T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

NTRU BENZERİ BAZI KRİPTOSİSTEMLER VE KARŞILAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Gülbahar ÇAL
Danışman: Dr. Öğr. Üyesi Ömer KÜSMÜŞ

VAN – 2025

T.C.
VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI

NTRU BENZERİ BAZI KRİPTOSİSTEMLER VE KARŞILAŞTIRILMASI

YÜKSEK LİSANS TEZİ

Gülbahar ÇAL

Tez Savunma Sınavı Jüri Üyeleri

Dr. Öğr. Üyesi Murat AK (Başkan)

Dr. Öğr. Üyesi Ömer KÜSMÜŞ (Danışman)

Dr. Öğr. Üyesi Turgut HANOYMAK (Üye)

VAN – 2025

KABUL VE ONAY SAYFASI

Van Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü, Matematik Anabilim Dalı'nda Dr. Öğr. Üyesi Ömer KÜSMÜŞ danışmanlığında, Gülbahar ÇAL tarafından sunulan "NTRU Benzeri Bazı Kriptosistemler ve Karşılaştırılması" başlıklı bu çalışma Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili hükümleri gereğince 01 /09 /2025 tarihinde aşağıdaki jüri tarafından oy birliği ile başarılı bulunmuş ve yüksek lisans tezi olarak kabul edilmiştir.

Başkan: Dr. Öğr. Üyesi Murat AK İmza:

Üye: Dr. Öğr. Üyesi Ömer KÜSMÜŞ İmza:

Üye: Dr. Öğr. Üyesi Turgut HANOYMAK İmza:

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun …. /.... /….. tarih ve ..... sayılı kararı ile onaylanmıştır.

İmza

……

Enstitü Müdürü

ETİK BEYAN

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

İmza
Gülbahar ÇAL

ÖZET

NTRU BENZERİ BAZI KRİPT66OSİSTEMLER VE KARŞILAŞTIRILMASI

ÇAL, Gülbahar
Yüksek Lisans Tezi, Matematik Anabilim Dalı
Danışman: Dr. Öğr. Üyesi Ömer KÜSMÜŞ
Eylül 2025, 67 sayfa

Bu tez beş bölümden oluşmaktadır. Birinci bölümde, açık anahtarlı kriptosistemlerin ardında yatan matematiksel zor problemlere ve kuantum bilgisayarlara karşı mevcut kriptosistemlerin durumuna değinilen giriş niteliğinde bilgilere yer verilmiştir.

İkinci bölümde, kuantum kriptografide önemli bir yeri olan NTRU kriptosistemi ve NTRU benzeri oluşturulan bazı kriptosistemlerle ilgili literatürde mevcut olan çalışmalara ilişkin kaynak bildirişleri sunulmuştur.

Üçüncü bölümde, polinom halkaları, kafes teorisi, NTRU ve benzeri kriptosistemlerin güvenliğinin dayandığı en kısa vektör problemi (SVP) ve en yakın vektör problemi (CVP) gibi kafes teorisinde yer alan matematiksel zor problemlere dair bazı bilgiler aktarılmıştır.

Dördüncü bölümde, teorik temelleri ve uygun parametre seçimi yapılarak elde edilen bir anahtar örneğiyle somut bir mesaj şifrelenip deşifrelenerek NTRU kriptosisteminde anahtar üretimi, şifreleme ve deşifreleme işlemlerinin nasıl yapıldığı aktarılmış ve MaTRU, CTRU, DTRU, ETRU ve QTRU gibi NTRU benzeri bazı kriptosistemler çalışılmıştır.

Beşinci bölümde, kuantum saldırılarına karşı NTRU kriptosisteminin sağladığı güvenlik ve etkililiğin, ele alınan NTRU benzeri diğer kriptosistemlerle kıyaslandığı bir tartışmaya yer verilmiştir.

Anahtar kelimeler: Açık anahtarlı kriptosistem, CTRU, DTRU, ETRU, Kafes, Kriptografi, Kuantum, MaTRU, NTRU, Saldırı, QTRU

ABSTRACT

SOME NTRU-LIKE CRYPTOSYSTEMS AND THEIR COMPARISONS

ÇAL, Gülbahar
M.Sc. Thesis, Department of Mathematics
Supervisor: Assist. Prof. Dr. Ömer KÜSMÜŞ
September 2025, 67 pages

This thesis consists of five chapters. The first chapter presents introductory information concerning the mathematically hard problems underlying public-key cryptosystems and the current status of existing cryptographic systems in the face of quantum computing.

The second chapter provides references to the existing literature on the NTRU cryptosystem—which holds a prominent place in quantum cryptography—as well as to several NTRU-like cryptosystems that have been developed subsequently.

In the third chapter, some fundamental notions related to polynomial rings, lattice theory, and the mathematically hard problems within this theory—such as the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP), which underpin the security of NTRU and related cryptosystems—are explained.

In the fourth chapter, the processes of key generation, encryption, and decryption in the NTRU cryptosystem are demonstrated by encrypting and decrypting a concrete message using a key generated through appropriate parameter selection based on theoretical foundations. Additionally, several NTRU-like cryptosystems such as MaTRU, CTRU, DTRU, ETRU and QTRU are examined in detail.

The fifth chapter offers a comparative discussion evaluating the security and efficiency of the NTRU cryptosystem against quantum attacks, in comparison with other NTRU-like cryptosystems addressed in the study.

Keywords: Attack, Cryptography, CTRU, DTRU, ETRU, Lattice, MaTRU, NTRU, Public key cryptosystem, QTRU, Quantum

TEŞEKKÜR

Bu tez çalışmasında, akademik olarak yardımlarıyla her türlü desteği bana sunan danışmanım Sayın Dr. Öğr. Üyesi Ömer KÜSMÜŞ'e ve beni lisans eğitimimden bu yana lisansüstü eğitim hususunda cesaretlendiren Sayın Dr. Öğr. Üyesi Turgut HANOYMAK'a teşekkür ederim. Ayrıca, bugüne kadar maddi ve manevi hiçbir desteğini benden esirgemeyen anne ve babama teşekkürlerimi sunarım.

2025

Gülbahar ÇAL

İÇİNDEKİLER

Sayfa

ÇİZELGELER LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamalarıyla aşağıda sunulmuştur.

Simgeler	**Açıklama**
$\subset$	Altküme
$\subseteq$	Altküme veya eşittir
$\Leftrightarrow$	Ancak ve ancak
$\exists$	Bazı
$>$	Büyüktür
$\geq$	Büyük veya eşittir
$\mathbb{N}$	Doğal sayılar kümesi
$\notin$	Elemanı değildir
$\in$	Elemanıdır
$\neq$	Eşit değildir
$=$	Eşittir
$\forall$	Her
$\mathcal{L}$	Kafes
$\mathbb{C}$	Kompleks sayılar kümesi
$<$	Küçüktür
$\leq$	Küçük veya eşittir
$\det(\mathcal{L})$	$\mathcal{L}$ kafesinin determinantı
$\mathbb{Z}$	Tamsayılar kümesi
$\langle p(x) \rangle$	$p(x)$ tarafından üretilen ideal
$\mathbb{Q}$	Rasyonel sayılar kümesi
$\mathbb{R}$	Reel sayılar kümesi
$\wedge$	Ve
$\vee$	Veya
$\approx$	Yaklaşık

Kısaltmalar	**Açıklama**
CVP	En Yakın Vektör Problemi
LLL	Lenstra-Lenstra-Lovasz Kafes İndirgeme Metodu
SVP	En Kısa Vektör Problemi

1. GİRİŞ

Açık anahtarlı kriptografi kavramı ilk kez 1976 yılında W. Diffie ve M. Hellman tarafından ortaya atılmıştır (Diffie ve Hellman, 1976). Bu yaklaşım, klasik simetrik şifreleme yöntemlerinin güvenlik açısından yetersiz kalmasından doğan bir ihtiyaç sonucu geliştirilmiştir. O zamandan bu yana birçok açık anahtarlı şifreleme sistemi (PKC) tasarlanmış ve araştırmacılar tarafından analiz edilerek güvenlik açıkları tespit edilmiştir. Açık anahtarlı kriptografi, dijital imzalar, anahtar dağıtımı ve anahtar değişim protokolleri gibi birçok temel kavramı içerir. Bu kavramlardan anahtar değişim protokolleri ve dijital imzalarla ilgili literatüre bakıldığında, Nathani ve Tripathi'nin (2017) kuaterniyonlar üzerinde anahtar değişim protokolleri konusundaki çalışması ve Satoh ve Araki'nin (1997), değişmeli olmayan bazı cebirsel yapılar üzerinde imza şeması tasarımı ile ilgili çalışması göze çarpmaktadır.

Hem simetrik hem de asimetrik kriptografik sistemlerin bazı matematiksel olarak zor problemlere dayanması gerektiği iyi bilinmektedir. Örneğin, RSA şifreleme sistemi, büyük bir bileşik sayı N için mod N işlemindeki kalan sınıflarının toplamsal abelyen grubu $\mathbb{Z}_N$'deki çarpımsal tersinir elemanlara (birimsellere) dayanır (Rivest vd., 1978). Bu nedenle RSA'nın güvenliği, büyük bileşik sayıların çarpanlara ayrılması probleminin zorluğuna bağlıdır. Diğer bir bilinen açık anahtarlı sistem olan ElGamal şifreleme algoritması ise, $\mathbb{Z}_N$'deki çarpımsal tersinir elemanların grubu olan $\mathbb{Z}_N^*$'daki ayrık logaritma probleminin zorluğuna dayanır (ElGamal, 1985).

Kuantum bilgisayarların gelişmesi ve özellikle Shor algoritmasının ortaya konması, hem çarpanlara ayırma hem de ayrık logaritma problemlerini etkin bir şekilde çözebilme yetisiyle bu sistemleri tehdit etmektedir (Shor, 1997). Bu sistemlerin güvenliğini sağlamak adına araştırmacılar, cebirsel ve sayı kuramsal yapıların bu sistemlere entegre edilmesi gerektiğini fark etmişlerdir. Örneğin, Hurley ve Hurley (2011), klasik sistemler olan RSA ve ElGamal yerine grup halkaları temelli yapılarla daha güçlü ve verimli kriptografik sistemler geliştirilebileceğini öne sürmüş ve ayrıca, eşlenik arama probleminin zorluğu nedeniyle, cebirsel temelli kriptosistemlerin, sayılar teorisi temelli sistemlere kıyasla daha güçlü olabileceğini belirtmiştir.

Güncel araştırmalarda, cebirsel olarak zor problemler bağlamında halkalar ve bu halkaların özel elemanlarına dayalı yeni şifreleme yaklaşımlarına yönelim artmıştır.

(Banin ve Tsaban, 2012) çalışmasında ayrık logaritma problemi Bergman'ın temsil edilemeyen halkası üzerinde ele alınmıştır. Mumtaz ve Ping (2019), RSA sistemine yönelik mevcut saldırıları ele alan kapsamlı bir derleme sunmuştur. Liu ve Ye (2018), hafif anahtar üretimi sağlayan kimliğe dayalı yeniden şifreleme yöntemi önermiştir. Inam ve Ali (2018), grup halkalarında tanımlı döngüsel matris grupları üzerinde inşa edilen yeni bir açık anahtarlı şifreleme sistemi tasarlamış ve güvenliğini analiz etmişlerdir. (Hanoymak ve Küsmüş, 2015)'te, sonlu devirli grupların integral grup halkalarının birimsel gruplarına dayalı simetrik ve asimetrik şifreleme sistemleri önerilmiştir. Bu protokolde, yalnızca tek taraflı konvolüsyon yöntemiyle mesajın şifrelenmesi sağlanmıştır, fakat bu yaklaşım seçilmiş açık metin saldırılarına karşı zayıf olabilir.

Myasnikov vd. (2011) grup kuramsal olarak kriptografide kullanılabilecek zor problemlere değinmiştir. Halkalarda da kriptografik açıdan kullanışlı olan matematiksel zor problemlere rastlamanın mümkün olduğu söylenebilir. Örneğin, grup halkalarındaki birimsellerin terslerinin bulunmasının oldukça zor bir işlem olduğu dikkate alındığında, bu birimsellerin uygulamalı kriptografi için önemli bileşenler olduğu söylenebilir. Dolayısıyla bu yapılar, yeni ve güvenli şifreleme sistemlerinin inşasında etkin biçimde kullanılabilir. Hanoymak ve Küsmüş (2015) bu zorluğu, kriptografik uygulamalarda birimsel problemi olarak adlandırmıştır.

Miller (1985), elliptik eğrilerin kriptografideki kullanımı üzerine çalışmıştır. NTRU ise, kuantum saldırılarına karşı güvenli oluşu ve RSA (Rivest vd., 1978), ECC (Koblitz, 1987), ElGamal (ElGamal, 1985) gibi klasik açık anahtarlı şifreleme sistemlerine kıyasla çok daha hızlı çalışması sayesinde dikkat çeken bir açık anahtarlı şifreleme algoritmasıdır ve Hoffstein, Pipher ve Silverman tarafından önerilmiştir (Hoffstein vd., 1998). Ayrıca, Goldreich vd. (1996) GGH kriptosistemini tanıtmışlardır (Silverman vd., 2008). Kuantum bilgisayarların büyük tamsayıların çarpanlara ayrılması ve ayrık logaritmaların hesaplanması gibi işlemleri etkin biçimde gerçekleştirebildiği gösterildikten sonra, yukarıda adı geçen geleneksel sistemlerin kuantum hesaplamaya karşı güvenlikleri zayıflamıştır (Shor, 1997). NTRU'nun en önemli özelliği, kuantum saldırılarına karşı dayanıklı olmasıdır. Bunun yanı sıra, hem şifreleme hem de şifre çözme işlemlerinin oldukça hızlı gerçekleşmesi, bu algoritmaya olan akademik ilgiyi artırmış ve kriptografi camiasında NTRU benzeri birçok yeni kriptosistemin geliştirilmesine bir motivasyon kaynağı oluşturmuştur. NTRU'nun güvenliği, kafes teorisine dayanan bazı

zor problemlere, özellikle En Kısa Vektör Problemi (SVP) ve En Yakın Vektör Problemi (CVP) gibi problemler üzerine kuruludur (Tekin, 2011). Bu problemler için şu an bilinen hiçbir polinomsal zamanlı algoritma bulunmamaktadır. LLL algoritması (Lenstra vd., 1982) gibi bazı yöntemler, bu problemler için en kısa vektörün bir üstel katını vererek yaklaşık çözümler sunabilmektedir. En kısa vektörün uzunluğu ile ilgili olarak, Hoffstein vd. (2003) tarafından bir kafesin en kısa vektör uzunluğunun yaklaşık değerinin formülize edilmesi üzerine yapılan çalışma örnek gösterilebilir.

2. KAYNAK BİLDİRİŞLERİ

NTRU ile ilgili literatür incelendiğinde, aşağıda özetlenen çalışmaların öne çıktığı görülmektedir. Bu kapsamda, Hoffstein ve Silverman (2003), NTRU kriptosisteminde tersinir olması gereken polinomun seçimi üzerine bir çalışma sunmuştur. Silverman (1998), bir polinomun hangi şartlarda tersinin mevcut olduğu üzerine olasılıksal bir sonuç vermiştir. Silverman (1999a, 2001), etkili bir NTRU kriptosisteminde parametrelerin seçimi konusunda çalışmalar yapmıştır. Ayrıca, bir polinomun tersinin hızlı bir şekilde hesaplanmasını amaçlayan bir algoritma sunulmuştur (Silverman, 1999b). Silverman ve Whyte (2003), olasılıksal olarak deşifreleme başarısızlığını tahmin etme üzerine çalışma yapmıştır.

Ajtai, (1996; 1998) kafes tabanını indirgeme algoritmalarının kriptografi açısından kullanılabilirliği üzerine çalışmıştır. Bir başka çalışmada, Dwork (1998), kriptografide kafeslerin uygulama alanlarına değinmiştir. Schnorr (1987), polinom zamanlı kafes tabanı indirgeme algoritmaları üzerine bir sınıflama yapmıştır. Cai (2000), çalışmasında SVP ve CVP'nin zorluklarına ilişkin bazı sonuçlar elde etmiştir. Goldreich vd. (1999) çalışmalarında SVP ile CVP'nin zorluklarını kıyas ettikleri bir çalışma sunmuşlardır. Bu çalışma sonucunda, SVP'nin CVP'den daha zor olmadığını göstermişlerdir.

İlgili literatüre bakıldığında, NTRU kriptosisteminin kriptanalizi ve bazı saldırı denemelerine de rastlamanın mümkün olduğu söylenebilir. Bu bağlamda, May (1999), kafes indirgeyerek NTRU kriptosisteminin kriptanalizi ile ilgili bir çalışma yapmıştır.

Ayrıca, Howgrave-Graham vd. (2003) tarafından, bir NTRU gizli anahtarına yapılan ortada buluşma saldırısı ile ilgili çalışma gerçekleştirilmiştir.

Hoffstein ve Silverman (2000) ve Howgrave-Graham vd. (2005) çalışmalarında temel ilkeleri aynı kalmak suretiyle NTRU'nun geliştirilmesini amaçlamıştır. Bu amaç doğrultusunda bugüne kadar birçok NTRU benzeri şifreleme sistemi önerilmiştir. Örneğin, MaTRU kriptosistemi, $R = \mathbb{Z}[X]/\langle X^n - 1\rangle$ halkası üzerinde tanımlı $k \times k$ boyutlu matrislerden oluşan M halkasında çalışmaktadır (Coglianese ve Goi, 2005). Kolayca farkedilebileceği üzere R, katsayıları tamsayı ve derecesi en fazla $n-1$ olan kesilmiş polinomlardan oluşur. Bu sistemde deşifrelemenin değişmeli yapılarla mümkün

olduğu ve dolayısıyla güvenlik anlamında bunun NTRU ile kıyaslandığında daha fazla bir güvenlik sağlamadığı belirtilmiştir (Vats, 2009).

Benzer mentaliteyle oluşturulan diğer sistemlerden CTRU kriptosistemi, kesilmiş polinomlardaki katsayıları tamsayılar halkasından almak yerine sonlu bir cisim (F_2) üzerinde tanımlı tek değişkenli polinomları katsayılar olarak ele alıp polinom katsayılı polinomlar kullanmayı öneren bir sistemdir ki bu yaklaşımın, LLL algoritması ya da Çin Kalan Teoremi temelli saldırılara karşı daha güçlü bir yapı sunduğu belirtilmektedir (Gaborit vd., 2002).

Vats (2009) tarafından sunulan NNRU kriptosistemi, Coppersmith ve Shamir (1997)'in gerçekleştirdiği türden kafes saldırılarını önlemek amacıyla geliştirilmiştir ki bu sistem; I_k $k \times k$ tipinde birim matrisi göstermek üzere,

$$M = M_k(\mathbb{Z}[X]/\langle X^n - 1\rangle)$$

şeklinde tanımlanan ve girdileri $R = \mathbb{Z}[X]/\langle X^n - 1\rangle$ halkasından gelen elemanlar olan bir matris halkası içinde işlem yapar.

Jarvis ve Nevins (2015) tarafından geliştirilen ETRU kriptosistemi, Eisenstein tamsayılar kümesi $\mathbb{Z}[\omega]$ üzerinde tanımlanmıştır. Diğer bir deyişle, ETRU

$$\mathbb{Z}[\omega][X]/\langle X^n - 1\rangle$$

halkasındaki kesilmiş polinomlarla işlem yapar. Burada, ω birimin kompleks ilkel küp köküdür.

Malekian vd. (2011) tarafından önerilen QTRU kriptosistemi, değişmeli olmayan bir yapı olan kuaterniyonlar cebiri üzerinde tanımlı kesilmiş polinomların ele alınmasıyla oluşturulmuş olan bir kriptosistemdir ki çalışmada 41 boyutlu anahtar yardımıyla, NTRU-167 ile eş bir güvenlik sağlanmıştır.

Camara vd. (2018), dual tamsayılar kullanarak DTRU adıyla NTRU benzeri bir başka sistem sunmuşlardır. DTRU kriptosisteminde, $\varepsilon^2 = 0$ olmak üzere $D = \mathbb{Z} + \varepsilon\mathbb{Z}$ halkasında tanımlı kesilmiş polinomlar ele alınmıştır. Ancak, DTRU kriptosisteminin NTRU ile kıyaslandığında etkili olmadığı belirtilmiştir (Camara vd., 2018).

İnternet-of-Things (IoT) uygulamaları için tasarlanmış grup teorisi temelli bir varyant olan bir diğer kriptosistem GTRU ismiyle sunulmuştur ki bu sistemin, kafes tabanlı saldırılara karşı NTRU'ya göre daha yüksek bir güvenlik seviyesi sunmaktadır (Shuai vd., 2019).

Parvathi ve Srinivasan (2020), matris Lie gruplarını kullanarak yeni bir NTRU benzeri açık anahtarlı şifreleme sistemi geliştirmiştir.

Hanoymak ve Küsmüş (2019), grup halkalarının birimsel elemanları üzerine kurulu kriptografik sistemlere ilişkin olarak dihedral grupların değişmeli olmayan grup halkalarına dayanan çok taraflı anahtar değişim protokolü ve simetrik şifreleme sistemi tasarlamışlardır.

Bir başka çalışmada, kesilmiş polinomlara entegre edildiğinde NTRU benzeri bir sistemle bağdaştırılabilme potansiyeline sahip integral grup halkalarındaki Bass devirli birimsel elemanlara dayalı bir açık anahtarlı şifreleme sistemi sunulmuştur (Küsmüş ve Hanoymak, 2022).

Kriptografik açıdan son derece önemli kavramlar hususunda gerekli olan sayılar teorisi ve cebirsel alt yapı için Cohen (1995), Milies ve Sehgal (2002) ve Passman (1977)'ın çalışmalarına başvurulabilir. Ayrıca, modern kriptografi üzerine Cao (2012)'nun çalışmasından da yararlanılabilir.

3. MATERYAL VE YÖNTEM

3.1 Polinom Halkaları ve Kesilmiş Polinomlar

Tanım 3.1.1 R bir halka olmak üzere, sonlu sayıda terimi sıfır olmayan bir

$$(a_0, a_1, \dots) \in R \times R \times \dots$$

dizisi yardımıyla oluşturulan

$$R[x] = \{a_0 + a_1 x + \cdots + a_n x^n : \forall i, a_i \in R, n \in \mathbb{N}\}$$

kümesi üzerinde tanımlı

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \begin{cases} \sum_{i=0}^{n} (a_i + b_i) x^i + \sum_{i=n+1}^{m} b_i x^i, & n < m \\ \sum_{i=0}^{n} (a_i + b_i) x^i, & n = m \\ \sum_{i=0}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i, & n > m \end{cases}$$

ve

$$\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{j=0}^{m+n} c_j x^j$$

öyle ki $\forall k \in \{0,1, \dots, m+n\}$ için $c_k = \sum_{j=0}^{k} a_j b_{k-j}$ işlemleriyle $(R[x], +, .)$ cebirsel yapısına polinom halkası ve her bir elemanına bir polinom denir. Bir $p(x) = \sum_{i=0}^{n} a_i x^i$ polinomunda, n sayısına $p(x)$ polinomunun derecesi denir ve $n = deg(p(x))$ ile gösterilir. Ayrıca, $p(x) = \sum_{i=0}^{n} a_i x^i$ polinomundaki $a_n \in R$, $p(x)$ polinomunun baş katsayısı olarak adlandırılır (Hungerford, 1974).

Örnek 3.1.1 $1 < n, n \in \mathbb{N}$ olmak üzere, $\mathbb{Z}_n[x]$ polinom halkasında, $(1+x)^n = 1 + x^n$ ve n defa toplam $(1+x) + (1+x) + \cdots + (1+x) = 0$ olduğu kolayca görülebilir.

Tanım 3.1.2 $R[x]$ bir R halkası üzerinde tanımlı polinom halkası olmak üzere $1 < N, N \in \mathbb{N}$ olmak üzere, $\langle x^N - 1 \rangle$ temel ideali ile oluşturulabilen,

$$\frac{R[x]}{\langle x^N - 1 \rangle} = \{f(x) + \langle x^N - 1 \rangle : f(x) \in R[x]\}$$

bölüm halkasının elemanlarına kesilmiş polinom denir. Aslında, bu tanım matematiksel olarak,

$$\frac{R[x]}{\langle x^N - 1 \rangle} = \{\sum_{i=0}^{N-1} \alpha_i x^i : \alpha_i \in R, x^N = 1\}$$

ile eş değerdir ki çalışma boyunca son yazılan form kullanılacaktır.

Örnek 3.1.2 $\frac{\mathbb{Z}_3[x]}{\langle x^4 - 1 \rangle}$ kesilmiş polinomlar halkası,

$$\frac{\mathbb{Z}_3[x]}{\langle x^4 - 1 \rangle} = \{\overline{k_0} + \overline{k_1}x + \overline{k_2}x^2 + \overline{k_3}x^3 : \overline{k_i} \in \mathbb{Z}_3, x^4 = 1\}$$

olup, söz konusu halkada, $(\bar{1} + \bar{2}x + \bar{2}x^2)(\overline{-1} + \bar{2}x - \bar{2}x^3) = \bar{1} + \bar{2}x + \bar{2}x^2 + \bar{2}x^3$ eşitliği kolayca görülebilir.

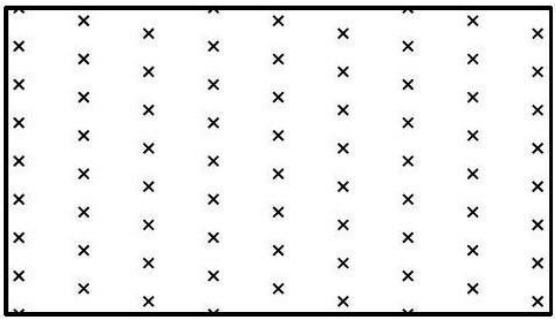
3.2 Kafes Teorisi

Tanım 3.2.1 $b_1, b_2, \dots, b_n \in \mathbb{R}^m$, n tane lineer bağımsız vektör olsun. Bu vektörlerin tamsayı katsayılı lineer kombinasyonlarının oluşturduğu kümeye kafes adı verilir ve

$$\mathcal{L} = \mathcal{L}(b_1, b_2, \dots, b_n) = \{\textstyle\sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}\}$$

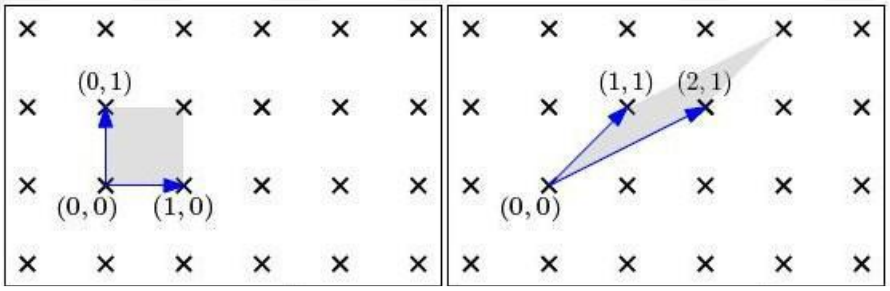
şeklinde gösterilir. Burada $\{b_1, b_2, \dots, b_n\}$ vektörlerine kafesin tabanı (veya bazı) denir. $B = [b_1, b_2, \dots, b_n] \in \mathbb{R}^{m.n}$ taban vektörlerini sütun kabul eden $m \times n$ tipinde matris olmak

üzere, B tarafından üretilen kafes $\mathcal{L} = \mathcal{L}(B) = \mathcal{L}(b_1, b_2, \ldots, b_n) = \{Bx \mid x \in \mathbb{Z}^n\}$ şeklinde ifade edilebilir (Tekin, 2011). Kafes, Şekil 3.1'de gösterildiği gibi periyodik yapılı n-boyutlu uzayda bir noktalar kümesi olarak görülebilir (Tekin, 2011).

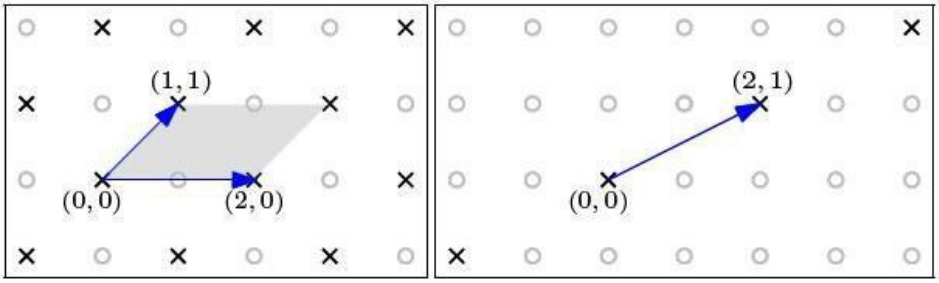


Şekil 3.1 $\mathbb{R}^2$ üzerinde bir kafes (Tekin, 2011)

n tamsayısına rank denir ve $rank(B)$ ile gösterilir. m tamsayısına ise kafesin boyutu denir ve $dim(\mathcal{L}(B))$ ile gösterilir. Rankı ve boyutu birbirine eşit olan kafese tam-rank kafes adı verilir (Tekin, 2011).



(a) $\mathbb{Z}^2$ 'nin bir tabanı (b) $\mathbb{Z}^2$ 'nin diğer bir tabanı



(c) $\mathbb{Z}^2$ 'nin bir tabanı değildir. (d) Tam rank olmayan bir kafes

Şekil 3.2 Bazı kafes tabanları (Tekin, 2011)

Şekil 3.2.(a)'da görülebileceği üzere, $(1,0)^T$ ve $(0,1)^T$ vektörlerinin ürettiği kafes $\mathbb{Z}^2$ dir (Tekin, 2011). İyi bilinen bir gerçektir ki bir kafesin tabanı tek türlü değildir (Tekin, 2011). Örneğin, Şekil 3.2.(b)'deki $(1,1)^T$ ve $(2,1)^T$ vektörleri de $\mathbb{Z}^2$ için üreteçlerdir (Tekin, 2011). $\mathbb{Z}^2$ aynı zamanda $(2005,1)^T$ ve $(2006,1)^T$ elemanlarıyla da oluşturulabilir (Tekin, 2011). Şekil 3.2 (a) ve Şekil 3.2 (b)'den farklı olarak $(1,1)^T$ ve $(2,0)^T$ vektörleri $\mathbb{Z}^2$'nin bir tabanı olamaz (Şekil 3.2.(c)'deki gibi) (Tekin, 2011). $(1,1)^T$ ve $(2,0)^T$ vektörleri, koordinatları toplamı çift sayı olan ikililerin oluşturduğu kafesi üretir (Tekin, 2011). Şekil 3.2 (a), Şekil 3.2 (b) ve Şekil 3.2 (c)'deki örnekler tam-rank olanlardır (Tekin, 2011). Ancak, Şekil 3.2.(d)'deki $\mathcal{L}((2,1)^T)$ kafesi tam-rank olmayan bir kafestir (Tekin, 2011). $\mathcal{L}((2,1)^T)$ kafesinin boyutu 2 ve rankı 1 dir. 1 boyutlu tam-rank kafese bir örnek $\mathbb{Z} = \mathcal{L}((1))$ kafesidir (Tekin, 2011).

$(v_1, v_2, \dots, v_n) \in \mathbb{R}^m$ lineer bağımsız vektörlerin kümesi olmak üzere, $(v_1, v_2, \dots, v_n)$'nin $\mathbb{Z}$'deki katsayılar ile oluşan lineer kombinasyonlarının kümesi yani

$$\mathcal{L} = \{a_1 v_1 + a_2 v_2 + \cdots + a_n v_n : a_1, a_2, \dots, a_n \in \mathbb{Z}\}$$

kafesi göz önüne alınsın. $\{v_1, v_2, \dots, v_n\}$ bir taban ve $\{w_1, w_2, \dots, w_n\} \in \mathcal{L}$ bir koleksiyon olmak üzere,

$$\begin{aligned} w_1 &= a_{11} v_1 + a_{12} v_2 + \cdots + a_{1n} v_n \\ w_2 &= a_{21} v_1 + a_{22} v_2 + \cdots + a_{2n} v_n \\ &\vdots \\ w_n &= a_{n1} v_1 + a_{n2} v_2 + \cdots + a_{nn} v_n \end{aligned}$$

formundadır (Silverman vd., 2008). Burada tüm a_{ij} formundaki katsayıların tamsayı olması gerektiğinden,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

matrisinin determinantının $det(A) = \pm 1$ olması gerektiği doğal olarak farkedilebilir (Silverman vd., 2008).

Kafes teorisinde matematiksel olarak çözülmesi zor olan bazı problemler mevcuttur. İlgili literatürde en kısa vektör problemi (SVP) olarak bilinen problem, ele alınan bir kafeste uzunluğu en kısa olan vektörün bulunması problemidir. Bununla ilgili algoritmik olarak değişik zorlukların üstesinden gelebilmek için, SVP değişik boyutlarıyla ele alınmıştır ki örneğin en kısa vektörü bulup, uzunluğunu verilen bir sayıyla kıyaslamak bunlardan bir tanesidir (Tekin, 2011). Bir $\mathcal{L}(\beta)$ kafesi ele alındığında, beklenen en kısa vektör uzunluğu, $\tau(\mathcal{L}(\beta))$ ile gösterilmek üzere, kısaca SVP $||v|| = \tau(\mathcal{L}(\beta))$ olacak şekildeki $v \in \mathcal{L}(\beta)$ vektörünün tespit edilmesine yönelik problemdir. Bu problemin Arama SVP, Optimizasyon SVP ve Karar SVP isimlendirmeleriyle alternatif tanımları Tekin (2011) tarafından ele alınmıştır. Kafes teorisinde SVP benzeri diğer bir problem de en yakın vektör problemi (CVP) olup, β bir kafes tabanı olmak üzere $\mathcal{L}(\beta)$ kafesi için, seçilen herhangi bir v vektörüne bir d metriğine göre $\mathcal{L}(\beta)$ içindeki en yakın vektörü bulma şeklinde tanımlanabilir.

3.3 LLL Taban İndirgeme Algoritması

(Tekin, 2011) çalışmasında bahsedildiği gibi bir kafesin çok sayıda farklı tabanı olabilir, ancak bu tabanlar içinde kısa ve birbirine dik vektörlerden oluşanlar daha büyük öneme sahiptir. Kafes indirgeme algoritmaları, amaç olarak kafesin mümkün olduğunca kısa vektörlerden meydana gelen bir tabanını ve aynı zamanda en kısa vektörü elde etmeye çalışır. Eğer kafesin boyutu düşükse, en kısa vektör sıralama tabanlı detaylı arama yöntemleri ile tespit edilebilir ancak yüksek boyutlu kafesler söz konusu olduğunda, ayrıntılı arama yöntemleri üstel zaman karmaşıklığına sahip olur (Schnorr ve Euchner, 1994; Tekin, 2011).

Lenstra vd. (1982) tarafından LLL adı verilen bir kafes indirgeme yöntemi önerilmiştir. Tekin (2011)'in de belirttiği gibi LLL algoritması, polinom zamanda çalışan

ve yaklaşık olarak kısa vektörleri elde edebilen bilinen tek yöntemdir. Bu yaklaşımda amaç, ortogonal bir taban elde etmektir.

Önerme 3.3.1 $\mathcal{L}$ bir kafes ve $\beta = \{u_1, u_2, \dots, u_n\}$ bu kafesin ortogonal bir tabanı olsun. Bu durumda en kısa vektör, ortogonal tabandaki vektörlerden biridir.

İspat. $U \in \mathcal{L}$ olsun. $\beta = \{u_1, u_2, \dots, u_n\}$ bir ortogonal taban ise, $\alpha_i \in \mathbb{Z}$ için,

$$U = \sum_{j=1}^{n} \alpha_j u_j$$

ve β ortogonal bir taban olduğundan,

$$||U||^2 = \sum_{j=1}^{n} {\alpha_j}^2 ||u_j||^2$$

ve dolayısıyla, $\forall j \in \{1,2, \dots, n\}$ için $||u_j||^2 \leq ||U||^2$ eşitsizliği geçerlidir. Böylece,

$$\min_{1 \leq j \leq n} ||u_j|| \leq ||u_j|| \leq ||U||$$

olup, iddia edildiği gibi en kısa vektör β ortogonal tabanının elemanıdır. ■

Gram-Schmidt ortogonalleştirme işlemi yardımıyla

$$u_i^* = u_i - \sum\nolimits_{i>j} \mu_{i,j}\, u_j^*$$

öyle ki

$$\mu_{i,j} = \frac{\langle u_i, u_j^* \rangle}{\langle u_j^*, u_j^* \rangle}$$

olup,

$$\pi_i: \mathbb{R}^m \longrightarrow \sum_{i \leq j} \mathbb{R}\, u_j^*$$

iz düşümü ile

$$\pi_i(x) = \sum_{j=1}^{n} \frac{\langle x, u_j^* \rangle}{\langle u_j^*, u_j^* \rangle} u_j^*$$

eşitliğine dayanarak $\pi_i(u_i) = {u_i}^*$ ortogonal vektörleri elde edilir. $\frac{1}{4} < \delta < 1$ eşitsizliğini sağlayan bir δ parametresiyle aşağıdaki tanım verilebilir (Micciancio, 1999).

Tanım 3.3.1 $\beta = \{u_1, u_2, \dots, u_n\}$ kümesi bir $\mathcal{L}$ kafesinin tabanı olsun. Eğer, aşağıdakiler sağlanırsa, β tabanına δ parametresiyle LLL indirgenmiştir denir (Tekin, 2011):

(1) $\forall i > j, \left|\mu_{i,j}\right| \leq 1/2$

(2) Herhangi iki ardışık u_i ve u_{i+1} vektörleri için, $\delta||\pi_i(u_i)||^2 \leq ||\pi_i(u_{i+1})||^2$

LLL algoritmasının temelde tek bir şarta bağlı olarak verilebildiği söylenebilir. Nitekim, algoritma şu şekilde verilir:

(1) β tabanının boyutunu indirgemek.

(2) Eğer bazı i değerleri için,

$$\delta||\pi_i(u_i)||^2 > ||\pi_i(u_{i+1})||^2$$

ise u_i ve u_{i+1} vektörlerinin yerlerini değiştirmek ve tekrar (1) adımına dönmek, aksi halde işlemleri durdurmak.

4. KAFES TABANLI BAZI KRİPTOSİSTEMLER

Bu bölümde, SVP ve/veya CVP problemine dayanan kafes tabanlı kriptosistemlerden olan NTRU kriptosistemine ve değişik cebirsel yapılar üzerinde türetilerek NTRU benzeri yapılan bazı kriptosistemlere yer verilmiştir.

4.1 NTRU

NTRU kriptosistemi, literatürde sıklıkla çalışılan kafes tabanlı kriptosistemlerden biri olup, Hoffstein vd. (1998) tarafından ortaya atılan ve döngüsel modüler kafeslere ilişkin bir kriptosistemdir. NTRU, temelde $\mathbb{Z}[x]/\langle x^N - 1\rangle$ halkası üzerindeki polinomların konvolüsyon çarpımlarına dayanan bir kriptosistem olup, sistemin parametreler dörtlüsü (N, p, q, d)'dir. Burada, sistemin etkin çalışabilmesi için bu parametrelerin bazı özelliklere sahip olması gerekmektedir. Daha açık olarak ifade etmek gerekirse, ilerleyen kısımlarda değinilecek olan şifreleme ve deşifreleme algoritmasının etkililiği için N parametresinin asal olarak seçilmesi gerektiğinin ve ayrıca, q/p değerinin de oldukça büyük ve $ebob(p, q) = 1$ olmasının sistemin etkililiği için büyük önem arz ettiği belirtilmiştir (Silverman vd., 2008). Sistemin dayandığı cebirsel yapılar;

$$\mathcal{R} = \mathbb{Z}[x]\Big/\langle x^N - 1\rangle, \mathcal{R}_p = \mathbb{Z}_p[x]\Big/\langle x^N - 1\rangle \text{ ve } \mathcal{R}_q = \mathbb{Z}_q[x]\Big/\langle x^N - 1\rangle$$

olmak üzere, bir

$$h(x) = h_0 + h_1 x + \cdots + h_{N-1}x^{N-1} \in \mathcal{R}_q$$

polinomu ile NTRU kriptosisteminin kafesi oluşturulabilir ki bu kafes

$$M_h^{NTRU} = \begin{bmatrix} 1 & 0 & \dots & 0 & h_0 & h_1 & \dots & h_{N-1} \\ 0 & 1 & \dots & 0 & h_{N-1} & h_0 & \dots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & h_1 & h_2 & \dots & h_0 \\ 0 & 0 & \dots & 0 & q & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & q & \dots & 0 \\ \vdots & \vdots & \ddots & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & \dots & q \end{bmatrix}$$

matrisinin satırları tarafından üretilen $2N$ boyutlu L_h^{NTRU} kafesidir (Silverman vd., 2008; Tekin, 2011).

M_h^{NTRU} matrisinin $n \times n$ şeklinde dört bloktan oluştuğuna dikkat edilmelidir. Nitekim;

- Sol üst blok; Birim matris I_n
- Sol alt blok; Sıfır matrisi 0_n
- Sağ alt blok; qI_n
- Sağ üst blok; $h(x)$ polinomunun katsayılarının döngüsel matrisi (Silverman vd., 2008)

Böylece, NTRU kriptosisteminin matrisini aşagıdaki gibi kısaltmak genellikle uygundur.

$$M_h^{NTRU} = \begin{pmatrix} I & h \\ 0 & qI \end{pmatrix}$$

NTRU sisteminde şifreleme ve deşifreleme işlemleri sırasında önemli bir nokta, mod alma işleminin tanımı yani aslında katsayıları indirgemektir. Bu işlemler sırasında oluşabilecek başarısızlıklardan kaçınmak için, polinomların (katsayılarının) ortalanması gerekmektedir (Silverman vd., 2008; Tekin, 2011). Yani, $f\,(modm)$ işleminde, f polinomunun katsayıları $[0, m)$ aralığında ele alınmaktansa ($\left\lfloor -\frac{m}{2} \right\rfloor, \left\lfloor \frac{m}{2} \right\rfloor$] aralığına indirgenmelidir (Tekin, 2011). Herhangi pozitif d_1 ve d_2 tamsayıları için

$$\mathcal{L}(d_1, d_2) = \left\{ a(x) \in \mathcal{R}: \begin{array}{c} a(x) \text{ içinde } d_1 \text{ adet katsayı } 1, \\ d_2 \text{ tane katsayısı } -1, \\ \text{geri kalan katsayılar } 0 \end{array} \right\}$$

Tekin (2011), f polinomunda 1 ve -1 olan katsayıların sayısının aynı olmadığı çünkü $f(1) = 0$ eşitliğini sağlayan bir polinomun (Hoffstein vd., 1998) çalışması gereğince

tersinir olamayacağını belirtmiştir. Anahtar üretimi, şifreleme ve deşifreleme işlemleri için gerekli olan; f, g polinomları, r rastgele polinomu ve bir m mesajının alındığı uzaylar sırasıyla $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_r$ ve $\mathcal{L}_m$ ile gösterilsin. $\mathcal{L}_f, \mathcal{L}_g$ ve $\mathcal{L}_r$ uzaylarının parametrik yapısı aşağıdaki gibi tanımlanmıştır.

- $\mathcal{L}_f = \mathcal{L}(d_f, d_f - 1)$
- $\mathcal{L}_g = \mathcal{L}(\, d_g, d_g\,)$
- $\mathcal{L}_r = \mathcal{L}(\, d_r, d_r\,)$

NTRU Anahtar Üretimi:

Bir $\mathcal{R} = \mathbb{Z}[x] \Big/ \langle\, x^N - 1 \rangle$ halkasından; yukarıda belirtilen parametrik şartlara uyacak ve hem $\mathcal{R}_p = \mathbb{Z}_p[x] \Big/ \langle\, x^N - 1 \rangle$ hem de $\mathcal{R}_q = \mathbb{Z}_q[x] \Big/ \langle\, x^N - 1 \rangle$ halkasında tersinir olacak şekilde bir f polinomu seçilir. Seçilen f polinomunun $\mathcal{R}_p$ halkasındaki tersi f_p^{-1} ve $\mathcal{R}_q$ halkasındaki tersi f_q^{-1} olmak üzere, $f.f_p^{-1} \equiv 1\ (mod\ p)$ ve $f.f_q^{-1} \equiv 1\ (mod\ q)$ denklikleri sağlanır. Benzer şekilde, $\mathcal{L}_g$ uzayından, yukarıdaki parametrik şartlar doğrultusunda bir g polinomu seçilerek,

$$h \equiv p.f_q^{-1} * g\ (mod\ q)$$

polinomu hesaplanır ki f gizli anahtarı ve h açık anahtarı üretilir.

NTRU Şifreleme:

$\mathcal{L}_m$ mesaj uzayından bir m mesajı (polinom olarak) seçilsin. Ayrıca, mesajın gizliliğini sağlamak adına $\mathcal{L}_r$ uzayından $\mathcal{L}_r = \mathcal{L}(\, d_r, d_r\,)$ olacak şekilde rastgele bir r polinomu da göz önüne alınarak, m mesajı

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

şeklinde şifrelenir (Tekin, 2011). Burada, rastgeleliğin farklı polinomlarla sisteme dahil edilmesinden kaynaklı olarak seçilen bir mesajın, birden farklı şekilde şifrelenmesi mümkündür.

NTRU Deşifreleme:

e şifreli mesajını çözmek için ilk olarak gizli anahtar olan f polinomunun $mod\ p$ altındaki tersinin kullanılarak,

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

ara işleminin yapılması gerekir. Daha sonra,

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

işlemiyle birlikte katsayıların $(-\left\lfloor\frac{q}{2}\right\rfloor, \left\lfloor\frac{q}{2}\right\rfloor)$ aralığına indirgenmesi yani diğer bir deyişle katsayıların ortalanması işleminin gerçekleştirilmesi çok büyük öneme sahiptir. Son olarak,

$$c \equiv f_p^{-1} * a'\ (mod\ p)$$

işlemiyle şifreli metni çözme işi tamamlanır. Burada dikkat edilmesi gereken bir husus şudur ki uygun parametreler ve katsayıların ortalanmasıyla birlikte, seçilen bir m mesajının şifrelenmiş metni tekrar deşifreleme işlemine tabi tutulduğunda yüksek ihtimalle yine m mesajının elde edileceği fakat uygun bir şekilde ele alınmayan ve ortalanmayan parametrelerle deşifreleme işleminin başarısızlıkla sonuçlanabileceği belirtilmiştir (Tekin, 2011).

NTRU kriptosisteminde şifreleme ve deşifreleme işlemlerinde başarıya ulaşmanın yani bir m mesajının şifrelenmesiyle elde edilen e mesajının deşifreleme işlemine tabi tutulmasıyla yine m mesajına ulaşabilmek için seçilmesi gereken parametre değerlerine ilişkin aşağıdaki teorem, uygulamada çok büyük bir öneme sahiptir.

Teorem 4.1.1 Eğer NTRU parametreler dörtlüsü (N, p, q, d),

$$(6d + 1)p < q$$

eşitsizliğini sağlayacak şekilde seçilirse, $c = m$ olur (Silverman vd., 2008).

Bu bağlamda, aşağıdaki örnekte parametreler yukarıdaki teoreme uygun olarak seçilmiştir.

Örnek 4.1.1 NTRU kriptosistemi için parametreleri $N = 7$, $q = 97$, $p = 5$, $d_f = 3$, $d_g = 2$ olan bir anahtar çifti üretilerek ve bu anahtarla $m = 1 + x + x^2$ mesajı şifrelenip daha sonra deşifre edilsin.

Burada, $f(x)$ polinomunun en fazla 6. dereceden ve üç tane katsayısı 1, iki tane katsayısı -1 ve diğer katsayılarının 0 olması gerektiği açıktır. Benzer şekilde $g(x)$ polinomu en fazla 6. Dereceden ve iki tane katsayısı 1, iki tane katsayısı -1 ve diğer katsayıları 0 olan bir polinom olmalıdır. Söz konusu polinomlar,

$$f(x) = -1 + x^2 - x^3 + x^5 + x^6$$

ve

$$g(x) = -1 - x + x^3 + x^5$$

olsun. $f(x)$ polinomunun (mod5) ve (mod32) de tersleri aşağıdaki gibidir.

$$f_p^{-1}(x) = f(x) = 2 + 2x + 2x^2 + 2x^3 - x^4 - 2x^5 + x^6 \ \ (mod5)$$

$$f_q^{-1}(x) = f(x) = -9 + 5x - 2x^2 - 47x^3 - 25x^4 - 36x^5 + 18x^6 \ \ (mod97)$$

$$f_p^{-1}(x) = (2 + 2x + 2x^2 + 2x^3 - x^4 - 2x^5 + x^6)$$

$$f_q^{-1}(x) = (-9 + 5x - 2x^2 - 47x^3 - 25x^4 - 36x^5 + 18x^6\ )$$

Böylece, verilen parametreler doğrultusunda $h(x)$ açık anahtarı

$$h(x) \equiv p.f_q^{-1}(x) * g(x)\ (mod q)$$

kuralıyla, aşağıdaki gibi hesaplanır.

$h(x) \equiv$
$5(-9 + 5x - 2x^2 - 47x^3 - 25x^4 - 36x^5 + 18x^6\ )(-1 + x^3 + x^5 - x^8)(mod 97)$

Yani,

$$h(x) \equiv (-180 - 395x - 50x^2 + 20x^3 + 475x^4 + 250x^5 - 120x^6)\ \ (mod 97)$$

$$h(x) \equiv (14 + 90x + 47x^2 + 20x^3 + 87x^4 + 56x^5 + 74x^6)\ \ \ (mod 97)$$

sonuç olarak gizli anahtar $f(x) = (-1 + \ x^2 - x^3 + x^5 + x^6)$

ve açık anahtar

$$h(x) = (14 + 90x + 47x^2 + 20x^3 + 87x^4 + 56x^5 + 74x^6)$$

olmak üzere, herhangi bir mesaj şifrelenebilip deşifrelenirken (f, h) anahtar çifti kullanılır. Şimdi, bir $m(x) = 1 + x + x^2$ mesajı (f, h) anahtar çifti yardımıyla şifrelenip deşifre edilsin. Bunun için ihtiyaç duyulan rastgele bir $r(x) \in \mathcal{L}(d, d)$ polinomu

$$r(x) = -1 - x - x^2 + x^3 + x^4 + x^5$$

olsun. Bu durumda,

$$e(x) \equiv r(x) * h(x) + m(x)\ (mod 97)$$

kuralı doğrultusunda,

$e(x) = (-1 - x - x^2 + x^3 + x^4 + x^5) * (14 + 90x + 47x^2 + 20x^3 + 87x^4 + 56x^5 + 74x^6) + (1 + x + x^2) \quad (mod 97)$

ve dolayısıyla

$$e(x) = (11 - 14x + 67x^2 - 13x^3 + 24x^4 - 12x^5 - 60x^6)$$

şifreli metni elde edilir. NTRU sistemine göre bu elde edilen şifreli mesajın deşifreleme işlemi bir ara işlem olan

$$a(x) \equiv f(x) * e(x) \ (mod 97)$$

işleminin yapılmasıyla başlar ki bu kuralla, $a(x)(mod 97)$

$$(-1 + x^2 - x^3 + x^5 + x^6)(11 - 14x + 67x^2 - 13x^3 + 24x^4 - 12x^5 - 60x^6)$$

yani,

$$a(x) \equiv (6 + 20x + 15x^2 - 15x^4 - 117x^5 + 94x^6) \ (mod 97)$$

elde edilir. Daha sonra, deşifreleme işlemi için bulunan bu $a(x)$ polinomunun $(modp)$ değeri hesaplanarak

$$a'(x) = (6 + 20x + 15x^2 + 82x^4 + 77x^5 + 94x^6) \equiv (1 + 2x^6) \ (mod\ 5)$$

elde edilir. Son olarak

$$c(x) \equiv f_p^{-1}(x) * a'(x) \ (modp)$$

hesaplamasıyla,

$$c(x) \equiv (2 + 2x + 2x^2 + 2x^3 - x^4 - 2x^5 + x^6) * (1 + 2x^6) \quad (mod 5)$$

yani, $c(x) \equiv (6 + 6x + 6x^2 - 5x^4 + 5x^6) \equiv (1 + x + x^2)\ (mod 5)$ elde edilir ki görülebileceği üzere $c = m$'dir.

4.2 MaTRU

Coglianese ve Goi (2005) tarafından önerilen MaTRU kriptosistemi temelde NTRU kriptosisteminde de kullanılan cebirsel yapıya yani $\mathcal{R} = \mathbb{Z}[X]/\langle X^n - 1\rangle$ kesilmiş polinomlar halkasına dayanmaktadır. Sunulan bu sistemde, $\mathcal{R}$ halkasındaki elemanlardan oluşan $k \times k$ tipindeki matrislerin $M_k(\mathcal{R})$ halkasında çalışılır. MaTRU sisteminde $p, q \in N$ kullanılır. Verilen p, q asal olabilir veya olmayabilir fakat $(p, q) = 1$ olmalıdır. Burada da tıpkı NTRU kriptosisteminde olduğu gibi $p << q$ yani q'nun p'den çok büyük olması gerekir. MaTRU kriptosisteminde de bir matris çarpımını $mod\ p$ ve $mod\ q$ indirgeme işlemi yapılır. Bir matrisin kısa olabilmesi için,

$$maks = maks_{M'deki\ polinomlar} polinom\ katsayıları$$

ve

$$min = min_{M'deki\ polinomlar} polinom\ katsayıları$$

olmak üzere,

$$|M|_\infty = maks - min$$

şeklinde tanımlanan uzunluk doğrultusunda, $|M|_\infty \leq p$ ise $M \in M_k(\mathcal{R})$ matrisi kısadır denir. Kısa matrislerin çarpılmasıyla daha büyük matrisler elde edileceği açıktır fakat yine de bu genişlik q 'dan daha küçük kalacaktır (Coglianese ve Goi, 2005). Kısalık ve genişlik şeklinde kullanılan bu tanımlar, $\mathcal{R}$ halkası için de söz konusudur. Nitekim, bir $r \in \mathcal{R}$ elemanı için,

$$maks(r) = r'deki\ katsayıların\ maksimumu$$

ve

$$min(r) = r'deki\ katsayıların\ minimumu$$

olmak üzere,

$$|r|_\infty = maks(r) - min(r)$$

ve ayrıca bir M matrisinin boyutu ile kastedilen değer de

$$|M| = \sqrt{\sum_{M'deki\ polinomlar} \sum (polinom\ katsayıları)^2}$$

şeklinde tanımlıdır (Coglianese ve Goi, 2005). Coglianese ve Goi (2005), ilgili kafesi

$$\mathcal{L}(d) = \left\{ M \in M_k(\mathcal{R}): \begin{array}{c} i = \left\lceil -\frac{p-1}{2} \right\rceil \ldots \left\lceil \frac{p-1}{2} \right\rceil \neq 0\ için\ M'deki\ her\ bir\ polinomun \\ i\ değerine\ eşit\ ortalama\ d\ tane\ katsayısı\ vardır, \\ geri\ kalan\ katsayılar\ 0'dır. \end{array} \right\}$$

şeklinde tanımlamışlardır. Burada, i'nin alabileceği değerlerin üste yuvarlama fonksiyonu ile elde edilebileceğini görmek zor değildir. Örneğin; $p = 3$ ve $n = 7$ parametreleri için $\mathcal{L}(3)$ kafesindeki polinomların üç tane katsayısının 1, üç tane katsayısının -1 ve geri kalan bir katsayısının sıfır olduğu farkedilebilir. Bilindiği üzere, MaTRU parametreleri; (n, k, p, q) ve

$$(\mathcal{L}_f, \mathcal{L}_\phi, \mathcal{L}_A, \mathcal{L}_w, \mathcal{L}_m) \subseteq M$$

matrislerinin sıralı beşlisini içermektedir. Burada, $\mathcal{L}_f$ gizli anahtarların geldiği uzaydır. $\mathcal{L}_\phi$ de tıpkı NTRU sisteminde olduğu gibi gerekli duyulan rastgele elemanların (ϕ, ψ) alındığı uzaydır. $\mathcal{L}_A$ uzayı, f, g, ϕ, ψ elemanları için kullanılır. Ayrıca, $\mathcal{L}_w$ açık anahtar uzayı ve $\mathcal{L}_m$ mesaj uzayıdır.

MaTRU Anahtar Üretimi:

Açık ve gizli anahtarlarını üretmek için $\mathcal{L}_A$ uzayında Bob $k \times k$ tipinde A ve B matrislerini seçer. Ayrıca rastgele kısa polinomlar $\alpha_0, \alpha_1, \dots, \alpha_{k-1} \in \mathcal{R}$ ve $\beta_0, \beta_1, \dots, \beta_{k-1} \in \mathcal{R}$ ele alır. Böylece $f, g \in \mathcal{L}_f$ için

$$f = \sum_{i=0}^{k-1} \alpha_i A^i$$

ve

$$g = \sum_{i=0}^{k-1} \beta_i B^i$$

matrislerini oluşturur. Burada f ve g matrislerinin (mod p) ve (mod q)'da tersinir olması gerekmektedir. Uygun parametre seçimi ile (mod p) ve (mod q)'da matrislerin tersleri sırasıyla $f_p^{-1}, f_q^{-1}, g_p^{-1}, g_q^{-1}$ şeklinde gösterilirse,

- $f_p^{-1} * f \equiv I(modp)$
- $f_q^{-1} * f \equiv I(modq)$
- $g_p^{-1} * g \equiv I(modp)$
- $g_q^{-1} * g \equiv I(modq)$

olur.

Bob' un gizli anahtarı f, g anahtarlarıdır. Bob ayrıca rastgele bir $w \in \mathcal{L}_w$ matrisi seçerek $h \in M$ açık anahtarını şu şekilde oluşturur.

$$h \equiv f_q^{-1} * w * g_q^{-1} \ (modq)$$

Dolayısıyla, Bob' un açık anahtarları h, A ve B' dir (Coglianese ve Goi, 2005).

MaTRU Şifreleme:

Bob' a gönderilecek bir mesajı şifrelemek için Alice, rastgele şu şekilde kısa polinomlar üretir:

$$\phi_0, \phi_1, \dots, \phi_{k-1}, \varphi_0, \varphi_1, \dots, \varphi_{k-1} \in \mathcal{R}$$

Daha sonra aşağıdaki hesaplamaları yapar:

$$\phi = \sum_{i=0}^{k-1} \phi_i A^i$$

ve

$$\varphi = \sum_{i=0}^{k-1} \varphi_i B^i$$

Hesaplamalar yapıldıktan sonra $m \in \mathcal{L}_m$ mesajını aşağıdaki yolla şifreler:

$$e \equiv p(\phi * h * \varphi) + m \ (mod q)$$

ve oluşturduğu şifreli mesajı Bob' a gönderir (Coglianese ve Goi, 2005).

MaTRU Deşifreleme:

Bob kendine gelen e şifreli mesajını aşağıdaki yolla çözer:

$$a \equiv f * e * g \quad (mod q)$$

İşlemleri yaparken polinomların katsayılarını, tıpkı NTRU sisteminde olduğu gibi $\left[\left\lfloor \frac{-q}{2} \right\rfloor, \left\lfloor \frac{q}{2} \right\rfloor\right]$ aralığına indirger ve devamında

$$a \equiv f * e * g \pmod{q}$$

ve

$$d \equiv f_p^{-1} * (f * e * g) * g_p^{-1} \pmod{p}$$

şeklinde düz metine ulaşır. (f, g) ve (ϕ, φ) çifti seçimi yaparken öncelikle d_f ve d_ϕ tanımlanır öyle ki

$$\mathcal{L}_f = \mathcal{L}(d_f), \qquad \mathcal{L}_\phi = \mathcal{L}(d_\phi)$$

A ve B matrisleri açık olmak üzere, f, g, ϕ ve φ matrislerinin güvenliği kısa polinomlar $\alpha_i, \beta_i, \phi_i, \varphi_i$' lerin bulunmasının zorluğuna dayanır. Bu nedenden dolayı polinomların sayısının maksimize edilmesi çok önemlidir. Burada yaklaşık olarak seçim $d_f \approx \frac{n}{p}$ ve $d_\phi \approx \frac{n}{q}$ şeklinde yapılır (Coglianese ve Goi, 2005).

A ve B matrislerinin seçimi, f ve ϕ matrisleri üretilirken matrislerin sadece değişmeli değil aynı zamanda kısa olmasına dikkat edilerek yapılır. Daha kısa matrisler, mod q' ya indirgenebilir ve şifreli metinin çözülebilir olmasını sağlayacak şekilde,

$$\left| p(\phi * w * \varphi) + f * m * g \right|_\infty$$

değerinin q'dan daha küçük olduğu matrislerdir. Burada, işlemlerin başarıyla sonuçlanması için A ve B matrisleri permütasyon matrisleri olarak seçilebilir (Coglianese ve Goi, 2005). Permütasyon matrisleri bilindiği üzere sadece 0 ve 1'i içeren matrislerdir öyle ki her satır ve sütunda sadece bir tane eleman 1 ve geri kalan elemanlar 0'dır. Seçilecek olan A ve B matrislerine ilave olarak, $\{A^0, A^1, \dots, A^{k-1}\}$ ve $\{B^0, B^1, \dots, B^{k-1}\}$ kümelerinin her ikisinin de lineer bağımsız olma özelliğini de sağlaması gerekir ki

$$\sum_{j=0}^{k-1} A^j = \sum_{j=0}^{k-1} B^j = \begin{pmatrix} 1 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 1 \end{pmatrix}$$

olmalıdır. Buradan da görülür ki f matrisi' nin her bir satır ve sütunu $\alpha_0, \alpha_1, \dots, \alpha_{k-1}$'lerin bazı permütasyonlarını içerir. Yani, her bir α_i elemanı; f matrisi içinde sadece k kez görünecektir. Örneğin;

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

şeklinde seçildiğinde,

$$A + A^2 + A^3 + I_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

ve dolayısıyla,

$$\sum_{i=0}^{3} \alpha_i A^i = \begin{bmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_3 & \alpha_0 & \alpha_1 & \alpha_2 \\ \alpha_2 & \alpha_3 & \alpha_0 & \alpha_1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_0 \end{bmatrix}$$

elde edilir. Benzer durum, g, ϕ ve φ matrisleri için de geçerlidir. Yani,

$$d_f \approx d_{\phi} \approx \frac{n}{p}$$

olduğundan,

$$|f| \approx \sqrt{k^2 |\alpha_i|^2} \approx \sqrt{\frac{(p-1)nk^2}{p}} \approx |g| \approx |\phi| \approx |\varphi|$$

geçerlidir (Coglianese ve Goi, 2005). f ve g matrislerine benzer olarak w matrisi de

$$\left| p(\phi * w * \varphi) + f * m * g \right|_{\infty}$$

küçük olacak şekilde kısa seçilmelidir. Güvenlik nedenlerinden dolayı, w matrisinin gizli tutulması önemlidir. Böylece w matrisinin seçileceği uzayı bulmak için,

$$\mathcal{L}_w = \mathcal{L}(\left\lfloor \frac{n}{p} \right\rfloor)$$

ele alınmalıdır. Buradan da w matrisinin boyutu

$$|w| = \sqrt{\frac{(p-1)nk^2}{p}}$$

olur (Coglianese ve Goi, 2005).

4.3 CTRU

Bilindiği üzere, NTRU sisteminin güvenliği SVP'ye dayanır ve anahtar boyutu kısa, şifreleme, deşifreleme hızlıdır. Şimdiye kadar verilen kafes tabanlı sistemler içinde en hızlı açık anahtarlı kriptosistem olan NTRU sisteminin dezavantajı kafes indirgeme saldırıları ve Çin Kalan Teoremi (CRT) saldırılarına karşı olan eksikliktir. Bu alt bölümde, NTRU kriptosistemindeki kesilmiş polinomların katsayılarında kullanılan $\mathbb{Z}$ yerine $\mathbb{F}_2$ üzerinde tanımlı tek değişkenli polinomlar halkasının kullanıldığı CTRU kriptosistemi tanıtılacaktır.

Gaborit vd. (2002) tarafından önerilen CTRU kriptosisteminde LLL algoritmasının rolünü lineer sistemler teorisinde önemli bir yeri olan Popov formu üstlenmektedir. Sonlu bir cisim üzerinde tanımlı $X^N - 1$'in köklerinin basit olmamasından dolayı CTRU kriptosisteminin CRT saldırılarına karşı daha güvenli olduğu değerlendirilmektedir (Gaborit vd., 2002). CTRU kriptosisteminde bir N pozitif tamsayısı ve $A = \mathbb{F}_2[T]$ polinomlar halkasından P ve Q gibi iki polinom kullanılmaktadır. Burada P, Q polinomları indirgenemezdir. P polinomunun derecesi $der(P) = s$ ve Q

polinomun derecesi $der(Q) = t$ öyle ki $2 \leq s \leq t$ ve $(t, s) = 1$ dir. Sistemde çalışılan halka:

$$\mathbb{F}_2[T][X] \Big/ \langle x^N - 1 \rangle$$

dir. Kolayca gözlemlenebilir ki P ve Q indirgenemez polinomlar olmak üzere,

$$A_P = A \Big/ (P)$$

ve

$$A_Q = A \Big/ (Q)$$

bölüm halkaları aslında sırasıyla $\mathbb{F}_{2^s}$ ve $\mathbb{F}_{2^t}$ sonlu cisimleridir. Benzer şekilde

$$R_P = R \Big/ (P)$$

ve

$$R_Q = R \Big/ (Q)$$

bölüm halkaları da polinomları indirgemek için kullanılan bölüm halkalarıdır. Gaborit vd. (2002) de bahsetmiştir ki, $ebob(s, t) = 1$ olmasıyla $\mathbb{F}_{2^s} \cap \mathbb{F}_{2^t} = \mathbb{F}_2$ olur ve üstelik NTRU kriptosisteminde olduğu gibi $mod\ (P)$'de ve $mod\ (Q)$'da yapılan indirgeme işlemlerinde aralarındaki bağımsızlık basit saldırıların önüne geçmede çok büyük bir öneme sahiptir. $\mathcal{R} = A[x]/\langle x^N - 1 \rangle$ olmak üzere, keyfi $d \leq t$ için tanımlanan

$$\mathcal{L}(d) = \{f \in \mathcal{R} : der(f) < d\}$$

uzayının boyutu 2^{Ns} olup, mesaj uzayı $M = \mathcal{L}(N, s)$ ve CTRU anahtarlarının tanımlandığı uzaylarla birlikte, taşıması gereken parametrik özellikler şu şekildedir (Gaborit vd., 2002):

Gizli anahtar çifti (f, g) ve rastgele polinom olan Q polinomunun üretildiği uzaylar

$$\mathcal{L}_f \coloneqq \mathcal{L}(d_f + 1),$$
$$\mathcal{L}_g \coloneqq \mathcal{L}(d_g + 1),$$
$$\mathcal{L}_\phi \coloneqq \mathcal{L}(d_{\phi+1})$$

formundadır öyle ki $d_f, d_g, d_\phi \leq t$.

CTRU Anahtar Üretimi:

L_f ve L_g uzaylarından sırasıyla R_P ve R_Q da tersinir olan bir f polinomu ve ayrıca g polinomu seçilir. (f, g) çifti sistemin gizli anahtarıdır.

$$(f, g) \in \mathbb{F}_{2^{d_f}}^N \times \mathbb{F}_{2^{d_g}}^N$$

ki en fazla $(d_f + d_g)N$ bit uzunluğundadır. Açık anahtar

$$h = \frac{g}{f}[mod(x^N - 1, Q)]$$

dur. Böylece $h \in \mathbb{F}_{2^{d_t}}^N$ öyle ki h, tN uzunluğundadır (Gaborit vd., 2002).

CTRU Şifreleme:

Tıpkı NTRU kriptosisteminde olduğu gibi, CTRU kriptosisteminde de bir rastgelelik faktörü olduğundan dolayı sistem deterministik değildir (Gaborit vd., 2002).

Seçilen bir $\mathcal{M} \in M$ mesajı, seçilen bir ϕ rastgele polinomu ile birlikte, h açık anahtarı yardımıyla,

$$e \equiv P\phi h + \mathcal{M}(modQ)$$

şeklinde şifrelenir. Dolayısıyla, $ef \equiv P\phi g + \mathcal{M}f(modQ)$ olur. Bununla eş zamanlı olarak, $s + d_\phi + d_g < t$ ve $s + d_f < t$ sağlanırsa, ef polinomunun $\mathcal{R}$'den olduğu düşünülür ve deşifreleme işlemine geçilebilir (Gaborit vd., 2002).

CTRU Deşifreleme:

$$e \equiv P\phi h + \mathcal{M}(modQ)$$

şifreli mesajına f polinomunun uygulanmasıyla,

$$\begin{aligned} ef\ (mod\ P) &\equiv P\phi hf + \mathcal{M}f(mod\ Q)(mod\ P) \\ &\equiv \mathcal{M}f\ (mod\ Q)(mod\ P) \end{aligned}$$

elde edilir ki böylece, f polinomunun $(mod\ P)$ tersinin uygulanmasıyla, $\mathcal{M} \in M$ mesajına ulaşılır (Gaborit vd., 2002).

4.4 DTRU

Bu alt bölümde, Camara vd., (2018) tarafından önerilen ve dual tamsayılar halkası üzerinde tanımlanan kesilmiş polinomlar yardımıyla oluşturulan, NTRU benzeri bir kriptosistem çalışılmaktadır.

Tanım 4.4.1 $\varepsilon^2 = 0$ olmak üzere,

$$D = \mathbb{Z} + \varepsilon\mathbb{Z} = \{z = a + \varepsilon b : a, b \in \mathbb{Z}, \varepsilon^2 = 0\}$$

kümesi üzerinde tanımlanan

$$(a + \varepsilon b) + (c + \varepsilon d) = (a + c) + \varepsilon(b + d)$$

ve

$$(a+\varepsilon b)(c+\varepsilon d)=ac+\varepsilon ad+\varepsilon bc+\varepsilon^2 bd=ac+\varepsilon(ad+bc)$$

işlemleriyle $(D,+,.)$ bir halka olup bu halkaya *dual tamsayılar halkası* denir ve kısaca, $D=\mathbb{Z}[\varepsilon]$ ile gösterilir (Camara vd., 2018). Burada, $a\in\mathbb{Z}$ tamsayısına reel kısım ve $b\in\mathbb{Z}$ tamsayısına da imajiner (sanal) kısım denir ve sırasıyla $a=Re(z)$ ve $b=Im(z)$ ile gösterilir.

Tanım 4.4.2 $\varphi: D\to\mathbb{N}$ aşağıdaki özellikleri sağlayan bir fonksiyon olsun.

(1) $\forall z\in D,\ \varphi(z)\geq 0$

(2) $\forall z\in D,\ \forall t\in D\backslash J_D$ (J_D sıfır bölen elemanların kümesi) için,

$$\varphi(z)\leq\varphi(zt)$$

(3) $\forall z\in D,\ \forall t\in D\backslash J_D$ için, $\exists(q,r)\in D^2, z=tq+r$ öyle ki

$$\varphi(r)<\varphi(t)$$

Bu durumda, φ fonksiyonuna *sözde-norm* denir (Camara vd., 2018).

Teorem 4.4.1 φ bir sözde-norm olmak üzere, (D,φ) bir sözde-Öklit halkası olsun. Eğer, $z,t\in D$ ve J_D sıfır bölen elemanların kümesi ve $t\in D\backslash J_D$ ise, o zaman

$$\exists(q,r)\in D^2, z=tq+r$$

öyle ki $r=0$ veya $\varphi(r)<\varphi(t)/4$ (Camara vd., 2018). Burada sözde-bölme algoritması aşağıdaki gibidir (Camara vd., 2018):

Girdi: $z\in D$ ve $t\in D\backslash J_D$.

Çıktı: $(q,r)\in D$ öyle ki $z=qt+r$, $\varphi(r)<\varphi(t)/4$.

(1) $a_1\leftarrow Re(z\bar{t})$, $a_2\leftarrow Im(z\bar{t})$ ve $n=t\bar{t}$

(2) $i=1,2$ için $a_i=nq_i+r_i$

(3) $q=q_1+q_2\varepsilon, r=z-tq$

Örnek 4.4.1 $z = 121 - 26\varepsilon$ ve $t = 3 - 51\varepsilon$ olmak üzere, $q = 40 + 677\varepsilon$ ve

$$r = z - tq = 1 - 17\varepsilon$$

elde edilir.

Şimdi, $z \in D$ olmak üzere, $\frac{D}{zD}[x]$ polinom halkası ve $f, g \in \frac{D}{zD}[x]$ ele alınsın.

Tanım 4.4.3 Eğer $f', g' \in \frac{D}{zD}[x]$ öyle ki $ff' + gg' \equiv 1(modz)$ ise bu durumda, f ve g polinomlarına *eş-asal* denir ve $f \wedge g = 1$ ile gösterilir (Camara vd., 2018).

p bir asal sayı olmak üzere $f_i, g_i \in \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ için, $f = f_1 + \varepsilon f_2$ ve $g = g_1 + \varepsilon g_2$ polinomları ele alındığında, f ve g polinomlarının terslerinin nasıl hesaplanacağı ile ilgili aşağıdaki algoritma göz önüne alınabilir.

Sözde-Genişletilmiş Öklit Algoritması:

Girdi: $f = f_1 + \varepsilon f_2 \in \frac{D}{pD}[x]$ ve $g = g_1 + \varepsilon g_2 \in \frac{D}{pD}[x]$ öyle ki $f_i, g_i \in \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$.

Çıktı: $ebob(f_1, f_2) \neq 1$ ise f polinomu $\frac{D}{pD}[x]/\langle g(x)\rangle$ halkasında tersinir değildir. Eğer, $ebob(f_1, f_2) = 1$ ise

(1) $(u_1, v_1) \in \frac{\mathbb{Z}}{p\mathbb{Z}}[x]$ öyle ki $f_1u_1 + g_1v_1 = 1$ $(\in \frac{\mathbb{Z}}{p\mathbb{Z}}[x])$.

(2) $h \leftarrow -f_2u_1 + g_1v_1$, $u_2 \leftarrow u_1h$ ve $v_2 \leftarrow v_1h$

(3) $u \leftarrow u_1 + \varepsilon u_2 \leftarrow u_1 + \varepsilon u_1h$ ve $v \leftarrow v_1 + \varepsilon v_2 \leftarrow v_1 + \varepsilon v_1h$ olmak üzere

$$fu + gv = 1$$

Bir $z \in D\backslash\mathbb{Z}$ için $\frac{D}{zD}[x]/\langle g(x)\rangle$ halkasında bir polinomun tersinin varlığını incelemek literatürde açık bir problem olarak değerlendirilmektedir (Camara vd., 2018).

Şimdi, D bir sözde-Öklit halkası ve $(p, q) \in D^2$ olmak üzere, $\frac{D}{pD}[x]/\langle x^N - 1\rangle$ ve $\frac{D}{qD}[x]/\langle x^N - 1\rangle$ polinom halkaları üzerinde NTRU benzeri bir sistemin nasıl kurulabileceği üzerine tartışılabilir. $R = D[x]$,

$$R_p = \frac{D}{pD}[x]/\langle x^N - 1\rangle$$

ve

$$R_q = \frac{D}{qD}[x]/\langle x^N - 1\rangle$$

olsun. $\mathcal{L}_m \subseteq R_p$, $\mathcal{L}_g \subseteq R_q$ve $\mathcal{L}_f, \mathcal{L}_\phi \subseteq R$ olmak üzere; anahtar üretimi, şifreleme ve deşifreleme aşağıdaki gibidir.

DTRU Anahtar üretimi:

q/p değerinin oldukça büyük olduğu bir $(p, q) \in \mathbb{Z} \times \mathbb{Z}$ seçilsin. Bu durumda, hem R_p hem de R_q'da tersinir olacak şekilde rastgele ama küçük katsayılı bir $f \in \mathcal{L}_f$ polinomu ele alınsın öyle ki $\frac{D}{pD}[x]/\langle x^N - 1\rangle$ ve $\frac{D}{qD}[x]/\langle x^N - 1\rangle$ halkalarındaki tersleri sırasıyla f_p ve f_q olsun. Bu durumda, yine rastgele ama küçük katsayılı olacak şekilde bir $g \in \mathcal{L}_g$ ile birlikte açık anahtar,

$$h = pf_q * g \in R_q$$

şeklinde üretilebilir (Camara vd., 2018).

DTRU Şifreleme:

$$a, b \in \mathcal{L}_m = \left\{-\frac{p-1}{2}, \dots, -1, 0, 1, \dots \frac{p-1}{2}\right\} (p \text{ tekse})$$

veya

$$a, b \in \mathcal{L}_m = \left\{-\frac{p}{2}, \dots, -1,0,1, \dots \frac{p}{2}\right\} (p \text{ çiftse})$$

olmak üzere, bir $m = a + \varepsilon b$ mesajını şifrelemek için, bir $\phi, \psi \in \mathcal{L}_\phi$ alarak,

$$e = \phi * h + \psi * h^2 + m \ (mod q)$$

şifreli metni elde edilebilir (Camara vd., 2018).

DTRU Deşifreleme:

Şifreli metin $e \in R_q$ geldiğinde ilk olarak $a = f^2 * e \ (mod q)$ hesaplanır ve a'nın katsayılarının değeri $[\left\lfloor -\frac{q}{2} \right\rfloor, \left\lfloor \frac{q}{2} \right\rfloor]$ aralığına düşürülür. Daha sonra,

$$m = f_p^2 * a \ (mod p)$$

düz metnine ulaşılır (Camara vd., 2018).

4.5 ETRU

Bu alt bölümde, Jarvis ve Nevins (2015) tarafından ETRU adıyla çalışılan ve Eisenstein tamsayılar halkası üzerinde kurulan bir diğer NTRU benzeri kriptosistem ele alınmıştır. Alt bölümde yer alan bilgilerde Nevins vd. (2010), Jarvis ve Nevins (2015) ve Jarvis (2011)'den yararlanılmıştır.

Şimdi; ω, birimin bir kompleks küp kökü olsun. Yani, $\omega^3 = 1$. Bu durumda

$$\omega = \frac{1}{2}(-1 + i\sqrt{3})$$

olacağı açıktır ki Eisentein tamsayılar halkası

$$\mathbb{Z}[\omega] = \{a + b\omega \,|\, a, b \in \mathbb{Z}, \omega^3 = 1\}$$

şeklinde tanımlıdır. Uzunluk,

$$q = a + b\omega \;\Rightarrow\; |q|^2 = a^2 + b^2 - ab$$

formülü ile belirlenebilir. $\mathbb{C}$ 'de birimin n. köklerinden oluşan devirli alt grup için μ_n yazılırsa

$$\mu_3 = \{1, \omega, \omega^2 = -1 - \omega\}$$

ve

$$\mu_6 = \{\pm 1, \pm\omega, \pm\omega^2\}$$

örnekleri elde edilir ki bunlar $\mathbb{Z}[\omega]$'da kapsanır. $\mathbb{Z}[\omega]$'dan $\mathbb{R}^2$'ye bir gömme (embedding) vardır ki bu,

$$f: \mathbb{Z}[\omega] \to \mathbb{Z}^2$$
$$f(a + b\omega) = (a, b)$$

toplamsal grup izomorfizmasıdır ve bu durumda $\alpha = a + b\omega$ ile sağdan çarpım

$$\langle\alpha\rangle = \begin{bmatrix} a & b \\ -b & a - b \end{bmatrix}$$

matrisi ile yapılır (Jarvis ve Nevins, 2015). Burada,

$$f\big((a + b\omega)(a + b\omega)\big) = (a, b)\begin{bmatrix} a & b \\ -b & a - b \end{bmatrix}$$

olduğuna dikkat edilmelidir. Bu $g: \mathbb{Z}[\omega] \to \mathbb{C} \simeq \mathbb{R}^2$

$$g(a + b\omega) = \left(a - b/2\right) + i\left(\sqrt{3}b/2\right)$$

izometrik halka monomorfizmasından farklıdır ve kullanımı hesaplama açısından daha verimlidir (Jarvis ve Nevins, 2015). Ayrıca, cebirsel tamsayılar halkaları arasında kullanılan ve $\mathbb{Q}$'nun reel olmayan kuadratik genişlemelerine özgü olan şey, bu izometrik gömmenin görüntüsünün $\mathbb{R}^2$'de bir kafes olmasıdır (Aslında, iki boyutlu bir küre-paketleme kafesi) ki bu özellik $\mathbb{Z}[\omega]'$nin elemanlarının daha yoğun olması anlamına gelir (Jarvis ve Nevins, 2015).

NTRU' yu $\mathbb{Z}[\omega]$ 'ya taşımak için ilk adım aralarında asal olacak şekilde $p, q \in \mathbb{Z}[\omega]$ elemanlarını seçmektir. Pratikte, $mod\ p$ ve $mod\ q$ tersini alma algoritmasının etkinliği için bu sayılar asal ya da asal kuvveti şeklinde seçilebilir (Jarvis ve Nevins, 2015).

Teorem 4.5.1 μ_6 kümesi, $\mathbb{Z}[\omega]$ 'nin tüm tersinir elemanlarını içerir. Yani, $U(\mathbb{Z}[\omega])$ tüm tersinir elemanların kümesi olmak üzere,

$$\mu_6 = U(\mathbb{Z}[\omega])$$

ve $\mathbb{Z}[\omega]$ 'nin tüm asalları, $1 - \omega$;

$$p \equiv 2(mod 3)$$

olan p rasyonel asalları ve $|q|^2 = p$, $p \equiv 1(mod 3)$ olan $q \in \mathbb{Z}[\omega]$ elemanlarıdır ki böylece, (bir birimselle çarpma farkıyla) en küçük Eisenstein asalları:

$$p = 1 - w \ (|p|^2 = 3)\ ,\ p = 2 \ (|p|^2 = 4) \ \text{ ve } \ p = 2 + 3\omega \ (|p|^2 = 7)$$

dir (Jarvis ve Nevins, 2015).

ETRU Anahtar Üretimi:

ETRU sistemini tanımlamak için öncelikli olarak tercihen asal olacak şekilde bir N tamsayısı seçilir.

$$\mathcal{R}^{\varepsilon} = {\mathbb{Z}[\omega][x]}\Big/{\langle x^N - 1\rangle}$$

halkasındaki polinomların katsayılarının $\mathbb{Z}[\omega]'$dan gelen kesilmiş polinomlar olduğuna dikkat edilmelidir. Benzer şekilde, $\mathbb{Z}[\omega]$ halkasından aralarında asal olacak şekilde

$$|q| >> |p|$$

yani q'nun, p'den çok fazla büyük olduğu elemanlar seçilerek, herhangi bir $\alpha \in \mathbb{Z}[\omega]$ için $\mathcal{R}_{\alpha}^{\varepsilon}$ indirgenmiş polinomlar halkası oluşturulur öyle ki,

$$\mathcal{R}_{\alpha}^{\varepsilon} = \{p(x) \in \mathcal{R}^{\varepsilon} \,\big|\, p(x) \ (mod\alpha)\ 'ya\ indirgenmiş\}$$

Bu durumda not edilmelidir ki

$$f \in \mathcal{R}^{\varepsilon} \Rightarrow f = f_0 + f_1 x + \cdots + f_{N-1} x^{N-1}$$

ve $f_i = a_i + b_i \omega$.

Tanım 4.5.1 Voronoi hücresi, bir düzlem veya daha yüksek boyutlu bir uzayda seçilmiş bir noktalar kümesi için tanımlanan özel bir geometrik yapıdır. Daha basit haliyle seçilen o noktalar kümesindeki her bir noktaya en yakın olan tüm noktaları içeren bölgedir (Voronoi, 1908a; 1908b).

Teknik olarak, $p = \{p_1, p_2, \ldots, p_n\}$ noktalar kümesi için

$$V(p_i) = \{x \in \mathbb{R}^2 \,\big|\, d(x, p_i) \leq d\big(x, p_j\big), \forall j \neq i\}$$

bir Voronoi hücresidir. Yani, bir x noktası, sadece p_i noktasına diğer noktalardan daha yakınsa p_i 'nin Voronoi hücresinde yer alır. Ayrıca $\alpha \in \mathbb{Z}[\omega]$ için, $\langle \alpha \rangle = \langle \alpha, \alpha\omega \rangle$ bir kafes olup, D_α $(modq)$'da indirgenmiş elemanlar kümesi, $\langle \alpha \rangle$' nın orijininde yer alan Voronoi hücresinde bulunan elemanlar kümesi olarak tanımlanabilir öyle ki

$$f \in \mathcal{R}_\alpha^\varepsilon \Leftrightarrow \forall f_i \in D_\alpha$$

olur (Jarvis ve Nevins, 2015).

Aslında Voronoi hücresi ile SVP arasındaki ilişki şu şekilde açıklanabilir. Bir kafeste aranan en kısa vektörler kümesi orijinin Voronoi hücresidir. $f \in \mathcal{R}^\varepsilon$ olmak üzere,

$$f = \{f_0, f_1 x, \dots, f_{N-1} x^{N-1}\}$$

için $\forall f_i = a_i + b_j\omega$ olup

$$(a_0, b_0, a_1, b_1, \dots, a_{N-1}, b_{N-1}) \in \mathbb{Z}^{2N}$$

vektörü elde edilir. ETRU sisteminde basitlik olması açısından p parametresi $p = 2$ olarak ele alınır. ($p = 2 + 3\omega$ durumu (Jarvis, 2011)'da çalışılmış olup fazladan bazı indirgeme algoritmaları gerektirmektedir. $0 < r < 1$ olarak alınan sayı ve $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\phi$ uzayları da μ_6' dan seçilen yaklaşık rN sıfırdan farklı katsayılı olsun. Buradan,

$$\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_\phi \subseteq \mathcal{R}^\varepsilon$$

küme seçimleri aşağıdaki şekilde yapılır:

$\mathcal{L}_g$ ve $\mathcal{L}_\phi$' deki polinomlar $x - 1$ $(modq)$ ile bölünebilir şekilde ele alınır. Yani,

$$\mathcal{L}_g = \{g(x) \,|\, x - 1 \,|\, g(x) \quad (modq)\}$$

$$\mathcal{L}_\phi = \{q(x) \,|\, x - 1 \,|\, \phi(x) \quad (modq)\}$$

kafesleri incelenir. Böylece, s parametresi 3'ün rN' ye en yakın katı olsun ve rastgele $^{s}/_{3}$ tane katsayılar üçlüsü seçilsin ($\{1, \omega, \omega^2\}$ veya $\{-1, -\omega, -\omega^2\}$). $\mathcal{L}_\phi$' deki polinomların her biri ayrıca $\psi(1) = 0$ eşitliğini sağlasın. t parametresi rN 'ye en yakın tamsayı olmak üzere $\mathcal{L}_f$, t sayıda sıfırdan farklı ve μ_6 'dan gelen katsayılı polinomlar içerir. Bilinir ki $f \in \mathcal{L}_f$ tersinirdir. Tıpkı NTRU'daki gibi $\mathcal{L}_f$'nin rastgele seçilmiş bir elemanı yüksek olasılıkla tersinirdir. Her bir ETRU katsayısı tamsayıların bir çifti olduğundan dolayı, N dereceli bir ETRU örneği, $2N = N'$ dereceli bir NTRU ile kıyaslanabilir.

ETRU' daki f, g ve ϕ polinomlarının her biri Eisenstein tamsayı katsayısı, $a + b\omega$' yı temsil eden bir (a, b) tamsayı çifti olarak ele alınır ve μ_6' daki katsayılar için a ve b üçlü NTRU' daki polinomların tüm N' katsayıları gibi $\{-1, 0, 1\}$ kümesinden değerler alır. Bahsedilen üçlü NTRU katsayılarının $\{-1, 0, 1\}$ olduğu NTRU kriptosistemidir. NTRU'da olduğu gibi, f_q polinomu, f'nin mod q'daki tersi olmak üzere,

$$h = f_q * g \ (mod\ q)$$

açık anahtarı elde edilir (Jarvis ve Nevins, 2015).

ETRU Şifreleme:

$$\tilde{h} \equiv p.h \ (mod q)$$

olmak üzere

$$e \equiv \phi.\tilde{h} + m \ \ (mod q)$$

(Jarvis ve Nevins, 2015)

ETRU Deşifreleme:

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

olmak üzere $m = f_p.a\ (modp)$ olacağından, ETRU'nun şifreleme ve deşifreleme karmaşıklığını hesaplamak için tamsayılardaki toplamanın maliyetinin hesaplanması gerekir. $N' = 2N$ olduğunda ETRU ve NTRU' nun polinomlardaki bu maliyetini hesapladığımızda aynı olduğu kolayca görülebilir (Jarvis ve Nevins, 2015).

$(n-1)$. dereceden iki polinomun konvolüsyon çarpımının normalde n^2 halka çarpımı içerdiği bilinen bir gerçektir. Böylece $\mathcal{R}^{\varepsilon}$'da bu maliyet $3N^2$'dir. NTRU'da ise

$$(N')^2 \approx 4N^2$$

olur ki burada neden ETRU'da maliyetin $3N^2$ olduğu şu yaklaşımla bulunabilir; iki polinom

$$p(x) = (a_0 + b_0\omega) + (a_1 + b_1\omega)x + \cdots + (a_{N-1} + b_{N-1}\omega)x^{N-1}$$

ve

$$q(x) = (c_0 + d_0\omega) + (c_1 + d_1\omega)x + \cdots + (c_{N-1} + d_{N-1}\omega)x^{N-1}$$

şeklinde olursa her bir katsayıda aslında bir de $(a + b\omega)(c + d\omega)$ çarpma işlemi yapmak gerekir. Her ne kadar bu işlemde $ac, ad, bc,$ ve bd olmak üzere dört işlem gerekli gibi görünse de bd terimi ac, ad ve bc yardımıyla otomotik olarak elde edilebilir (Jarvis ve Nevins, 2015). O yüzden aslında 4 değil 3 işlem yeterlidir. Her katsayıda 3 işlem olmak üzere N^2 tane katsayılı polinomda $3N^2$ işlem yeterli olur. Yani sonuç olarak, Eisenstein polinomlarında çarpma işlemi, tamsayı katsayılı polinomlardaki çarpma işleminden daha hızlıdır.

Teorem 4.5.2 $q \in \mathbb{Z}[\omega]$ ve D_q, $(modq)$ indirgenmiş elemanların kümesi olsun.

$$B_s = [-s, s] \times [-s, s] \subset \mathbb{R}^2$$

olmak üzere

$$\{(c, d) \,|\, c + d\omega \in D_q\} \subset B_{\frac{2|q|}{3}}$$

(Jarvis ve Nevins, 2015).

İspat. Voronoi hücresi $V_q \supset D_q$ 'nun köşeleri için iddiayı doğrulamak yeterlidir. $q = 1$ için V_1 'in köşeleri

$$\pm\frac{1}{3}(1 + 2\omega)\,, \pm\frac{1}{3}(1 - \omega) \text{ ve } \pm\frac{1}{3}(2 + \omega)$$

şeklinde elde edilebilir. $q = a + b\omega$ olsun. V_1' in köşelerini q ile çarpma ile V_q elde edilir. Her köşeyi $c + d\omega$ biçiminde yazmak $c, d \in S$ öyle ki

$$S = \{\frac{\pm 1}{3}(2a - b), \frac{\pm 1}{3}(a + b), \frac{\pm 1}{3}(2b - a)\}$$

sonucunu verir. Direkt olarak, $|q|^2 = a^2 + b^2 - 2ab$ eşitliği kullanılarak, bu terimlerin her birinin mutlak değerce en fazla $2|q|/3$ olduğu ve S 'nin bir elemanının bu sınıra eşit olmasının; $a = 0$, $b = 0$ ya da $a = b$ olduğunda mümkün olduğu görülür. Eğer S 'deki her bir elemanın karesi en fazla $|q|^2/3$ olsaydı, o zaman

$$(a + b)(2a - b) \geq 0, (a + b)(a - 2b) \leq 0 \text{ ve } (a - 2b)(2a - b) \geq 0$$

elde edilirdi.

Bu durum, sadece bir çarpanın (ve dolayısıyla S 'nin bir elemanının) sıfır olması durumunda geçerlidir. Bunun üzerine de S'nin diğer iki elemanı $|q|/\sqrt{3}$ olur (Jarvis ve Nevins, 2015). ■

Bir h açık anahtarı, $(modq)$ da indirgenmiş N katsayılı bir polinom olup, her katsayı, (Jarvis ve Nevins, 2015)'e göre $\lceil log_2(4|q|/3) \rceil$ uzunluğunda ikili dizi olarak saklanabilen iki tamsayıdan oluşur. Bu yüzden ETRU açık anahtar boyutu

$$K^{\varepsilon} = 2N \left\lceil log_2 \left(\frac{4|q|}{3} \right) \right\rceil$$

olur (Jarvis ve Nevins, 2015).

4.6 QTRU

Bu alt bölümde çalışılan bilgiler, kuaterniyon cebirleri üzerine kurulan kesilmiş polinom halkalarıyla QTRU ismiyle sunulmuş (Malekian ve Zakerolhosseini, 2010; Malekian vd., 2011) çalışmalarından faydalanılmıştır.

Tanım 4.6.1

$$Q_8 = \langle i, j : i^2 = j^2, i^4 = 1, iji = -j \rangle$$

grubuna kuaterniyon grubu denir.

Kuaterniyon grubu üzerinde tanımlı $\mathbb{R}$-lineer genişleme, kuaterniyonlar cebiri kavramını doğurmaktadır.

Tanım 4.6.2

$$H = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{R}, k = ij\}$$

kümesi üzerinde tanımlı,

$$(\alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k) + (\alpha_2 + \beta_2 i + \gamma_2 j + \delta_2 k)$$
$$= (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)i + (\gamma_1 + \gamma_2)j + (\delta_1 + \delta_2)k$$

toplama işlemi ve

$$(\alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k)(\alpha_2 + \beta_2 i + \gamma_2 j + \delta_2 k) =$$
$$(\alpha_1(\alpha_2 - \beta_1\beta_2 - \gamma_1\gamma_2 - \delta_1\delta_2) + (\alpha_1\beta_2 + \beta_1\alpha_2 + \gamma_1\delta_2 - \delta_1\gamma_2)i$$
$$+(\alpha_1\gamma_2 + \gamma_1\alpha_2 + \delta_1\beta_2 - \beta_1\delta_2)j + (\alpha_1\delta_2 + \delta_1\alpha_2 + \beta_1\gamma_2 - \gamma_1\beta_2)k$$

çarpma işlemlerinin halka aksiyomlarını sağladığı ve üstelik

$$\mathbb{R} \times H \to H$$
$$(\lambda, \alpha + \beta i + \gamma j + \delta k) \longmapsto \lambda\alpha + \lambda\beta i + \lambda\gamma j + \lambda\delta k$$

etkisiyle, H kuaterniyonlar cebiri olarak adlandırılır. H kümesinin aynı zamanda bir $\mathbb{R}$-modül olduğunu farketmek zor değildir. $q = \alpha + \beta i + \gamma j + \delta k \in H$ kuaterniyonunun eşleniği,

$$\bar{q} = \alpha - \beta i - \gamma j - \delta k$$

şeklinde ve normu da,

$$N(q) = N(\bar{q}) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

eşitliği ile tanımlıdır. Açıktır ki

$$\forall q \in H\backslash\{0\}, q^{-1} = \bar{q}/N(q)$$

Aslında, kuaterniyon cebirleri, reel sayılar cismi yerine daha genel bir yapı üzerinde de tanımlanabilir: $ab \neq 0$ olmak üzere, değişmeli ve birimli bir R halkası üzerinde

$$\frac{(a,b)}{R} = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in R, k = ij, i^2 = a, j^2 = b, k^2 = -ab, iji = -j\}$$

yapısı tanımlanabilir ki R birimli değişmeli ve karakteristiği ikiden farklı bir halka olmak üzere,

$$A = \frac{(a,b)}{R}$$

yapısı oluşturulduğunda, $a = b = -1$ ve $\mathbb{R}$ reel sayılar cismi ile,

$$H = \frac{(-1,-1)}{\mathbb{R}}$$

iyi bilinen Hamilton kuaterniyon cebiri elde edilir (Malekian vd., 2011).

Tanım 4.6.3 Eğer $R = \mathbb{F}$ karakteristiği 0 olan bir cisim ve $q \in \frac{(a,b)}{\mathbb{F}}$ için $N(q) = 0$ olması $q = 0$ olmasını gerektirirse, bu durumda $A = \frac{(a,b)}{R}$ cebirsel yapısı, bir Öklit bölüm halkasıdır denir (Malekian vd., 2011).

Tanım 4.6.4 Tüm integral kuaterniyonların

$$\mathbb{L} = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, k = ij\}$$

kümesine Lipschitz kuaterniyonlar kümesi denir ki $\mathbb{R}^4$ içinde bir kafes teşkil eder (Malekian vd., 2011).

Şimdi, QTRU kriptosistemi için gerekli olan kuaterniyon cebirleri tanımları verilebilir. Öncelikle, GF_p ve GF_q ile sırasıyla p ve q asal sayılarına karşılık gelen sonlu cisimler gösterilsin. QTRU sistemi temelde,

$$\mathbb{L}_p = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in GF_p\}$$

ve

$$\mathbb{L}_q = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in GF_q\}$$

sonlu split cebirlerine dayanır (Malekian vd., 2011). Yani, $\mathbb{L}_p$ ve $\mathbb{L}_q$ yapıları sırasıyla girdileri GF_p ve GF_q gelen 2×2 matrisler halkasına izomorf yapılardır. Ayrıca, $\mathbb{L}$ Lipschitz kuaterniyonlarının normlu bölüm cebirleri olduğu bilinmektedir (Malekian vd., 2011).

$$\sigma_p : \mathbb{Z} \rightarrow \mathbb{Z}_p, \sigma_p(x) = x \ (mod\ p)$$

ve

$$\sigma_q : \mathbb{Z} \rightarrow \mathbb{Z}_q, \sigma_q(x) = x \ (mod\ q)$$

halka homomorfizmaları ele alınsın. Bu durumda, $\vartheta_p : \mathbb{L} \rightarrow \mathbb{L}_p$ ve $\vartheta_q : \mathbb{L} \rightarrow \mathbb{L}_q$ dönüşümleri sırasıyla,

$$\vartheta_p(\alpha + \beta i + \gamma j + \delta k) = \sigma_p(\alpha) + \sigma_p(\beta) i + \sigma_p(\gamma) j + \sigma_p(\delta) k$$

ve

$$\vartheta_q(\alpha + \beta i + \gamma j + \delta k) = \sigma_q(\alpha) + \sigma_q(\beta) i + \sigma_q(\gamma) j + \sigma_q(\delta) k$$

şeklinde elde edilir (Malekian vd., 2011).

Önerme 4.6.1 $\mathcal{H} := \langle h_0, h_1, h_2, h_3 \rangle \in \mathbb{L}_p$ ve $\mathcal{F}\mathcal{H} = \mathcal{G}$ kuaterniyon denkleminin en az bir çözümünün olduğu kabul edilsin. Bu durumda, tüm çözümler, $\mathbb{Z}^8$'de 8 boyutlu bir tamsayı kafesi teşkil eder (Malekian vd., 2011).

İspat. $\mathcal{F} = \langle f_0, f_1, f_2, f_3 \rangle$ ve $\mathcal{G} = \langle g_0, g_1, g_2, g_3 \rangle$ için, $\mathcal{F}\mathcal{H} = \mathcal{G}$ eşitliği aşağıdaki sistemi verir:

$$f_0 h_0 - f_1 h_1 - f_2 h_2 - f_3 h_3 = g_0 + k_0 p$$
$$f_0 h_1 + f_1 h_0 + f_2 h_3 - f_3 h_2 = g_1 + k_1 p$$

$$f_0h_2 - f_1h_3 + f_2h_0 + f_3h_1 = g_2 + k_2p$$
$$f_0h_3 + f_1h_2 - f_2h_1 + f_3h_0 = g_3 + k_3p$$

ki

$$M_h{}^{QTRU} = \begin{bmatrix} 1 & 0 & 0 & 0 & h_0 & h_1 & h_2 & h_3 \\ 0 & 1 & 0 & 0 & -h_1 & h_0 & -h_3 & h_2 \\ 0 & 0 & 1 & 0 & -h_2 & h_3 & h_0 & -h_1 \\ 0 & 0 & 0 & 1 & -h_3 & -h_2 & h_1 & h_0 \\ 0 & 0 & 0 & 0 & p & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & p & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & p & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & p \end{bmatrix}$$

satırları tarafından üretilen L_h^{QTRU} kafesi, $M_h{}^{QTRU}$ matrisinin satırlarının lineer bağımsız olmasıyla bir full-rank kafestir ve yukarıdaki sistemden açıkça görülebilir ki,

$$\langle f_0, f_1, f_2, f_3, -k_0, -k_1, -k_2, -k_3 \rangle M_h{}^{QTRU} = \langle f_0, f_1, f_2, f_3, g_0, g_1, g_2, g_3 \rangle$$

olduğundan,

$$\langle f_0, f_1, f_2, f_3, g_0, g_1, g_2, g_3 \rangle \in L_h^{QTRU}$$

olur. Tersine, $M_h{}^{QTRU}$ matrisinin satırlarının bir lineer kombinasyonu alındığında yukarıdaki sistemi sağlayan bir $\langle f_0, f_1, f_2, f_3, g_0, g_1, g_2, g_3 \rangle$ formu elde edilir. Böylece, ispat tamamlanır (Malekian vd., 2011). ■

Şimdi,

$$A = \frac{(-1,-1)}{\mathbb{Z}[x]/\langle x^N - 1 \rangle}$$

$$A_p = \frac{(-1,-1)}{\mathbb{Z}_p[x]/\langle x^N - 1 \rangle}$$

ve

$$A_q = \frac{(-1,-1)}{\mathbb{Z}_q[x]/\langle x^N - 1\rangle}$$

halkaları ele alınsın. QTRU kriptosistemi için temel kabullerden biri basitlik olması açısından, p, q ve N sayılarının asal olarak seçilmesidir (Malekian vd., 2011).

Tanım 4.6.5

$$f_i(x) = \sum_{j=0}^{N-1} f_{i,j} x^j = [f_{i,0}, f_{i,1}, \dots, f_{i,N-1}]$$

olmak üzere bir

$$F = f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \in A$$

kuaterniyonu için

$$||F||_\infty = \underset{0\le i\le 3\ \ 0\le j\le N-1}{\text{maks}} f_{i,j} - \underset{0\le i\le 3\ \ 0\le j\le N-1}{\min} f_{i,j}$$

ve

$$||F||_2 = \sqrt{\sum_{i=0}^{3}\sum_{j=0}^{N-1} {f_{i,j}}^2}$$

(Malekian vd., 2011). $\mathcal{L}_f, \mathcal{L}_g, \mathcal{L}_m, \mathcal{L}_\phi \subset A$ olmak üzere, QTRU kriptosistemi (N, p, q) parametrelerine bağlı olarak inşa edilir ve anahtar üretimi, şifreleme ve deşifreleme aşağıdaki gibi yapılır.

QTRU Anahtar Üretimi:

$||.||_\infty$ normuna göre küçük iki F ve G kuaterniyonu rastgele üretilir. Burada, dikkat edilmelidir ki,

$$F = f_0 + f_1 i + f_2 j + f_3 k$$

ve

$$G = g_0 + g_1 i + g_2 j + g_3 k$$

öyle ki $f_0, f_1, f_2, f_3 \in \mathcal{L}_f$ ve $g_0, g_1, g_2, g_3 \in \mathcal{L}_g$. Ayrıca F kuaterniyonu, hem A_p hem de A_q içinde tersinir olmalıdır. Bunun ise seçilen f_0, f_1, f_2, f_3 elemanlarına bağlı olduğu hemen farkedilebilir. ${F_p}^{-1}$ ve ${F_q}^{-1}$, F kuaterniyonunun sırasıyla A_p ve A_q içindeki tersleri olsun. Bu durumda,

$${F_p}^{-1} = \left({f_0}^2 + {f_1}^2 + {f_2}^2 + {f_3}^2\right).(\zeta_0 + \zeta_1 i + \zeta_2 j + \zeta_3 k)$$

ve

$${F_q}^{-1} = \left({f_0}^2 + {f_1}^2 + {f_2}^2 + {f_3}^2\right).(\eta_0 + \eta_1 i + \eta_2 j + \eta_3 k)$$

olmak üzere, açık anahtar

$$H = {F_q}^{-1}.G \in A_q$$

kuaterniyonudur (Malekian vd., 2011).

QTRU Şifreleme:

Şifreleme prosedüründe sistem ilk olarak $\phi_0, \phi_1, \phi_2, \phi_3 \in \mathcal{L}_\phi$ olan bir

$$\phi = \phi_0 + \phi_1 i + \phi_2 j + \phi_3 k$$

kuaterniyonunu üretir. Aynı zamanda, $m_0, m_1, m_2, m_3 \in \mathcal{L}_m$ olmak üzere bir

$$m = m_0 + m_1 i + m_2 j + m_3 k$$

mesajı,

$$E = pH.\phi + m \in A_q$$

şeklinde şifrelenir (Malekian vd., 2011).

QTRU Deşifreleme:

Gelen bir E şifreli mesajını çözmek için QTRU sisteminde izlenmesi gereken yol aşağıdaki gibidir: F gizli anahtarı yardımıyla,

$$\begin{aligned} B \coloneqq F.E &= F.(pH.\phi + m)\ (mod\ q) \\ &= F.(pH.\phi) + F.m\ (mod\ q) \\ &= pF.F_q^{-1}.G.\phi + F.m\ (mod\ q) \\ &= pG.\phi + F.m \in A_q \end{aligned}$$

şeklinde elde edilen B kuaterniyonunun dört polinomundaki katsayıların hepsi $mod\ q$ indirgenmiş olmalıdır ve NTRU benzeri oluşturulan diğer sistemlerdeki gibi tüm katsayılar pozitif aralıktan olacak şekilde değil de katsayıların ortalanması olarak da değerlendirilebilen $(-\frac{q}{2}, \frac{q}{2}]$ aralığında olacak şekilde dizayn etme işlemine tabi tutulmalıdır (Malekian vd., 2011). Diğer bir deyişle, $\{-\frac{q}{2}+1, \dots, \frac{q}{2}\}$ ayrık temsilciler kümesinin elemanlarıyla katsayılar yeniden yazılmalıdır. Burada, $B \in \frac{\mathbb{Z}_q[x]}{\langle x^N-1\rangle}$ elemanı tam olarak $B\ (mod\ p)$ indirgenmiş olduğunda,

$$B = pG.\phi + F.m \in A$$

olacaktır. Sonra, $(mod\ p)$ işlemiyle $pG.\phi$ teriminin ortadan kalkmasıyla birlikte,

$$F.m\ (mod\ p)$$

kalır ki en son bu terime; katsayıların ortalanması yani $[\left\lfloor -\frac{p}{2} \right\rfloor, \left\lfloor \frac{p}{2} \right\rfloor]$ aralığında terimlerin yeniden dizayn edilerek F_p^{-1} ters elemanı uygulandığında $F_p^{-1}.F.m = m$ şifrelenen düz metin mesajına ulaşılır (Malekian vd., 2011).

5. TARTIŞMA VE SONUÇ

Bu tezde, kuantum sonrası dönemde önem kazanan kriptografik yaklaşımlar çerçevesinde, halka tabanlı bir yapı üzerine inşa edilen NTRU kriptosistemi ve buna benzer şekilde tasarlanan MaTRU, CTRU, DTRU, ETRU ve QTRU gibi sistemler kapsamlı bir şekilde ele alınmıştır. Öncelikle NTRU kriptosisteminin temel matematiksel yapısı ayrıntılı olarak incelenmiş; sistemin halka yapısı, kafes teorisiyle olan ilişkisi ve şifreleme–deşifreleme süreçleri açıklanarak, sistemin hem teorik hem de uygulamalı yönleri ortaya konmuştur. Silverman vd. (2008)'ın belirttiği eşitsizlik doğrultusunda uygun parametreler seçilerek oluşturulan bir anahtar örneğiyle, seçilen bir mesajın şifrelenip deşifrelenmesi işlemleri altında gerçekten de olasılıksal NTRU sisteminde deşifreleme işleminin düz metin mesajının tamamen kendisini verdiği somut olarak görülmüştür. NTRU'nun güvenliğinin temel dayanaklarından biri olan SVP (En Kısa Vektör Problemi) ve CVP (En Yakın Vektör Problemi) gibi çözümü zor problemler ile olan bağlantısı vurgulanmıştır. Klasik RSA ya da ElGamal gibi çarpanlara ayırma problemi ya da ayrık logaritma problemi temelli sistemlere kıyasla NTRU'nun kuantum bilgisayarlar karşısında sunduğu direncin önemi tartışılmıştır.

NTRU'nun performans açısından oldukça avantajlı olduğu; anahtar boyutlarının görece düşük olması, şifreleme ve deşifreleme işlemlerinin hızlı gerçekleşmesini etkilediğinden günümüzde hala güvenlik anlamında geçerliliğini koruyan bir sistem olduğu ve düşük enerji tüketimi gerektiren uygulamalarda tercih edilebileceği düşünülmektedir. Ancak, avantajlarının yanında, sistemin parametre seçimi konusundaki hassasiyetleri ve belirli saldırı türlerine (özellikle seçilen mesaj saldırıları ve çin kalan teoremi (CRT) saldırıları) karşı sistemin geliştirilmesi gerektiği farkedilmiştir (Gaborit vd., 2002). Bu yönüyle, NTRU'nun sadece teorik değil, aynı zamanda uygulamada da barındırdığı güvenlik açıklarının olabileceği ve bu açıdan sistemsel olarak gelişime açık bir sistem olduğu düşünülmektedir. Bu tezde, NTRU temel alınarak geliştirilen MaTRU, CTRU, DTRU, ETRU ve QTRU gibi bazı kriptosistemlerin ortaya çıkış motivasyonları matematiksel açıdan tartışılmış, dayandığı cebirsel yapılar tanım ve ön bilgileri ile verilmiş ve bu sistemlerin, NTRU'daki bazı zayıflıkları gidermeyi amaçladıkları görülmüştür.

Tezde ele alınan sistemlerden bir tanesi olan MaTRU kriptosisteminde anahtarların matris çiftleri ve matrislerin değişmeli olmayan yapılar olması, kaba kuvvet saldırıları konusunda çok büyük bir öneme sahiptir. Değişmeli olmayan yapılarda anahtarların denenme hızının genelde değişmeli yapılara göre daha yavaş olması düşünülebilir. Nitekim, kaba kuvvet saldırılarında saldırganın olası tüm (f, g) anahtar çiftini, $f * h * g$ olacak şekilde denemesi gerekmektedir. A ve B matrisleri açık ve f ve g matrisleri de $2k$ tane polinomdan oluştuğu için, her birinin $n-1$. dereceden olması da düşünüldüğünde denenebilecek olası tüm anahtar çiftlerinin sayısı

$$\left(\frac{n!}{(n-(p-1)d_f)!\, d_f!^{(p-1)}}\right)^{2k}$$

dır (Coglianese ve Goi, 2005). Bu da göstermektedir ki MaTRU kriptosistemi için kullanılan matrislerin boyutları ile anahtar güvenliği arasında bir doğru orantı mevcuttur. Ayrıca, (N, p, q, d) NTRU kriptosistemin parametreleri ve (n, k, p, q) MaTRU kriptosisteminin parametreleri olmak üzere, düz metin mesajlarının boyutlarının karşılaştırılması $N = nk^2$ ilişkisi ile mümkün olup, işlem hızı NTRU için $\mathcal{O}(N^2)$ iken MaTRU kriptosisteminde $\mathcal{O}(n^2k^3)$ olduğundan, MaTRU kriptosisteminin değişmeli olmayan yapılar içermesine rağmen, şifreleme-deşifreleme hızının NTRU kriptosistemine nazaran daha yüksek olması bir hayli ilginçtir (Coglianese ve Goi, 2005).

CTRU kriptosistemine yapılacak olası bir kaba kuvvet saldırısında,

$$e - \phi h \ (mod\ q)$$

değerlerinin hesaplanması için denenebilecek tüm durumlar doğrudan ϕ ve g parametrelerine bağlı olduğundan, anahtar güvenliği ile $\mathcal{L}_\phi$ ve $\mathcal{L}_g$ kafeslerinin büyüklükleri arasında bir doğru orantıdan bahsedilebilir ve ayrıca NTRU sistemiyle aynı N parametresinin CTRU için yaklaşık olarak aynı zaman karmaşıklığı sunmasından dolayı güvenlik analizi yaparken N parametrelerinin karşılaştırılmasının önemli olmadığı belirtilmiştir. (Gaborit vd., 2002).

Dual tamsayılara dayalı olarak üretilen DTRU kriptosisteminde de anahtar güvenliğinin,

$$|\mathcal{L}(d)| = \binom{N}{d}\binom{N-d}{d}\binom{N-2d}{d}\binom{N-3d}{d} = \frac{N!}{(d!)^4(N-4d)!}$$

eşitliğine bağlı olduğu belirtilmiştir (Camara vd., 2018).

Eisenstein tamsayıları üzerinde kurulan ETRU kriptosisteminde Jarvis ve Nevins (2015), NTRU kriptosistemine yapılabilecek en güçlü saldırıların kafes saldırıları olduğunu ve ETRU parametrelerinin NTRU'daki (N, q) parametreleri ile karşılaştırıldığında, eğer $N' \approx 2N$ ve $q' \approx \frac{8}{3}q$ şeklinde seçim yapılırsa ETRU'nun NTRU'ya eşit ya da ondan daha fazla güvenlik sağladığını belirtmiştir. Bu da parametrik ayarlamalarla mümkün olduğu için uygulanabilirlik açısından ETRU'nun da etkili bir sistem olduğu düşünülmektedir.

Kuaterniyonlar cebirine dayalı olarak NTRU benzeri oluşturulan QTRU kriptosisteminde Malekian vd. (2011), önerdikleri sistemin 41 boyutlu olması durumunda NTRU-167 ile eş değer bir güvenlik sağlamaktadır. Ayrıca tüm kriptosistemlerde olduğu gibi QTRU kriptosisteminde de açık anahtarları bilen bir saldırgan, deşifreleme işleminin başarıya ulaşması adına kısa anahtar bulabilmek için olası tüm durumları denemek zorundadır. QTRU sisteminde

$$|\mathcal{L}(f)|(\approx |\mathcal{L}(g)|)$$

olup

$$|\mathcal{L}(f)| = \binom{N}{d_f}^4 \binom{N-d_f}{d_f}^4 = \frac{(N!)^4}{\left(d_f!\right)^8 \left(N-2d_f\right)!^4}$$

ve

$$|\mathcal{L}(g)| = \binom{N}{d_g}^4 \binom{N-d_g}{d_g}^4 = \frac{(N!)^4}{\left(d_g!\right)^8 \left(N-2d_g\right)!^4}$$

olarak elde edilmiştir ki uygun parametreli bir QTRU kriptosistemine karşı yapılan kaba kuvvet saldırılarının başarıya ulaşmasının pratikte imkansız olduğu değerlendirilmektedir (Malekian vd., 2011).

Malekian vd. (2011), QTRU kriptosisteminin gerek değişmeli olmayan yapılarda çalışması ve gerekse NTRU kriptosistemine göre dört kat fazla işlem içermesi nedeniyle NTRU'dan daha düşük bir şifreleme-deşifreleme hızına sahip olsa da, kafes ataklarına karşı NTRU'dan daha dirençli olduğunu belirtmiştir.

NTRU benzeri yapılan kriptosistemler çalışıldığında farkedilmiş olmalıdır ki kuantum saldırılara karşı deterministik olarak üretilen kriptosistemler güvenlik açısından etkili değildir. Bu doğrultuda, Vats (2008), iki elemanlı bir cisim üzerinde tanımlı tek değişkenli polinomlarla oluşturulan kesilmiş polinomlar üzerindeki CTRU kriptosisteminin polinom zamanlı bir algoritmayla kırıldığını göstermiştir. Böylece, uygulamada CTRU kriptosisteminin etkili olmadığı söylenebilir.

Camara vd. (2018) DTRU kriptosisteminin NTRU kadar güvenli olabileceğini fakat katsayıları dual tamsayılarla oluşturulan kesilmiş polinomların terslerini almak için etkili ve kalanı tek türlü verecek şekilde bir bölme algoritmasının zorluğunu ve sistemin daha fazla etkili olmadığını belirtmiştir ki bu da literatürdeki DTRU'ya olan ilgiyi olumsuz etkileyecektir denebilir.

Sırasıyla Coglianese ve Goi (2005), Gaborit vd. (2002), Camara vd. (2018), Jarvis ve Nevins (2015) ve Malekian vd. (2011) tarafından yapılan çalışmalardan yararlanılarak incelenen MaTRU, CTRU, DTRU, ETRU ve QTRU kriptosistemlerinin NTRU ile karşılaştırılması aşağıda sunulan Çizelge 5.1 ve Çizelge 5.2 ile kısaca özetlenmiştir.

Çizelge 5.1 NTRU benzeri bazı kriptosistemlerin karşılaştırılması-I

Kriptosistem	Cebirsel Yapı	Sistemin Avantajları	Sistemin Dezavantajları
NTRU	$\mathbb{Z}[X]/\langle X^n - 1\rangle$	Standardize olması	Kafes tabanı indirgeme algoritmalarının gelişmesiyle ortaya çıkan güvenlik tehdidi
MaTRU	$M_k(\mathbb{Z}[X]/\langle X^n - 1\rangle)$	Şifreleme-deşifreleme hızının uygun parametrelerle NTRU'dan 2.5 kat hızlı olabilmesi	Deşifrelemedeki değişmeli anahtarların güvenlik açığına sebebiyet verebilmesi
CTRU	$\mathbb{F}_2[T][X]/\langle X^n - 1\rangle$	-	Kırılmıştır. (Vats, 2008)

Çizelge 5.2 NTRU benzeri bazı kriptosistemlerin karşılaştırılması-II

Kriptosistem	Cebirsel Yapı	Sistemin Avantajları	Sistemin Dezavantajları
NTRU	$\mathbb{Z}[X]/\langle X^n - 1\rangle$	Standardize olması	Kafes tabanı indirgeme algoritmalarının gelişmesiyle ortaya çıkan güvenlik tehdidi
DTRU	$D[X]/\langle X^n - 1\rangle$ öyle ki $D = \mathbb{Z} + \varepsilon\mathbb{Z}$ ve $\varepsilon^2 = 0$	NTRU güvenliğine (yaklaşık olarak) sahip olma potansiyeli	Bölme algoritması oluşturma zorluğu ve sistemin daha etkili olmayışı
ETRU	$\mathbb{Z}[\omega][X]/\langle X^n - 1\rangle$ öyle ki $\omega^3 = 1$	Daha küçük anahtar boyutlarıyla daha hızlı hesaplamalar ve güvenlik	Standardize olmaması
QTRU	$A[X]/\langle X^n - 1\rangle$ öyle ki $A = \left(\frac{-1,-1}{\mathbb{Z}}\right)$	Değişmeli olmayan işlemlerle daha fazla güvenlik potansiyeli	NTRU'dan dört kat daha yavaş çalışması

Sonuç olarak, bu tezde etkili ya da güvenli olup olmamasından bağımsız olarak çalışılan söz konusu NTRU benzeri kriptosistemlerin altında yatan cebirsel yapıların kriptografik uygulamalarda nasıl kullanılabileceği ele alınmıştır. Kuantum bilgisayarların gelecekte daha güçlü ve daha yaygın olacağı fikrine dayanarak, özellikle kafes tabanlı saldırılara karşı daha güçlü sistemler oluşturmak adına araştırmacıların bu yönde ilgisinin artarak devam edeceği düşünülmektedir.

KAYNAKLAR

Ajtai, M. (1996). *Generating hard instances of lattice problems*. Electronic Colloquium on Computational Complexity (ECCC), TR96-007. https://eccc.weizmann.ac.il/eccc-reports/1996/TR96-007/index.html?utm_source=chatgpt.com

Ajtai, M. (1998). The shortest vector problem in L2 is NP-hard for randomized reductions. In **Proceedings of the 30th Annual ACM Symposium on Theory of Computing (pp. 10–19).** ACM.

Banin, M., Tsaban, B. (2012). The discrete logarithm problem in Bergman's non-representable ring. *Journal of Mathematical Cryptology*, 6, 171-182.

Cai, JY. (2000). The Complexity of Some Lattice Problems. In: ***Bosma, W. (eds) Algorithmic Number Theory. ANTS 2000. Lecture Notes in Computer Science***, vol 1838. Springer, Berlin, Heidelberg. https://doi.org/10.1007/10722028_1

Camara, M. G., Sow, D., Sow, D. (2018). DTRU1: First generalization of NTRU using dual integers. *International Journal of Algebra*, 12(7), 257–271.

Cao, Z. (2012). ***New directions of modern cryptography*** (1st ed.). CRC Press. https://doi.org/10.1201/b14302

Cohen, H. (1995). ***A course in computational algebraic number theory.*** Springer-Verlag.

Coglianese, M., Goi, B. M. (2005). MaTRU: A new NTRU-based cryptosystem. In S. Maitra, C. E. Veni Madhavan, & R. Venkatesan (Eds.), *Progress in Cryptology – INDOCRYPT 2005* (Vol. 3797). Springer.

Coppersmith, A., Shamir, A. (1997). Lattice attacks on NTRU. In ***Proceedings of EUROCRYPT '97*** (Vol. 1233, pp. 52–61). Springer.

Diffie, W., Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22, 644–654.

Dwork, C. (1998). ***Lattices and their application to cryptography***. Lecture Notes, Stanford University, Spring 1998.

ElGamal, T. (1985). A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31, 469–472.

Gaborit, P., Ohler, J., & Solé, P. (2002). *CTRU: A polynomial analogue of NTRU* (Research Report No. 4621). INRIA. https://hal.inria.fr/inria-00071964/

Goldreich, O., Goldwasser, S., Halevi, S. (1996). *Public key cryptosystems from lattice reduction problems*. Electronic Colloquium on Computational Complexity (ECCC), TR96-056. https://eccc.weizmann.ac.il/report/1996/056/

Goldreich, O., Micciancio, D., Safra, S., Seifert, J. P. (1999). Approximating shortest lattice vectors is not harder than approximating closest lattice vectors. *Information Processing Letters*, 71(2), 55–61.

Hanoymak, T., Küsmüş, Ö. (2015). On construction of cryptographic systems over units of group rings. *International Electronic Journal of Pure and Applied Mathematics*, 9(1), 37–43.

Hanoymak, T., Küsmüş, Ö. (2019). A new multi-party key exchange protocol and symmetric key encryption scheme over non-commutative group rings. *International Journal of Information Security Science*, 8(1), 11–16.

Hoffstein, J., Pipher, J., Silverman, J. H. (1998). NTRU: A ring-based public key cryptosystem. In *Algorithmic Number Theory* (Vol. 1423, pp. 267–288). Lecture Notes in Computer Science. Springer.

Hoffstein, J., Silverman, J. H. (2003). Random small Hamming weight products with applications to cryptography. *Discrete Applied Mathematics*, 130, 37–49.

Hoffstein, J., Silverman, J. H. (2000). Optimizations for NTRU. In ***Public Key Cryptography and Computational Number Theory*.** Warsaw.

Hoffstein, J., Silverman, J. H., Whyte, W. (2003). *Estimated breaking times for NTRU lattices*. NTRU Cryptosystems Technical Report 12 – Version 2. Erişim tarihi:1 Eylül 2025. Erişim adresi: https://ntru.org/f/tr/tr012v2.pdf

Howgrave-Graham N., Silverman, J. H., Whyte W. (2003). *A meet-in-the-middle attack on an NTRU private key*. NTRU Cryptosystems Technical Report 4 – Version 2. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://ntru.org/f/tr/tr004v2.pdf

Howgrave-Graham, N., Silverman, J. H., Whyte, W. (2005). Choosing parameter sets for NTRUEncrypt with NAEP and SVES-3. In ***Topics in Cryptology*** – CT-RSA (Vol. 3376, pp. 118–135). Lecture Notes in Computer Science.

Hungerford, T.W. (1974). ***Algebra***. Springer.

Hurley, B., Hurley, T. (2011). Group ring cryptography. *International Journal of Pure and Applied Mathematics*, 69, 67–86.

Inam, S, Ali, R. (2018). A new ElGamal-like cryptosystem based on matrices over group ring. *Neural Computing and Applications*, 29, 1279-1283.

Jarvis, K., Nevins, M. (2015). ETRU: NTRU over the Eisenstein integers. *Designs, Codes and Cryptography*, 74, 219-242.

Jarvis, K. (2011). *NTRU over the Eisenstein integers*. M.Sc. Thesis, University of Ottawa, Canada.

Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177), 203–209.

Küsmüş, Ö., Hanoymak, T. (2022). A novel public key encryption scheme based on Bass cyclic units in integral group rings. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(2), 579-589. https://doi.org/10.1080/09720529.2020.1756042

Lenstra, A. K., Lenstra, H. W., Jr., Lovász, L. (1982). Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261(4), 515–534.

Liu, L., Ye, J. (2018) Identity-based re-encryption scheme with lightweight re-encryption key generation. *Journal of Discrete Mathematical Sciences and Cryptography*, 21(1), 41-57.

Malekian, E., Zakerolhosseini, A. (2010). QTRU: A non-associative and high speed public key cryptosystem. In **Proceedings of IEEE Computer Society**, 83–90.

Malekian, E., Zakerolhosseini, A., Mashatan, A. (2011). QTRU: Quaternionic version of the NTRU public-key. *The ISC International Journal of Information Security*, 3(1), 29–42.

May, A. (1999). *Cryptanalysis of NTRU*. preprint. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d9afae316fc92954f2c23bf85bc15b3c328ed2c8

Micciancio, D. (1999). *Lattices in cryptography and cryptanalysis*. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: http://cseweb.ucsd.edu/~daniele/CSE207C/

Milies, C. P., Sehgal, S. K. (2002). ***An introduction to group rings.*** Kluwer Academic Publishers.

Miller, V. (1985). Use of elliptic curves in cryptography. In ***Advances in Cryptology – CRYPTO '85*** (Vol. 218, pp. 417–426). Lecture Notes in Computer Science. Springer.

Mumtaz, M., Ping, L. (2019). Forty years of attacks on the RSA cryptosystem: A brief survey. *Journal of Discrete Mathematical Sciences and Cryptography*, 22(1), 9-29, https://doi.org/10.1080/09720529.2018.1564201

Myasnikov, A., Shpilrain, V., Ushakov, A. (2011). Non-commutative cryptography and complexity of group-theoretic problems. *American Mathematical Society*, 177. https://doi.org/10.1090/surv/177

Nathani, S., Tripathi, B. P. (2017). Key exchange protocol based on quaternions. *Advances in Computational Sciences and Technology*, 10(8), 2333–2343.

Nevins, M., Karimianpour, C., Miri, A. (2010). NTRU over rings beyond Z. *Designs, Codes and Cryptography*, 56, 65–78.

Parvathi, P.M.S., Srinivasan, C. (2020). Matrix Lie group as an algebraic structure for NTRU-like cryptosystem. *Journal of Discrete Mathematical Sciences and Cryptography*, 23(7), 1455-1464, https://doi.org/10.1080/09720529.2020.1753302

Passman, D. S. (1977). ***The algebraic structure of group rings***. Wiley.

Rivest, R. L., Shamir, A., Adleman, L. (1978). A method for obtaining digital signature and public key cryptosystems. *Communications of the ACM*, 21, 120–126.

Satoh, T., Araki, K. (1997). On construction of signature scheme over a certain noncommutative ring. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E80-A(1), 40-45.

Schnorr, C. P. (1987). A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, 53, 201–224.

Schnorr, C. P., Euchner, M. (1994). Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Mathematical Programming*, 66, 181–199.

Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5), 1484–1509.

Shuai, L., Xu, H., Miao, L., Zhou, X. (2019). A group-based NTRU-like public-key cryptosystem for IoT. *IEEE Access*, 7, 75732–75740. https://doi.org/10.1109/ACCESS.2019.2920860

Silverman, J. H. (1998). *Invertibility in truncated polynomial rings*. NTRU Cryptosystems Technical Report 9. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://ntru.org/f/tr/tr009v1.pdf

Silverman, J. H. (1999a). *Almost inverses and fast NTRU key creation*. NTRU Cryptosystems Technical Report 14. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://ntru.org/f/tr/tr014v1.pdf

Silverman, J. H. (1999b). *High-speed multiplication of (truncated) polynomials*. NTRU Cryptosystems Technical Report 10. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://ntru.org/f/tr/tr010v1.pdf

Silverman, J. H., Pipher, J., Hoffstein, J. (2008). ***An introduction to mathematical cryptography***, Springer, New York, NY.

Silverman, J. H. (2001). *Wraps, gaps and lattice constants.* NTRU Cryptosystems Technical Report 11 – Version 2. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://ntru.org/f/tr/tr011v2.pdf

Silverman, J. H., Whyte, W. (2003). *Estimating decryption failure probabilities for NTRUEncrypt.* NTRU Cryptosystems Technical Report 18. Erişim tarihi: 31 Ağustos 2025. Erişim adresi: https://www.ntru.org/f/tr/tr018v1.pdf

Tekin, S. (2011). *NTRU Kriptosistemi*, Yüksek lisans tezi. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul, Türkiye.

Vats, N. (2008). Algebraic cryptanalysis of CTRU cryptosystem. In X. Hu & J. Wang (Eds.), *Computing and combinatorics: COCOON 2008* (Lecture Notes in Computer Science, Vol. 5092, pp. 235–244). Springer. https://doi.org/10.1007/978-3-540-69733-6_24

Vats, N. (2009). NNRU: A non-commutative analogue of NTRU. arXiv preprint, arXiv:0902.1891v1.

Voronoi, G. (1908a) Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Deuxième mémoire. Recherches sur les parallélloèdres primitifs. *Journal für die Reine und Angewandte Mathematik (Crelles Journal)*, 1908(134), 198-287. https://doi.org/10.1515/crll.1908.134.198

Voronoi, G. (1908b) Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites. *Journal für die Reine und Angewandte Mathematik (Crelles Journal)*, 1908(133), 97-102. https://doi.org/10.1515/crll.1908.133.97

ÖZ GEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Gülbahar ÇAL

Eğitim Bilgileri

Lisans

Üniversite : Van Yüzüncü Yıl Üniversitesi
Fakülte : Fen Fakültesi
Bölüm : Matematik Bölümü
Mezuniyet Yılı : 2023

VAN YÜZÜNCÜ YIL ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
LİSANSÜSTÜ TEZ ORİJİNALLİK RAPORU

Tarih 09/09/2025

Tez Başlığı: NTRU Benzeri Bazı Kriptosistemler ve Karşılaştırılması

Yukarıda başlığı belirtilen tez çalışmamın, kapak sayfası, giriş, ana bölümler ve sonuç bölümlerinden oluşan toplam 53 (elliüç) sayfalık kısmına ilişkin, 09/09/2025 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre tezimin benzerlik oranı %8 (sekiz)'dir.

Uygulanan filtreler aşağıda verilmiştir:

- Kabul ve onay sayfası hariç,
- Teşekkür hariç,
- İçindekiler hariç,
- Simge ve kısaltmalar hariç,
- Gereç ve yöntemler hariç,
- Kaynakça hariç,
- Alıntılar hariç,
- Tezden çıkan yayınlar hariç,
- 7 kelimeden daha az örtüşme içeren metin kısımları hariç (Limit match size to 7 words)

Van Yüzüncü Yıl Üniversitesi Lisansüstü Tez Orijinallik Raporu Alınması ve Kullanılmasına İlişkin Yönergeyi inceledim ve bu yönergede belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini bilgilerinize arz ederim.

09.09.2025

Adı Soyadı: Gülbahar ÇAL
Öğrenci No: 23910024003
Anabilim Dalı: Matematik
Programı: Matematik
Statüsü: (X) Yüksek Lisans ( ) Doktora

DANIŞMAN	**ENSTİTÜ ONAYI**
UYGUNDUR	UYGUNDUR