MDS Kod Tabanlı Gizlilik Paylaşım Şemasında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek

Derya Arda[1] Ercan Buluş[2]

[1]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne
[2]Bilgisayar Mühendisliği Bölümü, Namık Kemal Üniversitesi, Çorlu

[1]e-posta: deryaa@trakya.edu.tr [2] e-posta: ercanbulus@nku.edu.tr

Özetçe

Bir (k,n) Gizlilik Paylaşım Şeması, kriptografik anahtarlar gibi gizli veriyi korumak için geliştirilmiş bir tekniktir. Bu şemada gizlilik n paylaşımcı arasında dağıtılmıştır ve bu paylaşımcılardan sadece herhangi k tanesi bir araya gelerek gizliliği yeniden elde edebilirken, k' dan daha az paylaşımcı bir araya gelerek gizlilik hakkında hiçbir bilgi elde edemezler. Bu şemadaki amaç yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmaktır. Gizlilik Paylaşım Şeması ilk olarak 1979 yılında Shamir ve Blakley tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Daha sonraları literatürde pek çok gizlilik paylaşım şemaları önerilmiştir. Bunlardan bazıları McEliece ve Sarwate tarafından önerilen hata doğrulama kod tabanlı gizlilik paylaşım şemasıdır. 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 çalışmada (n+1, k) MDS (maksimum uzaklıkla ayrılabilen) kod kullanarak bir (k, n) eşik gizlilik paylaşım şeması tasarlandı. Aynı zamanda hata doğrulama kod tekniklerinden faydalanılarak, gizlilik paylaşım şemasında hileli katılımcılar tespit edilip onların bozuk paylaşımları düzeltilip gizliliğin yeniden elde edildiği gösterildi.

1. Giriş

Çağdaş kriptografi ve kodlama teorisi 60 yıldan daha fazla başarılı bir tarihe sahiptir. 1948' de Claude Shannon "Haberleşmenin Matematiksel Teorisi" adlı makalesinde bilgi teorisi ve kodlama teorisi gibi iki disiplini başlatıp geliştirmiştir.[3] Daha sonra Nyquist ve Hardley'in teorilerini genişleterek bilginin ölçülmesine olasılık kavramını eklemiştir. Böylelikle bilgi kuramı ile kriptoloji arasındaki bağıntıyı kurmuştur ve kripto sistemlerin matematiksel esaslarını belirlemiştir.

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.

Kriptografide diğer önemli bir mesele şifreleme algoritmalarında kullanılan anahtarın korunması ve saklanması problemidir. Bir (k,n) Gizlilik Paylaşım Şeması, kriptografik anahtarlar gibi gizli veriyi korumak için geliştirilmiş bir tekniktir. Gizlilik paylaşım şeması yapılacak saldırılara karşı anahtarın tek bir kullanıcıda bulunmaktansa pek çok kullanıcıya dağıtılarak güvenliğini arttırmak için tasarlanmış bir yapıdır. Bu şema ilk olarak 1979 yılında Shamir [1] ve Blakley [2] tarafından birbirlerinden bağımsız olarak ortaya atılmıştır. Daha sonraları literatürde pek çok gizlilik paylaşım şemaları önerilmiştir. Bunlardan bazıları hata doğrulama kod tabanlıdır [5,6]. Örneğin bunlardan birisi McEliece ve Sarwate tarafından önerilen hata doğrulama kod tabanlı gizlilik paylaşım şemasıdır [6].

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 çalışmada (n+1, k) MDS (maksimum uzaklıkla ayrılabilen) kod kullanarak bir (k, n) eşik gizlilik paylaşım şeması tasarlandı. Aynı zamanda hata doğrulama kod tekniklerinden faydalanılarak, gizlilik paylaşım şemasında hileli katılımcılar tespit edilip onların bozuk paylaşımları düzeltilip gizliliğin yeniden elde edildiği gösterildi.

2. Gizlilik Paylaşım Şeması

Gizlilik paylaşımı anahtar yönetimi ve anahtar dağıtımı ile ilişkilidir. Bu anahtar dağıtım ve yönetim problemi bütün kriptosistemlerde oldukça sık rastlanan bir problemdir.
Temel olarak bir (k,n) gizlilik paylaşım şemasında d gizliliği n kişi arasında dağıtılır ve her hangi k kişi veya daha fazlası birleşerek gizliliği yeniden elde edebilir. Ancak $k-1$ veya daha az kişi gizliliği elde edemezler [4,7].

3. Kodlama Teorisinde Kullanılan Temel Kavramlar

Tanım 3.1. (Minimum uzaklık): C kodunun elemanları olan kod kelimeleri arasındaki uzaklıkların en küçüğüne C kodunun minimum uzaklığı denir ve $d(C)$ ile gösterilir [9].

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

Tanım 3.2. (Doğrusal Kod) : q elemanlı cisme Galois cismi denir. $GF(q)$ veya IF_q ile gösterilir . Burada p bir asal sayı $n \in N$ olmak üzere $q = p^n$ biçimindedir.

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

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

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

C, $[n,k,d]$ parametreli bir doğrusal kod ise kodun eleman sayısı $M = q^k$, kodun oranı $R = \frac{k}{n}$, dir [10].

Tanım 3.3. (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 kelimelerinin ağırlıklarının en küçüğüne C kodunun minimum ağırlığı denir ve $w(c)$ ile gösterilir [10].

Tanım 3.4. (Üreteç Matris) $[n,k]$ şeklindeki C bir doğrusal 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 kelimeleri, G matrisinin satırlarının doğrusal bileşimidir. $G = (I_k | A)$ bu üreteç matrisi standart formdadır [10].

Tanım 3.5. (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 [10].

4. MDS Kodlar ve Özellikleri

Tanım 4.1. C bir $[n,k,d]$ doğrusal kod ise, $k + d \le n + 1$ '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].

Önerme 4.1. d uzaklığına sahip bir C doğrusal kodunun H kontrol matrisinin her $d-1$ sütunları doğrusal bağımsızdır. Tanımlandığı gibi bir MDS kod $n-k+1$ uzaklığa sahiptir. Böylece, kontrol matrisinin her $n-k$ sütunlarının kümesi doğrusal bağımsızdır.[11]

Önerme 4.2. A'nın her kare alt matrisinin determinantı sıfırdan farklı ($\det \neq 0$) ve tekil olmayan (nonsingular) 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. [11]

5. GF(2^n) sonlu cisminde Reed-Solomon Kodlar ve MDS Kodlar

Tanım 5.1. Sonlu cisim adından da anlaşılacağı üzere sonlu sayıda elemana sahip bir 'cisim'dir. Sonlu cismin sahip olduğu eleman sayısı sonlu cismin düzenini belirler [12].

Tanım 5.2. GF(2) üzerinde oluşturulan m. Dereceden p(X) polinomu m'den daha küçük dereceli polinomlara bölünemiyorsa p(X) GF(2) üzerinde indirgenemez denir [13].

Örnek1 : $GF(2^3)$ sonlu cisim üzerinde $x^3 + x + 1$ indirgenemez polinomuna göre minimum Hamming uzaklığı 5 olan ve en fazla 2 hata düzeltebilen bir Reed Solomon kod inşa edelim. α, GF(2^3) cisminde bir üreteçtir. Bu cismin elemanları aşağıdaki Tablo1 ile gösterilmiştir.

Kod kelimesinin uzunluğu $n = q - 1 = 8 - 1 = 7$

Hata düzeltme kapasitesi $t = \frac{d-1}{2} = \frac{5-1}{2} = 2$

g(x) üreteç polinomunun derecesi $2t = 4 = n - k \Rightarrow$

$7 - k = 4 \Rightarrow k = 3$

Boyutu k=3'tür.

Dolayısıyla $n - k + 1 = 5$ (singleton sınırı) (n,k,d;q) = (7, 3, 5; 8) olan bir MDS koddur.

Tablo1: GF(2^3) cisminin elemanları

Sayısal karşılığı	Polinomsal gösterimi	İkili karşılığı
1	α^0	001
2	$\alpha^1 = \alpha$	010
4	α^2	100
3	$\alpha^3 = \alpha + 1$	011
6	$\alpha^4 = \alpha^2 + \alpha$	110
7	$\alpha^5 = \alpha^2 + \alpha + 1$	111
5	$\alpha^6 = \alpha^2 + 1$	101
1	$\alpha^7 = 1$	001

$g(x) = (x + \alpha^0)(x + \alpha^1)(x + \alpha^2)(x + \alpha^3)$ üreteç polinomudur [14].

$g(x) = x^4 + \alpha^2 x^3 + \alpha^5 x^2 + \alpha^5 x + \alpha^6$. Buradan üreteç matrisini oluşturalım.

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

Sistematik forma dönüştürülmüş G üreteç matrisi aşağıda gösterilmiştir.

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

Kontrol Matrisi H,

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

6. GF(2^3) sonlu cisminde (7,3,5) MDS kodu ile Gizlilik Paylaşımı ve Hileli Katılımcıları Tespit etmek ve Kimliklendirmek

6.1. (7,3,5) MDS kod ile Gizlilik Paylaşımı

(7,3,5) MDS kodun üreteç matrisi G yukarıda elde edilmişti. 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. C kodu için 6 paylaşımcı P_1, P_2, P_3, P_4 ,P_5 ,P_6 olsun

Örneğin seçtiğimiz bilgi vektörü $s=[1,\alpha^6,\alpha^5]$ olsun. Bu bilgi vektörünün sorumlu olduğu kod kelimesi,

$t=(t_0,t_1,t_2,t_3,t_4,t_5,t_6)=sG=\left[1,\alpha^6,\alpha^5,\alpha,\alpha^3,\alpha^4,\alpha^2\right]$ ve

paylaşımlar Tablo2'de gösterilmiştir.

Tablo 2 Katılımcıların gizli paylaşım değerleri

Paylaşımlar	Gizli Değerler
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

MDS kod tabanlı gizlilik paylaşımı için daha detaylı bir örnek [7] numaralı kaynakta gösterilmiştir.

6.2. MDS kod ile Gizlilik Paylaşımında Hileli Katılımcıları Tespit Etmek ve Kimliklendirmek

MDS kod tabanlı gizlilik paylaşım şemalarında, bu kodların etkin kod çözme algoritmaları olduğu için hileli katılımcılara karşı oldukça ilgi çekici yapılardır.

Teorem1: 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.[8]

Örnek 2: Örnek 1'de [7,3,5] MDS kod için hileli katılımcıları tespit edip, düzletme 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. Bu örnekte hileli katılımcıları tespit etmek için Reed-Solomon Kodların sendrom kod çözme algoritması kullanılmıştır. Daha detaylı bilgiye [14] numaralı kaynaktan ulaşılabilir.

1. Hileli katılımcı var mı yok mu tespit et.
   Diyelim $P_1=\alpha^6$, $P_2=\alpha$, $P_3=\alpha^2$ paylaşım bilgilerini gönderdi. P_2 ve P_3 yanlış bilgi gönderdi. Ya da bunlar hileli katılımcılar olsun. Diğer katılımcıların bilgileri ise $P_0=1$, $P_4=\alpha^3$, $P_5=\alpha^4$, $P_6=\alpha^2$

Öncelikle hata olup olmadığını tespit etmek için alınan kod kelimesi eşlik sınama matrisinin transpozesi ile çarpılır ve sonuç sıfır değilse hata var yani hileli katılımcı var demektir.

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

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

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. Aşağıdaki denkleme göre hatalı olan bileşenin yerleri tespit edilir.

Örneğimize göre çözelim.

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

Hata yeri polinomu 6.1 denklem ile gösterilmiştir.

$\sigma_A(x)=\sigma_0+\sigma_1x+\sigma_2x^2+...+x^e$ 6.1

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

Bu durumda hata yeri polinomundan faydalanarak,

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

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

4. Hatalı olan bileşenler 6.2 denklemi ile düzeltilir.

$$\begin{pmatrix} a_1^0 & a_2^0 & \dots & a_e^0 \\ a_1^1 & a_2^1 & \dots & a_e^1 \\ . & & & \\ . & & & \\ a_1^{e-1} & a_2^{e-1} & \dots & a_e^{e-1} \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ . \\ . \\ b_e \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ \\ \\ s_{e-1} \end{pmatrix} \qquad 6.2$$

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

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

Denklem sistemi çözümünden

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

$a_1 = \alpha^2$ ve $a_2 = \alpha^3$ pozisyonlarında hata oluşmuştu. Yani P_2 ve P_3 katılımcıları hileli katılımcılardı. Bu hileli katılımcıların hatalı verileri doğru verilerle düzeltilir. Yani

$a_1 = \alpha^2$ yerine $b_1 = \alpha^6$ ile düzeltilir.

$a_2 = \alpha^3$ yerine $b_2 = \alpha^4$

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

Hata vektörü yani hileli katılımcıların tespit edildiği vektör $e = (0,0,\alpha^2,\alpha^3,0,0,0)$ düzeltilip "w" ile XOR işlemi $e = (0,0,\alpha^6,\alpha^4,0,0,0)$

yapıldığında doğru kod kelimesine ulaşılır.

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

$$c = (1, \alpha^6, \alpha^5, \alpha, \alpha^3, \alpha^4, \alpha^2)$$

7. Sonuç

Gizlilik paylaşım şemaları güvenliği arttırmak için geliştirilmiş kriptografik anahtar yönetimi ve anahtar dağıtımı ile ilişkili bir kavramdır. Çeşitli yapılarda gizlilik paylaşım şemaları mevcuttur. Bunlardan bazıları kodlama teorisi tabanlı gizlilik paylaşım şemalarıdır. Bu çalışmada kodlama teorisi ile özellikle MDS kodlar ile ilişkilendirilmiş bir gizlilik paylaşım şemasında hileli katılımcılar olduğu zaman bunların hata doğrulama tekniklerinden faydalanılarak tespit edilip kimliklendirildiği gösterilmiştir.

8. Kaynakça

[1] Shamir, " How to share a secret", Communications of the ACM 22 (11) (1979) 612-613.

[2] Blakely, G. R., "Safeguarding cryptography keys", Proc. AFIPS 1979 National Computer Conference, 48, (1979), 313-317.

[3] C.E. Shannon "A Mathematical Theory of Communication" http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf

[4] Arda D., Buluş E., Akgün F., Yerlikaya T., "Secret Sharing Scheme in Cryptographic Key Management Problem", International Scientific Conference UNITECH'08 Gabrovo,2008

[5] Bhondo C., De Santis A., Gargano L., Vaccaro U., "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,1993.

[6] McEliece R. J., Sarwate D. V., "On sharing secrets and Reed Solomon Codes", Comm. ACM 24, 583-584,1981.

[7] Arda D., Buluş E., Yerlikaya T., "MDS Kod tabanlı Kriptografik Gizlilik Paylaşım Şeması, 4. International Information Security&Cryptology Conference ISCTURKEY , Ankara,2010

[8] C. Ding , T. Laihonen , A. Renvall, " Linear Multisecret-Sharing Schemes and Error-Correcting Codes" volume 3, pages 1023-1036, Journal of Universal Computer Science, 1997

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

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

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

[12] Bilgiç H., "Soyut Matematik Ders Notları", Kahramanmaraş Sütçü İmam Üniversitesi, Eylül 2009.

[13] Zorlu Y., " Reed-Solomon Kodların AWGN ve Rayleigh Kanallarda Başarım Analizi", Yüksek Lisans Tezi, Temmuz 2006.

[14] A.A. Bruen, M. A. Forcinito, " Cryptography, Information Theory, and Error-Correction", John Wiley&sons, Inc.,Hoboken, New Jersey, 2005.