KODLAMA TEORİSİNİN
KRİPTOGRAFİK AÇIDAN İNCELENMESİ

Derya ARDA

DOKTORA TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
Tez Yöneticisi: Yrd. Doç. Dr. Ercan BULUŞ

EDİRNE - 2011

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KODLAMA TEORİSİNİN KRİPTOGRAFİK AÇIDAN İNCELENMESİ

Derya ARDA

DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Yöneticisi : Yrd. Doç. Dr. Ercan BULUŞ

EDİRNE – 2011

T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KODLAMA TEORİSİNİN KRİPTOGRAFİK AÇIDAN İNCELENMESİ

Derya ARDA

DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Bu tez . 05 / 09 /2011. tarihinde aşağıdaki jüri tarafından kabul edilmiştir.

. . . . . .
Yrd. Doç. Dr. Ercan BULUŞ
Tez Yöneticisi

. . . . . .
Doç. Dr. Selim KARA
Üye

. . . . . .
Yrd. Doç. Dr. M. Tolga SAKALLI
Üye

. . . . . .
Yrd. Doç. Dr. Tarık YERLİKAYA
Üye

. . . . . .
Yrd. Doç. Dr. Erdinç UZUN
Üye

Doktora Tezi

Trakya Üniversitesi Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Bölümü

ÖZET

İletişim sistemlerinin günlük hayatımızın vazgeçilmez parçaları haline gelmesiyle hızlı, hatasız ve güvenli sayısal bilgi iletimi gerekliliği önemli bir konu olarak karşımıza çıkmaktadır. Kodlama teorisi, iletişim alanında kaynakların, kanalların, alıcıların bilgi karakteristiklerini incelemek, bilginin iletimini optimize etmek ve iletimin güvenilirliğini sağlamak amacıyla kullanılmaktadır. Kriptografi ise bilgi güvenliğini inceleyen bir bilim dalıdır. Kriptografi' nin amacı iki ya da daha fazla kişinin haberleşmesinde gizlilik, veri bütünlüğü, doğrulama ve inkar edememe esaslarını birleştirerek mesajın güvenli iletişimini sağlamaktır.

Kriptografi sadece bilgi saklaması ve aktarması problemine güvenli bir çözüm aramaktan ibaret değildir. Kriptosistemlerde kullanılan anahtarın güvenli bir şekilde saklanması gerekmektedir. Böyle bir probleme çözüm olarak birçok Gizlilik Paylaşım Şemaları önerilmiştir. Gizlilik Paylaşım Şeması kriptografik anahtar yönetimi ve anahtar dağıtımı ile ilişkili önemli bir kavramdır.

Bu tezde ilk önce Kodlama teorisi ve Kriptografide kullanılan matematiksel tanımlar, teoremler ve bu bilimler ile ilgili genel bilgiler verilmiştir. Daha sonra Gizlilik Paylaşım Şemaları incelenmiş ve özellikle kodlama teorisinde Reed-Solomon(RS) Kodlarla ilişkilendirilmiş Gizlilik Paylaşım Şemaları üzerinde durulmuş ve uygulamaları gerçekleştirilmiştir. İlk olarak Shamir'in Lagrange İnterpolasyon tabanlı Gizlilik Paylaşım Şeması incelenmiş ve uygulaması yapılmıştır. Daha sonra GF(q) ve GF(2^n) sonlu cisim uzaylarında tanımlanan ve

kodlama teorisinde hata düzeltme kapasitesi en fazla olan MDS(Maximum Distance Separable) kod tabanlı Gizlilik Paylaşım Şemalarının uygulamaları gerçekleştirilmiştir. Burada Reed-Solomon kodlar özel MDS kodlardır.

En son olarak RS kodların hata düzeltme algoritmalarından faydalanılarak, üretilen MDS kod tabanlı Gizlilik Paylaşım Şemalarında hileli katılımcılar olması durumunda bu katılımcıların yanlış verilerinin düzeltilerek gizliliğin yeniden elde edilebildiği gösterilmiştir. Bir (n, k, d) MDS kod, minimum Hamming mesafesi d=n-k+1 en fazla olan kodlar olduğu için en çok hileli katılımcıları tespit edip verileri düzeltme yeteneğine sahiptir.

Anahtar Kelimeler: Kodlama Teorisi, Kriptografi, Gizlilik Paylaşım Şemaları, Reed-Solomon Kodlar, MDS kodlar, Hilekar Tespit etme ve Kimliklendirme

Yıl: 2011

Sayfa: 165

Doctorate Thesis

Trakya University Graduate School of
Natural and Applied Sciences
Department of Computer Engineering

ABSTRACT

Fast, correct and secure transmission of digital information have become more important issue nowadays since communication systems are crucial for daily life. Coding theory is used to examine the characteristics of information sent through communication channel which cover the source, the channel and the receiver. Also, it is used to optimize the transmission of the information and provide secure transmission. On the other hand, cryptography is the science of information security and aims to provide secure communication by combining the following four objectives: confidentiality, integrity, authentication and non-repudiation.

Cryptography does not only deal with the securely storing and transferring sensitive information, but the keys used in cryptosystems should also be kept securely. Therefore, in the literature, there are many proposals of secret sharing schemes. A secret sharing scheme is an important concept related with cryptographic key management and distribution.

In this thesis, firstly, some mathematical background, definitions and theorems related with coding theory and cryptography are given. Then, secret sharing schemes, secret sharing schemes associated with Reed-Solomon Codes are examined and applications of them are developed. From secret sharing schemes, Shamir's Lagrange Interpolation based secret sharing schemes is examined and an application of it is developed. Then, MDS (Maximum Distance Separable) code,

which is defined over GF(q) and GF(2^n) and are those with the greatest error correcting capability, based secret sharing scheme applications are developed. Here, Reed-Solomon Codes are special MDS codes.

At last, if MDS code based secret sharing schemes include cheating participants, it is shown that the secret can be obtained correctly by taking the benefit of error correcting algorithms of RS codes and correcting the wrong data of them. An (n, k, d) MDS code has the ability of indentifying the most number of cheating participants and correcting the wrong data of them since the minimum Hamming distance d=n-k+1 is maximal for these codes.

.

Key Words: Coding Theory, Cryptography, Secret Sharing Schemes, Reed Solomon Codes, MDS Codes, Cheater Detection and Identification

TEŞEKKÜR

Bu tez çalışmasının her aşamasında beni düşünceleri ile yönlendiren ve bilgilerinden faydalandığım Tez yöneticisi hocam Yrd. Doç. Dr. Ercan BULUŞ' a teşekkür ederim.

Tez çalışmam süresince tez izleme komitemde bulunan ve bana olumlu düşünceleri ile destek olan hocalarım Doç. Dr. Selim KARA ve Yrd. Doç. Dr. M. Tolga SAKALLI' ya teşekkür ederim.

Ayrıca tez çalışmam esnasında yardımlarını esirgemeyen arkadaşlarım Yrd. Doç. Dr. Altan MESUT, Yrd. Doç. Dr. Andaç MESUT, Yrd. Doç. Dr. Tarık YERLİKAYA, Arş. Gör. Fatma BÜYÜKSARAÇOĞLU SAKALLI ve Öğr. Gör. Bora ASLAN'a teşekkür ederim.

Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü tüm çalışma arkadaşlarıma tez boyunca verdikleri moral desteği ve yardımlarından ötürü teşekkür ederim.

Tez çalışmam süresince bana sürekli destek olan ve motive eden sevgili eşim Doç. Dr. Ertan ARDA' ya ve manevi desteği için biricik kızım Doğa'ya teşekkür ederim.

Her zaman desteklerini üzerimde hissettiğim sevgili annem, babam ve abim'e sonsuz teşekkürlerimi sunarım.

Eylül 2011 Derya ARDA

İÇİNDEKİLER

ÖZET ..... **i**
ABSTRACT ..... **iii**
TEŞEKKÜR ..... **v**
İÇİNDEKİLER ..... **vi**
ŞEKİLLER LİSTESİ ..... **xi**
TABLOLAR LİSTESİ ..... **xii**
GİRİŞ **1**
BÖLÜM 1 ..... **5**
1. MATEMATİKSEL ALT YAPI **5**
1.1. Cebirsel Yapılar 5
1.1.1. Yarı Gruplar 5
1.1.2. Grup 6
1.1.3. Halka 6
1.1.4. Cisim 7
1.2. Sonlu Cisim 8
1.2.1. Galois Cisimleri 8
1.2.3. Sonlu Cisim Üzerinde Matematiksel İşlemler 10
1.3. Sayılar Teorisi 16
1.3.1.Bölünebilirlik 16
1.3.2. Bölünebilirlik Özellikleri 16
1.3.3. Tamsayılar için Bölüm Algoritması 17
1.3.4. En Büyük Ortak Bölen(Greatest Common Divisor-GCD) 17
1.3.5. Asal Sayı 18
1.3.6. Aritmetiğin Esas Teoremi 19
1.3.7. Euler Fi (ϕ) Fonksiyonu (Euler Phi Function) 19
1.3.8. Öklid Algoritması (Euclidean Algorithm) 20
1.3.9. Genişletilmiş Öklid Algoritması (Extended Euclidean Algorithm) 21

1.3.10. Aritmetik Tersi 24
1.3.11 Denklik Teorisi (Theory of Congruence (Modularity)) 26
1.3.12. Çin Kalan Teoremi (Chinese Remainder Theorem) 26
BÖLÜM 2 28
2. KRİPTOLOJİ 28
2.1. Kriptolojinin Temelleri 28
2.2. Bilgi Güvenliği Kavramları 29
2.3. Kriptografik Algoritmalar 30
2.3.1.Simetrik Şifreleme Algoritmaları 31
2.3.2. Asimetrik Şifreleme Algoritmaları 32
2.4. Anahtar Yönetimi 33
2.5. Kriptografik Protokoller 35
BÖLÜM 3 36
3. KODLAMA TEORİSİ 36
3.1. Giriş 36
3.2. Sonlu cisim üzerinde vektör uzayı 40
3.3. Kodlama Teorisindeki Temel Kavramlar 43
3.4. Lineer Kodlar 46
3.5. Lineer Kodların Dekodlaması 50
BÖLÜM 4 53
4. GİZLİLİK PAYLAŞIM ŞEMALARI 53
4.1 Giriş 53
4.2. Gizlilik Paylaşım Şeması 54
4.3. Shamir'in Lagrange İnterpolasyon Polinom Tabanlı Gizlilik Paylaşım Şeması 56
4.4.Çin Kalan Teoremi Tabanlı Eşik Gizlilik Paylaşım Şemaları 59
4.4.1. Asmuth-Bloom Gizlilik Paylaşım Şeması 59
4.5. Hata Doğrulama Kodları ve Gizlilik Paylaşımı 63
4.5.1.Erişim Yapıları 64
BÖLÜM 5 65
5. REED-SOLOMON KODLAR 65
5.1. Reed Solomon Kodlarının Tanımı 65

5.2. Kodlama 66
5.3. Kod Çözme 67
5.3.1. Hata Belirteci Hesabı 68
5.3.2. Hata Yeri Polinomunu Tespit Etmek İçin Kullanılan Yöntemler 71
5.3.2.1. Reed Solomon Kodların Sendrom Dekodlaması 71
5.3.2.2 RS Kodların Öklid Algoritması Kullanarak Çözülmesi 74
5.4. Chien Araştırması 77
5.5. Forney Algoritması 77
BÖLÜM 6 78
6. MDS KODLAR 78
6.1.MDS Kodların Özellikleri 79
6.2. MDS Kod Tabanlı Gizlilik Paylaşım Şeması 80
BÖLÜM 7 83
7. LAGRANGE İNTERPOLASYON TABANLI GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI 83
8. GF(q) ASAL CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI 88
8.1.GF(7) Asal Cisminde üretilen (6, 3, 4) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması 88
8.1.1. (6, 3, 4)= (n, k, d) kodunun üreteç matrisinin elde edilmesi 88
8.1.2. (n, k, d)=(6, 3, 4) MDS Kodu ile (k, n-1)=(3, 5) eşik Gizlilik Paylaşım Şeması Oluşturulması 90
8.2. GF(11) Asal Cisminde üretilen (10, 6, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması 91
8.2.1 (10, 6, 5)=(n, k, d) kodunun üreteç matrisinin elde edilmesi 91
8.2.2. (n, k ,d)=(10, 6, 5) MDS Kodu ile (k, n-1)=(6, 9) eşik Gizlilik Paylaşım Şeması Oluşturulması 92
8.3.GF(13) Asal Cisminde üretilen (12, 8, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması 94
8.3.1 (12, 8, 5)=(n, k, d) kodunun üreteç matrisinin elde edilmesi 94
8.3.2. (n, k, d)=(12, 8, 5) MDS Kodu ile (k, n-1)=(8, 11) eşik Gizlilik Paylaşım Şeması Oluşturulması 94

BÖLÜM 9.....96
9. GF(2^n) SONLU CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI.....96
9.1. $GF(2^3)$ Sonlu Cisim uzayında (7, 3, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması.....96
9.2. GF(2^4) Sonlu Cisim uzayında üretilen (8, 4, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması.....103
9.3. GF(2^4) Sonlu Cisim uzayında üretilen (11, 5, 7) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması.....106
9.4. GF(2^4) Sonlu Cisim uzayında üretilen (15, 5, 11) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması.....109
9.5. GF(2^8) Sonlu Cisim uzayında üretilen (16, 8, 9) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması.....112
BÖLÜM 10.....119
10. GF(2^n) SONLU CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE OLUŞTURULAN GİZLİLİK PAYLAŞIM ŞEMASINDA HİLELİ KATILIMCILARI TESPİT ETMEK VE KİMLİKLENDİRMEK.....119
10.1. Hilekar Problemi.....119
10.2. GF(2^3) Sonlu Cisim Uzayında (7, 3, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Sendrom Dekodlama Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirmek.....120
10.3. GF(2^3) Sonlu Cisim Uzayında (7, 3, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirmek Uygulaması.....123
10.4. GF(2^4) Sonlu Cisimde Üretilen (8, 4, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirme Uygulaması.....125
10.5. GF(2^4) Sonlu Cisimde Üretilen (11, 5, 7) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirme Uygulaması.....131
11. SONUÇLAR VE DEĞERLENDİRME.....136
TEZ SÜRESİNCE YAPILAN ÇALIŞMALAR.....137

KAYNAKLAR.....139
ÖZGEÇMİŞ.....149

ŞEKİLLER LİSTESİ

Şekil 2.1. Şifreleme Yöntemleri

Şekil 2.2. Simetrik Şifreleme Algoritması Genel Yapısı

Şekil 2.3. Asimetrik Şifreleme Algoritması Genel Yapısı

Şekil 3.1. Kodlama Türleri

Şekil.3.2. Basit bir haberleşme sistemi

Şekil 4.1 Gizlilik Paylaşım tabanlı haberleşme şeması

Şekil 5.1. Reed-Solomon kod çözme diyagramı

TABLOLAR LİSTESİ

Tablo 1.1. GF(7) Cismi Üzerinde Toplama Ve Çarpma İşlemleri 9
Tablo 1.2. GF(2^4)' de elemanların tersi ve polinomsal gösterimi 12
Tablo 1.3. $GF(2^4)$ 'ün elemanlarının farklı gösterilişleri.....14
Tablo 1.4. GF(2^4)'ün elemanlarının minimal polinomları 15
Tablo 5.1. Anahtar denklemini çözmek için Öklid algoritması 75
Tablo 7.1. (4,10) Eşik Şemanın Paylaşım Değerleri Gizliliğin Yeniden Elde Edilmesi 83
Tablo 7.2 (4,10) Eşik Şemanın k=4 eşik değer ile gizliliğin elde edilmesi.....84
Tablo 7.3. (8,20) Eşik Şemanın Paylaşım Değerleri.....85
Tablo 7.4 (8,20) Eşik Şemanın k = 8 eşik değer ile gizliliğin elde edilmesi.....85
Tablo 7.5. (5,15) Eşik Şemanın Paylaşım Değerleri.....86
Tablo 7.6 (5,15) Eşik Şemanın k=5 eşik değer ile gizliliğin elde edilmesi.....87
Tablo 8.1 GF(7) asal cisminde (6,3,4) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri 90
Tablo 8.2 GF(11) asal cisminde (10,6,5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri.....92
Tablo 8.3 GF(13) asal cisminde (12,8,5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri.....95
Tablo 9.1 GF(2^3) sonlu cisminde (7,3,5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri 98
Tablo 9.2 (7,3,5) MDS kod için Gizlilik Paylaşım Değerleri 101
Tablo 9.3. GF(2^4)'ün elemanlarının olası gösterimleri 103
Tablo 9.4.(8,4,5) MDS kod ile Gizlilik Paylaşım Şemasında Paylaşım Değerleri. 105
Tablo 9.5. GF(2^4)'de (11,5,7) MDS kodu ile oluşturulan (5,10) Eşik Gizlilik Paylaşım Şemasının paylaşım değerleri 108
Tablo 9.6. (k,n-1)=(5,10) Eşik Gizlilik Paylaşım Şemasında k=5 adet Katılımcı ile Gizliliği Elde Etme 109

Tablo 9.7. GF(2^4)'de (15,5,11) MDS kodu ile oluşturulan (5,14) Eşik Gizlilik Paylaşım Şemasının paylaşım değerleri 111
Tablo 9.8. (k,n-1)=(5,14) Eşik Gizlilik Paylaşım Şemasında k=5 adet Katılımcı ile Gizliliği Elde Etme 112
Tablo 9.9. GF(2^8)'de (16,8,9) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasında paylaşım değerleri 114
Tablo 9.10. (k,n-1)=(8,15) Eşik Gizlilik Paylaşım Şemasında k=8 adet Katılımcı ile Gizliliği Elde Etme 115
Tablo 9.11. $\beta = \alpha + 1$ üreteci ile $p(x)=x^8+x^4+x^3+x+1$ indirgenemez polinomuna göre GF(2^8) sonlu cisminin elemanlarının gösterimi 118
Tablo 10.1. (7,3,5) MDS kod için doğru Paylaşım Değerleri 124
Tablo 10.2. (7,3,5) MDS kod için Gizlilik Paylaşım Şemasında Hileli katılımcıların olması durumu 124
Tablo 10.3. (8,4,5) MDS kod için Paylaşım Değerleri 126
Tablo 10.4. (8,4,5) MDS kod için Gizlilik Paylaşım Şemasında Hileli katılımcıların olması durumu 126
Tablo 10.5. (8,4,5) MDS kod tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları tespit etmek için Öklid algoritması sonuçları 127
Tablo 10.6. GF(2^4)'de (11,5,7) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasında doğru paylaşım değerleri 132
Tablo 10.7. GF(2^4)'de (11,5,7) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasında hileli katılımcıların olması durumu 133
Tablo 10.8. Hileli katılımcıları bulmak için kullanılan Öklid algoritmasının sonuçları 134

GİRİŞ

Kodlama teorisi, birçok bilim dalı için önemli bir rol oynamaktadır. Bunlardan bazıları şöyle sıralanabilir: Matematik alanında istatistik biliminde, bilgisayar alanında şifreleme konusunda, haberleşme alanında, haberleşme karmaşıklığını en düşük seviyeye indirmek ve kaynakların etkin biçimde temsil edilmesini sağlamak için kullanılmaktadır. Kodlama, iletişim alanında kaynakların, kanalların, alıcıların bilgi karakteristiklerini incelemek, bilginin iletimini optimize etmek ve iletimin güvenilirliğini sağlamak amacıyla kullanılmaktadır.

İletişim sistemlerinin günlük hayatımızın vazgeçilmez parçaları haline gelmesiyle, hızlı ve hatasız sayısal bilgi iletimi gerekliliği de önemli bir konu olarak karşımıza çıkmaktadır. Haberleşme sistemlerinde bilginin iletimi için vericiden gönderilen mesaj işareti, işaretin gönderildiği kanaldan ve aynı zamanda verici ve alıcı devrelerinden kaynaklanan işareti bozucu etkilerden dolayı, bozulmaya uğrar ve alıcıda gönderilenden farklı bir bilgi alınabilir. Bu durum haberleşme sisteminin hatalı mesaj göndermesi olarak adlandırılır. Kanal kodlama, sayısal haberleşme sisteminde, alıcıda alınan bilgi bitlerinde meydana gelebilecek bu hataları ortadan kaldırmayı amaçlayan geniş bir araştırma alanıdır.

Kodlama teorisinin başlangıcı olarak Claude Shannon'un 1948 yılında yayınlamış olduğu "A Mathematical Theory of Communication" adlı makalesi kabul edilir (Shannon, 1948). Başlangıç sayılan bu teoriden sonra kodlama teorisi gürültü kanalları boyunca veri iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenmiştir.

Kriptografi ise bilgi güvenliğini inceleyen bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen

matematiksel yöntemler üzerine yapılan çalışmalar kriptografinin önemli konularıdır. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da koruma amacı güderler.

Kriptografi ve kodlama teorisinin bilgi iletişiminde amaçları farklıdır. Yukarıda da anlatıldığı gibi kriptografinin amacı iki ya da daha fazla kişinin haberleşmesinde gizlilik, veri bütünlüğü, doğrulama ve inkar edememe esaslarını birleştirerek mesajın güvenli iletişimini sağlamaktır. Kodlama teorisinin amacı ise gürültülü kanallar boyunca veri iletimi ve bozulan mesajı düzeltme gibi konularla ilgilenmek, doğru iletim oranı yüksek zaman ve enerji tasarrufu sağlayan kodlama yöntemlerini geliştirmektir.

Kriptografi sadece bilgi saklaması ve aktarması problemine güvenli bir çözüm aramaktan ibaret değildir. E-imza, e-para ve e-seçim vs. gibi farklı kullanım alanları da bulunmaktadır. Bu problemlere çözüm getiren protokoller, şifreleme sistemlerine ek olarak, "kriptografik temel taşları" diyebileceğimiz yöntemler kullanmaktadır. Bunlardan bazıları şunlardır:

- Gizlilik Paylaşımı (Secret Sharing)
- Sıfır Bilgi İspatları(Zero-Knowledge Prof)
- Kör İmzalar

Gerçek yaşamda yatırım sektörü göz önünde bulundurulduğunda gizli dokümanların güvenli bir şekilde muhafaza edilmesi ya da kaybolmasını engellemek gereklidir Bu durumda gizli anahtarın dürüst bir kişi tarafından muhafaza edilmesi gerekmektedir. Ancak böyle bir gizlilik durumunda anahtarın kaybolması ya da değişikliğe uğraması söz konusu olabilir. Gizli anahtarın kaybolması durumunda ise depolanan bilgilere bir daha ulaşılması mümkün olamayacaktır.

Ayrıca kriptografik işlemler sırasında yetkinin birden fazla kullanıcı arasında paylaştırılması gereken durumlar vardır. Örneğin bir bankanın çok gizli kriptografik anahtarı, bir anahtar paylaşım yöntemi kullanarak, belli bir sayıda katılımcının gizli bilgiye ulaşabileceği; ancak daha az sayıda katılımcı ile ulaşılamayacağı şekilde bir grup insan arasında paylaştırılır.

Yukarıda bahsedilen sorunlara ilk çözüm olarak 1979'da Shamir (Shamir, 1979) ve Blakley (Blakley, 1979) Gizlilik Paylaşım Şeması fikrini ortaya atmıştır. Bu şemadaki amaç anahtar yönetim sorumluluğunu tek bir kullanıcıya vermektense pek çok kullanıcı arasında dağıtarak güvenliği sağlamaktır.

Gizlilik paylaşım şeması kriptografik anahtar yönetimi ve anahtar dağıtımı ile ilişkili önemli bir kavramdır. Bu anahtar dağıtım ve yönetim problemi bütün kriptosistemlerde oldukça sık rastlanan bir problemdir.

Literatürde birçok anahtar paylaşım yöntemleri mevcuttur. Bunlardan en temeli Shamir'in polinom tabanlı gizlilik paylaşım şemasıdır. George Blakley gizliliği yeniden elde etmek için geometrik metot kullanan geometrik gizlilik paylaşım şemasını ortaya çıkarmıştır. Asmuth-Bloom (Asmuth ve Bloom , 1983) ve Mignotte (Mignotte, 1983) Çin kalan teoremi tabanlı eşik gizlilik paylaşım şemasını sunmuşlardır. Daha sonraki çalışmalarda hata doğrulama kod tabanlı gizlilik paylaşım şemaları önerilmiştir (Bhondo vd. , 1993 ; McEliece ve Sarwate , 1981). Örneğin McEliece ve Sarwate Reed Solomon Kod tabanlı gizlilik paylaşım şemasını önermiştir (McEliece ve Sarwate , 1981).

Bu tezde ilk önce gizlilik paylaşım şemasının en temelini oluşturan Shamir'in gizlilik paylaşım şemasının bir uygulaması gerçekleştirilmiştir. Ayrıca tezin temel amacı olan kriptografide anahtar dağıtım ve yönetim problemine çözüm getiren gizlilik paylaşım şemasına kodlama teorisindeki tekniklerden faydalanılarak uygulanabildiği gösterilmiştir. Özellikle hata doğrulama kod tabanlı gizlilik paylaşım şemaları oluşturulurken, minimum Hamming mesafesi en fazla olan dolayısıyla en fazla hata düzeltebilen kodlar olarak (n, k, d) Reed-

Solomon kodların d=n-k+1 Singleton sınırı ile tanımlanan MDS kodlar kullanılmıştır. Bu uygulamalar seçilen farklı uzaylarda gerçekleştirilmiştir. Birincisi, GF(q) asal cisim üzerinde elde edilen çeşitli MDS kodlar ile ilişkilendirilmiş gizlilik paylaşım şemaları uygulanmıştır. Seçilen n uzunluklu k boyutlu d minimum mesafeye sahip olan (n,k,d) MDS kodun, erişim yapıları olarak en az k kadar paylaşımcının bilgilerinden gizliliğin yeniden elde edilebildiği gösterilmiştir. Seçilen ikinci uzay $GF(2^n)$ sonlu cisim uzayıdır. Bu uzayda da elde edilen çeşitli MDS kodlar ile oluşturulan Gizlilik Paylaşım Şemaları uygulamalarla gösterilmiştir.

Bu şemalarda paylaşımcıların dürüst olması yani kendilerine ait olan verileri doğru vermesi durumunda gizliliğin yeniden elde edilebildiği gösterilmiştir. Aksi takdirde gizli veriye ulaşmak mümkün olmamaktadır. Böyle bir problem olduğu durumda yani dürüst olmayan katılımcılar olması halinde kullanılan kodun hata düzeltme algoritmalarından faydalanılır. Hata düzeltme algoritmaları ile dürüst olmayan katılımcılar tespit edilip, onların yanlış verileri düzeltilerek gizliliğin yeniden elde edilmesi sağlanır.

Tezin son bölümünde, MDS kod tabanlı gizlilik paylaşım şemasında dürüst olmayan katılımcılar olması durumunda Reed-Solomon kodun bir hata düzeltme algoritması olan Öklid algoritmasından faydalanılarak bu katılımcılar tespit edilip yanlış verilerinin düzeltilerek gizliliğin yeniden elde edilebildiği uygulamalarla gösterilmiştir.

BÖLÜM 1

1. MATEMATİKSEL ALT YAPI

Bu bölümde kodlama teorisi ve kriptografide kullanılan bazı matematiksel tanımlardan ve teoremlerden bahsedilmiştir. Bu tanımlar ile ilgili daha geniş bilgilere (Stinson, 2002 ; Ling ve Xing, , 2004 ; Lidl ve Niederreiter, 1994 ; Moreira ve Farrell, 2006) kaynaklarından ulaşılabilir.

1.1. Cebirsel Yapılar

Tanım 1. 1 Üzerinde en az bir işlem tanımlı olan ve bu işleme göre bazı şartları sağlayan kümeye bir cebirsel yapı denir. Eğer A kümesi üzerinde bir * işlemi tanımlanmışsa (A,*) ikilisi tek işlemli bir cebirsel yapıdır. Benzer şekilde, Δ başka bir işlem ise $(A,*,\Delta)$ yapısı iki işlemli bir cebirsel yapıdır (Bilgiç, 2009).

1.1.1. Yarı Gruplar

Tanım 1. 2. S, boş olmayan bir küme ve $*$, S üzerinde tanımlı bir işlem olsun. S kümesi üzerinde tanımlanan * işleminin birleşme özelliği varsa (S,*) sistemine bir yarı grup denir. Eğer işlem hem birleşme hem de değişme özelliğine sahip ise (S, *) yapısı değişken yarı grup adını alır. Birim elemanı olan yarı gruplara da monoid denir (Bilgiç, 2009).

1.1.2. Grup

Tanım 1. 3. G boş olmayan bir küme ve $*$, G'de bir ikili işlem olsun. Eğer aşağıdaki dört şart sağlanıyorsa $(G,*)$ sistemine bir grup denir.

i) Her $a,b \in G$ için $a*b \in G$. (Kapalılık)

ii) Her $a,b,c \in G$ için $(a*b)*c = a*(b*c)$. (Birleşme)

iii) Her $a \in G$ için $a*e = e*a = a$ olacak şekilde $e \in G$ vardır. (Birim eleman)

iv) Her $a \in G$ için $a*b = b*a = e$ olacak şekilde $b \in G$ vardır. (Ters eleman)

Bunlara ilaveten eğer

v) Her $a,b \in G$ için $a*b = b*a$. (Değişme)

özelliği varsa $(G,*)$ sistemine bir abelyen (değişmeli) grup denir (Bilgiç, 2009).

1.1.3. Halka

Tanım 1.4. Boş olmayan bir H kümesi üzerinde $\oplus$(toplama) ve $\otimes$(çarpma) ikili işlemleri tanımlansın. Eğer aşağıdaki şartlar sağlanıyorsa $(H,\oplus,\otimes)$ iki işlemli cebirsel yapısına bir halka denir.

a) $(H,\oplus)$ bir abelyen gruptur.

b) $(H,\otimes)$ bir yarı gruptur.

c) $\otimes$ işleminin $\oplus$ üzerine dağılma özelliği vardır (Bilgiç, 2009).

Örnek 1. 1. Bilinen toplama ve çarpma işlemlerine göre Z, Q, R ve C kümeleri birer halkadır. Yine, bilinen matris toplaması ve matris çarpması işlemlerine göre 2×2 tipindeki reel matrislerin kümesi bir halkadır (Bilgiç, 2009).

Örnek 1. 2. S → (e, a, b, c) S üzerinde (*) aşağıdaki gibi tanımlansın.

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

(*) işleminin birleşme özelliği vardır ve dolayısı ile yarı gruptur. Örneğin (e*c) *b = e * (c*b) şeklindedir ve etkisiz eleman e dir. Dolayısı ile bu yapı monoid bir yapıdır.

$a^1 = a$

$a^2 = a * a = b$

$a^3 = a * a * a = b * a = c$

$a^4 = a * a * a * a = b * a * a = c * a = e$

a^n biçiminde (e, a, b, c) nin her elemanı yaratılabilir dolayısı ile a'ya grubun üreteci denir. Grubun bir üreteci olduğu için halka gruptur. Grubun her elemanı sadece bir sütun ve satırda bulunduğundan sonlu bir gruptur (Aslan, 2008).

1.1.4. Cisim

Tanım 1. 5. Boş olmayan bir H kümesi üzerinde $\oplus$(toplama) ve $\otimes$(çarpma) ikili işlemleri tanımlansın. $\oplus$ işleminin birim elemanını 0_H ile gösterelim. Eğer aşağıdaki şartlar sağlanıyorsa $(H,\oplus,\otimes)$ iki işlemli cebirsel yapısına bir cisim denir.

a) $(H,\oplus)$ bir abelyen gruptur.

b) $(H/\{0_H\},\otimes)$ bir abelyen gruptur.

c) $\otimes$ işleminin $\oplus$ üzerine dağılma özelliği vardır.

Örnek 1. 3. Bilinen toplama ve çarpma işlemlerine göre Q, R ve C kümeleri birer cisimdir. Modulo 7 toplama ve çarpma işlemlerine göre $Z_7 = \{0,1,2,3,4,5,6\}$ kümesi bir cisimdir.

1.2. Sonlu Cisim

Sonlu cisimler ve onun bir alt kümesi olan Galois cisimleri matematiğin diğer alanlarındaki önemi dışında kodlama teorisi ve kriptografi gibi uygulamalarda da sıkça kullanılır.

Tanım 1. 6. Sonlu cisim adından da anlaşılacağı üzere sonlu sayıda elemana sahip bir 'cisim'dir. Sonlu cismin sahip olduğu eleman sayısı sonlu cismin düzenini belirler. Aynı sayıda elemana sahip tüm sonlu cisimler eş yapılıdır. Bu demektir ki tamamıyla aynı matematiksel yapıyı gösterirler sadece elemanlarının gösterilişinde farklılıklar vardır (Bilgiç, 2009).

1.2.1. Galois Cisimleri

Tanım 1. 7. GF(p) Asal Cisimler

'p' bir asal sayı olmak üzere p sayıda elemana sahip bir küme Z_p={0,1,2,…,p-1}, üzerinde mod p toplama '+' ve mod p çarpma '*' işlemlerinin tanımlanmasıyla, p sayıda elemana sahip bir sonlu cisim elde edilir. Bu sonlu cisim $GF(p)$ olarak adlandırılır. 'p', $GF(p)$'nin karakteristiğidir. Bir başka deyişle, p bir asal sayı

olmak üzere, p sayıda elemana sahip bir sonlu cisim Galois cismi olarak adlandırılır ve $GF(p)$ olarak gösterilir (Başkök, 2007).

Örnek 1. 4. Aşağıdaki Tablo 1.1'te GF(7) üzerinde tanımlı toplama ve çarpma işlemleri gösterilmiştir.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tablo 1. 1. GF(7) Cismi Üzerinde Toplama ve Çarpma İşlemleri

Tanım 1. 8. GF(p^n), Genişletilmiş Cisim

$GF(p)$ bir Galois cismi olmak üzere, $q = p^n$ elemanlı $GF(p^n)$ cismi oluşturulabilir. Bu yeni cisme $GF(p)$'nin 'Genişletilmiş cismi' denilir. 'p' $GF(p^n)$'nin karakteristiği olarak adlandırılır.

$GF(p^n)$'nin elemanları n adet $GF(p)$ elemanından oluşur. Bu nedenle GF(p^n)'nin Galois cismi koşullarını sağlayabilmesi için n. dereceden bir 'indirgenemez polinomu' kullanılır. Bu şekilde 'toplama' ve 'çarpma' işlemleri sonucunda elde edilen değerlerin $GF(p^n)$ içerisinde kalması sağlanır (Başkök, 2007).

Tanım 1. 9. GF(2^n) İkili Cisim

Galois cisimlerinde karakteristik olarak '2'nin kullanılması (p=2), cisim üzerinde tanımlanan matematiksel işlemlerin gerçekleştirilmesini çok kolaylaştırmaktadır.

Bu nedenle yazılım ve donanım uygulamalarında, kriptografik algoritmaların gerçeklenmesinde yaygın olarak $GF(2^n)$ kullanılmaktadır.

$GF(2^n)$ ile oluşturulan sonlu cisimler, 'ikili sonlu cisimler' olarak adlandırılmaktadır. Çünkü $GF(2^n)$'nin elemanları yan yana yazılmış bitler, $\{0,1\}$, halinde gösterilebilmektedir (Başkök, 2007).

1.2.3. Sonlu Cisim Üzerinde Matematiksel İşlemler

Hata düzelten kodların tasarımında ve kriptografide $GF(q = p^m)$ üzerinde oluşturulan polinomlar ve bu polinomlar arasındaki matematiksel işlemler büyük önem taşımaktadır. Bu bölümde katsayıları *GF(q)*'nun elemanı olan polinomlar arasındaki matematiksel işlemlerin gerçekleştirilmesi ve *GF(q*)'nun oluşturulması açıklanacaktır.

1.2.3.1. Toplama

Polinomsal gösterimde, aynı cisim içerisinde bulunan iki elemanın toplanması ya da çıkarılması işlemi, standart polinomların toplama ve çıkarma işlemi gibidir. Sonlu cisim aritmetiğinde elemanlar $\{0,1\}$ katsayılarına sahip polinomlar olarak temsil edilebildiğinden toplama işlemi katsayılarının basitçe modulo 2 aritmetiğine göre XOR toplamıdır denilebilir (Aslan, 2008).

Örnek 1. 5. a = (01110111) ve b = (10110101) olsun. O zaman a + b = 11000010 olacaktır. Polinomsal olarak göstermek gerekirse a = $X^6 + X^5 + X^4 + X^2 + X + 1$ ve b = $X^7 + X^5 + X^4 + X^2 + 1$ olarak ifade edilir. Buradan a + b = $X^7 + X^6 + X$ olarak elde edilir.

1.2.3.2. Çarpma

Sonlu cisim aritmetiğinde çarpma polinomların birbirleri ile aritmetik çarpımı şeklindedir. Fakat çarpma sonucunda doğal olarak sonlu cismin derecesinden daha yüksek dereceli elemanlar oluşabilir. O zaman bu elemanları sonlu cisimin derecesinden küçük olacak şekilde cismi oluşturan indirgenemez polinom aracılığı ile indirgemek gerekir. Dolayısı ile bu işlem indirgenemez polinoma göre indirgeme ya da mod alma işlemidir (Aslan, 2008).

Örnek 1.6. $a = 1101$ ve $b = 0101$ ve indirgenemez polinom $X^4 + X + 1$ seçilsin. Bu değerlere göre

$$\begin{aligned} a.b &= (X^3 + X^2 + 1).(X^2 + 1) \\ &= (X^5 + X^4 + X^2 + X^3 + X^2 + 1) \\ &= X^5 + X^4 + X^3 + 1 \\ &= X^2 + X + X + 1 + X^3 + 1 \\ &= X^3 + X^2 \end{aligned}$$

$$\begin{aligned} X^1 &= X \\ &\vdots \\ X^4 &= X + 1 \\ X^5 &= X^2 + X \\ &\vdots \\ X^{15} &= 1 \end{aligned}$$

şeklinde olacaktır (Aslan, 2008).

1.2.3.3. Ters Alma

n bit iki polinomun çarpımının kalanı seçilen indirgenemez polinoma göre 1 ise o zaman iki polinom birbirinin o indirgenemez polinoma göre tersidir denir. İndirgenemez bir polinoma göre ters alma işlemi için iki yöntem önerilebilir. Bu yöntemlerden ilki $GF(2^n)$ için tablo oluşturmaktır. Eğer n değeri küçük bir değer ise bu yöntem etkili olabilir.

Örnek 1. 7: $GF(2^4)$ için indirgenemez polinom olarak $X^4+X^3+X^2+X+1$'i seçilsin. Bu cismin karakteristiği 2, eleman sayısı 16 ve bu cisimdeki bir üreteç eleman $\beta=(0011)=\alpha+1$ dir. Bu β üreteç elemanının üslerini düşünelim (Aslan, 2008).

$$\beta^0=(0001),\beta^1=(0011),\beta^2=0101),\beta^3=(1111)$$
$$\beta^4=(1110),\beta^5=(1101),\beta^6=(1000),\beta^7=(0111)$$
$$\beta^8=(1001),\beta^9=(0100),\beta^{10}=(1100),\beta^{11}=(1011)$$
$$\beta^{12}=(0010),\beta^{13}=(0110),\beta^{14}=(1010),\beta^{15}=(0001)$$

Dolayısıyla $a\in GF(2^n)$ ve $a=\beta^i$ olmak üzere a'nın çarpmaya göre tersi $a^{-1}=\beta^{(-i)\bmod(2^n-1)}$ şeklinde verilebilir. Bunu göz önüne alarak elemanların tersi ve polinomsal yazılışları aşağıdaki gibidir.

β^0	(0001)	1	Tersi	β^{15}	(0001)	x
β^1	(0011)	$X+1$	Tersi	β^{14}	(1010)	x^3+x
β^2	(0101)	X^2+1	Tersi	β^{13}	(0110)	x^2+x
β^3	(1111)	x^3+x^2+x+1	Tersi	β^{12}	(0010)	x
β^4	(1110)	x^3+x^2+x	Tersi	β^{11}	(1011)	x^3+x+1
β^5	(1101)	x^3+x^2+1	Tersi	β^{10}	(1100)	x^3+x^2
β^6	(1000)	x^3	Tersi	β^9	(0100)	x^2
β^7	(0111)	x^2+x+1	Tersi	β^8	(1001)	x^3+1
β^8	(1001)	x^3+1	Tersi	β^7	(0111)	x^2+x+1
β^9	(0100)	x^2	Tersi	β^6	(1000)	x^3
β^{10}	(1100)	x^3+x^2	Tersi	β^5	(1101)	x^3+x^2+1
β^{11}	(1011)	x^3+x+1	Tersi	β^4	(1110)	x^3+x^2+x
β^{12}	(0010)	x	Tersi	β^3	(1111)	x^3+x^2+x+1
β^{13}	(0110)	x^2+x	Tersi	β^2	(0101)	x^2+1
β^{14}	(1010)	x^3+x	Tersi	β^1	(0011)	$x+1$
β^{15}	(0001)	1	Tersi	β^0	(0001)	1

Tablo 1. 2. GF(2^4)' de elemanların tersi ve polinomsal gösterimi

Tanım 1. 10. GF(2) üzerinde oluşturulan m. Dereceden p(x) polinomu m'den daha küçük dereceli polinomlara bölünemiyorsa p(x) GF(2) üzerinde indirgenemez denir (Moreira ve Farrell, 2006).

Tanım 1. 11. GF(2) üzerinde indirgenemez p(x) polinomunun böldüğü $X^n + 1$ polinomu için $n=2^m - 1$ ise p(x) ilkel bir polinomdur (Moreira ve Farrell, 2006).

Örneğin $p(x) = x^4 + x + 1$ polinomu 4'ten daha az dereceli bir polinoma bölünemez ve bu nedenle GF(2) üzerinde indirgenemez polinomdur. p(x) , $x^{15} + 1$ i böler fakat $1 \le n \langle 15$ olmak üzere başka bir x^n+1 polinomunu bölemez. Bu nedenle p(x) ilkel bir polinomdur.

İlkel polinomlar Galois Alanlarının oluşturulmasında kullanılırlar. Galois alanının oluşturulması için GF(2) içinde α sembolü tanımlansın, öyle ki $\alpha.0 = 0,\ \alpha.1 = \alpha$ olsun.

p(a) = 0 olarak verilir. Örnek olarak $p(x) = x^4 + x + 1$ polinomundan $GF(2^4)$ oluşturulsun.

$$p(\alpha) = \alpha^4 + \alpha + 1 = 0$$
$$\alpha^4 = \alpha + 1$$
$$\alpha^5 = \alpha.\alpha^4 = \alpha.(\alpha + 1) = \alpha^2 + \alpha$$
$$\alpha^6 = \alpha.\alpha^5 = \alpha.(\alpha^2 + \alpha) = \alpha^3 + \alpha^2$$
$$\alpha^7 = \alpha.\alpha^6 = \alpha.(\alpha^3 + \alpha^2) = \alpha^4 + \alpha^3 = \alpha + 1 + \alpha^3 = \alpha^3 + \alpha + 1$$

Bu işlemler $GF(2^4)$'ün tüm elemanları için tekrarlanırsa, her elemana bir polinom karşı düşer. p_i ,bir polinomun i. katsayısı olmak üzere, her eleman 4 bitlik $p_0 p_1 p_2 p_3$ vektörüyle de ifade edilebilir. Tablo 1.3' te $GF(2^4)$'ün tüm elamanlarının polinomsal ve vektörel gösterimleri verilmiştir (Moreira ve Farrell, 2006).

Ondalık Gösterim	Polinomsal Gösterim	Vektörel Gösterim	Eleman
0	0	0000	0
1	$\alpha^0 = 1$	0001	1
2	α	0010	α
4	α^2	0100	α^2
8	α^3	1000	α^3
3	$\alpha + 1$	0011	α^4
6	$\alpha^2 + \alpha$	0110	α^5
12	$\alpha^3 + \alpha^2$	1100	α^6
11	$\alpha^3 + \alpha + 1$	1011	α^7
5	$\alpha^2 + 1$	0101	α^8
10	$\alpha^3 + \alpha$	1010	α^9
7	$\alpha^2 + \alpha + 1$	0111	α^{10}
14	$\alpha^3 + \alpha^2 + \alpha$	1110	α^{11}
15	$\alpha^3 + \alpha^2 + \alpha + 1$	1111	α^{12}
13	$\alpha^3 + \alpha^2 + 1$	1101	α^{13}
9	$\alpha^3 + 1$	1001	α^{14}

Tablo 1. 3. $GF(2^4)$ 'ün elemanlarının farklı gösterilişleri

Katsayıları gerçel sayılar olan bir polinomun sanal kökleri olması gibi, katsayıları *GF(2)*'den alınan bir polinomun kökleri *GF(2^m)*'den olabilir. Örneğin $p(x) = x^4 + x^3 + 1$ *GF(2)* üzerinde indirgenemez bir polinomdur. p(0)=p(1)=1 olduğundan p(X)'in *GF(2)* de bir kökü yoktur. Fakat *GF(2^4)*'ün elemanı olan $\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$ p(x)'in kökleridir ve bunlar,

$p(\alpha^7) = p(\alpha^{11}) = p(\alpha^{13}) = p(\alpha^{14}) = 0$

$p(x) = (x+\alpha^7)(x+\alpha^{11})(x+\alpha^{13})(x+\alpha^{14})$

$p(x) = x^4 + x^3 + 1$

olarak belirlenir.

Teorem 1. 1: f(x), $GF(2)$ üzerinde tanımlı bir polinom, $\beta \in GF(2^m)$ olmak üzere, eğer β f(x)'in kökü ise $i \geq 0$ için β^{2^i} de f(x)'in bir köküdür (Moreira ve Farrell, 2006).

Eleman	**Minimal Polinom**
0	x
1	$x+1$
$\alpha, \alpha^2, \alpha^4, \alpha^8$	$x^4 + x + 1$
$\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$	$x^4 + x^3 + x^2 + x + 1$
α^5, α^{10}	$x^2 + x + 1$
$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$	$x^4 + x^3 + x + 1$

Tablo 1. 4. GF(2^4)'ün elemanlarının minimal polinomları

Tanım 1. 12. Eğer $\Phi(x), \Phi(\beta) = 0$ koşulunu sağlayan minimum dereceli polinom ise $\Phi(x)$'e β'nın minimal polinomu denir. GF(2^4)'ün elemanlarının minimal polinomları Tablo 1.4'te verilmiştir (Moreira ve Farrell,2006).

1.3. Sayılar Teorisi

1.3.1.Bölünebilirlik

a ve b verilen tamsayılar olsun. Eğer $b = a.d$ eşitliğini sağlayan bir d sayısı varsa a b'yi böler (b, a tarafından bölünür ya da a, b'nin bir çarpanı) denir ve $a|b$ şeklinde gösterilir.

Her $b\rangle 1$ tamsayısı en azından iki pozitif bölene sahiptir; bunlar 1 ve b'dir (Keyman ve Yıldırım, 2004).

Örnek 1. 8. *1.* $15|0$, çünkü $0 = 15.0$

2. $16|48$, çünkü $48 = 16.3$

1.3.2. Bölünebilirlik Özellikleri

Bütün $a, b, c \in Z$ için, aşağıdakiler doğrudur (Keyman ve Yıldırım, 2004).

1. $a|a$
2. Eğer $a|b$ ve $b|c$ ise $a|c$.
3. Eğer $a|b$ ve $a|c$ ise bütün $x, y \in Z$ için $a|bx + cy$ ifadesi doğrudur.
4. Eğer $a|b$ ve $b|a$ ise $a = \pm b$

1.3.3. Tamsayılar için Bölüm Algoritması

Eğer a ve b, $b \geq 1$ olmak koşulu ile, tamsayılar ise a'nın b'ye bölümü q tamsayısı gibi bir bölüm ve r tamsayısı gibi bir kalan verir.

$$a = qb + r, 0 \leq r \langle b$$

Üstelik q ve r tektir. Bu bölümün kalanı $a \bmod b$ olarak gösterilir (Keyman ve Yıldırım, 2004).

Örnek 1. 9. Eğer a=73, b=17 ise q=4 ve r=5'tir. Böylece 73 mod17=5'tir.

1.3.4. En Büyük Ortak Bölen(Greatest Common Divisor-GCD)

a ve b her ikisi birlikte 0 olmamak koşulu ile iki tamsayı olsun. a ve b'nin en büyük ortak böleni, a ve b'yi bölen en büyük d tamsayısıdır. a ve b'nin en büyük ortak böleni $\gcd(a,b)$ ya da kısaca (a,b) ile gösterilir (Keyman ve Yıldırım, 2004).

Teorem 1. 2. a ve b her ikiside birlikte 0 olmayacak şekilde tamsayılar olsun. $\gcd(a,b) = ax + by$ eşitliğini sağlayan x ve y tamsayılar her zaman vardır.

Örnek 1. 10. 540 ile 168'in en büyük ortak böleni aşağıdaki gibi bulunabilir (Aslan, 2008).
a'yı b' ye bölerek ve tekrar tekrar her kalanı, sıfır kalan elde edene kadar bölünene bölünür.

gcd(540,168) =

168	36
144	4
24	

36	24
24	1
12	

24	12
24	2
0	

540	168
504	3
36	

gcd(540,128) = gcd(168,36) = gcd(36,24) = gcd(24,12)= 12

ax+by

12 = 540x + 168y

540 = 168.3+36

168 = 36.4+24

36 = 24.1+12

12 = 36 - 24.1

12 = 36 - (168- 36.4).1

12 = 5.36 -168

12 = 5(540-168.3) – 168

12 = 540.5 -168.16

x = 5 y= -16 olarak yazılabilir.

1.3.5. Asal Sayı

Tanım 1. 13. 1'den büyük, 1 ve kendisinden başka böleni olmayan tamsayılara asal sayı denir. Asal olmayan sayılara da bölünebilir sayı denir.

Tanım 1. 14. İki tamsayı a,b olmak üzere $\gcd(a,b)=1$ şeklinde ise bu iki tamsayı birbirlerine göre asaldır denir ve bu durumda x ve y gibi iki tamsayı $ax+by=1$ olacak şekilde vardır.

1.3.6. Aritmetiğin Esas Teoremi

$n \geq 2$ olan her tamsayı asal sayıların çarpımları şeklinde tek olarak yazılır. Yani,

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

Sayısında p_k lar farklı asal sayıları e_k lar da pozitif tamsayıları göstermektedir (Keyman ve Yıldırım, 2004).

Örnek 1. 11. $4200 = 2^3.3.5^2.7$

1.3.7. Euler Fi (ϕ) Fonksiyonu (Euler Phi Function)

Tanım 1. 15. $a \geq 1$ ve $m \geq 1$ olsun. Eğer $\gcd(a,m) = 1$ ise a ve m için aralarında asal denir. Z_m de m ile aralarında asal olan tamsayıların sayısı genellikle $\phi(m)$ ile tanımlanır ve bu fonksiyona Euler Phi Fonksiyonu denir (Aslan, 2008).

Teorem 1. 3. $\phi(m)$, m'nin asal üslerinin çarpanlarına ayrılması ile bulunabilir. p_i'ler farklı asal sayılar olmak üzere $e_i > 0$ ve $1 \leq i \leq n$ için sırasıyla m ve $\phi(m)$ (1.1) ifadesindeki gibi gösterilebilir.

$$m = \prod_{i=1}^{n} p_i^{e_i}, \qquad \phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i-1}) \tag{1.1}$$

Örnek 1. 12. $\phi(98)$ değerini bulalım. Yani 98'den küçük 98 ile aralarında asal olan tamsayıların sayısını bulalım (Aslan, 2008).

$$m = 98 = 2.7^2 \Rightarrow \phi(98) = (2^1 - 2^0).(7^2 - 7^1) = 1.42 = 42$$

1.3.8. Öklid Algoritması (Euclidean Algorithm)

a ve b şeklinde olan iki tamsayının en büyük ortak bölenini asal çarpanlarına ayırarak ve ortak çarpanların en büyüğünü alarak bulabiliriz. Eğer a ve b büyük sayılarsa bunların asal çarpanlarını bulmak zor olur; bunun sonucunda da en büyük ortak böleni bulmak da zorlaşır. Sayılar teorisinin önemli bir araştırma alanı da büyük tamsayıların daha çabuk çarpanlarına ayırma üzerinedir. Eğer a ve b'nin asal çarpanları biliniyorsa, gcd(a,b)'yi bulmak için hızlı bir yol vardır. O da öklid algoritmasıdır.

Öklid Algoritması şöyle çalışır.

- a>b olmak üzere, a, b'ye bölünür. Bölüm q_1 ve kalan r_1 olsun.

$$a= b.q_1 + r_1$$

- İkinci bölme işlemi gerçekleştirilir. b, r_1'e bölünür ve bölüm q_2 kalan ise r_2 olur.

$$b= q_2. r_1 + r_2$$

- Üçüncü olarak r_1, r_2'ye bölünür ve bölüm q_3 kalan ise r_3 olur.

$$r_1= q_3 .r_2 + r_3$$

.

- Son olarak r_{n-1}, r_n'e bölünür ve bölüm q_{n+1} kalan ise $r_{n+1}=0$ olur.

$$r_{n-1}=q_{n+1} . r_n +r_{n+1}$$

- $r_{n+1}=0$ olduğu için r_n değeri a ve b tamsayılarının en büyük ortak böleni olur. Yani gcd(a,b)=r_n 'dir.

Bu algoritmadaki işlemler sonsuza kadar gitmez, çünkü 0 ile a tamsayısı arasında sonlu sayıda tamsayı vardır.(Keyman ve Yıldırım, 2004)

Öklid algoritmasını Algoritma 1.1'deki gibi ifade edebiliriz (Stinson , 2002).

Öklid(a,b) →

$r_0 \leftarrow a$

$r_1 \leftarrow b$

$m \leftarrow 1$

while($r_m \neq 0$)

$$\left\{ \begin{array}{l} q_m \leftarrow \left\lfloor \dfrac{r_{m-1}}{r_m} \right\rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m+1 \end{array} \right\}$$

$m \leftarrow m-1$

return$(q_1, q_2 \ldots q_m, r_m)$

r_m=gcd(a,b)

Algoritma 1. 1. Öklid Algoritması

1.3.9. Genişletilmiş Öklid Algoritması (Extended Euclidean Algorithm)

Öklid algoritması sadece a ve b tamsayılarının d = gcd(a,b) ifadesinde sadece d'yi hesaplarken Genişletilmiş Öklid Algoritması bu değerin yanında ax+by = d denklemindeki a ve b katsayılarını da bulmak için olanak vermektedir. Genişletilmiş Öklid Algoritması Algoritma 1. 2'de verilmiştir.

Extended_Euclidean(a,b) →

$$a_0 \leftarrow a$$
$$b_0 \leftarrow b$$
$$t_0 \leftarrow 0$$
$$t \leftarrow 1$$
$$s_0 \leftarrow 1$$
$$q \leftarrow \left\lfloor \frac{q_0}{b_0} \right\rfloor$$
$$\text{while}(r > 0)$$
$$\begin{cases} \text{temp} \leftarrow t_0 - qt \\ t_0 \leftarrow t \\ t \leftarrow \text{temp} \\ \text{temp} \leftarrow s_0 - qs \\ s_0 \leftarrow s \\ s \leftarrow \text{temp} \\ a_0 \leftarrow b_0 \\ b_0 \leftarrow r \\ q \leftarrow \left\lfloor \frac{q_0}{b_0} \right\rfloor \\ r \leftarrow q_0 - qb_0 \end{cases}$$
$$r \leftarrow b_0$$
$$\text{return}(r, s, t)$$

Algoritma 1. 2 Genişletilmiş Öklid Algoritması

Algoritma sonucunda dönen değerler r = gcd(a,b) ve sa + tb = r şeklinde kullanılır (Stinson , 2002).

Örnek 1. 13. gcd(24,138)'in sonucu kaçtır? gcd(24,138) = ax +by ifadesinde x ve y sayıları kaç olur?

$$138 = 5 \cdot 24 + 18$$
$$24 = 1 \cdot 18 + 6 \quad \text{ise gcd}(24,138) = 6$$
$$18 = 3 \cdot 6 + 0$$

Bu sonuç Öklid algoritması ile bulunur.

x ve y ise Genişletilmiş Öklid Algoritması ile aşağıdaki şekilde bulunur.

gcd(24,138) = 6

$$\begin{aligned} 6 &= 24 - 1 \cdot 18 \\ &= 24 - 1 \cdot (138 - 5.24) \\ &= 24 - 1 \cdot 138 + 5 \cdot 24 \\ &= 6 \cdot 24 - 1 \cdot 138 \end{aligned}$$

Yani,

$6 = 6 \cdot 24 + (-1) \cdot 138$. Buradan x = 6 ve y = -1 bulunur.

Örnek 1. 14. gcd(1547,560)'ın sonucu kaçtır? gcd(1547,560) = ax+ by ifadesinde x ve y sayıları kaç olur?

$$1547 = 2 \cdot 560 + 427$$
$$560 = 1 \cdot 427 + 133$$
$$427 = 3 \cdot 133 + 28$$
$$133 = 4 \cdot 28 + 21$$
$$28 = 1 \cdot 21 + 7 \quad \text{ise gcd}(1547,560) = 7$$
$$21 = 3 \cdot 7 + 0$$

x ve y aşağıdaki şekilde bulunur.

$$
\begin{aligned}
7 &= 28 - 1\cdot 21 \\
&= 28 - 1(133 - 4\cdot 28) && = 28 - 1\cdot 133 + 4\cdot 28 \\
&= 5\cdot 28 - 1\cdot 133 && = 5\cdot(427 - 3\cdot 133) - 1\cdot 133 \\
&= 5\cdot 427 - 15\cdot 133 - 1\cdot 133 && = 5\cdot 427 - 16\cdot 133 \\
&= 5\cdot 427 - 16\cdot(560 - 1\cdot 427) && = 5\cdot 427 - 16\cdot 560 + 16\cdot 427 \\
&= 21\cdot 427 - 16\cdot 560 && = 21\cdot(1547 - 2\cdot 560) - 16\cdot 560 \\
&= 21\cdot 1547 - 42\cdot 560 - 16\cdot 560 && = 21\cdot 1547 - 58\cdot 560
\end{aligned}
$$

Yani,

$7 = 21\cdot 1547 + (-58)\cdot$ y dir.

Buradan x = 21 ve y = -58 bulunur.

1.3.10. Aritmetik Tersi

$a \neq 0$ her hangi bir tamsayı olmak üzere, eğer $a.a^* \equiv 1 \bmod n$ denkliğini sağlayan bir a^* tamsayısı var ise bu a^* sayısına a'nın mod n'e göre aritmetik tersi denir.

Teorem 1. 4. Eğer $\gcd(a,n) = 1 \Rightarrow a$ 'nın mod n'e göre aritmetik tersi vardır.

Örnek 1. 15. $\bmod 26$ 'ya göre 15'in tersi nedir?
Burada Öklid algoritmasını kullanarak gcd(15,26)=1 olacak şekilde x ve y sayılarını bulacağız.

$$15x + 26y = 1$$

Olacak şekilde x ve y sayılarını bulalım.

$$26 = 15 \cdot 1 + 11$$
$$15 = 11 \cdot 1 + 4$$
$$11 = 4 \cdot 2 + 3$$
$$4 = 3 \cdot 1 + 1$$

Buradan 1'i çekip, diğerlerindeki kalanı çekip bu denklemde yerine yazmaya çalışacağız.

$$1 = 4 - 3 \cdot 1$$
$$1 = 4 - 1 \cdot (11 - 4 \cdot 2)$$
$$1 = 3 \cdot 4 - 11$$
$$1 = 3 \cdot (15 - 1 \cdot 11) - 11$$
$$1 = 3 \cdot 15 - 4 \cdot 11$$
$$1 = 3 \cdot 15 - 4 \cdot (26 - 15)$$
$$1 = 7 \cdot 15 - 4 \cdot 26$$

O halde 15'in tersi 7'dir.

Örnek 1. 16. $-6^{-1}(\text{mod}17)=?$

$-6=11\text{mod}17$

$11^{-1}= x \text{ mod}17$

$17 = 11.1 + 6$
$11 = 6.1 + 5$
$6= 5.1 + 1$

$1 = 6 - 5.1$
$1 = 6 - (11-6)$
$1 = 2.6 -11$
$1 =2(17 -11) – 11$
$1=2.17 -3.11$

11'in katsayısı (-3) bu da-3=14 mod17'dir. O halde

$(-6)^{-1}=14\text{mod}(17)$'dir.

1.3.11 Denklik Teorisi (Theory of Congruence (Modularity))

Tanım 1. 16. m pozitif bir tamsayı olsun. $a,b \in Z$ için $m|(a-b)$ ise a b 'ye mod m'e göre denktir denir ve $a \equiv b \bmod m$ ile gösterilir (Mezenes vd., 1996).

Teorem 1. 5 (Fermat's Little Theorem) Eğer p asal bir sayı ise ve gcd(a,p)=1 koşulunu sağlıyorsa

$a^{p-1} \equiv 1 \pmod{p}$ denkliği her zaman doğrudur.

Tanım 1. 17. Eğer p ve q, $a^p \equiv a \pmod{p}$ ile $a^q \equiv a \pmod{q}$ denkliklerini sağlayan farklı asal sayılar ise $a^{pq} \equiv a \pmod{pq}$ dur (Keyman ve Yıldırım, 2004).

Örnek 1.17. $2^{1000000} \equiv ? \pmod 7$

p=7 p-1=6

1000000=6.166666+4 yani $1000000 \equiv 4 \pmod 6$

Böylece

$$2^{1000000} = (2^6)^{166666}.2^4 \equiv 1.2^4 = 16 \equiv 2 \bmod 7$$

1.3.12. Çin Kalan Teoremi (Chinese Remainder Theorem)

Çin kalan teoremi belirli denklik sistemlerini çözme metodudur. Farzedelim ki $m_1, m_2, ..., m_r$ pozitif tamsayılar ver her $i \neq j$ için $obeb(m_i, m_j) = 1$ olsun. $a_1, a_2, ..., a_r$ tam sayıları verildiğinde

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\cdots \\ x &\equiv a_r \bmod m_r \end{aligned} \qquad (1.2)$$

denklik sisteminin Z de tek bir çözümü vardır ve denklik kümelerinin çözümü şöyledir. $m_1, m_2, ..., m_r$ modülüne göre

$$x \equiv a_1 b_1 \frac{M}{m_1} + \ldots + a_r b_r \frac{M}{m_r} (\text{mod } M) \quad (1.3)$$

ve

b_i' ler $b_i \frac{M}{m_i} \equiv 1 \bmod(m_i)$ denklik sistemi ile elde edilir (Stinson , 2002).

BÖLÜM 2

2. KRİPTOLOJİ

2.1. Kriptolojinin Temelleri

Herhangi bir mesajı, anlaşılamayan bir şekle dönüştüren ve anlaşılamayan şifreli mesajı tekrar anlaşılabilir mesaja çeviren yöntem ve prensipleri içeren şifreleme tasarımı ve kullanımını anlatan haberleşme konusuna kriptoloji denir. Kriptoloji iki bölüme ayrılır: Kriptografi ve kriptanaliz.

Kriptografi bilgi güvenliğini inceleyen bir bilim dalıdır. Güvenilirlik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği konularıyla ilgilenen matematiksel yöntemler üzerine yapılan çalışmalar kriptografinin önemli konularıdır. Bu yöntemler, bir bilginin iletimi esnasında karşılaşılabilecek aktif ya da pasif ataklardan bilgiyi dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da koruma amacı güderler.

Kriptanalizin amacı ise şifrelenmiş bir mesajın içeriğinin elde edilmesidir. Bu nedenle şifreleme işleminin kontrolü için daima gizli bir anahtar kullanılır. Bazı kriptografik uygulamalarda, bu gizli anahtarlar güvenli bir kanal aracılığı ile yetkili alıcıya iletilmelidir (Schneider , 1996).

2.2. Bilgi Güvenliği Kavramları

Bir bilginin güvenli olarak iletileceğinden ya da elde edilmiş bir bilginin güvenli bir şekilde elde edilmiş olduğundan bahsedilebilmesi için, kullanılan iletişim sistemlerinin sahip olması beklenebilecek bazı güvenlik kavramları vardır:

Gizlilik (*privacy/confidentiality):* Bilgiyi görme yetkisi olanlar dışındaki herkesten gizli tutmaktır.

Kimlik Denetimi (*authentication/identification):* İletimi gerçekleştirilen bir mesajın göndericisinin gerçekten gönderen kişi olduğunun garantisidir.

Veri Bütünlüğü (*data integrity):* Bütünlük bir bağlantının tamamı ya da tek bir veri parçası için, mesajın gönderildiği gibi olduğuna, üzerinde hiçbir değişiklik, ekleme, yeniden düzenleme yapılmadığının garantisidir.

İnkar Edememe (*non-repudation):*alıcının veya göndericinin iletilen mesajı inkar edememesidir. Böylece bir mesaj gönderildiğinde alıcı göndericinin mesajı gönderdiğini, benzeri biçimde gönderici de, alıcının mesajı aldığını ispatlayabilir.

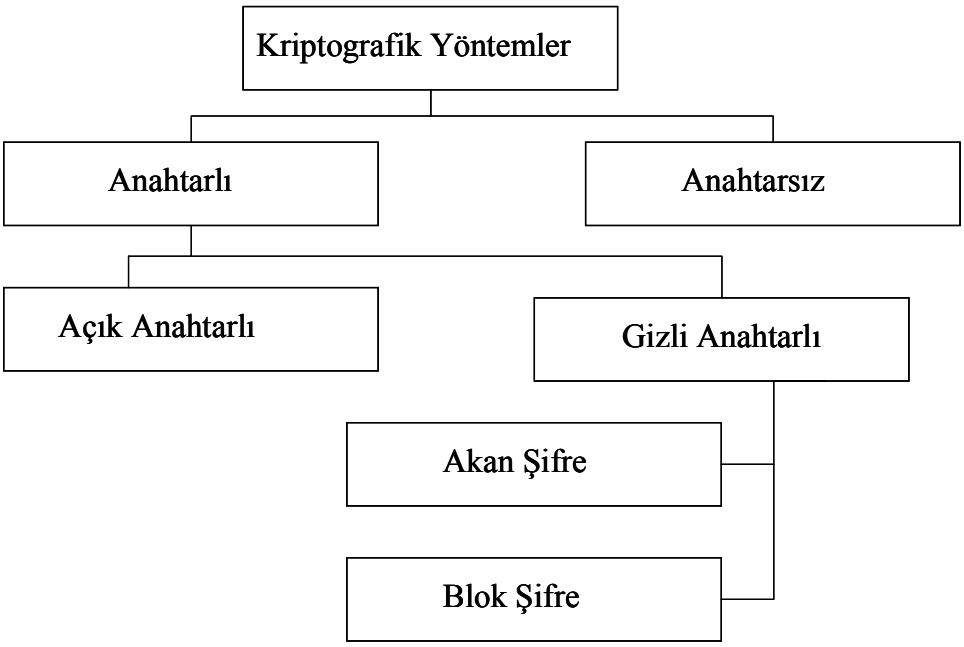
Erişim Kontrolü (*access control*): İzinsiz kişi ya da uygulamaların erişmemeleri gereken kaynaklara erişemeyecekleri garantisidir. Ağ güvenliği bağlamında, erişim kontrolü, ana bilgisayar sistemlerine erişimleri kontrol etme ve limitlendirme yetisidir. Bu kontrolü başarmak için, erişimi kazanmaya çalışan her varlık ilk olarak tanımlanmalı veya doğrulanmalıdır. Erişim kontrolü servisleri kimlik denetimi yapılmış varlıkların kaynaklara ancak kendilerine izin verilen şekilde erişebilecekleri garantisini vermekle yükümlüdür.

2.3. Kriptografik Algoritmalar

Tüm modern algoritmalar şifreleme ve çözme işlemlerini kontrol etmek için bir anahtar kullanırlar; bir mesaj sadece kullanılan anahtar şifreleme anahtarıyla uyuştuğunda çözülebilir.

Şifreleme süresince Şekil 2.1'de gösterildiği gibi anahtarlı ve anahtarsız olmak üzere iki farklı yöntem kullanılabilir. Özet(Hash) fonksiyonları, sıkıştırma fonksiyonları anahtarsız yöntemlere örnek olarak gösterilebilir. Anahtarlı kriptosistemler iki ana başlık altında listelenebilir:

- Simetrik anahtarlı şifreleme (veya gizli-anahtarlı şifreleme) ,
- Asimetrik şifreleme (veya açık-anahtarlı şifreleme) (Koblitz, 1994)



Şekil 2.1. Şifreleme Yöntemleri

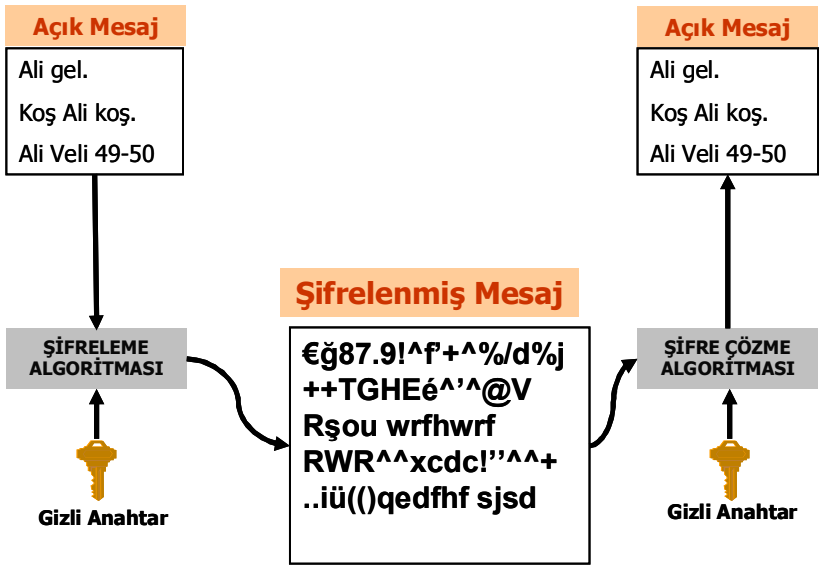
2.3.1.Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmalarında mesajın şifrelenmesinde ve çözülmesinde tek bir gizli anahtar kullanılır. Şifreleme işlemlerini gerçekleştirdikten sonra şifreli metni alıcıya gönderirken şifreli metinle birlikte gizli anahtarı da alıcıya güvenli bir şekilde göndermesi gerekmektedir. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve çözme işlemleri gerçekleştirebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır.

Simetrik anahtarlı kriptosistemler, blok ve akan şifreleme olmak üzere ikiye ayrılır (Tsunoo vd, 2002) ;(DES, 1977) ;(Diffie ve Hellman, 1976) ; (AES, 2001).

Simetrik şifreleme algoritmaları şunlardır:

- Blok şifreleme algoritmaları (AES, DES, IDEA, Skipjack, RC5 …)
- Akan (Stream) Şifreleme algoritmaları(RC2, RC4…)



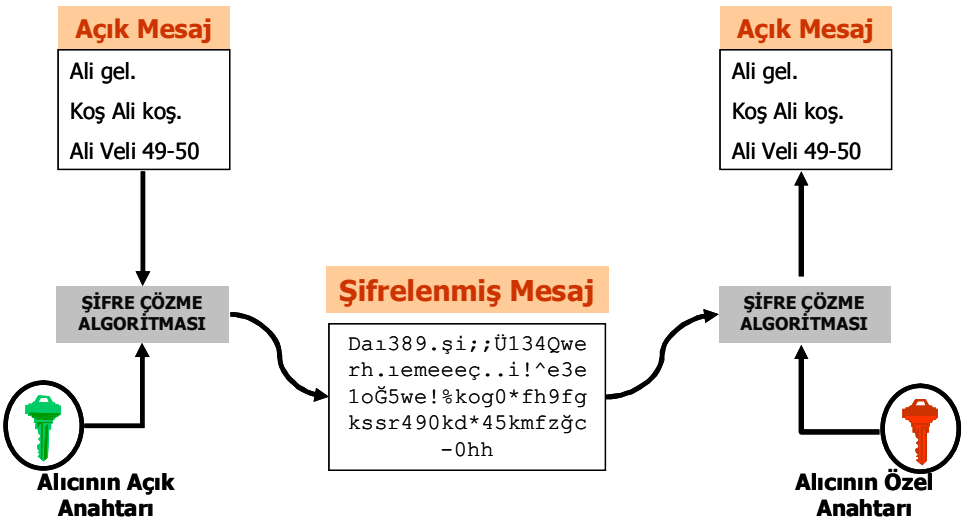
Şekil 2.2. Simetrik Şifreleme Algoritması Genel Yapısı

2.3.2. Asimetrik Şifreleme Algoritmaları

Açık anahtarlı kriptosistemlerde ya da başka bir deyişle asimetrik şifrelemede her bir tarafın sahip olduğu açık (e) ve gizli (d) olarak adlandırılan bir anahtar çifti kullanılır. Şifreleme anahtarı olarak kullanılan e'nin gizli olması gerekmez. Açık anahtarlı şifrelemenin altında yatan temel düşünce açık anahtar, e, verildiği halde şifre çözme anahtarı olarak kullanılan d'nin bulunmasının zor olmasına dayanır. Açık anahtarlı sistemler sayısal imza ve anahtar değişim protokolleri gibi uygulamalarda kullanılır（Rivest vd., 1978) ; (Ellison ve Schneier, 2000).

Asimetrik şifreleme algoritmaları şunlardır:

- RSA
- El Gamal
- Eliptik Eğri Sistemleri
- Diffie-Hellman anahtar belirlemesi
- Kod-tabanlı Kriptosistemler (McEliece, 1978) ; (Niederreiter, 1986)



Şekil 2.3. Asimetrik Şifreleme Algoritması Genel Yapısı

Kriptografik bir algoritmanın güvenli olması algoritmanın gizli olmasını gerektirmez. Kerckhoff'un prensibine göre gizli anahtar hariç algoritmanın bütün ayrıntıları bilinmesine rağmen kırılamıyorsa algoritma güvenlidir. Bir kriptografik algoritmanın yaşam süreci şöyle özetlenebilir: Algoritmanın tasarlanması, matematiksel analizlerinin yapılması, yayınlanması, diğer uzmanlar tarafından değerlendirilmesi (matematiksel/istatistiksel analizlerle), yazılımsal ve donanımsal olarak uygulanması, standardizasyonu ve endüstriyel bir ürün haline gelmesidir (Pellikaan vd., 2011).

2.4. Anahtar Yönetimi

Asimetrik algoritmalarda her iki kullanıcı veriyi farklı anahtar bilgisi ile şifreler ve çözer. Bu amaçla her bir kullanıcı biri gizli diğeri açık iki anahtar kullanır. Açık anahtar bilgisi alıcı tarafa herhangi bir koruma yapılmadan iletilir. Açık anahtarı alan taraf bu bilgiden şifreyi çözmek amacı ile kullanacağı gizli anahtarı üretir. Açık anahtarın üçüncü bir kişinin eline geçmesi tek başına hiç bir şey ifade etmez. Hem simetrik hem de asimetrik algoritmaların temel özelliği yapılarının açık olarak bilinmesidir. Böylece şifreleme algoritmalarının tasarımında, şifrelenmiş verinin anahtar bilgisi olmadan şifrenin çözülememesi ilkesi göz önüne alındığından, iletişim güvenliği, şifreleme anahtarlarının güvenliği problemine indirgenmiştir (Diffie ve Hellman, 1976).

Kriptografik anahtarların üretilmelerinden dağıtılmalarına ve kullanılmalarına kadar olan sürecin sıkı bir denetim altına alınması kriptografik işlemlerin güvenilirliği açısından büyük öneme sahiptir. Bu işlemlerin tümüne anahtar yönetimi denir. Anahtar yönetiminin en zayıf halkası, dış müdahalelere tümüyle açık olan anahtarların güvenli bir şekilde dağıtılması işlevidir. Geleneksel olarak kriptografiden yararlanan, askeri ve diplomatik servisler, bu problemi, anahtarları, güvenilir kuryeler aracılığı ile ileterek çözmüşlerdir. Ancak bu oldukça pahalı ve yavaş bir yöntemdir.

Günümüzde kişilerin veya kuruluşların gereksindiği bilgi miktarı geçmiş on yılla karşılaştırıldığında hızla yükselmiştir. Bunun sonucu olarak iletişim olanakları ile birlikte iletişim ortamları da değişmiştir. Bugün artık sistem tasarımcıları çağın gerektirdiği bilgiyi işlemek üzere bilgisayarları geliştirmişler ve verilerin hızlı bir şekilde iletilebilmesini sağlamak amacı ile veri ağlarını tasarlamışlardır. Veri işlenmesinde kullanılan bilgisayar ağları, veri işleyen ana bilgisayar birimlerinden, kontrol birimlerinden ve terminallerden oluşur. Tüm bu yapılar birbirlerine veri bağları ile bağlıdırlar. Veri bağları uydu ve mikrodalga bağlantıları olabileceği gibi anahtarlanmış veya anahtarlanmamış iletişim hatları da olabilirler. Veri ağı birbirine veri bağları ile bağlı düğümlerden (ana bilgisayarlar) ve veri ağının yalnızca ana bilgisayarlar üzerinden kullanabilen terminallerden oluşmaktadır. Veri ağının temel işlevi bir kullanıcının (kişi veya programın) diğer kullanıcı ile haberleşmesi için gerekli erişim yolunu sağlamaktır. Veri ağlarının bu yapısı isteyen kullanıcının bu sistemleri kullanmasını sağlamakla birlikte ortaya iletişim sırasında kullanılan gizli mesajların korunması problemini de çıkarmaktadır. Her ne kadar mesaj güvenliği kriptografik işlemlerle sağlansa da şifreleme anahtarlarının güvenli bir biçimde üretilmesi ve kullanıcılara dağıtılması problem olmaya devam etmektedir (Levi ve Özcan, 2002).

Gizlilik Paylaşım Şemaları kriptografik anahtar dağıtım ve yönetim problemine çözüm getiren bir metottur. İlk olarak Shamir (Shamir, 1979) ve Blakley 1979'da (Blakley, 1979) birbirlerinden bağımsız olarak Gizlilik Paylaşım Şemasını önermiştir. Bu şemadaki amaç anahtar yönetim sorumluluğunu tek bir kullanıcıya vermektense pek çok kullanıcı arasında dağıtarak güvenliği sağlamaktır. Bu konu ile ilgili daha detaylı bilgiler Bölüm 4'te açıklanmıştır.

2.5. Kriptografik Protokoller

Kriptografi sadece bilgi saklaması ve aktarması problemine güvenli bir çözüm aramaktan ibaret değildir. Elektronik imza, elektronik para ve elektronik seçim vs gibi farklı kullanım alanları da bulunmaktadır. Bu problemlere çözüm getiren protokoller, bahsi geçen şifreleme sistemlerine ek olarak, "kriptografik temel taşları" diyebileceğimiz yöntemler kullanılmaktadır. Bunlardan bazıları şunlardır:

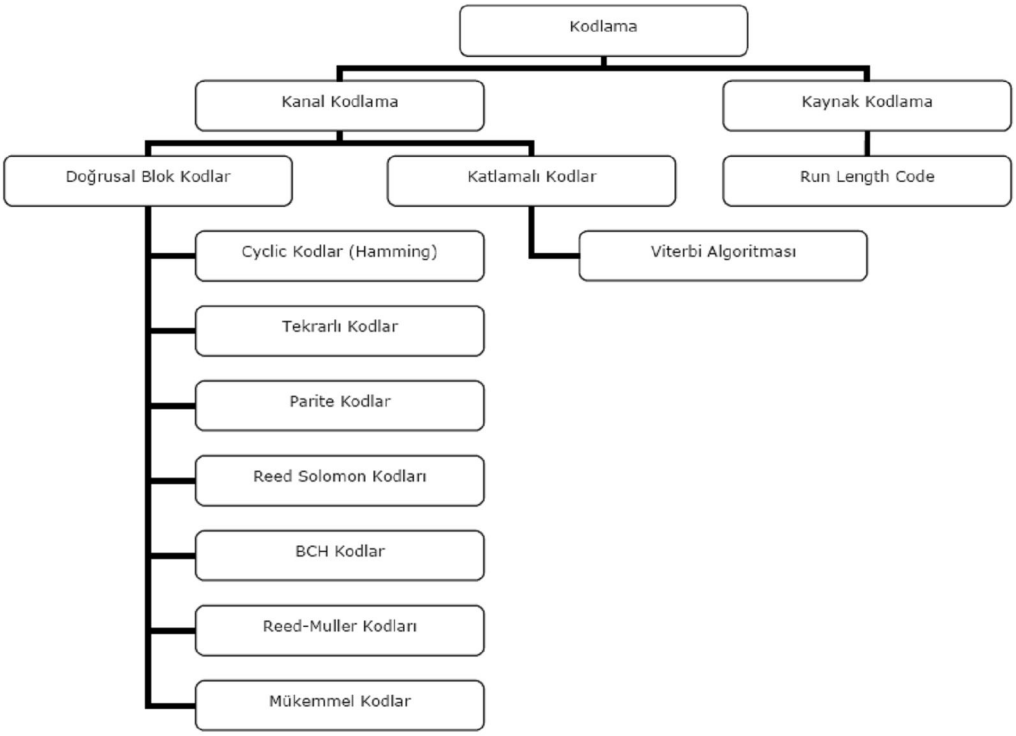
- Gizlilik Paylaşımı (Secret Sharing)
- Sıfır Bilgi İspatları (Zero- Knowledge Prof)
- Kör İmzalar

BÖLÜM 3

3. KODLAMA TEORİSİ

3.1. Giriş

Kodlama teorisi, birçok bilim dalı için önemli bir rol oynamaktadır. Bunlardan bazıları şöyle sıralanabilir: Matematik alanında istatistik biliminde, bilgisayar alanında şifreleme konusunda, haberleşme alanında, haberleşme karmaşıklığını en düşük seviyeye indirmek ve kaynakların etkin biçimde temsil edilmesini sağlamak için kullanılmaktadır. Kodlama, iletişim alanında kaynakların, kanalların, alıcıların bilgi karakteristiklerini incelemek, bilginin iletimini optimize etmek ve iletimin güvenilirliğini sağlamak amacıyla kullanılmaktadır (Richardson ve Urbanke, 2005).



Şekil 3.1. Kodlama Türleri

Kodlama, kanal ve kaynak kodlama olarak iki ana gruba ayrılabilir. Kaynak kodlamada, bilgiyi daha etkin biçimde temsil etmek için verinin boyutu azaltılır. Günlük hayatta sıkça karşılaştığımız "sıkıştırma" programları, bu kodlamanın bir uygulamasıdır. Sıkıştırma işlemi, daha az yer kaplamak amacıyla dosyaların boyutlarının küçültülmesidir. Kanal kodlamada ise verinin iletimini oluşabilecek bozulmalara karşı daha güvenli şekilde yapabilmek amacıyla bilgiye fazladan bitler eklenir. Bu nedenle bilginin boyutu artar (Pless, 1989).

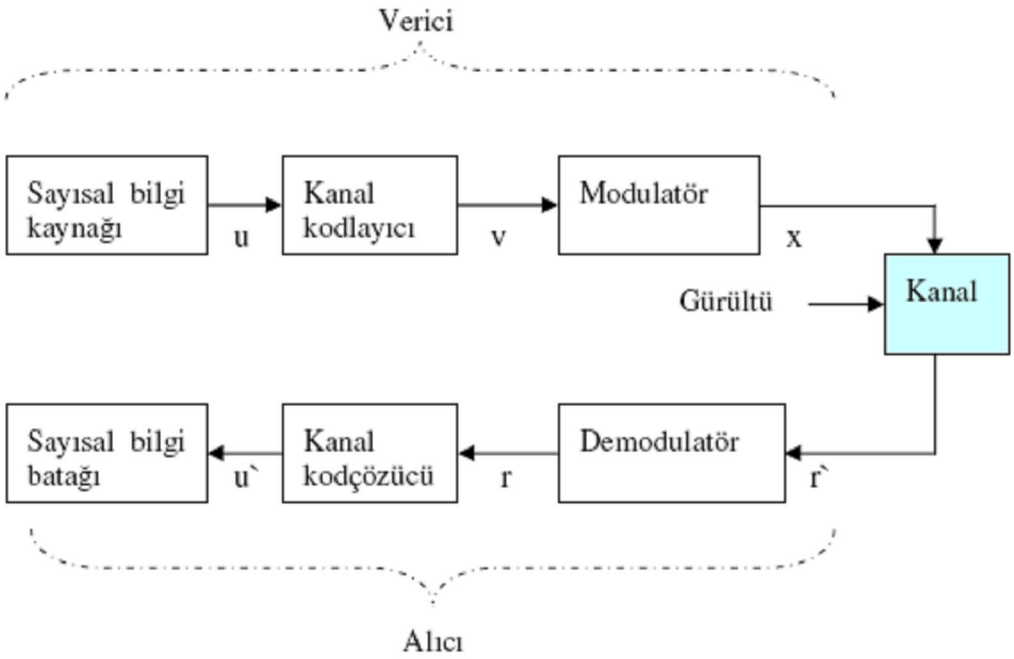
İletişim sistemlerinin günlük hayatımızın vazgeçilmez parçaları haline gelmesiyle, hızlı ve hatasız sayısal bilgi iletimi gerekliliği de önemli bir konu olarak karşımıza çıkmaktadır. Haberleşme sistemlerinde bilginin iletimi için vericiden gönderilen mesaj işareti, işaretin gönderildiği kanaldan ve aynı zamanda verici ve alıcı devrelerinden kaynaklanan işareti bozucu etkilerden dolayı, bozulmaya uğrar ve alıcıda gönderilenden farklı bir bilgi alınabilir. Bu durum haberleşme sisteminin

hatalı mesaj göndermesi olarak adlandırılır. Kanal kodlama, sayısal haberleşme sisteminde, alıcıda alınan bilgi bitlerinde meydana gelebilecek bu hataları ortadan kaldırmayı amaçlayan geniş bir araştırma alanıdır.

Örneğin cep telefonlarında, yüksek frekanslı radyo iletiminden kaynaklanan gürültü ve bozulmaları düzeltmek için kanal kodlama kullanılmaktadır. Modemlerde ve telefon iletiminde de kanal kodlama kullanılmaktadır.

Kanal kodlama teoreminde kanal kapasitesinin teorik sınırı ile ilgili olarak, Shannon (Shannon, 1948) ortaya koyduğu teoreminde, kodlama oranının kanal kapasitesinden küçük olması durumunda, bilginin uygun bir biçimde kodlanmasıyla, gürültülü bir kanalda bilgi iletimi esnasında oluşan hataların istenilen en düşük oranlara indirilebileceğini ispatlamıştı. Ancak bu işlemin nasıl yapılacağı bir problem olarak bırakılmıştı (Lin ve Costello, 2004). Bu teorem ile birlikte yeni kanal kodlama araştırma alanı ortaya çıkmıştır. Bu alanda yapılan çalışmaların en önemli amacı, kodlaması ve kod çözmesi kolay ve mümkün olduğunca küçük hata oranları sağlayan kodları bulmaktır (Bossert, 1999).

Sayısal haberleşme sisteminde iletilecek bilgi bitleri çok değişik amaçlara yönelik birçok aşamadan geçer. Burada kanal kodlama üzerinde durduğumuzdan, Şekil 3.2 ile gösterilen basit bir haberleşme sisteminde, en temel işlem blokları ve kanal kodlama işlemi ile ilgili bloklar gösterilmiştir.



Şekil.3.2. Basit bir haberleşme sistemi

Günümüzde kanal kodlama, "blok kodlar" ve "katlamalı kodlar" seklinde iki ayrı temel biçimde incelenmektedir (Akbaş, 2007).

Literatürde bulunan önemli blok kodlardan bazıları, Hamming kodları (Hamming, 1950), Reed-Muller kodları (Muller, 1954 ve Reed, 1954), ürün (product) kodları (Elias, 1954), |u|u+v| inşası kodları (Macwilliams, 1977 ve Plotkin), Golay kod (Golay, 1949 ve Wicker, 1995), çevrimsel (cyclic) kodlar (Prange, 1957), BCH (Bose, Chaudhuri and Hocquenghem) kodları (Hocquenghem, 1959 ve Bose, Chaudhuri, 1960), Reed-Solomon kodları (Reed, Solomon, 1960), Genelleştirilmiş dizi kodları (Generalised Array Codes, GAC) (Honary, Markarian, Farrel, 1993), Turbo kodları (Berrou, Glavieux, 1993, 1996, 1998), Düşük yoğunluklu parite kontrol kodları (Low Density Parity Check Codes, LDPC) (Gallager, 1962 ve 1963, Mackay, Neal 1996) ve ürün yığılma kodları (Product Accumulate, PA, codes) (Narayanan, Georghiades, 2004) olarak karşımıza çıkmaktadır.

3.2. Sonlu cisim üzerinde vektör uzayı

Tanım 3. 1 F_q**,** q dizili bir sonlu cisim olsun. V boş olmayan bir küme F_q da seçilen skalerle çarpma ve toplama işlemleriyle aşağıdaki durumları gerçekliyorsa F_q üzerinde bir vektör uzayıdır. Burada her $u,v,w \in V$ ve her $\lambda,\mu \in F_q$'dur (Ling ve Xing, 2004).

i. $u+v \in V$

ii. $(u+v)+w = u+(v+w)$

iii. Bütün $v \in V$ için $0+v = v = v+0$ özelliğini sağlayan bir $0 \in V$ vardır.

iv. Her $u \in V$ için $u+(-u) = 0 = (-u)+u$ sağlayan bir $(-u) \in V$ vardır.

v. $u+v = v+u$

vi. $\lambda v \in V$

vii. $\lambda(u+v) = \lambda u + \lambda v, (\lambda+\mu)u = \lambda u + \mu u$

viii. $(\lambda\mu)u = \lambda(\mu u)$

Tanım 3. 2 V, $F_q$üzerinde bir vektör uzayı olsun. $\alpha_1,\alpha_2,...,\alpha_k \in F_q$ skaler çarpımlar olmak üzere $v_1,v_2,...,v_k \in V$ vektörlerinin lineer kombinasyonu $w = \alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k v_k$ olarak tanımlanan bir vektördür (Ling ve Xing, 2004).

Tanım 3. 3 V, $F_q$üzerinde bir vektör uzayı olsun. V'de $\{v_1,v_2,...,v_k\}$ vektörlerinin kümesi

$$\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_k v_k = 0 \Rightarrow \alpha_1 = \alpha_2 = ... = \alpha_k = 0$$

koşulunu sağlıyorsa lineer bağımsızdır. Ancak bütün skalerleri sıfır değilse lineer bağımlıdır (Ling ve Xing, 2004).

Örnek 3.1

i) 0 içeren her S kümesi lineer bağımlıdır.

ii) Her F_q için $\{(0001),(0010),(0100)$ kümesi lineer bağımsızdır.

Tanım 3. 4 V, $F_q$üzerinde bir vektör uzayı olsun. $S = \{v_1, v_2, ..., v_k\}$ V'nin boş olmayan bir alt kümesi olsun**.** S'nin kapsayanı(span)

$$\langle S \rangle = \{\alpha_1 v_1 + ... + \alpha_k v_k : \alpha_i \in F_q\}$$

olarak tanımlanır. S boş ise <S>={0} olarak tanımlanır (Ling ve Xing, 2004).

Örnek 3.2. S={0100, 0011, 1100} alalım. S ile üretilmiş C kümesini bulalım.

0100 + 0011 = 0111,
0100 + 1100 = 1000,
0011 + 1100 = 1111 ve
0100 + 0011 + 1100 = 1011 ve sıfır vektörü.

C=<S>={ 0000, 0100, 0011, 1100, 0111, 1000, 1111, 1011} dir.

Tanım 3. 5 V, F_q üzerinde bir vektör uzayı olsun. $V = \langle B \rangle$ ve B lineer bağımsız ise V'nin boş olmayan bir $B = \{v_1, v_2, ..., v_k\}$ kümesi V için bir taban (basis) olarak tanımlanır (Ling ve Xing, 2004).

Örnek 3. 3.

S={1001, 1101, 1011} lineer bağımsız bir küme ve
C =<S>= {0000, 1001, 1101, 0100, 0010, 0110, 1011,1111}

O halde S, C için bir tabandır.

Tanım 3. 6 Bir vektör uzayı için her tabandaki elemanların sayısı uzayın boyutu (dimension) olarak adlandırılır. Bununla beraber bir vektör uzayı için bütün tabanlar aynı sayıda elemanlar içerir (Ling ve Xing, 2004).

Örnek 3. 4. Örnek 3. 3'deki C kümesinin boyutu 3'tür. Çünkü C'nin tabanı olan S kümesinin eleman sayısı 3'tür.

Tanım 3. 7. $v = v_1, v_2, ..., v_n$ ve $w = w_1 w_2 ... w_n \in F_q^n$ olsun.,

i) v ve w'nin skaler çarpımı

$$v.w = v_1 w_1 + v_2 w_2 + ... + v_n w_n \in F_q$$

ii) Eğer v.w=0 ise v ve w vektörlerinin ortogonal olduğu söylenir

iii)S F_q^n'nin boş olmayan bir alt kümesi olsun. S'nin $S^{\perp}$ ortogonal komplementi aşağıdaki gibi tanımlanır (Ling ve Xing, 2004).

$$S^{\perp} = \{v \in F_q^n : \forall s \in S \; için \; v.s = 0\}$$

Not: C'nin dual kodu, $C^{\perp}$ Eğer C=<S> ise $C^{\perp} = S^{\perp}$'dir.

Örnek 3. 5.

S={0100,0101}, $S^{\perp}$ ortogonal komplementlerini bulalım.

$S^{\perp}$'nin $\alpha_1\alpha_2\alpha_3\alpha_4$ vektörü S'deki her vektöre ortogonal olmak zorundadır.

$\alpha_1 0 + \alpha_2 1 + \alpha_3 0 + \alpha_4 0 = 0$
$\alpha_1 0 + \alpha_2 1 + \alpha_3 0 + \alpha_4 1 = 0$
$\alpha_2 = 0$
$\alpha_2 + \alpha_4 = 0 \; \therefore \alpha_2 = \alpha_4 = 0$
α_1 ve α_3'*te* kısıtlama yoktur. Böylece kümemiz

$C^{\perp} = S^{\perp} = \{0000,1000,0010,1010\}$ olur.

Teorem 3. 1 S, F_q^n'nin bir alt kümesi olsun (Ling ve Xing, 2004).

$$\dim(\langle S \rangle) + \dim(S^{\perp}) = n$$

3.3. Kodlama Teorisindeki Temel Kavramlar

Tanım 3. 8.(Kod Sözcüğü). R , m elemanlı bir halka olsun.

$$R^n = \{ u = (u_1, u_2, ..u_n) \mid u_i \in R \}$$

olmak üzere R^n kümesinin M elemanlı C (sol) alt modülüne, uzunluğu n olan M elemanlı bir lineer kod denir ve (n, M) ile gösterilir. C kodunun herhangi bir elemanına kod sözcüğü adı verilir (Chapman,1996).

Tanım 3. 9.(Uzaklık Fonksiyonu). u ve v, R^n kümesinin iki elemanı olmak üzere u ve v arasındaki Hamming uzaklığı

$$d(u,v) = \left| \{ i \mid u_i \neq v_i \} \right|$$

şeklinde tanımlanır ve

$$d : R^n \times R^n \longrightarrow IN \cup \{0\}$$
$$(u,v) \longrightarrow d(u,v)$$

şeklinde tanımlanan bu dönüşüm aşağıdaki özellikleri sağlar.

i) $\forall u,v \in R^n$ *için* $d(u,v) \geq 0$, $d(u,v) = 0 \Leftrightarrow u = v$

ii) $\forall u,v \in R^n$ *için* $d(u,v) = d(v,u)$

ii) $\forall u,v,t \in R^n$ *için* $d(u,v) \leq d(u,t) + d(t,v)$ (Chapman,1996).

Tanım 3. 10.(Minimum Uzaklık) C kodunun minimum (Hamming) uzaklığı

$$d = d(C) = \min_{\substack{u,v \in C \\ u \neq v}} d(u,v)$$

şeklinde tanımlanır.

Uzunluğu n, eleman sayısı M, minimum uzaklığı d olan bir C lineer kodu kısaca (n, M, d) ile gösterilir (Chapman,1996).

Tanım 3. 11 (Ağırlık Fonksiyonu). x, IF_q^n vektör uzayının herhangi bir elemanı olmak üzere x'in sıfırdan farklı bileşenlerin sayısına x elemanının ağırlığı denir ve $w(x)$ ile gösterilir.

Bir C kodunun sıfırdan farklı tüm kod sözcüklerin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir (Chapman, 1996).

Örnek 3. 6.

w(0000000) = 0

w(1111111) =7

w(1022001) = 4

w(1011001) = 4

Minimum ağırlık w(C) = 4'tür.

Önerme 3. 1. x , y , IF_q^n vektör uzayının herhangi iki elemanı olmak üzere

$d(x, y) = w(x - y)$ 'tir (Chapman, 1996).

Teorem 3. 2. Bir C lineer kodunun minimum uzaklığı ile minimum ağırlığı eşittir (Chapman, 1996).

Örnek 3. 7. d(00111,11001)=4,

d(00122,12001)=5

Örnek 3. 8. C={0000, 1100, 0011, 1111}

C kodu için n=4 (kod uzunlukları), M=4 Kod kelimeleri sayısı ya da C kümesinin eleman sayısı, d=2 (minimum uzaklık)'tır. C, (4, 4, 2) şeklinde gösterilen ikili kodtur

Tanım 3. 12. Bir C kodlamasında b gönderilen kelime ve b^* alınan kelime olmak üzere

$$b^* = b \oplus e$$

dir. Bu durumda

$$e = b^* - b$$

olur. Buradaki e ifadesi B^n kümesinin keyfi bir elemanıdır. Bu şekilde tanımlanan e ifadesine hata vektörü adı verilir (Chapman, 1996).

Örnek 3. 9. B^6 grubunda yapılan kodlamada b^*=100011 ve b=111001 olsun. Bu durumda e=011010 dır. Burada e ifadesinin ağırlığı kod sözünde kaç hata olduğunu gösterir. Örnekte w(e)=3 olduğundan kodlamada 3 hata olmuştur diyebiliriz.

Gerçek iletişim sistemlerinde alıcının eline sadece b^* geçeceğinden b ve e değerleri hakkında bir bilgiye sahip olmayacaktır. Zaten kodlama teorisinin amacı kanalda meydana gelen mevcut e değerlerini tespit edip bunları düzelterek b^* değerlerinden b ifadelerine ulaşmaktır. Fakat kanalda oluşan her e tespit edilemez ve düzeltilemez.

Tanım 3. 13. (Tespit Edilebilen Hatalar) Bir (m,n) kodlamasında eğer

$$a \in C \text{ için } a \oplus e \notin C$$

ise e hata vektörü tespit edilebilirdir denir. Bu durumda eğer

$$a \in C \text{ için } a \oplus e \in C$$

ise e hata vektörü tespit edilemezdir denir (Chapman,1996).

Teorem 3. 3. Bir (m, n)kodlamasında ağırlığı en fazla k olan hata vektörlerinin tespit edilebilmesi için gerek ve yeter şart herhangi iki kod söz arasındaki minimum uzaklığın en az (k+1) olmasıdır (Chapman,1996).

Tanım 3. 14. (Düzeltilebilen Hatalar) $\forall b \in C$ için $D(b \oplus e) = b$ ise e hata vektörü düzeltilebilirdir denir. (Chapman,1996)

Teorem 3. 4. Bir (m,n) kodlamasında ağırlığı en fazla k olan hatalar düzeltilebilir ise herhangi iki kod söz arasındaki minimum uzaklık en az (2k+1) olur (Chapman,1996).

Teorem 3. 5. Kod sözleri arasında minimum uzaklığın 2k+1 olduğu bir kodlamada ağırlığı en fazla k olan hatalar düzeltilebilirdir (Chapman,1996).

3.4. Lineer Kodlar

$v(n,q) = F_q^n$, n uzunluğunda ve q elemanlı sonlu bir cisim üzerinde tanımlanmış bir vektör uzayı olsun.

Tanım 3. 15 $V(n,q)$ vektör uzayının alt vektör uzayına lineer kod denir. Eğer C kodunun boyutu k ise o zaman C koduna bir [n, k] kodu denir. Aynı zamanda C kodunun minimum uzaklığı d ise C koduna bir [n, k, d] - kodu denir.(Roman, 1992)

Örnek 3. 10. C_1 ve C_2 kodları aşağıdaki şekilde olsun:

C_1={ 11000, 01110, 10011, 00101} ve C_2 ={00000, 10110, 01011, 11101} .C_1'deki bütün kod sözlerin toplamı gözönüne alındığında,
$11000 + 01110 = 10110 \notin C_1$ olduğundan C_1 lineer bir kod değildir. C_2 deki bütün kod sözler toplamı gözönüne alındığında,

$$00000 + 10110 = 10110 \in C_2$$
$$00000 + 01011 = 01011 \in C_2$$
$$00000 + 11101 = 11101 \in C_2$$
$$10110 + 01011 = 11101 \in C_2$$
$$10110 + 11101 = 01011 \in C_2$$
$$01011 + 11101 = 10110 \in C_2$$

C_2 kodunun lineer bir kod olduğu görülür.

Tanım 3. 16 C kodunun elemanları olan kod sözler arasındaki ağırlıkların en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir. Yani,

$$w(C) = \min\{w(x,y) | x, y \in C, x \neq y\}$$

dir (Roman, 1992).

Tanım 3. 17. C lineer bir kod ise $d(C)=w(C)$ dir. Yani, lineer bir kodun minimum uzaklığı minimum ağırlığına eşittir (Roman, 1992).

Genel olarak bir (n, M) kodun minimum uzaklığını bulmak için $\binom{M}{2}$ tane uzaklık hesaplamak gerekir. Ancak kod lineer ise sadece (M-1) tane kodsözün ağırlığına bakmak kodun minimum uzaklığını bulmak için yeterlidir. Örneğin; C kodunun eleman sayısı 4 ise C kodunun minimum uzaklığını bulmak için C kodundaki her kod sözün birbiriyle olan uzaklıklarını hesaplamak için $\binom{4}{2} = 6$ işlem yapmak gerekirken, eğer bu lineer kod ise 4-1=3 tane işlem yapmak gerekir. Dolayısıyla kodun eleman sayıları büyük olduğu düşünüldüğünde kodun lineer olması oldukça kolaylık sağlar.

Örnek 3. 11 C ={00000, 10110, 01011, 11101} lineer kodunun uzaklığı iki şekilde bulunabilir. Birincisi; kodun minimum uzaklığı hesaplanır. Bunun için kod sözlerin birbirine olan uzaklıkları bulunur. Buradan,

$$d_1(00000,10110) = 3 \qquad d_4(10110,01011) = 4$$
$$d_2(00000,01011) = 3 \qquad d_5(10110,11101) = 3$$
$$d_3(00000,11101) = 4 \qquad d_6(01011,11101) = 3$$

elde edilir. Dolayısıyla kodun minimum uzaklığı,

$$d(C) = \min\{d_1, d_2, d_3, d_4, d_5, d_6\} = 3$$

İkincisi; C lineer kod olduğundan kodun minimum uzaklığı kodun minimum ağırlığına eşittir. Bunun için;

$$w_1(10110) = 3$$
$$w_2(01011) = 3$$
$$w_3(11101) = 4$$

Buradan,

$$w(C) = \min\{w_1, w_2, w_3\} = 3 = d(C)$$

elde edilir. Böylece her iki durumda minimum uzaklık 3'tür.

Tanım 3. 18. C bir lineer kod olsun. Satırları C kodunun bir baz vektörlerinden oluşan *kxn* boyutlu G matrisine, C kodunun üreteç matrisi denir. Eğer *G* matrisi *C* kodunun üreteç matrisi ise *C* kodunun kod sözleri, *G* matrisinin satırlarının lineer birleşimidir. Yani,

$$C = \{xG | x \in V(k,q)\}$$

şeklindedir.

Elementer satır işlemleri (satırların yerlerini değiştirmek, satırları sıfırdan farklı bir skaler ile çarpmak ve skalerle çarpılmış bir satırı diğerine eklemek) bir matrise uygulanırsa, bu matrisin satır uzayı (satırların lineer birleşimlerinden oluşan vektör uzayı) değişmez (Roman, 1992).

Teorem 3. 6. G üreteç matrisi I_k, $k \times k$ mertebeli birim matris, A, $k \times (n-k)$ mertebeli bir matris olmak üzere $(I_k | A)$ şeklinde bir matrise denktir. Bu biçimdeki haline, G'nin standart formu adı verilir (Roman, 1992).

Örnek 3. 12. *C* lineer kodu C={00000, 10110, 01011, 11101}şeklinde olsun. *C* lineer kodu için muhtemel üreteç matrisi

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

şeklinde alınabilir. G üreteç matrisi standart formdadır. V(2,2)'nin kod sözleri,

$$xG = (x_1, x_2)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (x_1, x_2, x_1, x_1 + x_2, x_2)$$

şeklinde kodlanır. Bu kod sözler $(x_1, x_2, x_1, x_1 + x_2, x_2)$ şeklindedir.

G matrisi standart formda olduğu için orjinal mesaj ya da söz, kodlanmış kod sözlerin ilk $k = 2$ koordinatlarında bulunur. Bu kodlama sistematik bir kodlamadır.

Tanım 3. 19. C bir lineer [n,k]- kodu olsun.

$$C^{\perp} = \{y \in V(n,q) | \langle y, x \rangle = 0, \forall x \in C\}$$

şeklinde tanımlanan $C^{\perp}$ koduna lineer kodun duali denir (Roman, 1992).

Teorem 3. 7.

1. C bir lineer [n,k]-kodu olsun. Bu takdirde, C lineer kodun duali de [n, n-k] kodudur.

2. C lineer kod ise $(C^{\perp})^{\perp} = C$ dir (Roman, 1992).

Tanım 3. 20. C kodunun üreteç matrisi $G = (I_k | A)$ olmak üzere; $GH^T = 0$ şartını sağlayan $H = (-A^T | I_{n-k})$ matrisine C kodunun kontrol matrisi denir (Roman, 1992).

Gerçekten,

$$GH^T = (I_k | A) \begin{pmatrix} -A \\ I_{n-k} \end{pmatrix} = -A + A = 0$$

olduğu görülür. Bu ise H matrisinin satırları ile G matrisinin satırlarının birbirine dik olduklarını gösterir. Ayrıca, $rank(H) = n - k = boy(C^{\perp})$ olduğundan, H matrisi $C^{\perp}$ kodunun bir üreteç matrisidir (Roman, 1992).

Örnek 3. 13. C lineer kodu aşağıdaki gibi olsun:

$$C = \{00000, 10110, 01011, 11101\}$$

Bu kodun üreteç matrisi

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} = (I_2 | A)$$

şeklinde ve standart formdadır.

Burada $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ve $A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ dır. C kodunun kontrol matrisi, $H = \left(-A^T | I_{n-k}\right)$ şeklinde olacağından $H = \left(-A^T | I_3\right)$ dır. Buradan

$$H = \left(-A^T | I_3\right) = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Elde edilir. (Z_2 üzerinde $-A^{\perp} = A^{\perp}$ dir.)

H kontrol matrisi $C^{\perp}$ kodunun üreteç matrisi olduğundan, H kontrol matrisinin satırlarının lineer toplamı $C^{\perp}$ kodunun elemanları olan kod sözleri verir. Bunlar,

$$C^{\perp} = \{00000,10100,11010,01001,01110,11101,10011,00111\}$$

dir.

3.5. Lineer Kodların Dekodlaması

Tanım 3.21. C kodu, kontrol matrisi H olan bir lineer kod olsun. Herhangi bir $x \in C$ için, Hx^T ifadesine x kod sözünün sendromu denir ve bu sendrom s ile gösterilir. Dolayısıyla, $x \in C$ olması için gerek ve yeter şart x kod sözünün sendromunun sıfır olmasıdır. Yani, alınan x kod sözü orjinal kod söz (hatasız giden kod söz) ise $Hx^T = 0$ dır (Roman, 1992).

Tanım 3. 22. Sendrom dekodlama işlemi aşağıdaki gibi tanımlanır:

1. Eğer sendrom değeri sıfır ise o zaman alınan kod söz, orjinal kod sözdür.

2. Eğer sendrom değeri H kontrol matrisinin i inci sütunu ise alınan kod sözün $i.$ bileşeninde hata vardır.

3. Eğer sendrom değeri ne sıfır ne de H kontrol matrisinin bir sütunu değilse alınan kod sözde en az iki hata vardır (Trappe ve Washington, 2002).

Örnek.3.14 $C = \{00000, 10110, 01011, 11101\}$ lineer kodunun üreteç ve kontrol matrislerini aşağıdaki gibi olsun:

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

1. Alınan kod söz r =10110 olsun. Alınan kod sözde hata olup olmadığını anlamak için sendrom hesaplanır. Dolayısıyla,

$$s = Hr^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = (000)$$

olur. Buradan sendrom s = (000) bulunur. Bu da alınan kod sözün hata içermediğini yani alınan kod sözün orjinal kod söz olduğunu gösterir.

2. Alınan kod söz r =10111 olsun. Bu taktirde sendrom,

$$s = Hr^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = (001)$$

olur. Elde edilen s =(001) sendromu alınan kod sözün hatalı olduğunu gösterir. Sendrom değeri, H kontrol matrisinin 5 inci sütunu olduğundan alınan vektörün 5 inci bileşeninde hata olduğunu gösterir. Buradan alınan vektörün 5 inci bileşeni düzeltilerek orjinal kod söz olan

x =10110 elde edilir.

3. Alınan kod söz r =11010 olsun. Bu taktirde sendrom

$$s = Hr^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = (111)$$

olur. Elde edilen s = (111) sendromu alınan kod sözün hatalı olduğunu gösterir. Sendrom değeri s = (111), H kontrol matrisinin herhangi bir sütununu vermediğinden alınan kod sözde en az 2 hata vardır.

BÖLÜM 4

4. GİZLİLİK PAYLAŞIM ŞEMALARI

4.1 Giriş

Gerçek yaşamda yatırım sektörü göz önünde bulundurulduğunda gizli dokümanların güvenli bir şekilde muhafaza edilmesi ya da kaybolmasını engellemek gereklidir Bu durumda gizli anahtarın dürüst bir kişi tarafından muhafaza edilmesi gerekmektedir. Ancak böyle bir gizlilik durumunda anahtarın kaybolması ya da değişikliğe uğraması söz konusu olabilir. Gizli anahtarın kaybolması durumunda ise depolanan bilgilere bir daha ulaşılması mümkün olamayacaktır (Secret Sharing ,CPT, 2006).

Gizlilik paylaşım şeması kriptografik anahtar yönetiminde kullanılan oldukça önemli bir yapıdır (Pang ve Wang, 2005);(Shao ve Cao, 2005) ; (Yang vd., 2004) ; (Zhao vd., 2007). Yukarıda bahsedilen sorunlara çözüm olarak 1979'da Shamir (Shamir, 1979) ve Blakley (Blakley, 1979) Gizlilik Paylaşım Şeması fikrini ortaya atmıştır. Bu şemadaki amaç anahtar yönetim sorumluluğunu tek bir kullanıcıya vermektense pek çok kullanıcı arasında dağıtarak güvenliği sağlamaktır. Gizlilik Paylaşım Şemaları önemli bir kaynağa erişimi sınırlandırmak gereken her durum için kullanılabilir. Örneğin nükleer bir bombayı fırlatma sorumluluğu tek bir kişiye vermek istenmez. Bunu yapmak için iki kişiden aynı anda kendilerine ait anahtarları ve parolalarının girilmesi istenebilir. Bu örnek gizlilik paylaşım kavramı ile karşılanmaktadır.

Shamir'in Gizlilik Paylaşım Şeması Lagrange İnterpolasyon polinomu tabanlıdır. Shamir'in Şemasında temel fikir, gizlilik en fazla n kullanıcı arasında paylaştırılır ve en az k kullanıcı paylaşımlarını birleştirerek gizliliği yeniden elde edebilir. Bu (k, n) eşik gizlilik paylaşımı olarak adlandırılır (Shamir, 1979).

George Blakely gizliliği yeniden elde etmek için geometrik metot kullanan geometrik gizlilik paylaşım şemasını ortaya çıkarmıştır. Çin kalan teoremi tabanlı eşik gizlilik paylaşım şemaları Mignotte (Mignotte, 1983) ve Asmuth-Bloom (Asmuth ve Bloom, 1983) tarafından bulunmuştur. Bu şemalarda çin kalan teoremi boyunca özel seçilmiş tam sayı dizileri kullanılır.

Daha sonraki çalışmalarda hata doğrulama kod tabanlı gizlilik paylaşım şemaları önerilmiştir (Bhondo vd., 1993) ; (McEliece ve Sarwate, 1981). Örneğin McEliece ve Sarwate Reed Solomon Kod tabanlı gizlilik paylaşım şemasını önermiştir (McEliece ve Sarwate, 1981).

4.2. Gizlilik Paylaşım Şeması

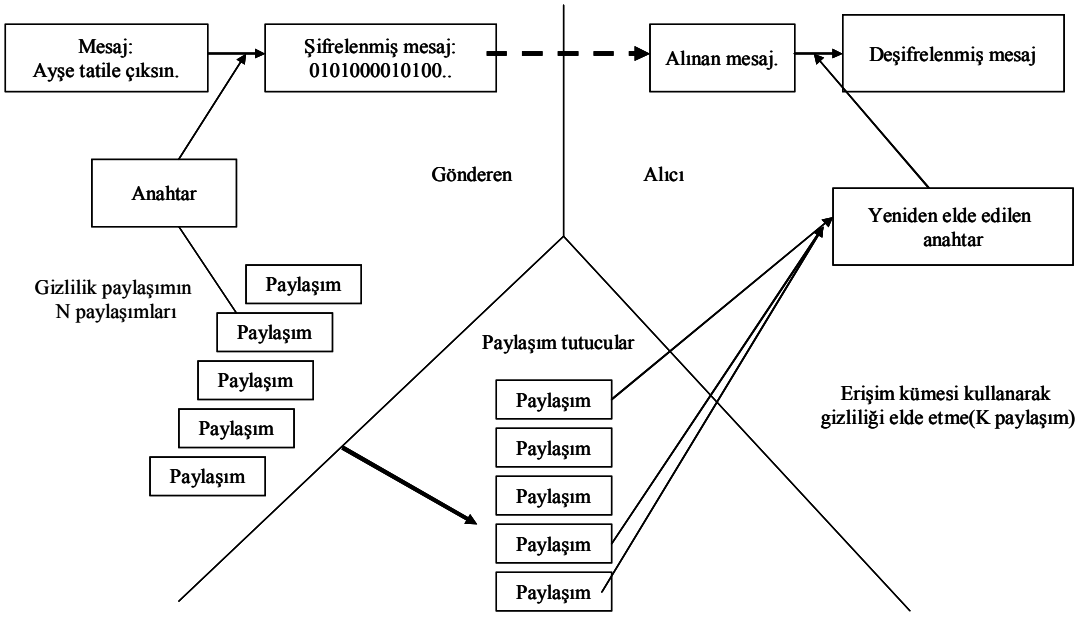
Gizlilik paylaşım şeması sonlu sayıda kişiler veya kuruluşlar arasında bir gizli bilgiyi paylaştırma yoludur. Ancak bu paylaşılan gizli bilgi eşik değerdeki alt kümeler ile yeniden elde edilebilir. Bu alt kümelerin oluşturduğu küme şemanın erişim yapısıdır.

Gizlilik paylaşımı anahtar yönetimi ve anahtar dağıtımı ile ilişkilidir. Bu anahtar dağıtım ve yönetim problemi bütün kriptosistemlerde oldukça sık rastlanan bir problemdir.

Tanım 4. 1. Bir gizlilik paylaşım şemasında D dağıtıcı ve $P_1,...,P_n$ katılımcılar olmak üzere aşağıdaki protokoller gerçekleştirilir.

- **Dağıtım:** D dağıtıcı s gizliliği $1 \le i \le n$ olmak üzere her P_i katılımcılarına s_i paylaşımlarını dağıtır.
- **Yeniden elde etme:** s gizliliği, s_i paylaşımlarının birleştirilmesi ile yeniden elde edilir. Burada $i \in A$ ve $A \subseteq \{P_1,...,P_n\}$ olmak üzere her yetkilendirilmiş katılımcıların kümesi ile gizlilik elde edilir.

Tanım 4. 2. $P_1,...,P_n$'nin bütün yetkilendirilmiş alt kümelerinin Γ ile gösterilen kümesi erişim yapısı olarak adlandırılır. Genellikle erişim yapısı Γ monotondur. Şöyleki: eğer $A \in \Gamma$ ve $A \subseteq B$ ve aynı zamanda $B \subseteq \Gamma$ ise bütün $A, B \subseteq \{P_1,...,P_n\}$ dir.



Şekil 4.1 Gizlilik Paylaşım tabanlı haberleşme şeması

Şekil 4.1. (Thibault ve Vincent, 2009) kaynağından alınmıştır.

Aşağıda gizlilik paylaşım şemasının güvenlik gereksinimleri vurgulanmıştır.

(i) Her yetkilendirilmiş katılımcılar kümesi paylaşımlarını birleştirerek *s* gizliliğini elde edebilirler.
(ii) Her yetkilendirilmemiş katılımcılar kümesi paylaşımlarını birleştirdiğinde *s* gizliliği hakkında hiçbir bilgiyi elde edemezler

Bu güvenlik gereksinimlerini doğrulayan Gizlilik Paylaşım Şeması mükemmel olarak adlandırılır.

Eşik kriptografi, (k,n) eşik gizlilik paylaşım şeması ile ilişkilendirildiğinde erişim yapısı $\Gamma = \{A \subseteq \{P_1,...,P_n\} : |A| \geq k\}, 1 \leq k \leq n$. (k,n) eşik şemasında, k katılımcının olduğu her grup gizliliği elde edebilir, fakat k-1 ve daha az katılımcı gizliliği elde edemez (Schoenmaker, 2011).

4.3. Shamir'in Lagrange İnterpolasyon Polinom Tabanlı Gizlilik Paylaşım Şeması

Shamir (Shamir, 1979) tarafından önerilen gizlilik paylaşımı için ilk şema polinom interpolasyon tabanlıdır. Bir (k,n) gizlilik paylaşımını elde etmek için, $p \rangle n$ büyük bir asal sayı ve Z_p sonlu bir cisim, k eşik değer ve $a_0 \in Z_p$ gizliliği göstersin. $a_1,...,a_{k-1} \in Z_p$ rastgele elemanları seçilip $k-1$ dereceli polinomu kurulur.

$$f(x) = (a_{k-1}x^{k-1} + ... + a_1 x + a_0) \in Z_p[\mathrm{x}] \qquad (4.1)$$

Paylaşım Kısmı:

Paylaşımlar aşağıdaki denklem ile elde edilir ve kullanıcılara dağıtılır.

$$h(x) \equiv (a_{k-1}x^{k-1} + ... + a_1 x + a_0) \bmod p \tag{4.2}$$

$y_i = h(x_i) \bmod p$ eşitsizliğine göre anahtar parçaları (x_i, y_i) şeklinde kullanıcılara dağıtılır. k noktası $k-1$ dereceli polinomu, $h(x)$ ve a_0 gizliliğini belirlemek için yeterlidir.

Gizliliği Yeniden Elde Edilmesi:

$h(x)$ lagrange polinomundan yeniden elde edilir. İlk olarak $l_k(x)$ polinomu şu şekilde tanımlanır.

$$l_t(x) = \prod_{\substack{i=1 \\ i \neq t}}^{k} \frac{x - x_i}{x_t - x_i} \bmod(p) \tag{4.3}$$

Lagrange interpolasyon polinomu:

$$p(x) = \sum_{t=1}^{k} y_t l_t(x) \tag{4.4}$$

$h(x)$ polinomunu ve gizli mesajı yeniden elde etmek için $p(x)$ polinomu hesaplanmalıdır (Denning, 1982) ; (Trappe ve Washington, 2006) ; (Zhu vd., 2005).

$$h(x) \equiv \sum_{t=1}^{k} y_t \prod_{\substack{j=1 \\ j \neq t}}^{k} \frac{x - x_j}{x_t - x_j} (\bmod p) \tag{4.5}$$

Örnek 4. 1.

(k,n)=(4,6) eşik şemasını kuralım. Şemada 6 katılımcı var ve bunlardan herhangi 4 tanesi gizliliği belirleyebilir. Ancak 3 kişi gizlilik hakkında hiçbir şey belirleyemez. Eşik değerimiz 4'tür.

Farzedelim ki s=13 sayısı gizliliğimiz olsun. Bu gizli bir kelime veya anahtar olabilir. p=17 asal bir sayı ve $a_1, a_2, a_3 \in Z_{17}$ rastgele olarak seçilsin. Aşağıdaki polinomdan

$$h(x) = (x^3 + 2x^2 + 3x + 13) \bmod 17$$

Bu polinomu kullanarak 6 paylaşımcıya (x,h(x)) anahtar parçası dağıtılsın.

$$h(1) = 19 \bmod 17 = 2$$
$$h(2) = 35 \bmod 17 = 1$$
$$h(3) = 67 \bmod 17 = 16$$
$$h(4) = 121 \bmod 17 = 2$$
$$h(5) = 203 \bmod 17 = 16$$
$$h(6) = 319 \bmod 17 = 13$$

(1,2), (2,1), (3,16), (4,2), (5,16), (6,13) Anahtar parçaları 6 paylaşımcıya ayrı ayrı dağıtılır.

Şimdi farzedelim ki 1, 2, 3 ve 4 paylaşımcıları gizliliği yeniden elde etmek için bir araya gelmek istesinler. Lagrange interpolasyon polinomunu kullanarak gizliliği elde etmeye çalışalım:

$$h(x) = [2\frac{(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + 1.\frac{(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} +$$
$$16\frac{(x-2)(x-1)(x-4)}{(3-2)(3-1)(3-4)} + 2\frac{(x-3)(x-2)(x-1)}{(4-3)(4-2)(4-1)}] \bmod 17$$

$$h(x) = [2.14(x-2)(x-3)(x-4) + 1.9(x-1)(x-3)(x-4)$$
$$+ 16.8(x-2)(x-1)(x-4) + 2.3(x-3)(x-2)(x-1)] \bmod 17$$

$$h(x) = [11(x-2)(x-3)(x-4) + 9(x-3)(x-2)(x-1)$$
$$+ 9(x-2)(x-1)(x-4) + 6(x-3)(x-2)(x-1)] \bmod 17$$

$$h(x) = [11(x^3 - 9x^2 + 26x - 24) + 9(x^3 - 8x^2 + 19x - 12)$$
$$+ 9(x^3 - 7x^2 + 14x - 8) + 6(x^3 - 6x^2 + 11x - 6)] \bmod 17$$

$$h(x) = [35x^3 - 270x^2 + 649x - 480] \bmod 17$$

$$h(x) = x^3 + 2x^2 + 3x + 13$$

Bu polinom görüldüğü gibi orijinal h(x) polinomudur. Ayrıca sabit terim olan 13 gizliliktir. Örnekte görüldüğü gibi 4 katılımcı kendi paylaşımlarını kullanarak gizliliği elde etmiş oldular (Arda vd., 2008).

4.4.Çin Kalan Teoremi Tabanlı Eşik Gizlilik Paylaşım Şemaları

Çin kalan teoremi tabanlı eşik gizlilik paylaşımı için birkaç çeşit şema önerilmiştir. Bu şemalar Mignotte (Mignotte, 1983) ve Asmuth-Bloom (Asmuth vd., 1983) tarafından bulunmuştur. Bu şemalarda Çin kalan teoremi boyunca özel bir sırada tam sayı dizileri kullanılır.

4.4.1. Asmuth-Bloom Gizlilik Paylaşım Şeması

Asmuth-Bloom gizlilik paylaşım şemasında gizliliği dağıtma ve yeniden elde etme işlemleri aşağıdaki gibi yapılmaktadır.

- ***Dağıtım İşlemleri****:* n kullanıcılı bir gurup arasında K gizliliğini paylaştırmak için dağıtıcı şu işlemleri yapar:

İkili guruplar halinde birbirlerine göre asal olan pozitif tamsayılar kümesinde m_0>K bir asal sayı olmak şartı ile $m_0 < m_1 < m_2 ..... < m_n$ olarak seçilmektedir. Bunun sonucunda da aşağıdaki eşitsizlik sağlanmaktadır.

$$\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1} \tag{4.6}$$

M, $\prod_{i=1}^{t} m_i$ 'yi göstersin. Daha sonra dağıtıcı aşağıdaki değeri hesaplar.

$$y = K + \alpha m_0 \tag{4.7}$$

Buradaki α , $0 \le y < M$ koşulunu sağlayan rastgele üretilmiş pozitif bir tamsayıdır. i. kullanıcının paylaşımları $1 \le i \le n$ aralığında, aşağıdaki denklemden elde edilir.

$$y_i = y \bmod m_i \tag{4.8}$$

- ***Birleştirme İşlemi:*** *t* kullanıcının gizliliği yeniden elde etmek için bir araya gelerek oluşturduğu küme *S* olsun. M_S, $\prod_{i \in S} m_i$ demektir.

Çin kalan teoremi kullanılarak $i \in S$ için Z_{M_S} 'deki y aşağıdaki denklem sistemi ile bulunur.

$$y \equiv y_i (\bmod m_i) \tag{4.9}$$

Gizlilik ise

$$K = y \bmod m_0 \tag{4.10}$$

ile bulunur.

Çin kalan teoremine göre *y*, Z_{M_S} 'de tek bir çözümdür. $y < M \le M_S$ olduğu için, çözüm aynı zamanda Z_M'de de tektir.

Asmuth-Bloom gizlilik paylaşım şemasında t'den daha az katılımcı birleşerek gizlilik hakkında hiçbir bilgi elde edemezler. Bundan dolayı bu şema mükemmele yakın bir şemadır. Anahtar adaylarının her biri gizliğe ulaşabilecek eşit güce sahip değildir (Kaya vd., 2007) ; (Iftene, 2007).

Örnek 4. 2. Çin Kalan Teoremi Tabanlı Asmuth- Bloom (t, n)=(4, 5) Gizlilik Paylaşım Şemasını Oluşturmak.

$2 \le t \le n$ şartını sağlayan (t, n)=(4, 5) gizlilik paylaşım şemasını kuralım. Asmuth-Bloom tarafından önerilen çin kalan teoremi tabanlı eşik şemaya göre özel bir sırada tamsayılar seçilir. Seçilen sayılar birbirlerine göre asal sayılardır. Paylaşımlar K gizli değerle ilişkili bir sayının denklik sınıflarıdır. Seçilen tam sayılar kümesi aşağıdaki şartları sağlamalıdır (Denning, 1982).

1. $m_0 \rangle K$
2. $\mathrm{m}_0 \langle m_1 \langle ... \langle m_n$
3. $\mathrm{ebob(p,m_i)} = 1, \mid \forall i$
4. $\mathrm{ebob(m_i}, m_j) = 1,\ \mathrm{i} \neq \mathrm{j}$ için
5. $\mathrm{m}_0 m_{n-t+2} .. m_n \langle m_1 .. m_t$

Buna göre sayıları şu şekilde seçelim.

$m_0 \langle m_1 \langle m_2 \langle m_3 \langle m_4 \langle m_5$
$11 \langle 13 \langle 17 \langle 19 \langle 21 \langle 23$

K=10 paylaşılacak gizlilik(anahtar) olsun.

M=$m_1.m_2.m_3.m_4$=13.17.19.21=88179 sayısı alınır. Ve $[0,(M/m_0)-1]$ oranında rastgele bir α sayısı seçilir. Buna göre $\alpha = 7$ alalım.

$K' = K + \alpha m_0$ formulü ile yeni anahtar elde edilir.

$K' = 10 + 7.11 = 87$

5 kişi arasında dağıtılan paylaşımlar şöyledir.

$$K_1 = K' \bmod m_1 = 87 \bmod 13 = 9$$
$$K_2 = K' \bmod m_2 = 87 \bmod 17 = 2$$
$$K_3 = K' \bmod m_3 = 87 \bmod 19 = 11$$
$$K_4 = K' \bmod m_4 = 87 \bmod 21 = 3$$
$$K_5 = K' \bmod m_5 = 87 \bmod 23 = 18$$

$$I_1 = (K_1, m_1) = (9,13)$$
$$I_2 = (K_2, m_2) = (2,17)$$
$$I_3 = (K_3, m_3) = (11,19)$$
$$I_4 = (K_4, m_4) = (3,21)$$
$$I_5 = (K_5, m_5) = (18,23)$$

bunlar 5 kullanıcı arasında dağıtılan anahtarlardır.

Şimdi K anahtarını eşik değerdeki kullanıcı ile yeniden elde etmeye çalışalım. Kullandığımız örnekte beş paylaşımdan rastgele seçilen dört paylaşımcı K gizli anahtarı yeniden elde edebilirler. Örneğin (I_1, I_2, I_3, I_4) kullanıcıları K'yı yeniden elde etmek istesinler.

$$x \equiv 9 \bmod 13$$
$$x \equiv 2 \bmod 17$$
$$x \equiv 11 \bmod 19$$
$$x \equiv 3 \bmod 21$$

Çin kalan teoremi standartları kullanılarak yukarıdaki denklik sisteminin çözümünden K' elde edilir. Bunun için öncelikle

$$y_1 = inv(M/m_1, m_1) = inv(88179/13,13) = 4$$
$$y_2 = inv(M/m_2, m_2) = inv(88179/17,17) = 9$$
$$y_3 = inv(M/m_3, m_3) = inv(88179/19,19) = 4$$
$$y_4 = inv(M/m_4, m_4) = inv(88179/21,21) = 20$$

Burada sayıların birbirlerine göre terslerinin hesaplanmasında genişletilmiş öklit algoritmasından faydalanılmıştır.

$$K' = \left[\frac{M}{m_1} y_1 K_1 + \frac{M}{m_2} y_2 K_2 + \frac{M}{m_3} y_3 K_3 + \frac{M}{m_4} y_4 K_4 \right] \bmod M$$
$$K' = 87$$

$K = K' - \alpha m_0 = 10$ olarak gizli anahtara ulaşılır (Arda ve Buluş, 2009).

4.5. Hata Doğrulama Kodları ve Gizlilik Paylaşımı

Shamir (Shamir,1979) ve Blakley (Blakley, 1979) 1979'da bağımsız olarak aşağıdaki durumları gerçekleyen gizlilik paylaşımı için (S,T) threshold (eşik) şeması olarak adlandırılan formülü geliştirmişlerdir.

(P1) Her T paylaşımlar gizliliği belirler,
(P2) Ancak T-1 veya birkaç paylaşım gizlilik hakkında hiçbir bilgiyi elde edemez.

Shamir GF(q) üzerinde T dereceli monik bir polinomda sabit terimi gizlilik olan ve diğer T-1 katsayıları rastgele seçilen $(1 \le T \le S \le q)$ (S,T) eşik şeması kurmuştur. S, paylaşımları GF(q)'nun sıfır olmayan ayrık değerlerinin bu polinomda aldığı değerlerdir. McEliece ve Sarwate(McEliece ve Sarwate, 1981) q^k kod kelimeleri ile n=S+1 blok uzunluklu q-dizili maksimum uzaklıkla ayrılabilen (MDS) kodlar açısından inşa edilen (S,T) eşik şemasının genelleştirilmiş formülünü vermiştir. Bu (n,k) MDS kodu minimum uzaklığı d=n-k+1olan q-dizili lineer bir koddur. x_1 gizliliği bir kod kelimesinin ilk değeridir. Paylaşım listeleri S=n-1 olan $[x_2,x_3,\ldots,x_n]$'dir. Bilgi kümesinden (n,k) MDS koddaki bir kod kelimesinin rastgele seçilebilen her 'k' bileşeni, gizli bileşeni elde edebilir. Bu (P1) özelliği T=k için doğrulanır. Ancak ilk x_1 bileşeni diğer $k-1$ bileşenlerle elde edilemez. Bu (P2) özelliğini doğrular. MDS kod bir Reed-Solomon kod olduğunda, bu (S,T) eşik şemasının McEliece- Sarwate inşası Shamir tarafından önerilen şemaya eşitlenebilir ve interpolasyon polinomu açısından formüle edilebilir (Massey, 1993) ; (Massey , 1995).

4.5.1.Erişim Yapıları

Bazen gizlilik paylaştırılırken bazı kullanıcıların diğerlerinden daha fazla erişim ayrıcalığına sahip olması istenir. Örneğin, farz edelim Ali bankanın müdürü, Barış, Can ve Deniz banka memuru olsun. Ali herhangi bir banka memuru ile birlikte gizliliğe erişebilir ancak diğer banka memurları Ali olmadan gizliliğe erişemezler. Yukarıdaki durumdaki gibi gizliliği belirleyebilen bütün paylaşım kümelerinden oluşan gizlilik paylaşım şemalarının erişim yapılarının bir tanımı olabilir. Burada yetkili olmayan kullanıcılar içeren alt kümeler gizliliği belirleyemezler. Mesela aşağıdaki paylaşım kümelerinden oluşan erişim yapıları {A,B}, {A,C} ve {A,D} olsun. Buradaki A,B,C ve D sırasıyla Ali, Barış, Can ve Deniz için paylaşımları göstermektedir. Bu gizlilik paylaşımı için (S,Γ) erişim yapısı olarak tanımlanır. Bu yapı için gizlilik, aşağıdaki durumlarda S paylaşımlar içine dönüştürülebilir:

(P3) Γ 'de bulunan her kümedeki paylaşım bilgileri gizliliği belirleyebilir ancak,

(P4) Γ 'de bulunmayan bir kümedeki paylaşım bilgileri gizlilik hakkında hiçbir bilgiyi ortaya çıkaramaz. (Massey, 1995).

BÖLÜM 5

5. REED-SOLOMON KODLAR

5.1. Reed Solomon Kodlarının Tanımı

Reed- Solomon (RS) kodları ikili olmayan BCH kodlarının bir alt kümesidir. RS kodları çevrimsel kodlardır. Reed ve Solomon tarafından 1960 yılında tanımlanmıştır. RS kodları sabit *k* ve *n* değerleri için en yüksek minimum Hamming uzaklığa sahiptir.

İkili BCH kodları, ikili olmayan kodlara genelleştirilebilir. *p* bir asal sayı, *q*, *p*'nin bir kuvveti, *s* ve *t* herhangi iki tamsayı olmak üzere, blok uzunluğu $n = q^s - 1$, parite kontrol sembolü sayısı, $n - k = 2st$ olan bir ikili olmayan BCH kodu vardır. Bu kod, $2st$ parite kontrol sembolü yardımıyla, *t* veya daha az sayıda hatalı sembolü düzeltme yeteneğine sahiptir. İkili BCH kodlarının üreteç polinomunun katsayıları GF(2)'nin elemanı iken, ikili olmayan BCH kodunun üreteç polinomunun katsayıları $GF(q^s)$'in elemanıdır. Üreteç polinomunun kökleri ise $\alpha, \alpha^2, ..., \alpha^{2t}$'dir. $\phi_i(X)$ α^i'nin minimal polinomu olmak üzere üreteç polinom,

$$g(X) = OKEK\{\phi_1(X), \phi_2(X), ... \phi_{2t}(X)\} \qquad (5.1)$$

ile verilir. Her bir minimal polinomun derecesi s veya daha azdır. Bu nedenle $g(X)$'in derecesi $2st$ olabilir. dolayısıyla $g(X)$ tarafından üretilen kod $2st$ parite kontrol sembolü içerir.

RS kodları, ikili olmayan BCH kodları içinde $s = l$ alınarak elde edilir, t hata düzelten RS kodunun parametreleri,

Blok uzunluğu : $n = q - 1$
Parite kontrol bit sayısı : $n - k = 2t$
Minimum uzaklık : $d_{\min} = 2t + 1$

olarak verilir. RS kodlarının önemli bir özelliği minimum Hamming uzaklığının her zaman parite kontrol sembolü sayısından bir fazla olmasıdır. α^i GF(q = p^m) 'in sıfırdan farklı bir ilkel elemanı ve $\phi(X)$ 'in bir kökü olmak üzere t hata düzelten doğrusal, dairesel(cyclic) ve blok kod olan RS kodunun üreteç polinomu,

$$\begin{aligned} g(X) &= (x+\alpha)(x+\alpha^2)....(x+\alpha^{2t}) \\ &= g_0 + g_1 x + g_2 x^2 + ... + g_{2t-1} x^{2t-1} + x^{2t} \end{aligned} \tag{5.2}$$

ile verilir. g_i 'ler $GF(q = p^m)$ 'nin elemanıdır ve $\alpha, \alpha^2, ..., \alpha^{2t}$, $g(X)$ 'in kökleridir. $g(X)$ 'in derecesi en fazla $2t$ 'dir. $g(X)$ tarafından üretilen kod $(n, n-2t)$ kodudur (Zorlu , 2006) ; (Moreira ve Farrell, 2006).

Örnek 5. 1: $GF(2^4)$ üzerinde üç hata düzelten (15,9) RS kodu için üreteç polinomu,

$$\begin{aligned} g(X) &= (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6) \\ &= \alpha^6 + \alpha^9 x + \alpha^6 x^2 + \alpha^4 x^3 + \alpha^{14} x^4 + \alpha^{10} x^5 + x^6 \end{aligned}$$

kullanılır.

5.2. Kodlama

$k = n - 2t$ olmak üzere, kodlanacak mesaj polinomu,

$$m(x) = m_0 + m_1 x + ... + m_{k-1} x^{k-1} \tag{5.3}$$

olsun. RS kod sözcükleri k sembollük mesaj polinomu $m(x)$ 'in $g(x)$ üreteç polinomu ile çarpılması sonucu elde edilebilir; fakat elde edilen kod sözcük sistemik halde olmayacaktır. Sadece $GF(q)$ içinde $g(x)$ 'e tam olarak bölünen sözcükler RS

kod sözcükleri olabileceği dikkate alınırsa kodlama, bir bölme işlemi ile gerçekleştirilebilir. $m(x)$ polinomu, x^{n-k} ile çarpılıp $g(x)$'e bölünsün. Bölümden kalan $p(x)$, $x^{n-k}m(x)$ ifadesine eklenirse elde edilecek polinom $g(x)$'e tam olarak bölünebilir ve bu polinomla ifade edilen kod sözcük $v(x)$ sistematik haldedir.

5.3. Kod Çözme

Bu bölümde RS kodlarının çözümü için kullanılan yöntemler açıklanacaktır. Doğrusal blok kodlarında ve ikili BCH kodlarında kod çözme işlemine hata belirtecinin hesabı ile başlanır. Hata belirtecinin hesabının ardından hata yerleri bulunur ve hatalı bitler düzeltilir. Ikili olmayan BCH kodlarında dolayısıyla RS kodlarında da kod çözme işleminin ilk adımı hata belirteci hesabıdır, fakat hata yerleri bulunduktan sonra ikili kodlardan farklı olarak hata değerlerinin de bulunması gerekir. Çünkü RS kodları bitler üzerinde değil bir kaç bitten oluşan sözcükler üzerinde çalışır. RS kodlarının çözümünde izlenecek adımlar aşağıdaki gibidir.

1. Hata belirteçlerinin hesabı
2. Hata yeri polinomu $s(X)$'in bulunması
3. $s(X)$'in kökleri olan hata yerlerinin bulunması (Chine araştırması)
4. Hata değerlerinin hesaplanması (Forney algoritması)
5. Hatalı sözcüklerin düzeltilmesi

Hata belirteçlerinin hesabında tek bir yöntem kullanılırken hata yeri polinomunun belirlenmesinde bir kaç yöntem kullanılabilir. Bu bölümde her bir yöntem örneklerle incelenecektir (Zorlu, 2006).

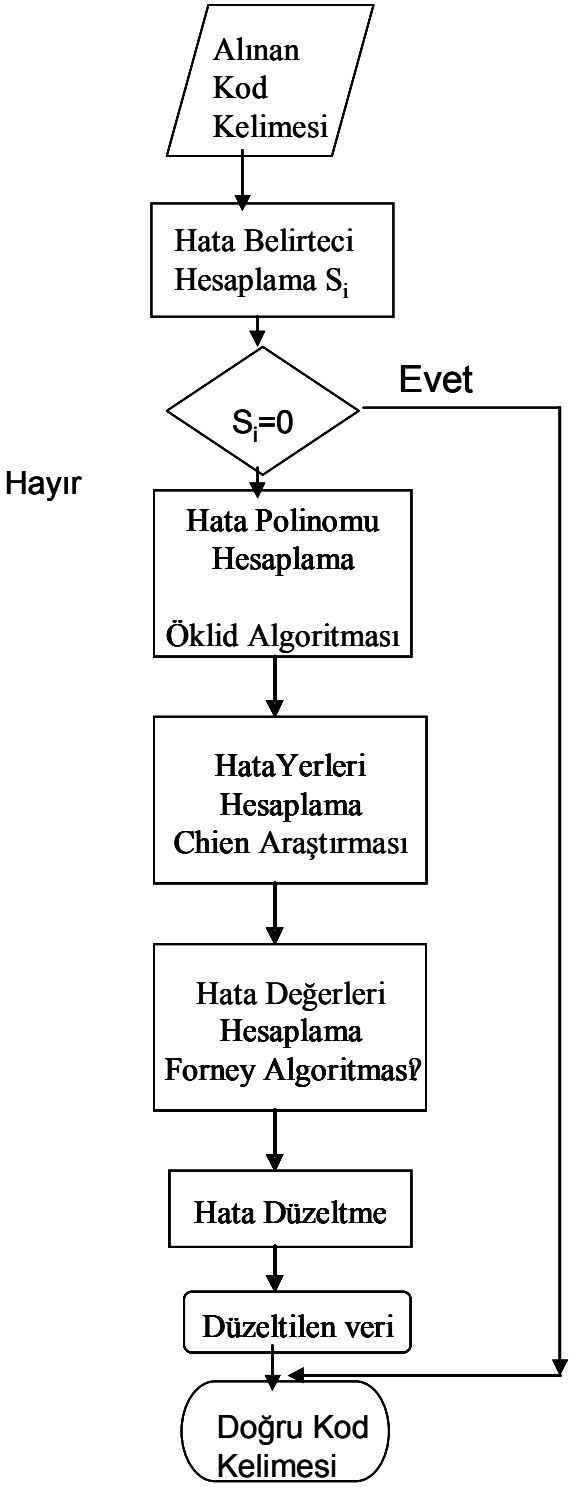
5.3.1. Hata Belirteci Hesabı

Gönderilen kod sözcük $v(x)$, alınan sözcük $r(x)$ olmak üzere kanal tarafından üretilen gürültü $e(x)$,

$$\begin{aligned} v(x) &= v_0 + v_1 x + \ldots\ldots\ldots + v_{n-1} x^{n-1} \\ r(x) &= r_0 + r_1 x + \ldots\ldots\ldots + r_{n-1} x^{n-1} \\ e(x) &= r(x) + v(x) = e_0 + e_1 x + \ldots\ldots\ldots + e_{n-1} x^{n-1} \end{aligned} \qquad (5.4)$$

olarak tanımlanır.

Aşağıda Şekil 5.1'de RS kod çözücü devrenin akış şeması verilmektedir.



Şekil 5.1. Reed-Solomon kod çözme diyagramı

Hata sözcüğü $e(X), X^{j1}, X^{j2}, ..., X^{jv}$, olmak üzere toplam v yerde hata üretmiş ise $0 \le j_1 \le n-1$ olmak üzere, hata polinomu,

$$e(X) = e_{j_1} X^{j_1} + e_{j_2} X^{j_2} + ... + e_{j_v} X^{j_v} \tag{5.5}$$

olarak bulunur. Hatanın düzeltilebilmesi için hata yerleri X^{j_i} 'ler ve hata değerleri e_{j_i} 'ler bilinmelidir. $l = 1,2,....,v$ olmak üzere,

$$\beta_l = \alpha^{j_l} \tag{5.6}$$

tanımlanır ise hata belirteçleri 5.7 eşitlikleriyle hesaplanabilir.

$$\begin{aligned} S_1 &= r(\alpha) = e_{j_1}\beta_1 + e_{j_2}\beta_2 + ...e_{jv}\beta_v \\ S_2 &= r(\alpha^2) = e_{j_1}\beta_1^{\,2} + e_{j_2}\beta_2^{\,2} + ...e_{jv}\beta_v^{\,2} \\ &.. \\ &.. \\ S_{2t} &= r(\alpha^{2t}) = e_{j_1}\beta_1^{\,2t} + e_{j_2}\beta_2^{\,2t} + ...e_{jv}\beta_v^{\,2t} \end{aligned} \tag{5.7}$$

alınan sözcükte t hata varsa 5.7 eşitlikleri 5.8 ile ifade edilebilir.

5.7 eşitliklerinde görüldüğü gibi sendromlar, üretici polinomun kökleri için hata polinomunun aldığı değerlerdir.

Sendromların oluşturduğu polinom 5.8'de verilmiştir.

$$S_k = \sum_{i=1}^{t} e_{j_i} \beta_i^k \tag{5.8}$$

5.7 eşitliklerinde görüldüğü gibi sendromlar, üretici polinomun kökleri için hata polinomunun aldığı değerdir.

Kod çözme işleminin amacı 5.8 ile verilen hata belirteçlerini üreten maksimum t hatadan oluşan hata dizisini bulmaktır (Zorlu , 2006).

5.3.2. Hata Yeri Polinomunu Tespit Etmek İçin Kullanılan Yöntemler

5.3.2.1. Reed Solomon Kodların Sendrom Dekodlaması

Diyelim ki verinin gürültülü kanaldan iletimi esnasında bazı bileşenleri bozuldu ve hatalı iletildi. Bu durumda hataların düzeltilmesi gerekir. Bu aşamada aşağıdaki sıra izlenmektedir.

Sendrom dekodlamayı (7, 3, 5 ;8) MDS kod üzerinde uygulayalım. Alınan vektör $w = (1, \alpha, 0, \alpha, \alpha^6, 1, 0)$ olsun. Varsayalım e=2 hata var.

Öncelikle hata olup olmadığını tespit etmek için alınan kod söz kontrol matrisinin transpozesi ile çarpılır ve sonuç sıfır değilse hata var demektir.

$$w.H^T = 0 \Rightarrow hata\ yok$$
$$w.H^T \neq 0 \Rightarrow hata\ \text{var}$$

Örneğimizde alınan vektör $w.H^T = (\alpha^3, 1, 1, \alpha^4) \neq 0$ olduğu için hata vardır. Şimdi iletilen doğru kod sözü bulmaya çalışalım.

1- Sendrom hesaplama.
Sendrom polinomu $w(x) = 1 + \alpha x + \alpha x^3 + \alpha^6 x^4 + x^5$

Sendrom polinomundan $s_0, s_1, ..., s_{e-1}$ sendromları hesaplanır.

$s_0 = w(\alpha^0) = w(1) = \alpha^6$

$s_1 = w(\alpha) = \alpha^5$

$s_2 = w(\alpha^2) = 1$

$s_3 = w(\alpha^3) = 0$

2- Hata yeri bulma

$$\begin{pmatrix} s_0 & s_1 & \ldots s_{e-1} \\ s_1 & s_2 & \ldots . s_e \\ . & . & . \\ . & & \\ s_{e-1} & s_e & \ldots . s_{2e-2} \end{pmatrix} \begin{pmatrix} \sigma_0 \\ \sigma_1 \\ . \\ . \\ \sigma_{e-1} \end{pmatrix} = \begin{pmatrix} s_e \\ s_{e-1} \\ . \\ . \\ . \\ . \\ . \\ s_{2e-1} \end{pmatrix} \qquad (5.9)$$

5.9 denkleminden hatalı olan bileşenin yerleri tespit edilir.

Örneğimize göre çözelim.

$$\begin{pmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & 1 \end{pmatrix} \begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \Rightarrow \sigma_0 = \alpha^3 \text{ ve } \sigma_1 = \alpha$$

Hata yeri polinomu 5.10 denklem ile gösterilmiştir.

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + \ldots + x^e \qquad (5.10)$$

$\sigma_A(x) = (x - a_1).....(x - a_e)$ formunda düzenlenip $a_1, \ldots, a_e$ bulunur. Bunlar oluşan hataların yerlerini gösterir.

Bu durumda hata yeri polinomu,

$\sigma_A(x) = \alpha^3 + \alpha x + x^2 = (x-1)(x-\alpha^3)$

$a_1 = 1,\ a_2 = \alpha^3$ hata yerleri bulunur.

3. Hatalı olan bileşenler 5.11 denklemi ile düzeltilir.

$$\begin{pmatrix} a_1^0 & a_2^0 & \dots & a_e^0 \\ a_1^1 & a_2^1 & \dots & a_e^1 \\ . & & & \\ . & & & \\ a_1^{e-1} & a_2^{e-1} & \dots & a_e^{e-1} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_e \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \\ \\ s_{e-1} \end{pmatrix} \tag{5.11}$$

$$\begin{pmatrix} a_1^0 & a_2^0 \\ a_1^1 & a_2^1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & \alpha^3 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} \alpha^6 \\ \alpha^5 \end{pmatrix}$$

Denklem sistemi çözümünden

$b_1 = \alpha^2$ ve $b_2 = 1$ elde edilir.

$\alpha^0 = 1$ ve α^3 yerlerinde hata oluşmuştu.

$a_1 = 1$ yerine $b_1 = \alpha^2$
$a_2 = \alpha^3$ yerine $b_2 = 1$ ile düzeltilir.

Alınan vektör $w = (1, \alpha, 0, \alpha, \alpha^6, 1, 0)$

Hata vektörü $e = (\alpha^0, 0, 0, \alpha^3, 0, 0, 0)$
$e = (\alpha^2, 0, 0, 1, 0, 0, 0)$ düzeltilip "w" ile XOR işlemi yapıldığında doğru kod sözcüğüne ulaşılır (Bruen ve Forcinito, 2005).

$$c = w \oplus e = (1, \alpha, 0, \alpha, \alpha^6, 1, 0) \oplus (\alpha^2, 0, 0, 1, 0, 0, 0) = (\alpha^6, \alpha, 0, \alpha^3, \alpha^6, 1, 0)$$

5.3.2.2 RS Kodların Öklid Algoritması Kullanarak Çözülmesi

RS kodlarının çözümünde Öklid (Euclid) yöntemi de kullanılabilir. Öklid yöntemi, *A* ve *B* olarak verilen herhangi iki tamsayı veya polinomun ortak bölenlerinin en büyüğü (OBEB), *C*'yi verir. Ayrıca *C=SA+TB* eşitliğini sağlayan *S* ve *T* tamsayıları veya polinomlarını da bulur. Anahtar eşitliği 5.12 biçimde ifade edilirse öklid yöntemiyle $\sigma(X)$ ve $W(X)$ polinomları bulunabilir.

$$\sigma(X)S(X) - \mu(X)X^{n-k} = -W(X) \tag{5.12}$$

Bu algoritma X^{n-k} ve $S(X)$ polinomlarına uygulanmakta ve böylece i. tekrarda 5.13 eşitliği elde edilir.

$$r_i(X) = s_i(X)X^{n-k} + t_i(X)S(X) \tag{5.13}$$

İşlemler 5.14'de verilen koşula kadar devam eder.

$$\deg\{r_i(X)\} \le \left[\frac{n-k}{2}\right] + 1 \tag{5.14}$$

Diğer yandan bölme işlemlerinin sonucunda elde edilen 5.15.'deki polinomları birinci dereceden polinoma dönüştürmek için GF(q) cisminin bir elemanı olan λ sabiti ile çarpılır (Moreira ve Farrell, 2006).

$$\begin{aligned} W(X) &= -\lambda r_i(X) \\ \sigma(X) &= \lambda t_i(X) \end{aligned} \tag{5.15}$$

Örnek 5. 2. $p(x) = 1 + x^2 + x^3$ ilkel polinomu ile üretilen $GF(2^3)$ üzerinde tanımlanmış $C_{RS}(7,3)$ RS kodu için alınan vektör $r = (000\ 000\ 011\ 000\ 111\ 000\ 000)$ olsun. Hata polinomunu ve çözülmüş vektörü öklid algoritmasını kullanarak belirleyelim.

Alınan vektörün polinomsal ifadesi aşağıdaki gibidir.

$$r(x) = \alpha^6 x^2 + \alpha^4 x^4$$

Sendrom vektörünün bileşenleri hesaplanır.

$$s_1 = r(\alpha) = \alpha + \alpha = 0$$
$$s_2 = r(\alpha^2) = \alpha^6$$
$$s_3 = r(\alpha^3) = \alpha^4$$
$$s_4 = r(\alpha^4) = \alpha^4$$

Daha sonra sendrom polinomu belirlenir.

$$S(X) = \alpha^6 X + \alpha^4 X^2 + \alpha^4 X^3$$

Öklid algoritması Tablo5.1 kullanılarak uygulanmıştır.

i	$r_i = r_{i-2} - q_i r_{i-1}$	q_i	$t_i = t_{i-2} - q_i t_{i-1}$
-1	$X^{n-k} = X^4$		0
0	$S(X) = \alpha^4 X^3 + \alpha^4 X^2 + \alpha^6 X$		1
1	$\alpha^3 x^2 + \alpha^2 x$	$\alpha^3 x + \alpha^3$	$\alpha^3 x + \alpha^3$
2	$\alpha^4 x$	$\alpha\ x + \alpha^5$	$\alpha^4 x^2 + \alpha^3 x + \alpha^5$

Tablo 5. 1. Anahtar denklemini çözmek için Öklid algoritması

Burada

$$W_1(x) = \alpha^4$$
$$\sigma_1(x) = \alpha^4 x^2 + \alpha^3 x + \alpha^5$$

$\sigma_1(x)$ polinomunu birinci dereceden polinoma dönüştürmek için $GF(2^3)$ Galois cisminin $\lambda = \alpha^3$ elemanıyla çarpılır. Böylece

$$W(x) = x$$
$$\sigma(x) = x^2 + \alpha^6 x + \alpha$$

elde edilir.

Chien araştırması ile hata yeri polinomundan hatalı olan yerler tespit edilir. Yani $\sigma(x)$ denkleminde x yerine $GF(2^3)$ Galois cisminin tüm elemanları yazıldığında sıfır eşitliğini sağlayan elemanlar hata yerlerini göstermektedir.
Bu yerler α^3, α^5'tür. Böylece

$$\alpha^3 = \alpha^{-j1} = \alpha^{-4} \Rightarrow j_1 = 4$$
$$\alpha^5 = \alpha^{-j2} = \alpha^{-2} \Rightarrow j_2 = 2$$

Hatalar $j_1 = 4$ ve $j_2 = 2$ pozisyonlarındaki yerlerdedir. Hata yeri polinomunun türevi

$\sigma'(X) = \alpha^6$ dir.

Böylece hata değerleri

$$e_{j1} = \frac{W(\alpha^{-j1})}{\sigma'(\alpha^{-j1})} = \frac{W(\alpha^3)}{\sigma'(\alpha^3)} = \frac{\alpha^3}{\alpha^6} = \alpha^{-3} = \alpha^4$$
$$e_{j2} = \frac{W(\alpha^{-j2})}{\sigma'(\alpha^{-j2})} = \frac{W(\alpha^5)}{\sigma'(\alpha^5)} = \frac{\alpha^5}{\alpha^6} = \alpha^{-1} = \alpha^6$$

Hata polinomu

$$e(x) = \alpha^6 x^2 + \alpha^4 x^4$$

elde edilir. Daha sonra alınan vektöre hata polinomu eklenerek doğrulanmış olur (Moreira ve Farrell, 2006).

5.4. Chien Araştırması

Hata yeri belirleyici polinomun katsayıları bulunduktan sonra, yapılacak işlem köklerinin bulunmasıdır. Bunun için Chien araştırma yöntemi kullanılır (Chien, 1964). Bu yöntemde amaç hata yeri polinomunu sıfır yapan sonlu cisim elemanlarını bulmaktır. Hata yerleri de bulunan kökün sonlu cisimde tersi olan elemanlardır (Galstad, 2009).

Örnek 5. 2'de (7,3) kodunda,

$\alpha^3 = \alpha^{-j1} = \alpha^{-4} \Rightarrow j_1 = 4$

$\alpha^5 = \alpha^{-j2} = \alpha^{-2} \Rightarrow j_2 = 2$

Olarak hata yerleri $j_1 = 4$ ve $j_2 = 2$ olarak tespit edilir.

5.5. Forney Algoritması

Forney algoritması aşağıdaki denklemi kullanarak hatalı olan yerlerdeki hata değerlerinin çözümü için tasarlanmış bir algoritmadır (Galstad, 2009).

$$e_{i_k} = \frac{W(\alpha_k^{-1})}{\sigma'(\alpha_k^{-1})} \tag{5.16}$$

Örnek 5. 2'de (7,3) kodu için hata değerleri şöyledir.

$$e_{j1} = \frac{W(\alpha^{-j1})}{\sigma'(\alpha^{-j1})} = \frac{W(\alpha^3)}{\sigma'(\alpha^3)} = \frac{\alpha^3}{\alpha^6} = \alpha^{-3} = \alpha^4$$

$$e_{j2} = \frac{W(\alpha^{-j2})}{\sigma'(\alpha^{-j2})} = \frac{W(\alpha^5)}{\sigma'(\alpha^5)} = \frac{\alpha^5}{\alpha^6} = \alpha^{-1} = \alpha^6$$

BÖLÜM 6

6. MDS KODLAR

MDS (Maksimum Uzaklıkla Ayrılabilen) kodlar hata kontrol kodlarının önemli bir sınıfıdır. Bu kodlar birçok özelliğe sahiptir. En önemlileri arasında GF(q) sonlu cisim üzerinde (n, k, d) MDS kodu için minimum hamming mesafesi d= n-k+1 olan Singleton sınırına sahip olmasıdır. Bu özelliğinden dolayı hata kontrol yeteneği açısından optimaldir. MDS kodların hata tespit edebilen ve düzeltebilen hata sembollerinin sayısı diğer kodlardan daha fazladır. Bu sebepten ötürü veri iletimi için depolama sistemlerinde ve iletişim sistemlerinde oldukça sık kullanılmaktadır.

Önerme 6.1 (Singleton Sınırı): C bir [n,k,d] kod ise, $k + d \leq n + 1$ 'dir. Minimum hamming mesafesi $d = n - k + 1$ olan (n, k, d) kodları (MDS) maksimum uzaklıkla ayrılabilen kodlar olarak adlandırılır. Kodlama teorisindeki önemli kodlardan birisi de maksimum uzaklıkla ayrılabilen kodlardır. Çünkü bu tür kodlar, n ve k verildiğinde d'si (dolayısıyla, düzeltilebilme kapasitesi) en fazla olan kodlardır.

Örneğin minimum uzaklığı 3 olan (4,2) ternary (yani elemanları {0,1,2}'den oluşan) Hamming kod bir MDS koddur.

6.1.MDS Kodların Özellikleri

Önerme 6.2. d uzaklığına sahip bir C lineer kodunun H kontrol matrisinin her d-1 sütunları lineer bağımsızdır.

Tanımlandığı gibi bir MDS kod n-k+1 uzaklığa sahiptir. Böylece, kontrol matrisinin her n-k sütunlarının kümesi lineer bağımsızdır (Pieprzyk ve Zhang, 2004).

Önerme 6. 3. A'nın her kare alt matrisi nonsingular($\det \neq 0$) ise aşağıdaki G üreteç matrisi ile bir (n, k, d) kodu MDS koddur.

$$G = [I_{kxk} A_{kx(n-k)}]$$

Bu üreteç matrisinin her k sütunu lineer bağımsızdır.
MDS kodların en iyi bilinen sınıfı Reed-Solomon kodlardır (Pieprzyk ve Zhang, 2004).

Önerme 6.4. Eğer C bir MDS kod ise onun dual kodu olan (n, n-k, k+1)$_q$ $C^{\perp}$ 'da bir MDS koddur (Pieprzyk ve Zhang, 2004).

Önerme 6.5: (Mükemmel Eşik Şemalar ve MDS kodlar) Eğer gizlilik, $[v_1, v_2, ..., v_n]$ n uzunluklu q-dizili bir kod sözünün ilk değeri olarak alınırsa ve sonraki k-1 değerleri rastgele seçilirse, son n-k değerler hesaplanırsa, $[v_1, v_2, ..., v_n]$ q-dizili (n, k) lineer MDS kodunda bir kod sözcüğüdür. $[v_2, ..., v_n]$ paylaşımlar olmak üzere bu (n, k) MDS kod (N=n-1, T=k) mükemmel eşik gizlilik paylaşım şemasını oluşturur (Massey, 2001).

6.2. MDS Kod Tabanlı Gizlilik Paylaşım Şeması

G üreteç matrisi açıktır. Ancak bilgi vektörü dağıtıcı tarafından gizli olarak seçilir. Burada $s' \in GF(q)$ gizliliği göstersin. $g_0 = (g_{00}, g_{10}, ..., g_{k-1,0})^T$, G üreteç matrisinin ilk sütunu olsun. $s = (s_0, s_1, ..., s_{k-1})$, $GF(q^k)$' da seçilmiş bir bilgi vektörüdür. Burada $s' = sg_0 = \sum_{i=0}^{k-1} s_i g_{i0}$ s bilgi vektörünün sorumlu olduğu kod söz $t = (t_0, t_1, ...t_{n-1}) = sG$ dir. Her P_i paylaşımcılarına t_i bilgileri paylaştırılır. İlk bileşen olan $t_0 = s'$, t kod sözünün gizli bileşenidir.

Bu yapıyı bir örnek üzerinde açıklayalım. $GF(3)$ üzerinde bir lineer C $[n+1, k, d] = [4,2,3]$ ternary Hamming kod olan MDS kodunu alalım. S=n, T=k olan (T,S) yani (2,3) eşik gizlilik paylaşım şemasını belirler.

Bu kod için bilgi vektörleri k=2 olduğu için $s = [s_0, s_1]$ 2 uzunluğunda elemanları $GF(3)$' te olan bir vektördür. Örneğin seçilen bilgi vektörü $s = [2,2]$ olsun. Bu bilgi vektörünün sorumlu olduğu kod söz,

$$t = (t_0, t_1, t_2, t_3) = sG = [22]\begin{bmatrix} 1012 \\ 0111 \end{bmatrix} = [2210]$$

Burada gizlilik t kod sözünün $t_0 = 2$ olan ilk bileşenidir. Diğer bileşenler ise P_1=2, P_2=1, P_3=0 olarak paylaşımcılara dağıtılır. Paylaşımlar kümesi $t_{i_1}, t_{i_2}, ..., t_{i_m}$ ile belirlenir. O halde paylaşımlar kümesi $S = \{P_1, P_2, P_3\}$'tür. Burada $1 \le i_1 \langle i_2 \langle ... \langle i_m \le n$ ve $m \le n$ olmak koşulu ile bu paylaşımlar kümesi t_0 gizli bileşeni belirleyebilir..

Gizliliği hesaplamak oldukça kolaydır. $g_0 = \sum_{j=1}^{m} x_j g_{i_j}$ denklem sistemi

çözülerek x_j bilinmeyenleri bulunur ve daha sonra gizlilik $t_0 = sg_0 = \sum_{j=1}^{m} x_j sg_{i_j} = \sum_{j=1}^{m} x_j t_{i_j}$ denklem sisteminin çözümünden elde edilir (Özadam vd., 2007) ; (Xiaoqing ve Zhiguo, 2004).

Örneğe tekrar dönüldüğünde MDS kodunun boyutu k=2 olduğu için erişim kümesi en az 2 paylaşımcıdan oluşmak zorundadır. O halde T=2 olmalıdır. İki paylaşımcıdan daha az paylaşımcı gizli bileşeni yeniden elde edemez.

$$\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_2 P_3\}\}$$

Minimum erişim kümeleri kullanılarak gizli bileşene ulaşılır.

$\{P_1, P_2\}$ erişim kümesi kullanılarak gizli bileşeni elde edelim. Öncelikle aşağıdaki denklem sisteminden x_i bilinmeyenleri bulunur

$$g_0 = \sum_{j=1}^{m} x_j g_{i_j} = \sum_{j=1}^{2} x_j g_j = x_1 g_1 + x_2 g_2$$

$$g_0 = x_1 g_1 + x_2 g_2$$
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = x_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + x_2 \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$
$$1 = 0 + x_2 \Rightarrow x_2 = 1$$
$$0 = x_1 + x_2 \Rightarrow 0 = x_1 + 1 \Rightarrow x_1 = 2$$

$$t_0 = x_1 P_1 + x_2 P_2$$
$$t_0 = 2.2 + 1.1$$
$$t_0 = 1 + 1 = 2$$

$t_0 = 2$ gizli bileşene ulaşılır.

$\{P_1, P_3\}$ erişim kümesi kullanılarak gizli bileşeni elde etmeye çalışalım.

$$g_0 = x_1 g_1 + x_3 g_3$$
$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = x_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix} + x_3 \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$
$$1 = 0 + 2x_3 \Rightarrow x_3 = 2$$
$$0 = x_1 + x_3 \Rightarrow 0 = x_1 + 2 \Rightarrow x_1 = 1$$

$t_0 = x_1 P_1 + x_3 P_3$

$t_0 = 1.2 + 2.0$

$t_0 = 2$

{P_2,P_3} erişim kümesi kullanılarak gizli bileşeni elde etmeye çalışalım

$g_0 = x_2 g_2 + x_3 g_3$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = x_2 \begin{bmatrix} 1 \\ 1 \end{bmatrix} + x_3 \begin{bmatrix} 2 \\ 1 \end{bmatrix}$$

$1 = x_2 + 2x_3 \Rightarrow x_3 = 1, x_2 = 2$

$0 = x_2 + x_3 \Rightarrow$

$t_0 = x_2 P_2 + x_3 P_3$

$t_0 = 2.1 + 1.0$

$t_0 = 2$

Gözlemlendiği gibi en az iki katılımcının paylaşımları kullanılarak gizli bileşen elde edilebilmektedir. İkiden az katılımcının olduğu durumda gizli bileşeni elde etmek mümkün değildir. Bu bize $(n+1, k) = (4,2)$ ve minimum uzaklığı $d = 3$ olan MDS kod ile $(k, n) = (2,3)$ bir Shamir Eşik Gizlilik Paylaşım şeması kurulabildiğini göstermektedir. Bu şema mükemmel olarak adlandırılır (Arda vd., 2010)

BÖLÜM 7

7. LAGRANGE İNTERPOLASYON TABANLI GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI

NetBeans.IDE 6.9.1 java kodu ile gerçekleştirilen lagrange interpolasyon tabanlı birkaç gizlilik paylaşım şemaları sonuçları aşağıda verilmiştir (Wagner, 2003).

(k,n) = (4,10) Eşik Şeması Uygulaması ve Sonuçları

Paylaşım Kısmı

P=997(asal sayı)	S=125(gizlilik)
$f(x) = 125 + 796x + 24x^2 + 682x^3$	
$1 \le i \le n$	$f(i)$paylasim gizli degerleri
1	630
2	290
3	206
4	482
5	225
6	536
7	522
8	287
9	932
10	567

Tablo 7. 1. (4,10) Eşik Şemanın Paylaşım Değerleri

Gizliliğin Yeniden Elde Edilmesi

P=997(asal sayı)	
k (eşik değer)	$f(i)$paylasim gizli degerleri
1	630
4	482
6	536
10	567
S=125(gizlilik elde edildi)	

Tablo 7. 2 (4,10) Eşik Şemanın k=4 eşik değer ile gizliliğin elde edilmesi

(k,n) = (8,20) Eşik Şeması Uygulaması ve Sonuçları

Paylaşım Kısmı

P=991(asal sayı)	S=458(gizlilik)
$f(x) = 458 + 733x + 87x^2 + 293x^3 + 395x^4 + 239x^5 + 914x^6 + 24x^7$	
$1 \le i \le n$	$f(i)$paylasim gizli degerleri
1	170
2	872
3	660
4	273
5	64
6	174
7	3
8	9
9	938

10	543
11	733
12	435
13	984
14	315
15	790
16	988
17	255
18	216
19	334
20	457

Tablo 7.3. (8,20) Eşik Şemanın Paylaşım Değerleri

Gizliliğin Yeniden Elde Edilmesi

P=991(asal sayı)	
k (eşik değer)	$f(i)$paylasim gizli degerleri
3	660
5	64
7	3
10	543
11	733
12	435
14	315
18	216
S=458(gizlilik elde edildi)	

Tablo 7. 4. (8,20) Eşik Şemanın k = 8 eşik değer ile gizliliğin elde edilmesi

(k, n) = (5, 15) Eşik Şeması Uygulaması ve Sonuçları

Paylaşım Kısmı

P=1928049029 (asal sayı)	S=12345678(gizlilik)
$f(x) = 12345678 + 1233383461x + 1575624655x^2 + 442255554x^3 + 1707354259x^4$	
$1 \le i \le n$	$f(i)$paylasim gizli degerleri
1	1114865549
2	1076343216
3	389447370
4	34319309
5	1478572938
6	893147682
7	720602660
8	34871540
9	325409626
10	1641095800
11	662183493
12	340545830
13	259430485
14	489557739
15	1589120480

Tablo7. 5. (5,15) Eşik Şemanın Paylaşım Değerleri

Gizliliğin Yeniden Elde Edilmesi

P=1928049029 (asal sayı)	
k (eşik değer)	$f(i)$paylasim gizli degerleri
1	1114865549
4	34319309
5	1478572938
8	34871540
13	259430485
S=12345678(gizlilik elde edildi)	

Tablo7. 6. (5,15) Eşik Şemanın k=5 eşik değer ile gizliliğin elde edilmesi

BÖLÜM 8

8. GF(q) ASAL CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI

8.1.GF(7) Asal Cisminde üretilen (6, 3, 4) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

Bu bölümdeki MDS kodlarla yapılan gizlilik paylaşım şemaları sonuçları C kodu ile gerçekleştirilmiştir. Gizliliği yeniden elde etmede denklem sisteminin çözümünde kramer metodundan faydalanılmıştır. Sistemin karmaşıklığı kullanılan matrisin boyutu ve determinant alma zorluk derecesi ile ilişkilidir.

8.1.1. (6, 3, 4)= (n, k, d) kodunun üreteç matrisinin elde edilmesi

GF(7) uzayında yani q=7 dizili elemanları $F = Z_7 = \{0,1,2,3,4,5,6\}$ olan bir (n, k, d)=(6, 3, 4) olan lineer C kodu MDS koddur. $\alpha = 3$, GF(7) cisminin 6. dereceden ilkel elemanıdır. Çünkü $\alpha^{q-1} = 1 \bmod q$ denkliğine göre $3^6 \equiv 1 \bmod 7$ dir. $\alpha = 3$ ile, GF(7) uzayındaki tüm elemanlar elde edilmektedir.

$$3^1 \equiv 3 \bmod 7$$
$$3^2 \equiv 2 \bmod 7$$
$$3^3 \equiv 6 \bmod 7$$
$$3^4 \equiv 4 \bmod 7$$
$$3^5 \equiv 5 \bmod 7$$
$$3^6 \equiv 1 \bmod 7$$

Bu kodun üreteç polinomu

$$g(x) = (x+3)(x+3^2)(x+3^{2t=n-k}) = (x+3)(x+3^2)(x+3^3)$$
$$g(x) = 6 + x + 3x^2 + x^3$$

Buradan üreteç matrisini elde edebiliriz.

$$G = \begin{pmatrix} 6 & 1 & 3 & 1 & 0 & 0 \\ 0 & 6 & 1 & 3 & 1 & 0 \\ 0 & 0 & 6 & 1 & 3 & 1 \end{pmatrix}$$

Bu matrisi, elementer satır işlemleri ile standart üreteç matris formuna dönüştürürsek oluşan yeni üreteç matris şöyledir.

$$G = \begin{pmatrix} 1 & 0 & 0 & 6 & 1 & 3 \\ 0 & 1 & 0 & 3 & 3 & 6 \\ 0 & 0 & 1 & 6 & 4 & 6 \end{pmatrix} \text{ ve kontrol matrisi } H = \begin{pmatrix} 6 & 3 & 6 & 1 & 0 & 0 \\ 1 & 3 & 4 & 0 & 1 & 0 \\ 3 & 6 & 6 & 0 & 0 & 1 \end{pmatrix}$$

8.1.2. (n, k, d)=(6, 3, 4) MDS Kodu ile (k, n-1)=(3, 5) eşik Gizlilik Paylaşım Şeması Oluşturulması

(6, 3, 4) MDS kod ile (3,5) bir eşik gizlilik paylaşım şeması kurulabilir. Bu kod için bilgi vektörleri k=3 olduğu için $s = [s_0, s_1, s_2]$ 3 uzunluğunda elemanları $GF(7)$'te olan bir vektördür. Örneğin seçtiğimiz bilgi vektörü $s = [2,3,5]$ olsun. Bu bilgi vektörünün sorumlu olduğu kod söz,

$$t = (t_0, t_1, t_2, t_3, t_4, t_5) = sG = [235].\begin{bmatrix} 100613 \\ 010336 \\ 001646 \end{bmatrix} = [235235]$$

Burada gizlilik t kod sözünün $t_0 = 2$ olan ilk bileşenidir. Diğer bileşenler ise P_1=3, P_2=5, P_3=2, P_4=3, P_5 =5 olarak paylaşımcılara dağıtılır. Paylaşımlar kümesi $t_{i_1}, t_{i_2}, ..., t_{i_m}$ ile belirlenir. O halde paylaşımlar kümesi $S = \{P_1, P_2, P_3, P_4, P_5\}$ 'tür.

Paylaşımlar	**Gizli Değerler**
t_0 (gizli bileşen)	**2**
P_1= (1. Katılımcı)	3
P_2= (2. Katılımcı)	5
P_3= (3. Katılımcı)	2
P_4= (4. Katılımcı)	3
P_5= (5. Katılımcı)	5

Tablo 8. 1 GF(7) asal cisminde (6, 3, 4) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri

Seçilen MDS kodun boyutu k=3 olduğu için gizliliği elde etmek için erişim kümesi en az üç katılımcıdan oluşmak zorundadır.

Minimal erişim kümesi $\binom{n}{k}=\binom{5}{3}=10$ tanedir. Aşağıdaki minimal erişim kümelerindeki P_1, P_2, P_3, P_4, P_5 sırayla 1, 2, 3, 4, 5 ile gösterilmiştir.

$$S=\{(1,2,3),(1,2,4),(1,2,5)(2,3,4),(2,3,5),(3,4,5),(1,3,4),(1,3,5),(1,4,5)(2,4,5)\}$$

Bu minimal erişim kümelerinden herhangi bir küme ile gizliliği belirleyebiliriz. $\{P_3,P_4,P_5\}$ erişim kümesi kullanılarak gizli bileşeni elde edelim. Öncelikle aşağıdaki denklem sisteminden x_i bilinmeyenleri bulunur

$$g_0=\sum_{j=1}^{k}x_j g_{i_j}=\sum_{j=1}^{3}x_j g_j=x_3g_3+x_4g_4+x_5g_5$$

Daha sonra t_0 gizli bileşen aşağıdaki denklem ile elde edilir.

$$t_0=sg_0=\sum_{j=1}^{k}x_j sg_{i_j}=\sum_{j=1}^{k}x_j t_{i_j}$$

Sonuç olarak gizlilik olan t_0=2 elde edilmiştir.

8.2. GF(11) Asal Cisminde üretilen (10, 6, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

8.2.1 (10, 6, 5)=(n, k, d) kodunun üreteç matrisinin elde edilmesi

GF(11) uzayında yani q=11 dizili elemanları $F=Z_{11}=\{0,1,2,3,4,5,6,7,8,9,10\}$ olan bir (n, k, d) =(10, 6, 5) olan lineer C kodu MDS koddur. $\alpha=2$, GF(11) cisminin 10. dereceden ilkel elemanıdır. GF(11) uzayında (10, 6, 5) MDS kodu g(x) üreteç polinomu ve G standart formda üreteç matrisi ile (6, 9) eşik gizlilik paylaşım şeması kurulmuştur.

$$g(x) = (x+2)(x+2^2)(x+2^3)(x+2^4) = (x^4 + 3x^3 + 5x^2 + 8x + 1)$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 8 & 5 & 3 \\ 0 & 1 & 0 & 0 & 0 & 0 & 8 & 2 & 4 & 7 \\ 0 & 0 & 1 & 0 & 0 & 0 & 4 & 7 & 8 & 5 \\ 0 & 0 & 0 & 1 & 0 & 0 & 6 & 8 & 4 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 7 & 7 & 10 & 3 \\ 0 & 0 & 0 & 0 & 0 & 1 & 8 & 5 & 3 & 1 \end{pmatrix}$$

8.2.2. (n, k ,d)=(10, 6, 5) MDS Kodu ile (k, n-1)=(6, 9) eşik Gizlilik Paylaşım Şeması Oluşturulması

(10, 6, 5) MDS kod ile (6, 9) bir eşik gizlilik paylaşım şeması kurulabilir. Bu kod için bilgi vektörü elemanları $GF(11)$'te olan bir $s = [6, 3, 5, 7, 8, 9]$ vektörü olsun. Bu bilgi vektörünün sorumlu olduğu kod söz, t = (6, 3, 5, 7, 8, 9, 0, 4, 8, 4) dir.

Paylaşımlar	**Gizli Değerler**
t_0= gizli bileşen	**6**
P_1= (1. Katılımcı)	3
P_2= (2. Katılımcı)	5
P_3= (3. Katılımcı)	7
P_4= (4. Katılımcı)	8
P_5= (5. Katılımcı)	9
P_6= (6. Katılımcı)	0
P_7= (7. Katılımcı)	4
P_8= (8. Katılımcı)	8
P_9= (9. Katılımcı)	4

Tablo 8. 2. GF(11) asal cisminde (10, 6, 5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri

Seçilen MDS kodun boyutu k=6 olduğu için gizliliği elde etmek için erişim kümesi en az altı katılımcıdan oluşmak zorundadır.

Bunlardan bazılarını S kümesi ile gösterelim. Aşağıdaki minimal erişim kümelerindeki P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9 sırayla 1, 2, 3, 4, 5, 6, 7, 8, 9 ile gösterilmiştir.

S={(123456),(123457),(123458),(123459),(134567),(134568),(134569),(145678), (145679),(146789),(234567),(234568)}

$\{P_2, P_3, P_4, P_6, P_7, P_9\}$ erişim kümesi kullanılarak gizli bileşeni elde edelim. Öncelikle aşağıdaki denklem sisteminden x_i bilinmeyenleri bulunur

$$g_0 = \sum_{j=1}^{k} x_j g_{i_j}$$

Daha sonra t_0 gizli bileşen aşağıdaki denklem ile elde edilir.

$$t_0 = sg_0 = \sum_{j=1}^{k} x_j sg_{i_j} = \sum_{j=1}^{k} x_j t_{i_j}$$

Sonuç olarak t_0=6 elde edilmiştir.

8.3.GF(13) Asal Cisminde üretilen (12, 8, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

8.3.1 (12, 8, 5)=(n, k, d) kodunun üreteç matrisinin elde edilmesi

GF(13) uzayında yani q=13 dizili elemanları $F = Z_{13} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$ olan bir (n, k, d) =(12, 8, 5) olan lineer C kodu MDS koddur. $\alpha = 2$, GF(13) cisminin 12. dereceden ilkel elemanıdır. GF(13) uzayında (12, 8, 5) MDS kodu g(x) üreteç polinomu ve G standart formdaki üreteç matrisi ile (8, 11) eşik gizlilik paylaşım şeması kurulmuştur.

$$g(x) = (x+2)(x+2^2)(x+2^3)(x+2^4) = (x^4 + 9x^3 + 7x^2 + 2x + 10)$$

$$G = \begin{pmatrix} 1&0&0&0&0&0&0&0&12&5&6&11 \\ 0&1&0&0&0&0&0&0&1&5&4&4 \\ 0&0&1&0&0&0&0&0&12&6&3&7 \\ 0&0&0&1&0&0&0&0&8&2&9&12 \\ 0&0&0&0&1&0&0&0&2&11&2&3 \\ 0&0&0&0&0&1&0&0&9&9&3&1 \\ 0&0&0&0&0&0&1&0&3&7&2&7 \\ 0&0&0&0&0&0&0&1&8&2&10&4 \end{pmatrix}$$

8.3.2. (n, k, d)=(12, 8, 5) MDS Kodu ile (k, n-1)=(8, 11) eşik Gizlilik Paylaşım Şeması Oluşturulması

(12, 8, 5) MDS kod ile (8, 11) bir eşik gizlilik paylaşım şeması kurulabilir. Bu kod için bilgi vektörü elemanları $GF(13)$'te olan bir $s = [10,3,5,7,8,9,10,11]$ vektörü olsun. Bu bilgi vektörünün sorumlu olduğu kod söz,

t = (10, 3, 5, 7, 8, 9, 10, 11, 12, 6, 11, 11) dir.

Paylaşımlar	**Gizli Değerler**
t_0= gizli bileşen	**10**
P_1= (1. Katılımcı)	3
P_2= (2. Katılımcı)	5
P_3= (3. Katılımcı)	7
P_4= (4. Katılımcı)	8
P_5= (5. Katılımcı)	9
P_6= (6. Katılımcı)	10
P_7= (7. Katılımcı)	11
P_8= (8. Katılımcı)	12
P_9= (9. Katılımcı)	6
P_{10}= (10. Katılımcı)	11
P_{11}= (11. Katılımcı)	11

Tablo 8. 3. GF(13) asal cisminde (12, 8, 5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri

Yine yukarıdaki örneklerde anlatıldığı gibi rastgele seçilen $P_2, P_3, P_5, P_7, P_8, P_9, P_{10}, P_{11}$ sekiz katılımcıdan gizli bileşen t_0=10 olarak, yazılan C kodu ile hesaplanmıştır.

BÖLÜM 9

9. GF(2^n) SONLU CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE GİZLİLİK PAYLAŞIM ŞEMASI UYGULAMASI

Bu bölümde MDS kod tabanlı gizlilik paylaşım şeması uygulamaları yazılan C# kodu ile gerçekleştirilmiştir. Gizliliği elde etmede yine kramer metodundan faydalanılmıştır. Sistemin karmaşıklığı seçilen sonlu cisim uzayının büyüklüğü ve matrisin boyutu ile artmaktadır.

9.1. $GF(2^3)$ Sonlu Cisim uzayında (7, 3, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

$GF(2^3)$ sonlu cisim uzayında $x^3 + x + 1$ indirgenemez polinoma göre (7, 3, 5) MDS kodun üreteç polinomu ve standart formdaki üreteç matrisi G aşağıda verilmiştir.

$$g(x) = (x+1)(x+\alpha)(x+\alpha^2)(x+\alpha^3)$$

$$G = \begin{pmatrix} 1 & 0 & 0 & \alpha^6 & \alpha^5 & \alpha^5 & \alpha^2 \\ 0 & 1 & 0 & \alpha & \alpha^2 & \alpha^4 & 1 \\ 0 & 0 & 1 & \alpha^6 & \alpha^6 & \alpha^3 & \alpha \end{pmatrix} \cong \begin{pmatrix} 1 & 0 & 0 & 5 & 7 & 7 & 4 \\ 0 & 1 & 0 & 2 & 4 & 6 & 1 \\ 0 & 0 & 1 & 5 & 5 & 3 & 2 \end{pmatrix}$$

Bu kod (3, 6) eşik gizlilik paylaşım şemasını belirler. Bu durum en fazla 6 paylaşımcının olduğunu ve en az 3 paylaşımcının birleşerek gizliliği elde edebileceğini söyler. 6 paylaşımcı P_1, P_2, P_3, P_4, P_5, P_6 olsun. Kontrol matrisi H'dır.

$$H = \begin{pmatrix} \alpha^6 & \alpha & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^5 & \alpha^2 & \alpha^6 & 0 & 1 & 0 & 0 \\ \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha^2 & 1 & \alpha & 0 & 0 & 0 & 1 \end{pmatrix}$$

Şimdi gizlilik paylaşım şeması oluşturalım.

Burada $s' \in GF(q)$ gizliliği göstersin. $g_0 = (g_{00}, g_{10}, ..., g_{k-1,0})^T$, G üreteç matrisinin ilk sütunu olsun. $s = (s_0, s_1, ..., s_{k-1})$, $GF(q^k)$' da seçilmiş bir bilgi vektörüdür. Burada $s' = sg_0 = \sum_{i=0}^{k-1} s_i g_{i0}$ s bilgi vektörünün sorumlu olduğu kod söz $t = (t_0, t_1, ..t_{n-1}) = sG$ dir. Her P_i paylaşımcılarına t_i bilgileri paylaştırılır. İlk bileşen olan $t_0 = s'$, t kod sözünün gizli bileşenidir. Bu kod için bilgi vektörleri k=3 olduğu için $s = [s_0, s_1, s_2]$ 3 uzunluğunda elemanları $GF(2^3)$'te olan bir vektördür. Örneğin seçtiğimiz bilgi vektörü $s = [1, \alpha^6, \alpha^5]$ olsun. Bu bilgi vektörünün sorumlu olduğu kod söz,

$t = (t_0, t_1, t_2, t_3, t_4, t_5, t_6) = sG = \left[1, \alpha^6, \alpha^5, \alpha, \alpha^3, \alpha^4, \alpha^2\right]$ ve paylaşımlar Tablo 9.1'de gösterilmiştir. Paylaşım kısmı için C#' da yazılan programın pseudo kodu aşağıdaki gibidir.

Paylaşım Kısmı

S = Bilgi Vektörü
G= Üreteç Matrisi
SG=0
for i=0 **to** Ureteç Matrisinin Kolon sayısı
Begin
    for j=0 **to** Bilgi Vektörünün Kolon sayısı
    Begin
        SG[i] = SG[i] **xor** Sonlu_cisimde_carpma(S[j], B[j,i])
    End
End

Paylaşımlar	**Gizli Değerlerin Cisim Elemanları ile Gösterimi**
t_0 (gizli bileşen)	**1**
P_1= (1. Katılımcı)	α^6
P_2= (2. Katılımcı)	α^5
P_3= (3. Katılımcı)	α
P_4= (4. Katılımcı)	α^3
P_5= (5. Katılımcı)	α^4
P_6= (6. Katılımcı)	α^2

Tablo 9. 1. GF(2^3) sonlu cisminde (7,3,5) MDS kod ile elde edilen katılımcıların gizli paylaşım değerleri

MDS kodunun boyutu k=3 olduğu için erişim kümesi en az 3 paylaşımcıdan oluşmak zorundadır. Üç paylaşımcıdan daha az paylaşımcı gizli bileşeni yeniden

elde edemez. En az 3 paylaşımcının olduğu $\binom{6}{3} = 20$ kadar erişim kümeleri ile gizli bileşene ulaşılır.

$$S = \{\{P_1,P_2,P_3\},\{P_1,P_2,P_4\},\{P_1,P_2,P_5\},\{P_1,P_2,P_6\},\{P_1,P_3,P_4\},\{P_1,P_3,P_5\},\{P_1,P_3,P_6\},$$
$$\{P_1,P_4,P_5\},\{P_1,P_4,P_6\},\{P_1,P_5,P_6\},\{P_2,P_3,P_4\},\{P_2,P_3,P_5\},\{P_2,P_3,P_6\},\{P_2,P_4,P_5\}$$
$$\{P_2,P_4,P_6\},\{P_2,P_5,P_6\}\{P_3,P_4,P_5\},\{P_3,P_4,P_6\},\{P_3,P_5,P_6\}\{P_4,P_5,P_6\}\}$$

S kümesinden seçilen $\{P_1,P_2,P_3\}$ erişim kümesi ile gizli bileşeni elde edelim.

$$g_0 = \sum_{j=1}^{k} x_j g_{i_j} = \sum_{j=1}^{3} x_j g_j = x_1 g_1 + x_2 g_2$$

$$g_0 = x_1 g_1 + x_2 g_2 + x_3 g_3$$

$$\begin{bmatrix}1\\0\\0\end{bmatrix} = x_1\begin{bmatrix}0\\1\\0\end{bmatrix} + x_2\begin{bmatrix}0\\0\\1\end{bmatrix} + x_3\begin{bmatrix}\alpha^6\\\alpha\\\alpha^6\end{bmatrix}$$

$$1 = \alpha^6 x_3 \Rightarrow x_3 = \alpha$$

$$0 = x_1 + \alpha x_3 \Rightarrow 0 = x_1 + \alpha^2 \Rightarrow x_1 = \alpha^2$$

$$0 = x_2 + \alpha^6 x_3 \Rightarrow 0 = x_2 + \alpha^6\alpha \Rightarrow x_2 = \alpha^7 = 1$$

Daha sonra gizlilik $t_0 = sg_0 = \sum_{j=1}^{k} x_j sg_{i_j} = \sum_{j=1}^{k} x_j t_{i_j}$ denklem sisteminin çözümünden elde edilir (Özadam vd., 2007) ; (Xiaoqing ve Zhiguo, 2004) ; (Arda vd., 2010).

$$t_0 = x_1 P_1 + x_2 P_2 + x_3 P_3$$

$$t_0 = \alpha^2.\alpha^6 + 1.\alpha^5 + \alpha.\alpha$$

$$t_0 = \alpha^8 + \alpha^5 + \alpha^2$$

$$t_0 = \alpha + \alpha^2 + \alpha + 1 + \alpha^2$$

$$t_0 = 1$$

$t_0 = 1$ gizli bileşen elde edilir.

Gizliliği yeniden elde etmek için C#' da yazılan programın pseudo kodu aşağıdaki gibidir.

[n,k,d] kod için gizliliği yeniden elde etme

if katılımcı sayısı<n-k **then**

begin

b= katılımcı vektörü

g0= üreteç matrisi[katılımcı]

D=determinant(g0)

For i=0 **to** katılımcı sayısı

Begin

c=g0[katılımcı-i]

det[i]=determinant(c)

x[i]= Sonlu_cisimde_carpma(det[i],1/D)

end

t0 = 0

For i=0 **to** katılımcı sayısı

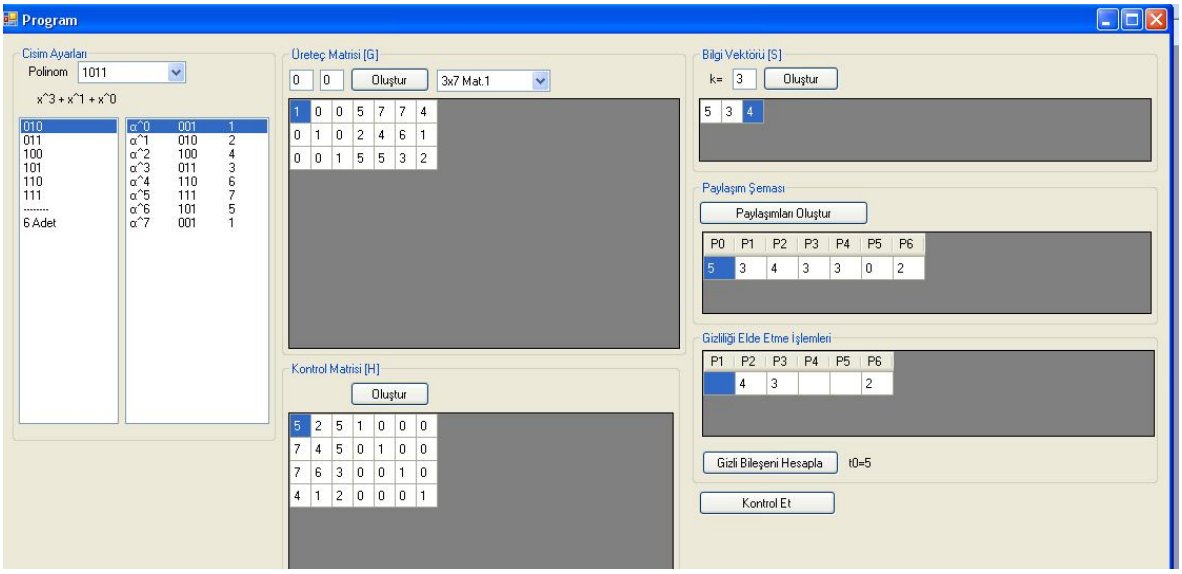
Begin

to= to xor Sonlu_cisimde_carpma(x[i],b[i])

End

End

Yukarıda açıklanan örnek temel alınarak başka bir bilgi vektörü için aşağıda C#'da yazılan örnek bir uygulama gösterilmiştir.



Paylaşım Kısmı

Girilen bilgi vektörü s=[5, 3, 4] için elde edilen paylaşımlar aşağıdaki Tablo 9.2'de gösterilmiştir.

Paylaşımlar	Gizli Değerler(ondalık gösterimi)
t_0 (gizli bileşen)	**5**
P_1= (1. Katılımcı)	3
P_2= (2. Katılımcı)	4
P_3= (3. Katılımcı)	3
P_4= (4. Katılımcı)	3
P_5= (5. Katılımcı)	0
P_6= (6. Katılımcı)	2

Tablo 9. 2 GF(2^3) sonlu cisminde (7, 3, 5) MDS kod için Gizlilik Paylaşım Değerleri

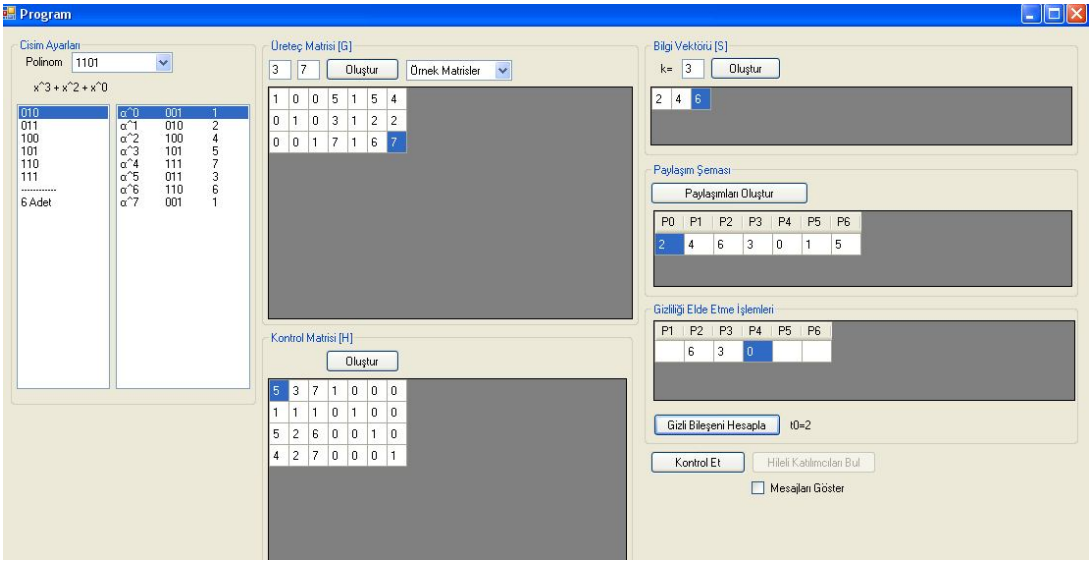
Gizli Veriyi Yeniden Elde Etme Kısmı

Burada seçilen rastgele {P_2, P_3, P_6}katılımcıları bir araya gelerek t_0=5 gizli bileşenini elde edebilirler.

Aşağıdaki program çıktısı ise GF(2^3) sonlu cisim uzayında (7, 3, 5) MDS kodun $g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$ üreteç polinomlu $x^3 + x^2 + 1$ indirgenemez polinoma göre elde edilen farklı üreteç matris ile oluşturulan Gizlilik Paylaşım Şemasını göstermektedir.

$$G = \begin{pmatrix} 1 & 0 & 0 & 5 & 1 & 5 & 4 \\ 0 & 1 & 0 & 3 & 1 & 2 & 2 \\ 0 & 0 & 1 & 7 & 1 & 6 & 7 \end{pmatrix}$$

Girilen bilgi vektörü s=[2, 4, 6] ve paylaşımlar {P_1, P_2, P_3, P_4, P_5, P_6 }= {4, 6, 3, 0, 1, 5}dir. Rastgele seçilen en az 3 katılımcı kümesi olan {P_2, P_3, P_4}ile t_0=2 gizli bileşenin elde edildiği aşağıda gösterilmiştir.



9.2. GF(2^4) Sonlu Cisim uzayında üretilen (8, 4, 5) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

(8, 4, 5) kısaltılmış RS kod aynı zamanda MDS koddur. Bu kodun GF(2^4) sonlu cisminde $1+x+x^4$ indirgenemez polinomuna göre üreteç polinomu g(x)'tir. Ayrıca bu uzayda üretilen cisim elemanları Tablo 9.3'te gösterilmiştir.

Ondalık Gösterim	Polinomsal Gösterim	Vektörel Gösterim	Eleman
0	0	0000	0
1	$\alpha^0 = 1$	0001	1
2	α	0010	α
4	α^2	0100	α^2
8	α^3	1000	α^3
3	$\alpha+1$	0011	α^4
6	$\alpha^2+\alpha$	0110	α^5
12	$\alpha^3+\alpha^2$	1100	α^6
11	$\alpha^3+\alpha+1$	1011	α^7
5	α^2+1	0101	α^8
10	$\alpha^3+\alpha$	1010	α^9
7	$\alpha^2+\alpha+1$	0111	α^{10}
14	$\alpha^3+\alpha^2+\alpha$	1110	α^{11}
15	$\alpha^3+\alpha^2+\alpha+1$	1111	α^{12}
13	$\alpha^3+\alpha^2+1$	1101	α^{13}
9	α^3+1	1001	α^{14}

Tablo 9. 3. GF(2^4)'ün elemanlarının olası gösterimleri

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$$
$$= \mathrm{x}^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}$$

Üreteç matrisi

$$G = \begin{bmatrix} \alpha^{10}\alpha^3\alpha^6\alpha^{13}1\ 0\ 0\ 0 \\ 0\ \alpha^{10}\alpha^3\alpha^6\alpha^{13}1\ 0\ 0 \\ 0\ 0\ \alpha^{10}\alpha^3\alpha^6\alpha^{13}1\ 0 \\ 0\ 0\ 0\ \alpha^{10}\alpha^3\alpha^6\alpha^{13}1 \end{bmatrix}$$

G matrisine satır sütün işlemleri yapılarak standart forma getirilebilir. Bu şekilde üretilen yeni matris aşağıdaki gibidir.

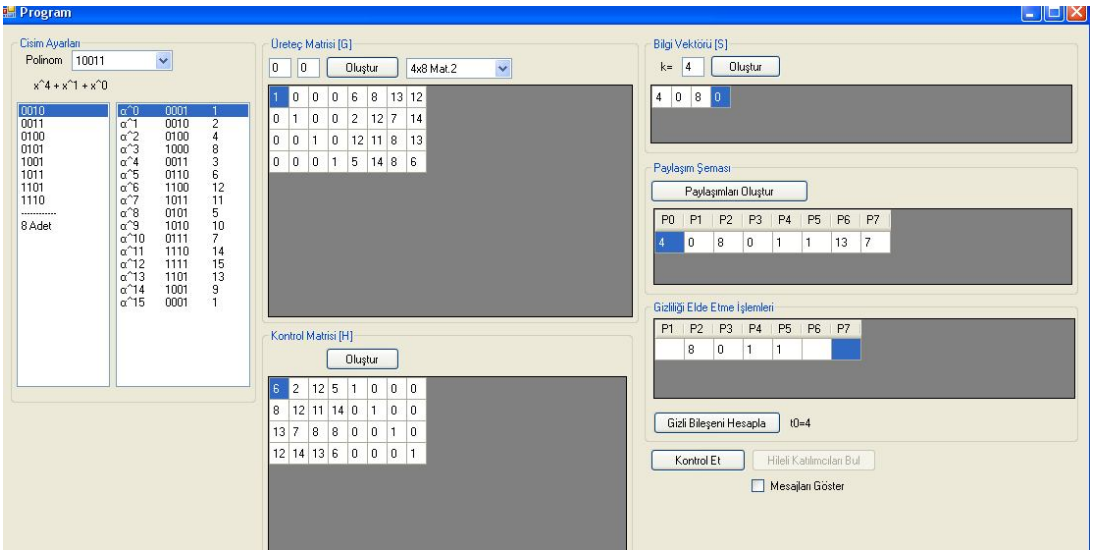
$$G = \begin{bmatrix} 1\ 0\ 0\ 0\ \alpha^5\alpha^3\alpha^{13}\alpha^6 \\ 0\ 1\ 0\ 0\ \alpha\ \alpha^6\alpha^{10}\alpha^{11} \\ 0\ 0\ 1\ 0\ \alpha^6\alpha^7\alpha^3\alpha^{13} \\ 0\ 0\ 0\ 1\ \alpha^8\alpha^{11}\alpha^3\alpha^5 \end{bmatrix} = \begin{bmatrix} 1\ 0\ 0\ 0\ 6\ 8\ 13\ 12 \\ 0\ 1\ 0\ 0\ 2\ 12\ 7\ 14 \\ 0\ 0\ 1\ 0\ 12\ 11\ 8\ 13 \\ 0\ 0\ 0\ 1\ 5\ 14\ 8\ 6 \end{bmatrix}$$

Bu koddan (4, 7) eşik şeması kurulur. Verilen bilgi mesajı $m = [\alpha^2, 0, \alpha^3, 0]$ olsun. Bu bilgi mesajının sorumlu olduğu kod sözcüğü $c = mG = [\alpha^2, 0, \alpha^3, 0, 1, 1, \alpha^{13}, \alpha^{10}]$ dur. Burada ilk bileşen gizliliği temsil etmektedir.

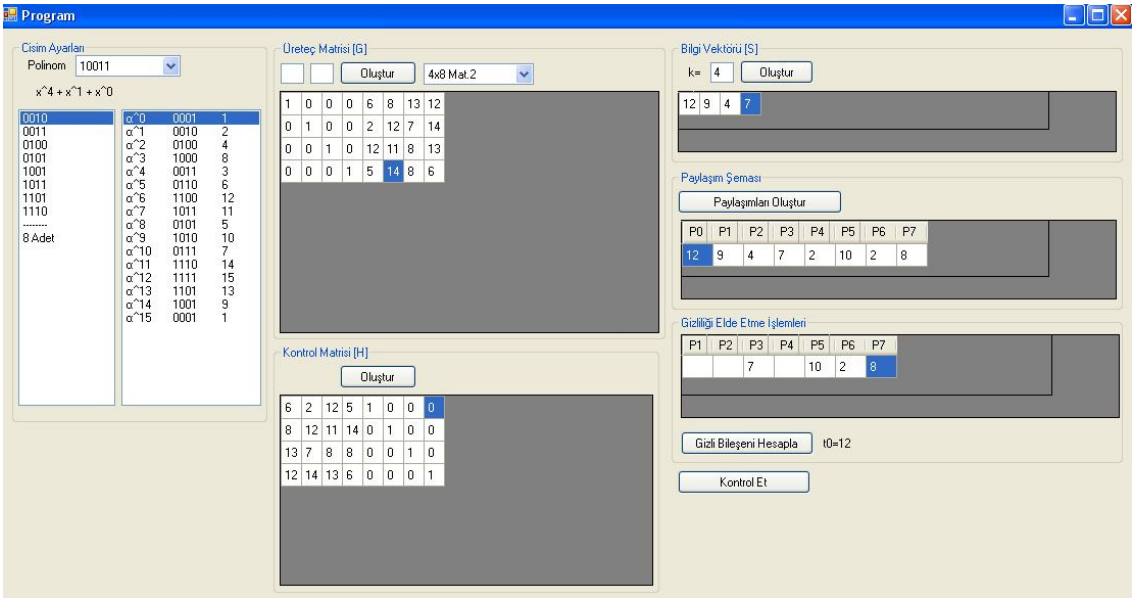
Paylaşımlar	Gizli Değerlerin Ondalık Gösterimi	Gizli Değerlerin Cisim elemanları ile Gösterimi
t_0 (gizli bileşen)	**4**	α^2
P_1= (1. Katılımcı)	0	0
P_2= (2. Katılımcı)	8	α^3
P_3= (3. Katılımcı)	0	0
P_4= (4. Katılımcı)	1	1
P_5= (5. Katılımcı)	1	1
P_6= (6. Katılımcı)	13	α^{13}
P_7= (7. Katılımcı)	7	α^{10}

Tablo 9. 4. (8, 4, 5) MDS kod ile Gizlilik Paylaşım Şemasında Paylaşım Değerleri

(8, 4, 5) MDS kodunun boyutu k=4 olduğu için erişim kümesi en az 4 paylaşımcıdan oluşmak zorundadır. Dört paylaşımcıdan daha az paylaşımcı gizli bileşeni yeniden elde edemez. Aşağıda {P_2 ,P_3, P_4, P_5} katılımcılar kümesi ile gizliliğin t_0=4 olarak elde edildiği C#' da yazılan programın çıktısı ile gösterilmiştir.



Başka bir bilgi vektörü ile ilde edilen paylaşımlar ve gizliliğin elde edilmesi sonuçları aşağıda program sonucunda gösterilmiştir.



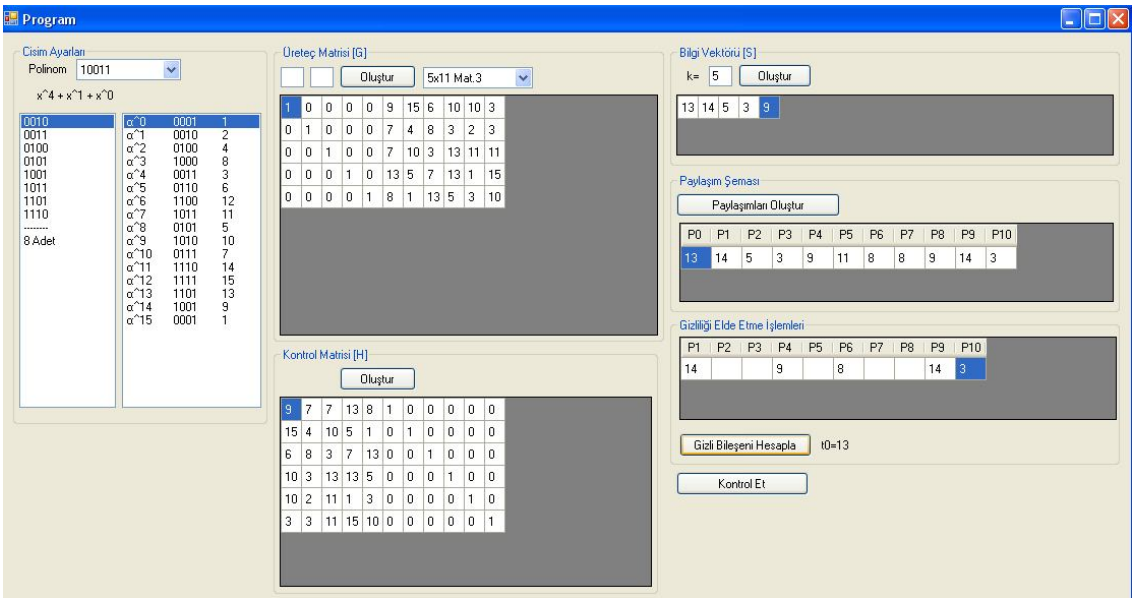
9.3. GF(2^4) Sonlu Cisim uzayında üretilen (11, 5, 7) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

$GF(2^4)$ sonlu cisim uzayında $x^4 + x + 1$ indirgenemez polinoma göre (11, 5, 7) MDS kodun üreteç polinomu ve standart forma getirilmiş üreteç matrisi G ondalık gösterimleri ile aşağıda verilmiştir.

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)$$
$$g(x) = x^6 + \alpha^{10}x^5 + \alpha^{14}x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 9 & 15 & 6 & 10 & 10 & 3 \\ 0 & 1 & 0 & 0 & 0 & 7 & 4 & 8 & 3 & 2 & 3 \\ 0 & 0 & 1 & 0 & 0 & 7 & 10 & 3 & 13 & 11 & 11 \\ 0 & 0 & 0 & 1 & 0 & 13 & 5 & 7 & 13 & 1 & 15 \\ 0 & 0 & 0 & 0 & 1 & 8 & 1 & 13 & 5 & 3 & 10 \end{pmatrix}$$

Aşağıda s=(13, 14, 5, 3, 9) şeklinde girilen bilgi vektörü için oluşturulan gizlilik ve paylaşım değerleri ve gizliliğin yeniden elde edilmesi gösterilmiştir.



Yukarıdaki program çıktısında girilen s=(13, 14, 5, 3, 9) bilgi vektörüne göre elde edilen gizlilik ve paylaşım değerleri aşağıdaki Tablo 9.5'de verilmiştir.

Paylaşım Kısmı

Paylaşımlar	**Gizli Değerlerin İkili Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	**1110**	**13**
P_1= (1. Katılımcı)	1000	14
P_2= (2. Katılımcı)	0101	5
P_3= (3. Katılımcı)	1001	3
P_4= (4. Katılımcı)	1010	9
P_5= (5. Katılımcı)	0010	11
P_6= (6. Katılımcı)	0010	8
P_7= (7. Katılımcı)	1010	8
P_8= (8. Katılımcı)	1010	9
P_9= (9. Katılımcı)	0011	14
P_{10}= (10. Katılımcı)	0001	3

Tablo 9. 5. GF(2^4)'de (11, 5, 7) MDS kodu ile oluşturulan (5,10) Eşik Gizlilik Paylaşım Şemasının paylaşım değerleri

Aşağıdaki Tablo.9. 6'da yazılan program sonucu olarak {P_1, P_4, P_6, P_9, P_{10}} katılımcılarının paylaşımlarını birleştirerek gizliliği elde ettikleri gösterilmiştir. Bu katılımcılar kümesi rastgele alınmıştır. Gizliliği elde etmek için 10 paylaşımcıdan rastgele en az 5 adet katılımcının birleşmesi gerekmektedir.

Gizliliği Yeniden Elde Etme Kısmı

K=5 adet Katılımcı	**K adet katılımcının Paylaşımları**
P_1= (1. Katılımcı)	14
P_4= (4. Katılımcı)	9
P_6= (6. Katılımcı)	8
P_9= (9. Katılımcı)	14
P_{10}= (10. Katılımcı)	3
t_0= gizli bileşen	**13**

Tablo 9.6. (k, n-1)=(5, 10) Eşik Gizlilik Paylaşım Şemasında k=5 adet Katılımcı ile Gizliliği Elde Etme

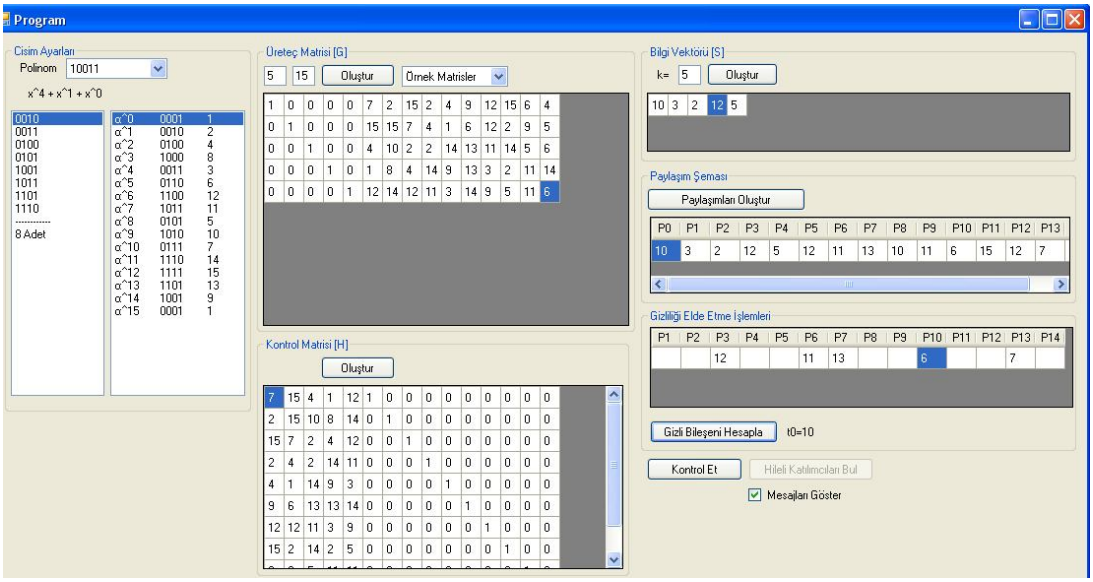
9.4. GF(2^4) Sonlu Cisim uzayında üretilen (15, 5, 11) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

$GF(2^4)$ sonlu cisim uzayında $x^4 + x + 1$ indirgenemez polinoma göre (15,5,11) MDS kodun üreteç polinomu ve standart formdaki üreteç matrisi G ondalık gösterimler şeklinde aşağıda verilmiştir.

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6)(x+\alpha^7)(x+\alpha^8)(x+\alpha^9)(x+\alpha^{10})$$
$$g(x) = x^{10} + \alpha^2 x^9 + \alpha^3 x^8 + \alpha^9 x^7 + \alpha^6 x^6 + \alpha^{14} x^5 + \alpha^2 x^4 + \alpha x^3 + \alpha^6 x^2 + \alpha x + \alpha^{10}$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 7 & 2 & 15 & 2 & 4 & 9 & 12 & 15 & 6 & 4 \\ 0 & 1 & 0 & 0 & 0 & 15 & 15 & 7 & 4 & 1 & 6 & 12 & 2 & 9 & 5 \\ 0 & 0 & 1 & 0 & 0 & 4 & 10 & 2 & 2 & 14 & 13 & 11 & 14 & 5 & 6 \\ 0 & 0 & 0 & 1 & 0 & 1 & 8 & 4 & 14 & 9 & 13 & 3 & 2 & 11 & 14 \\ 0 & 0 & 0 & 0 & 1 & 12 & 14 & 12 & 11 & 3 & 14 & 9 & 5 & 11 & 6 \end{pmatrix}$$

Aşağıda s=(10, 3, 2, 12, 5) şeklinde girilen bilgi vektörü için oluşturulan gizlilik ve paylaşım değerleri ve gizliliğin yeniden elde edilmesi gösterilmiştir.



Yukarıdaki program çıktısında girilen s=(10, 3, 2, 12, 5) bilgi vektörüne göre elde edilen gizlilik ve paylaşım değerleri aşağıdaki Tablo 9. 7'de verilmiştir.

Paylaşım Kısmı

Paylaşımlar	**Gizli Değerlerin İkili Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	**1010**	**10**
P_1= (1. Katılımcı)	0011	3
P_2= (2. Katılımcı)	0010	2
P_3= (3. Katılımcı)	1100	12
P_4= (4. Katılımcı)	0101	5
P_5= (5. Katılımcı)	1100	12
P_6= (6. Katılımcı)	1011	11
P_7= (7. Katılımcı)	1101	13
P_8= (8. Katılımcı)	1010	10
P_9= (9. Katılımcı)	1011	11
P_{10}= (10. Katılımcı)	0110	6
P_{11}= (11. Katılımcı)	1111	15
P_{12}= (12. Katılımcı)	1100	12
P_{13}= (13. Katılımcı)	0111	7
P_{14}= (14. Katılımcı)	0100	4

Tablo 9. 7. GF(2^4)'de (15, 5, 11) MDS kodu ile oluşturulan (5, 14) Eşik Gizlilik Paylaşım Şemasının paylaşım değerleri

Aşağıdaki Tablo 9. 8'da yazılan program sonucu olarak {P_3, P_6, P_7, P_{10}, P_{13}} katılımcılarının paylaşımlarını birleştirerek gizliliği elde ettikleri gösterilmiştir. Bu katılımcılar kümesi rastgele alınmıştır. Gizliliği elde etmek için 14 paylaşımcıdan rastgele en az 5 adet katılımcının birleşmesi gerekmektedir.

Gizliliği Yeniden Elde Etme Kısmı

K=5 adet Katılımcı	**K adet katılımcının Paylaşımları**
P_3= (3. Katılımcı)	12
P_6= (6. Katılımcı)	11
P_7= (7. Katılımcı)	13
P_{10}= (10. Katılımcı)	6
P_{13}= (13. Katılımcı)	7
t_0= gizli bileşen	**10**

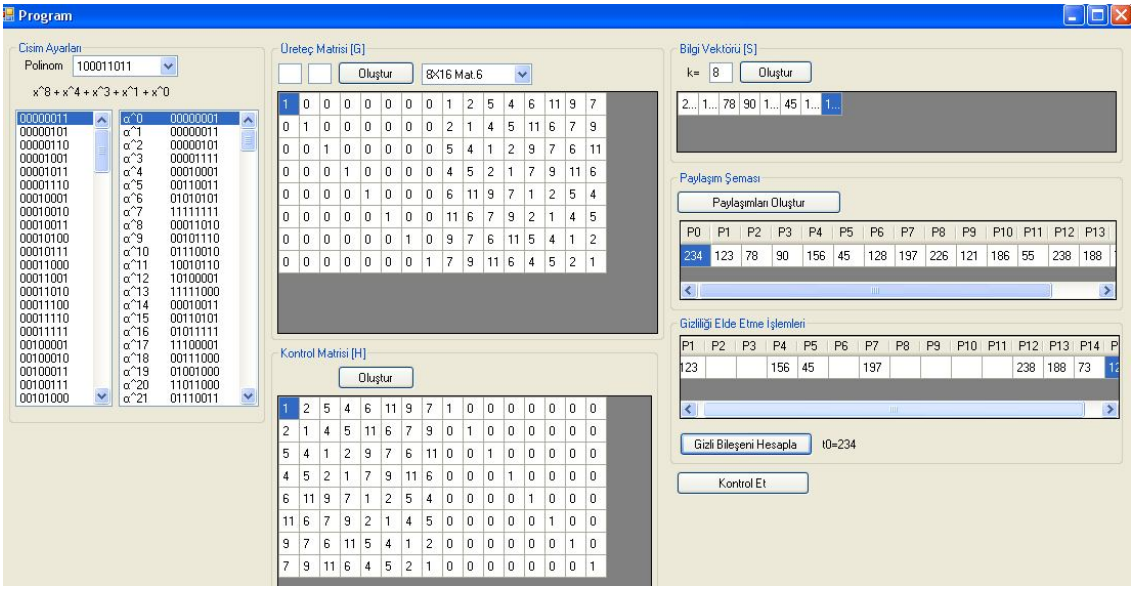
Tablo 9. 8. (k, n-1)=(5, 14) Eşik Gizlilik Paylaşım Şemasında k=5 adet Katılımcı ile Gizliliği Elde Etme

9.5. GF(2^8) Sonlu Cisim uzayında üretilen (16, 8, 9) MDS Kod ile Gizlilik Paylaşım Şeması Uygulaması

GF(2^8) sonlu cisim uzayında (16, 8, 9) MDS kodun indirgenemez polinomu $x^8 + x^4 + x^3 + x + 1$ göre seçilmiştir. Bu polinomun üreteci $\beta = \alpha + 1$ dir. Buna göre üretilen cismin elemanları ve üreteç matrisi aşağıdaki gibi olacaktır. Aşağıdaki matris (Aslan vd., 2011) makalesinden alınmıştır.

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 5 & 4 & 6 & 11 & 9 & 7 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1 & 4 & 5 & 11 & 6 & 7 & 9 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 5 & 4 & 1 & 2 & 9 & 7 & 6 & 11 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 & 5 & 2 & 1 & 7 & 9 & 11 & 6 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 6 & 11 & 9 & 7 & 1 & 2 & 5 & 4 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 11 & 6 & 7 & 9 & 2 & 1 & 4 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 9 & 7 & 6 & 11 & 5 & 4 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7 & 9 & 11 & 6 & 4 & 5 & 2 & 1 \end{pmatrix}$$

Aşağıda s=(234, 123, 78, 90, 156, 45, 128, 197) şeklinde girilen bilgi vektörü için oluşturulan gizlilik ve paylaşım değerleri ve gizliliğin yeniden elde edilmesi gösterilmiştir.



Yukarıdaki program çıktısında girilen s=(234, 123, 78, 90, 156, 45, 128, 197) bilgi vektörüne göre elde edilen gizlilik ve paylaşım değerleri aşağıdaki Tablo 9. 9'da verilmiştir.

Mesaj Vektörünün GF(2^8) uzayında ikili karşılığı şöyledir.

$m = (111010100111101101001110010110101001110000101101100000000011000101)$

Elde edilen kod söz c=mG ile elde edilir. Elde edilen kod kelimesi 8 bitlik bloklara bölünerek ilk bileşen gizlilik, diğerleri paylaşım değerleri olarak dağıtılır. Aşağıdaki Tablo 9. 9'de paylaşım değerleri verilmiştir. Hesaplamalar ve sonuçlar C# kodu ile gerçekleştirilmiştir.

Paylaşım Kısmı

Mesaj Vektörü	**(234, 123, 78, 90, 156, 45, 128, 197)**

Paylaşımlar	**Gizli Değerlerin İkili Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	**11101010**	**234**
P_1= (1. Katılımcı)	01111011	123
P_2= (2. Katılımcı)	01001110	78
P_3= (3. Katılımcı)	01011010	90
P_4= (4. Katılımcı)	10011100	156
P_5= (5. Katılımcı)	00101101	45
P_6= (6. Katılımcı)	10000000	128
P_7= (7. Katılımcı)	11000101	197
P_8= (8. Katılımcı)	11100010	226
P_9= (9. Katılımcı)	01111001	121
P_{10}= (10. Katılımcı)	10111010	186
P_{11}= (11. Katılımcı)	00110111	55
P_{12}= (12. Katılımcı)	11101110	238
P_{13}= (13. Katılımcı)	10111100	188
P_{14}= (14. Katılımcı)	01001001	73
P_{15}= (15. Katılımcı)	01111100	124

Tablo 9. 9. GF(2^8)'de (16, 8, 9) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasın'da paylaşım değerleri

Gizliliği Yeniden Elde Etme Kısmı

Paylaşımlar	**Gizli Değerlerin İkili Gösterimi**	**Gizli Değerlerin Ondalık karşılığı**
t_0= gizli bileşen	**11101010**	**234**
P_1= (1. Katılımcı)	01111011	123
P_4= (4. Katılımcı)	10011100	156
P_5= (5. Katılımcı)	00101101	45
P_7= (7. Katılımcı)	11000101	197
P_{12}= (12. Katılımcı)	11101110	238
P_{13}= (13. Katılımcı)	10111100	188
P_{14}= (14. Katılımcı)	01001001	73
P_{15}= (15. Katılımcı)	01111100	124

Tablo 9. 10. (k,n-1)=(8,15) Eşik Gizlilik Paylaşım Şemasında k=8 adet Katılımcı ile Gizliliği Elde Etme

Üreteç	**Binary**	**Hex.**		**Üreteç**	**Binary**	**Hex**
β^{0}	00000001	01		β^{53}	00111100	3C
β^{1}	00000011	03		β^{54}	01000100	44
β^{2}	00000101	05		β^{55}	11001100	CC
β^{3}	00001111	0F		β^{56}	01001111	4F
β^{4}	00010001	11		β^{57}	11010001	D1
β^{5}	00110011	33		β^{58}	01101000	68
β^{6}	01010101	55		β^{59}	10111000	B8
β^{7}	11111111	FF		β^{60}	11010011	D3
β^{8}	00011010	1A		β^{61}	01101110	6E
β^{9}	00101110	2E		β^{62}	10110010	B2
β^{10}	01110010	72		β^{63}	11001101	CD
β^{11}	10010110	96		B^{64}	01001100	4C
β^{12}	10100001	A1		β^{65}	11010100	D4
β^{13}	11111000	F8		β^{66}	01100111	67
β^{14}	00010011	13		β^{67}	10101001	A9
β^{15}	00110101	35		β^{68}	11100000	E0
β^{16}	01011111	5F		β^{69}	00111011	3B
β^{17}	11100001	E1		β^{70}	01001101	4D
β^{18}	00111000	38		β^{71}	11010111	D7
β^{19}	01001000	48		β^{72}	01100010	62
β^{20}	11011000	D8		β^{73}	10100110	A6
β^{21}	01110011	73		β^{74}	11110001	F1
β^{22}	10010101	95		β^{75}	00001000	08
β^{23}	10100100	A4		β^{76}	00011000	18
β^{24}	11110111	F7		β^{77}	00101000	28
β^{25}	00000010	02		β^{78}	01111000	78
β^{26}	00000110	06		β^{79}	10001000	88
β^{27}	00001010	0A		β^{80}	10000011	83
β^{28}	00011110	1E		β^{81}	10011110	9E
β^{29}	00100010	22		β^{82}	10111001	B9
β^{30}	01100110	66		β^{83}	11010000	D0
β^{31}	10101010	AA		β^{84}	01101011	6B
β^{32}	11100101	E5		β^{85}	10111101	BD
β^{33}	00110100	34		β^{86}	11011100	DC
β^{34}	01011100	5C		β^{87}	01111111	7F
β^{35}	11100100	E4		β^{88}	10000001	81
β^{36}	00110111	37		β^{89}	10011000	98
β^{37}	01011001	59		β^{90}	10110011	B3
β^{38}	11101011	EB		β^{91}	11001110	CE
β^{39}	00100110	26		β^{92}	01001001	49
β^{40}	01101010	6A		β^{93}	11011011	DB
β^{41}	10111110	BE		β^{94}	01110110	76
β^{42}	11011001	D9		β^{95}	10011010	9A
β^{43}	01110000	70		β^{96}	10110101	B5
β^{44}	10010000	90		β^{97}	11000100	C4
β^{45}	10101011	AB		β^{98}	01010111	57
β^{46}	11100110	E6		β^{99}	11111001	F9
β^{47}	00110001	31		β^{100}	00010000	10
β^{48}	01010011	53		β^{101}	00110000	30
β^{49}	11110101	F5		β^{102}	01010000	50
β^{50}	00000100	04		β^{103}	11110000	F0
β^{51}	00001100	0C		β^{104}	00001011	0B
β^{52}	00010100	14		β^{105}	00011101	1D

β^{106}	00100111	27		β^{161}	10111010	BA
β^{107}	01101001	69		β^{162}	11010101	D5
β^{108}	10111011	BB		β^{163}	01100100	64
β^{109}	11010110	D6		β^{164}	10101100	AC
β^{110}	01100001	61		β^{165}	11101111	EF
β^{111}	10100011	A3		β^{166}	00101010	2A
β^{112}	11111110	FE		β^{167}	01111110	7E
β^{113}	00011001	19		β^{168}	10000010	82
B^{114}	00101011	2B		β^{169}	10011101	9D
β^{115}	01111101	7D		β^{170}	10111100	BC
β^{116}	10000111	87		β^{171}	11011111	DF
β^{117}	10010010	92		β^{172}	01111010	7A
β^{118}	10101101	AD		β^{173}	10001110	8E
β^{119}	11101100	EC		β^{174}	10001001	89
β^{120}	00101111	2F		β^{175}	10000000	80
β^{121}	01110001	71		β^{176}	10011011	9B
β^{122}	10010011	93		β^{177}	10110110	B6
β^{123}	10101110	AE		β^{178}	11000001	C1
β^{124}	11101001	E9		β^{179}	01011000	58
β^{125}	00100000	20		β^{180}	11101000	E8
β^{126}	01100000	60		β^{181}	00100011	23
β^{127}	10100000	A0		β^{182}	01100101	65
β^{128}	11111011	FB		β^{183}	10101111	AF
β^{129}	00010110	16		β^{184}	11101010	EA
β^{130}	00111010	3A		β^{185}	00100101	25
β^{131}	01001110	4E		β^{186}	01101111	6F
β^{132}	11010010	D2		β^{187}	10110001	B1
β^{133}	01101101	6D		β^{188}	11001000	C8
β^{134}	10110111	B7		β^{189}	01000011	43
β^{135}	11000010	C2		β^{190}	11000101	C5
β^{136}	01011101	5D		β^{191}	01010100	54
β^{137}	11100111	E7		β^{192}	11111100	FC
β^{138}	00110010	32		β^{193}	00011111	1F
β^{139}	01010110	56		β^{194}	00100001	21
β^{140}	11111010	FA		β^{195}	01100011	63
β^{141}	00010101	15		β^{196}	10100101	A5
β^{142}	00111111	3F		β^{197}	11110100	F4
β^{143}	01000001	41		β^{198}	00000111	07
β^{144}	11000011	C3		β^{199}	00001001	09
β^{145}	01011110	5E		β^{200}	00011011	1B
β^{146}	11100010	E2		β^{201}	00101101	2D
β^{147}	00111101	3D		β^{202}	01110111	77
β^{148}	01000111	47		β^{203}	10011001	99
β^{149}	11001001	C9		β^{204}	10110000	B0
β^{150}	01000000	40		β^{205}	11001011	CB
β^{151}	11000000	C0		β^{206}	01000110	46
β^{152}	01011011	5B		β^{207}	11001010	CA
β^{153}	11101101	ED		β^{208}	01000101	45
β^{154}	00101100	2C		β^{209}	11001111	CF
β^{155}	01110100	74		β^{210}	01001010	4A
β^{156}	10011100	9C		β^{211}	11011110	DE
β^{157}	10111111	BF		β^{212}	01111001	79
β^{158}	11011010	DA		β^{213}	10001011	8B
β^{159}	01110101	75		β^{214}	10000110	86
β^{160}	10011111	9F		β^{215}	10010001	91

β^{216}	10101000	A8		β^{250}	01101100	6C
β^{217}	11100011	E3		β^{251}	10110100	B4
β^{218}	00111110	3E		β^{252}	11000111	C7
β^{219}	01000010	42		β^{253}	01010010	52
β^{220}	11000110	C6		β^{254}	11110110	F6
β^{221}	01010001	51		β^{255}	00000001	01
β^{222}	11110011	F3				
β^{223}	00001110	0E				
β^{224}	00010010	12				
β^{225}	00110110	36				
β^{226}	01011010	5A				
β^{227}	11101110	EE				
β^{228}	00101001	29				
β^{229}	01111011	7B				
β^{230}	10001101	8D				
β^{231}	10001100	8C				
β^{232}	10001111	8F				
β^{233}	10001010	8A				
β^{234}	10000101	85				
β^{235}	10010100	94				
β^{236}	10100111	A7				
β^{237}	11110010	F2				
β^{238}	00001101	0D				
β^{239}	00010111	17				
β^{240}	00111001	39				
β^{241}	01001011	4B				
β^{242}	11011101	DD				
β^{243}	01111100	7C				
β^{244}	10000100	84				
β^{245}	10010111	97				
β^{246}	10100010	A2				
β^{247}	11111101	FD				
β^{248}	00011100	1C				
β^{249}	00100100	24				

Tablo 9. 11. $\beta = \alpha + 1$ üreteci ile $p(x)=x^8+x^4+x^3+x+1$ indirgenemez polinomuna göre $GF(2^8)$ sonlu cisminin elemanlarının gösterimi

Yukarıdaki Tablo 9.11. (Aslan, 2008) kaynağından alınmıştır.

BÖLÜM 10.

10. GF(2^n) SONLU CİSİM UZAYINDA ÜRETİLEN MDS KODLAR İLE OLUŞTURULAN GİZLİLİK PAYLAŞIM ŞEMASINDA HİLELİ KATILIMCILARI TESPİT ETMEK VE KİMLİKLENDİRMEK

10.1. Hilekar Problemi

Bu bölüme kadar gizlilik paylaşım şemasında katılımcıların hep dürüst olması durumları varsayılarak gizliliğin yeniden elde edilmesi anlatılmıştır. Bununla beraber Anahtar Dağıtım Merkezinin dürüst olduğu ve katılımcıların dürüst olmadığı durumlar vardır.

Shamir'in *(k,n)* eşik şemasında eğer n paylaşımdan bir veya daha fazlası hilekar ise gizliliği bazı *k* paylaşımlar kümesi ile doğru olarak elde etmek mümkün olmayabilir. Hilekarları tespit etme ve kimliklendirme gizliliği doğru olarak yeniden elde etmede çok önemlidir (Araki, 2007 ; Brickell vd., 1990 ; CarpentieriM, 1995 ; CarpentieriM vd., 1994 ; He J. vd., 1998 ; Kurosawa vd., 1995, ; Ogata vd., 2006 ; Pieprzyk vd., 2002 ; Rabin vd.,1989 ; Tompa vd., 1989) yazarlar makalelerinde gizliliği yeniden elde etmede kesinlikle *k* paylaşımcının olmasını göz önünde bulundurmuşlardır. (Bhndo vd., 1993 ; McEliece vd., 1981) yazarlar ise makalesinde hilekarları tespit etmek için kodlama tekniklerinden faydalanan hata doğrulama kod tabanlı gizlilik paylaşım şemasını önermişlerdir. Örneğin McEliece ve Sarwate (McEliece vd., 1981) Reed-Solomon kod tabanlı gizlilik paylaşım şemasını tanımlamıştır. Onların şemasının performansı en fazla *t* adet hilekar içeren

her *k+2t* dürüst katılımcı grubu ile gizliliğin doğru bir şekilde elde edilmesini garanti eder (Harn ve Lin, 2009).

Bu bölümde MDS kod kullanarak oluşturulan gizlilik paylaşım şemasında dürüst olmayan katılımcılar olması durumu incelenmiş ve uygulaması gerçekleştirilmiştir.

Teorem 10. 1: Gizlilik paylaşımı için bir $[k,n]$ eşik şemasında, $k+j$ katılımcılar gizliliği belirleyebilmek için bir araya geldiklerinde $\left[(n-k)/2\right]+k+j-n$'e kadar hileli katılımcının yanlış verisi düzeltilebilir.

İspat: G , [n,k,n-k+1] MDS kodun bir üreteç matrisi olsun. Bu kod $[(n-k)/2]$ hatayı düzeltebilir. Farz edelim $k+j$ katılımcılar arasında t hileli katılımcı var. Eğer $t \le [(n-k)/2]+k+j-n$ ise, burada n paylaşımda en fazla $[(n-k)/2]$ hata vardır. Böylece *t* hata düzeltilebilir.
j parametresi $(n-k+2)/2 \le j \le n-k$ eşitliğini sağlarsa, hileli katılımcıları düzeltebilme yeteneğine sahip olduğu söylenebilir. Bütün n katılımcılar bir araya geldiğinde, sistem $n-k$ hileli katılımcıyı tespit edip, $[(n-k)/2]$ kadarını düzeltebilir (Ding vd., 1997).

10.2. GF(2^3) Sonlu Cisim Uzayında (7, 3, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Sendrom Dekodlama Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirmek

Örnek 10.1: GF(2^3) sonlu cisim uzayında x^3+x+1 indirgenemez polinoma göre (7, 3, 5) MDS kod için hileli katılımcıları tespit edip, düzeltme aşamalarına bakalım. Bu kod $t=(n-k)/2=2$ hata düzeltme kapasitesine sahiptir. Teorem 1'e göre k+j katılımcı bir araya gelip hileli katılımcıları bulabilir. Bu durumda $4 \le j$ şartı altında hileli katılımcıları tespit edebilirler. Diyelim ki P_1, P_2, P_3

katılımcılarından iki tanesi yanlış bilgi gönderdi. Bu aşamaları aşağıdaki gibi gösterelim.

1. Hileli katılımcı var mı yok mu tespit et.

Diyelim $P_1 = \alpha^6,\ \mathrm{P}_2 = \alpha,\ \mathrm{P}_3 = \alpha^2$ paylaşım bilgilerini gönderdi. P_2 ve P_3 yanlış bilgi gönderdi. Ya da bunlar hileli katılımcılar olsun. Diğer katılımcıların bilgileri ise $P_0 = 1,\ \mathrm{P}_4 = \alpha^3,\ \mathrm{P}_5 = \alpha^4, P_6 = \alpha^2$

Öncelikle hata olup olmadığını tespit etmek için alınan kod sözü kontrol matrisinin transpozesi ile çarpılır ve sonuç sıfır değilse hata var demektir.

$$w.H^T = 0 \Rightarrow \textit{hata yok}$$
$$w.H^T \neq 0 \Rightarrow \textit{hata var}$$

Bu durumda alınan vektör $w = (1, \alpha^6, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^2)$ dur. $w.H^T = (1, \alpha^5, \alpha^2, 1) \neq 0$ olduğu için hileli katılımcılar var demektir.

2. Sendromları hesapla.

Sendrom polinomu $w(x) = 1 + \alpha^6 x + \alpha x^2 + \alpha^2 x^3 + \alpha^3 x^4 + \alpha^4 x^5 + \alpha^2 x^6$

Sendrom polinomundan $s_0, s_1, ..., s_{e-1}$ sendromları hesaplanır.

$$s_0 = w(\alpha^0) = w(1) = \alpha^3$$
$$s_1 = w(\alpha) = \alpha^3$$
$$s_2 = w(\alpha^2) = 0$$
$$s_3 = w(\alpha^3) = \alpha$$

3. 10.1 denkleminden hatalı olan bileşenin yerleri tespit edilir.

Örneğimize göre çözelim.

$$\begin{pmatrix} \alpha^3 & \alpha^3 \\ \alpha^3 & 0 \end{pmatrix} \begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha \end{pmatrix} \Rightarrow \sigma_0 = \alpha^5 \ \text{ ve } \ \sigma_1 = \alpha^5 \qquad (10.1)$$

Hata yeri polinomu 10. 2 denklem ile gösterilmiştir.

$$\sigma_A(x) = \sigma_0 + \sigma_1 x + \sigma_2 x^2 + ... + x^e \qquad (10.2)$$

$\sigma_A(x) = (x - a_1).....(x - a_e)$ formunda düzenlenip $a_1,...,a_e$ bulunur. Bunlar hileli katılımcıları tespit eder.

Bu durumda hata yeri polinomundan faydalanarak,

$\sigma_A(x) = \alpha^5 + \alpha^5 x + x^2 = (\alpha^3 + x)(\alpha^2 + x)$

$a_1 = \alpha^2$, $a_2 = \alpha^3$ hata yerleri bulunur. Yani P_2 ve P_3 katılımcıları hileli katılımcılardır.

4. Hatalı olan bileşenler 10.3 denklemi ile düzeltilir.

$$\begin{pmatrix} a_1^0 & a_2^0 & ... & a_e^0 \\ a_1^1 & a_2^1 & ... & a_e^1 \\ . & & & \\ . & & & \\ a_1^{e-1} & a_2^{e-1} & ... & a_e^{e-1} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_e \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \\ \\ s_{e-1} \end{pmatrix} \qquad (10.3)$$

$$\begin{pmatrix} a_1^0 & a_2^0 \\ a_1^1 & a_2^1 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ \alpha^2 & \alpha^3 \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^3 \end{pmatrix}$$

Denklem sistemi çözümünden

$b_1 = \alpha^6$ ve $b_2 = \alpha^4$ elde edilir.

$a_1 = \alpha^2$ ve $a_2 = \alpha^3$ yerlerinde hata oluşmuştu.

$a_1 = \alpha^2$ yerine $b_1 = \alpha^6$
$a_2 = \alpha^3$ yerine $b_2 = \alpha^4$ ile düzeltilir.

Alınan vektör $w = (1, \alpha^6, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^2)$

Hata vektörü $e = (0,0,\alpha^2,\alpha^3,0,0,0)$ $e = (0,0,\alpha^6,\alpha^4,0,0,0)$ düzeltilip "w" ile XOR işlemi yapıldığında doğru kod sözüne ulaşılır.

$$c = w \oplus e = (1,\alpha^6,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^2) \oplus (0,0,\alpha^6,\alpha^4,0,0,0) = (1,\alpha^6,\alpha^5,\alpha,\alpha^3,\alpha^4,\alpha^2)$$

10.3. GF(2^3) Sonlu Cisim Uzayında (7, 3, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirmek Uygulaması

Aşağıda C#' da gerçekleştirilen program ile (7, 3, 5) MDS kod ile gizlilik paylaşımında hileli katılımcılar olması durumu ve bunların tespit edilip doğrulandıktan sonra gizli bileşenin elde edilmesi tablolandırılarak gösterilmiştir.

$GF(2^3)$ sonlu cisim uzayında $x^3 + x^2 + 1$ indirgenemez polinoma göre (7,3,5) MDS kodun üreteç polinomu ve standart formdaki üreteç matrisi G ondalık gösterimi ile aşağıda verilmiştir.

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)$$

$$G = \begin{pmatrix} 1 & 0 & 0 & 5 & 1 & 5 & 4 \\ 0 & 1 & 0 & 3 & 1 & 2 & 2 \\ 0 & 0 & 1 & 7 & 1 & 6 & 7 \end{pmatrix}$$

Paylaşım Kısmı

Mesaj Vektörü	**(2, 4, 5)**

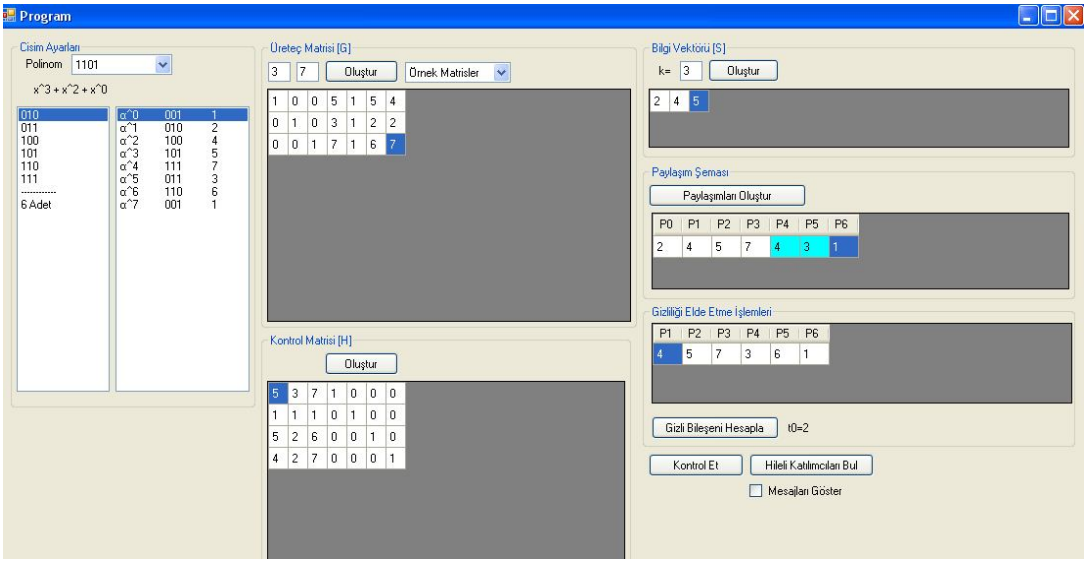
Paylaşımlar	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	**2**
P_1= (1. Katılımcı)	4
P_2= (2. Katılımcı)	5
P_3= (3. Katılımcı)	7
P_4= (4. Katılımcı)	3
P_5= (5. Katılımcı)	6
P_6= (6. Katılımcı)	1

Tablo 10. 1. (7, 3, 5) MDS kod için doğru Paylaşım Değerleri

Diyelim ki P_4 ve P_5 katılımcılarının değerleri yanlıştır. Yani bunlar hileli katılımcılardır ya da her hangi bir sebepten dolayı bozulmuş veya kaybolmuş verilerdir. Aşağıdaki Tablo 10. 2'de hileli katılımcıların yanlış verileri ve diğer katılımcıların doğru verileri gösterilmektedir.

Paylaşımlar	**Gizli Değerlerin Ondalık Gösterimi**
t_0 (gizli bileşen)	2
P_1= (1. Katılımcı)	4
P_2= (2. Katılımcı)	5
P_3= (3. Katılımcı)	7
P_4= (4. Katılımcı)	**4**
P_5= (5. Katılımcı)	**3**
P_6= (6. Katılımcı)	1

Tablo 10. 2. (7,3,5) MDS kod için Gizlilik Paylaşım Şemasında Hileli katılımcıların olması durumu



Yukarıda program çıktısında gösterildiği gibi P_4 ve P_5 hileli katılımcılardır. Bunların yanlış verileri düzeltilerek gizlilik t_0=2 olarak eşik değerdeki katılımcı ile elde edilmiştir.

10.4. GF(2^4) Sonlu Cisimde Üretilen (8, 4, 5) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirme Uygulaması

Örnek 10. 2: Diyelim ki kurulan şemada dürüst olmayan hileli katılımcılar olsun. Böyle bir durumda uygulanan kodun hata bulma algoritması kullanılarak hileli katılımcılar tespit edilip onların hatalarını düzelterek gizli bileşen yeniden elde edilebilir.

Bir önceki bölümde üreteç matrisi verilen (8, 4, 5) MDS kod kullanarak üretilen Gizlilik Paylaşım Şemasında hileli katılımcılar varsa bunun nasıl tespit edildiğini inceleyelim. Bu kodun hata doğrulama, aynı zamanda hileli katılımcıları tespit etme ve doğrulama kapasitesi $t = (n - k/2) = 2$ dir. Daha fazla hileli katılımcıyı tespit edemez.

Verilen bilgi mesajı $m = [\alpha^2, 0, \alpha^3, 0] = [4, 0, 8, 0]$ olsun. Bu bilgi mesajının sorumlu olduğu kod sözcüğü aynı zamanda katılımcıların paylaşım değerleri $c = mG = [\alpha^2, 0, \alpha^3, 0, 1, 1, \alpha^{13}, \alpha^{10}]$ dir. Burada ilk bileşen gizliliği temsil etmektedir.

Paylaşımlar	**Gizli Değerlerin Cisim elemanları ile Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0 (gizli bileşen)	α^2	**4**
P_1= (1. Katılımcı)	0	0
P_2= (2. Katılımcı)	α^3	8
P_3= (3. Katılımcı)	0	0
P_4= (4. Katılımcı)	1	1
P_5= (5. Katılımcı)	1	1
P_6= (6. Katılımcı)	α^{13}	13
P_7= (7. Katılımcı)	α^{10}	7

Tablo 10. 3. (8, 4, 5) MDS kod için Paylaşım Değerleri

Diyelim ki P_2 ve P_4 katılımcılarının değerleri yanlıştır. Yani bunlar hileli katılımcılardır ya da her hangi bir sebepten dolayı bozulmuş veya kaybolmuş verilerdir. Aşağıdaki Tablo 10. 4'de hileli katılımcıların yanlış verileri ve diğer katılımcıların doğru verileri gösterilmektedir.

Paylaşımlar	**Gizli Değerlerin Cisim elemanları ile Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0 (gizli bileşen)	α^2	4
P_1= (1. Katılımcı)	0	0
P_2= (2. Katılımcı)	α	**2**
P_3= (3. Katılımcı)	0	0
P_4= (4. Katılımcı)	α^2	**4**
P_5= (5. Katılımcı)	1	1
P_6= (6. Katılımcı)	α^{13}	13
P_7= (7. Katılımcı)	α^{10}	7

Tablo 10. 4. (8, 4, 5) MDS kod için Gizlilik Paylaşım Şemasında Hileli katılımcıların olması durumu

Şimdi bu katılımcıların nasıl tespit edildiğini ve gönderdikleri yanlış verilerinin düzeltilerek gizli bileşeni elde etmek için uygulanan aşamaları anlatalım.

1. Sendromlar hesaplanır
2. Hata yerleri (ya da hangi katılımcı olduğu) tespit edilir.
3. Hatalar düzeltilir.
4. Kod çözme işlemi tamamlanıp gizli bileşen elde edilir.

1. Sendrom Hesaplama

Alınan polinom

$$r(x) = \alpha^2 + \alpha x^2 + \alpha^2 x^4 + x^5 + \alpha^{13} x^6 + \alpha^{10} x^7$$

$$S_1(\alpha) = 1$$

$$S_2(\alpha^2) = \alpha^{12}$$

$$S_3(\alpha^3) = \alpha^{10}$$

$$S_4(\alpha^4) = \alpha^{11}$$

Sendrom polinomu

$$S(x) = 1 + \alpha^{12} x + \alpha^{10} x^2 + \alpha^{11} x^3$$

	$r_i(X)$	q_i	$t_i = t_{i-2} - q_i t_{i-1}$
-1	x^4		0
0	$S(X)$		1
1	$\alpha^{12} x^2 + \alpha x + \alpha^3$	$\alpha^4 x + \alpha^3$	$\alpha^4 x + \alpha^3$
2	$x + \alpha^{12}$	$\alpha^{14} x + \alpha^8$	$\alpha^3 x^2 + \alpha^7 x + \alpha^{12}$

Tablo 10. 5. (8, 4, 5) MDS kod tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları tespit etmek için Öklid algoritması sonuçları

$W_1(x) = x + \alpha^{12}$

$\sigma_1(x) = \alpha^3 x^2 + \alpha^7 x + \alpha^{12}$

$\sigma_1(x)$ polinomunu birinci dereceden polinoma dönüştürmek için $GF(2^4)$ Galois cisminin $\lambda = \alpha^{12}$ elemanıyla çarpılır. Böylece

$$W(x) = \alpha^{12} x + \alpha^9$$
$$\sigma(x) = x^2 + \alpha^4 x + \alpha^9$$

elde edilir.

Çin araştırması ile hata yeri polinomundan hatalı olan yerler tespit edilir.

Bu yerler α^{11}, α^{13}'tür. Böylece

$\alpha^{11} = \alpha^{-j1} = \alpha^{-4} \Rightarrow j_1 = 4$

$\alpha^{13} = \alpha^{-j2} = \alpha^{-2} \Rightarrow j_2 = 2$

$j_1 = 4$ $j_2 = 2$ yerlerinde hata vardır. Yani bizim uyguladığımız gizlilik paylaşım şemasında P_2 *ve* P_4 katılımcıları dürüst olmayan katılımcılardır. Yanlış bilgi göndermişler. Şimdi bu hatalı iletilen verileri düzeltme işlemlerine bakalım. Öncelikle hata yeri polinomunun türevini alalım.

$\sigma'(x) = \alpha^4$

Hata değerleri

$$e_{j1} = \frac{W(\alpha^{-j1})}{\sigma'(\alpha^{-j1})} = \frac{W(\alpha^{11})}{\sigma'(\alpha^{11})} = \frac{\alpha^{12}}{\alpha^4} = \alpha^8$$

$$e_{j2} = \frac{W(\alpha^{-j2})}{\sigma'(\alpha^{-j2})} = \frac{W(\alpha^{13})}{\sigma'(\alpha^{13})} = \frac{\alpha^{13}}{\alpha^4} = \alpha^9$$

Hata polinomu

$e(x) = \alpha^9 x^2 + \alpha^8 x^4$

Böylece alınan vektöre hata vektörü eklenerek doğru vektör elde edilir

$d(x) = r(x) + e(x) = [\alpha^2, 0, \alpha^3, 0, 1, 1, \alpha^{13}, \alpha^{10}]$

Şimdi rastgele seçilen P_1, P_2, P_5, P_7 katılımcıları ile gizli bileşeni elde edebiliriz.

$$g_0 = \sum_{j=1}^{k} x_j g_{i_j} = \sum_{j=1}^{4} x_j g_j = x_1 g_1 + x_2 g_2 + x_5 g_5 + x_7 g_7$$

$x_1 = \alpha^8, x_2 = \alpha^8, x_5 = \alpha^5, x_7 = \alpha^{11}$ elde edilir.

Gizli bileşen $t_0 = sg_0 = \sum_{j=1}^{k} x_j sg_{i_j} = \sum_{j=1}^{k} x_j t_{i_j}$ denklem sisteminin çözümü ile elde edilir.

$t_0 = x_1 P_1 + x_2 P_2 + x_5 P_5 + x_7 P_7$

$t_0 = \alpha^4$

Hileli katılımcıları bulmak için C#' da yazılan programın pseudo kodu aşağıdaki gibidir.

(n,k,d) kodun Hileli Katılımcıları Bulma

```
r=hatalı paylaşım vektörü
For i=0 to n-k
        Begin
                S[i]= r[cismin primitif elemanı ^ i+1]
        End
W= Euclidean_Algoritması_kalan(S)
Sigma= Euclidean_Algoritması_bolum(S)
hata=0
For i=0 to cismin elaman sayısı
        Begin
                Kok=0
                Kok=kok xor sigma[cismin i. elemanı]
        if kok=0 then
                Begin
                        Kok[hata]=cisim[i]
                        hata=hata + 1
                End
```

End

Sigma_t=turev_al(sigma)

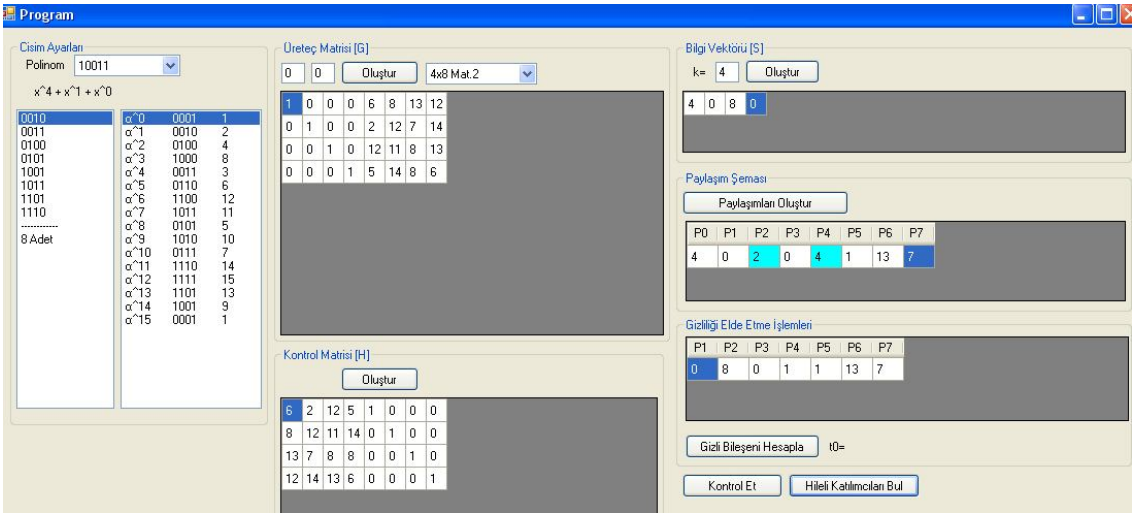
For i=0 **to** hata

Begin

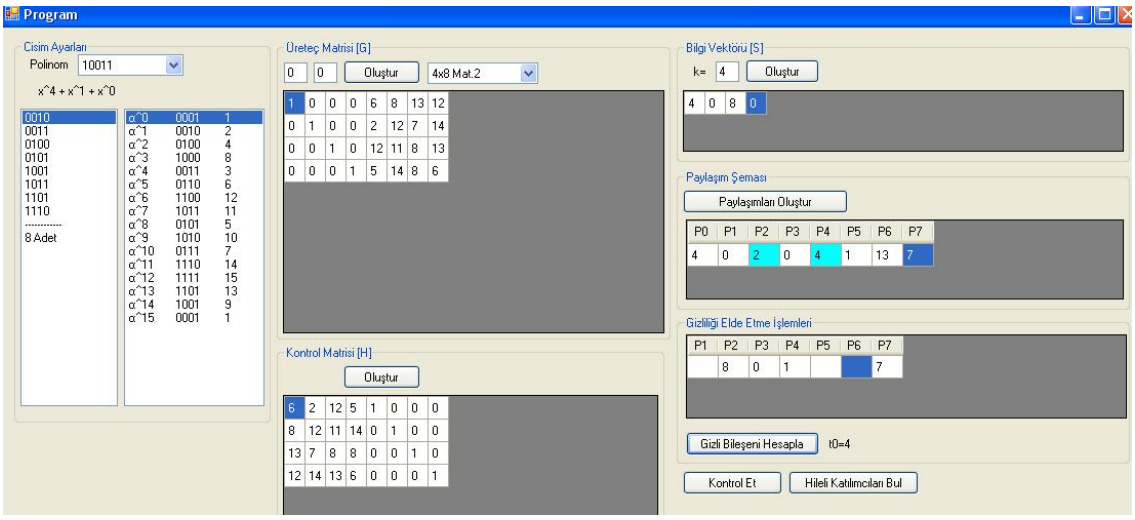
E[i]=W[1/kok[i]] / sigma_t[1/kok[i]]

End

Yukarıda açıkça anlatılan aşamalar yazılan C # program kodu ile gerçekleştirilmiş ve ekran çıktısı aşağıda gösterilmiştir.



Programda da gösterildiği gibi P_2 ve P_4 katılımcıları hileli katılımcılardır. Bir sonraki adımda onların yanlış verileri düzeltilerek rastgele dört katılımcı ile gizliliğin t_0=4 olarak yeniden elde edildiği gösterilmiştir.



10.5. GF(2^4) Sonlu Cisimde Üretilen (11, 5, 7) MDS Kodu ile Oluşturulan Gizlilik Paylaşım Şemasında Öklid Algoritması Kullanarak t-Hileli Katılımcıları Tespit Etmek Ve Kimliklendirme Uygulaması

Aşağıda C#' da gerçekleştirilen program ile üreteç matrisi bir önceki bölümde verilen (11, 5, 7) MDS kod ile gizlilik paylaşımında hileli katılımcılar olması durumu ve bunların tespit edilip doğrulandıktan sonra gizli bileşenin elde edilmesi tablolandırılarak gösterilmiştir. Bu kodun hata doğrulama, aynı zamanda hileli katılımcıların yanlış verilerini düzeltme kapasitesi $t = (n - k/2) = 3$ tür.

Paylaşım Kısmı

Mesaj Vektörü	**(3, 10, 12, 13, 9)**

Paylaşımlar	**Gizli Değerlerin Cisim Elemanları ile Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	α^4	**3**
P_1= (1. Katılımcı)	α^9	10
P_2= (2. Katılımcı)	α^6	12
P_3= (3. Katılımcı)	α^{13}	13
P_4= (4. Katılımcı)	α^{14}	9
P_5= (5. Katılımcı)	α^4	3
P_6= (6. Katılımcı)	α^3	8
P_7= (7. Katılımcı)	α^3	8
P_8= (8. Katılımcı)	α^5	6
P_9= (9. Katılımcı)	α	2
P_{10}= (10. Katılımcı)	α^{10}	7

Tablo 10. 6. GF(2^4)'de (11, 5, 7) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasın' da doğru paylaşım değerleri

P_1, P_4, ve P_7 yanlış veri göndermiş olsun. Yani hileli katılımcılar olsun.

Paylaşımlar	**Gizli Değerlerin Cisim Elemanları ile Gösterimi**	**Gizli Değerlerin Ondalık Gösterimi**
t_0= gizli bileşen	α^4	3
P_1= (1. Katılımcı)	α^7	**11**
P_2= (2. Katılımcı)	α^6	12
P_3= (3. Katılımcı)	α^{13}	13
P_4= (4. Katılımcı)	α^5	**6**
P_5= (5. Katılımcı)	α^4	3
P_6= (6. Katılımcı)	α^3	8
P_7= (7. Katılımcı)	α^{10}	**7**
P_8= (8. Katılımcı)	α^5	6
P_9= (9. Katılımcı)	α	2
P_{10}= (10. Katılımcı)	α^{10}	7

Tablo 10. 7. GF(2^4)'de (11, 5, 7) MDS kodu ile oluşturulan Gizlilik Paylaşım Şemasın'da hileli katılımcıların olması durumu

	$r_i(X)$	q_i	$t_i = t_{i-2} - q_i t_{i-1}$
-1	x^6		0
0	$S(X) = \alpha^9 x^5 + \alpha^5 x^4 + \alpha^{14} x^3 + \alpha^9 x^2 + \alpha^6 x + \alpha^4$		1
1	$\alpha^{13} x^4 + \alpha^4 x^3 + x^2 + \alpha x + \alpha^6$	$\alpha^6 x + \alpha^2$	$\alpha^6 x + \alpha^2$
2	$\alpha^8 x^3 + \alpha^9 x^2 + \alpha^8 x + \alpha^7$	$\alpha^{11} x + \alpha^{12}$	$\alpha^2 x^2 + \alpha^8 x + \alpha^3$
3	$w = x^2 + \alpha^3 x + \alpha^7$	$\alpha^5 x + \alpha$	$\alpha^7 x^3 + \alpha^8 x^2 + \alpha^4 x + \alpha^{10}$
4			$\sigma = x^3 + \alpha\ x^2 + \alpha^{12} x + \alpha^3$

Tablo 10. 8. Hileli katılımcıları bulmak için kullanılan Öklid algoritmasının sonuçları

$\sigma = x^3 + \alpha\ x^2 + \alpha^{12} x + \alpha^3$ $\qquad w = x^2 + \alpha^3 x + \alpha^7$

$\sigma' = x^2 + \alpha^{12}$

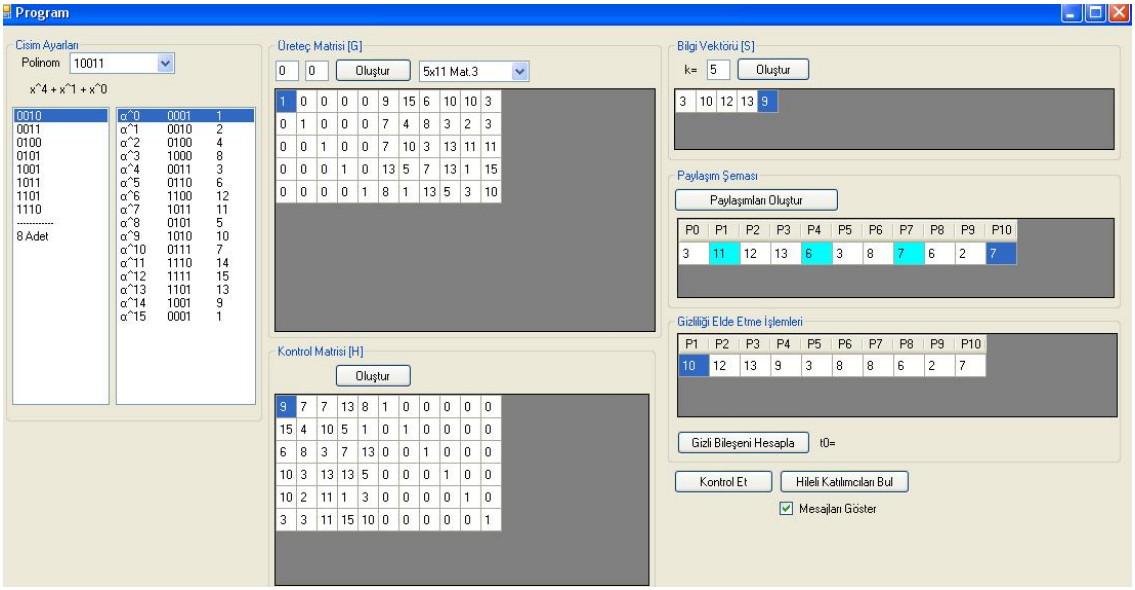
$e(x) = \alpha^{12} x^7 + \alpha^{12} x^4 + x$

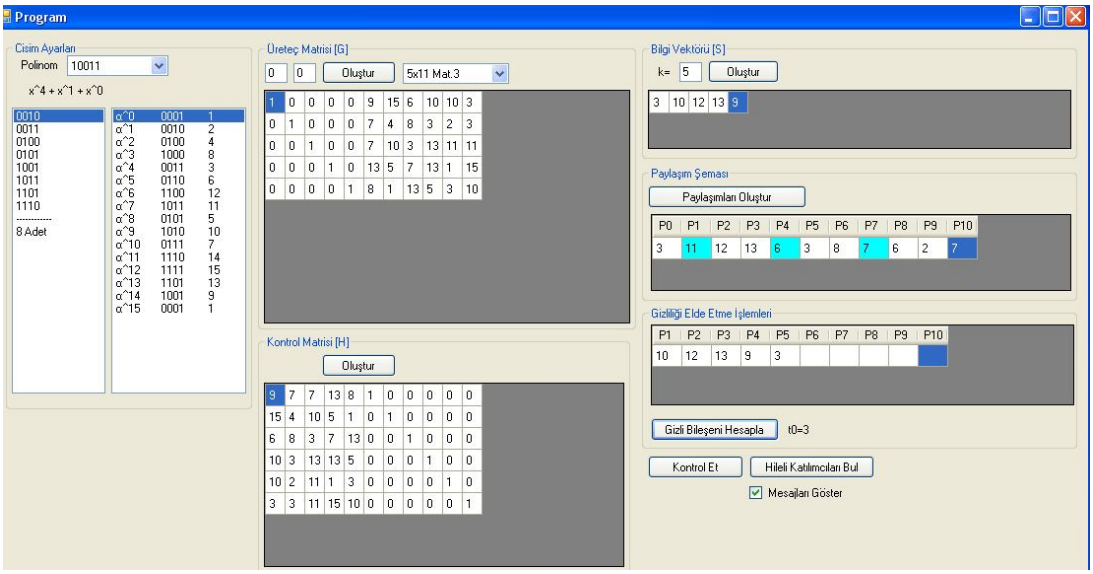
Hataları düzeltilmiş

vektör:

$\alpha^{10} x^{10} + \alpha x^9 + \alpha^5 x^8 + \alpha^3 x^7 + \alpha^3 x^6 + \alpha^4 x^5 + \alpha^{14} x^4 + \alpha^{13} x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^4$

Hileli katılımcıların yanlış verileri düzeltildikten sonra rastgele seçilen beş katılımcı ile gizliliğin t_0 =3 olarak yeniden elde edildiği durumun ekran çıktısı aşağıda gösterilmiştir.





Seçilecek farklı bilgi vektörleri için hileli katılımcıları tespit etmek ve kimliklendirmek mümkündür.

11. SONUÇLAR VE DEĞERLENDİRME

Bu tezde güvenliği arttırmak için geliştirilmiş kriptografik anahtar yönetimi ve anahtar dağıtımı ile ilişkili Gizlilik paylaşım şemaları incelenmiştir. Çeşitli yapılarda gizlilik paylaşım şemaları mevcuttur. Bunlardan bazıları kodlama teorisi tabanlı gizlilik paylaşım şemalarıdır. Bu tezde kodlama teorisi ile özellikle RS kodların özel bir sınıfı olan MDS kodlar ile ilişkilendirilmiş gizlilik paylaşım şemalarının kurulabildiği ve verilen kodlarla yapılan dağıtım şeması ve eşik değerdeki paylaşımlarla gizli bileşene ulaşılabildiği gösterilmiştir. Sonuç olarak MDS kodlar ile Gizlilik Paylaşım Şemaları oluşturmak mümkündür.

Ayrıca Gizlilik paylaşım şemalarında hileli katılımcılar olduğu zaman gizliliği yeniden elde etmek her zaman mümkün değildir. Hatalı veriyi tespit etmek ve kimliklendirmek gizliliği yeniden elde etmede oldukça önemlidir. Bu tezde ayrıca MDS kod kullanarak tasarlanan Gizlilik paylaşım şemasında, hileli katılımcılar olması durumu incelenmiş ve RS kodların hata doğrulama kod tekniklerinden faydalanılarak hileli katılımcılar tespit edilip onların bozuk paylaşımları düzeltilerek gizliliğin yeniden elde edildiği gösterilmiştir.

MDS kodlar minimum Hamming mesafesi en fazla olan kodlar olduğu için hata düzeltme kapasitesi dolayısıyla an fazla hileli katılımcı bulma özelliğine sahiptir.

TEZ SÜRESİNCE YAPILAN ÇALIŞMALAR

Uluslararası Kongre ve Sempozyum Bildirileri

1. Arda D., Buluş E., Yerlikaya T., " MDS Kod Tabanlı Kriptografik Gizlilik Paylaşım Şeması", pp 118-121, 4th International Information Security & Cryptology Conference ISC2010, Ankara, TÜRKİYE, Mayıs 2010

2. Arda D., Buluş E., "Cryptographic Shamir Secret Sharing Scheme and Relations with Reed Solomon Codes", International Scientific Conference Unitech'09 Proceedings, I-399 - I-402 pp., Gabrovo, Bulgaristan, Kasım 2009

3. Arda D., Buluş E., Akgün F., Yerlikaya T.,"Secret Sharing Schemes in Cryptographic Key Management Problem", International Scientific Conference Unitech'08 Proceedings, I-292 - I-295 pp, UNITECH'08, Gabrovo-BULGARISTAN, Kasım-2008

4. Akgün F., Buluş E.**,** Arda D., "A research about European and USA communication system for 3G", International Scientific Conference Unitech'08 Proceedings , I-277 - I-282 pp ,UNITECH'08, Gabrovo-BULGARISTAN, Kasım-2008

5. Arda D., Buluş H. N, Buluş E, "Performance Comparasion Between English and Turkish Alphabet according to The Cryptanalysis of Afine Ciphers", Page 366-370, VolumeI, International Scientific Conference Unitech 2007, Gabrovo-BULGARIA, November-2007

Ulusal Kongre ve Sempozyum Bildirileri

1. Arda D., Buluş E., "Çin Kalan Teoremini Kullanan bir Gizlilik Paylaşım Şeması", ITUSEM2009 IV.İletişim Teknolojileri Ulusal Sempozyumu, 23-26 pp., Adana-TÜRKİYE, Ekim-2009

2. Arda D., Buluş E., "MDS Kod Tabanlı bir Asimetrik Kriptosistemi Uygulaması", ITUSEM2009 ,IV.İletişim Teknolojileri Ulusal Sempozyumu, 83-88 pp., Adana, TÜRKİYE, Ekim-2009

KAYNAKLAR

Akbaş, T., 2007, “Geometrik inşa kodlarının üretimi ve başarımı”, Doktora Tezi, İstanbul.

Arda D., Buluş E., Yerlikaya T., 2010, “ MDS Kod Tabanlı Kriptografik Gizlilik Paylaşım Şeması”, pp 118-121, 4th International Information Security & Cryptology Conference ISC2010, Ankara, TÜRKİYE.

Arda D., Buluş E., 2009, "Çin Kalan Teoremini kullanan bir Gizlilik Paylaşım Şeması", pp 23-26, ITUSEM2009, IV.İletişim Teknolojileri Ulusal Sempozyumu, Adana TÜRKİYE.

Arda D., Buluş E., Akgün F., Yerlikaya T., 2008, “ Secret Sharing Scheme in Cryptographic Key Management Problem”, International Scientific Conference UNITECH’08 Gabrovo.

Arda D., Buluş E., 2009, “MDS Kod Tabanlı bir Asimetrik Kriptosistemi Uygulaması”, pp 83-88, ITUSEM2009, IV.İletişim Teknolojileri Ulusal Sempozyumu, Adana-TÜRKİYE.

Araki T., 2007, “ Efficient *(k, n)* threshold secret sharing schemes secure against cheating from $n-1$ cheaters”. In: Proceedings of ACISP’07, LNCS, vol. 4586, pp. 13–142. Springer-Verlag

Aslan F. Y., Sakallı M. T., Aslan B., Bulut S., 2011 “A New Involutory 4×4 MDS Matrix for the AES-like Block Ciphers”, International Review on Computers and Software, Vol. 6, n.1, pp. 96-103.

Asmuth C. A. , Bloom J.,1983, “A modular approach to key safeguardin”, IEEE Transactions on Information Theory, IT-29(2): 208-210.

Aslan B., 2008, “Boole Fonksiyonları ve S-Kutularının Kriptografik Özelliklerinin İncelenmesi ve Ters Haritalama Tabanlı Cebirsel Açıdan Güçlendirilmiş Bir S-Kutusu Önerisi”, Yüksek Lisans Tezi.

Başkök M.D., “AES Şifreleme Algoritmasının Modellenmes*i*”, Master Tezi, Ekim 2007.

Bilgiç H., 2009, “Soyut Matematik Ders Notları”, Kahramanmaraş Sütçü İmam Üniversitesi.

Brickell E.F., Stinson D.R.,1990, “ The detection of cheaters in threshold schemes” In: Proceedings of Crypto’88,LNCS, vol. 403, pp. 564–577. Springer-Verlag .

Bose, R. C. ve Ray-Chaudhuri, D. K., 1960, “On a Class of Error Correcting Binary Group Codes”, Information Control, 3: 68-79.

Bossert, M., 1999, “Channel Coding”, Wiley, 0-471-98277.

Berrou, C., Glavieux, A. ve Thitimajshima, P., 1993, “Near Shannon Limit Error-Correcting Coding and Decoding: Turbo Codes”, Proc. IEEE Intl Conf. Commun. (ICC 93), pp.1064-70, Geneva, Switzerland.

Berrou, C. ve Glavieux, A., 1996, “Near Optimum Error Correcting and Decoding: Turbo codes”, IEEE Trans. Commun., COM-44:1261-71.

Blakley, G. R., 1979, “ Safeguarding cryptography keys”, Proc. AFIPS 1979 National Computer Conference, 48, 313-317.

Bhondo C., De Santis A., Gargano L., Vaccaro U., 1993, " Secret sharing schemes with veto capabilities", In: Proceedings of the First French-Israeli Workshop on Algebraic Coding, LNCS, vol.781, pp. 82- 89. Springer-Verlag.

Bruen A. A., Forcinito M. A., 2005, " Cryptography, Information Theory, and Error-Correction", John Wiley&sons, Inc.,Hoboken, New Jersey.

CarpentieriM., De Santis A., Vaccaro U.,1994, " Size of shares and probability of cheating in threshold schemes" In: Proceedings of Eurocrypt'93, LNCS, vol. 765, pp. 118–125. Springer-Verlag.

CarpentieriM.,1995, " A perfect threshold secret sharing scheme to identify cheaters" Des. Codes Cryptogr. 5(3),183–187.

Chapman, H. 1996, "Coding Theory", St Edmundsbury Pres, 12-105, Great Britian.

Chien R. T., 1964, " Cyclic decoding procedure for the Bose-Chaudhuri Hocquenghem codes." IEEE Transactions on Information Theory, IT-10:357–363

Ding C. , Laihonen T., Renvall A., 1997, " Linear Multisecret-Sharing Schemes and Error-Correcting Codes" volume 3, pages 1023-1036, Journal of Universal Computer Science.

Diffie W., Hellman M.E.,1976, "New Directions in Cryptography", IEEE Trans. IT-22, no. 6, 644–654.

Denning D. E. R, 1982, "Cryptography and Data Security", Addison-Wesley Publishing Company.

Elias, P., 1954, "Error-Free Coding", IRE Trans. Inform. Theory, PGIT-4: 29-37.

Ellison C., Schneier B.,2000, "*Ten* Risks of PKI: What You're Not Being Told About Public Key Infrastructure", Computer Security Journal, vol. 16, no. 1, pp. 1-7.

Golay, M. J. E., 1949, "Notes on Digital Coding", Proc. IEEE, 37:657.

Gallager, R. G., 1962, "Low Density Parity Check Codes", IRE Trans. Inform. Theory, IT-8: 21-28.

Gallager, R. G., 1963, "Low Density Parity Check Codes MIT Press, Cambridge.

Galstad J., 2009, "Reed Solomon Error Correction Coding, JRM Consultants,Inc. http://www.jrmconsultants.com/images/ecc_whitepaper.pdf

Harn L., Lin C., 2009, " Detection and identification of cheaters in (t,n) secret sharing scheme", Des. Codes Cryptography, 52 (1), 15-24.

Hamming, R. W., 1950, "Error Detecting and Error Correcting Codes", Bell Sys. Tech. J., 29:147-60.

Hocquenghem, A., 1959, "Codes Corecteurs d'erreurs", Chiffres, 2:147-56.

He J., Dawson E.,1998, " Shared secret reconstruction" Des. Codes Cryptogr. 14(3), 221–237

Iftene S., 2007, " Secret Sharing Schemes with Applications in Security Protocols", Ph.D. Thesis.

Kaya K, Selçuk A. A., 2007, " Threshold cryptography based on Asmuth-Bloom secret sharing", Information Sciences, 177(19):4148-4160.

Keyman E., Yıldırım M., 2004, "Kriptografiye Giriş Ders Notları", Uygulamalı Matematik Enstitüsü Kriptoloji Bölümü ODTU.

Koblitz, N., 1994, "A course in Number theory and Cryptography", Springer Verlag

Kurosawa K., Obana S., Ogata W.,1995, " *t*-cheater identifiable *(k, n)* secret sharing schemes" In: Proceedings of Crypto'95, LNCS, vol. 963, pp. 410–423. Springer-Verlag

Ling, S., Xing, C., 2004, " Coding Theory-A first course", Cambridge University.

Lidl R., Niederreiter H.,1994, " Introduction to finite fields and their applications", Revised edition, Cambridge University Press.

Levi A., Özcan M.,2002, "Açık Anahtar Tabanlı Şifreleme Neden Zordur?" Türkiye Bilişim Konferansı.

Lin, S.ve Costello, D. J., 2004, "Error Control Coding", second edition, Prentice Hall, 0-13-017973-6.

Li, J., Narayanan, K. R. ve Georghiades, C. N., 2004, "Product Accumulate Codes: A Class of Codes with Near-Capacity Performance and Low Decoding Complexity", IEEE Trans.Inform. Theory, vol.50, no.1, pp. 31-46.

McEliece R. J., Sarwate D. V., 1981,"On sharing secrets and Reed Solomon Codes", Comm. ACM 24, 583-584.

Moreire J. C., Farrell P.G., 2006 "Essential of Error-Control Coding"John Wiley &Sons Ltd, West Sussex, England.

Mezenes, A., J., Van Oorschot, P., C. And Vanstone, S.,October 1996, "A., Handbook of Applied Crptography", CRC Press,

Muller, D.E., 1954, “Applications of Boolean Algebra to SwiKKhing Circuits Design and to Error Detection”, IRE Trans., EC-3: 6-12.

Macwilliams, F. J. ve Sloane N. J. A., 1977, “The Theory of Error-Correcting Codes”, North Holland, Amsterdam, 0- 444-85193-1.

McEliece R.J, 1978,“. A public-key cryptosystem based on algebraic coding theory.”DSN Prog. Rep., Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, Jet Prop. Lab., California Inst. Technol.,Pasadena, CA.

Mackay, D. J. C. ve Neal, R. M., 1996, “Near Shannon Limit performance of Low Density Parity Check Codes, Electronics Letter, 32(18): 1645-46.

Mignotte M., 1983, “How to share a secret”, In T. Beth, editor, Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuertein, 1982, volume 149 of Lecture Notes in Computer Science, pages 371-375. Springer- Verlag.

Massey J.L., 2001, “Some Applications of Code Duality in Cryptography”, in Matemática Contemporânea, vol. 21 (Eds. N. Rocco and S. Sidki).Sociedade Brasileira de Matemática, pp. 187- 209.

Moreira J.C., Farrell P.G., 2006 “Essentials of Error-Control Coding”, John Wiley&Sons, Ltd.

National Institute of Standards and Technology. Data encryption standard (DES). Federal Information Processing StandardsPublication, National Technical Information Service, Spring_eld, VA, Apr., rea_rmed version available online at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf ,46(3), 1977.

National Institute of Standards and Technology. Advanced encryption standard (AES). Federal Information Standards Publication http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 197(26), 2001.

Niederreiter H., 1986, " Knapsack-type cryptosystems and algebraic coding theory." Prob. Contr. Inform. Theory, 15(2):157–166, 1986.

Ogata W., Kurosawa K., Stinson D.R., 2006," "Optimum secret sharing scheme secure against cheating" SIAM J. Discrete Math. 20(1), 79–95 .

Özadam H., Özbudak F., Saygı Z., 2007, "Secret sharing schemes and linear codes", Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı 101-106, Ankara, Türkiye

Pang L.-J., Wang Y.-M , 2005, "A new (t,n) multi-secret sharing scheme based on Shamir's secret sharing", Applied Mathematics and Computation 167, 840-848.

Pellikaan R, Wu X.W, Bulygin S., 2011, "Error Correcting codes and Cryptology", Cambridge University Pres.

Pless, V., 1989, "Introduction to the Theory of Error-Correcting Codes"

Plotkin, M., 1960, "Binary Codes with Specific Minimum Distance", IEEE Trans. Inform.Theory, IT-34: 1152-1187.

Pieprzyk J., Zhang X.M., 2004, "Ideal threshold schemes from mds codes.",Discrete Mathematics and Theoretical Computer Science, 6(2):471-482.

Prange, E., 1957, "Cyclic Error-Correcting Codes in two Symbols", AFCRC-TN-57,103, Air Force Cambridge Research Center, Cambridge.

Pieprzyk J., Zhang X.M.,2002, " Cheating prevention in linear secret sharing" In: Proceedings of ACISP'02, LNCS, vol. 2384, pp. 121–135. Springer-Verlag

Reed, I. S., 1954, "A class of Multiple-Error-Correcting Codes and the Decoding Scheme", IRE Trans., IT-4: 38-49.

Reed, I. S. ve Solomon, G., 1960, "Polynomial Codes over Certain Finite Fields", J. Soc.Ind. Applied Mathematics, 8: 300-304.

Rivest R.,. Shamir A., Adleman L.,1978, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, v. 21, n. 2, pp. 120-126.

Richardson, T., Urbanke, R., 2005, "Modern Coding Theory", http://lthcwww.epfl.ch/mct/index.php

Rabin T., Ben-Or M.,1989, " Verifiable secret sharing and multiparty protocols with honest majority", In: Proceedings of the 21st Annual ACM Symposium on the Theory of Computing, pp. 73–85.

ROMAN S., 1992, "Coding and Information Theory", Graduate Text in Mathematics, Springer Verlag.

Schoenmaker B., 2011, "Cryptography 2/Cryptographic Protocols", Lecture Notes Part 1 Cryptographic Protocols, version 0.999, The Netherlands.

Stinson D. R., 2002, "Cryptography: Theory and Practice", Second Edition, CRC Press.

Shao J., Cao Z.-F., 2005,"A new efficient (t,n) verifiable multi-secret sharing (VMSS) based on YCH scheme", Applied Mathematics and Computation 168, 135-140.

Schneider B., 1996, ”Applied Cryptography Second Edition”, John Wiley & Sons, Inc.,New York.

Shannon, C. E., 1948, “A Mathematical Theory of Communication”, Bell Sys. Tech. J.,pp.379-423 (Part 1); pp. 623-656 (Part 2)

Secret Sharing ,CPT, 2006,Version 3.

Shamir,A., 1979, “How to share a secret”, Communication of the ACM, 22, 612-613.

Tsunoo Y., Tsujihara E., Minematsu K., Miyauchi H.,2002, ”Cryptanalysis of Block Ciphers Implemented on Computers with Cache”, ISITA.

Trappe W., Washington L.C., 2002, “Introduction to Cryptography with Coding Theory”, Prentice Hall.

Thibault P., Vincent P.,2009, “Training course report Generalisation of Shamir Secret Sharing Scheme”, India.

Trappe W., Washington L.,2006, “ Introduction to Cryptography with Coding Theory Second Edition”, Pearson Prentice Hall.

Tompa M., Woll H., 1989, “ How to share a secret with cheaters” J. Cryptol. 1(3), 133–138

Wicker, S. B., 1995, “Error Control Systems for Digital Communications and Storage”,Prentice Hall, Englewood Cliffs,N.J., 0132008092.

Wagner, N. R.,2003 “The Laws of Cryptography with Java Code”. [PDF].

Xiaoqing T.,Zhiguo W, 2004, “New secret sharing scheme based on lin-ear code”. Applied Mathematics - A Journal of Chinese Universities,19(2):160-166.

Yang C.-C., Chang T.-Y., Hwang M.-S., 2004, “A (t,n) multi-secret sharing scheme”, Applied Mathematics and Computation 151, 483–490.

Zhao J., Zhang J., Zhao R., 2007, “ A practical verifiable multi-secret sharing scheme”, Computer Standards & Interfaces 29 (1) ,138–141.

Zorlu Y., 2006, “ Reed-Solomon Kodların AWGN ve Rayleigh Kanallarda Başarım Analizi”, Yüksek Lisans Tezi.

Zhu B., Bao F., Deng R.H., Kankanhalli M. S., Wang G., 2005, “ Efficient and robust key management for large mobile ad hoc Networks”, Computer Networks, Volume 48, Issue 4, Pages 657-682.

ÖZGEÇMİŞ

Derya ARDA 1975 yılında Kırklareli' de doğdu. İlk ve Orta öğrenimini Babaeski' de tamamladıktan sonra 1994 yılında girdiği Trakya Üniversitesi Fen-Edebiyat Fakültesi Matematik Bölümünden 1998 yılında mezun oldu. 1999 yılında Trakya Üniversitesi Müh. Mim. Fak. Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi kadrosuna atandıktan sonra 2000-2003 yılları arasında Trakya Üniversitesi Fen Bilimleri Enstitüsüne bağlı olarak Bilgisayar Mühendisliği Anabilim Dalında Yüksek Lisans eğitimini tamamladı. 2005 yılında aynı enstitüde Doktora eğitimine başladı. Evli ve bir kızı olan Derya ARDA halen Trakya Üniversitesi Müh. Mim. Fak. Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır.