikle NTRU sistemi kuantum saldırılara karşı oldukça dirençlidir.

Asimetrik şifrelemenin birçok türü bugün kırılmış veya kırılmak üzeredir. Peter Shor un tanımladığı algoritma yeterli zaman içinde grup tabanlı ve büyük asal sayıların çarpımına dayanan açık anahtar (asimetrik) şifreleme yöntemlerinin kırılacağını göstermektedir. Bu bağlamda gruptan daha kompleks yapıların ve bunların üzerinde kurulu cebirsel kriptolojinin metodları üretilmiştir. Bugün halen bu post kuantum denilen kriptolojik metodların en ünlüsü ve halen kırılmamış olanı NTRU dur. Ne yazık ki kuantum sonrası bilgisayar ve yazılım şirketlerinin kendi alanlarında yaptıkları büyük yatırımlar bir gün mutlaka NTRU nun da kırılabileceğini öngörmemize olanak sunmaktadır. Bu matematikçilerin şimdilik daha güçlü bir cebirsel materyal desteği ile NTRU kriptosistemini korunaklı tutmaları elzemdir. Kendisinden önce üretilmiş tüm açık anahtar şifreleme yöntemlerinden daha güçlü oluşunun yanı sıra birçok parametre ve değişken barındırması onu matematik manipülasyonlarla geliştirmeye davetiye çıkarmaktadır. Eminim ve umut ediyorum ki NTRU daha birçok matematikçinin ilgisini çekecek ve yeni kriptolojik protokollerin, saldırı algoritmalarının ve dijital imza yöntemlerinin gelişimine ışık tutacaktır.

Modern açık anahtar kriptolojik sistemler genel olarak, sayılar teorisinin zarif teoremleri, püre ve soyut cebirin denklem, teorem ve önermelerinin üzerine inşa edilmiştir. Bir sayının çarpanlarına ayrılabilmesi, büyük asallar seçimi, ayrık logaritma problemi, homeomorfik

yapılar, izomorfik dönüşümler, Galois halkaları, modül ve ideal teorilerinin getirdikleri ve sonuç olarak harika ve tutarlı soyut yapılar üzerinde gelişmiş cebir literatürü modern kriptolojiye yeni bir kapı açmaktadır; Kuantum kriptolojisi. Açık ve kesindir ki gelecek dünyanın bilgisayar teknolojileri daha güçlü ve hızlı olacaktır. Bu bağlamda bir matematik yapı üzerine kurulmuş kriptolojik sistemlere daha öldürücü saldırılar düzenlenebilecektir. İşte bu sebepledir ki yeni, genel ve daha kompleks kriptolojik sistemler üretilmelidir. Tarihte olduğu gibi bu gelecek kuantum bilgisayar riskinden korunmak için matematiksel kriptoloji şimdiden daha dirençli ve kapsamlı yapılar önermelidir.

NTRU kriptosisteminin önemi Shor' un 1997 de yaptığı çalışmadan sonra artarak devam etmiştir. Shor, 1997 de yeterli süre sonunda herhangi bir asalın ayrıştırılabileceğini ve herhangi bir logaritma probleminin çözülebileceğini gösterince latis tabanlı kriptosistemler ilgi çekmeye başlamıştır. Zira henüz latis tabanlı bir sistemin güvenlik açığına rastlanmamıştır. Bunlar arasında, sadece latis yapısına haiz olmayıp ayrıca polinom halkası özelliğinden ötürü NTRU konuşulmaya, çalışılmaya ve tartışılmaya başlanmıştır. Güçlü cebirsel altyapısı, zengin parametreleri, dijital imza ve doğrulama gibi versiyonlarının da oluşu sebebiyle farklı varyasyonları, farklı halkalarda ve farklı parametrelerle yayınlanmaya devam etmektedir. Gelecekte, dijital çağın getirdikleri arasında IOT(nesnelerin interneti) teknolojilerinin nereye ulaşacağını hayal edemediğimiz için NTRU kriptosistemleri matematiksel merak ve dürtülerle koruma kalkanı içerisine alacak çalışmalara ilham olması adına …

10. ARAŞTIRMACILAR İÇİN GELECEK PERSPEKTİFİ VE ÖNERİLER

NTRU tabanlı iki kriptosistemi birbiri ile karşılaştırmak pek mümkün değildir. Çünkü farklı parametrelerle farklı cebirsel yapılar üzerinde kurulu iki sistemin birbirine nazaran artıları ve eksileri olabilmektedir. Bununla birlikte bir kriptosistem, başlangıçta amaçlanan protokolleri ile ve sonuçta gözlenen çıktıları karşılaştırılarak daha iyi analiz edilebilir. Bir sistem hızlı olmayı baz alıp kolaylığı ve efektifliği amaçlarken başka bir sistem güvenli olmayı hedefleyebilir. En somut gözlemler ise ataklarla ortaya çıkmaktadır. Kendisine düzenlenen ataklara güncel çözümler sunan bir sistem çalışmaya devam etmektedir. Bu bağlamda, teorik bir çalışma olan bu tezin çıktıları,

- Galois halkaları yerine başka bir halkada veya cisimde,
- $x^N - 1$ modülü yerine genel bir f modülü alarak,
- sisteme daha farklı biçimlerde ve daha fazla sayıda anahtar ekleyerek,
- tezin çıktılarını oluşturan, Galois halkaları üzerinde polinom modüllerle birlikte ve dijital imza versiyonu olacak biçimde özetlenebilecek NTRU incelemelerinin, güvenlik ve karşılaştırma analizleri, optimizasyonları ve kriptoanalizleri uygun programlardan destek alarak,
- yine bu üç farklı çıktının latisleri oluşturularak daha kapsamlı latis yapılar üzerinde kriptosistem incelenebilir.
- Sistem $R = Z[x, y]/(x^N - 1, y^N - 1))$ gibi daha genel bir halkada incelenebilir. Hem halkanın hem de modülün büyümesinin sisteme cebirsel etkileri gözlenebilir.

11. KODLAR

11.1. NTRU Kriptosisteminin İşleyişine Dair Algoritmik Bir Örnek

```
alfabe={"A","B","C","Ç","D","E","F","G","Ğ","H","I","İ","J","K","L","M","N","O
","Ö","P","R","S","Ş","T","U","Ü","V","Y","Z"," "};

duzMetin="MEHMET SEVER"

mKatsayiListesi=FirstPosition[alfabe,#][[1]]&/@ Characters[duzMetin]

m=KatsayiListesindenPolinomGetir[mKatsayiListesi]

n=Prime[RandomInteger[{5,10}]]

 MEHMET SEVER

 {16,6,10,16,6,24,30,22,6,27,6,21}

 16+6 x+10 x^2+16 x^3+6 x^4+24 x^5+30 x^6+22 x^7+6 x^8+27 x^9+6 x^10+21 x^11

 p=Prime[23] (* p tek olmalı *)

 RastgelePolinomSec[N_]:=Table[RandomInteger[{10,10000000}],N];

KatsayiListesindenPolinomGetir[KL_]:=Sum[KL[[i]]*x^(i-
1),{i,1,Length[KL]}];

toplam[f_,g_,k_,n_]:=Module[{i,j,sonuc=0,fL,gL},

   fL=CoefficientList[f,x,Max[Exponent[f,x],Exponent[g,x]]+1];

   gL=CoefficientList[g,x,Max[Exponent[f,x],Exponent[g,x]]+1];

   For[i=1,i<=Length[aaL],i++,

    For[j=1,j<=Length[bbL],j++,

      If[Mod[i-1+j-1,n]==k,sonuc+=aaL[[i]]bbL[[j]]];

      ];
```

```
    ];

   sonuc

   ];

f_⊗g_:=KatsayiListesindenPolinomGetir[Table[toplam[f,g,k,n],{k,0,n-1}]];

 g=KatsayiListesindenPolinomGetir[RastgelePolinomSec[n]]

r=KatsayiListesindenPolinomGetir[RastgelePolinomSec[n]]

F1=KatsayiListesindenPolinomGetir[RastgelePolinomSec[n]]

F2=KatsayiListesindenPolinomGetir[RastgelePolinomSec[n]]
```

$$3180072+1351491\,x+5544406\,x^2+9658469\,x^3+9312901\,x^4+9858171\,x^5+5339039\,x^6+5165031\,x^7+598010\,x^8+8214266\,x^9+4057426\,x^{10}+2190938\,x^{11}+2122154\,x^{12}+2421895\,x^{13}+8289828\,x^{14}+3930115\,x^{15}+6744943\,x^{16}+8829006\,x^{17}+7826012\,x^{18}+4849624\,x^{19}+8136628\,x^{20}+8305837\,x^{21}+6070686\,x^{22}$$

$$4569576+4345721\,x+9033363\,x^2+2311585\,x^3+1790987\,x^4+4532575\,x^5+7507054\,x^6+2553122\,x^7+7313847\,x^8+7523105\,x^9+4985345\,x^{10}+6458572\,x^{11}+4140441\,x^{12}+1547919\,x^{13}+4635832\,x^{14}+1409507\,x^{15}+5334400\,x^{16}+5453749\,x^{17}+4116777\,x^{18}+4618265\,x^{19}+1600124\,x^{20}+5732661\,x^{21}+6125483\,x^{22}$$

$$8866300+1302574\,x+6413680\,x^2+22265\,x^3+9561914\,x^4+5021278\,x^5+4201670\,x^6+1920641\,x^7+1433355\,x^8+3903787\,x^9+4068498\,x^{10}+9713524\,x^{11}+5286361\,x^{12}+6530420\,x^{13}+833300\,x^{14}+4343536\,x^{15}+6247792\,x^{16}+4876921\,x^{17}+8576589\,x^{18}+3000481\,x^{19}+5020920\,x^{20}+6873168\,x^{21}+9826415\,x^{22}$$

$$4102217+6708129\,x+5000641\,x^2+1879366\,x^3+8261351\,x^4+7209764\,x^5+2756579\,x^6+8691832\,x^7+7226318\,x^8+1176122\,x^9+3120286\,x^{10}+9148717\,x^{11}+5027127\,x^{12}+7603375\,x^{13}+2519265\,x^{14}+9900561\,x^{15}+3858535\,x^{16}+7761550\,x^{17}+8058412\,x^{18}+8181962\,x^{19}+1955050\,x^{20}+5737491\,x^{21}+5981604\,x^{22}$$

p=Prime[RandomInteger[{1000,10000}]]

q=Prime[RandomInteger[{10001,20000}]]

f=1+Expand[p q F_1]

invf=1+Expand[p q F_2]

h=invf⊗g

20431

171761

$$31114054328903301+4571056495202834\,x+22507200068596880\,x^2+78133428784615\,x^3+33555137056528774\,x^4+17620914755030498\,x^5+14744706208014970\,x^6+6740007491323231\,x^7+5029999587494805\,x^8+13699360590828917\,x^9+14277372501385518\,x^{10}+34087174296054284\,x^{11}+18551157005311751\,x^{12}+2291686979580622 0\,x^{13}+2924257184200300\,x^{14}+1524254932537217 6\,x^{15}+21925057771977872\,x^{16}+17114330098436711\,x^{17}+30097386294471699\,x^{18}+10529434921764671\,x^{19}+17619658443891720\,x^{20}+24119657868973488\,x^{21}+34483336923897265\,x^{22}$$

$$14395700868113048+23540494924747839\,x+17548494383603231\,x^2+6595163239219706\,x^3+28991137661046841\,x^4+25300857042348124\,x^5+9673522074361789\,x^6+30501802675941512\,x^7+25358949150145138\,x^8+4127304941792902\,x^9+10949860497131426\,x^{10}+32105125901194547\,x^{11}+17641440352378857\,x^{12}+26682136046944625\,x^{13}+8840728159311615\,x^{14}+34743533699583951\,x^{15}+13540560055488185\,x^{16}+27237211506096050\,x^{17}+28278974180062292\,x^{18}+28712541892900342\,x^{19}+6860757239854550\,x^{20}+20134284502621581\,x^{21}+20990937801561564\,x^{22}$$

$$6+4\,x+3\,x^2+4\,x^3+x^5$$

e=PolynomialMod[p h⊗r+m,q]

122602+81730 x+61303 x^2+81740 x^3+6 x^4+20455 x^5+30 x^6+22 x^7+6 x^8+27 x^9+6 x^{10}+21 x^{11}

m_1=PolynomialMod[e⊗f,q]

6+4 x+3 x^2+4 x^3+x^5

m_2=PolynomialMod[invf⊗m_1,p]

6+4 x+3 x^2+4 x^3+x^5

m

16+6 x+10 x^2+16 x^3+6 x^4+24 x^5+30 x^6+22 x^7+6 x^8+27 x^9+6 x^{10}+21 x^{11}

11.2. NTRU Kriptosisteminde Modül Parametresinin Büyütülmesine Dair Algoritmik Bir Örnek

(* FONKSİYONLAR *)

```
KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-1),{i,1,Length[KL]}]];


KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@KK);


HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];


Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];
```

```
Mods[a_,p_]:=If[Mod[a,p]-5<-((p-1)/2),Mod[a,p],Mod[a,p]-5];


PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];


(* MESAJ AYARLAMASI *)

alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S
","T","U","V","Y","Z"," "};


duzMetin="MEHMET SEVER";


harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[duzMetin];


mKatsayiListesi=#-1&/@(IntegerDigits[#,3]&/@harfKonumlari//Flatten);


m[x_]=KatsayiListesindenPolinomGetir[mKatsayiListesi, x]


(* SABİTLER *)
```

```
Unprotect[N];

N=Prime[53] (* N tek olmalı, ancak genelde asal alınır *)

Protect[N];


p=Prime[23] (* p tek olmalı *)


q=Prime[128] (* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)


(* TANIMLAMALAR *)

F[x_]=HalkadanRastgelePolinomSec[N,{-1,0,1},x];


G[x_]=HalkadanRastgelePolinomSec[N,{-1,0,1},x];


f[x_]=1+Expand[p F[x]];


g[x_]=Expand[p G[x]];


c[x_]=PolynomialGCD[f[x],x^N-1]


f_p[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^N-1,x][[2,1]],p,x];
```

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^N-1,x][[2,1]],q,x];

h[x_]=PolynomialMods[f_q[x]g[x],q,x];

r[x_]=HalkadanRastgelePolinomSec[N,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],N,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],N,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

mmm[x_]=PolynomialMods[a[x],3,x]

m[x]

$x^4+x^5+x^6+x^{11}+x^{12}-x^{13}+x^{15}+x^{16}-x^{17}+x^{18}-x^{19}-x^{20}+x^{22}+x^{23}-x^{25}+x^{27}+x^{29}+x^{30}$

241

83

719

1

$86+86\,x+362\,x^2+545\,x^3+32\,x^4+481\,x^5+194\,x^6+357\,x^7+603\,x^8+74\,x^9+170\,x^{10}+672\,x^{11}+436\,x^{12}+272\,x^{13}+562\,x^{14}+474\,x^{15}+80\,x^{16}+256\,x^{17}+699\,x^{18}+303\,x^{19}+421\,x^{20}-x^{21}+297\,x^{22}+463\,x^{23}+303\,x^{24}+673\,x^{25}+43\,x^{26}+419\,x^{27}+467\,x^{28}+9\,x^{29}+400\,x^{30}+471\,x^{31}+305\,x^{32}+262\,x^{33}+503\,x^{34}+225\,x^{35}+537\,x^{36}+427\,x^{37}+158\,x^{38}+132\,x^{39}+262\,x^{40}+38\,x^{41}+313\,x^{42}+3\,x^{43}+697\,x^{44}+36\,x^{45}+660\,x^{46}+293\,x^{47}-x^{48}+177\,x^{49}+558\,x^{50}+332\,x^{51}+610\,x^{52}+216\,x^{53}+691\,x^{54}+286\,x^{55}+252\,x^{56}+602\,x^{57}+52\,x^{58}+61\,x^{59}+616\,x^{60}+279\,x^{61}+258\,x^{62}+510\,x^{63}+467\,x^{64}+523\,x^{65}+696\,x^{66}+196\,x^{67}+413\,x^{68}+692\,x^{69}+85\,x^{70}+663\,x^{71}+52\,x^{72}+45\,x^{73}+76\,x^{74}+444\,x^{75}+479\,x^{76}+550\,x^{77}+218\,x^{78}+110\,x^{79}+332\,x^{80}+697\,x^{81}+644\,x^{82}+248\,x^{83}+679\,x^{84}+73\,x^{85}+634\,x^{86}+673\,x^{87}+444\,x^{88}+604\,x^{89}+39\,x^{90}+17\,x^{91}+335\,x^{92}+197\,x^{93}+37\,x^{94}+10\,x^{95}+700\,x^{96}+220\,x^{97}+696\,x^{98}+704\,x^{99}+252\,x^{100}+390\,x^{101}+559\,x^{102}+246\,x^{103}+599\,x^{104}+434\,x^{105}+144\,x^{106}+620\,x^{107}+442\,x^{108}+29\,x^{109}+453\,x^{110}+169\,x^{111}+113\,x^{112}+447\,x^{113}+311\,x^{114}+673$

$x^{115}+312\ x^{116}+321\ x^{117}+100\ x^{118}+222\ x^{119}+275\ x^{120}+395\ x^{121}+218\ x^{122}+391$
$x^{123}+157\ x^{124}+139\ x^{125}+684\ x^{126}+675\ x^{127}+557\ x^{128}+357\ x^{129}+539\ x^{130}+675$
$x^{131}+550\ x^{132}+521\ x^{133}+392\ x^{134}+620\ x^{135}+428\ x^{136}+587\ x^{137}+411\ x^{138}+349$
$x^{139}+353\ x^{140}+32\ x^{141}+40\ x^{142}+350\ x^{143}+570\ x^{144}+56\ x^{145}+160\ x^{146}+80$
$x^{147}+387\ x^{148}+227\ x^{149}+109\ x^{150}+554\ x^{151}+223\ x^{152}+27\ x^{153}+467\ x^{154}+22$
$x^{155}+364\ x^{156}+229\ x^{157}+248\ x^{158}+50\ x^{159}+628\ x^{160}+466\ x^{161}+667\ x^{162}+389$
$x^{163}+244\ x^{164}+627\ x^{165}+20\ x^{166}+660\ x^{167}+35\ x^{168}+425\ x^{169}+304\ x^{170}-3$
$x^{171}+550\ x^{172}+99\ x^{173}+218\ x^{174}+94\ x^{175}+536\ x^{176}+172\ x^{177}+150\ x^{178}+174$
$x^{179}+489\ x^{180}+499\ x^{181}+626\ x^{182}+336\ x^{183}+626\ x^{184}+391\ x^{185}+335\ x^{186}+242$
$x^{187}+696\ x^{188}+507\ x^{189}+334\ x^{190}+469\ x^{191}+114\ x^{192}+307\ x^{193}+642\ x^{194}+362$
$x^{195}+17\ x^{196}+20\ x^{197}+669\ x^{198}+340\ x^{199}+471\ x^{200}+77\ x^{202}+333\ x^{203}+652$
$x^{204}+703\ x^{205}+507\ x^{206}+250\ x^{207}+434\ x^{208}+696\ x^{209}+539\ x^{210}+529\ x^{211}+106$
$x^{212}+466\ x^{213}+692\ x^{214}+477\ x^{215}+447\ x^{216}+420\ x^{217}+455\ x^{218}+296\ x^{219}+671$
$x^{220}+357\ x^{221}+228\ x^{222}+536\ x^{223}+634\ x^{224}+552\ x^{225}+369\ x^{226}+447\ x^{227}+367$
$x^{228}+11\ x^{229}+34\ x^{230}+68\ x^{231}+643\ x^{232}+167\ x^{233}+87\ x^{234}+252\ x^{235}+436$
$x^{236}+58\ x^{237}+151\ x^{238}+71\ x^{239}+350\ x^{240}$

$-2-2\ x+25\ x^{2}+42\ x^{3}+27\ x^{4}+61\ x^{5}+23\ x^{6}+20\ x^{7}+17\ x^{8}+69\ x^{9}-x^{10}+3\ x^{11}+16$
$x^{12}+18\ x^{13}+59\ x^{14}+54\ x^{15}+75\ x^{16}+2\ x^{17}+30\ x^{18}+49\ x^{19}+x^{20}+77\ x^{21}+43$
$x^{22}+43\ x^{23}+49\ x^{24}+4\ x^{25}+38\ x^{26}-x^{27}+47\ x^{28}+4\ x^{29}+63\ x^{30}+51\ x^{31}+51\ x^{32}+8$
$x^{33}+54\ x^{35}+34\ x^{36}+7\ x^{37}+70\ x^{38}+44\ x^{39}+8\ x^{40}+33\ x^{41}+59\ x^{42}-2\ x^{43}+28$
$x^{44}+31\ x^{45}+74\ x^{46}+39\ x^{47}+77\ x^{48}+6\ x^{49}+55\ x^{50}-5\ x^{51}+24\ x^{52}+45\ x^{53}+22$
$x^{54}+32\ x^{55}-2\ x^{56}+16\ x^{57}+47\ x^{58}+56\ x^{59}+30\ x^{60}+25\ x^{61}+4\ x^{62}+7\ x^{63}+47$
$x^{64}+20\ x^{65}+27\ x^{66}+25\ x^{67}+76\ x^{68}+23\ x^{69}-3\ x^{70}+77\ x^{71}+47\ x^{72}+40\ x^{73}+71$
$x^{74}+24\ x^{75}+59\ x^{76}+47\ x^{77}+47\ x^{78}+22\ x^{79}-5\ x^{80}+28\ x^{81}+58\ x^{82}+77\ x^{83}+10$
$x^{84}+68\ x^{85}+48\ x^{86}+4\ x^{87}+24\ x^{88}+18\ x^{89}+34\ x^{90}+12\ x^{91}-2\ x^{92}+26\ x^{93}+32$
$x^{94}+5\ x^{95}+31\ x^{96}+49\ x^{97}+27\ x^{98}+35\ x^{99}-2\ x^{100}+53\ x^{101}+56\ x^{102}+75\ x^{103}+13$
$x^{104}+14\ x^{105}+56\ x^{106}+34\ x^{107}+22\ x^{108}+24\ x^{109}+33\ x^{110}-2\ x^{111}+25\ x^{112}+27$
$x^{113}+57\ x^{114}+4\ x^{115}+58\ x^{116}+67\ x^{117}+12\ x^{118}+51\ x^{119}+21\ x^{120}+58\ x^{121}+47$
$x^{122}+54\ x^{123}+69\ x^{124}+51\ x^{125}+15\ x^{126}+6\ x^{127}+54\ x^{128}+20\ x^{129}+36\ x^{130}+6$
$x^{131}+47\ x^{132}+18\ x^{133}+55\ x^{134}+34\ x^{135}+8\ x^{136}+x^{137}+74\ x^{138}+12\ x^{139}+16$
$x^{140}+27\ x^{141}+35\ x^{142}+13\ x^{143}+67\ x^{144}+51\ x^{145}+72\ x^{146}+75\ x^{147}+50\ x^{148}+56$
$x^{149}+21\ x^{150}+51\ x^{151}+52\ x^{152}+22\ x^{153}+47\ x^{154}+17\ x^{155}+27\ x^{156}+58\ x^{157}+77$
$x^{158}+45\ x^{159}+42\ x^{160}+46\ x^{161}-2\ x^{162}+52\ x^{163}+73\ x^{164}+41\ x^{165}+15\ x^{166}+74$
$x^{167}+30\ x^{168}+5\ x^{169}+50\ x^{170}+75\ x^{171}+47\ x^{172}+11\ x^{173}+47\ x^{174}+6\ x^{175}+33$

$x^{176}+x^{177}+62\ x^{178}+3\ x^{179}+69\ x^{180}-4\ x^{181}+40\ x^{182}-x^{183}+40\ x^{184}+54\ x^{185}-2$
$x^{186}+71\ x^{187}+27\ x^{188}+4\ x^{189}-3\ x^{190}+49\ x^{191}+26\ x^{192}+53\ x^{193}+56\ x^{194}+25$
$x^{195}+12\ x^{196}+15\ x^{197}+3\ x^{199}+51\ x^{200}-5\ x^{201}+72\ x^{202}-4\ x^{203}+66\ x^{204}+34\ x^{205}+4$
$x^{206}-4\ x^{207}+14\ x^{208}+27\ x^{209}+36\ x^{210}+26\ x^{211}+18\ x^{212}+46\ x^{213}+23\ x^{214}+57$
$x^{215}+27\ x^{216}+35\ x^{218}+42\ x^{219}+2\ x^{220}+20\ x^{221}+57\ x^{222}+33\ x^{223}+48\ x^{224}+49$
$x^{225}+32\ x^{226}+27\ x^{227}+30\ x^{228}+6\ x^{229}+29\ x^{230}+63\ x^{231}+57\ x^{232}-4\ x^{233}-x^{234}-2$
$x^{235}+16\ x^{236}+53\ x^{237}+63\ x^{238}+66\ x^{239}+13\ x^{240}$

$2+2\ x+2\ x^{2}+2\ x^{3}+2\ x^{4}+x^{5}+2\ x^{6}+2\ x^{9}+2\ x^{10}+x^{12}+2\ x^{13}+x^{14}+2\ x^{16}+x^{17}+x^{20}+2$
$x^{21}+x^{23}+x^{25}+x^{26}+2\ x^{27}+2\ x^{28}+x^{30}+2\ x^{32}+x^{33}+2\ x^{34}+x^{37}+2\ x^{38}+x^{40}+2$
$x^{41}+x^{42}+x^{44}+2\ x^{47}+2\ x^{48}+2\ x^{51}+x^{52}+x^{54}+x^{55}+2\ x^{57}+x^{58}+x^{59}+x^{60}+2$
$x^{64}+x^{65}+x^{67}+2\ x^{68}+2\ x^{69}+x^{70}+x^{72}+x^{74}+2\ x^{76}+x^{77}+2\ x^{78}+2\ x^{79}+2\ x^{80}+x^{81}+2$
$x^{82}+2\ x^{83}+x^{84}+x^{85}+x^{86}+x^{87}+x^{89}+2\ x^{91}+2\ x^{92}+2\ x^{93}+x^{94}+x^{95}+x^{96}+x^{97}+2$
$x^{99}+x^{102}+2\ x^{104}+2\ x^{105}+2\ x^{107}+x^{108}+2\ x^{109}+x^{111}+2\ x^{112}+2\ x^{114}+x^{115}+x^{118}+2$
$x^{120}+2\ x^{121}+2\ x^{122}+x^{123}+x^{124}+x^{125}+2\ x^{128}+2\ x^{130}+x^{132}+2\ x^{133}+2\ x^{134}+2\ x^{135}+2$
$x^{136}+2\ x^{137}+x^{139}+2\ x^{140}+2\ x^{141}+x^{142}+2\ x^{143}+2\ x^{145}+x^{146}+2\ x^{147}+2\ x^{149}+x^{150}+2$
$x^{151}+x^{152}+2\ x^{154}+x^{155}+x^{156}+x^{157}+2\ x^{158}+2\ x^{159}+x^{160}+x^{161}+x^{162}+2\ x^{163}+x^{164}+2$
$x^{166}+2\ x^{168}+2\ x^{169}+x^{170}+x^{172}+2\ x^{174}+x^{175}+2\ x^{176}+x^{177}+x^{181}+2\ x^{182}+2$
$x^{184}+x^{185}+2\ x^{186}+2\ x^{187}+x^{190}+x^{191}+x^{193}+2\ x^{195}+2\ x^{196}+2\ x^{197}+x^{199}+2$
$x^{202}+x^{204}+x^{205}+x^{207}+2\ x^{208}+2\ x^{210}+x^{211}+x^{212}+x^{213}+2\ x^{214}+2\ x^{218}+2\ x^{219}+2$
$x^{220}+2\ x^{223}+x^{224}+x^{228}+2\ x^{229}+x^{230}+2\ x^{231}+x^{232}+2\ x^{233}+x^{236}+x^{237}+x^{238}+2$
$x^{239}+2\ x^{240}$

$x^{4}+x^{5}+x^{6}+x^{11}+x^{12}-x^{13}+x^{15}+x^{16}-x^{17}+x^{18}-x^{19}-x^{20}+x^{22}+x^{23}-x^{25}+x^{27}+x^{29}+x^{30}$

11.3. NTRU Kriptosisteminde Mesaj Polinomuna Rotasyon Uygulanışına Dair Algoritmik Bir Örnek

```
(* FONKSİYONLAR *)

KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-
1),{i,1,Length[KL]}]];


KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@K
K);
```

```
HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];


Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];


Mods[a_,p_]:=Module[
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];


PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
```

```
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
  ];
PolinomdanMesajiAl[pol_,x_]:=Module[
  {katsayilar},
  katsayilar=CoefficientList[pol,x];

katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,Length[katsayilar]+3-Mod[Length[katsayilar],3]]];
  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]
  ];

(* SABİTLER *)
alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S","T","U","V","Y","Z"," "}
M=37; (* M tek olmalı, ancak genelde asal alınır *)

p=3;(* p tek olmalı *)

q=31 ;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)
 {A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,R,S,T,U,V,Y,Z, }
 (* TANIMLAMALAR *)
F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];
G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];
```

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}$

$1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

$G[x_]=x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

$m[x_]=x^{15}-x^{12}+x^7-1$

r[x_]=$x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\ x+3\ x^3+3\ x^9+3\ x^{12}+3\ x^{17}$

$-4+4\ x-10\ x^2+15\ x^3-5\ x^4+12\ x^5+5\ x^6+15\ x^7-11\ x^8+13\ x^9-12\ x^{10}+5\ x^{11}-x^{12}+x^{13}-6\ x^{14}+12\ x^{15}-9\ x^{16}-13\ x^{17}+11\ x^{18}-4\ x^{19}-8\ x^{20}-9\ x^{21}+14\ x^{22}$

$8+x+4\ x^2-8\ x^5+5\ x^6+10\ x^7+3\ x^8-14\ x^9-5\ x^{10}+7\ x^{11}-3\ x^{12}+14\ x^{13}-6\ x^{14}-14\ x^{15}+8\ x^{16}-14\ x^{18}+12\ x^{19}-15\ x^{21}-13\ x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15\ x-5\ x^2-14\ x^3+15\ x^4-10\ x^5+15\ x^6-14\ x^7+12\ x^8-9\ x^9-x^{10}-7\ x^{11}-10\ x^{12}+3\ x^{13}-8\ x^{14}+8\ x^{15}+6\ x^{16}-15\ x^{17}+10\ x^{18}+8\ x^{19}+4\ x^{20}-15\ x^{21}+5\ x^{22}$

$5-3\ x+6\ x^2+3\ x^3+6\ x^4-5\ x^7+3\ x^9+3\ x^{10}-9\ x^{11}-x^{12}+6\ x^{13}+7\ x^{15}-3\ x^{17}-3\ x^{19}-6\ x^{20}+3\ x^{21}+6\ x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

G[x_]=$x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

mesaj="MEHMET SEVER";

m[x_]=MesajdanPolinomUret[mesaj,x]

r[x_]=$x^{19}-x^{15}+x^{10}+x^8+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

PolinomdanMesajiAl[mm[x],x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\ x+3\ x^3+3\ x^9+3\ x^{12}+3\ x^{17}$

$12-9\ x-8\ x^2+6\ x^3-2\ x^4+14\ x^6+10\ x^7+10\ x^8-6\ x^9-x^{10}-13\ x^{11}+3\ x^{12}-x^{13}-15\ x^{14}+7\ x^{15}+x^{16}+2\ x^{17}-3\ x^{19}+10\ x^{20}-9\ x^{21}-15\ x^{22}-9\ x^{23}-8\ x^{24}+6\ x^{25}-13\ x^{27}+2\ x^{28}+13\ x^{29}+15\ x^{30}-15\ x^{31}-7\ x^{33}-2\ x^{34}-2\ x^{35}+11\ x^{36}$

$15+x-10\ x^2-6\ x^3+x^4-7\ x^5-2\ x^6-12\ x^8-12\ x^9-2\ x^{10}-3\ x^{11}+13\ x^{12}-4\ x^{13}-4\ x^{14}+15\ x^{15}+2\ x^{16}-13\ x^{17}+12\ x^{18}+6\ x^{19}-7\ x^{20}-14\ x^{21}+12\ x^{22}+2\ x^{23}-2\ x^{24}+9\ x^{25}-9\ x^{26}-6\ x^{27}+12\ x^{28}+8\ x^{29}-15\ x^{30}-14\ x^{31}+15\ x^{32}-3\ x^{33}-14\ x^{34}+10\ x^{35}+6\ x^{36}$

$-x^3+x^5-x^6+x^7+x^8-x^{12}+x^{14}+x^{15}-x^{16}+x^{18}+x^{19}-x^{20}+x^{21}-x^{22}-x^{23}-x^{24}+x^{26}+x^{27}-x^{29}-x^{30}+x^{32}+x^{34}+x^{35}$

$-x^2+x^6+x^8+x^{10}-x^{15}+x^{19}$

$9+10\,x+2\,x^2-8\,x^3-7\,x^4-9\,x^5+6\,x^6+2\,x^7-7\,x^8+9\,x^9+15\,x^{10}+11\,x^{11}-11\,x^{12}-3\,x^{13}+15\,x^{14}-x^{15}+3\,x^{16}-10\,x^{17}+10\,x^{18}+9\,x^{19}+2\,x^{20}-5\,x^{21}+11\,x^{22}-7\,x^{23}+2\,x^{24}+6\,x^{25}+13\,x^{26}+8\,x^{27}-13\,x^{28}+x^{29}+3\,x^{30}-5\,x^{32}+3\,x^{33}-4\,x^{34}-7\,x^{35}+3\,x^{36}$

$-3-6\,x+3\,x^2+2\,x^3-6\,x^4+x^5-x^6-2\,x^7+7\,x^8-6\,x^9-3\,x^{10}-12\,x^{11}-x^{12}+9\,x^{13}-5\,x^{14}+13\,x^{15}+5\,x^{16}-3\,x^{17}+x^{18}-2\,x^{19}-4\,x^{20}-2\,x^{21}+8\,x^{22}-x^{23}-7\,x^{24}+9\,x^{25}+13\,x^{26}+4\,x^{27}-3\,x^{28}+2\,x^{29}-13\,x^{30}+3\,x^{31}+4\,x^{32}+9\,x^{33}+x^{34}+x^{35}-3\,x^{36}$

$-x^3+x^5-x^6+x^7+x^8-x^{12}+x^{14}+x^{15}-x^{16}+x^{18}+x^{19}-x^{20}+x^{21}-x^{22}-x^{23}-x^{24}+x^{26}+x^{27}-x^{29}-x^{30}+x^{32}+x^{34}+x^{35}$

MEHMET SEVER

11.4. NTRU Kriptosisteminde Mesaj Polinomuna Rotasyon ve İzomorfizma Etkisinin Birlikte İşleyişine Dair Algoritmik Bir Örnek

```
(* FONKSİYONLAR *)

KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-1),{i,1,Length[KL]}]];


KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@KK);


HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];


Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];


Mods[a_,p_]:=Module[
```

```
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];

PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-
1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
  ];
PolinomdanMesajiAl[pol_,x_]:=Module[
  {katsayilar},
  katsayilar=CoefficientList[pol,x];

katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,L
ength[katsayilar]+3-Mod[Length[katsayilar],3]]];
```

```
  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]

  ];


(* SABİTLER *)

alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S
","T","U","V","Y","Z"," "};

M=67; (* M tek olmalı, ancak genelde asal alınır *)

p=7;(* p tek olmalı *)


q=71;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)

 (* TANIMLAMALAR *)

F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus-
>q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];
```

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}$

$1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

$G[x_]=x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

$m[x_]=x^{15}-x^{12}+x^7-1$

$r[x_]=x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3 x+3 x^3+3 x^9+3 x^{12}+3 x^{17}$

$-4+4 x-10 x^2+15 x^3-5 x^4+12 x^5+5 x^6+15 x^7-11 x^8+13 x^9-12 x^{10}+5 x^{11}-x^{12}+x^{13}-6 x^{14}+12 x^{15}-9 x^{16}-13 x^{17}+11 x^{18}-4 x^{19}-8 x^{20}-9 x^{21}+14 x^{22}$

$8+x+4 x^2-8 x^5+5 x^6+10 x^7+3 x^8-14 x^9-5 x^{10}+7 x^{11}-3 x^{12}+14 x^{13}-6 x^{14}-14 x^{15}+8 x^{16}-14 x^{18}+12 x^{19}-15 x^{21}-13 x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15 x-5 x^2-14 x^3+15 x^4-10 x^5+15 x^6-14 x^7+12 x^8-9 x^9-x^{10}-7 x^{11}-10 x^{12}+3 x^{13}-8 x^{14}+8 x^{15}+6 x^{16}-15 x^{17}+10 x^{18}+8 x^{19}+4 x^{20}-15 x^{21}+5 x^{22}$

$5-3 x+6 x^2+3 x^3+6 x^4-5 x^7+3 x^9+3 x^{10}-9 x^{11}-x^{12}+6 x^{13}+7 x^{15}-3 x^{17}-3 x^{19}-6 x^{20}+3 x^{21}+6 x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

$r[x_]=x^{19}-x^{15}+x^{10}+x^8+x^6-x^2;$

mesaj="ABCDEFGHIJKLMNOPRSTUVYZ";

M=2Quotient[StringLength[mesaj],2]+57; (* M tek olmalı, ancak genelde asal alınır *)

k=4;

$p=3^k$;(* p tek olmalı *)

$q=Prime[EulerPhi[k^2\ p]];$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2;$

f[x_]=1+Expand[p F[x]];

$G[x_]=x^{17}+x^{12}+x^9+x^3-x;$

```
g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];


m[x_]=MesajdanPolinomUret[mesaj,x];

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x];

mesaj2=PolinomdanMesajiAl[mm[x],x]

mesaj==mesaj2

 ABCDEFGHIJKLMNOPRSTUVYZ

 True
```

11.5. NTRU Kriptosisteminin Galois Halkaları Üzerindeki İşleyişine Dair Algoritmik Bir Örnek

```
(* FONKSİYONLAR *)

KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-1),{i,1,Length[KL]}]];


KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@KK);
```

```
HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];


Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];


Mods[a_,p_]:=Module[
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];


PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
```

```
  ];

PolinomdanMesajiAl[pol_,x_]:=Module[

  {katsayilar},

  katsayilar=CoefficientList[pol,x];


katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,Length[katsayilar]+3-Mod[Length[katsayilar],3]]];

  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]

  ];


(* SABİTLER *)

alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S","T","U","V","Y","Z"," "};

M=67; (* M tek olmalı, ancak genelde asal alınır *)

p=7;(* p tek olmalı *)


q=71;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)

 (* TANIMLAMALAR *)

F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus-
```

>q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}$

$1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

$G[x_]=x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q]][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

$m[x_]=x^{15}-x^{12}+x^7-1$

$r[x_]=x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

```
a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]
```

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\,x^2-3\,x^4+3\,x^8-3\,x^9+3\,x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\,x+3\,x^3+3\,x^9+3\,x^{12}+3\,x^{17}$

$-4+4\,x-10\,x^2+15\,x^3-5\,x^4+12\,x^5+5\,x^6+15\,x^7-11\,x^8+13\,x^9-12\,x^{10}+5\,x^{11}-x^{12}+x^{13}-6\,x^{14}+12\,x^{15}-9\,x^{16}-13\,x^{17}+11\,x^{18}-4\,x^{19}-8\,x^{20}-9\,x^{21}+14\,x^{22}$

$8+x+4\,x^2-8\,x^5+5\,x^6+10\,x^7+3\,x^8-14\,x^9-5\,x^{10}+7\,x^{11}-3\,x^{12}+14\,x^{13}-6\,x^{14}-14\,x^{15}+8\,x^{16}-14\,x^{18}+12\,x^{19}-15\,x^{21}-13\,x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15\,x-5\,x^2-14\,x^3+15\,x^4-10\,x^5+15\,x^6-14\,x^7+12\,x^8-9\,x^9-x^{10}-7\,x^{11}-10\,x^{12}+3\,x^{13}-8\,x^{14}+8\,x^{15}+6\,x^{16}-15\,x^{17}+10\,x^{18}+8\,x^{19}+4\,x^{20}-15\,x^{21}+5\,x^{22}$

$5-3\,x+6\,x^2+3\,x^3+6\,x^4-5\,x^7+3\,x^9+3\,x^{10}-9\,x^{11}-x^{12}+6\,x^{13}+7\,x^{15}-3\,x^{17}-3\,x^{19}-6\,x^{20}+3\,x^{21}+6\,x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

```
r[x_]=x^19-x^15+x^10+x^8+x^6-x^2;

mesaj="ABCDEFGHIJKLMNOPRSTUVYZ";

M=2Quotient[StringLength[mesaj],2]+57; (* M tek olmalı, ancak genelde asal alınır *)
```

```
k=4;

p=3^k;(* p tek olmalı *)

q=Prime[EulerPhi[k^2 p]];

F[x_]=x^18-x^9+x^8-x^4-x^2;

f[x_]=1+Expand[p F[x]];

G[x_]=x^17+x^12+x^9+x^3-x;

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=MesajdanPolinomUret[mesaj,x];

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+Konvolusyon[m[x],x^k,M,x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x];

mesaj2=PolinomdanMesajiAl[mm[x],x]

mesaj==mesaj2

 ABCDEFGHIJKLMNOPRSTUVYZ

 True
```

11.6. NTRU Kriptosisteminde m Mesaj Polinomuna Bir İzomorfizma Etkisi ve İşleyişine Dair Algoritmik Bir Örnek

```
(* FONKSİYONLAR *)
```

```
KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-1),{i,1,Length[KL]}]];

KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@KK);

HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];

Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];

Mods[a_,p_]:=Module[
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];

PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
```

```
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-
1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
  ];
PolinomdanMesajiAl[pol_,x_]:=Module[
  {katsayilar},
  katsayilar=CoefficientList[pol,x];

katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,L
ength[katsayilar]+3-Mod[Length[katsayilar],3]]];
  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]
  ];

(* SABİTLER *)
alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S
","T","U","V","Y","Z"," "};
M=67; (* M tek olmalı, ancak genelde asal alınır *)
p=7;(* p tek olmalı *)

q=71;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)
 (* TANIMLAMALAR *)
```

F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}$

$1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

$G[x_]=x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

m[x_]=$x^{15}-x^{12}+x^7-1$

r[x_]=$x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\ x+3\ x^3+3\ x^9+3\ x^{12}+3\ x^{17}$

$-4+4\ x-10\ x^2+15\ x^3-5\ x^4+12\ x^5+5\ x^6+15\ x^7-11\ x^8+13\ x^9-12\ x^{10}+5\ x^{11}-x^{12}+x^{13}-6\ x^{14}+12\ x^{15}-9\ x^{16}-13\ x^{17}+11\ x^{18}-4\ x^{19}-8\ x^{20}-9\ x^{21}+14\ x^{22}$

$8+x+4\ x^2-8\ x^5+5\ x^6+10\ x^7+3\ x^8-14\ x^9-5\ x^{10}+7\ x^{11}-3\ x^{12}+14\ x^{13}-6\ x^{14}-14\ x^{15}+8\ x^{16}-14\ x^{18}+12\ x^{19}-15\ x^{21}-13\ x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15\ x-5\ x^2-14\ x^3+15\ x^4-10\ x^5+15\ x^6-14\ x^7+12\ x^8-9\ x^9-x^{10}-7\ x^{11}-10\ x^{12}+3\ x^{13}-8\ x^{14}+8\ x^{15}+6\ x^{16}-15\ x^{17}+10\ x^{18}+8\ x^{19}+4\ x^{20}-15\ x^{21}+5\ x^{22}$

$5-3\ x+6\ x^2+3\ x^3+6\ x^4-5\ x^7+3\ x^9+3\ x^{10}-9\ x^{11}-x^{12}+6\ x^{13}+7\ x^{15}-3\ x^{17}-3\ x^{19}-6\ x^{20}+3\ x^{21}+6\ x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

```
 mesaj="ABCDEFGHIJKL";

derm=StringLength[mesaj]*3-1;

M=2Quotient[StringLength[mesaj],2]+300; (* M tek olmalı, ancak genelde asal alınır *)

k=RandomInteger[{1,Min[M-derm-1,15]}](* Esas denklem bu şekilde: RandomInteger[{1,M-derm-1}] ancak k değerini çok büyük alırsak Mathematica hesaplamayı yapamıyor.*)

p=3^k;(* p tek olmalı *)

q=Prime[EulerPhi[k^2 p]];

F[x_]=x^18-x^9+x^8-x^4-x^2;

f[x_]=1+Expand[p F[x]];

G[x_]=x^17+x^12+x^9+x^3-x;

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q]][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=MesajdanPolinomUret[mesaj,x];

m2[x_]=m[x]x^k//Expand;

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m2[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x];

mm2[x_]=PolynomialRemainder[mm[x]x^M-k,x^M-1,x];
```

```
mesaj2=PolinomdanMesajiAl[mm2[x],x];

mesaj==mesaj2

 13

 True
```

11.7. NTRU Kriptosisteminde Modüllerin Polinom Olarak Seçilmesine Dair Algoritmik Bir Örnek

```
 (* FONKSİYONLAR *)

KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-
1),{i,1,Length[KL]}]];



KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@K
K);



HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolin
omGetir[RandomChoice[KatKum,N],x];



Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];



Mods[a_,p_]:=Module[
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];
```

```
PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-
1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
  ];
PolinomdanMesajiAl[pol_,x_]:=Module[
  {katsayilar},
  katsayilar=CoefficientList[pol,x];

katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,L
ength[katsayilar]+3-Mod[Length[katsayilar],3]]];
  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]
  ];

(* SABİTLER *)
```

```
alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S
","T","U","V","Y","Z"," "};

M=67; (* M tek olmalı, ancak genelde asal alınır *)

p=7;(* p tek olmalı *)


q=71;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)

 (* TANIMLAMALAR *)

F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus-
>q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

 -1+x^4+x^6+x^7+x^9+x^11+x^12-x^13-x^14-x^17-x^19-x^21

 1+x+x^4-x^6+x^7+x^9+x^10+x^11-x^13-x^14-x^15-x^17-x^18+x^19+x^20
```

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

F[x_]=$x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

G[x_]=$x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

m[x_]=$x^{15}-x^{12}+x^7-1$

r[x_]=$x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\ x+3\ x^3+3\ x^9+3\ x^{12}+3\ x^{17}$

$-4+4\ x-10\ x^2+15\ x^3-5\ x^4+12\ x^5+5\ x^6+15\ x^7-11\ x^8+13\ x^9-12\ x^{10}+5\ x^{11}-x^{12}+x^{13}-6\ x^{14}+12\ x^{15}-9\ x^{16}-13\ x^{17}+11\ x^{18}-4\ x^{19}-8\ x^{20}-9\ x^{21}+14\ x^{22}$

$8+x+4\ x^2-8\ x^5+5\ x^6+10\ x^7+3\ x^8-14\ x^9-5\ x^{10}+7\ x^{11}-3\ x^{12}+14\ x^{13}-6\ x^{14}-14\ x^{15}+8\ x^{16}-14\ x^{18}+12\ x^{19}-15\ x^{21}-13\ x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15\,x-5\,x^2-14\,x^3+15\,x^4-10\,x^5+15\,x^6-14\,x^7+12\,x^8-9\,x^9-x^{10}-7\,x^{11}-10\,x^{12}+3\,x^{13}-8\,x^{14}+8\,x^{15}+6\,x^{16}-15\,x^{17}+10\,x^{18}+8\,x^{19}+4\,x^{20}-15\,x^{21}+5\,x^{22}$

$5-3\,x+6\,x^2+3\,x^3+6\,x^4-5\,x^7+3\,x^9+3\,x^{10}-9\,x^{11}-x^{12}+6\,x^{13}+7\,x^{15}-3\,x^{17}-3\,x^{19}-6\,x^{20}+3\,x^{21}+6\,x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

```
mesaj="ABCDEFGHIJKL";

derm=StringLength[mesaj]*3-1;

M=2Quotient[StringLength[mesaj],2]+300; (* M tek olmalı, ancak genelde asal alınır *)

k=RandomInteger[{1,Min[M-derm-1,15]}](* Esas denklem bu şekilde: RandomInteger[{1,M-derm-1}] ancak k değerini çok büyük alırsak Mathematica hesaplamayı yapamıyor.*)

p=3^k;(* p tek olmalı *)

q=Prime[EulerPhi[k^2 p]];

F[x_]=x^18-x^9+x^8-x^4-x^2;

f[x_]=1+Expand[p F[x]];

G[x_]=x^17+x^12+x^9+x^3-x;

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];
```

```
θi_[x_]:=θi[x]=SelectFirst[({{-1,#[[1]]},{0,#[[2]]},{1,#[[3]]}}&/@Permutations[{-
1,0,1}])[[i+1]],#[[1]]==x&][[2]];

θ̆i_[x_]:=θ̆i[x]=SelectFirst[({{-1,#[[1]]},{0,#[[2]]},{1,#[[3]]}}&/@Permutations[{-
1,0,1}])[[i+1]],#[[2]]==x&][[1]];

γ[i_]:=γ[i]=Mod[i,6];

ϕγ_[m_,θ_,x_]:=Module[
  {i,katsayiListesi=CoefficientList[m[x],x],yeniKatsayiListesi={},katsayi},
  For[i=1,i<=Length[katsayiListesi],i++,
   katsayi=katsayiListesi[[i]];
   AppendTo[yeniKatsayiListesi,θγ[i-1][katsayi]];
   ];
  KatsayiListesindenPolinomGetir[yeniKatsayiListesi,x]
 ];
m[x_]=MesajdanPolinomUret[mesaj,x]
m2[x_]=ϕγ[m,θ,x];
r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];
y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m2[x],q,x];
a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];
mm[x_]=PolynomialMods[a[x],p,x];
mm2[x_]=ϕγ[mm,θ̆,x]
mesaj2=PolinomdanMesajiAl[mm2[x],x];
mesaj
```

mesaj2

mesaj==mesaj2

13

$-1-x-x^3-x^4+x^5-x^6-x^8-x^9-x^{12}+x^{14}-x^{15}+x^{16}-x^{17}-x^{18}+x^{19}-x^{21}+x^{22}+x^{23}-x^{25}-x^{26}-x^{28}-x^{31}+x^{32}-x^{35}$

$-1-x-x^3-x^4+x^5-x^6-x^8-x^9-x^{12}+x^{14}-x^{15}+x^{16}-x^{17}-x^{18}+x^{19}-x^{21}+x^{22}+x^{23}-x^{25}-x^{26}-x^{28}-x^{31}+x^{32}-x^{35}$

ABCDEFGHIJKL

ABCDEFGHIJKL

True

ABCDEFGHIJKL==List<>VG<>{A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,P,R,S,T,U,V,Y,Z, }[[25]]<>HUCSJDKH

Permutations[{-1,0,1}]

{{-1,0,1},{-1,1,0},{0,-1,1},{0,1,-1},{1,-1,0},{1,0,-1}}

MapThread[f,{{-1,0,1},{{-1,0,1},{-1,1,0},{0,-1,1},{0,1,-1},{1,-1,0},{1,0,-1}}}]

MapThread[f,{{-1,0,1},{{-1,0,1},{-1,1,0},{0,-1,1},{0,1,-1},{1,-1,0},{1,0,-1}}}]

{{-1,#[[1]]},{0,#[[2]]},{1,#[[3]]}}&/@Permutations[{-1,0,1}]

{{{-1,-1},{0,0},{1,1}},{{-1,-1},{0,1},{1,0}},{{-1,0},{0,-1},{1,1}},{{-1,0},{0,1},{1,-1}},{{-1,1},{0,-1},{1,0}},{{-1,1},{0,0},{1,-1}}}

m[x]

$-1-x-x^3-x^4+x^5-x^6-x^8-x^9-x^{12}+x^{14}-x^{15}+x^{16}-x^{17}-x^{18}+x^{19}-x^{21}+x^{22}+x^{23}-x^{25}-x^{26}-x^{28}-x^{31}+x^{32}-x^{35}$

kat=CoefficientList[m[x],x]

{-1,-1,0,-1,-1,1,-1,0,-1,-1,0,0,-1,0,1,-1,1,-1,-1,1,0,-1,1,1,0,-1,-1,0,-1,0,0,-1,1,0,0,-1}

ϕγ[m,x]

{-1,-1,-1,0,1,-1,-1,1,0,0,-1,0,-1,1,1,0,0,1,-1,0,-1,0,0,-1,0,-1,0,1,1,0,0,-1,1,1,-1,1}

KatsayiListesindenPolinomGetir[{-1,-1,-1,0,1,-1,-1,1,0,0,-1,0,-1,1,1,0,0,1,-1,0,-1,0,0,-1,0,-1,0,1,1,0,0,-1,1,1,-1,1}]

KatsayiListesindenPolinomGetir[{-1,-1,-1,0,1,-1,-1,1,0,0,-1,0,-1,1,1,0,0,1,-1,0,-1,0,0,-1,0,-1,0,1,1,0,0,-1,1,1,-1,1}]

11.8. NTRU Kriptosisteminde Modüllerin Polinom Olarak Seçilmesine Dair Algoritmik Bir Örnek

(* FONKSİYONLAR *)

KatsayiListesindenPolinomGetir[KL_,x_]:=Module[{i},Sum[KL[[i]]*x^(i-1),{i,1,Length[KL]}]];

KatsayiKuralindanPolinomGetir[KK_,x_]:=Plus@@(#[[2]]x^#[[1]][[1]]&/@KK);

HalkadanRastgelePolinomSec[N_,KatKum_,x_]:=KatsayiListesindenPolinomGetir[RandomChoice[KatKum,N],x];

Konvolusyon[f_,g_,N_,x_]:=PolynomialMod[f g,x^N-1];

```
Mods[a_,p_]:=Module[
  {b=Mod[a,p],r},
  If[b-p<-((p-1)/2),r=b,r=b-p];
  r
  ];

PolynomialMods[pol_,p_,x_]:=Module[
  {katsayilar=CoefficientList[pol,x]},
  katsayilar=Mods[#,p]&/@katsayilar;
  KatsayiListesindenPolinomGetir[katsayilar,x]
  ];
MesajdanPolinomUret[m_,x_]:=Module[
  {harfKonumlari,mKatsayiListesi},
  harfKonumlari=FirstPosition[alfabe,#][[1]]&/@ Characters[m];
  mKatsayiListesi=#-
1&/@(PadLeft[IntegerDigits[#,3],3]&/@harfKonumlari//Flatten);
  KatsayiListesindenPolinomGetir[mKatsayiListesi, x]
  ];
PolinomdanMesajiAl[pol_,x_]:=Module[
  {katsayilar},
  katsayilar=CoefficientList[pol,x];
```

```
katsayilar=If[Mod[Length[katsayilar],3]==0,katsayilar,PadRight[katsayilar,Length[katsayilar]+3-Mod[Length[katsayilar],3]]];

  StringJoin[alfabe[[#]]&/@(FromDigits[#+1,3]&/@Partition[katsayilar,3])]

  ];


(* SABİTLER *)

alfabe={"A","B","C","D","E","F","G","H","I","J","K","L","M","N","O","P","R","S","T","U","V","Y","Z"," "};

M=67; (* M tek olmalı, ancak genelde asal alınır *)

p=7;(* p tek olmalı *)


q=71;(* q, p den biraz büyük olmalı ve (p,q)=1 olmalı *)

 (* TANIMLAMALAR *)

F[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

G[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

f[x_]=1+Expand[p F[x]];

g[x_]=Expand[p G[x]];

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q][[2,1]],q,x];

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x];

m[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x]

r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x];
```

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x];

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}$

$1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$-1+x^4+x^6+x^7+x^9+x^{11}+x^{12}-x^{13}-x^{14}-x^{17}-x^{19}-x^{21}==1+x+x^4-x^6+x^7+x^9+x^{10}+x^{11}-x^{13}-x^{14}-x^{15}-x^{17}-x^{18}+x^{19}+x^{20}$

$F[x_]=x^{18}-x^9+x^8-x^4-x^2$

f[x_]=1+Expand[p F[x]]

$G[x_]=x^{17}+x^{12}+x^9+x^3-x$

g[x_]=Expand[p G[x]]

f_q[x_]=PolynomialMods[PolynomialExtendedGCD[f[x],x^M-1,x,Modulus->q]][[2,1]],q,x]

h[x_]=PolynomialMods[Konvolusyon[f_q[x],g[x],M,x],q,x]

$m[x_]=x^{15}-x^{12}+x^7-1$

$r[x_]=x^{19}+x^{10}+x^6-x^2$

y[x_]=PolynomialMods[Konvolusyon[r[x],h[x],M,x]+m[x],q,x]

a[x_]=PolynomialMods[Konvolusyon[f[x],y[x],M,x],q,x]

mm[x_]=PolynomialMods[a[x],p,x]

m[x]==mm[x]

$-x^2-x^4+x^8-x^9+x^{18}$

$1-3\ x^2-3\ x^4+3\ x^8-3\ x^9+3\ x^{18}$

$-x+x^3+x^9+x^{12}+x^{17}$

$-3\,x+3\,x^3+3\,x^9+3\,x^{12}+3\,x^{17}$

$-4+4\,x-10\,x^2+15\,x^3-5\,x^4+12\,x^5+5\,x^6+15\,x^7-11\,x^8+13\,x^9-12\,x^{10}+5\,x^{11}-x^{12}+x^{13}-6\,x^{14}+12\,x^{15}-9\,x^{16}-13\,x^{17}+11\,x^{18}-4\,x^{19}-8\,x^{20}-9\,x^{21}+14\,x^{22}$

$8+x+4\,x^2-8\,x^5+5\,x^6+10\,x^7+3\,x^8-14\,x^9-5\,x^{10}+7\,x^{11}-3\,x^{12}+14\,x^{13}-6\,x^{14}-14\,x^{15}+8\,x^{16}-14\,x^{18}+12\,x^{19}-15\,x^{21}-13\,x^{22}$

$-1+x^7-x^{12}+x^{15}$

$-x^2+x^6+x^{10}+x^{19}$

$-3-15\,x-5\,x^2-14\,x^3+15\,x^4-10\,x^5+15\,x^6-14\,x^7+12\,x^8-9\,x^9-x^{10}-7\,x^{11}-10\,x^{12}+3\,x^{13}-8\,x^{14}+8\,x^{15}+6\,x^{16}-15\,x^{17}+10\,x^{18}+8\,x^{19}+4\,x^{20}-15\,x^{21}+5\,x^{22}$

$5-3\,x+6\,x^2+3\,x^3+6\,x^4-5\,x^7+3\,x^9+3\,x^{10}-9\,x^{11}-x^{12}+6\,x^{13}+7\,x^{15}-3\,x^{17}-3\,x^{19}-6\,x^{20}+3\,x^{21}+6\,x^{22}$

$-1+x^7-x^{12}+x^{15}$

True

```
mesaj="ABCDEFGHIJKL";

derm=StringLength[mesaj]*3-1;

M=2derm+13; (* M tek olmalı, ancak genelde asal alınır *)

p=3;(* p tek olmalı *)

q=97;

F[x_]=x^18-x^9+x^8-x^4-x^2;

f[x_]=1+Expand[p F[x]];

G[x_]=x^17+x^12+x^9+x^3-x;

g[x_]=Expand[p G[x]];
```

```
fq[x_]=PolynomialRemainder[PolynomialMods[PolynomialExtendedGCD[f[
x],x^M-1,x,Modulus->q][[2,1]],q,x],Q[x],x];

h[x_]=PolynomialRemainder[PolynomialMods[Konvolusyon[fq[x],g[x],M,x],
q,x],Q[x],x];

Q[x_]=Module[

  {qq},

  qq[x_]=HalkadanRastgelePolinomSec[derm +4,{-1,0,1},x];

  While[PolynomialGCD[qq[x],x^M-1]!=1,

   qq[x_]=HalkadanRastgelePolinomSec[M-1,{-1,0,1},x]

   ];

  qq[x]

  ];

P[x_]=Module[

  {pp},

  pp[x_]=HalkadanRastgelePolinomSec[derm +1,{-1,0,1},x];

  While[PolynomialGCD[pp[x],x^M-1]!=1||PolynomialGCD[pp[x],Q[x]]!=1,

   pp[x_]=HalkadanRastgelePolinomSec[derm+1,{-1,0,1},x]

   ];

  pp[x]

  ];

Pq[x_]=PolynomialExtendedGCD[P[x],Q[x],x][[2,1]];

m[x_]=MesajdanPolinomUret[mesaj,x]
```

```
r[x_]=HalkadanRastgelePolinomSec[M,{-1,0,1},x];

y[x_]=PolynomialRemainder[PolynomialMods[Konvolusyon[r[x],h[x],M,x]+
P[x]m[x],q,x],Q[x],x];

a[x_]=PolynomialRemainder[PolynomialMods[Konvolusyon[f[x],y[x],M,x],q
,x],Q[x],x];

b[x_]=PolynomialMods[PolynomialRemainder[Pq[x]a[x],Q[x],x],q,x];

mm[x_]=PolynomialMods[b[x],p,x];
```

$$-1-x-x^3-x^4+x^5-x^6-x^8-x^9-x^{12}+x^{14}-x^{15}+x^{16}-x^{17}-x^{18}+x^{19}-x^{21}+x^{22}+x^{23}-x^{25}-x^{26}-x^{28}-x^{31}+x^{32}-x^{35}$$

$$-1-x-x^3-x^4+x^5-x^6-x^8-x^9-x^{12}+x^{14}-x^{15}+x^{16}-x^{17}-x^{18}+x^{19}-x^{21}+x^{22}+x^{23}-x^{25}-x^{26}-x^{28}-x^{31}+x^{32}-x^{35}$$

KAYNAKLAR

[1] Nagpaul, S.R., Jain, S.K. (2005). Topics in Applied Abstract Algebra, 15th Edition, Thomson Learning, Inc., Belmont, USA.

[2] Katz, J., Lindell, Y. (2014). Introduction to Modern Cryptography, CRC Press, Boca Raton, USA.

[3] Yan, S.Y. (2002). Number Theory for Computing, Springer Science and Business Media, Berlin, Germany.

[4] Bauer, C:P. (2013). Secret History: The Story of Cryptology, Rosen, K.H., Editor.; CRC Press, Boca Raton, USA.

[5] Baldoni, M.W., Ciliberto, C., Cattaneo, G.M.P. (2009). Elementary Number Theory, Cryptography and Codes, Springer-Verlag Heidelberg, Berlin, Germany.

[6] Oppliger, R. (2011). Contemporary Cryptography, Artech House, Inc., Norwood, USA.

[7] Talbot, J., Welsh, D. (2006). Complexity and Cryptography: An Introduction, 13rd Edition, Cambridge University Press, Cambridge, UK.

[8] Delfs, H., Knebl, H. (2002). Introduction to Cryptography: Principles and Applications, 2nd Edition, Maurer, U. Editor.; Springer-Verlag Heidelberg, Newyork, USA.

[9] Stinson, D.R., Paterson, M. (2018). Cryptography: Theory and Practice, CRC Press, Boca Raton, USA.

[10] Schneier, B. (2007). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley and Sons, Inc., New Jersey, USA.

[11] Davis, D. M. (1993). The Nature and Power of Mathematics, Princeton University Press, New Jersey, USA.

[12] Paar, C., Pelzl, J. (2009). Understanding Cryptography: a Textbook for Students and Practitioners, Springer Science and Business Media, Berlin, Germany.

[13] Rosen, K.H. (1986). Elementary Number Theory and Its Applications, AT&T Information System Laboratories, Bell Telephone Laboratories, New Jersey,USA.

[14] Menezes, A.J., van Oorschot, P.C., Vanstone, S.A. (1997). Handbook of Applied Cryptography, CRC Press, Boca Raton, USA.

[15] Yan, S.Y. (2013). Computational Number Theory and Modern Cryptography, John Wiley and Sons, Singapore Pte, Ltd., Singapore.

[16] Mollin, R.A. (2002). RSA and Public-Key Cryptography, CRC Press, Boca Raton, USA.

[17] Yan, S. Y. (2013). Quantum Attacks on Public-Key Cryptosystems, Springer US.

[18] Yan, S. Y. (2009). Primality Testing and Integer Factorization in Public-Key Cryptography, Springer Science and Business Media, New York, USA.

[19] Myasnikov, A., Shpilrain, V., Ushakov, A. (2008). Group-Based Cryptography, Springer Science and Business Media, Berlin, Germany.

[20] Chen, K. (Editor). (2004). Progress on Cryptography: 25 Years of Cryptography in China, Kluwer Academic Publishers, Boston, USA.

[21] Robling Denning, D. E. (1982). Cryptography and Data Security, Addison-Wesley Longman Publishing Co., Inc., USA.

[22] Mollin, R.A. (2000). An Introduction to Cryptography, 2nd Edition, CRC Press, Boca Raton, USA.

[23] Alster, K., Urbanowicz, J., Williams, H. C. (Editors.). (2011). Public-Key Cryptography and Computational Number Theory: Proceedings of the International Conference Organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000. Walter de Gruyter, Berlin Germany.

[24] Özdemir, A.Ş. (2015). Sayılar Teorisi Şifreleme ve Sihirli Kare Uygulamalarıyla, Marmara, Üniversitesi Yayınları, İstanbul, Türkiye.

[25] Ağargün, G., Ersoy, B.A., Oral, K.H., Alan, M., Kutan Aygör, N. (2015). Soyut Cebir, Birsen Yayın Dağıtım Ltd. Şti., İstanbul, Türkiye.

[26] Çallıalp, F., Tekir, Ü. (2009). Değişmeli Halkalar ve Modüller, Birsen Yayın Dağıtım Ltd. Şti., İstanbul, Türkiye.

[27] Mullen, G. L., Panario, D. (2013). Handbook of Finite Fields, CRC Press, Boca Raton, USA.

[28] Betten, A., Braun, M., Fripertinger, H., Kerber, A., Kohnert, A., Wassermann, A. (2006). Error-Correcting Linear Codes: Classification by Isometry and Application, 18th Edition, Springer Science and Business Media, Berlin, Germany.

[29] Childs, L.N. (2019). Cryptology and Error Correction: An Algebraic Introduction and Real-World Applications, Springer Nature Switzerland, Cham, Switzerland.

[30] Van Tilborg, H.C.A. (1988). Fundamentals of Cryptology: a Professional Reference and Interactive Tutorial, Kluwer Academic Publishers, Boston, USA.

[31] da Rocha Jr, V.C. (2014). Elements of Algebraic Coding Systems, Momentum Press, New York, USA.

[32] Persichetti, E. (2012) Improving the Efficiency of Code-Based Cryptography. PhD Thesis, University of Auckland, Auckland, New Zeland, 1-142.

[33] Rose, M. (2011). Lattice-Based Cryptography: a Practical Implementation. Master Thesis, University of Wollongong, Wollongong, Australia, 1-105.

[34] McEliece, R.J. (2004). The Theory of Information and Coding, Cambridge University Press, Cambridge, UK.

[35] Huffman, W.C., Pless, V. (2010). Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, UK.

[36] Doumen, J.M. (2003). Some Applications of Coding Theory in Cryptography. PhD Thesis, Technische Universiteit Eindhoven, Eindhoven, The Netherlands.

[37] Ten Valls, R. (2017). Cyclic Codes as Submodules of Rings and Direct Product of Rings, Universitat Autònoma de Barcelona, Barcelana, Spain.

[38] Cohen, H. (1993). A Course in Computational Algebraic Number Theory, 138th Edition, Springer-Verlag Heidelberg, Berlin, Germany.

[39] Kaplansky, I. (1995). Fields and Rings, Chicago Lectures in Mathematica, Reprint of 2nd Edition, University of Chicago Press, Chicago, USA.

[40] Nguyen, H.B. (2014). An Overview On The Ntru Cryptographic System. Master Thesis, San Diego State University, San Diego, USA, 1-49.

[41] Hong, Z. (2001). Survey of Computational Assumptions Used in Cryptography Broken or not by Shor's Algorithm. PhD Thesis, McGill University, Montréal, Canada, 1-86.

[42] Galbraith, S.D. (2012). Mathematics of Public Key Cryptography, Cambridge University Press, New York, USA.

[43] Hoffstein, J., Pipher, J., Silverman, J.H. (2008). An Introduction to Mathematical Cryptography, 1st Edition, Springer Science and Business Media, New York, USA.

[44] Adámek, J. (2011). Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory, John Wiley and Sons, Inc., New Jersey, USA.

[45] Hoffstein, J., Pipher, J., Silverman, J.H. (1996). NTRU: A New High Speed Public Key Cryptosystem. 16th Annual International Cryptology Conference (Crypto' 96), 18-22 August, Santa Barbara, California, USA.

[46] Hoffstein, J., Pipher, J., Silverman, J. H. (1998). NTRU: A Ring-Based Public Key Cryptosystem. Buhler J.P. Editor.; Algorithmic Number Theory, ANTS 1998, Lecture Notes in Computer Science, 1423, 267-288.

[47] Hoffstein, J., Silverman, J. H. (1999). Reaction Attacks Against the NTRU Public Key Cryptosystem. Technical Report 15. https://ntru.org/f/tr/tr015v1.pdf.

[48] Hoffstein, J., Lieman, D., Pipher, J., Silverman, J. H. (1999). NTRU: A Public Key Cryptosystem, NTRU Cryptosystems, Inc. https://www.ntru.com

[49] Singh, S., Padhye, S. (2016). Generalisations of NTRU Cryptosystem. Security and Communication Networks, 9(18), 6315-6334.

[50] Shen, X., Du, Z., Chen, R. (2009). Research on NTRU algorithm for mobile java security. International Conference on Scalable Computing and Communications, 8th International Conference on Embedded Computing . (ScalCom-EmbeddedCom 2009), 25-27 September, Dalian, China.

[51] Zhan, X., Zhang, R., Xiong, Z., Zheng, Z., Liu, Z. (2013). Efficient implementations of NTRU in wireless network. Communications and Network, 5(3C), 485-492.

[52] Howgrave-Graham N., Silverman J.H., Whyte W. (2005) Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3, Menezes, A. Editor.; Topics in Cryptology – CT-RSA 2005, CT-RSA 2005, Lecture Notes in Computer Science, 3376, 118-135.

[53] IEEE P1363 Working Group. (2005). Standard Specifications for Public Key Cryptography. IEEE P1363/D20 (Draft Version 20).

[54] Nitaj, A. (2015). The Mathematics of the NTRU Public Key Cryptosystem. IGI Global.

[55] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Whyte, W. (2009). Practical Lattice-Based Cryptography: NTRUEncrypt and NTRUSign, The LLL Algorithm, Nguyen, P., Vallée, B. Editors.; Springer, Berlin, Heidelberg, Germany.

[56] Gama, N., Nguyen, P. Q. (2008). Predicting Lattice Reduction. Smart N. Editor.; Advances in Cryptology-EUROCRYPT 2008, Lecture Notes in Computer Science, 4965, 31-51.

[57] Howgrave-Graham, N. (2007). A Hybrid Meet-In-The-Middle and Lattice Reduction Attack on NTRU. Menezes A. Editor.; Advances in Cryptology - CRYPTO 2007, Lecture Notes in Computer Science, 4622, 150-169.

[58] Hall, C., Goldberg, I., Schneier, B. (1999). Reaction Attacks Against Several Public-Key Cryptosystem. International Conference on Information and Communications Security (ICICS' 99), Lecture Notes in Computer Science, 1726, 2-12.

[59] Hoffstein, J., Silverman, J. H. (2000). Reaction Attacks Against the NTRU Public Key Cryptosystem. Technical Report 15. https://ntru.org/f/tr/tr015v2.pdf.

[60] Gentry, C. (2001). Key Recovery and Message Attacks on NTRU-Composite. Pfitzmann B. Editor.; Advances in Cryptology-EUROCRYPT 2001, Lecture Notes in Computer Science, 2045, 182-194.

[61] Jaulmes, É., Joux, A. (2000). A Chosen-Ciphertext Attack Against NTRU. Bellare M. Editor.; Advances in Cryptology-CRYPTO 2000, Lecture Notes in Computer Science, 1880, 20-35.

[62] Coppersmith D., Shamir A. (1997). Lattice Attacks on NTRU. Fumy W. Editor.; Advances in Cryptology-EUROCRYPT 1997, Lecture Notes in Computer Science, 1233, 52-61.

[63] Micciancio, D., Voulgaris, P. (2010). Faster Exponential Time Algorithms for the Shortest Vector Problem. Proceedings of the 2st Annual ACM-SIAM Symposium on Discrete Algorithms, Society for Industrial and Applied Mathematics, 1468-1480.

[64] Nguyen P.Q. (2009). Hermite's Constant and Lattice Algorithms, The LLL Algorithm, Nguyen, P., Vallée, B. Editors.; Springer, Berlin, Heidelberg, Germany.

[65] Silverman, J. H. (1998). Plaintext awareness and the NTRU PKCS. Technical Report 07. https://ntru.org/f/tr/tr007v1.pdf.

[66] Silverman, J. H. (1999). Estimated Breaking Times for NTRU Lattices. Technical Report 12. https://ntru.org/f/tr/tr012v1.pdf.

[67] Mol P., Yung M. (2008). Recovering NTRU Secret Key from Inversion Oracles. Cramer R. Editor.; Public Key Cryptography-PKC 2008, Lecture Notes in Computer Science, 4939, 18-36.

[68] Hoffstein, J., Silverman, J. (2001). Optimizations for NTRU. Proceedings of the Conference of Public-Key Cryptography and Computational Number Theory, 77-88.

[69] Hoffstein, J., Howgrave-Graham, N., Pipher, J., Silverman, J. H., Whyte, W. (2007). Hybrid Lattice Reduction and Meet in the Middle Resistant Parameter Selection for NTRU-Encrypt. Submission/contribution to IEEE, p1363, 1(2007-02), 1.

[70] Hirschhorn, P. S., Hoffstein, J., Howgrave-Graham, N., Whyte, W. (2009). Choosing NTRUEncrypt Parameters in Light of Combined Lattice Reduction and MITM Approaches. Abdalla M., Pointcheval D., Fouque P.A., Vergnaud D. Editors; Applied Cryptography and Network Security, ACNS 2009, Lecture Notes in Computer Science, 5536, 437-455.

[71] Gaborit, P., Ohler, J., Solé, P. (2002). CTRU, a Polynomial Analogue of NTRU. INRIA 2002, Rapport de recherche, RR-4621. http://www.inria.fr/rrrt/rr-4621.html.

[72] Coglianese, M., Goi, B. M. (2005). MaTRU: A New NTRU-Based Cryptosystem. Maitra S., Veni Madhavan C.E., Venkatesan R. Editors.; Progress in Cryptology - INDOCRYPT 2005, Lecture Notes in Computer Science, 3797, 232-243.

[73] Kouzmenko, R. (2006). Generalizations of the NTRU cryptosystem. Diploma Project, École Polytechnique Fédérale de Lausanne, Winter Semester 2005–2006.

[74] Malekian E., Zakerolhosseini A. (2010). NTRU-Like Public Key Cryptosystems beyond Dedekind Domain up to Alternative Algebra. Gavrilova M.L., Tan C.J.K., Moreno E.D. Editors.; Transactions on Computational Science X, Lecture Notes in Computer Science, 6340, 25-41.

[75] Jarvis, K., Nevins, M. (2015). ETRU: NTRU over the Eisenstein Integers. Designs, Codes and Cryptography, 74(1), 219-242.

[76] Malekian, E., Zakerolhosseini, A., Mashatan, A. (2011). QTRU: Quaternionic Version of the NTRU Public-Key Cryptosystems. ISeCure-The ISC International Journal of Information Security, 3(1), 29-42.

[77] Banks, W.D., Shparlinski, I.E. (2002). A Variant of NTRU with Non-Invertible Polynomials. Menezes A., Sarkar P. Editors.; Progress in Cryptology-INDOCRYPT 2002, Lecture Notes in Computer Science, 2551, 62-70.

[78] Nayak, R., Sastry, C. V., Pradhan, J. (2008). A Matrix Formulation for NTRU Cryptosystem. 16th IEEE International Conference on Networks, 12-14 December, New Delhi, India.

[79] Malekian, E., Zakerolhosseini, A., Mashatan, A. (2009). QTRU: A Lattice Attack Resistant Version of NTRU PKCS Based on Quaternion Algebra. Preprint, Available from the Cryptology ePrint Archive: https://eprint.iacr.org/2009/386.pdf.

[80] Nanda, A. K., Nayak, R., Awasthi, L. K. (2015). NTRU with Gaussian Integer Matrix. Journal of Advanced Research in Computer Science and Software Engineering, 5, 359-365.

[81] Hoffstein, J., Pipher, J., Silverman, J. H. (2001). NSS: An NTRU Lattice-Based Signature Scheme. Pfitzmann B. Editor.; Advances in Cryptology-EUROCRYPT 2001, Lecture Notes in Computer Science, 2045, 211-228.

[82] Mironov, I. (2001). A Note on Cryptanalysis of the Preliminary Version of the NTRU Signature Scheme. Available from the Cryptology ePrint Archive: https://eprint.iacr.org/2001/005.pdf.

[83] Hoffstein, J., Pipher, J., Silverman, J. H. (2001). Enhanced Encoding and Verification Methods for the NTRU Signature Scheme. Technical Report 17. https://ntru.org/f/tr/tr017v2.pdf.

ÖZGEÇMİŞ

1985 yılında Gaziantep' te doğdu. İlk, orta ve lise öğrenimini aynı şehirde tamamladı. Lisans öğrenimini 2008 yılında Kahramanmaraş Sütçü İmam Üniversitesi Matematik Bölümü' nde ve yüksek lisans öğrenimini 2012 yılında Atatürk Üniversitesi Matematik Anabilim Dalı' nda tamamladı. Doktora öğrenimine Marmara Üniversitesi Matematik Anabilim Dalı' nda devam etmektedir. Halen, Ağrı İbrahim Çeçen Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü' nde araştırma görevlisi olarak çalışmaktadır.