ÜS HARİTALAMA TABANLI CEBİRSEL 8-BİT GİRİŞ 8-BİT ÇIKIŞLI S-KUTULARININ SINIFLANDIRILMASI

[1]Bora Aslan, [2]M.Tolga SAKALLI, [3]Ercan BULUŞ

[1]Kırklareli Üniversitesi, Lüleburgaz Meslek Yüksekokulu, Lüleburgaz-Kırklareli
[2]Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Edirne
[3]Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği, Çorlu-Tekirdağ
boraaslan@trakya.edu.tr, tolga@trakya.edu.tr, ercanbulus@corlu.edu.tr

ABSTRACT

Since inversions mapping based S-boxes give good results from the point of cryptographic properties, S-boxes designed by this technique are used in symmetric cipher design such as AES cipher design. In addition, we can see inversion mapping as the special case of power mapping in GF(2^n). In our study, we classify 8-bit to 8-bit S-boxes based on power mappings in GF(2^8) according to the DDT and LAT distributions which are very important cryptographic properties for differential cryptanalysis and linear cryptanalysis respectively. We also give mathematical preliminaries needed for classifying these algebraic S-boxes.

Key words: S-boxes, Power Mappings, Classification

1.GİRİŞ

Boole fonksiyonları ve vektörel boole fonksiyonları (S-kutuları) blok ve akan şifreleme yöntemlerinde kullanılan, doğrusal olmayan ve şifreye güvenliğini veren en önemli elemanlardır. S-kutuları için kriptografik özelliklerden biri olan doğrusal olmama özelliği önemli bir özelliktir. Bununla beraber doğrusal saldırılar için önemli olan LAT (Linear Approximation Table-Doğrusal Yaklaşım Tablosu), diferansiyel saldırılar için önemli olan DDT (Difference Distribution Table-Fark Dağılım Tablosu-XOR Tablosu), bütünlük (completeness), çığ (avalanche), katı çığ (strict avalanche) gibi kriptografik özellikler S-kutularının doyurması gerektiren özellikler olarak karşımıza çıkmaktadır [1].

S-kutularının tasarım tekniklerine örnek olarak pseudo-random üretim, sonlu cisimde ters haritalama, sonlu cisimde üs haritalama ve heuristik teknikler verilebilir. Sonlu cisimde ters alma işlemi, üs haritalama işleminin özel bir durumu olarak görülebilir ve bu iki teknik ile doğrusal olmama ölçüsü yüksek ve diğer kriptografik özellikleri iyi S-kutuları elde edilebilir. Bunun yanında bu tasarım teknikleri kullanılarak tasarlanan S-kutuları monomial tabanlı polinomlara dayalı üs haritalama ve ters alma gibi cebirsel işlemler olduğu için doğrusal denklik [2] [3] ve S-kutularının cebirsel ifadesinde bazı basit cebirsel yaklaşımlar [4] gibi istenmeyen özellikleri de beraberinde getirmektedir.

Yine de bu istenmeyen özellikler şifreye bir saldırı olarak hala kullanılamamışlardır.

Kriptografide APN (Almost Perfect Nonlinear-Hemen Hemen Kusursuz Doğrusal Olmayan) fonksiyonlar diferansiyel kriptanalize karşı simetrik şifre tasarımında dayanıklılık sundukları için özel ilgi gösterilen fonksiyonlardır. Bu alanda yapılan ve literatürde yer alan çeşitli çalışmalar [5][6][7][8][9] [10][11] şeklinde verilebilir. APN fonksiyonlar $x \in GF(q),\ q = p^n$ ve p asal sayı olmak üzere $f(x+a)+f(x)=b$ denkleminde herhangi bir $a \setminus 0 \in GF(q)$ değerine karşılık maksimum $b \in GF(q)$ değeri 2 olan fonksiyonlardır ve diğer bir deyişle 2 uniform fonksiyonlar adı da verilmektedir. Bizim çalışmamızda $GF(2^8)$ 'de üs fonksiyonlarının sınıflandırılması yapılacağı için kendimizi $p=2$ olacak şekilde sınırlandırdık.

Diğer yandan bijektif (birebir ve örten) S-kutuları her ne kadar zorunlu olmasada tercih edilen S-kutularıdır. Ancak fonksiyon $x \to x^d$, $\mathrm{OBEB}(d, 2^n-1)=1$ ise birebir ve örten bir fonksiyondur. Bu kısıt altında birebir ve örten ve APN bir üs fonksiyon $GF(2^8)$ 'de yoktur. Bu da daha kötü uniform dağılımına sahip üs fonksiyonlarının S-kutusu tasarımında kullanılması fikrini gündeme getirmiştir AES şifresinin tasarımcıları byte yapısındaki şifre tasarım felsefesinden ödün vermeden Nyberg'in [12] önerdiği ters haritalama tabanlı ve APN fonksiyon dağılımına yakın sonuç veren S-kutusunu şifrelerinde kullanmışlardır.

2001 yılında AES (Advanced Encryption Standard) olarak seçilen doğrusal [13] ve diferansiyel [14] saldırılara dayanıklı olan Rijndael şifresi Nyberg'in önerdiği sonlu cisimde ters haritalama tabanlı bir S-kutusunu kullanmaktadır ve cebirsel ifadesi aşağıdaki gibidir

$$f(x) = x^{-1}, \quad x \in GF(2^8), \quad f(0) = 0.$$

Bu haritalama basit cebirsel bir ifade olduğu için ters haritalama işleminden sonra ikili bir affine (doğrusal) dönüşüm kullanılarak bu basit cebirsel ifade iyileştirme yoluna gidilmiştir. Bu dönüşüm doğrusal ve diferansiyel saldırılara karşı herhangi bir iyileştirme sağlamamakla beraber $GF(2^8)$'de S-kutusu ifadesini daha karmaşık hale getirmektedir. $GF(2^8)$ üzerine, $GF(2^8)$ indirgenemez polinom $x^8 + x^4 + x^3 + x + 1$ ile tanımlanmıştır, Lagrange interpolasyonu kullanılarak elde edilen AES S-kutusunun cebirsel ifadesi aşağıdaki gibi verilebilir.

$$S(x) = "63" + "05"x^{254} + "09"x^{253} + "f9"x^{251} + "25"x^{247} + "f4"x^{239} + "01"x^{223} + "b5"x^{191} + "8f"x^{127}.$$

Bununla beraber AES S-kutusunun tasarımında ters haritalama yerine $x \to x^{127}$ üs fonksiyonu kullanılsaydı AES S-kutusunun cebirsel ifadesi

$$S(x) = "63" + "09"x^{254} + "f9"x^{253} + "25"x^{251} + "f4"x^{247} + "01"x^{239} + "b5"x^{223} + "8f"x^{191} + "05"x^{127}$$

şeklinde olacaktı. Dolayısıyla terimlerdeki benzerlik üs fonksiyonlarının sınıflandırılması ile ilgili olarak bizi motive etmiştir ve $GF(2^8)$ de tüm üs fonksiyonları için DDT ve LAT dağılımları çalışmamızda incelenmiştir. Ayrıca LAT dağılımındaki en büyük değer S-kutusunun doğrusal olmama kriteri ile ilişkili olduğu için üs fonksiyonu ile tasarlanacak S-kutularının doğrusal olmama ölçüsüde verilebilir. Bu çalışmada Maxwell'in [11] çalışmasındaki bulgulara ek olarak $GF(2^8) \to GF(2^8)$ üs fonksiyonları için LAT dağılımları ve DDT dağılımları elde edilmiştir.

$GF(2^8)$'de 30 indirgenemez polinom bulunmaktadır ve bunların 16'sı asal polinomdur [15]. İndirgenemez polinomları taban alarak oluşturulacak her cisim arasında izomorfizm olduğu için bu indirgenemez polinomlardan biriyle oluşturulacak sonlu cisimde incelenecek herhangi bir üs fonksiyonu aynı kriptografik özelliği verecektir. Biz çalışmamızda AES S-kutusunun tasarımında kullanılan $x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomunu kullanarak $GF(2^8)$ de sonlu cisim oluşturup olası tüm üs fonksiyonlarının bu cisimde davranışlarını inceledik ve üs fonksiyonlarını LAT ve DDT dağılımlarına göre sınıflandırdık.

2.MATEMATİK ALT YAPI

$S : GF(2^n) \to GF(2^n)$ olmak üzere n-bit giriş ve n-bit çıkışa sahip bir S-kutusu olsun. O zaman herhangi verilen $a, b, \Gamma_a, \Gamma_b \in GF(2^n)$ için $XOR(a,b)$, herhangi $a \setminus 0$ ve b için $S(x) + s(x+a) = b$ denklemindeki b değerlerinin sayısını tanımlar ve denklem (1) deki gibi gösterilebilir [16]. S için denklem (1) de a ve b değerleri sırasıyla giriş farkı ve çıkış farkı olarak isimlendirilir.

$$XOR(a,b) = \#\left\{x \in GF(2^n) \mid S(x) + S(x+a) = b\right\} \quad (1)$$

Buna ek olarak $N_L(\Gamma_a, \Gamma_b)$, herhangi $\Gamma_a \setminus 0$ ve Γ_b için $x \in GF(2^n)$ olmak üzere $\Gamma_a \bullet x = \Gamma_b \bullet S(x)$ denklemini sağlayan değerlerin sayısını tanımlar ve (2) denklemindeki gibi gösterilebilir [16]. S için denklem (2) de Γ_a ve Γ_b değerleri sırasıyla giriş maskesi ve çıkış maskesi olarak isimlendirilir. Denklem (3)'te herhangi bir giriş ve çıkış maskesi değerine göre LAT tablosu değerinin nasıl elde edileceği verilmiştir.

$$N_L(\Gamma_a, \Gamma_b) = \#\left\{x \in GF(2^n) \mid \Gamma_a \bullet x = \Gamma_b \bullet S(x)\right\} \quad (2)$$

($x \bullet y$ nokta ürün olarak isimlendirilir.)

$$LAT(\Gamma_a, \Gamma_b) = \#\left\{x \in GF(2^n) \mid \Gamma_a \bullet x = \Gamma_b \bullet S(x)\right\} - 2^{n-1} \quad (3)$$

$GF(q)$, q elemanlı sonlu bir cisim ve q, p^n olacak şekilde asal bir sayının üssü olsun. $f : GF(q) \to GF(q)$ olan fonksiyonları ele alalım. $a, b \in GF(q)$ olmak üzere $\nabla_f(q)$ değeri q

$$\nabla_f(q) = \text{maks}\left\{XOR(a,b) : a, b \in GF(q), a \neq 0\right\}$$

değerinden az ise fonksiyon için doğrusal değildir deriz. Diğer yandan bir S-kutusu için doğrusal olmama ölçüsü NLM_S değeri LAT değeri ile ilişkili olarak denklem (4)'te verilmiştir.

$$NLM_S = 2^{n-1} - \text{maks}\left|LAT_S(\Gamma_a, \Gamma_b)\right| \quad (4)$$

Yukarıda verilen tanımlara ilişkin olarak diferansiyel ve doğrusal saldırılara karşın S-kutusunun iyi davranış gösterebilmesi için S-kutusunun hem DDT hem de LAT değerlerinin

maksimum değerinin olduğunca küçük olması istenen özellikler arasındadır.

Tanım 1. $f(x)=x^d$ fonksiyonu $GF(p^n)$ üzerine bir fonksiyon olsun. $\nabla_f = 2$ şeklindeki haritalara APN denir.

Tanım 2. $a,b \in GF(p^n)$ olmak üzere f fonksiyonu için $XOR(a,b)$ ve g fonksiyonu için $XOR(a,b)$ değerlerinin listesi birbirleri ile aynı ise f ve g fonksiyonları denktir denir [11].

Tanım 3. Bir tamsayı d 'i içeren mod N 'e göre cyclotomic koset

$$C_d = \left\{d, dp, ..., dp^{n-1}\right\} \pmod N$$

şeklinde bir settir ve d, $dp^n \equiv d \pmod N$ olacak şekilde en küçük tamsayıdır [17].

Teorem 1. $f(x)=x^d$ fonksiyonu için cyclotomic koset üzerindeki $XOR(a,b)$ sabittir [11].

$\left\{dp^i : i = 0,1,...,n-1\right\}$

$(XOR_{dp^i}(a,b) = XOR(a,b) \quad i = 0,1,...,n-1$ için)

İspat.

$$\left|\left\{x : (x+a)^{dp^i} + x^{dp^i} = b\right\}\right|$$

$$= \left|\left\{x : (x^{p^i}+a)^d + (x^{pi})^d = b\right\}\right|$$

$$= \left|\left\{y : (y+a)^d + y^d) = b\right\}\right| \quad (y = x^{p^i} \text{ olmak üzere})$$

Teorem 2. $a \neq 0$ için $XOR(a,b) = XOR(1, ba^{-d})$ dir [11].

Önerme 1. $x \in GF(2^n)$ ve n çift olmak üzere $GF(2^n)$ cisminde ters haritalama işlemi $f(x)=x^{-1}$, $f(0)=0$ fark dağılımına göre 4-uniformdur [12].

Önerme 2. $x \in GF(2^n)$ ve n çift olmak üzere $GF(2^n)$ cisminde $f(x)=x^d$ fonksiyonu $i = 1,2,..,n-1$ olmak üzere $d = 2^n - 2^i - 1$ ise fonksiyon fark dağılımına göre 4-uniformdur.

İspat. $GF(2^n)$ cisminde ters haritalama işlemi için $d = 2^n - 2$ dir. Dolayısıyla Teorem 1'e göre $(x^{2^n-2})^{2^i \bmod(2^n-1)}$ fonksiyonuda önerme 1 deki gibi aynı fark dağılımını verecektir. Dolayısıyla

$$(x^{2^n-2})^{2^i \bmod(2^n-1)} = (x^{2^n-1-1})^{2^i \bmod(2^n-1)} = x^{(-2^i) \bmod(2^n-1)}$$

anlamına gelmektedir ki bu da $d = 2^n - 2^i - 1$ üssünün fark dağılımına göre 4-uniform olduğunu göstermektedir.

Teorem 2'den yola çıkarak $GF(2^8)$ de üs haritalama sonucu elde edilecek S-kutuları için $2^8 \times 2^8$ boyutunda DDT tablosu değerleri yerine $XOR(1,b)$ değerlerinin elde edilmesi yeterli olacağını söyleyebiliriz. Aynı şekilde $2^8 \times 2^8$ boyutunda LAT tablosu değerleri yerine $LAT(1,\Gamma_b)$ değerlerinin elde edilmesi yeterli olacaktır. Diğer bir deyişle $2^8 \times 2^8$ boyutundaki her iki tablo yerine 1×2^8 tablo için dağılımlarının verilmesi yeterlidir. Önerme 1 gereği $GF(2^8)$ de ters haritalama işlemi yani $x \to x^{254}$ üs haritalama işlemi 4 uniform dağılım göstermektedir (1 tane 4, 126 tane 2 ve 129 tane 0 değeri). Teorem 1, önerme 1 ve önerme 2 gereği $x \to x^{127}$, $x \to x^{191}$, $x \to x^{223}$, $x \to x^{239}$, $x \to x^{247}$, $x \to x^{251}$, $x \to x^{253}$ üs haritalama fonksiyonlarıda aynı kriptografik özellikleri göstereceklerdir. Bu üs haritalama fonksiyonları aynı cyclotomik kosette olduklarında denk fonksiyonlardır ve aynı sınıfa konabilir.

3.GF(2^8)'DE ÜS FONKSİYONLARININ SINIFLANDIRILMASI

Çalışmamızda $GF(2^8) \to GF(2^8)$ şeklindeki cebirsel haritalamalar için üs fonksiyonları incelendiği için ilk olarak bir indirgenemez polinom seçilmiştir. Seçilen indirgenemez polinom AES S-kutusunun kullandığı $x^8 + x^4 + x^3 + x + 1$ polinomudur. Bu polinom için α kökü ilkel eleman olmadığı için $\beta = \alpha + 1$ ilkel elemanı kullanılarak cisim oluşturulmuştur:

$$(\beta^1 = "03", \beta^2 = "05", ..., \beta^{254} = "f6", \beta^{255} = "01").$$

Daha sonra herhangi bir üs fonksiyonu için S-kutusu oluşturulmuş ve bu S-kutusu için herhangi bir satırına ait DDT ve LAT değerlerinin mutlak değerlerinin dağılımları elde edilmiştir. Tablo 1, tüm sınıfların bir gösterimini yapmakla beraber DDT ve LAT değerlerinin maksimum değerlerini göstermekte ve oluşturulan S-kutularının doğrusal

olmama değerlerini % miktarları ile beraber vermektedir.

Sınıflardan 3, 9, 39, 5, 21, 95, 111, 25, 63, 55, 15, 45, 27, 85 olanlar bijektif S-kutuları değildir.

Tablo 1: $GF(2^8)$ de tüm üs fonksiyonlarının tek satırları için DDT ve LAT Dağılımlarına göre Sınıflandırılması

Sınıf (d)	Sınıf Elemanları	∇_S	$\lvert N_{Lmaks}\rvert$	Doğrusal Olmama Değeri NLM_S (%)
3	(3 6 12 24 48 96 192 129)	2	16	112 (%93)
9	(9 18 36 72 144 33 66 132)	2	16	112 (%93)
39	(39 78 156 57 114 228 201 147)	2	16	112 (%93)
5	(5 10 20 40 80 160 65 130)	4	32	96 (%80)
21	(21 42 84 168 81 162 69 138)	4	16	112 (%93)
95	(95 190 125 150 245 235 215 175)	4	16	112 (%93)
111	(111 222 189 123 246 237 219 183)	4	16	112 (%93)
127	(127 254 253 251 247 239 223 191)	4	16	112 (%93)
7	(7 14 28 56 112 224 193 131)	6	32	96 (%80)
25	(25 50 100 200 145 35 70 140)	6	32	96 (%80)
37	(37 74 148 41 82 164 73 146)	6	32	96 (%80)
63	(63 126 252 249 243 231 207 159)	6	24	104 (%87)
11	(11 22 44 88 176 97 194 133)	10	32	96 (%80)
29	(29 58 116 232 209 163 71 142)	10	32	96 (%80)
13	(13 26 52 104 208 161 67 134)	12	32	96 (%80)
55	(55 110 220 185 115 230 205 155)	12	32	96 (%80)
59	(59 118 236 217 179 103 206 157)	12	32	96 (%80)
15	(15 30 60 120 240 225 195 135)	14	12	116 (%97)
45	(45 90 180 105 210 165 75 150)	14	12	116 (%97)
17	(17 34 68 136)	16	8	120 (%100)
19	(19 38 76 152 49 98 196 137)	16	24	104 (%87)
23	(23 46 92 184 113 226 197 139)	16	32	96 (%80)
31	(31 62 124 248 241 227 199 143)	16	16	112 (%93)
47	(47 94 188 121 242 229 203 151)	16	24	104 (%87)
53	(53 106 212 169 83 166 77 154)	16	32	96 (%80)
61	(61 122 244 223 211 167 79 158)	16	32	96 (%80)
91	(91 182 109 218 181 107 214 173)	16	16	112 (%93)
119	(119 238 221 187)	22	16	112 (%93)
27	(27 54 108 216 177 99 198 141)	26	48	80 (%67)
43	(43 86 172 89 178 101 202 149)	30	48	80 (%67)
87	(87 174 93 186 117 234 213 171)	30	48	80 (%67)
51	(51 102 204 153)	50	12	116 (%97)
85	(85 170)	84	10	118 (%98)
1	(1 2 4 8 16 32 64 128)	256	128	0 (%0)

Bunun yanında 3 (Gold) [6], 9 (Gold) [6] , 39 [7] (Kasami) sınıfları APN fonksiyonlardır. 5, 21, 95 ve 127 sınıfları diferansiyel fark dağılımı için 4. uniformdur. Ancak sadece 127 sınıfı bijektifdir. 7, 25, 37 ve 63 sınıfları ise 6 uniformdur. Buna ek olarak bu dört sınıftan 7 ve 37 sınıfları aynı fark dağılımını vermektedir (157 tane 0, 84 tane 2, 1 tane 4 ve 14 tane 6). 6 dağılımına sahip fakat bijektif olmayan 25 sınıfı 172 tane 0, 48 tane 2, 28 tane 4 ve 8 tane 6 içerirken bijektif olmaya diğer bir sınıf olan 63, 156 tane 0, 86 tane 2 ve 14 tane 6 içermektedir.

$S : GF(2^n) \to GF(2^n)$ şeklindeki bir S-kutusu için maksimum doğrusal olmama değeri NLM_{Smaks} değeri $2^n - 2^{\frac{n}{2}-1}$ (n çift) olarak verilebilir. Dolayısıyla herhangi bir S kutusu için

elde edilecek NLM_S değerinin $NLM_{S\max}$ değerine oranı bize % olarak o S-kutusunun doğrusal olmama değerini verecektir. Tablo 1 de % değerleri bu şekilde elde edilmiştir. Tablo 1 de $|N_{Lmaks}(a,b)|$ değerleri verilmiştir. Örneğin 3, 9, 39 APN fakat bijektif olmayan fonksiyonlar için bir satır LAT dağılımı 0 sayısı 65 tane, $|8|$ sayısı 170 tane, $|16|$ sayısı 21 tane, 7 ve 37 sınıfı için 0 sayısı 105 tane, $|8|$ sayısı 120 tane, $|16|$ sayısı 30 tane, $|32|$ sayısı 1 tane, 127 sınıfı için 0 sayısı 17 tane, $|2|$ sayısı 48 tane, $|4|$ sayısı 36 tane, $|6|$ sayısı 40 tane, $|8|$ sayısı 34 tane, $|10|$ sayısı 24 tane, $|12|$ sayısı 36 tane, $|14|$ sayısı 16 tane, $|16|$ sayısı 5 tane şeklinde verilebilir.

4.SONUÇLAR

Bu çalışmada üs haritalama tabanlı 8-bit giriş 8-bit çıkışlı S-kutuları sınıflandırılmıştır. Bu sınıflandırmaya göre elde edilen sonuçların önemli bir kısmı verilmiştir. 7-bit ve 9-bit giriş çıkışlı S-kutuları içinde aynı çalışma genişletilebilir.

Elde edilen sınıflar içerisinde kriptografik özellikler açısından en iyi sonuçları veren fonksiyonların APN fonksiyonlar olduğu söylenebilir. Diğer yandan bijektif S-kutuları açısından ise 127 sınıfı her iki kriptografik özellikler açısından iyi sonuçlar vermektedir. Dolayısıyla S-kutusu tasarımında herhangi bir 127 sınıf elemanı kullanılabilir (Nitekim AES S-kutusu bu sınıfın 254 elemanını kullanmaktadır). 7 ve 37 sınıfları da kriptografik özellikler açısından çok ta kötü sonuçlar vermemektedir.

Bu çalışma sırasında fark edilen diğer önemli bir nokta ise her sınıftaki elemanın üs derecesinin aynı hamming ağırlığına sahip olmasıdır. Bu da S-kutusu tasarımında kullanılacak ikili affine dönüşümün yerine göre elde edilecek S-kutusundaki cebirsel ifadesindeki terim sayısı ve terimlerine göre sınıflandırma yapmanın mümkün olduğunu göstermektedir.

KAYNAKLAR

[1] M. T. Sakallı, E. Buluş, A. Şahin, F. Büyüksaraçoğlu, "Ters Haritalama Tabanlı S-kutularının Cebirsel Açıdan İyileştirilmesi", ISC'07 Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara-Türkiye, 13–14 Aralık 2007.

[2] J. Fuller, W Millan, "Linear redundancy in S-boxes", Proceedings of the Fast Software Encryption (FSE 2003), Lecture Notes in Computer Sci-ence, vol. 2887, pp. 74–86 Springer, Berlin, (2003).

[3] A. M. Youssef., S.E. Tavares., "Affine equivalence in the AES round function", Discrete Applied Mathematics, Elsevier, (2005).

[4] A. M. Youssef, S.E. Tavares, G.Gong, "On Some probabilistic approximations for AES-like s-boxes", Discrete Mathematics, Elsevier, 2006.

[5] T. Bending and D. Fon-Der- Flaas, "Crooked functions, bent functions and distance regular graphs", Electronic Journal of Combi natronics, 5:R34, 14, 1998.

[6] R. Gold, "Maximal recursive sequences with 3-valued recursive crosscorrelation functions", IEEE Transactions on Information Theory, 14:154–156, 1968.

[7] T. Kasami, "The weight enumerators for several classes of subcodes of the second order Reed-Muller codes", Information and Control, 18:369-394, 1971.

[8] A. Canteaut, P. Charpin, and H. Dobbertin, "Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture", IEEE Transactions on Information Theory, 46:4-8, 2000.

[9] H. D. L. Hollman and Q. Xiang, "A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences", Finite Fields and their Applications, 7:253–286, 2001.

[10] H. Dobbertin, "Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5", In Finite Fields and Applications, pages 113–121. Springer, 1999.

[11] M. S. Maxwell, "Almost Perfect Nonlinear functions and related combinatorial structures", Phd Thesis, 2005.

[12] K. Nyberg, "Differentially uniform mappings for cryptography", Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, vol. 765, Springer, Berlin, pp. 55-64, 1994.

[13] M. Matsui, "Linear cryptanalysis method for DES Cipher", Adv. Cryptology, Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, Springer, Berlin, 1994.

[14] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", J.Cryptology, 1991.

[15] M. T. Sakallı, "Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi", Phd Thesis, 2006.

[16] K. Chun, S. Kim, S. Lee, S. H. Sung, S.Yoon, "Differential and Linear cryptanalysis for 2-round SPNs", Information Processing Letters, Elsevier, 2002.

[17] A. M. Youssef, G. Gong, " On the Interpolation Attacks on Block Ciphers", 7 the International Workshop on Fast Software Encryption, pages 109–120, 2000.