T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DESTEK AYIRMA ALGORİTMASI VE McELIECE ŞİFRELEME SİSTEMİNDE ZAYIF ANAHTARLAR

YÜKSEK LİSANS TEZİ

Ekrem EMRE

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

Haziran 2014

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

DESTEK AYIRMA ALGORİTMASI ve McELIECE ŞİFRELEME SİSTEMİNDE ZAYIF ANAHTARLAR

YÜKSEK LİSANS TEZİ

Ekrem EMRE

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

Bu tez 09/06/2014 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. Mehmet ÖZEN Jüri Başkanı	Doç. Dr. Metin YAMAN Üye	Doç. Dr. Sıtkı DUMAN Üye

TEŞEKKÜR

Eğitim hayatım süresince beni özveri ile yetiştiren tüm öğretmen ve öğretim üyesi hocalarıma teşekkürü bir borç bilirim. Bilhassa, tez çalışmamın her aşamasında bilgi ve tecrübeleriyle beni yönlendiren Sayın Prof. Dr. Mehmet ÖZEN' e en içten teşekkürlerimi sunarım.

Ayrıca eğitim hayatım boyunca maddi ve manevi desteklerini üzerimden esirgemeyen aileme de teşekkür ediyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$\mathbb{F}_p$	: p elemanlı sonlu cisim
wt	: Hamming ağırlığı
$C^{\perp}$	: C lineer kodunun duali
W_C	: C kodunun Hamming ağırlık sayacı
S_n	: {1,2,…,n} kümesinin simetri grubu.
Aut_C	: C kodunun otomorfizm grubu
C_i	: C kodunun i'inci bileşene gore delikli kodu
DAA	: Destek Ayırma Algoritması
$\mathcal{H}$	: Hull kod
Fr	: Frobenius dönüşümü

ŞEKİLLER LİSTESİ

ÖZET

Anahtar kelimeler: Goppa Kodlar, McEliece Şifreleme Sistemi, Denk Kodlar, Destek Ayırma Algoritması ve Zayıf Anahtarlar.

Bu tez dört bölümden oluşmaktadır. Birinci bölümde bazı temel tanım ve önermeler verilmiştir.

İkinci ve üçüncü bölümlerde denk kodlar arasındaki permütasyonu elde etmek için kullanılan bir yöntem olan Destek Ayırma Algoritması (Support Splitting Algorithm) ve McEliece Şifreleme Sisteminde Zayıf Anahtarlar konusuna değinilmiştir.

Son olarak dördüncü bölümde Destek Ayırma Algoritmasına alternatif bir metot verilmiş ve beşinci bölümde de bazı önerilerde bulunulmuştur.

SUPPORT SPLITTNG ALGORITHM AND THE WEAK KEYS IN THE MCELIECE CRYPTOSYSTEM

SUMMARY

Key Words: Goppa Codes, McEliece Cryptosystems, Equivalance Codes, Support Splitting Algorithm and Weak Keys.

This thesis consists of five chapters. In the first chapter some essential definitions and theorems are given.

In the chapters two and three The Support Splitting Algorithm which is used to find permutation between equivalent codes and The Weak Keys in The McEliece Cryptosystem are mentioned.

At last, in the chapter four an alternative method to Support Splitting Algorithm is given, and in the chapter five some suggestions are given.

BÖLÜM 1. GİRİŞ

1.1. Tanım ve Önermeler

Önerme 1.1.1 [1] Pozitif bir n tamsayısı verildiğinde, her i tamsayısı

$$i = qn + r$$

biçiminde ifade edilebilir. Burada $r, 0 < r < n - 1$ şartını sağlayan bir tam sayı ve q ise herhangi bir tam sayıdır. Ayrıca r sayısı $mod - n$ kalan, q sayısı ise bölüm olarak adlandırılır ve $i = r\ mod\ n$ biçiminde ifade edilir.

Tanım 1.1.1 [1] Pozitif bir n tamsayısı için olası tüm $mod - n$ kalanlarının kümesini $R_n = \{0,1, \dots, n - 1\}$ ile gösterirsek ve her $r, s \in R_n$ için R_n üzerinde

$$r + s = (r + s)\ mod\ n \text{ ve } r * s = rs\ mod\ n$$

şeklinde $mod - n$ toplama ve $mod - n$ çarpma işlemlerini tanımlarsak R_n üzerinde bu işlemlerle işlem yapmaya $mod - n$ aritmetik denir.

Tanım 1.1.2. [1] $G = \{a, b, c, \dots\}$ kümesi verildiğinde, bu küme üzerinde aşağıdaki özellikleri sağlayan bir $\oplus$ işlemi varsa G kümesine grup denir.

i. $\forall\ a, b \in G$ için $a \oplus b \in G$ dir (kapalılık özelliği).
ii. $\forall\ a, b, c \in G$ için $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ (birleşme özelliği).
iii. $\forall\ a \in G$ için G kümesinde $0 \oplus a = a \oplus 0 = a$ olacak şekilde bir 0 elemanı vardır (birim eleman özelliği).
iv. $\forall\ a \in G$ için G kümesinde $(-a) \oplus a = a \oplus (-a) = 0$ olacak şekilde bir $-a$ elemanı vardır. (ters eleman özelliği).

Eğer $\forall\, a, b \in G$ için $a \oplus b = b \oplus a$ özelliği sağlanıyorsa bu gruba değişmeli grup ya da Abel grubu denir. Ayrıca eğer G kümesi sonlu ise bu gruba sonlu grup ve gruptaki eleman sayısına da grubun mertebesi denir.

Önerme 1.1.2. [1] $R_n = \{0,1, \dots, n-1\}$ kümesi $mod - n$ toplama işlemi altında bir gruptur. Bu grup $\mathbb{Z}_n$ şeklinde de gösterilir.

Tanım 1.1.3. [1] G sonlu bir grup ve $g \in G$ olmak üzere bu grubun her elemanı $g \oplus g \oplus \dots \oplus g$ şeklinde g elemanının sonlu toplamları şeklinde ifade edilebiliyorsa G grubuna sonlu dairesel grup denir. Buna göre $G = \{g, g \oplus g, \dots, \}$ yazılabilir.

Önerme 1.1.3. [1] Mertebesi n olan ve g ile üretilen dairesel grup
$\{0g, 1g, \dots, (n-1)g\}$ şeklindedir. Burada

$$ig = \underbrace{g \oplus g \oplus \dots \oplus g}_{i\ sayıda}\ , 1 \le i \le n-1, 0g = 0$$

şeklinde tanımlanır. Buna göre ayrıca $ig \to i$ dönüşümü altında $G, \mathbb{Z}_n$ ye izomorf olur.

Tanım 1.1.4. [1] G bir grup ve $S \subseteq G$ olsun. Eğer S kümesi de aynı işlem altında bir grup ise bu gruba G grubunun alt grubu denir.

Önerme 1.1.4. [1] Sonlu bir grubun her alt grubunun mertebesi grubun mertebesini böler.

Önerme 1.1.5. [1] G sonlu bir grup ve $g \in G$ olmak üzere $S(g) = \{g, g \oplus g, \dots\}, G$ nin sonlu dairesel bir alt grubudur. Ayrıca $m \in \mathbb{Z}_n$ olmak üzere

$$|S(m)| = \frac{n}{gcd(m,n)}$$

yazılabilir. Burada $gcd(m.n), m$ ve n tamsayılarının en büyük ortak bölenidir.
Buna göre $S(m) = \mathbb{Z}_n$ olması için gerek ve yeter şart $gcd(m,n) = 1$ olmasıdır.

Tanım 1.1.5. [1] $\mathbb{F}$ bir küme, $\oplus$ ve $*$ işlemleri aşağıdaki özellikleri sağlayan $\mathbb{F}$ üzerinde tanımlı iki işlem olsun. Bu durumda $\mathbb{F}$ kümesine cisim denir.

i. $\mathbb{F}$ kümesi $\oplus$ işlemi altında değişmeli bir gruptur (birim eleman 0 ile gösterilir). Toplamsal grup da denir.
ii. $\mathbb{F}^* = \mathbb{F} - \{0\}$ kümesi $*$ işlemi altında değişmeli bir gruptur (birim elemanı 1 ile gösterilir). Çarpımsal grup da denir.
iii. $\forall a, b, c \in \mathbb{F}$ için $(a \oplus b) * c = (a * c) \oplus (b * c)$ yazılabilir.

Önerme 1.1.6. [1] Her p asal sayısı için $R_p = \{0,1, \dots, p-1\}$ kümesi mod-p toplama ve mod-p çarpma işlemleri altında bir cisimdir ve $\mathbb{F}_p$(asal kalan cismi) ile gösterilir.

Önerme 1.1.7. [1] $\mathbb{F}$ sonlu bir cisim olsun. Buna göre $S(1) = \{1,1 \oplus 1, \dots,\}$, $\mathbb{F}$ cisminin sonlu bir alt cismidir. Ayrıca $S(1), p$ sayıda eleman içeriyorsa p bir asal sayıdır ve bu cisim $\mathbb{F}_p$ cismine izomorftur. Burada p sayısına $\mathbb{F}$ cisminin karakteristiği de denir.

Tanım 1.1.6. [1] Katsayıları bir $\mathbb{F}$ cisminin elemanları olan tüm polinomların kümesi $\mathbb{F}[x]$ ile gösterilir.

Tanım 1.1.7. $g(x)$, derecesi m olan bir polinom olmak üzere, eğer x^m teriminin katsayısı 1'e eşit ise, $g(x)$' e monik polinom denir.

Önerme 1.1.8. [1] $g(x)$, derecesi m olan monik bir polinom olmak üzere her $f(x)$ polinomu

$$f(x) = q(x)g(x) + r(x)$$

biçiminde ifade edilebilir. Burada $r(x)$, derecesi m den küçük olan bir polinomdur. Bu durumda $r(x)$ polinomuna $mod - g(x)$ kalan denir ve $f(x) = r(x)\ mod\ g(x)$ yazılır.

Tanım 1.1.8. [1] $f(x)$ ve $g(x)$ polinomları için $f(x) = q(x)g(x)$ olacak şekilde bir $q(x)$ polinomu bulunabiliyorsa $g(x)$ polinomuna $f(x)$ polinomunun bir böleni denir.

Tanım 1.1.9. [1] Bir $f(x)$ polinomunun kendisinden ve 1 den farklı monik bir $g(x)$ böleni varsa, $g(x)$ polinomuna $f(x)$ polinomunun bir çarpanı denir. Ayrıca derecesi 1'e eşit veya daha büyük olup çarpanı olmayan bir polinoma indirgenemez polinom ve indirgenemez olup aynı zamanda monik olan bir polinoma asal polinom denir.

Önerme 1.1.9. [1] $\mathbb{F}$ herhangi bir cisim olmak üzere, $\forall f(x) \in \mathbb{F}[x]$ monik polinomu $\mathbb{F}[x]$ de asal polinomların çarpımı şeklinde tek türlü olarak(çarpanların sırası düşünülmeksizin) yazılabilir

Önerme 1.1.10. [1] $\mathbb{F}$ herhangi bir cisim olmak üzere, derecesi m olan monik bir polinom $\mathbb{F}$ üzerinde en fazla m tane köke sahip olabilir.

Önerme 1.1.11. [1] $\mathbb{F}$ herhangi bir cisim olmak üzere, $\mathbb{F}^*$ çarpımsal grubu verilen bir pozitif n tamsayısı için mertebesi n olan en fazla bir tane dairesel alt grup içerebilir ve eğer böyle bir dairesel alt grup varsa elemanları, $\beta \in \mathbb{F}^*$ olmak üzere $1, \beta, \beta^2, \dots, \beta^{n-1}$ şeklindedir ve $x^n - 1 = 0$ denklemini sağlarlar. Ayrıca bu alt cisme β tarafından üretilen çarpımsal dairesel alt grup denir. Eğer bu grup $\mathbb{F}^*$ grubuna eşitse β ya primitif eleman denir.

Önerme 1.1.12. [1] $\mathbb{F}_q$, q elemanlı bir cisim olmak üzere $\mathbb{F}_q^*$ çarpımsal grubunun $q - 1$ sayısını tam bölen pozitif her d tamsayısı için mertebesi d olan çarpımsal bir alt grubu vardır.

Tanım 1.1.10. [1] $\beta \in \mathbb{F}_q$ olmak üzere, $\mathbb{F}_p[x]$ de $g(\beta) = 0$ şartını sağlayan derecesi en küçük olan monik $g(x)$ polinomuna β nın minimal polinomu denir.

Önerme 1.1.13. [1] $\beta \in \mathbb{F}_q$ elemanının minimal polinomu $g(x)$ olmak üzere $\mathbb{F}_q$ cisminin β elemanını içeren en küçük alt cismi $\mathbb{F}[x]/g(x)$ cismine izomorftur.

Önerme 1.1.14. [1] Karakteristiği p olan q elemanlı her $\mathbb{F}_q$ cismi bir $\mathbb{F}[x]/g(x)$ cismine izomorftur. Burada $g(x) \in \mathbb{F}_p[x]$ bir asal polinomdur. Buna göre $q = p^{derg(x)}$ yazılabilir. Ayrıca $g(x) \in \mathbb{F}_p[x]$, derecesi m olan asal bir polinom olmak üzere, p^m elemanlı tüm cisimler $\mathbb{F}[x]/g(x)$ cismine izomorftur.

Önerme 1.1.15. [1] $g(x), p^m$ elemanlı bir $\mathbb{F}$ cisminin minimal bir polinomu olsun. Buna göre $g(x)$ polinomunun kökleri $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{n-1}}$ şeklindedir. Burada n, m sayısını bölen pozitif bir tamsayıdır. Dahası $g(x)$ polinomu $x^{p^n} - x$ polinomunu böler.

Önerme 1.1.16. [1] $x^{p^m} - x$ polinomu $\mathbb{F}_p$ üzerinde tekrarsız olarak $\mathbb{F}_p[x]$ deki asal polinomların çarpımı şeklindedir. Ayrıca $\mathbb{F}_p[x]$ deki asal polinomların dereceleri m yi böler.

Önerme 1.1.17. [1] Her m pozitif tamsayısı ve asal p tam sayısı için için derecesi m olan asal bir $g(x) \in \mathbb{F}_p[x]$ polinomu vardır.

Önerme 1.1.18. [1] p^m elemanlı her cisim, m sayısını bölen pozitif her n tamsayısı için p^n elemanlı bir alt cisim içerir.

p^m elemanlı bir cisim $\mathbb{F}$ ve bu cismin p^n elemanlı bir alt cismi $\mathcal{F}$ olsun. Buna göre n pozitif tam sayısının m pozitif tam sayısını bölmesi gerektiği şu şekilde gösterilebilir: $m = q.n + r\,, 0 \leq r < n$ olmak üzere $\mathcal{F}^*$ çarpımsal dairesel grubu $\mathbb{F}^*$ çarpımsal dairesel grubunun alt grubu olduğundan $p^n - 1$ sayısı $p^m - 1$ sayısını böler. Dolayısıyla

$p^n \equiv 1\ mod\ (p^n - 1)$

yazılabileceğinden

$p^m - 1 \equiv p^{q.n+r} - 1 \equiv (p^n)^q p^r - 1 \equiv p^r - 1 \equiv 0 \, mod \, (p^n - 1)$

$\Longrightarrow p^r - 1 = 0 \Longrightarrow r = 0$

elde edilir. O halde n pozitif tam sayısı m pozitif tam sayısını böler.

Örnek 1.1.1. $\mathbb{F}_{2^4}$ cisminin tüm elemanları $x^{2^4} - x$ polinomunun kökleridir. Ayrıca $\mathbb{F}_2$ üzerinde derecesi 4' ün böleni olan asal polinomlar $x^{2^4} - x$ polinomunun asal çarpanlarıdırlar ve bu polinomların dereceleri 4' ü böler. Dolayısıyla bu polinomların dereceleri 1,2 veya 4 olabilir. Ayrıca $\beta \in \mathbb{F}_{2^4}$ elemanının minimal polinomu $m_\beta(x) = x^4 + x + 1$ olsun. Buna göre β yı içeren en küçük alt cisim $\mathbb{F}[x]/m_\beta(x)$ polinomal kalan cismine izomorf olacağından β primitif elemandır. Diğer minimal polinomlar aşağıdaki gibidir.

$m_0(x) = x$
$m_1(x) = (x + 1),$
$m_{\beta^5}(x) = (x - \beta^5)(x - \beta^{10}) = x^2 + x + 1$
$m_{\beta^7}(x) = (x - \beta^7)(x - \beta^{14})(x - \beta^{13})(x - \beta^{11}) = x^4 + x^3 + 1$
$m_{\beta^3}(x) = (x - \beta^3)(x - \beta^6)(x - \beta^{12})(x - \beta^9) = x^4 + x^3 + x^2 + x + 1$

Ayrıca $x^2 + x = x(x + 1)$ ve $x^4 + x = x(x + 1)(x^2 + x + 1)$ yazılabileceğinden $\mathbb{F}_{2^4}$ cisminin alt cisimleri $\{0 , 1\}$ ve $\{0 ,1 , \beta^5, \beta^{10}\}$ olarak bulunur.

Tanım 1.1.11. [2] H girdileri 0 ve 1 lerden oluşan herhangi bir matris olsun. Buna göre

$Hx^t = 0$

denklemini sağlayan tüm x vektörlerinin oluşturduğu kümeye parite kontrol matrisi H olan bir lineer kod denir. Burada işlemler mod 2 ye göre yapılır.

Tanım 1.1.12. [2] $x = x_1 x_2 \dots x_n$ kod sözü için Hamming ağırlığı $x_i \neq 0$ şartını sağlayan sembollerin sayısı olarak tanımlanır ve $wt(x)$ şeklinde gösterilir.

Tanım 1.1.13. [2] Lineer bir kodun iki kod sözü $x\ ve\ y$ olmak üzere bu iki kod söz arasındaki Hamming uzaklığı $x-y$ kod sözünün Hamming ağırlığı yani $wt(x-y)$ olarak tanımlanır.

Tanım 1.1.14. [2] Parite kontrol matrisi H ve üreteç matrisi G olan lineer kodu C ile gösterirsek, parite kontrol matrisi G ve üreteç matrisi H olan koda C kodunun duali denir ve $C^{\perp}$ ile gösterilir.

Lineer kodlar için bir diğer önemli parametre ağırlık sayacıdır.

Tanım 1.1.15. [2] A_i ile $[n,k]-$lineer C kodunda ağırlığı i olan kodsözlerin sayısını gösterelim. Buna göre;

$$W_C(x,y)=\sum_{i=0}^{n} A_i x^{n-i}y^i=\sum_{u\in C} x^{n-wt(u)}y^{wt(u)}$$

olarak tanımlanan $W_C(x,y)$ polinomuna C kodunun ağırlık sayacı denir. Ağırlık sayacında $x=1$ alınabilir ve

$$W_C(1,y)=\sum_{i=0}^{n} A_i y^i=\sum_{u\in C} y^{wt(u)}$$

yazılabilir.

Tanım 1.1.16. [3] X,n elemanlı herhangi bir küme olsun. Bu durumda X üzerinde tanımlı tüm permütasyonların kümesi bileşke işlemiyle beraber bir grup oluşturur ve bu gruba X in simetri grubu denir ve kısaca S_n ile gösterilir.

Tanım 1.1.17. [3] G bir grup olmak üzere $G\times X\to X$ şeklinde bir dönüşüm için $g\in G, x\in X$ olmak üzere $(g,x)\in G\times X$ elemanının bu dönüşüm altındaki görüntüsünü $g.x$ şeklinde gösterirsek aşağıdaki iki şartın sağlanması durumunda X kümesine bir G -set denir.

i. $e.x = x, \forall x \in X$ (e, G grubunun brim elemanıdır).

ii. $(g_1 g_2).x = g_1.(g_2.x),\ \forall g_1, g_2 \in G$ ve $\forall x \in X$.

Tanım 1.1.18. [3] $x \in X, G.x = \{g.x |\ g \in G\}$ kümesine x elemanının G altındaki orbiti denir.

Buna göre X üzerinde $\sim$ bağıntısını $x, y \in X,\ x \sim y \Leftrightarrow y = g.x, \exists g \in G$ olarak tanımlarsak X üzerinde bir denklik bağıntısı tanımlamış oluruz ve $x \in X$ elemanının denklik sınıfı $G.x$ olur. Buna göre $G.x$ orbitleri X kümesinin bir parçalanışını tanımlar.

1.2. McEliece Şifreleme Sistemleri

Tanım 1.2.1. Verilen bir algoritma için, girdinin uzunluğu n ve $P(x)$ herhangi bir polinom olmak üzere algoritmanın tamamlanması için gereken süre en fazla $P(n)$ kadar ise bu algoritmaya polinomal zamanlıdır denir.

Tanım 1.2.2. [4] ζ, polinomial zamanlı bir t-hata düzelten algoritması bilinen F_2 üzerinde tanımlı (n, k) −kodların(n uzunluğunda k boyutlu lineer kodlar) bir ailesi olsun. Buna göre McEliece tipinde bir şifreleme sistemi aşağıdaki adımlardan oluşur.

I. $\Gamma \in \zeta$ kodu(gizli kod) ve $\pi \in S_n$ permütasyonu birlikte gizli anahtarı oluşturur.
II. $C = \pi(\Gamma)$ kodunun bir üreteç matrisi G açık anahtarı oluşturur.
III. $mG + e$ şeklinde şifrelenen m mesajı π permütasyonu ve polinomal zamanlı t-hata düzelten algoritma kullanılarak kolaylıkla elde edilebilir. Burada e Hamming ağırlığı t olan hata vektörüdür.

[5] de gösterildiği üzere $mG + e$ vektöründen hareketle mG vektörünü bulmak zor bir problem olduğundan, McEliece parametreleri [6] için sistem bu noktada güvenlidir. Sistemin güvenliği ayrıca C kodundan hareketle π permütasyonunu ve Γ kodunu elde etmenin zorluğuna bağlıdır. Bu noktada sistemin güvenliği seçilen ζ kod ailesine bağlıdır [7].

Tanım 1.2.3. [4] $L = (\alpha_1, \alpha_2, \dots, \alpha_n)$, F_{2^m} elemanlarının sıralı bir kümesi ve g, t dereceli F_{2^m} üzerinde tanımlı F_{2^m} de hiçbir kökü olmayan bir polinom olsun(üreteç polinom). Buna göre $\Gamma(L, g)$ ile gösterilen Goppa kodu;

$$\forall j, 0 \leq j < t, \sum_{\alpha \in L} z_\alpha \frac{\alpha^j}{g(\alpha)} = 0 \qquad \textbf{(1.1)}$$

(1.1) denklemini sağlayan $c = \left(c_{\alpha_1}, c_{\alpha_2}, \dots, c_{\alpha_n}\right) \in F_2^n$ vektörlerinden oluşur. Bu denklem matris formunda

$$\underbrace{\left[c_{\alpha_1}\ c_{\alpha_2} \dots c_{\alpha_n}\right]}_{c} \underbrace{\begin{bmatrix} g^{-1}(\alpha_1) & g^{-1}(\alpha_2) & \dots & g^{-1}(\alpha_n) \\ g^{-1}(\alpha_1)\alpha_1 & g^{-1}(\alpha_2)\alpha_2 & \dots & g^{-1}(\alpha_n)\alpha_n \\ & \vdots & & \\ g^{-1}(\alpha_1)\alpha_1^{t-1} & g^{-1}(\alpha_2)\alpha_2^{t-1} & \dots & g^{-1}(\alpha_n)\alpha_n^{t-1} \end{bmatrix}^t}_{H} = 0$$

şeklinde de ifade edilebilir. Dolayısıyla H matrisi $\Gamma(L, g)$ Goppa kodunun parite kontrol matrisidir. Buna göre $\Gamma(L, g)$ Goppa kodunun boyutu k ve Hamming ağırlığı d olmak üzere, $k \geq n - mt$ ve $d \geq t + 1$ yazılabilir [8].

Örnek 1.2.1. $f(x)$ polinomunu, $f(x) = x^4 + x^3 + 1$ şeklinde tanımlarsak, f polinomu F_2 üzerinde asaldır. Buna göre $\alpha \in F_{2^4}$, $f(\alpha) = 0$ olmak üzere F_{2^4} cismi Tablo 1.1. deki gibi olur.

Tablo 1.1. F_{2^4} cisminin elemanları

$\alpha^0 = 1$	$\alpha^4 = \alpha^3 + 1$	$\alpha^8 = \alpha^3 + \alpha^2 + \alpha$	$\alpha^{12} = \alpha + 1$
$\alpha^1 = \alpha$	$\alpha^5 = \alpha^3 + \alpha + 1$	$\alpha^9 = \alpha^2 + 1$	$\alpha^{13} = \alpha^2 + \alpha$
$\alpha^2 = \alpha^2$	$\alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{10} = \alpha^3 + \alpha$	$\alpha^{14} = \alpha^3 + \alpha^2$
$\alpha^3 = \alpha^3$	$\alpha^7 = \alpha^2 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + 1$	

$\Gamma(L, g)$ Goppa kodu için $g(x) = x^3 + x + 1$ ve $L = F_{2^4}$ olmak üzere Tablo 1.2. deki değerler kullanılırsa H sendrom matrisi aşağıdaki gibi elde edilir.

Tablo 1.2. $g^{-1}(\alpha_i)$ elemanlarının değerleri

$g(1)^{-1} = 1$	$g(\alpha^4)^{-1} = \alpha^{10}$	$g(\alpha^8)^{-1} = \alpha^5$	$g(\alpha^{12})^{-1} = \alpha^4$
$g(\alpha)^{-1} = \alpha^{10}$	$g(\alpha^5)^{-1} = \alpha^{10}$	$g(\alpha^9)^{-1} = \alpha^8$	$g(\alpha^{13})^{-1} = \alpha^{14}$
$g(\alpha^2)^{-1} = \alpha^5$	$g(\alpha^6)^{-1} = \alpha^2$	$g(\alpha^{10})^{-1} = \alpha^5$	$g(\alpha^{14})^{-1} = \alpha^7$
$g(\alpha^3)^{-1} = \alpha$	$g(\alpha^7)^{-1} = \alpha^{11}$	$g(\alpha^{11})^{-1} = \alpha^{13}$	

$$H = \begin{pmatrix} 1 & \alpha^{10} & \alpha^5 & \alpha & \alpha^{10} & \alpha^{10} & \alpha^2 & \alpha^{11} & \alpha^5 & \alpha^8 & \alpha^5 & \alpha^{13} & \alpha^4 & \alpha^{14} & \alpha^7 \\ & & & & & & & . & & & & & & & \\ 1 & \alpha^{11} & \alpha^7 & \alpha^4 & \alpha^{14} & 1 & \alpha^8 & \alpha^3 & \alpha^{13} & \alpha^2 & 1 & \alpha^9 & \alpha & \alpha^{12} & \alpha^6 \\ & & & & & & & . & & & & & & & \\ 1 & \alpha^{12} & \alpha^9 & \alpha^7 & \alpha^3 & \alpha^5 & \alpha^{14} & \alpha^{10} & \alpha^6 & \alpha^{11} & \alpha^{10} & \alpha^5 & \alpha^{13} & \alpha^{10} & \alpha^5 \end{pmatrix}$$

Üreteç matris $GH^t = 0$ eşitliğini sağlayacağından G üreteç matrisi aşağıdaki gibi elde edilir.

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Buna göre $\Gamma(L, g)$ Goppa kodu aşağıdaki gibi olur.

0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 1 0 1 0 1 1 0 0 0 1 1 0
1 0 1 1 0 0 0 0 1 0 1 1 1 0 1 1 1 1 1 0 1 0 1 1 0 0 1 0 0
1 0 0 0 0 1 0 1 0 0 1 1 0 1 1 1 1 0 0 1 1 1 1 0 1 0 0 0 1 0
0 1 0 0 1 0 1 0 0 1 1 1 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

1.3. Goppa Kodların Dekodlanması

(1.1) denkleminin sağlanması için gerek ve yeter şart $\sum_{\alpha\in L}\frac{c_\alpha}{z-\alpha}\equiv 0\ mod\ g(z)$ denkleminin sağlanmasıdır. Dolayısıyla alınan mesaj r ile kodsöz c ile ve hata vektörü de e ile gösterilirse $r=c+e$ olmak üzere

$$\sum_{\alpha\in L}\frac{r_\alpha}{z-\alpha}\equiv\sum_{\alpha\in L}\frac{c_\alpha+e_\alpha}{z-\alpha}\equiv\sum_{\alpha\in L}\frac{c_\alpha}{z-\alpha}+\sum_{\alpha\in L}\frac{e_\alpha}{z-\alpha}\equiv\sum_{\alpha\in L}\frac{e_\alpha}{z-\alpha}\quad modg(z)$$

elde edilir. Buna göre

$$S(z)\equiv\sum_{\alpha\in L}\frac{r_\alpha}{z-\alpha}\ modg(z) \tag{1.2}$$

$$\sigma(z)=\prod_{\substack{\alpha\in L\\ e_\alpha\neq 0}}(z-\alpha) \tag{1.3}$$

$$\eta(z)\equiv S(z)\sigma(z)\ modg(z) \tag{1.4}$$

$$\eta(z)=\sum_{\alpha\in L}\frac{e_\alpha}{z-\alpha}\prod_{\substack{\alpha\in L\\ e_\alpha\neq 0}}(z-\alpha)=\sum_{\substack{\alpha\in L\\ e_\alpha\neq 0}}e_\alpha\prod_{\substack{\alpha\in L\\ e_\alpha\neq 0\\ \beta\neq\alpha}}(z-\beta) \tag{1.5}$$

Sırasıyla $S(z)$, $\sigma(z)$ ve $\eta(z)$ polinomları (1.2) , (1.3) ve (1.5) ifadeleriyle tanımlanırsa, c kodsözünü elde edebilmek için (1.4) denklemini sağlayan en küçük dereceli σ ve η polinomlarının bulunması gerekir [9].

1.3.1. Berlekamp-Massey algoritması

Algoritma I. [10] (1.4) denkleminde $g(z)=z^{2t}$ özel durumu için $\sigma(z)=\Lambda_0+\Lambda_1 z+\cdots+\Lambda_v z^v, \Lambda_0=1$ olmak üzere η polinomunun derecesi (1.5) ifadesine göre en fazla $v-1$ olabilir. Dolayısıyla

$\sum_{k=0}^{v} \Lambda_k S_{j-k} = 0\,,\ \ v+1 \le j \le 2t$ **(1.6)**

eşitliği yazılabilir. Bu eşitlikten hareketle σ polinomunu şu şekilde bulunabilir:

$$\sigma^{(0)}(x) = 1\ , \sigma^{(i)}(z) = \sum_{k=0}^{L_i} \Lambda_k z^k\,, 1 \le i \le 2t$$

olmak üzere

$$d_i = \sum_{k=0}^{L_i} \Lambda_k S_{j-k}$$

değerine göre aşağıdaki eşitlikler tanımlansın.

$$\sigma^{(i+1)}(z) = \sigma^{(i)}(z)\,,\quad d_i = 0$$

$$\sigma^{(i+1)}(z) = \sigma^{(i)}(z) - d_p^{-1} d_i z^{i-p} \sigma^{(p)}(z)\,,\quad d_i \neq 0$$

Burada $\sigma^{(p)}(x)$ polinomu, $d_p \neq 0$ koşulunu sağlayan $\sigma^{(i)}(z)$ polinomundan önceki herhangi bir polinomdur. Ayrıca $\{S_1, S_2, \dots, S_{N-1}\}$ kümesini üretip $\{S_1, S_2, \dots, S_{N-1}, S_N\}$ kümesini üretemeyen minimal polinomun uzunluğu L ile ve $\{S_1, S_2, \dots, S_{N-1}, S_N\}$ kümesini üreten minimal polinomun uzunluğu L' ile gösterilirse

$$L' \ge \max\{L\,, N - L\}$$

yazılabilir. Dolayısıyla yukarıdaki iterasyonlarla elde edilecek minimal polinomun derecesi en fazla t kadar olur.

Örnek 1.3.1. Algoritma I' i kullanarak $(\alpha^4, \alpha, \alpha^8, 1, \alpha^{12}, \alpha^2, \alpha^5, \alpha^{11})$ kümesinin minimal polinomu Tablo 1.3.' e göre $\sigma(z) = 1 + \alpha^{11} z + \alpha^2 z^2 + \alpha^{13} z^3 + \alpha^{14} z^4$ olarak bulunur.

Tablo 1.3. d_i değerlerine karşılık gelen $\sigma^{(i)}(x)$ polinomları

i	S_i	$\sigma^{(i)}(x)$	d_i
1	α^4	1	α^4
2	α	1	α
2	α	$1+\alpha^{12}z$	0
3	α^8	$1+\alpha^{12}z$	α^3
3	α^8	$1+\alpha^{7}z$	0
4	1	$1+\alpha^{7}z$	0
5	α^{12}	$1+\alpha^{7}z$	α^2
5	α^{12}	$1+\alpha^{7}z+\alpha^{14}z^2+\alpha^{11}z^3$	0
6	α^2	$1+\alpha^{7}z+\alpha^{14}z^2+\alpha^{11}z^3$	α^3
6	α^2	$1+\alpha^{9}z+\alpha z^2+\alpha^{11}z^3$	0
7	α^5	$1+\alpha^{9}z+\alpha z^2+\alpha^{11}z^3$	1
7	α^5	$1+\alpha^{5}z+\alpha^{12}z^2+\alpha^{10}z^3+\alpha^{4}z^4$	0
8	α^{11}	$1+\alpha^{5}z+\alpha^{12}z^2+\alpha^{10}z^3+\alpha^{4}z^4$	α^{14}
8	α^{11}	$1+\alpha^{11}z+\alpha^{2}z^2+\alpha^{13}z^3+\alpha^{14}z^4$	0

Algoritma II [9] (1.4) denkleminin, derecesi n olan herhangi bir g polinomu için çözümü aşağıdaki gibi elde edilebilir.

1.adım. $0 \le i \le n-1$, $z^i S(z) mod g(z)$ polinomlarında z^{n-1} terimlerinin katsayıları a_i olmak üzere $h(z) = a_0 + a_1 z + \cdots + a_{t-1} z^{n-1}$ polinomu tanımlanır.

2.adım.

$h(z)\sigma^*(z) \equiv \eta^*(z) mod\ z^n$, n çift ise

$h(z)\sigma^*(z) \equiv \eta^*(z) mod\ z^{n-1}$, n tek ise

denklemini sağlayan derecesi en küçük olan σ^* ve η^* polinomları Algoritma I kullanılarak bulunur.

3.adım. $\sigma^*(z) = c_0 + c_1 z + \cdots + c_r z^r$, $N = max\{der\sigma^*, der\eta^* + 1\}$, $r \leq N$ olmak üzere

$$\sigma(z) = c_0 z^N + c_1 z^{N-1} + \cdots + c_r z^{N-r}$$

polinomu elde edilir. Böylece en fazla t hata düzelten polinomal zamanlı bir algoritma elde edilmiş olur

1.3.2. Patterson algoritması

$\Gamma(L, g)$ Goppa kodu F_2 üzerinde tanımlandığı zaman

$$S(z)\sigma(z) \equiv \sigma'(z)\, mod g(z) \qquad \textbf{(1.7)}$$

yazılabilir. Buna göre $a \in \Gamma(L, g)$ olması için gerek ve yeter şart

$$S_a(z) = 0\, mod g(z) \Leftrightarrow g(z) | \sigma_a'(z)$$

olduğundan ve F_2 de herhangi bir polinom $\sigma = \alpha^2 + z\beta^2$ şeklinde ifade edilebileceğinden $\sigma' = \beta^2$ polinomu her zaman bir tam karedir. Dolayısıyla

$$g(z) | \sigma_a'(z) \Leftrightarrow g^2(z) | \sigma_a'(z)$$

yazılabileceğinden $\Gamma(L, g) = \Gamma(L, g^2)$ elde edilir. Bu sonuca göre $derg = t$ olmak üzere $d \geq 2t + 1$ yazılabilir. [10]
(1.7) denklemine geri dönülürse $\sigma = \alpha^2 + z\beta^2$ olmak üzere

$$(\alpha^2 + z\beta^2)S \equiv \beta^2\, mod g$$

yazılabilir. Ayrıca S polinomunun tüm kökleri F_{2^m} cisminin elemanı olduğundan ve g polinomunun F_{2^m} üzerinde kökü olmadığından S ve g polinomları aralarında asladır. Dolayısıyla $Sh \equiv 1\, mod g$ olacak şekilde bir h polinomu bulunabilir. Buna göre

$Sh(\alpha^2 + z\beta^2) \equiv h\beta^2 \ \ mod g$

veya

$$(h + z)\beta^2 \equiv \alpha^2 \ \ mod g \qquad \textbf{(1.8)}$$

yazılabileceğinden ve (1.8) denkleminin sağ tarafı tam kare bir ifade olduğundan denklemin sol tarafı da tam kare bir ifade olmalıdır. Buna göre $h + z \equiv d^2 \ mod g$ olacak şekilde bir d polinomu bulunabilir. Dolayısıyla $d^2\beta^2 \equiv \alpha^2 \ mod g$ veya

$$d\beta \ \equiv \alpha \ \ mod g \qquad \textbf{(1.9)}$$

yazılabilir. Berlekamp-Massey algoritması kullanılarak (1.9) denkleminde α ve β polinomları bulunabilir ve böylece $\sigma = \alpha^2 + z\beta^2$ polinomu bulunmuş olur [9].

BÖLÜM 2. DESTEK AYIRMA ALGORİTMASI

Tanım 2.1. [11] $I_n = \{1,2,\dots,n\}$ indis kümesi ve $x = (x_i)_{I_n} \in C$ olmak üzere $des(x) = \{i \in I_n | \, x_i \neq 0\}$ kümesine x kodsözünün desteği denir.

Tanım 2.2. [11] C kodsözü verildiğinde $des(C) = \bigcup_{x \in C} des(x)$ şeklinde tanımlı kümeye C kodunun desteği denir.

Tanım 2.3. [11] F_2 üzerinde tanımlı n uzunluğunda C ve C' kodları verildiğinde eğer C' kodunun kodsözleri C kodunun kodsözlerinin koordinatlarına bir $\pi \in S_n$ permütasyonu uygulanmasıyla elde edilebiliyorsa(bu durumu kısaca $C' = \pi(C)$ şeklinde de ifade edilebilir.) bu iki koda denktirler denir ve $C \sim C'$ yazılır.

Yukarıdaki tanıma göre C kodunun indis kümesi I_n ise $\pi(C)$ kodunun indis kümesinin $\pi(I_n)$ olacağı açıktır. Bu tezde aksi belirtilmedikçe C ile n uzunluğunda ve F_2 cismi üzerinde lineer bir kodu ifade edilmiştir.

Tanım 2.4. [11] C kodu için $\sigma(C) = C$ koşulunu sağlayan $\sigma \in S_n$ permütasyonlarının oluşturduğu gruba C nin otomorfizm grubu denir. Bu tezde, C kodu verildiğinde C nin otomorfizm grubu Aut_C ile gösterilmiştir.

Tanım 2.5. [11] $J \subseteq I_n$ olmak üzere, C kodunun kod sözlerinin J ile indislenen koordinatlarının yerlerine sıfır yazılmasıyla elde edilen koda C kodunun delikli kodu denir ve C_J ile gösterilir. $J = \{i\}$ olması durumunda kısaca C_i yazılır.

Örnek 2.1. Örnek 1.2.1 deki Goppa kodunda, $J = \{1,15\}$ olmak üzere, 1' inci ve 15' inci bileşenler sıfır olarak alınırsa $\Gamma_J(L, g)$ kodu

0 1 1 1 1 1 1 1 1 1 1 1 1 1 0	0 0 1 1 0 1 0 1 1 0 0 0 1 1 0
0 0 1 1 0 0 0 0 1 0 1 1 1 0 0	0 1 1 1 1 0 1 0 1 1 0 0 1 0 0
0 0 0 0 0 1 0 1 0 0 1 1 0 1 0	0 1 0 0 1 1 1 1 0 1 0 0 0 1 0
0 1 0 0 1 0 1 0 0 1 1 1 0 0 0	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

olarak elde edilir.

Önerme 2.1. [11] C kodu verildiğinde her $\pi \in S_n$ permütasyonu $J \subseteq I_n$ indisi için

$$\pi(C_J) = \pi(C)_{\pi(J)}$$

yazılabilir.

İspat. C kodunun kod sözleri alt alta yazılırsa mxn boyutlu bir M matrisi ve C_J kodunun kod sözleri alt alta yazılırsa yine mxn boyutlu bir M_J matrisi elde edilir. Burada M matrisi ile M_J matrislerinin J ile indislenen sütun vektörleri hariç diğer tüm sütun vektörleri aynı olup M_J matrisinin J ile indislenen sütun vektörleri sıfırdır. Benzer şekilde $\pi(C)$ ve $\pi(C_J)$ kodlarının kod sözleri alt alta yazılırsa mxn boyutlu M' ve M'' matrisleri elde edilir. Buna göre M_J matrisinin sütun vektörleri α_j ile gösterilirse M'' matrisinin sütun vektörleri α_j vektörlerinin σ permütasyonu ile yeniden sıralanmasından şeklindedir. Dolayısıyla M'' matrisinin sütun vektörleri β_j ile gösterilirse $\forall j \notin J, 1 \leq j \leq n$ için $\beta_j = \alpha_{\sigma(j)}$ ve $\forall j \in J$ için $\beta_j = 0$ yazılabileceğinden ve M'' ile $M'_{\sigma(J)}$ matrislerinin boyutları aynı olduğundan

$$M'' = M'_{\sigma(J)} \Longrightarrow \sigma(C_J) = \sigma(C)_{\sigma(J)}$$

elde edilir.

Sonuç 2.1. C ve C' kodları denk ise yani $\exists\pi \in S_n$ için $C' = \pi(C)$ ise $J' = \pi(J)$ olmak üzere C_J ve C'_j, kodları da denktirler.

Tanım 2.6. [11] $\forall\sigma \in S_n$ permütasyonu için $T(C) = T\big(\sigma(C)\big)$ koşulunu sağlayan bir T dönüşümüne invaryant denir.

Tanım 2.7. [11] F herhangi bir küme ve S, F üzerinde değerler alan bir dönüşüm olsun. Eğer $\forall i \in I_n,\ \forall\sigma \in S_n$,

$$S(C,i) = S\big(\sigma(C), \sigma(i)\big)$$

koşulu sağlanıyorsa S dönüşümüne F üzerinde bir imza denir.

Önerme 2.2. [11] V bir invaryant olmak üzere

$$S_V(C,i) = V(C_i)$$

olarak tanımlanan S_V dönüşümü bir imzadır.

İspat. $\forall\sigma \in S_n,\ \ S_V\big(\sigma(C), \sigma(i)\big) = V\big(\sigma(C)_{\sigma(i)}\big) = V(\sigma(C_i) = V(C_i) = S_V(C,i).$

Tanım 2.8. [11] S, F üzerinde değerler alan bir imza ve

$$P = \{P_f\}_{f\in F}\ ,\ P_f = \{\ i \in I_n |\ S(C,i) = f \in F\}$$

olmak üzere P kümesine I_n indis kümesinin (C,S) –parçalanışı ve P_f kümelerine de parçalanışın sınıfları denir.

Tanım 2.9. [11] $P = \{P_f\}_{f\in F}$ ve $P' = \{P'_f\}_{f\in F}$, I_n indis kümesinin iki parçalanışı olmak üzere $\forall f \in F$, $|P_f| = |P'_f|$ oluyorsa P ve P' parçalanışlarına denktirler denir ve bu durumda $P \sim P'$ yazılır.

Tanım 2.10. [11] Bir C kodu ve S imzası verildiğinde eğer

$\exists\, i\,,\ j\ \in\ I_n$ için $S(C,i)\ \neq\ S(C,j)$

yazılabiliyorsa S imzasına C kodu için bir diskriminant, eğer

$\forall\, i\ ,\ j\ \in\ I_n$ için $S(C,i) \neq S(C,j)$

oluyorsa tam diskriminant denir.

Önerme 2.3. [11] (C,S) –parçalanışı P ile gösterilirse $(\sigma(C),S)$ –parçalanışı $\sigma(P)$ ye eşit olur.

İspat. (C,S) ve $(\sigma(C),S)$ parçalanışları sırasıyla $P=\{P_f\}_{f\in F}$ ve $P'=\{{P'}_f\}_{f\in F}$ olmak üzere,

$(\Rightarrow)$: $j\in\ \sigma(P_f)$ ve $\exists i\in P_f\ ,\ j=\sigma(i)$, olmak üzere

$f=\ S(C,i)=S\big(\sigma(C),\sigma(i)\big)=S(\sigma(C),j)\ \Longrightarrow j\in {P'}_f\ \Longrightarrow \sigma(P_f)\subseteq {P'}_f$

elde edilir.

$(\Leftarrow)$: $j\in {P'}_f\ \Longrightarrow j=\sigma(i),\ \ \exists i\in I_n,\ f=S(\sigma(C),j)=S\big(\sigma(C),\sigma(i)\big)=S(C,i)$

$\Longrightarrow i\in P_f\ ,\ j\in\sigma(P_f)\ \Longrightarrow {P'}_f\ \subseteq\ \sigma(P_f)$ yazılabilir. Buna göre

$\forall f\in F$ için ${P'}_f=\sigma(P_f)$ yazılabileceğinden

$P'=\sigma(P)$

elde edilir.

Sonuç 2.2. C ve C' kodları verildiğinde $P = (C, S)$ ve $P' = (C', S)$ olmak üzere $C' = \pi(C),\ \pi \in S_n$ ise $P' = \pi(P)$ yazılabilir.

Sonuç 2.3. $Aut_{\ C}$ grubu birimden farklı ise C kodu için tam diskriminant yoktur.

Önerme 2.4. $C' \sim C$ olmak üzere S imzası C kodu üzerinde tam diskriminant ise C ile C' arasındaki permütasyon bulunabilir.

İspat. $C' = \pi(C)$ olmak üzere (C, S) ve (C', S) parçalanışlarını sırasıyla P ve P' ile gösterilirse $P' = \pi(P)$ yazılabilir ve S, C üzerinde tam diskriminant olduğundan dolayı her bir sınıf tek bir elemandan oluşacağından π permütasyonu belirlenmiş olur.

Örnek 2.2. $C = \{1111, 0111, 1010, 0001\}, C' = \{1111, 1110, 0011, 0100\}$ denk kodlar ve $C' = \pi(C)$ olmak üzere

Tablo 2.1. C ve C' kodları için $C_i,\ C_i',\ W_{C_i}(x)$ ve $W_{C_i'}(x)$ değerleri

$\boldsymbol{i}$	$\boldsymbol{C_i}$	$\boldsymbol{W_{C_i}(x)}$	$\boldsymbol{C'_i}$	$\boldsymbol{W_{C'_i}(x)}$
1	0111,0111,0010,0001	$2x + 2x^3$	0111,0110,0011,0100	$x + 2x^2 + x^3$
2	1011,0011,1010,0001	$x + 2x^2 + x^3$	1011,1010,0011,0000	$1 + 2x^2 + x^3$
3	1101,0101,1000,0001	$2x + x^2 + x^3$	1101,1100,0001,0100	$2x + x^2 + x^3$
4	1110,0110,1010,0000	$1 + 2x^2 + x^3$	1110,1110,0010,0100	$2x + 2x^3$

Tablo 2.1.' e göre

$W_{C'_1}(x) = W_{C_2}(x) \implies 1 = \pi(2)$

$W_{C'_2}(x) = W_{C_4}(x) \implies 2 = \pi(4)$

$W_{C'_3}(x) = W_{C_3}(x) \implies 3 = \pi(3)$

$W_{C'_4}(x) = W_{C_1}(x) \implies 4 = \pi(1)$

yazılabileceğinden $\pi = (1\ 4\ 2)$ elde edilir.

Tanım 2.11. [11] C kodu ve S imzası verildiğinde yukarıda anlatıldığı gibi C kodunun supportunun bir (C, S) –parçalanışının elde edildiği yönteme Destek Ayırma Algoritması denir. Bu tezde Destek Ayırma Algoritması kısaca DAA şeklinde gösterilmiştir.

Uygulamada DAA(Destek Ayırma Algoritması) uygulanırken invaryant olarak genelde Hamming ağırlık sayacı kullanılır ve bu durumda en büyük zorluk, kodların boyutu arttıkça ağırlık sayacının hesaplanmasıdır. Bu nedenle Hull kod kavramı tanımlanmıştır. [12]

Tanım 2.12. [13] C, n uzunluğunda lineer bir kod ve $C^{\perp}, C$ kodunun duali olmak üzere

$$\mathcal{H}(C) = C \cap C^{\perp}$$

şeklinde tanımlanan koda C kodunun Hull kodu denir.

Lemma 2.1. [11] C ve C' n uzunluğunda iki kod olmak üzere her $\sigma \in S_n$ permütasyonu için

$$\sigma(C \cap C') = \sigma(C) \cap \sigma(C')$$

yazılabilir.

Lemma 2.2. C, n uzunluğunda lineer bir kod olmak üzere $\forall x, y \in C$ için

$$x = (x_i)_{i \in I_n}, y = (y_i)_{i \in I_n}, x.y = xy^t = \sum_{i \in I_n} x_i\, y_i$$

şeklinde tanımlı skaler çarpım, permütasyon işlemi altında değişmez.

İspat. $:\Rightarrow \forall x \in C$ ve $\forall y \in C^{\perp}$ için $\overline{x} = \sigma(x), \overline{y} = \sigma(y)$ olmak üzere σ permütasyonuna karşılık gelen matris P ile gösterilirse permütasyon matrisin ortogonallik ($P^t = P^{-1}$) [14] özelliğinden dolayı

$$\overline{x}\,\overline{y} = (xP^t)(yP^t)^t = (xP^t)(Py^t) = (xP^{-1})(Py^t) = xy^t = x.y = 0$$

olarak istenen elde edilir.

Lemma 2.3. [11] C, n uzunluğunda lineer bir kod ve $C^{\perp}, C$ kodunun dualini göstermek üzere her $\sigma \in S_n$ permütasyonu için

$$[\sigma(C)]^{\perp} = \sigma(C^{\perp})$$

yazılabilir.

İspat: Lemma 2.2 den $\sigma(C^{\perp}) \subseteq [\sigma(C)]^{\perp}$ olduğu açıktır. $boy(C) = k$ olmak üzere

$$boy(C^{\perp}) = n - k, boy\big(\sigma(C)\big) = k, boy\big(\sigma(C^{\perp})\big) = n - k, boy([\sigma(C)]^{\perp}) = n - k$$

$$boy\big(\sigma(C^{\perp})\big) = boy([\sigma(C)]^{\perp}) \text{ ise } [\sigma(C)]^{\perp} = \sigma(C^{\perp})$$

elde edilir.

Önerme 2.5. [11] C ve C', n uzunluğunda iki lineer kod olmak üzere $C \sim C'$ ise

$$\mathcal{H}(C) \sim \mathcal{H}(C')$$

yazılabilir.

İspat . $\sigma\big(\mathcal{H}(C)\big) = \sigma(\, C \cap C^{\perp}) = \sigma(C) \cap \sigma(C^{\perp}) = \sigma(C) \cap [\sigma(C)]^{\perp} =$
$\mathcal{H}\big(\sigma(C)\big) = \mathcal{H}(C').$

BÖLÜM 3. MCELIECE ŞİFRELEME SİSTEMİNDE ZAYIF ANAHTARLAR

Önerme 2.3. e göre C ve C' kodları verildiğinde eğer bu kodlar denk ise bunlara karşılık gelen $P = (C, S)$ ve $P' = (C', S)$ parçalanışları da denk olur. Ancak bunun tersi her zaman doğru değildir. Daha açık bir ifadeyle P ve P' parçalanışlarının denk olması C ve C' kodlarının denk olduklarını göstermez. Ancak pratikte, P ve P' parçalanışlarının sınıflarının hepsi tek bir elemandan oluşmadığı zaman kodların uzunlukları yeterince büyük olduğu takdirde $(n \geq 1024)$ bunun doğru olduğu varsayılabilir. Yine Önerme 2.3. den i ve j elemanları eğer Aut_C grubuna göre aynı orbitte ise $S(C, i) = S(C, j)$ yazabiliriz. Ancak bunun tersi her zaman doğru değildir. Dolayısıyla $S(C, i) = S(C, j)$ olması göre i ve j nin Aut_C grubuna göre aynı orbitte oldukları anlamına gelmez. Ancak yine de $S(C, i) = S(C, j)$ koşulunu sağlayan elemanların oluşturduğu sınıflar Aut_C grubuna göre orbitlerin birleşiminden oluşacağından eğer Aut_C grubuna göre orbitleri biliyorsak bundan hareketle bazı sonuçlara varılabilir [4].

Tanım 3.1. $Fr: F_{2^m} \to F_{2^m}$ olmak üzere $Fr(z) = z^2$ şeklinde tanımlı dönüşüme Frobenius dönüşümü denir.

Önerme 3.1. [2] $\Gamma(L, g)$ Goppa kodu için g üreteç polinomu F_2 üzerinde tanımlanırsa Aut_Γ grubu Frobenius dönüşümü tarafından üretilir.

Önerme 3.1' e göre $L = F_{2^m}$ olmak üzere L nin Aut_Γ grubuna göre orbitlerine ayrılmış şekli $\mathcal{P}_L$ ile gösterilirse $\mathcal{P}_L \sim DAA(C)$ olup olmadığına bakılarak g üreteç polinomunun F_2 üzerinde tanımlanıp tanımlanmadığı anlaşılabilir. Dolayısıyla denenmesi gereken g polinomlarının sayısı azalmış olur. Bu nedenle bu tip Goppa kodları zayıf anahtarlar olarak adlandırılır [4].

Örnek 3.1.

$L = F_{2^4} = \{1\ ,\alpha\ ,\alpha^2,\ \alpha^3,\alpha^4\ ,\ \alpha^5\ ,\alpha^6\ ,\alpha^7\ ,\alpha^8\ ,\alpha^9\ ,\alpha^{10}\ ,\alpha^{11}\ ,\alpha^{12}\ ,\alpha^{13}\ ,\alpha^{14}\ \}$ olmak üzere L nin her bir elemanına $Fr(z) = z^2$ dönüşümü uygulanmasıyla elde edilen $\mathcal{P}_L$ parçalanışı aşağıdaki gibi elde edilir.

$$\mathcal{P}_L = \{\underbrace{1}_{\alpha^0}\ ,\underbrace{\{\alpha,\alpha^2,\alpha^4,\alpha^8\}}_{\alpha^1},\underbrace{\{\alpha^3,\alpha^6,\alpha^{12},\alpha^9\}}_{\alpha^3},\underbrace{\{\alpha^5,\alpha^{10}\}}_{\alpha^5},\underbrace{\{\alpha^7,\alpha^{14},\alpha^{13},\alpha^{11}\}}_{\alpha^7}\}$$

Örnek 3.2. Örnekte 2.1 ile verilen Goppa koduna DDA(Destek Ayırma Algoritması) uygulanırsa Tablo 3.1.' e göre

Tablo 3.1. Γ_i kodları için $W_{\Gamma_i}(x)$ Hamming ağırlık sayaçları

$\boldsymbol{i}$	$\boldsymbol{W_{\Gamma_i}(x)}$
0	$x^{14}+x^8+4x^7+x^6+1$
1	$x^{13}+2x^8+3x^7+x^6+1$
2	$x^{13}+2x^8+3x^7+x^6+1$
3	$x^{13}+2x^8+3x^7+x^6+1$
4	$x^{13}+2x^8+3x^7+x^6+1$
5	$x^{13}+x^9+x^8+2x^7+2x^6+1$
6	$x^{13}+2x^8+3x^7+x^6+1$
7	$x^{13}+x^9+x^8+2x^7+2x^6+1$
8	$x^{13}+2x^8+3x^7+x^6+1$
9	$x^{13}+2x^8+3x^7+x^6+1$
10	$x^{13}+x^9+x^8+2x^7+2x^6+1$
11	$x^{13}+x^9+x^8+2x^7+2x^6+1$
12	$x^{13}+2x^8+3x^7+x^6+1$
13	$x^{13}+x^9+x^8+2x^7+2x^6+1$
14	$x^{13}+x^9+x^8+2x^7+2x^6+1$

$P = \{1\ ,\{\ \alpha\ ,\alpha^2,\ \alpha^4,\alpha^8\ ,\ \alpha^3\ ,\alpha^6\ ,\alpha^{12}\ ,\alpha^9\ \}\ ,\{\alpha^5\ ,\alpha^{10}\ ,\alpha^7\ ,\alpha^{14}\ ,\alpha^{13}\ ,\alpha^{11}\ \}\}$

şeklinde P parçalanışı elde edilir. Dikkat edilirse

$\{\alpha^5, \alpha^{10}, \alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\} = \{\alpha^5, \alpha^{10}\} \cup \{\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}\}$

$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^3, \alpha^6, \alpha^{12}, \alpha^9\} = \{\alpha, \alpha^2, \alpha^4, \alpha^8\} \cup \{\alpha^3, \alpha^6, \alpha^{12}, \alpha^9\}$

yazılabileceğinden üreteç polinomun F_2 cismi üzerinde tanımlandığı varsayımında bulunulabilir. Gerçekten de $g(x) = x^3 + x + 1$ olduğundan g üreteç polinomu F_2 cismi üzerinde tanımlanmıştır.

Tanım 3.2. [4] $\Gamma(L, g)$ Goppa kodunun, supportu $\mathcal{P}_L$ parçalanışının sınıflarının birleşiminden oluşan kodsözlerinin oluşturduğu alt koduna, idempotent alt kodu denir ve $I(L, g)$ ile gösterilir.

Önerme 3.2. $\forall \sigma \in Aut_{I(L,g)}$ ve $\forall x \in I(L, g)$ için $\sigma(x) = x$ yazılabilir.

İspat. $des(x)$(x'in desteği) kümesi $\mathcal{P}_L$ parçalanışının sınıflarının birleşiminden oluştuğundan ve her bir sınıf σ permütasyonu altında değişmez olduğundan bunların her hangi bir birleşimi de σ permütasyonu altında değişmez. Dolayısıyla

$des(\sigma(x)) = des(x)$

yazılabileceğinden ve F_2 de supportu aynı olan iki vektör eşit olacağından

$\sigma(x) = x$

yazılabilir.

Önerme 3.3. Denk C ve C' kodları verilmiş olsun. Buna göre $C' = \pi(C)$, $P = SSA(C)$ ve $P' = \pi(P)$ olmak üzere, C kodunun, desteği P parçalanışının sınıflarının birleşiminden oluşan tüm kod sözlerinin oluşturduğu alt kodu ${}_PC$ ile gösterilirse $\pi({}_PC) = {}_{P'}C'$ yazılabilir. Ayrıca F_2 cismi üzerinde tanımlı n uzunluğundaki tüm vektörlerin kümesi F_2^n ile gösterilirse ${}_PC = {}_P(F_2^n) \cap C$ yazılabilir.

İspat . C ve C' kodlarının kod sözlerini alt alta yazarak elde edilen mxn boyutlu matrisleri sırası ile M ve M' ile ve ${}_PC$ ve $\pi({}_PC)$ kodlarının kod sözlerini alt alta yazılmasıyla elde edilen mxn boyutlu matrisler sırası ile ${}_PM$ ve M'' şeklinde gösterilsin. Buna göre ${}_PM$ matrisinin i-inci satır vektörü α'_{ij} ile ve M'' matrisinin i-inci satır vektörü ise β'_i şeklinde gösterilirse

$$\beta'_i = \pi(\alpha'_{ij}) = \alpha'_{i\pi(j)}$$

yazılabilir. Burada her i değeri için, j ler P parçalanışının sınıflarının bir birleşimini oluşturacağından $\pi(j)$ değerleri de $\pi(P)$ parçalanışının sınıflarının bir birleşimini oluşturur. Dolayısıyla M'' ve ${}_P{}'M'$ matrislerinin boyutları aynı olduğundan

$$M'' = {}_P{}'M' \Longrightarrow \pi({}_PC) = {}_P{}'C'$$

elde edilir. Ayrıca ${}_PC$ alt kodunun tanımından

$${}_PC = {}_P(F_2^n) \cap C$$

yazılabileceği açıktır.

Sonuç 3.1. [4] $\Gamma(L,g)\sim C$ ise $I(L,g)\sim {}_PC$ yazılabilir.

İspat) $\Gamma(L,g)\sim C$ ise $\pi\big(\Gamma(L,g)\big) = C$ ve $\pi(\mathcal{P}_L) = P$ olmak üzere

$${}_PC = {}_P(F_2^n) \cap C = {}_{\pi(\mathcal{P}_L)}\pi(F_2^n) \cap \pi\big(\Gamma(L,g)\big) = \pi\left({}_{\mathcal{P}_L}(F_2^n) \cap \Gamma(L,g)\right)$$

$$= \pi(I(L,g)).$$

BÖLÜM 4. ALTERNATİF METOT

F_2 cismi üzerinde n uzunluğunda ve m tane kod sözden oluşan bir C kodu verildiğinde kod sözleri alt alta yazarsak mxn boyutlu bir M matrisi elde ederiz. M matrisinin satır vektörlerini $\alpha_i', (1 \leq i \leq m)$ şeklinde ve sütun vektörlerini de $\alpha_j (1 \leq j \leq n)$ şeklinde gösterelim. Şimdi V ve V' kümeleri sırası ile $I_m = \{1,2,\dots,m\}$ ve $I_n = \{1,2,\dots,n\}$ indis kümelerinin herhangi alt kümeleri olmak üzere, satır ve sütun vektörleri ile V ve V' kümeleri üzerinde bir d fonksiyonu tanımlayıp buna göre I_m ve I_n kümelerinin bir parçalanışını elde edelim.

Tanım 4.1.[15] $d(\alpha_i', V) =$ "α_i' vektörünün V kümesi tarafından indislenen koordinatlarındaki 1' lerin sayısıdır" .

Tanım 4.2.[15] $d(\alpha_j, V') =$ "α_j vektöründe V' kümesi tarafından indislenen koordinatlarındaki 1' lerin sayısıdır".

Tanım 4.3.[15] I_n kümesinin bir parçalanışı $\{V_1, V_2, \dots, V_{N'}\}$ olsun. Buna göre $\forall i_{p_1}, i_{p_2} \in I_m$ aynı sınıftadır ancak ve ancak $d\left(\alpha'_{i_{p_1}}, V_{r'}\right) = d\left(\alpha'_{i_{p_2}}, V_{r'}\right), \forall r,$ $1 \leq r' \leq N'$ dır .

Tanım 4.4.[15] I_m kümesinin bir parçalanışı $\{V_1', V_2', \dots, V_N'\}$ olsun. Buna göre $\forall j_{p_1}, j_{p_2} \in I_n$ aynı sınıftadır ancak ve ancak $d\left(\alpha_{j_{p_1}}, V_r'\right) = d\left(\alpha_{j_{p_2}}, V_r'\right), \forall r, 1 \leq r \leq N$ dır .

Tanım 4.2' ye göre I_m kümesinin bir parçalanışını elde ederiz. Çünkü bu tanıma göre her eleman bir sınıfa aittir ve farklı iki sınıf ortak eleman içermez. Benzer şekilde Tanım 4.3' e göre de I_n kümesinin bir parçalanışını elde ederiz. Dolayısıyla aşağıdaki önermeyi yazabiliriz.

Önerme 4.1. I_m kümesinin bir parçalanışı $\{V_1', V_2', \dots, V_N'\}$ olsun. Buna göre $\forall \alpha_j, 1 \leq j \leq n$ vektörleri için

$$\sum_{r=1}^{N} d(\alpha_j, V_r') = w(\alpha_j)$$

yazılabilir. Benzer şekilde I_n kümesinin bir parçalanışı $\{V_1, V_2, \dots, V_{N\prime}\}$ olsun. Buna göre $\forall \alpha'_i, 1 \leq i \leq m$ vektörleri için

$$\sum_{r\prime=1}^{N\prime} d(\alpha_i', V_{r\prime}) = w(\alpha_i')$$

yazılabilir.

Sonuç 4.1. I_n nin bir parçalanışı $\pi_k^{Sn} = \left\{V_1, V_2, \dots, V_{t_k'}\right\}$ olmak üzere Tanım 4.2. den I_m nin bir

$$\pi_{k+1}^{Sr} = \{V_1', V_2', \dots, V_{t_{k+1}'}'\}$$

parçalanışını ve benzer şekilde Tanım 4.3' den π_{k+1}^{Sr} ye göre I_n nin bir

$$\pi_{k+1}^{Sn} = \{V_1, V_2, \dots, V_{t_{k+1}'}\}$$

parçalanışını elde edebiliriz. Buna göre başlangıç değeri,

$$\pi_0^{Sn} = \{V_1\}, V_1 = [1,2, \dots, n]$$

olarak seçilirse Önerme 4.1. den dolayı, eğer i ve j elemanları başlangıçta farklı sınıflarda iseler daha sonra ki adımlarda da farklı sınıflarda olacaklarından

$\pi_{N+1}^{Sr} = \pi_N^{Sr}$ veya $\pi_{N+1}^{Sn} = \pi_N^{Sn}$

şartını sağlayan bir N sayısı bulunacaktır. Sonuç olarak verilen C koduna karşılık sırasıyla $I_m = \{1,2,\dots,m\}$ ve $I_n = \{1,2,\dots,n\}$ kümelerinin parçalanışlarından oluşan bir

$\pi_C = (\pi_C^{Sr}, \pi_C^{Sn})$; $\pi_C^{Sr} = \pi_N^{Sr}$, $\pi_C^{Sn} = \pi_N^{Sn}$

parçalanışı elde edilmiş olur.

Önerme 4.2. C koduna bir $\sigma \in S_n$ permütasyonu uygulanarak C' kodunun elde edildiğini kabul edelim. Bu durumda $\pi_C = (\pi_C^{Sr}, \pi_C^{Sn})$ ve $\pi_{C'} = (\pi_{C'}^{Sr}, \pi_{C'}^{Sn})$ olmak üzere

$\pi_C^{Sr} = \pi_{C'}^{Sr}$ ve $\pi_C^{Sn} = \sigma(\pi_{C'}^{Sn})$

yazılabilir.

İspat. $(\pi_0^{Sn})_{C'} = (W_1)$, $W_1 = [1,2,\dots,n]$, $(\pi_0^{Sn})_C = (V_1)$, $V_1 = \sigma(W_1)$ olmak üzere $\forall i \in I_m, \forall j \in I_n$ elemanları için

$\beta'_{ij} = \alpha'_{i\sigma(j)}$

yazılabilir. Buna göre

$d(\beta'_i, W_1) = d\big(\alpha'_i, \sigma(W_1)\big) = d(\alpha'_i, V_1)$

yazılabileceğinden

$(\pi_1^{Sr})_C = (\pi_1^{Sr})_{C'}$

elde edilir. Dolayısıyla $\forall V'_r \in (\pi_1^{Sr})_C$ ve $\forall W'_r \in (\pi_1^{Sr})_{C'}$ parçalanışları için

$V_r' = W_r'$

yazılabilir. $\forall j \in I_n$ elemanı için $\beta_j = \alpha_{\sigma(j)}$ yazılabileceğinden bu sonuca göre

$d(\beta_j, W_r') = d(\alpha_{\sigma(j)}, V_r')$

elde edilir. Dolayısıyla

$(\pi_1^{Sn})_C = \sigma[(\pi_1^{Sn})_{C'}]$

yazılabileceğinden $\forall V_{r'} \in (\pi_1^{Sn})_C$ ve $\forall W_{r'} \in (\pi_1^{Sn})_{C'}$ parçalanışları için

$V_{r'} = \sigma(W_{r'})$

elde edilir. O halde $n = 1$ için hipotezimiz doğrudur.

Şimdi $n = k$ için hipotezin doğru olduğu kabul edilsin. Buna göre

$(\pi_k^{Sn})_C = \sigma[(\pi_k^{Sn})_{C'}]$

olmak üzere $\forall V_{r'} \in (\pi_k^{Sn})_C$, $\forall W_{r'} \in (\pi_k^{Sn})_{C'}$ parçalanışları için

$V_{r'} = \sigma(W_{r'})$

yazılabilir. Dolayısıyla $\forall i \in I_m$ için

$d(\beta_i', W_{r'}) = d(\alpha_i', \sigma(W_{r'})) = d(\alpha_i', V_{r'})$

yazılabileceğinden

$(\pi_{k+1}^{Sr})_C = (\pi_{k+1}^{Sr})_{C'}$

elde edilir. Sonuç olarak $\forall V_r' \in (\pi_{k+1}^{Sr})_C$, $\forall W_r' \in (\pi_{k+1}^{Sr})_{C'}$ parçalanışları için

$V_r' = W_r'$

yazılabilir. Buna göre

$d(\beta_j, W_r') = d(\alpha_{\sigma(j)}, V_r'))$

yazılabileceğinden

$(\pi_{k+1}^{Sn})_C = \sigma[(\pi_{k+1}^{Sn})_{C'}]$

elde edilir. Dolayısıyla $\forall V_{r'} \in (\pi_{k+1}^{Sn})_C$, $\forall W_{r'} \in (\pi_{k+1}^{Sn})_{C'}$ parçalanışları için

$V_{r'} = \sigma(W_{r'})$

yazılabileceğinden istenen elde edilir.

Şimdi $\pi^{Sr} = \{V_1, V_2, \dots, V_{N'}\}$ ve $\pi^{Sn} = \{V_1', V_2', \dots, V_N'\}$ parçalanışları üzerinde bir sıralama tanımlayalım.

Tanım 4.5. [15] $\forall V_{r_1'}$, $V_{r_2'} \in \pi^{Sr}$ elemanları için;

$V_{r_1'} < V_{r_2'} \Leftrightarrow \forall j_1 \in V_{r_1'}$, $\forall j_2 \in V_{r_2'}$, $d(\alpha_{j_1}, V_r') \neq d(\alpha_{j_2}, V_r')$

koşulunu sağlayan en küçük $1 \leq r \leq N$ sayısı için

$d(\alpha_{j_1}, V_r') < d(\alpha_{j_2}, V_r')$

şartı sağlanır.

Tanım 4.6.[15] $\forall V'_{r_1}$, $V'_{r_2} \in \pi^{Sn}$ elemanları için;

$V'_{r_1} < V'_{r_2} \Leftrightarrow \forall i_1 \in V'_{r_1}$, $\forall i_2 \in V'_{r_2}$, $d(\alpha'_{i_1}, V_{r'}) \neq d(\alpha'_{i_2}, V_{r'})$

koşulunu sağlayan en küçük $1 \leq r' \leq N'$ sayısı için

$d(\alpha'_{i_1}, V_{r'}) < d(\alpha'_{i_2}, V_{r'})$

şartı sağlanır.

Sonuç 4.2. Önerme 4.2. ye göre, denk C ve C' kodları verildiğinde $\forall V_{r_1}, V_{r_2} \in \pi_C^{Sn}$ parçalanışları için eğer

$V_{r_1} < V_{r_2}$

ise $\forall j'_1 \in W_{r_1}$, $\forall j'_2 \in W_{r_2}$ elemanları için

$j_1 = \sigma(j'_1) \in V_{r_1}$ ve $j_2 = \sigma(j'_2) \in V_{r_2}$

olmak üzere

$$d(\beta_{j'_1}, W'_r) = d\left(\alpha_{\sigma(j'_1)}, V'_r\right) = d(\alpha_{j_1}, V'_r) < d(\alpha_{j_2}, V'_r) = d\left(\alpha_{\sigma(j'_2)}, W'_r\right)$$

$$= d(\beta_{j'_2}, W'_r) \Longrightarrow W_{r_1} < W_{r_2}$$

yazılabileceğinden parçalanışlar üzerinde tanımladığımız sıralamanın permütasyon altında korunduğunu söyleyebiliriz.

Sonuç 4.3. C ve C' gibi iki kod verildiğinde π_C^{Sr} ve $\pi_{C'}^{Sr}$ parçalanışlarının aynı olup olmadığına bakılarak bu iki kodun denk olup olmadıkları hakkında tahminde bulunulabilir. Eğer bu iki kod denk ise π_C^{Sn} ve $\pi_{C'}^{Sn}$ parçalanışları kullanılarak M ve M' matrislerinin sütun vektörleri karşılaştırılırsa aradaki permütasyon bulunabilir. Şimdi bunu bir örnekle açıklayalım.

Örnek 4.1 $C = \{100110, 010110, 011001, 101010, 011001, 001011\}$ şeklinde bir C kodu verilmiş olsun. Buna göre kod sözleri alt alta yazarsak aşağıdaki M matrisini elde ederiz.

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

M matrisine algoritmayı uygularsak;

$\boldsymbol{k = 0}$:

$\pi_0^{Sn} = ([1,2,3,4,5,6])$

$\boldsymbol{k = 1}$:

$d(*, V_1) = 3,3,3,3,3,3 \quad \Longrightarrow \quad \pi_1^{Sr} = ([1,2,3,4,5,6])$

$d(*, V_1') = 2,3,4,2,4,3 \quad \Longrightarrow \quad \pi_1^{Sn} = ([1,4],[2,6],[3,5])$

$\boldsymbol{k = 2}$:

$d(*, V_1) = 2,1,0,1,0,0$

$d(*, V_2) = 0,1,2,0,2,1 \quad \Longrightarrow \quad \pi_2^{Sr} = ([6],[3,5],[4],[2],[1])$

$d(*, V_3) = 1,1,1,2,1,2$

$d(*, V_1') = 0,0,1,0,1,1$

$d(*, V_2') = 0,2,2,0,0,2$

$d(*, V_3') = 1,0,1,0,1,0 \quad \Longrightarrow \quad \pi_2^{Sn} = ([4],[1],[2],[5],[6],[3])$

$d(*, V_4') = 0,1,0,1,1,0$

$d(*, V_5') = 1,0,0,1,1,0$

$\Longrightarrow \pi_C^{Sr} = ([6],[3,5],[4],[2],[1]) \quad , \quad \pi_C^{Sn} = ([4],[1],[2],[5],[6],[3])$

olarak bulunur. Burada $d(*, V_j)$ veya $d(*, V_i')$ ifadelerinde "*" ile tüm sütun veya satır vektörleri ifade edilmektedir. $C' = \{010011, 011001, 101100, 110010, 101100, 110100\}$ şeklinde C' kodu verilmiş olsun. Buna göre kod sözleri alt alta yazarsak aşağıdaki M' matrisini elde ederiz.

$$M' = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

M' matrisine algoritmayı uygularsak;

$\boldsymbol{k = 0}$:

$\pi_0^{Sn} = ([1,2,3,4,5,6])$

$\boldsymbol{k = 1}$:

$d(*, V_1) = 3,3,3,3,3,3 \quad \Longrightarrow \quad \pi_1^{Sr} = ([1,2,3,4,5,6])$

$d(*, V_1') = 4,4,3,3,2,2 \quad \Longrightarrow \quad \pi_1^{Sn} = ([5,6],[3,4],[1,2])$

$\boldsymbol{k = 2}$:

$d(*, V_1) = 2,1,0,1,0,0$

$d(*, V_2) = 0,1,2,0,2,1 \implies \pi_2^{Sr} = ([6],[3,5],[4],[2],[1])$

$d(*, V_3) = 1,1,1,2,1,2$

$d(*, V_1') = 1,1,0,1,0,0$

$d(*, V_2') = 2,0,2,2,0,0$

$d(*, V_3') = 1,1,0,0,1,0 \implies \pi_2^{Sn} = ([6],[5],[3],[2],[4],[1])$

$d(*, V_4') = 0,1,1,0,0,1$

$d(*, V_5') = 0,1,0,0,1,1$

$\implies \pi_C^{Sr} = ([6],[3,5],[4],[2],[1]) \quad , \quad \pi_C^{Sn} = ([6],[5],[3],[2],[4],[1])$

yazılabilir. Dolayısıyla $k = 0,1,2$ için $(\pi_k^{Sr})_{C'} = (\pi_k^{Sr})_C$ yazılabileceğinden bu iki kodun denk olduğu tahmininde bulunabiliriz. Buna göre π_C^{Sn} ve $\pi_{C'}^{Sn}$ parçalanışları karşılaştırılırsa

$\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 2$, $\sigma(4) = 6$, $\sigma(5) = 1$, $\sigma(6) = 4$

yazılabileceğinden $\sigma = (1\ 3\ 2\ 5)(4\ 6)$ olarak σ permütasyonu bulunur.

BÖLÜM 5. SONUÇLAR VE ÖNERİLER

C ve C' gibi iki kod verildiğinde sırasıyla bu kodlara karşılık gelen M ve M' matrisleri bulunup 4. Bölümde anlatılan algoritma uygulanırsa, $\pi_C = (\pi_C^{Sr}, \pi_C^{Sn})$ ve $\pi_{C'} = (\pi_{C'}^{Sr}, \pi_{C'}^{Sn})$ olmak üzere $\pi_{C'}^{Sr} = \pi_C^{Sr}$ eşitliğinin sağlanıp sağlanmadığına bakılarak verilen kodların denk olup olmadığı hakkında yorumda bulunulabilir. Eğer verilen kodlar denk ise $\pi_{C'}^{Sn}$ ve π_C^{Sn} parçalanışları karşılaştırılarak bu kodlar arasındaki permütasyon bulunabilir.

KAYNAKLAR

[1] http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-451-principles-of-digital-communication-ii-spring-2005/lecture-notes/chap7.pdf, Erişim Tarihi: 23.01.2013.

[2] F. J. MACWİLLİAMS AND N. J. A. SLAONE, The Theory of Error-Correcting Codes, North-Holland, 1977.

[3] MINKING EIE, A Course on Abstract Algebra, World Scientific Publishing Company, 2010.

[4] N.SENDRIER, Weak keys in the McEliece public-key cryptosystem, IEEE Transactions on Information Theory, 47(3):1207-1211, 2001.

[5] E. PETRANK AND R. M. ROTH, Is code equivalance easy to decide? IEEE Transactions on Information Theory, 43(5):1602-1604, 1997.

[6] R. J. MCELIECE, A public-key cryptosystem based on algebraic coding theory, The Deep Space Network Progress Report, 42-44:114-116, 1978.

[7] V. M. SİDEL'NİKOV AND S. O. SHESTAKOV, On cryptosystem based on generalized Red-Solomon codes, Discrete mathematics (in russian), 4(3):57-63, 1992.

[8] http://indocrypt09.inria.fr/goppa.pdf, Erişim Tarihi: 16.02.2013.

[9] N. J. PATTERSON, The algebraic decoding of Goppa codes, IEEE Transactions on Information Theory, 21: 203-307, 1975.

[10] TOOD K. MOON, Error Correction Coding: Mathematical Methods and Algorithms, Wiley, 2005

[11] N. SENDRİER, Finding the permutation between equivalent codes: the support splitting algorithm, IEEE Transactions on Information Theory, 46(4):1193-1203, 2000.

[12] E. R. BERLEKAMP, R. J. MCELIECE, AND H. C. VAN TILBORG, On the inherent interactability of certain coding problems, IEEE Transactions on Information Theory, 24(3), 1978.

[13] E. F. ASSMUS, JR AND J. D. KEY, Affine and projective planes. Discrete Mathematics, 83:161-187, 1990.

[14] JAMES E. GENTLE, Matrix Algebra: Theory, Computations and Applications in Statistics, Springer, 2007.

[15] I.G. BOUYUKLİEV, About the Code Equivalance, World Scientific Series on Coding Theory and Cryptology, 3:126-151, 2007.

ÖZGEÇMİŞ

Ekrem EMRE, Kütahya' da doğdu. İlkokul, ortaokul ve lise eğitimini Tavşanlı'da tamamladı. 2006 yılında Dumlupınar Üniversitesi Matematik bölümünü bitirdi. 2010 yılında Sakarya Üniversitesi Matematik Bölümü Cebir ve Sayılar Teorisi Anabilim Dalında Yüksek Lisans Programına başladı.