MDS KOD TABANLI BİR ASİMETRİK KRİPTOSİSTEMİ UYGULAMASI

[1]Derya ARDA **[2]Ercan BULUŞ**

[1]Trakya Ünv. Müh.Mim.Fak.
Bilgisayar Müh. Bölümü 22030 Edirne
[2]Namık Kemal Ünv. Çorlu Müh. Mim.
Fak. Bilgisayar Müh. Bölümü Çorlu

[1]deryaa@trakya.edu.tr [2]ercanbulus@corlu.edu.tr

ÖZET

Güvenli bir şekilde haberleşmeyi sağlamak için ağırlıklı olarak kriptolojik yöntemlere başvurulmaktadır. Asimetrik yani Açık-anahtarlı sistemler gizlilik, bütünlük, inkar edememe ve asıllama gibi güvenlik mekanizmalarını sağlamak üzere geliştirilmiş kriptolojik yaklaşımlardan biridir. Açık-anahtar şifreleme için çok çeşitli teknikler vardır. Bunlardan birisi hata doğrulama kod tabanlı McEliece açık anahtar şifrelemesidir. Bu çalışmada bir hata doğrulama kod olan Reed-Solomon kodun özel bir durumu olan MDS(maksimum uzaklıkla ayrılabilen) kod kullanarak açık anahtar kriptosisteminin bir uygulaması gerçekleştirildi. Bu kriptosistemin güvenliği MDS kodun G üreteç matrisinin gizliliği ve G'nin tekrarlama sayısıdır. Kriptosistemin avantajı ise açık metinin büyüklüğünün şifreli metinin büyüklüğü ile aynı olmasıdır. Bu sistemin diğer sistemlerle karşılaştırıldığında daha ekonomik olduğu ve zamandan tasarruf sağladığı söylenebilir. Ayrıca böyle sistemler açık-metin şifreli-metin saldırılarına karşı dayanıklıdır.

Anahtar Kelimeler: Açık Anahtarlı Kriptosistem, Kriptografi, Kodlama Teorisi, MDS Kodlar

1. GİRİŞ

Çağdaş kriptografi ve kodlama teorisi 60 yıldan daha fazla başarılı bir tarihe sahiptir. 1948' de Claude Shannon[1] "Haberleşmenin Matematiksel Teorisi" adlı makalesinde bilgi teorisi ve kodlama teorisi gibi iki disiplini başlatıp geliştirmiştir.

Kriptografi ve kodlama teorisinin bilgi iletişiminde amaçları farklıdır. 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 iletim sırasında oluşan hataları doğrulamak anlamında güvenli iletişim sağlamaktır.

Hem kodlama teorisi hem de kriptografi bilgi çağımızda gerekli olmuştur. Son yıllarda özellikle internet yolu ile iletim, sıkıştırma ve depolamada veri miktarında büyük bir artış olmuştur. Bu sebepten dolayı etkin, güvenilir ve güvenli haberleşme ihtiyacı çok daha önem kazanmıştır. Hata-doğrulama kodları ve kriptografi bu problemleri çözmede temel rol oynamaktadır.

Kriptografide iki çeşit kriptosistem vardır. Bunlardan birisi simetrik(gizli anahtar) kriptosistemdir. Şifreleme ve şifreyi çözmede aynı anahtarın kullanıldığı yöntemdir. AES, DES, IDEA, Skipjack, RC5, RC2, RC4 gibi algoritmalar simetrik şifreleme algoritmalarıdır.

Diğer kriptosistem asimetrik(açık-anahtarlı) kriptosistemdir. Asimetrik şifreleme yönteminde şifreleme ve çözme anahtarları farklıdır. Anahtarlardan birinin şifrelediğini sadece diğeri çözebilir. Anahtarlardan birine açık anahtar, diğerine gizli anahtar adı verilir; açık anahtar herkese açıklanır. Bu tip sistemler son 30 yılda keşfedilmiş ve gelişmiştir. En önemli örneği RSA'dir.

Bu güne kadar açık anahtar kriptosistemin üç sınıfı bilinmektedir. Bunlardan birisi sayılar teorisi tabanlı sistemler, kafes tabanlı sistemler ve hata doğrulama kod tabanlı sistemlerdir.

Kod tabanlı açık anahtar kriptosistemi fikri neredeyse açık anahtar kriptografi kadar eskidir. Bu sistem ilk kez 1978'de McEliece[2] tarafından önerilmiştir. Bu sistem Goppa kod tabanlıdır. Bu orijinal yapı, açık anahtarı oldukça büyük olmasından dolayı henüz kırılamamıştır. Etkinliği de makul derecededir.

Daha sonraki araştırmalar boyunca daha güçlü bir sistem elde etmek için McEliece'in yapısının modifiye edilmesiyle uğraşılmıştır. Niederreiter [3], McEliece sisteminde kullanılan Goppa kod yerine Reed-Solomon kod , Sidelnikov[4] Reed-Muller kodunu, Janwa ve Moreno[5] cebirsel geometrik kod ve son zamanlarda Gaborit [6] BCH kod kullanmayı önermiştir.[14]

Bu çalışmada [12] nolu kaynaktaki makalede uygulanan Reed-Solomon kodunun özel bir durumu olan (n,k,d) MDS(maksimum uzaklıkla ayrılabilen) kod kullanarak bir açık anahtar kriptosistemi uygulaması gerçekleştirildi.

2. Kodlama Teorisinde Temel Tanımlar

Tanım 2.1(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 alt modülüne, uzunluğu n olan M elemanlı bir lineer kod denir ve (n , M) ile gösterilir. C kodunun herhangi bir elemanına codeword (kod sözcüğü) adı verilir.[9]

Tanım 2.2(Minimum uzaklık): C kodunun elemanları olan kodsözler arasındaki uzaklıkların en küçüğüne C kodunun minimum uzaklığı denir. d(C) ile gösterilir.[9]

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

Tanım 2.3: Kodlamada gönderilen kodsöz x ve buna karşılık olarak alınan kodsöz x' ise e hata vektörü olmak üzere $x' = x + e$'dir. e hata vektörünün ağırlığı kodsözde kaç hata meydana geldiğini gösterir.[8]

Tanım 2.4 (Lineer Kod) : q elemanlı cisme Galois cismi denir. GF(q) veya IF_q ile gösterilir . Burada p bir asal sayı n ∈ N olmak üzere q = p^n biçimindedir.

$$V(n,q) = IF_q^n = \{ x = (x_1, x_2, ..., x_n) \mid x_i \in IF_q \}$$

kümesi IF_q üzerinde n boyutlu bir vektör uzayı olmak üzere , IF_q^n'in bir C alt uzayına lineer kod denir.

C, IF_q^n vektör uzayının k boyutlu bir alt uzayı ise C lineer kodu $[n,k]$ ile d minimum uzaklığını da belirtilmek isteniyorsa $[n,k,d]$ ile gösterilir.

C , $[n,k,d]$ parametreli bir lineer kod ise kodun eleman sayısı M = q^k , kodun oranı R = $\frac{k}{n}$ dir.[7]

Tanım 2.5 (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 kodsözlerinin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(C)$ ile gösterilir.[7]

Tanım 2.5 (Üreteç Matris): C bir lineer[n,k] kodu olsun. Satırları C kodunun bir baz vektörlerinden oluşan *kxn* boyutlu G matrisine, S kodunun üreteç matrisi denir.

Eğer G matrisi C kodunun üreteç matrisi ise C kodunun kodsözleri, G matrisinin satırlarının lineer bileşimidir. $G = (I_k | A)$ bu üreteç matrisi sistematik formdadır.[7]

Tanım 2.6 (Kontrol Matris): 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.[7]

3. MDS KODLAR (Maximum Distance Separable-Maksimum uzaklıkla ayrılabilen)

C bir [n,k,d] lineer kod ise, $k + d \leq n + 1$'dir. $d = n - k + 1$ Singleton sınırı ile [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.[11]

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

3.1. MDS kodların Özellikleri

Önerme1: 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.

Önerme2: A'nın her kare alt matrisi nonsingular (det ≠ 0) ise aşağıdaki G üreteç matrisi ile bir [n,k,d] kodu MDS koddur.

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

MDS kodların en iyi bilinen sınıfı etkin inşa algoritmalarına sahip olan Reed-Solomon kodlardır.

Önerme3:Eğer C bir MDS kod ise onun dual kodu olan $C^{\perp}$'da MDS koddur.[11]

4. Kriptografik Algoritmalar

Günümüzde kullanılan kriptografik algoritmalar ikiye ayrılır. Bunlar, kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılırlar.

4.1.Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları şifreleme ve deşifreleme işlemleri için tek bir gizli anahtar kullanmaktadır. Simetrik şifreleme algoritmaları çok hızlı şifreleme ve deşifreleme işlemleri gerçekleştirebildiğinden dolayı günümüzde çok yaygın olarak kullanılmaktadır Bu algoritmalara örnek olarak DES, AES, 3DES, Blowfish, IDEA, RC4 ve SAFER verilebilir [13].

4.2.Asimetrik Şifreleme Algoritmaları

Asimetrik yani açık anahtarlı şifreleme sistemi fikri ilk önce Diffie-Hellman [10] tarafından 1970'lerde kullanılmıştır.

Simetrik şifreleme tekniğinde bulunan anahtar dağıtım problemini çözmek için şifreleme ve çözme işlemlerinin her birisi için ayrı ayrı anahtar kullanma prensibine dayanan bir şifreleme sistemi geliştirilmiştir. Bu anahtarlardan birine açık anahtar (public key), diğerine özel anahtar (private key) denir. Asimetrik algoritmalara örnek olarak RSA,ECC, Diffie-Hellman ve El Gamal verilebilir.[13]

5. MDS Kod kullanan Asimetrik Kriptosistemin Genel Yapısı

Diyelim ki C, kod uzunluğu n, boyutu k, minimum uzaklığı d ve G üreteç matrisine sahip olan lineer bir MDS kod olsun. Açık anahtarı ve özel anahtarı yaratmak için şu adımlar uygulanır:

1) (n,k,d) lineer MDS kod için kxn bir G üreteç matris seçilir.
2) Rastgele kxk binary non-singular $(\det \neq 0)$ S matrisi seçilir.
3) Rastgele nxn bir P permütasyon matrisi seçilir.
4) $\hat{G} = SGP$ kxn matris hesaplanır.
5) Açık anahtar $(\hat{G}, r)$, r G'nin tekrar sayısıdır.

Özel(gizli) anahtar (S,G,P) dir.

Şifreleme İşlemi

1) $(\hat{G}, r)$ açık anahtarı elde edilir.
2) k uzunluklu açık metin "m"ile gösterilsin.
3) $C_1 = m\hat{G}T,$
   $C_i = C_{i-1}\hat{G}T, \quad i = 1,2,...,r$

hesaplanır. T matrisi aşağıdaki formdadır.

$$T = \begin{pmatrix} I_{kxk} \\ 0_{n-kxk} \end{pmatrix}$$

$C = C_r$ şifreli metin elde edilir.

Şifre Çözme İşlemi

Şifrelemede yapılan işlemlerin tersi yapılır.

1) $C = C_r$ 'nin kayıp kayıp bileşenleri MDS kodun kod kelimeleri kullanılarak $\hat{C}_r$ bulunur.

2) $C_r = \hat{C}_r P^{-1}$ hesaplanır.

3) $C_{r-1} = \hat{C}_{r-1} S$ elde etmek için $C_r = (\hat{C}_{r-1} S)G$ denklem sistemi çözülür.

4) S^{-1} ile $C_{r-1}S$ çarpılarak C_{r-1} ulaşılır.

5) $C_1 = (mS)G$ denklem sistemine ulaşana kadar son dört adım (r-1) kez tekrarlanır. Bu denklemi çözerek mS elde edilir ve bu da S^{-1} ile çarparak 'm' açık metine ulaşırız.[12]

5.1. MDS Kod kullanarak Bir Asimetrik Kriptosistemi Uygulaması

Örnek: Diyelim ki C bir lineer [4,2,3] MDS kod olsun. Bu kodun üreteç matrisi G

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

S, 2x2'lik bir non-singular $(\det \neq 0)$ bir matris olsun. Onu da şu şekilde seçelim.

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

4x4'lük P permütasyon matrisi aşağıdaki gibi seçilsin,

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

Şimdi açık anahtar için $\hat{G}$ hesaplayalım.

$$\hat{G} = SGP = \begin{bmatrix} 10 \\ 11 \end{bmatrix} \begin{bmatrix} 1011 \\ 0112 \end{bmatrix} \begin{bmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{bmatrix}$$

$$\hat{G} = \begin{bmatrix} 0111 \\ 1120 \end{bmatrix}$$

Açık anahtar = $(\hat{G}, r)$'dir. Burada ki "r" üreteç matrisinin tekrarlama sayısıdır.
Gizli anahtarlar = (S,G,P)'dir.

Şimdi m=11 mesajını şifreleyelim. Öncelikle sabit bir formda olan bir T matrisi belirleyelim.

$$T = \begin{bmatrix} 10 \\ 01 \\ 00 \\ 00 \end{bmatrix}$$

Şifreleme adımları aşağıdaki gibidir. r =2 alalım. O zaman iki adımda şifreleme işlemini bitireceğiz.

1.

$$\hat{C}_1 = m\hat{G} = (11)\begin{pmatrix} 0111 \\ 1120 \end{pmatrix} = (1201)$$

2.

$$\hat{C}_1 T = (1201)\begin{pmatrix} 10 \\ 01 \\ 00 \\ 00 \end{pmatrix} = (12) = C_1$$

3.

$$C_1\hat{G} = \hat{C}_2 = (12)\begin{pmatrix} 0111 \\ 1120 \end{pmatrix} = (2021)$$

4.

$$\hat{C}_2 T = C_2 = (2021)\begin{pmatrix} 10 \\ 01 \\ 00 \\ 00 \end{pmatrix} = (20)$$

Deşifreleme için şifreleme sürecinin tersini yaparız.

1. MDS kodun kod kelimelerinden karşılaştırılarak C_2'nin kayıp bileşenleri hesaplanır.

$C = \{(0000),(1012),(0111),(1120),(2021),$
$(0222),(2210),(2102),(1201)\}$

(20--) ile başlayan kod kelimesi $\hat{C}_2 = (2021)$ dir.

2.

$$(2021)P^{-1} = (2021)\begin{pmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{pmatrix} = (0221)$$

3.

$$(0221) = (C_1 S)G$$
$$(0221) = (xy)\begin{pmatrix} 1011 \\ 0112 \end{pmatrix}$$
$$(0221) = (x \;\; y \;\; x+y \;\; x+2y)$$
$$x = 0,\ y = 2$$
$$C_1 S = (02)$$

4.

$$C_1 S = (02)$$
$$C_1 = (02)S^{-1}$$
$$C_1 = (02)\begin{pmatrix} 10 \\ 21 \end{pmatrix}$$
$$C_1 = (12)$$

5. MDS koddaki kod kelimeleri ile karşılaştırılarak C_1'in kayıp bileşenleri hesaplanır.

(12--) ile başlayan kod kelimesi $C_1 = (1201)$ dir.

6.

$$(1201)P^{-1} = (1201)\begin{pmatrix} 0100 \\ 1000 \\ 0010 \\ 0001 \end{pmatrix} = (2101)$$

7.

$$(2101) = (mS)G$$
$$(2101) = (xy)\begin{pmatrix} 1011 \\ 0112 \end{pmatrix}$$
$$(2101) = (x \;\; y \;\; x+y \;\; x+2y)$$
$$x = 2,\ y = 1$$
$$mS = (21)$$

8.

$$mS = (21)$$
$$m = (21)S^{-1}$$
$$m = (21)\begin{pmatrix} 10 \\ 21 \end{pmatrix}$$
$$m = (11)$$

m=11 açık metinine ulaşılır.

6. Sonuçlar

Bu kriptosistemin güvenliği MDS kodun G üreteç matrisinin gizliliği ve G'nin tekrarlama sayısıdır. Bu sisteme yapılacak olası saldırı açık metin-şifreli metin saldırılarıdır. Bunun için n. dereceden kxn bilinmeyenli $\binom{n}{k}xk$ lineer olmayan denklemleri çözmek gerekir. Bu da zor bir problemdir. Yani bu saldırılara karşı böyle bir sistem dayanıklıdır. Ve yüksek güvenlik seviyesine sahiptir. Ayrıca bu kriptosistemin avantajı açık metinin büyüklüğünün şifreli metinin büyüklüğü ile aynı olmasıdır.

7. Kaynaklar

[1]. C. E. Shannon: A mathematical theory of communication. Bell System Technical Journal, vol. 27, pp. 379–423 and 623–656, July and October, 1948

[2] R. J. McEliece, A public key cryptosystem based on algebraic coding theory, DSN progress report, 42-44:114-116, 1978

[3] H. Niederreiter, Knapsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory 15, 159-166, 1986.

[4] V.M. Sidelnikov, A public-key cryptosystem based on binary Reed-Muller codes, Discrete Mathematics and Applications, 4 No. 3, 1994

[5] H. Janwa, O. Moreno McEliece Public Key Cryptosystems Using Algebraic-Geometric Codes, Designs, Codes and Cryptography 8(3): 293–307, 1996

[6] P. Gaborit Shorter keys for code based cryptography, Proceedings of Workshop on Codes and Cryptography, Bergen, p. 81–90, 2005

[7] ROMAN S., Coding and Information Theory, Graduate Text in Mathematics, Springer Verlag, 1992.

[8] CHAPMAN H., Coding Theory. St Edmundsbury Press, 12-105, Great Britian, 1996.

[9] RAYMOND H., A first course in coding theory, Oxford Press, 1996.

[10] DIFFIE W. and HELLMAN M. E., New directions in cryptography, IEEE Transaction on Information Theory 22, pp. 644 – 654, 1976.

[11] "Some Applications of Code Duality in Cryptography", James L.Maasey, *www.mat.unb.br/~matcont/21_11.ps*

[12] Prof. Mohammed *S.* EL-Atrash, Dr. Fayik R. EL-Naowk, Public-key Cryptosystem Using MDS Code, J. AAqsa Unv.,8,2004.

[13] Mao, W., *Modern Cryptography: Theory &Practice*, Upper Saddle River, NJ: Prentice Hall PTR,2004.

[14] Lorenz Minder,Cryptography based on error correcting codes, 2007 Phd. Thesis.