T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ HALKASI ÜZERİNDE DEVİRLİ KODLAR YARDIMIYLA GÜVENLİ ŞİFRELEME

YÜKSEK LİSANS TEZİ

Neriman ŞOLT

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Murat GÜZELTEPE**

Haziran 2022

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

$\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ HALKASI ÜZERİNDE DEVİRLİ KODLAR YARDIMIYLA GÜVENLİ ŞİFRELEME

YÜKSEK LİSANS TEZİ

Neriman ŞOLT

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**

Bu tez 30/06/2022 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.

Jüri Başkanı	**Üye**	**Üye**

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Neriman ŞOLT
30.06.2022

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Murat GÜZELTEPE'ye teşekkürlerimi sunarım.

Çalışmamla ilgili bilgi ve desteğini almaktan çekinmediğim Doç. Dr. Selda ÇALKAVUR'a değerli desteklerinden dolayı teşekkürlerimi sunarım.

Hayatım boyunca her kararımda yanımda duran ve beni destekleyen kıymetli aileme teşekkürlerimi sunarım.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

R	: $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ halkası
S	: $\mathbb{F}_2+v\mathbb{F}_2$ halkası
$GF(q)$	: Galois cismi
$(G,*)$	: Grup
$(R,+,\bullet)$	: Halka
w_H	: Hamming ağırlığı
W_L	: Lee ağırlığı
d_L	: Lee uzaklığı
R/M	: R halkasının M idealine göre bölüm halkası

ÖZET

Anahtar kelimeler: Tek kullanımlık karakter dizisi ile şifreleme, devirli kodlar ile şifreleme, şifre çözme.

Bu çalışma dört bölümden oluşmaktadır. İlk bölümde cebir ve kodlama teorisi ile ilgili, çalışmanın diğer bölümlerinde kullanılan temel tanımlar ve teoremler verilmiştir.

İkinci bölümde tek kullanımlık karakter dizisi tanıtılmış ve $\mathbb{F}_2 + v\mathbb{F}_2$ halkası üzerindeki devirli kodlar kullanılarak geliştirilen güvenli şifreleme modeli incelenmiştir.

Üçüncü bölümde $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ halkası incelenmiş ve ikinci bölümde kullanılan yöntem bu halkaya uyarlanmıştır. Yeni şifreleme modeli elde edilmiştir ve örneklendirilmiştir. $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ halkası üzerinde güvenli şifreleme şeması oluşturulmuştur.

Son bölümde ise sonuçlara yer verilmiştir ve şifreleme şemasıyla ilgili yeni problemler önerilmiştir.

SECURE ENCRYPTION OVER THE RING $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ VIA THE CYCLIC CODES

SUMMARY

Keywords: Encryption with one time pad method, encryption with cyclic codes, decryption.

This study consists of four sections. In the first section, basic definitions and theorems are given that are used in other sections of study associated with coding theory and algebra.

In the second section, one time pad method is introduced and secure encryption method developed using cyclic codes over the ring $\mathbb{F}_2 + v\mathbb{F}_2$ is examined.

In the third section, the ring of $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ is examined and the method used in the second section is adapted to this ring. The new encryption model is obtained and exemplified. Secure encryption scheme is created over the ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$.

In the last section, the conclusions are given and new problems related to the encryption scheme are proposed.

BÖLÜM 1. GİRİŞ

Bu bölümde verilen temel tanım, teorem ve önermeler diğer bölümlerde kullanılacak ön bilgiler niteliğindedir.

1.1. Temel Tanım ve Teoremler

Tanım 1.1.1. $A\times A$ dan A ya bir fonksiyona A da bir ikili işlem denir.

"$*$", A da bir ikili işlem ve $a,b\in A$ olsun. (a,b) ikilisinin "$*$" işlemi altındaki görüntüsü $a*b$ ile gösterilir. Fonksiyon olma özelliklerinden $\forall a,b\in A$ için A da bir $a*b$ elemanının var olmasına işlemin kapalılığı denir [1].

Tanım 1.1.2. G boş olmayan bir küme ve "$*$", G de bir ikili işlem olsun. $(G,*)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa G ye bir grup denir.

1. "$*$" işleminin G de birleşme özelliği vardır. Yani, $\forall a,b,c\in G$ için, $a*(b*c)=(a*b)*c$ dir.
2. "$*$" işleminin, G de birim elemanı vardır. Yani , $\forall a\in G$ için, $a*e=e*a=a$ olacak şekilde $\exists a\in G$ vardır.
3. "$*$" işlemine göre, G deki her elemanın bir tersi vardır. Yani, $a\in G$ için $a*a^{-1}=a^{-1}*a=e$ olacak şekilde $\exists a^{-1}\in G$ vardır [1].

Tanım 1.1.3. G bir grup ve $\forall a,b\in G$ için $a*b=b*a$ oluyor ise G ye bir değişmeli (Abel) grup denir [1].

Tanım 1.1.4. $R \neq \varnothing$ kümesi üzerinde tanımlı iki ikili işlem "+" ve "•" olsun. Aşağıdaki aksiyomları sağlayan $(R,+,\bullet)$ cebirsel yapısına bir halka denir.

1. $(R,+)$ bir değişmeli gruptur.
2. "•" işleminin R de birleşme özelliği vardır.
3. "•" işleminin "+" işlemi üzerine sağdan ve soldan dağılma özellikleri vardır. Yani, $\forall a,b,c \in R$ için, $a\bullet(b+c) = a\bullet b + a\bullet c$ ve $(a+b)\bullet c = a\bullet c + b\bullet c$ dir.

Halkanın "+" işlemine göre etkisiz elemanına halkanın sıfır elemanı denir ve 0_R ile gösterilir. Halkanın "•" işlemine göre etkisiz elemanı varsa buna halkanın birim elemanı denir ve 1_R ile gösterilir. Birim elemanı olan halkaya birimli halka denir [1].

Tanım 1.1.5. R bir halka olsun. Eğer, her $a \in R$ için, $na = 0$ olacak şekilde bir $n > 0$ tam sayısı varsa, böyle $n > 0$ tam sayılarının en küçüğüne R halkasının karakteristiği denir. Eğer böyle bir $n > 0$ tam sayısı bulunamıyorsa R nin karakteristiği sıfır kabul edilir [1].

Tanım 1.1.6. $(R,+,\bullet)$ bir halka olmak üzere, $\forall a,b \in R$ için $a\bullet b = b\bullet a$ oluyor ise $(R,+,\bullet)$ halkasına değişmeli halka denir [2].

Tanım 1.1.7. Birimli bir R halkasında $a \in R$ için $ab = ba = 1_R$ olacak şekilde $b \in R$ varsa a elemanına terslenebilen eleman denir [1].

Tanım 1.1.8. R birimli ve değişmeli bir halka ve $R - \{0_R\} = R^*$, ikinci işlem "•" ya göre bir grup ise R ye bir cisim denir [1].

Tanım 1.1.9. R bir halka ve $\varnothing \neq S \subset R$ olsun. R deki işlemlere göre S alt kümesi kendi başına bir halka ise S ye R halkasının bir alt halkası denir [1].

Tanım 1.1.10. A, R halkasının bir alt kümesi olsun. R nin A yı kapsayan bütün alt halkalarının arakesitine A nın ürettiği alt halka denir ve bu $<A>$ ile gösterilir. A nın elemanlarına da $<A>$ nın üreteçleri denir [1].

Tanım 1.1.11. R bir halka ve $\varnothing \neq I \subset R$ olsun.

1. $\forall a,b \in I$ için $a-b \in I$,
2. $\forall a \in I$ ve $\forall r \in R$ için, $ra \in I$ (veya $ar \in I$)

ise I ya R nin bir sol (veya sağ) ideali denir. Hem sol hem de sağ bir ideale iki taraflı ideal veya kısaca ideal denir [1].

Tanım 1.1.12. A, R halkasının bir alt kümesi olsun. R nin, A yı kapsayan bütün ideallerinin arakesitine A nın ürettiği ideal denir ve bu (A) ile gösterilir. Eğer $A=\{a\}$ tek elemanlı bir küme ise A nın ürettiği ideale temel ideal denir ve bu (a) ile gösterilir [1].

Tanım 1.1.13. R değişmeli bir halka ve M de R nin kendisinden farklı bir ideali olsun. Eğer R nin M yi kapsayan M ve R den başka hiçbir ideali yoksa, M ye R nin bir maksimal ideali denir [1].

Tanım 1.1.14. R bir halka ve I, R nin bir ideali olsun. "$\equiv$" bağıntısı, $\forall a,b \in R$ için $a \equiv b \pmod{I} \Leftrightarrow a-b \in I$ olarak tanımlanır [1].

Önerme 1.1.1. Yukarıda tanımlanan "$\equiv$" bağıntısı R de bir denklik bağıntısıdır. Bu bağıntıya göre $r \in R$ nin denklik sınıfı $\bar{r} = r+I = \{r+a : a \in I\}$ dır. Bütün denklik sınıflarının kümesi R/I ile gösterilir [1].

Önerme 1.1.2. R halkasının, bir I idealine göre tanımlanan denklik sınıfları arasında $(a+I)\oplus(b+I)=(a+b)+I$ ve $(a+I)\odot(b+I)=(ab)+I$ ile tanımlanan "$\oplus$" ve "$\odot$" işlemlerine göre $R/I=\{r+I : r\in R\}$ bir halkadır. Bu halkaya R halkasının I idealine göre bölüm halkası denir [1].

Teorem 1.1.1. Birimli ve değişmeli bir R halkasının bir M idealinin, maksimal olması için gerek ve yeter koşul R/M bölüm halkasının bir cisim olmasıdır [1].

Tanım 1.1.15. R bir halka olsun. Eğer R halkası tek maksimal ideali olan bir halka ise R ye bir yerel (local) halka denir [2].

Tanım 1.1.16. R birimli ve değişmeli bir halka olmak üzere R halkasının tüm idealleri kapsama bağıntısına göre tam sıralı ise R halkasına sonlu zincir halkası denir [3].

Önerme 1.1.3. R sonlu zincir halkası ise her ideali esas idealdir ve R tek maksimal ideale sahiptir. R halkasının maksimal idealinin bir üreteci μ olsun. Bu durumda R halkasının tüm idealleri aşağıdaki gibi

$$R=\langle 1\rangle \supsetneq \langle \mu\rangle \supsetneq \langle \mu^2\rangle \supsetneq \ldots \supsetneq \langle \mu^{e-1}\rangle \supsetneq \langle \mu^{e}\rangle = \langle 0\rangle,$$

zincir şeklindedir [3].

Teorem 1.1.2. R birimli, değişmeli ve sonlu bir halka olmak üzere aşağıdaki koşullar denktir.

1. R bir yerel halkadır ve R nin maksimal ideali temel idealdir.
2. R bir yerel temel ideal halkasıdır.
3. R bir zincir halkasıdır [4].

Tanım 1.1.17. $(R,+,\bullet)$ ve $(M,\oplus,\odot)$ iki halka ve $g:R\to M$ bir fonksiyon olsun. Eğer $\forall a,b\in R$ için;

1. $g(a+b)=g(a)\oplus g(b)$ ve
2. $g(a\bullet b)=g(a)\odot g(b)$,

şartlarını sağlıyor ise g ye, R den M ye bir halka homomorfizması denir [5].

Teorem 1.1.3. $g:R\to R'$ bir halka homomorfizması olsun. Bu takdirde

1. M,R nin bir alt halkası ise $g(M)$ de R' nün bir alt halkasıdır.
2. I,R nin bir ideali ise $g(I)$ da $g(R)$ nin bir idealidir [5].

Tanım 1.1.18. $g:R\to M$ ye homomorfizması $1-1$ ve örten homomorfizma ise g ye bir izomorfizma denir ve $R\cong M$ şeklinde gösterilir [1].

Tanım 1.1.19. R bir halka, x bir bilinmeyen ve $a_0,a_1,\ldots,a_k$ lar R halkasının elemanları olmak üzere, $a_0+a_1x+\ldots+a_kx^k$ şeklindeki bir ifadeye katsayıları R den olan bir polinom denir. R halkasından katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir [1].

Tanım 1.1.20. R birimli bir halka ve $n,m\in\mathbb{Z}^+$ için

$$f(x)=a_0+a_1x+\ldots+a_nx^n\in R[x]$$
$$g(x)=b_0+b_1x+\ldots+b_mx^m\in R[x]$$

olsun. $c_i = \sum_{j=0}^{i} a_j b_{i-j}$ olmak üzere $R[x]$ kümesi üzerinde polinomların toplamı ve çarpımı aşağıdaki gibi tanımlanır [6]:

$$f(x)+g(x)=\sum_{i=0}^{\max(m,n)}(a_i+b_i)x^i,$$
$$f(x)\cdot g(x)=\sum_{i=0}^{m+n}(c_i x^i).$$

Önerme 1.1.4. R bir halka ise $R[x]$ de bir halkadır [1].

Önerme 1.1.5. R bir halka olsun.

1. R halkası birimli ise $R[x]$ halkası da birimlidir.
2. R halkası değişmeli ise $R[x]$ halkası da değişmelidir.
3. R halkası tamlık bölgesi ise $R[x]$ halkası da tamlık bölgesidir [1].

Tanım 1.1.21. R bir halka ve $(A,+)$ değişmeli grup olmak üzere $\forall r \in R$ ve $\forall a \in A$ için

$$f : R \times A \to A$$
$$(r,a) \to f(r,a) = ra,$$

şeklinde tanımlanan f fonksiyonu aşağıdaki özellikleri sağlıyorsa A değişmeli grubuna bir $R-$modül denir:

1. $\forall r \in R$, $\forall a,b \in A$ için, $r(a+b)=ra+rb$,
2. $\forall r,s \in R$, $\forall a \in A$ için, $(r+s)a=ra+sa$,
3. $\forall r,s \in R$, $\forall a \in A$ için, $r(sa)=(rs)a$,

4. $\forall a \in A$ için $1_R a = a$ [2].

Eğer R bir değişmeli halka değil ise sağ ve sol $R-$modül tanımı benzer şekilde yapılır.

Tanım 1.1.22. M bir $R-$modül ve $\varnothing \neq A \subset M$ olmak üzere $(A,+)$ grubu bir $R-$modül ise A ya M nin bir alt modülü denir [2].

Tanım 1.1.23. p bir asal sayı ve $n \in \mathbb{N}$ olmak üzere $q = p^n$ elemanlı cisme Galois cismi denir. Bu cisim $GF(q)$ veya $\mathbb{F}_q$ ile gösterilir [7].

1.2. Kodlama Teorisi ile İlgili Temel Tanım ve Teoremler

İnsanlığın var olmasıyla birlikte haberleşme bir ihtiyaç haline gelmiştir. İlk çağlardan beri insanlar birbirleriyle haberleşebilmek için çeşitli yöntemler geliştirmiştir. Yeni iletişim yöntemleri geliştikçe gizlilik kavramı ortaya çıkmıştır. Önemli bilgilerin gizlenmesi için ya yeni diller türetilmiştir ya da iletilmek istenilen mesaj gizlenerek iletilmiştir. Bilginin bu şekilde gizlenmesi kimi zaman bir resimle kimi zaman sembollerle sağlanmıştır. Mesajın gizlenmesi için kullanılan yöntemler günümüz kodlama teorisinin temelini oluşturmuştur.

Kodlama teorisi, gürültülü bir kanal boyunca gönderilen bilginin bozulması ihtimali düşünülerek bu bozulmaların (hataların) tespit edilmesi ve düzeltilmesi amacı ile ortaya çıkmıştır. Burada amaç cebirsel yapılar kullanılarak bilgiye bir takım eklemeler yapmaktır. Yapılan eklemeler sayesinde bilgi gizlenerek olası hatalar en aza indirgenir ve düzeltilir. Hataların tespit edilmesi ve düzeltilmesi için yapılan işlemlerin maliyeti ve performansı da son derece önemlidir. Kodlama teorisi de tam olarak bu konularla uğraşmaktadır. Kodlama teorisindeki amaç yüksek performanslı ve düşük maliyetli kodlar bulmaktır. Tüm bu işlemleri yaparken cebirsel yapıların kullanılmasıyla birlikte kodlama teorisi matematikçilerin çalışma alanını oluşturmuştur.

Çalışmanın bu kısmında kodlama teorisinde kullanılan kavramlarla ilgili genel tanım ve teoremler verilmiştir.

Tanım 1.2.1. $\mathbb{F}$ bir cisim ve $(V,+)$ bir grup olsun.

$$f:\mathbb{F}\times V\to V$$
$$(\lambda,w)\to f(\lambda,w)=\lambda w,$$

fonksiyonu aşağıdaki özellikleri sağlıyorsa V ye $\mathbb{F}$ cismi üzerinde bir vektör uzayı denir:

1. $1\in\mathbb{F}$ ve $\forall v\in V$ için, $1v=v$.
2. $\forall\lambda\in\mathbb{F}$ ve $\forall v,w\in V$ için, $\lambda(v+w)=\lambda v+\lambda w$.
3. $\forall\lambda,\mu\in\mathbb{F}$ ve $\forall v\in V$ için, $(\lambda+\mu)v=\lambda v+\mu v$.
4. $\forall\lambda,\mu\in\mathbb{F}$ ve $\forall v\in V$ için, $\lambda(\mu v)=(\lambda\mu)v$ [8].

Tanım 1.2.2. V, $\mathbb{F}$ cismi üzerinde bir vektör uzayı olsun ve $\varnothing\neq W\subseteq V$ sağlansın. W, V vektör uzayındaki işlemlere göre bir vektör uzayı ise W ye V nin bir alt vektör uzayı denir [8].

Tanım 1.2.3. $A=\{a_1,a_2,\ldots,a_q\}$, q elemalı bir küme olsun. Bu kümeye kod alfabesi denir.

1. A^n kümesinin boştan farklı bir C alt kümesine $q-$ lu blok kod ya da kısaca kod denir.
2. $u_1,u_2,\ldots,u_n\in A$ olmak üzere $u=(u_1,u_2,\ldots,u_n)\in C$ ise u ya n uzunluklu bir kodsöz denir. $u=(u_1,u_2,\ldots,u_n)$ kodu $u=(u_1u_2\ldots u_n)$ şeklinde de yazılır. Bu kodsözlerin sayısı $|C|$ ile gösterilir ve C nin büyüklüğü olarak adlandırılır.

3. n uzunluğunda ve M büyüklüğünde bir kod (n, M) kodu olarak tanımlanır [9].

Tanım 1.2.4. p bir asal sayı olmak üzere $p^k = q$ ve $\mathbb{F}_q$ sonlu bir cisim olsun. $\mathbb{F}_q^n$ vektör uzayının herhangi bir alt vektör uzayı bir lineer kod olarak tanımlanır [8].

Tanım 1.2.5. En az iki kodsöz içeren bir C kodunun minimum uzaklığı

$$d(C) = \min\{d(x, y) : x, y \in C, x \neq y\}$$

şeklinde tanımlanır [9].

Tanım 1.2.6. $x, \mathbb{F}_q^n$ vektör uzayında herhangi bir eleman olmak üzere x elamanının sıfırdan farklı bileşenlerinin sayısına x elemanının Hamming ağırlığı denir ve bu $w_H(x)$ ile gösterilir [9].

Teorem 1.2.1. $C, \mathbb{F}_q$ üzerinde bir lineer kod olsun. C kodunun minimum uzaklığı ile Hamming ağırlığı eşittir [9].

Tanım 1.2.7. $\mathbb{F}_q^n$ üzerinde x ve y iki vektör olmak üzere, vektörlerin birbirinden farklı koordinatlarının sayısına Hamming uzaklığı denir [10].

Tanım 1.2.8. C bir lineer kod olsun. σ dönüşümü kodsözleri $(c_0, c_1, \ldots, c_{n-1})$ şeklinde olan C kodu için $\sigma(C) = (c_{n-1}, c_0, \ldots, c_{n-2})$ şeklindeki herhangi bir devirli öteleme $\sigma(C) = C$ durumunu sağlıyorsa bu koda devirli kod denir [11].

Tanım 1.2.9. $\theta : \mathbb{F}_q^n \to \mathbb{F}_q[x]/(x^n - 1)$ dönüşümü

$\theta(c_0c_1\ldots c_{n-1}) = c_0 + c_1x + \ldots + c_{n-1}x^{n-1}$ şeklinde tanımlansın. Bu dönüşüm altında $C \subset \mathbb{F}_q^n$ lineer kodun her elemanı $\mathbb{F}_q[x]/(x^n-1), (n \neq 1)$ halkasındaki bir polinomla birebir eşleştirilir [9].

Örnek 1.2.1. $C = \{000, 011, 101, 110\}$ bir devirli kod olmak üzere $\theta(C) = \{0, 1+x, 1+x^2, x+x^2\} \subset \mathbb{F}_2[x]/(x^3-1)$ şeklinde kodsözler polinom olarak ifade edilir.

Teorem 1.2.2. C lineer kodu $\mathbb{F}_q$ vektör uzayının bir alt uzayı ve θ Tanım 1.2.9 daki dönüşüm olsun. C kodunun devirli kod olması için gerek ve yeter şart θ lineer dönüşümü altında C nin $\mathbb{F}_q[x]/(x^n-1)$ halkasının bir ideali olmasıdır [9].

Teorem 1.2.3. I, $\mathbb{F}_q[x]/(x^n-1)$ in bir ideali ve $g(x)$ de I da sıfırdan farklı en küçük dereceli monik bir polinom olsun. Bu durumda,

1. $g(x)$ polinomu I idealinin bir üretecidir ve bu üreteç tektir.
2. $g(x)$ polinomu x^n-1 polinomunu böler [9].

Tanım 1.2.10. C, $\mathbb{F}_q$ üzerinde tanımlı n uzunluğunda bir devirli koddur. C nin Tanım 1.2.9 daki θ dönüşümü altında sıfırdan farklı en küçük dereceli monik bir polinomu $g(x)$ olmak üzere, $g(x)$ polinomuna C kodunun üreteç polinomu denir ve $C = \langle g(x) \rangle$ şeklinde yazılır [9].

$\mathbb{F}_q[x]/(x^n-1)$ halkasının idealleri ile $\mathbb{F}_q^n$ uzayındaki devirli kodlar arasında birebir eşleme vardır. $g(x)$ polinomunun derecesi r dir ve $g(x)$ polinomu tarafından üretilen n uzunluklu bir C devirli kodu şu şekilde yazılır;

$C=\left\{a_j(x)g(x):a_j(x)\in\mathbb{F}_q[x]/\left(x^n-1\right),\deg\left(a_j(x)\right)<n-r\right\}$, $j=q^{n-r}$ [12].

Teorem 1.2.4. $x^n-1=\prod_{j=1}^{r}\left(p_j(x)\right)^{e_j}$, x^n-1 polinomunun $\mathbb{F}_q[x]$ de asal çarpanlara ayrılışı olmak üzere, $\mathbb{F}_q$ üzerinde n uzunluklu devirli kodların sayısı $\prod_{j=1}^{r}\left(e_j+1\right)$ dir. [9].

Örnek 1.2.2. x^6-1 polinomu asal çarpanlarına $x^6-1=\left(x+1\right)^2\left(x^2+x+1\right)^2$ şeklinde ayrılır. Teorem 1.2.4 den dolayı $\mathbb{F}_2$ üzerinde altı uzunluklu dokuz tane devirli kod vardır.

BÖLÜM 2. TEK KULLANIMLIK KARAKTER DİZİSİ İLE ŞİFRELEME

Kriptoloji yüzyıllardan beri bilim insanlarının çalışma alanı olmuştur. Geliştirilen ilk iletişim şekillerinden itibaren bilginin güvenli bir şekilde taşınması ve saklanması önemli hale gelmiştir. Günümüzde ilerleyen teknoloji ile birlikte bilgi güvenliğine olan ihtiyaç daha da artmaktadır. Bilginin taşınması sırasında, herhangi bir güvenlik sorunu oluştuğunda şifrenin çözülememesi için şifrenin kırılamaz olması önemlidir. Dolayısıyla kırılamaz şifre bulmak için yeni şifreleme modelleri çalışılmıştır. Kırılamaz şifre olarak varlığı ispatlanmış şifreleme modeli olan tek kullanımlık karakter dizisi (One Time Pad) bilginin güvenli bir şekilde taşınmasını garanti etmektedir.

1917 yılında Amerikan Telefon ve Telgraf şirketinde çalışan Gilbert Vernam adındaki bir mühendis, yeni bir şifreleme tekniği geliştirdi [13]. Bu şifreleme metodu Vernam şifresi olarak adlandırılmaktadır. Vernam şifresi ikilik sistem üzerinde kurulmuş bir şifreleme sistemidir. Sistemin güvenliği ve kırılamazlığı anahtar seçimi ile doğrudan ilişkilidir. Eğer en az şifrelenecek mesaj ile aynı boyutta rastgele bir anahtar seçilir ve bu anahtar bir defaya mahsus kullanılır ise o zaman şifreleme sistemine tek kullanımlık karakter dizisi veya tek kullanımlık sistem (One Time Pad) adı verilir. Bu çalışma boyunca sistem tek kullanımlık karakter dizisi olarak adlandırılacaktır. Sistem, yani tek kullanımlık karakter dizisi şu şekilde çalışır; n ikilik sistemde şifrelenecek metin, s ikilik sistemde şifreli metin ile aynı uzunlukta bir anahtar ve c ikilik sistemde şifrelenmiş metin olmak üzere,

$c = n + s$, *şifreleme algoritması*,
$n = c + s$, *şifre çözme algoritması*,

şeklinde ifade edilir [14]. Tek kullanımlık karakter dizisi yöntemi ile kriptografide matematik yaygın olarak kullanılmaya başlanmıştır. Bu bölümde öncelikle $\mathbb{F}_2$ halkası üzerinde devirli kodlar yardımıyla geliştirilen güvenli şifreleme modeli verilmiştir. Daha sonra $S = \mathbb{F}_2 + v\mathbb{F}_2$ halkasının cebirsel yapısı ile ilgili bilgiler verilmiştir. Son olarak S halkası üzerindeki devirli kodlar kullanılarak tek kullanımlık karakter dizisi yöntemiyle geliştirilen şifreleme modeli verilmiştir. Bu bölüm boyunca, halka yapıları üzerinde kurulan şifreleme modeli [12] numaralı kaynaktan referans olarak alınmıştır.

2.1. $\mathbb{F}_2$ Haklası Üzerinde Devirli Kodlar Yardımıyla Güvenli Şifreleme

Çalkavur ve Güzeltepe [12] devirli kodlar kullanarak $\mathbb{F}_2$ halkası üzerinde tek kullanımlık karakter dizisi yöntemiyle bir şifreleme modeli geliştirdi. Tek kullanımlık karakter dizisi ile geliştirdikleri modeli daha sonra $\mathbb{F}_2 + v\mathbb{F}_2$ halkasına uyarladılar.

Şifreleme modeli oluşturulurken öncelikle $\mathbb{F}_2$ halkası üzerinde l uzunluklu bir devirli kodsöz seçilir. Seçilen kodsöz n olarak adlandırılır ve derecesi r olan $g(x)$ üreteç polinomu seçilir. Devirli kodların özellliğinden dolayı kodsözün her devirli ötelemesi yeni bir kodsöz oluşturmaktadır. Oluşturulan her yeni kodsöz bilgiyi şifrelemede k olarak adlandırılan anahtar görevi görmektedir. Şifreli metni oluşturmak için $c = n + k$ işlemi uygulanır. Bu durumda şifreleme ve şifre çözme algoritması şu şekildedir;

Şifreleme Algoritması:

Şifrelenecek metin: $n_i = a_i(x)g(x)$, $0 \le i \le p^{l-r}$.

Anahtar: $k_i = x^t a_i(x)g(x)$, $k = k_1 k_2 ... k_n$ ve t devirli öteleme sayısını temsil etmektedir.

Şifreli metin: $c_i = n_i + k_i$. Burada n_i lerin birbirinden farklı olduğu durumlar düşünülmektedir.

Şifre Çözme Algoritması:

Şifreli metin: c_i.

Şifrelenen metin: $n_i = c_i + (p-1)k_i$.

Bu şifreleme modeli devirli kodların yapısına dayanmaktadır ve burada her bir kodsöz şifreleme modelinde anahtar olarak kullanılmaktadır. Kullanılan şifreleme modelinin özelliğinden dolayı anahtar şifrelenecek metin ile aynı uzunluktadır. Her şifreli metinde farklı anahtar kullanıldığı için anahtarın tahmini daha zordur.

Örnek 2.1.1. Altı uzunluklu devirli bir kod alınsın. Kodun $\mathbb{F}_2$ üzerinde parçalanışı $x^6-1=(x+1)^2(x^2+x+1)^2$ şeklindedir ve $\mathbb{F}_2$ üzerinde çalıştığımız için "−" yerine "+" yazılabilir. x^6-1 polinomunun tüm monik bölenleri üreteç polinomlardır ve bu üreteç polinomlar şu şekildedir;
$1,\ x+1,\ x^2+x+1,\ x^2+1,\ x^3+1,\ x^4+x^3+x+1,\ x^4+x^2+1,\ x^5+x^4+x^3+x+1,\ x^6+1$.

Kodu oluşturmak için yukarıdaki dokuz adet polinomdan herhangi biri seçilebilir, örnekte üreteç polinom olarak $g(x)=x^3+1$ seçilmiştir. $g(x)$ polinomu x^6-1 polinomunu bölen üçüncü dereceden bir polinomdur. Bir C kodunu oluşturmak için $a_i(x)\in \mathbb{F}_2[x]/(x^6-1)$ kümesinin elemanları $\{0,1,x,x^2,x+1,x^2+x,x^2+1,x^2+x+1\}$ şeklindedir.

Şifreleme: $n_i = a_i(x)g(x)$ şifrelenecek metin,

$k_i = x^t a_i(x)g(x)$ anahtar,

$c_i = n_i + k_i,\ 0 \le i \le 8$ şifrelenmiş metin olmak üzere $t=2$ olarak alınmıştır.

$$n_1 = a_1(x)\,g(x) = 1\left(x^3+1\right) = x^3+1 = 100100,$$
$$k_1 = x^2 n_1 = x^5 + x^2 = 001001,\ c_1 = n_1 + k_1 = 101101.$$

$$n_2 = a_2(x)\,g(x) = x\left(x^3+1\right) = x^4 + x = 010010,$$
$$k_2 = x^2 n_2 = x^3 + 1 = 100100, c_2 = n_2 + k_2 = 110110.$$

$$n_3 = a_3(x)\,g(x) = x^2\left(x^3+1\right) = x^5 + x^2 = 001001,$$
$$k_3 = x^2 n_3 = x^4 + x = 010010, c_3 = n_3 + k_3 = 011011.$$

$$n_4 = a_4(x)\,g(x) = (x+1)\left(x^3+1\right) = x^4 + x^3 + x + 1 = 110110,$$
$$k_4 = x^2 n_4 = x^5 + x^3 + x^2 + 1 = 101101, c_4 = n_4 + k_4 = 011011.$$

$$n_5 = a_5(x)\,g(x) = \left(x^2+x\right)\left(x^3+1\right) = x^5 + x^4 + x^2 + x = 011011,$$
$$k_5 = x^2 n_5 = x^4 + x^3 + x + 1 = 110110, c_5 = n_5 + k_5 = 101101.$$

$$n_6 = a_6(x)\,g(x) = \left(x^2+1\right)\left(x^3+1\right) = x^5 + x^3 + x^2 + 1 = 101101,$$
$$k_6 = x^2 n_6 = x^5 + x^4 + x^2 + x = 011011, c_6 = n_6 + k_6 = 110110.$$

$$n_7 = a_7(x)\,g(x) = \left(x^2+x+1\right)\left(x^3+1\right) = x^5 + x^4 + x^3 + x^2 + x + 1 = 111111,$$
$$k_7 = x^2 n_7 = x^5 + x^4 + x^3 + x^2 + x + 1 = 111111, c_7 = n_7 + k_7 = 000000.$$

$$n_8 = a_8(x)\,g(x) = 0\left(x^3+1\right) = 0 = 000000,$$
$$k_8 = x^2 n_8 = 0 = 000000,\quad c_8 = n_8 + k_8 = 000000.$$

Şifre Çözme: $n_i = c_i + (p-1)k_i$,

$$n_1 = c_1 + k_1 = x^3 + 1 = 100100,$$
$$n_2 = c_2 + k_2 = x^4 + x = 010010,$$
$$n_3 = c_3 + k_3 = x^5 + x^2 = 001001,$$
$$n_4 = c_4 + k_4 = x^4 + x^3 + x + 1 = 110110,$$
$$n_5 = c_5 + k_5 = x^5 + x^4 + x^2 + x = 011011,$$
$$n_6 = c_6 + k_6 = x^5 + x^3 + x^2 + 1 = 101101,$$
$$n_7 = c_7 + k_7 = x^5 + x^4 + x^3 + x^2 + x + 1 = 111111,$$
$$n_8 = c_8 + k_8 = 000000.$$

Örnekte her c_i için farklı anahtar kullanıldı. Her şifrelemede yeni bir anahtar kullanılarak anlamlı birçok şifreli mesaj elde edildi. Dolayısıyla anahtarı tahmin ederek şifreyi çözmek zorlaşır.

2.2. $\mathbb{F}_2 + v\mathbb{F}_2$ Haklası Üzerinde Devirli Kodlar Yardımıyla Güvenli Şifreleme

$S = \{0,1,v,1+v\}$, $v^2 = v$ değişmeli halkası $\mathbb{F}_2[v]/(v^2+v)$ şeklinde ifade edilebilen bir bölüm halkasıdır. Halkanın $\langle v \rangle$, $\langle 1+v \rangle$ olmak üzere iki adet maksimal ideali vardır. Dolayısıyla yarı yerel halka olarak adlandırılmaktadır. S halkası üzerinde tanımlı n uzunluğundaki bir C kodu S^n modülünün bir $S-$alt modülü olarak tanımlanır. Halkadaki elemanların Lee ağırlıkları şu şekildedir;

$$W_L(0) = 0,\ W_L(1) = 2,\ W_L(v) = W_L(1+v) = 1.$$

$a, b \in \mathbb{F}_2$ için $\gamma : S \to \mathbb{F}_2^2$ Gray dönüşümü şu şekildedir;

$$\gamma(a+bv) = (a, a+b).$$

$\varphi : S \to \mathbb{F}_2$ izdüşüm dönüşümü şu şekilde tanımlanır;

$$\varphi(a+bv) = a.$$

Halkanın elemanlarının Gray dönüşümü altındaki görüntüleri aşağıdaki gibidir,

$\gamma(0)=(00),\ \gamma(1)=(11),\ \gamma(v)=(01),\ \gamma(1+v)=(10).$

S halkası hakkında daha fazla bilgi için [15,16] kaynaklarına bakılabilir.

Önerme 2.2.1. $\gamma:\left(S^n,d_L\right)\to\left(\mathbb{F}_2^{2n},d_H\right)$ şeklinde tanımlanan Gray dönüşümü uzaklık koruyan bir dönüşümdür [17].

Teorem 2.2.1. C, S halkası üzerinde tanımlı n uzunluklu bir lineer kod ve $C_1=\left\{a\in\mathbb{F}_2^n \mid a+bv\in C,\ b\in\mathbb{F}_2{}^n\right\}$, $C_2=\left\{a+b\in\mathbb{F}_2^n \mid a+bv\in C\right\}$ şeklinde tanımlı iki lineer kod olmak üzere $\gamma(C)=C_1\otimes C_2$ şeklinde tanımlanır ve $|C|=|C_1|\cdot|C_2|$ dir. Bu Gray dönüşümü lineerdir [15].

Sonuç 2.2.1. C kodu $\gamma(C)=C_1\otimes C_2$ şeklinde tanımlanması durumunda C kodu $C=(1+v)C_1\oplus vC_2$ şeklinde tek türlü ifade edilir [15].

Teorem 2.2.2. $C=(1+v)C_1\oplus vC_2$ kodu S halkası üzerinde bir lineer kod olsun. C kodunun S halkası üzerinde devirli kod olması için gerek ve yeter şart C_1 ve C_2 lineer kodlarının devirli kod olmasıdır [15].

Teorem 2.2.3. S halkası üzerinde tanımlı n uzunluğunda bir C devirli kodu, $g(x)=(1+v)g_1(x)+vg_2(x)$ şeklinde tanımlı x^n-1 polinomunu bölen tek bir $g(x)$ polinomu tarafından üretilir. Eğer $g_1(x)=g_2(x)$ ise $g(x)=g_1(x)$ şeklindedir [15].

Teorem 2.2.4. C, S halkası üzerinde tanımlı n uzunluğunda devirli bir kod ise $g_1(x), g_2(x)$ sırasıyla C_1, C_2 devirli kodlarının üreteç polinomları olmak üzere $C = \langle (1+v)g_1(x), vg_2(x) \rangle$ ve $|C| = 2^{2n-\deg(g_1(x))-\deg(g_2(x))}$ şeklindedir [15].

Bölüm 2.1' de $\mathbb{F}_2$ halkasına uygulanan şifreleme modeli, $\mathbb{F}_2 + v\mathbb{F}_2$ halka yapısına uygulanarak yeni bir şifreleme modeli geliştirilmiştir.

$\mathbb{F}_2 + v\mathbb{F}_2$ halkasındaki devirli kodlar $C = (1+v)C_1 \oplus vC_2$ şeklinde tanımlanmaktadır. Burada ki C_1 ve C_2 kodları sırasıyla $g_1(x)$ ve $g_2(x)$ polinomları tarafından üretilmektedir. $g_1(x)$ ve $g_2(x)$ polinomları $x^n - 1$ polinomunun bir bölenidir. Şifreleme algoritmasını oluşturabilmek için $0 \le i \le |C_1|$, $0 \le j \le |C_2|$ şartlarına uygun $u_i \in C_1$, $k_i \in C_2$ kodsözleri seçilir.

Şifreleme Algoritması:

Şifrelenecek metin: $n_{i+|c_1|j} = u_i \times k_j \in \gamma(C),\ 0 \le i \lhd |C_1|,\ 0 \le j \lhd |C_2|$.

Anahtar: $k_j \in C_2,\ 0 \le j \lhd |C_2|$.

Şifreli metin: $c_{i+|C_1|j} = \gamma\left((1+v)u_i + vk_j\right)$.

Şifre Çözme Algoritması:

Şifreli metin : $c_{i+|C_1|j} = \gamma\left((1+v)u_i + vk_j\right)$.

Şifrelenen metin: $n_{i+|C_1|j} = \varphi\left[\gamma^{-1}\left(c_{i+|C_1|j}\right) + vk_j\right] \times k_j$.

Örnek 2.2.1. Beş uzunluklu bir devirli kodun $\mathbb{F}_2$ üzerinde çarpanlarına ayrılışı $x^5-1=(x+1)(x^4+x^3+x^2+x+1)$ şeklindedir. Üreteç polinom olarak $g_1(x)=x+1$, ve $g_2(x)=x^4+x^3+x^2+x+1$ seçilirse C_1 ve C_2 kodları sırasıyla g_1 ve g_2 polinomları tarafından üretilir. Elde edilen kodlar şu şekildedir;

$$C_1=\left\{\begin{matrix}00000,11000,01100,00110,00011,10001,10100,11110,\\11011,01001,01010,01111,11101,00101,10111,10010\end{matrix}\right\}$$
$$C_2=\{00000,11111\}$$

C_1 ve C_2 devirli kodlarından $i=0,1,2,\ldots,15$, $j=0,1$ olmak üzere kodsözler aşağıdaki gibi seçilebilir.

$u_0=00000$, $u_1=11000$, $u_2=01100$, $u_3=00110$, $u_4=00011$, $u_5=10001$,
$u_6=10100$, $u_7=11110$, $u_8=11011$, $u_9=01001$, $u_{10}=01010$, $u_{11}=01111$,
$u_{12}=11101$, $u_{13}=00101$, $u_{14}=10111$, $u_{15}=10010$, $k_0=00000$, $k_1=11111$.

Şifreleme:

$i=0, j=0$ durumunda $u_0=00000$ ve $k_0=00000$ elde edilir. Bu durumda şifrelenecek metin $n_0=u_0\times k_0=00000\times 00000=0000000000$ ve şifrelenmiş metin $c_0=\gamma\left[(1+v)u_0+vk_0\right]=\gamma(00000)=0000000000$ şeklinde elde edilir.

$i=2, j=1$ durumunda $u_2=01100$ ve $k_1=11111$ elde edilir. Bu durumda şifrelenecek metin $n_{18}=u_2\times k_1=01100\times 11111=0110011111$ ve şifrelenmiş metin $c_{18}=\gamma\left[(1+v)u_2+vk_1\right]=\gamma(v11vv)=0111110101$ şeklinde elde edilir.

$i=3, j=1$ durumunda $u_3=00110$ ve $k_1=11111$ elde edilir. Bu durumda şifrelenecek metin $n_{19}=u_3\times k_1=00110\times 11111=0011011111$ ve şifrelenmiş metin $c_{19}=\gamma\left[(1+v)u_3+vk_1\right]=\gamma(vv11v)=0101111101$ şeklinde elde edilir.

$i=8, j=1$ durumunda $u_8=11011$ ve $k_1=11111$ elde edilir. Bu durumda şifrelenecek metin $n_{24}=u_8\times k_1=11011\times 11111=1101111111$ ve şifrelenmiş metin $c_{24}=\gamma\left[(1+v)u_8+vk_1\right]=\gamma(11v11)=1111011111$ şeklinde elde edilir.

$i=13, j=1$ durumunda $u_{13}=00101$ ve $k_1=11111$ elde edilir. Bu durumda şifrelenecek metin $n_{29}=u_{13}\times k_1=00101\times 11111=0010111111$ ve şifrelenmiş metin $c_{29}=\gamma\left[(1+v)u_{13}+vk_1\right]=\gamma(vv1v1)=0101110111$ şeklinde elde edilir.

Şifre Çözme;

$c_0=0000000000, k_0=00000$ için $i=0, j=0$ olur ve şifre şu şekilde çözülür,

$$\begin{aligned} n_0 &= \varphi\left[\gamma^{-1}(c_0)+vk_0\right]\times k_0 \\ &= \varphi\left[\gamma^{-1}(0000000000)+v(00000)\right]\times(00000) \\ &= (00000)\times(00000) \\ &= (0000000000). \end{aligned}$$

$c_{18}=0111110101, k_1=11111$ için $i=2, j=1$ olur ve şifre şu şekilde çözülür,

$$\begin{aligned} n_{18} &= \varphi\left[\gamma^{-1}(c_{18})+vk_1\right]\times k_1 \\ &= \varphi\left[\gamma^{-1}(0111110101)+v(11111)\right]\times(11111) \\ &= (01100)\times(11111) \\ &= (0110011111). \end{aligned}$$

$c_{19}=0101111101, k_1=11111$ için $i=3, j=1$ olur ve şifre şu şekilde çözülür,

$$\begin{aligned} n_{19} &= \varphi\left[\gamma^{-1}(c_{19})+vk_1\right]\times k_1 \\ &= \varphi\left[\gamma^{-1}(0101111101)+v(11111)\right]\times(11111) \\ &= (00110)\times(11111) \\ &= (0011011111). \end{aligned}$$

$c_{24} = 1111011111,\ k_1 = 11111$ için $i = 8,\ j = 1$ olur ve şifre şu şekilde çözülür,

$$\begin{aligned} n_{24} &= \varphi\left[\gamma^{-1}\left(c_{24}\right) + vk_1\right] \times k_1 \\ &= \varphi\left[\gamma^{-1}(1111011111) + v\left(11111\right)\right] \times \left(11111\right) \\ &= \left(11011\right) \times \left(11111\right) \\ &= \left(1101111111\right). \end{aligned}$$

$c_{29} = 0101110111,\ k_1 = 11111$ için $i = 13,\ j = 1$ olur ve şifre şu şekilde çözülür,

$$\begin{aligned} n_{29} &= \varphi\left[\gamma^{-1}\left(c_{29}\right) + vk_1\right] \times k_1 \\ &= \varphi\left[\gamma^{-1}\left(0101110111\right) + v\left(11111\right)\right] \times \left(11111\right) \\ &= \left(00101\right) \times \left(11111\right) \\ &= \left(0010111111\right). \end{aligned}$$

Yapılan örnekte şifreleme modelinin anlaşılması için bazı şifreli metinler elde edildi. Diğer şifreli metinler aynı yöntemle elde edilebilmektedir. Bu şifreleme modelinde şifrelenecek metin ile aynı uzunlukta anahtar kullanılarak şifreleme yapıldı. Yetkisiz bir kişi şifreli mesajı çözmek istediğinde elde edeceği sonuçlar 10 bitlik olacaktır. Şifreleme modelini ve anahtarı bilmediği için ne kadar anlamlı mesajlar elde etse bile mesajı çözmesi imkansızdır. Bu durumda devirli kodlar yardımıyla kırılamaz şifreli metinler elde edilmiş olur. Zaten güvenli bir şifreleme modeli olan tek kullanımlık karakter dizisi devirli kodlarla birlikte farklı cebirsel halka yapıları üzerinde de güvenli bir şifreleme olanağı sunmaktadır.

BÖLÜM 3. $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ HALKASI ÜZERİNDE GÜVENLİ ŞİFRELEME

Bu bölümde öncelikle $R=\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ halkasının özellikleri verildi. Halka üzerindeki devirli kodlarla ilgili tanım ve teoremler verildikten sonra Bölüm 2 de verilen şifreleme modeli R halkasına uygulanmıştır. Daha sonra şifreleme modeli ile ilgili örnekler üzerinde şifreleme ve şifre çözme işlemleri yapılmıştır.

3.1. R Halkası Üzerinde Tanımlı Devirli Kodlar

$R,\ u^2=u,\ v^2=v,\ uv=vu$ halkası karakteristiği 2 olan 16 elemanlı sonlu bir halkadır. Halkanın 16 tane ideali vardır ve bunlardan 4 tanesi maksimal idealdir. Her ideali tek eleman tarafından üretildiği için esas ideal halkasıdır ve birden fazla maksimal ideale sahip olduğu için yarı yerel halkadır. Halkanın idealleri tam bir kapsama bağıntısı şeklinde yazılamadığı için zincir halkası değildir.
Halkaya ait maksimal idealler aşağıdaki gibidir [18];

$$
\begin{aligned}
I_{1+uv} &= \{0,1+uv,u+uv,v+uv,1+u,1+v,u+v,1+u+v+uv\},\\
I_{1+u+uv} &= \{0,v,uv,1+u,v+uv,1+u+v,1+u+uv,1+u+v+uv\},\\
I_{1+v+uv} &= \{0,u,uv,1+v,u+uv,1+u+v,1+v+uv,1+u+v+uv\},\\
I_{u+v+uv} &= \{0,u,v,uv,u+v+uv,v+uv,u+uv,u+v\}.
\end{aligned}
$$

Teorem 3.1.1. $f:R\to\mathbb{F}_2[u,v]/\langle u^2-u,\ v^2-v,\ uv-vu\rangle$

$x+yu+mv+nuv\to f(x+yu+mv+nuv)=\{x+yu+mv+nuv\}$ dönüşümü bir izomorfizmadır [18].

Tanım 3.1.1. R halkası üzerinde tanımlı n uzunluklu bir lineer kod, R^n modülünün bir R-alt modülü olarak tanımlanır [18].

R halkası ile Bölüm 2 de bahsedilen S halkası arasında bir izomorfizma aşağıdaki gibi tanımlanır;

$$R \cong S[u] / \langle u^2 = u,\ uv - vu \rangle = S + uS.$$

Tanımlanan izomorfizma sayesinde R halkasının elemanları S halkasının elemanları ile ifade edilebilmektedir. Önceki bölümde $\gamma : S \to \mathbb{F}_2^2,\ \gamma(a+bv) = (a, a+b)$ Gray dönüşümü verilmişti. Bu dönüşüm kullanılarak $a,b,c,d \in \mathbb{F}_2^n$ için $\phi : R \to \mathbb{F}_2^4$

$$\begin{aligned} \phi(a+bv+cu+duv) &= \phi(a+bv+u(c+dv)) \\ &= (\gamma(a+bv), \gamma(a+bv)+\gamma(c+dv)) \\ &= (a, a+b, a+c, a+b+c+d) \end{aligned}$$

şeklinde tanımlı ϕ fonksiyonu $R \to \mathbb{F}_2^4$ bir Gray dönüşümü olur [18].

Halkanın elemanlarının Gray dönüşümü altındaki görüntüsü şu şekildedir;

$$\begin{array}{llll} \phi(0)=(0000), & \phi(1+u)=(1010), & \phi(u+uv)=(0100), & \phi(1+v+uv)=(1101), \\ \phi(1)=(1111), & \phi(1+v)=(1100), & \phi(v+uv)=(0010), & \phi(1+u+uv)=(1011), \\ \phi(u)=(0101), & \phi(uv)=(0001), & \phi(1+uv)=(1110), & \phi(u+v+uv)=(0111), \\ \phi(v)=(0011), & \phi(u+v)=(0110), & \phi(1+u+v)=(1001), & \phi(1+u+v+uv)=(1000). \end{array}$$

Önceki bölümde $\varphi : S \to \mathbb{F}_2,\ \varphi(a+bv) = a$ izdüşüm fonksiyonu tanımlandı. Bu dönüşüm kullanılarak $\psi : R \to \mathbb{F}_2$

$$\begin{aligned}\psi\left(a+bv+cu+duv\right)&=\psi\left(a+bv+u\left(c+dv\right)\right)\\&=\left(\varphi\left(a+bv\right)\right)\\&=a\end{aligned}$$

şeklinde tanımlı ψ fonksiyonu $R\to\mathbb{F}_2$ bir izdüşüm fonksiyonu olur.

Tanım 3.1.2. w_H, $\mathbb{F}_2^4$ vektör uzayı üzerinde tanımlı Hamming ağırlığı olsun. $y=a+bu+cv+duv\in R$ elemanının Lee ağırlığı $w_L\left(y\right)$ ile gösterilir ve $w_L\left(y\right)=w_H\left(\phi\left(y\right)\right)$ olarak tanımlanır [18].

R halkasının bazı elemanlarının Lee ağırlıkları şu şekildedir;

$$\begin{aligned}&w_L\left(1\right)=w_H\left(\phi\left(1\right)\right)=w_H\left(1111\right)=4,\\&w_L\left(v+uv\right)=w_H\left(\phi\left(v+uv\right)\right)=w_H\left(0010\right)=1,\\&w_L\left(u+v+uv\right)=w_H\left(\phi\left(u+v+uv\right)\right)=w_H\left(0111\right)=3,\\&w_L\left(1+u+v\right)=w_H\left(\phi\left(1+u+v\right)\right)=w_H\left(1001\right)=2.\end{aligned}$$

Teorem 3.1.2. C, R üzerinde tanımlı n uzunluklu bir lineer kod olsun. C kodunun devirli olması için gerek ve yeter şart $R\left[x\right]\Big/\left\langle x^n-1\right\rangle$ bölüm halkasının bir ideali olmasıdır [18].

Teorem 3.1.3. C, R üzerinde tanımlı n uzunluklu bir lineer kod olmak üzere $\mathbb{F}_2$ üzerinde n uzunluklu C_1,C_2,C_3 ve C_4 kodları aşağıdaki gibi tanımlanır:

$$\begin{aligned}C_1&=\left\{a\in\mathbb{F}_2^{\,n}:\exists b,c,d\in\mathbb{F}_2^{\,n},a+bu+cv+duv\in C\right\},\\C_2&=\left\{a+b\in\mathbb{F}_2^{\,n}:\exists c,d\in\mathbb{F}_2^{\,n},a+bu+cv+duv\in C\right\},\\C_3&=\left\{a+c\in\mathbb{F}_2^{\,n}:\exists b,d\in\mathbb{F}_2^{\,n},a+bu+cv+duv\in C\right\},\\C_4&=\left\{a+b+c+d\in\mathbb{F}_2^{\,n}:a+bu+cv+duv\in C\right\}.\end{aligned}$$

Bu durumda $\phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ ve kodun eleman sayısı $|C| = |C_1||C_2||C_3||C_4|$ olur [18].

Sonuç 3.1.1. $\phi(C) = C_1 \otimes C_2 \otimes C_3 \otimes C_4$ ise bir C kodu

$$C = (1+u+v+uv)C_1 \oplus (u+uv)C_2 \oplus (v+uv)C_3 \oplus (uv)C_4,$$

şeklinde ifade edilir [18].

Teorem 3.1.4. R halkası üzerinde tanımlı $C = (1+u+v+uv)C_1 \oplus (u+uv)C_2 \oplus (v+uv)C_3 \oplus (uv)C_4$ lineer kodun devirli kod olması için gerek ve yeter şart C_1, C_2, C_3 ve C_4 kodlarının $\mathbb{F}_2$ üzerinde tanımlı devirli kodlar olmasıdır [18].

Teorem 3.1.5. $C = (1+u+v+uv)C_1 \oplus (u+uv)C_2 \oplus (v+uv)C_3 \oplus (uv)C_4$ kodu R halkası üzerinde tanımlı n uzunluklu bir devirli kod olmak üzere g_1, g_2, g_3 ve g_4 sırası ile C_1, C_2, C_3 ve C_4 kodlarının üreteç polinomları olsun. C bir devirli kod olmak üzere $\langle (1+u+v+uv)g_1, (u+uv)g_2, (v+uv)g_3, (uv)g_4 \rangle$ tarafından üretilir ve kodun eleman sayısı $|C| = 2^{4n-(der(g_1)+der(g_2)+der(g_3)+der(g_4))}$ dir [18].

Teorem 3.1.6. $C = (1+u+v+uv)C_1 \oplus (u+uv)C_2 \oplus (v+uv)C_3 \oplus (uv)C_4$ kodu R halkası üzerinde tanımlı n uzunluğunda devirli bir kod olmak üzere $C = \langle g(x) \rangle$ olacak şekilde tek bir $g(x) = (1+u+v+uv)g_1 + (u+uv)g_2 + (v+uv)g_3 + (uv)g_4$ vardır ve bu $g(x)$ polinomu $x^n - 1$ polinomunu böler [18].

Bölüm 2 de tanıtılan şifreleme modelini R halka yapısına uygulamak için bilinmesi gereken halka özellikleri bu bölümde verildi. R halkası ile ilgili daha fazla bilgi için [18] kaynağına bakılabilir. Çalışmanın bu kısmından sonra güvenli şifreleme modelini

R halka yapısına uygulamak için gereken şifreleme algoritması verilecektir ve örnekler üzerinde şifreleme modeli uygulanacaktır.

3.2. R Halkası Üzerinde Devirli Kodlar Yardımıyla Güvenli Şifreleme

$C=(1+u+v+uv)C_1 \oplus (u+uv)C_2 \oplus (v+uv)C_3 \oplus (uv)C_4$ kodu R halkası üzerinde tanımlı n uzunluğunda bir devirli kod olsun. Bu durumda $C=\langle g(x)\rangle$ olacak şekilde $\exists\, g(x)\in R[x]$ vardır. Teorem 3.1.6 da verilen bilgiden yararlanarak $g(x)$ polinomu $g(x)=(1+u+v+uv)g_1+(u+uv)g_2+(v+uv)g_3+(uv)g_4$ olacak şekilde tek türlü ifade edilir ve $g(x)$ polinomu x^n-1 polinomunu böler. Bu durumda C_1, C_2, C_3 ve C_4 kodları sırasıyla g_1, g_2, g_3 ve g_4 polinomları tarafından üretilir ve bu polinomlar x^n-1 polinomunu böler.

Bölüm 2 de verilen şifreleme modelini R halkasında uygulamak için u_i, s_j, m_k ve n_l kodsözleri sırasıyla C_1, C_2, C_3 ve C_4 kodlarından seçilirse $0\le i<|C_1|, 0\le j<|C_2|$, $0\le k<|C_3|$ ve $0\le l<|C_4|$ olur. Bu durumda şifreleme şeması aşağıdaki gibi olur:

Şifrelenecek metin:

$p_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=u_i\times s_j\times m_k\times n_l\in\phi(C)$, $0\le i<|C_1|$, $0\le j<|C_2|$, $0\le k<|C_3|$ ve $0\le l<|C_4|$.

Anahtar: $n_l\in C_4$, $0\le l<|C_4|$.

Şifreli metin:

$C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=\phi\left((1+u+v+uv)u_i+(u+uv)s_j+(v+uv)m_k+(uv)n_l\right)$.

Şifre Çözme Algoritması:

Şifreli metin:

$$C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l} = \phi\left(\left(1+u+v+uv\right)u_i + \left(u+uv\right)s_j + \left(v+uv\right)m_k + \left(uv\right)n_l\right).$$

Şifrelenen metin:

$$p_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l} = \psi\left[\phi^{-1}\left(C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}\right) + \left(uv\right)n_l\right] \times s_j \times m_k \times n_l.$$

Verilen şifreleme şemasının daha iyi anlaşılması için örnekler üzerinde incelendi. Örneklerde sadece bazı şifreli metinler elde edilmiştir ve şifreli metinlere şifre çözme işlemleri yapılmıştır. Diğer şifreli metinler aynı şekilde elde edilir.

Örnek 3.2.1. Üç uzunluklu kodun $\mathbb{F}_2$ üzerinde parçalanışı $x^3-1=(x+1)(x^2+x+1)$ şeklindedir. Bu örnek için seçilen $f_1(x)=f_2(x)=x+1$ ve $f_3(x)=f_4(x)=x^2+x+1$ üreteç polinomları sırasıyla $C_1=C_2=\{000,110,011,101\}$ ve $C_3=C_4=\{000,111\}$ devirli kodlarını üretir. Şifreleme modelinin oluşturulabilmesi için i, j, k ve l değerleri, $i=j=0,1,2,3$ ve $k=l=0,1$ olmak üzere $u_0=s_0=000$, $u_1=s_1=110$, $u_2=s_2=011$, $u_3=s_3=101$, $m_0=n_0=000$ ve $m_1=n_1=111$ kodsözleri seçilirse şifreleme algoritması aşağıdaki gibi olur:

Şifreleme:

$i=0,\ j=0,\ k=0,\ l=0$ durumuna karşılık $u_0=000,\ s_0=000,\ m_0=000,\ n_0=000$ olur. $p_0=u_0\times s_0\times m_0\times n_0=000\times 000\times 000\times 000=000000000000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$\begin{aligned} c_0 &= \phi\left(\left(1+u+v+uv\right)u_0 + \left(u+uv\right)s_0 + \left(v+uv\right)m_0 + \left(uv\right)n_0\right) \\ &= \phi\left(000\right) = 000000000000. \end{aligned}$$

$i=1,\ j=1,\ k=0,\ l=0$ durumuna karşılık $u_1=110,\ s_1=110,\ m_0=000,\ n_0=000$ olur. $p_5=u_1\times s_1\times m_0\times n_0=110\times 110\times 000\times 000=110110000000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_5 = \phi\left((1+u+v+uv)u_1 + (u+uv)s_1 + (v+uv)m_0 + (uv)n_0\right)$$
$$= 110011000000.$$

$i=0, j=1, k=1, l=1$ durumuna karşılık $u_0 = 000,\ s_1 = 110,\ m_1 = 111,\ n_1 = 111$ olur. $p_{52} = u_0 \times s_1 \times m_1 \times n_1 = 000 \times 110 \times 111 \times 111 = 000110111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{52} = \phi\left((1+u+v+uv)u_0 + (u+uv)s_1 + (v+uv)m_1 + (uv)n_1\right)$$
$$= 011101110011.$$

$i=0, j=3, k=0, l=1$ durumuna karşılık $u_0 = 000,\ s_3 = 101,\ m_0 = 000,\ n_1 = 111$ olur. $p_{44} = u_0 \times s_3 \times m_0 \times n_1 = 000 \times 101 \times 000 \times 111 = 000101000111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{44} = \phi\left((1+u+v+uv)u_0 + (u+uv)s_3 + (v+uv)m_0 + (uv)n_1\right)$$
$$= 010100010101.$$

$i=0, j=3, k=1, l=1$ durumuna karşılık $u_0 = 000,\ s_3 = 101,\ m_1 = 111,\ n_1 = 111$ olur. $p_{60} = u_0 \times s_3 \times m_1 \times n_1 = 000 \times 101 \times 111 \times 111 = 000101111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{60} = \phi\left((1+u+v+uv)u_0 + (u+uv)s_3 + (v+uv)m_1 + (uv)n_1\right)$$
$$= 011100110111.$$

$i=1, j=2, k=1, l=1$ durumuna karşılık $u_1 = 110,\ s_2 = 011,\ m_1 = 111,\ n_1 = 111$ olur. $p_{57} = u_1 \times s_2 \times m_1 \times n_1 = 110 \times 011 \times 111 \times 111 = 110011111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{57} = \phi\left((1+u+v+uv)u_1 + (u+uv)s_2 + (v+uv)m_1 + (uv)n_1\right)$$
$$= 101111110111.$$

Şifre çözme:

$c_0 = 000000000000,\ n_0 = 000$ için $i = j = k = l = 0$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_0 &= \psi\left[\phi^{-1}(000000000000) + (uv)n_0\right] \times s_0 \times m_0 \times n_0 \\ &= \psi\left[(000) + (000)\right] \times (000) \times (000) \times (000) \\ &= 000000000000. \end{aligned}$$

$c_5 = 110011000000,\ n_0 = 000$ için $i = j = 1,\ k = l = 0$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_5 &= \psi\left[\phi^{-1}(110011000000) + (uv)n_0\right] \times s_1 \times m_0 \times n_0 \\ &= (110) \times (110) \times (000) \times (000) \\ &= 110110000000. \end{aligned}$$

$c_{44} = 010100010101,\ n_1 = 111$ için $i = k = 0,\ j = 3,\ l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_{44} &= \psi\left[\phi^{-1}(010100010101) + (uv)n_1\right] \times s_3 \times m_0 \times n_1 \\ &= (000) \times (101) \times (000) \times (111) \\ &= 000101000111. \end{aligned}$$

$c_{52} = 011101110011,\ n_1 = 111$ için $i = 0,\ k = j = l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_{52} &= \psi\left[\phi^{-1}(011101110011) + (uv)n_1\right] \times s_1 \times m_1 \times n_1 \\ &= (000) \times (110) \times (111) \times (111) \\ &= 000110111111. \end{aligned}$$

$c_{57} = 101111110111,\ n_1 = 111$ için $i = k = l = 1,\ j = 2$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_{57} &= \psi\left[\phi^{-1}(101111110111) + (uv)n_1\right] \times s_2 \times m_1 \times n_1 \\ &= (110) \times (011) \times (111) \times (111) \\ &= 110011111111. \end{aligned}$$

$c_{60} = 011100110111,\ n_1 = 111$ için $i = 0,\ j = 3,\ k = l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$\begin{aligned} p_{60} &= \psi\left[\phi^{-1}(011100110111) + (uv)n_1\right] \times s_3 \times m_1 \times n_1 \\ &= (000) \times (101) \times (111) \times (111) \\ &= 000101111111. \end{aligned}$$

Bu örnekte C_1 ve C_2 kodu $f_1 = f_2$ polinomu ile C_3 ve C_4 kodu da $f_3 = f_4$ polinomu ile üretilmektedir. Bu seçimler değiştirilerek daha farklı şifreleme kombinasyonları da yapılabilir. Örnek olarak, sadece C_1 kodu f_1 polinomu ile üretilsin, C_2, C_3 ve C_4 kodları da f_2 polinomu ile üretilsin. O zaman $i = 0,1,2,3$ ve $j = k = l = 0,1$ olmak üzere $u_0 = 000,\ u_1 = 110,\ u_2 = 011,\ u_3 = 101,\ s_0 = m_0 = n_0 = 000$ ve $s_1 = m_1 = n_1 = 111$ kodsözleri seçilirse şifreleme algoritması aşağıdaki gibi olur:

Şifreleme:

$i = 3, j = 0, k = l = 1$ durumuna karşılık $u_3 = 101,\ s_0 = 000,\ m_1 = 111, n_1 = 111$ olur. $p_{27} = u_3 \times s_0 \times m_1 \times n_1 = 101 \times 000 \times 111 \times 111 = 101000111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$\begin{aligned} c_{27} &= \phi\left((1+u+v+uv)u_3 + (u+uv)s_0 + (v+uv)m_1 + (uv)n_1\right) \\ &= 101100111011. \end{aligned}$$

$i = 2, j = 1, k = 0, l = 1$ durumuna karşılık $u_2 = 011,\ s_1 = 111,\ m_0 = 000$ ve $n_1 = 111$ olur. $p_{22} = u_2 \times s_1 \times m_0 \times n_1 = 011 \times 111 \times 000 \times 111 = 011111000111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$\begin{aligned} c_{22} &= \phi\left((1+u+v+uv)u_2 + (u+uv)s_1 + (v+uv)m_0 + (uv)n_1\right) \\ &= 010111011101. \end{aligned}$$

$i=2, j=0, k=1, l=1$ durumuna karşılık $u_2=011$, $s_0=000$, $m_1=111$ ve $n_1=111$ olur.

$p_{26}=u_2\times s_0\times m_1\times n_1=011\times 000\times 111\times 111=011000111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{26}=\phi\left(\left(1+u+v+uv\right)u_2+\left(u+uv\right)s_0+\left(v+uv\right)m_1+\left(uv\right)n_1\right)$$
$$=001110111011.$$

$i=3, j=1, k=1, l=0$ durumuna karşılık $u_3=101$, $s_1=111$, $m_1=111$ ve $n_0=000$ olur.

$p_{15}=u_3\times s_1\times m_1\times n_0=101\times 111\times 111\times 000=101111111000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{15}=\phi\left(\left(1+u+v+uv\right)u_3+\left(u+uv\right)s_1+\left(v+uv\right)m_1+\left(uv\right)n_0\right)$$
$$=111001101110.$$

$i=1, j=1, k=1, l=1$ durumuna karşılık $u_1=110$, $s_1=111$, $m_1=111$ ve $n_1=111$ olur.

$p_{29}=u_1\times s_1\times m_1\times n_1=110\times 111\times 111\times 111=110111111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler uygulanır:

$$c_{29}=\phi\left(\left(1+u+v+uv\right)u_1+\left(u+uv\right)s_1+\left(v+uv\right)m_1+\left(uv\right)n_1\right)$$
$$=111111110111.$$

Şifre çözme:

$c_{15}=111001101110$, $n_0=000$ için $i=3, j=k=1, l=0$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{15}=\psi\left[\phi^{-1}\left(111001101110\right)+\left(uv\right)n_0\right]\times s_1\times m_1\times n_0$$
$$=\left(101\right)\times\left(111\right)\times\left(111\right)\times\left(000\right)$$
$$=101111111000.$$

$c_{22}=010111011101$, $n_1=111$ için $i=2, j=1, k=0, l=1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{22} = \psi\left[\phi^{-1}(010111011101) + (uv)n_1\right] \times s_1 \times m_0 \times n_1$$
$$= (011) \times (111) \times (000) \times (111)$$
$$= 011111000111.$$

$c_{26} = 001110111011$, $n_1 = 111$ için $i = 2, j = 0, k = l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{26} = \psi\left[\phi^{-1}(001110111011) + (uv)n_1\right] \times s_0 \times m_1 \times n_1$$
$$= (011) \times (000) \times (111) \times (111)$$
$$= 011000111111.$$

$c_{27} = 101100111011$, $n_1 = 111$ için $i = 3, j = 0, k = l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{27} = \psi\left[\phi^{-1}(101100111011) + (uv)n_1\right] \times s_0 \times m_1 \times n_1$$
$$= (101) \times (000) \times (111) \times (111)$$
$$= 101000111111.$$

$c_{29} = 111111110111$, $n_1 = 111$ için $i = 1, j = 1, k = l = 1$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{29} = \psi\left[\phi^{-1}(111111110111) + (uv)n_1\right] \times s_1 \times m_1 \times n_1$$
$$= (110) \times (111) \times (111) \times (111)$$
$$= 110111111111.$$

Yapılan uygulamada üreteç polinomlar değiştirilerek farklı şifreli metinler elde edildi. Bölüm 2 de yapılan örnek R halkası üzerinde de uygulanabilir. Bu durumda daha uzun kodsözler kullanılacağı için şifreli metinler daha uzun olacaktır. Kullanılan anahtar bir önceki örneğe göre daha uzun seçilecektir. Şifreleme sisteminin güvenliği anahtar ile doğru orantılı olduğu için daha uzun verilerle çalışmak sistemi daha güvenli hale getirmektedir.

Örnek 3.2.2. Beş uzunluklu bir kodun $\mathbb{F}_2$ üzerinde çarpanlarına ayrılışı $x^5-1=(x+1)(x^4+x^3+x^2+x+1)$ şeklindedir. C_1, C_2, C_3 ve C_4 lineer kodları sırası ile $g_1(x)=g_2(x)=x+1$ ve $g_3(x)=g_4(x)=x^4+x^3+x^2+x+1$ üreteç polinomları tarafından üretilsin.

$$C_1=C_2=\left\{\begin{matrix}00000,11000,01100,00110,00011,10001,10100,11110,\\11011,01001,01010,01111,11101,00101,10111,10010\end{matrix}\right\}$$
$$C_3=C_4=\{00000,11111\}.$$

C_1,C_2,C_3 ve C_4 devirli kodlarından $i=j=0,1,2,\ldots,15$, $k=l=0,1$ olmak üzere kodsözler aşağıdaki gibi seçilebilir:

$u_0=s_0=00000,\ u_1=s_1=11000,\ u_2=s_2=01100,\ u_3=s_3=00110,\ u_4=s_4=00011,$
$u_5=s_5=10001,\ u_6=s_6=10100,\ u_7=s_7=11110,\ u_8=s_8=11011,\ u_9=s_9=01001,$
$u_{10}=s_{10}=01010,\ u_{11}=s_{11}=01111,\ u_{12}=s_{12}=11101,\ u_{13}=s_{13}=00101,$
$u_{14}=s_{14}=10111,\ u_{15}=s_{15}=10010,\ m_0=n_0=00000,\ m_1=n_1=11111.$

Şifreleme:

$i=5, j=1, k=1, l=1$ durumuna karşılık $u_5=10001$, $s_1=11000$, $m_1=11111$ ve $n_1=11111$ olur.

$p_{789}=u_5\times s_1\times m_1\times n_1=10001\times11000\times11111\times11111=1000111000111111111$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler yapılır:

$$c_{789}=\phi\left((1+u+v+uv)u_5+(u+uv)s_1+(v+uv)m_1+(uv)n_1\right)$$
$$=11110111001100111011.$$

$i=0, j=3, k=0, l=0$ durumuna karşılık $u_0=00000$, $s_3=00110$, $m_0=00000$ ve $n_0=00000$ olur.

$p_{48}=u_0\times s_3\times m_0\times n_0=00000\times00110\times00000\times00000=000000011000000000000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler yapılır:

$$c_{48} = \phi\left(\left(1+u+v+uv\right)u_0 + \left(u+uv\right)s_3 + \left(v+uv\right)m_0 + \left(uv\right)n_0\right)$$
$$= 00000000010001000000.$$

$i=1, j=1, k=0, l=0$ durumuna karşılık $u_1 = 11000,\ s_1 = 11000,\ m_0 = 00000$ ve $n_0 = 00000$ olur.

$p_{17} = u_1 \times s_1 \times m_0 \times n_0 = 11000 \times 11000 \times 00000 \times 00000 = 1100011000000000000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler yapılır:

$$c_{17} = \phi\left(\left(1+u+v+uv\right)u_1 + \left(u+uv\right)s_1 + \left(v+uv\right)m_0 + \left(uv\right)n_0\right)$$
$$= 1100110000000000000.$$

$i=1, j=1, k=1, l=0$ durumuna karşılık $u_1 = 11000,\ s_1 = 11000,\ m_1 = 11111$ ve $n_0 = 00000$ olur.

$p_{273} = u_1 \times s_1 \times m_1 \times n_0 = 11000 \times 11000 \times 11111 \times 00000 = 1100011000111110000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler yapılır:

$$c_{273} = \phi\left(\left(1+u+v+uv\right)u_1 + \left(u+uv\right)s_1 + \left(v+uv\right)m_1 + \left(uv\right)n_0\right)$$
$$= 11101110001000100010.$$

$i=12, j=k=l=0$ durumuna karşılık $u_{12} = 11101,\ s_0 = 00000,\ m_0 = 00000$ ve $n_0 = 00000$ olur.

$p_{12} = u_{12} \times s_0 \times m_0 \times n_0 = 11101 \times 00000 \times 00000 \times 00000 = 1110100000000000000$ ile şifrelenecek metin elde edilir. Şifreli metni elde etmek için aşağıdaki işlemler yapılır:

$$c_{12} = \phi\left(\left(1+u+v+uv\right)u_{12} + \left(u+uv\right)s_0 + \left(v+uv\right)m_0 + \left(uv\right)n_0\right)$$
$$= 10001000100000001000.$$

Şifre çözme:

$c_{12} = 10001000100000001000,\ n_0 = 00000$ için $i=12, j=k=l=0$ değerlerini alır. Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{12} = \psi\left[\phi^{-1}(10001000100000001000) + (uv)n_0\right] \times s_0 \times m_0 \times n_0$$
$$= (11101) \times (00000) \times (00000) \times (00000)$$
$$= 11101000000000000000.$$

$c_{17} = 11001100000000000000$, $n_0 = 00000$ için $i = j = 1, k = l = 0$ değerlerini alır.

Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{17} = \psi\left[\phi^{-1}(11001100000000000000) + (uv)n_0\right] \times s_1 \times m_0 \times n_0$$
$$= (11000) \times (11000) \times (00000) \times (00000)$$
$$= 11000110000000000000.$$

$c_{48} = 00000000010001000000$, $n_0 = 00000$ için $j = 3, i = k = l = 0$ değerlerini alır.

Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{48} = \psi\left[\phi^{-1}(00000000010001000000) + (uv)n_0\right] \times s_3 \times m_0 \times n_0$$
$$= (00000) \times (00110) \times (00000) \times (00000)$$
$$= 00000001100000000000.$$

$c_{789} = 11110111001100111011$, $n_1 = 11111$ için $i = 5,\ j = k = l = 1,$ değerlerini alır.

Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{789} = \psi\left[\phi^{-1}(11110111001100111011) + (uv)n_1\right] \times s_1 \times m_1 \times n_1$$
$$= (100011) \times (11000) \times (11111) \times (11111)$$
$$= 10001110001111111111.$$

$c_{273} = 11101110001000100010$, $n_1 = 00000$ için $l = 0, i = j = k = 1,$ değerlerini alır.

Bu durumda şifre çözme algoritması aşağıdaki gibi olur:

$$p_{273} = \psi\left[\phi^{-1}(11101110001000100010) + (uv)n_0\right] \times s_1 \times m_1 \times n_0$$
$$= (11000) \times (11000) \times (11111) \times (00000)$$
$$= 11000110001111100000.$$

Yapılan örneklerde şifreleme modelinin anlaşılması için bazı şifreli metinler elde edildi. Tüm şifreli metinler aynı yöntemle elde edilebilir. Örneklerde veri ile aynı

uzunlukta bir anahtar kullanılarak şifreleme yapılmıştır. Tek kullanımlık karakter dizisi yöntemi ile yapılan şifrelemede, kullanılan anahtarın uzunluğu şifrenin güvenliği ile doğru orantılıdır ve bu yüzden anahtarın uzunluğu arttıkça şifreleme şeması daha güvenli hale gelmektedir. Şifreyi ele geçiren bir kişi birçok anlamlı mesaj elde edeceği için hangisinin mesaj olduğunu tahmin edemez. Bu durum şifrenin kırılamazlığını garanti etmektedir.

BÖLÜM 4. TARTIŞMA VE SONUÇ

Bu çalışmada tek kullanımlık karakter dizisi yöntemi kullanılarak devirli kodlar yardımıyla güvenli şifreleme modeli çalışılmıştır. İlk olarak $\mathbb{F}_2$ halkası üzerinde devirli kodlar kullanılarak oluşturulan şifreleme modeli incelenmiştir. $\mathbb{F}_2+v\mathbb{F}_2$ halka yapısı verilerek halka üzerinde oluşturulan şifreleme modeli incelenmiştir. Daha sonra $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ halka yapısı incelenmiş ve yeni şifreleme şemasının oluşturulabilmesi için halka üzerinde Gray dönüşümü ve izdüşüm fonksiyonu tanımlanmıştır. Son olarak incelenen şifreleme modeli $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2+uv\mathbb{F}_2$ halkasına uyarlanarak yeni şifreleme şeması oluşturulmuştur.

Bu alanda [12], [19] daki çalışmalar yapılmıştır. Bu modelin $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q+uv\mathbb{F}_q$ gibi farklı halkalara uyarlanması açık problemlerdir.

KAYNAKLAR

[1] Çallıalp, F., Örneklerle Soyut Cebir, Birsen Yayınevi, İstanbul, 2018.

[2] Hungerford, T. W., Algebra, Springer-Verlag, New York, 1974.

[3] Jitman, S., Ling, S., Udomkavanich, P., Skew Constacyclic Codes Over Finite Chain Rings, Advances In Mathematics of Communications, Vol. 6, No:1, 39-63, 2012.

[4] Charkani, M. E., Kabore, J., Primitive Idempotents and Constacyclic Codes Over Finite Chain Rings, Gulf Journal of Mathematics, Vol. 8, No:2, 55-67, 2020.

[5] Bayraktar, M., Soyut Cebir ve Sayılar Teorisi, Atatürk Üniversitesi Basımevi, Erzurum, 1988.

[6] Arıkan, A., Halıcıoğlu, S., Cebire Giriş, Palme Yayıncılık, Ankara, 2015.

[7] Roman, S., Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag, New York, 1992.

[8] http://www.fen.bilkent.edu.tr/~franz/lect/codes.pdf, Erişim Tarihi: 11.01.2022.

[9] Ling, S., Xing, C., Coding Theory, Cambridge University Press, 2004.

[10] Huffman, W. C., Pless, V., Fundamentals of Error Correcting Codes, Cambridge University Press, New York, 2003.

[11] Hill, R., A First Course in Coding Theory, The Oxford University, Oxford, UK, 1986.

[12] Çalkavur, S., Güzeltepe, M., Secure Encryption from Cyclic Codes, Sigma Journal of Engineering and Natural Sciences, Vol. 40, No. 2, 380-389, 2022.

[13] Topaloglu, N., Calp, M. H., Turk, B., Bilgi Güvenliği Kapsamında Yeni Bir Veri Şifreleme Algoritması Tasarımı ve Gerçekleştirilmesi, Bilişim Teknolojileri Dergisi, Vol: 9, No. 3, 291-301, 2016.

[14] Kuklová, Z., Coding Theory, Cryptography and Cryptographic Protocols-exercises with Solutions (given in 2006), Bachelor Thesis, Masarykova University, Brno, Spring 2007.

[15] Zhu, S., Wang, Yu, Shi, M., Some Results on Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$, IEEE Transactions on Information Theory, Vol: 56, No. 4, April 2010.

[16] Dougherty, S. T., Shiromoto, K., Maximum Distance Codes Over Rings of Order 4, IEEE Transactions on Information Theory, Vol: 47, No.1, 400-404, 2001.

[17] Qian, J., Quantum Codes from Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$, Journal of Information Computational Science, 1715-1722, 2013.

[18] Dertli, A., Halkalar Üzerinde Tanımlı Kodlar Hakkında Bazı Araştırmalar, Ondokuz Mayıs Üniversitesi, Fen Bilimleri Enstitüsü, Matematik Bölümü, Doktora Tezi, 2016.

[19] Güzeltepe, M., Çalkavur, S., Skew-Cyclic Codes Based Public-Key Cryptosystem Approach, Security and Privacy, Vol: 255, No. 2, 1-9, 2022.

ÖZGEÇMİŞ

Adı Soyadı **:** Neriman Şolt

ÖĞRENİM DURUMU

Derece	Eğitim Birimi	Mezuniyet Yılı
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Matematik	Devam Ediyor
Yüksek Lisans	Sakarya Üniversitesi / Fen Bilimleri Enstitüsü / Bilişim Sistemleri (Tezsiz)	2021
Lisans	Dokuz Eylül Üniversitesi / Fen Edebiyat Fakültesi / Matematik	2018
Lise	Karasu Şehit Üsteğmen İbrahim Abanoz Anadolu Lisesi	2012

YABANCI DİL

İngilizce

ESERLER (makale, bildiri, proje vb.)

1. Şolt, N., Çalkavur, S., Güzeltepe, M., Secure Encryption over The Ring F2+uF2+vF2+uvF2. ICAENS, Konya, 2022.

2. Güzeltepe, M., Şolt, N., Perfect Epsilon-Error Correcting Codes over Gaussian İntegers. ICEANS, Konya, 2022.