İÇİNDEKİLER

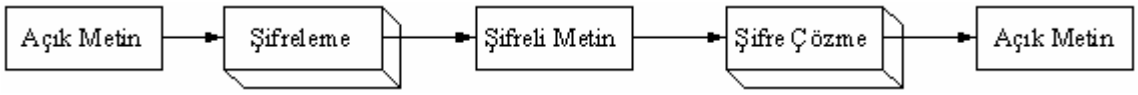
BÖLÜM 1

1. Giriş

Günümüzde bilgi güvenliği internetinde gelişimi ile birlikte bilginin güvenliğinin sağlanması gerekliliği açısından önemli hale gelmiştir. Kriptografi, verinin güvenli bir şekilde iletilmesi ile ilgilidir. Dolayısıyla güvenli şifreleme algoritması tasarımı kriptografi de çok önemli bir yer tutar.

1.1. Kriptografi

Yunanca gizli anlamına gelen "kript" ve yazı anlamına gelen "graf" kelimelerinden türetilen kriptografi anlaşılır bir mesajı anlaşılmaz hale dönüştürme ve tekrar anlaşılmaz mesajı anlaşılır hale geri dönüştürme işlemlerini kapsayan bir bilimdir. Şekil 1.1, şifreleme ve deşifreleme işlemlerini göstermektedir.



Şekil 1.1 Şifreleme ve deşifreleme yöntemi

Kriptografinin çok eski bir tarihi vardır. Eski mısırlılar yazılarını çeşitli hiyeroglif işaretlerle yazmışlar İbraniler ise kutsal kitaplarındaki bazı kelimeleri şifreli olarak aktarmışlardır. Julius Caesar (MÖ 100–44) zamanında devlet haberleşmesinde harflerin yerlerini değiştirmeye yönelik bir algoritmaya sahip olan Sezar şifresi kullanılmıştır. 730'lu yıllarda Abu Abd al-Rahman kriptografi üzerine bir kitap yazmıştır. Kitaptaki yöntemler 2. dünya savaşında kullanılan Enigma makinesi için ilham kaynağı olmuştur. Günümüzdeki modern şifre yöntemlerinin gelişmesi ise 1970'lerin ortasında DES (Data Encryption Standard) [1] algoritmasının IBM ve NSA tarafından ortaya atılması ile başlamıştır.

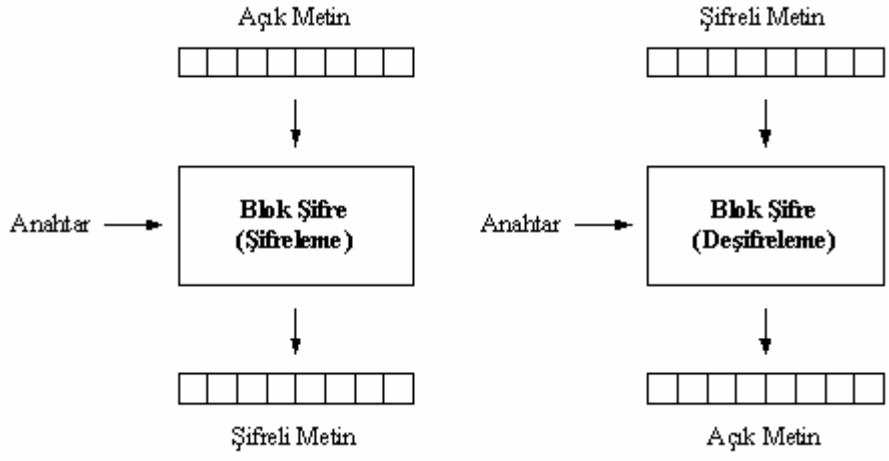
Günümüzde kullanılan modern şifreleme algoritmalarını üç grupta incelenebilir. Bunlardan ilki simetrik şifreleme algoritmalarıdır. Blok ve akan şifreler bu gruptadır. Bu algoritmalarda şifreleme ve deşifreleme için aynı gizli anahtar kullanılır. Bir diğer gruptaki algoritmalar asimetrik şifreleme algoritmalarıdır. Bu algoritmalarda yine şifreleme için gizli bir anahtar kullanılırken, deşifreleme işlemi için herkesin ulaşabileceği açık bir anahtar kullanılır. Son grupta olan şifreleme algoritmaları ise hash algoritmalarıdır. Bunlar verinin sıkı bir temsilini oluşturmak için kullanılırlar ve kimlik denetiminin sağlanmasında büyük rol oynarlar. Tablo 1.1 de, bu 3 gruptaki şifreleme algoritmalarına örnekler verilmiştir.

Simetrik Şifreleme Algoritmaları		Asimetrik Şifreleme Algoritmaları	Hash Algoritmaları
Blok Şifreler	Akan Şifreler		
-DES [1] -IDEA [2] -Square[3] -AES [4] -Camellia[5]	-RC4 [2] -Trivium[6] - HC-256 [7]	- RSA [2] - ElGamal [2] - ECC [8]	- MD4 [2] - MD5 [2] - SHA [2] -RIPEMD-160 [9]

Tablo 1.1 Üç gruba göre şifreleme algoritmalarına örnekler

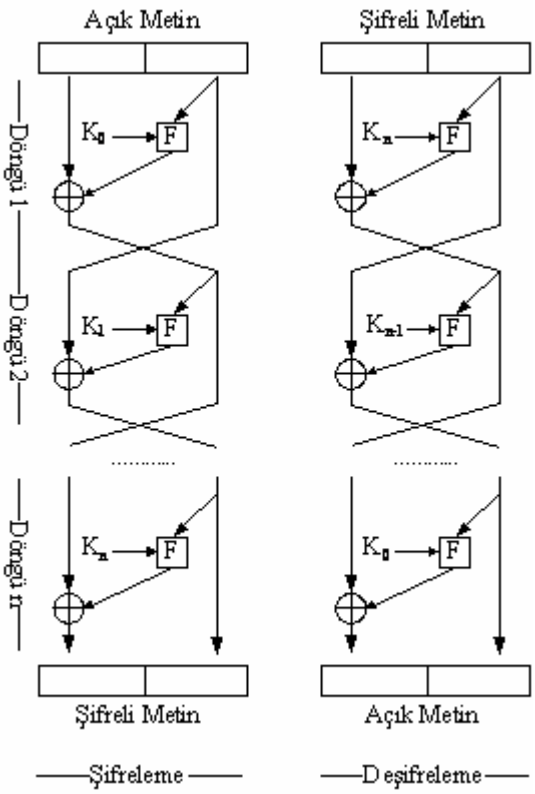
1.1.1. Blok Şifreler

Blok şifreleme algoritmaları açık metni sabit uzunluklu blok adı verilen bit grupları halinde işler. Bloklar bir anahtar aracılığı ile şifrelenerek şifreli metin ortaya çıkar. Deşifreleme işleminde yine aynı anahtar sayesinde şifreli metin açık metin haline getirilir.

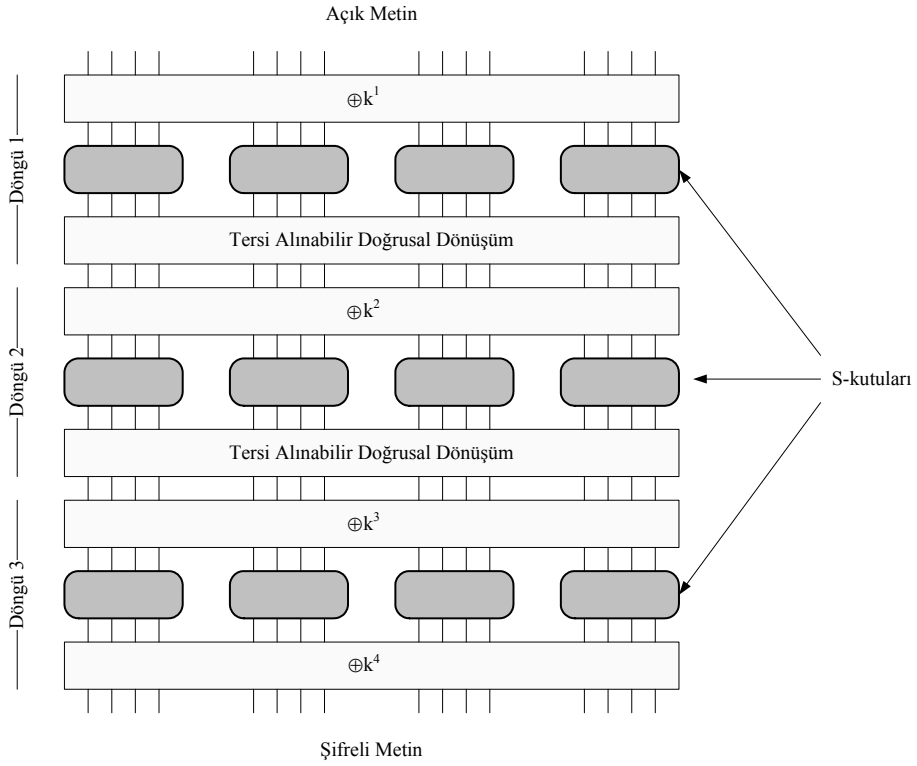


Şekil 1.2 Blok şifreleme ve deşifreleme

Blok şifreler, Shannon'un [10] önerdiği karıştırma (confusion) ve yayılma (diffusion) teknikleri üzerine kuruludur. Karıştırma şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken, yayılma açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır. Karıştırma yer değiştirme, yayılma ise doğrusal dönüşüm işlemleri ile gerçeklenir. Blok şifresi iki mimari üzerine kuruludur. Bunlar Feistel ağları ve Yerdeğiştirme-Permütasyon ağlarıdır (SPN) [11]. Her ikisi mimari de yerdeğiştirme ve doğrusal dönüşüm yapılarını kullanır. Ayrıca her iki mimari ürün şifrelerinin örneklerindendir. Yani birden fazla şifreleme işleminin birleşmesi ile oluşturulurlar. Tekrarlanan şifreler yine ürün şifreleridir ve aynı şifreleme adımının tekrarlanan uygulamasını içerir ve her şifreleme adımına döngü denir. Bir döngü birden fazla şifreleme adımı içerebilir. Genellikle her döngüde farklı anahtar materyali kullanılmaya özen gösterilir. Örneğin DES algoritması Feistel ağları tabanlı iken, AES (Advenced Encryption Standard) [4] algoritması SPN mimarisi tabanlı olarak tasarlanmıştır.



Şekil 1.3 Feistel ağı



Şekil 1.4 16 bit giriş-çıkışlı 3 döngülük bir örnek SPN ağı

Blok şifrelerin gücünü belirleyen bazı faktörler aşağıdaki gibidir.

- Anahtar: Blok şifrelerde anahtarın uzunluğu saldırılara karşı güçlü olacak şekilde seçilmelidir. DES algoritması 56-bit anahtar uzunluğu kullanırken, AES algoritması 128, 192, 256 bit anahtar uzunluklarını seçenekli olarak sunmaktadır. Bunun sayesinde şifrenin kaba kuvvet (brute-force) saldırısına karşı kırılabilirliği zorlaşmaktadır.

- Döngü sayısı: Blok şifreleme algoritmalarında döngü sayısı iyi seçilmelidir. Böylelikle doğrusal dönüşüm ve yerdeğiştirme işlemleri ile şifreleme algoritması daha da güçlenmektedir. Ayrıca şifrenin karmaşıklığının arttırılmasında çok önemli bir etkendir. Böylelikle saldırılara karşı açık metin iyi derecede korunabilir. Döngü sayısını belirleyebilmek için belirli bir teorik hesaplama olmamasına rağmen Lars Knudsen'e göre kabaca döngü sayısı

$$r \geq \frac{dn}{w} \tag{1.1}$$

(1.1) ifadesindeki gibi olmalıdır [12]. Bu ifadede r döngü sayısını, d yer değiştirme durumda bir word'ü almak için gerekli maksimum döngü sayısını, n blok genişliğini ve w ise tüm şifrede yer değiştirme durumuna giriş olan minimum word genişliğini temsil etmektedir. Bu duruma göre aşağıdaki tabloda bazı blok şifreleme algoritmaları için döngü sayıları verilmiştir.

Algoritma	Döngü Sayısı	[12]'ye göre olması gereken döngü sayısı
DES	16	21
IDEA	8	8
BlowFish	16	16
AES	10	16

Tablo 1.2 Döngü sayılarına göre bazı şifreleme algoritmaları

- S-kutuları (Yerdeğiştirme kutuları): Blok şifreleme algoritmalarının en önemli elemanı S-kutularıdır. Algoritmanın tek doğrusal olmayan elemanıdır. Bu yüzden iyi bir S-kutusu seçimi şifrenin karmaşıklığını doğrudan etkiler. Bu çalışmanın ilerleyen bölümlerinde S-kutuları ile ilgili ayrıntılı bilgiler verilecektir.

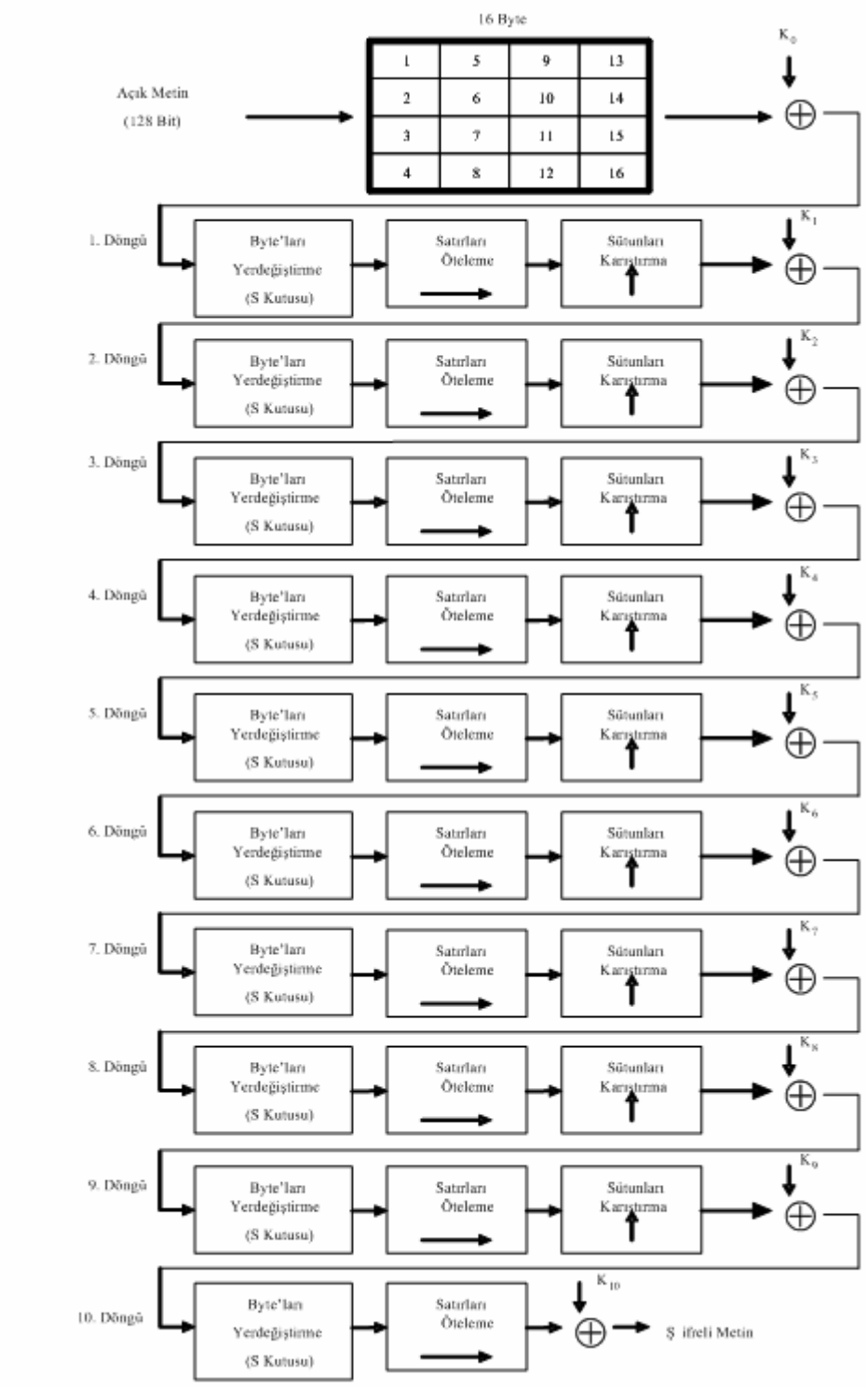
Günümüzdeki en güçlü blok şifreleme algoritmalarından bir tanesi AES algoritmasıdır. Belçikalı bilim adamları Vincent Rijmen ve Joan Daemen tarafından 1998 yılında önerilen Rijndael şifresi 2001 yılında standartlaştırılmış ve AES olarak literatürde yerini almıştır. AES şifresi bilinen tüm saldırılara karşı kendini güvenle korumuştur. Sadece indirgenmiş döngüler ile değiştirilmiş AES algoritmalarına karşı literatürde başarılı saldırılar mevcuttur.

DES algoritması 1970'li yıllarda IBM ve NSA ile birlikte öne sürüldüğünde 1990'lı yıllara kadar kendini başarı ile savunmuştur. DES 56 bit anahtar üzerinden açık metni şifrelemektedir. Anahtarın uzunluğunu değiştirmek mümkün değildir. Bu nedenle geniş anahtar arama saldırısı gibi saldırılara karşı yetersiz kalmıştır.

DES algoritması Feistel mimarisine sahiptir. Yani veri bloğu iki parçaya bölünerek şifreleme işlemi yapılmaktadır. Heys, 1994 yılındaki [13] çalışmasında, bir SPN algoritması kullanarak diferansiyel ve doğrusal kriptanalize karşı güçlü DES algoritmasına eşit güçte bir algoritmayı 8 döngüde sağlamıştır. Bu algoritma 64 bit blok uzunluğunda, 64 bit anahtar ve 8 bit girişli 8 bit çıkışlı rastgele S-kutuları kullanmaktadır. Bunun yanında S-kutularının güçlü hale getirilmesi için bazı çalışmalar da gerçekleştirilmiştir. Bunlar özetle rastgele S-kutuları, heuristic arama ile güçlü S-kutularının eldedilmesi, şifre içerisinde anahtar bağımlı olarak S-kutularının sırasının değiştirilmesi, matematiksel bağlamda saldırılara karşı güçlü S-kutuları tasarımı gibi olarak verilebilir. Bu çalışmaların birinde Nyberg [14] S-kutularının tasarımında sonlu cisimde ters alma yönteminin kullanılmasını önermiştir. Nyberg'in çalışmasından esinlenen AES tasarımcıları şifrelerinin tasarımında sonlu cisimde ters haritalama tabanlı bir S-kutusunu kullanmışlardır.

AES 128 bit veri bloklarını 128, 192, 256 bit anahtar seçenekleri ile şifreleyen bir algoritmadır. SPN mimarisi tabanlıdır. Döngü sayısı anahtar uzunluğuna göre değişmektedir. 128 bit anahtar uzunluğu için AES şifreleme algoritması 10 döngüde şifreleme yaparken 192 ve 256 bit anahtar uzunlukları için sırasıyla 12 ve 14 döngüde şifreleme yapmaktadır.

AES algoritmasında her döngü dört katmandan oluşur. İlk olarak 128 bit veri 4×4 byte matrisine dönüştürülür. Daha sonra her döngüde sırasıyla byte'ların yerdeğiştirmesi, satırları öteleme, sütunları karıştırma ve anahtar planlamadan gelen o döngü için belirlenen anahtar ile XOR'lama işlemleri yapılmaktadır. Byte'ların yerdeğiştirilmesinde 16 byte değerinin her biri 8 bit girişli ve 8 bit çıkışlı S-kutusuna sokulur. S-kutusu değerleri, Galois cismi (Galois Field-GF) $GF(2^8)$ de, 8 bitlik değerlerin $P(X) = X^8 + X^4 + X^3 + X + 1$ polinom tabanlı sonlu cisimde tersi alındıktan sonra doğrusal bir dönüşüme sokularak elde edilmektedir. Satırların ötelenmesi işleminde 4×4 byte matrisinde satırlar ötelenmiş ve sütunların karıştırılması işleminde herhangi bir sütun için o sütundaki değerler karıştırılmaktadır. Sütun karıştırma işleminde Galois cisminde iki sayının çarpım kavramı kullanılmaktadır. Döngünün son katmanında ise o döngüye ait anahtar ile XOR'lama yapılmaktadır.



Şekil 1.5 AES algoritması

Algoritmadaki sütunların karıştırılması bir SPN algoritmasına bakıldığında ek bir doğrusal dönüşüm işlemidir. Şekil 1.5'te 10 döngülük AES algoritması

gösterilmektedir. AES algoritmasındaki S-kutularının tasarımında sonlu cisimde ters alma işleminin kullanılması, doğrusal kriptanaliz için kullanılan doğrusal yaklaşım tablolarına ve diferansiyel kriptanaliz için kullanılan fark (difference) dağılım tablolarına girişlerin olabildiğince uniforma yakın olmasını sağlarken, sütun karıştırma işlemi saldırılarda az sayıda aktif S-kutusu kullanmayı imkânsız hale getirmektedir. AES şifresi hakkında daha detaylı bilgiyi [4]'ten elde edilebilir.

1.1.2. Akan Şifreler

Akan şifreleme algoritmaları, açık metnin bir karakterine bir seferde zamanla değişen bir şifreleme fonksiyonu kullanarak açık metnin karakterlerini ayrı ayrı şifreler. Akan şifreler eş zamanlı ve eş zamansız olmak üzere temelde ikiye ayrılırlar. Eş zamanlı akan şifrelerde anahtar dizisi, açık metin ve gizli anahtardan bağımsız olarak üretilir. Her iki şifreleme tipi de sonlu durum otomatıdır ancak eş zamansız akan şifrelerde anahtar dizisi, sabit uzunluktaki bir önceki şifreli metinlerin ve anahtarın bir fonksiyonu ile elde edilir. Bu şifreleme algoritmalarından eş zamansız akan şifrelerde şifreleme v şifreli metin sembolüne bağlı olduğu için bir iletim hatası durumunda v sembol sonra şifrenin tekrar eş zamanlaması mümkün olacaktır. Böyle bir durum söz konusu olduğunda öteki v sembol hatalı olacaktır. Yani hata yayılması eş zamanlı şifrelere göre kötüdür. Ancak eş zamanlama düşünüldüğünde eş zamansız şifreler eş zamanlı olanlara göre daha iyidir. Eş zamanlı şifrelerde eş zamanlama tekrar sağlanamaz.

Temelde bakıldığında akan şifreler donanım ve yazılım uygulamaları için geliştirilmiş akan şifreler olmak üzere iki farklı kategoriye ayrılabilir. Donanım tabanlı geliştirilen akan şifrelerinin yapıtaşları olarak doğrusal geri beslemeli öteleyici saklayıcılar (Linear Feedback Shift Registers) gösterilebilir. Bunun nedeni olarak donanımsal uygulamalardaki uygunlukları, üretilen serinin geniş periyoda sahip olması ve iyi istatistiksel özellikler göstermesi verilebilir. Doğrusal geri beslemeli saklayıcılarda ki doğrusallığın yok edilmesi için boole fonksiyonları kullanılarak elde edilen Doğrusal Olmayan Birleşim Üreteçleri (Nonlinear Combination Generators) ve Doğrusal Olmayan Filtre Üreteçleri (Nonlinear Filter Generators) akan şifrelerinin iki

farklı tasarım yöntemini temsil eder. Doğrusal Olmayan Birleşim Üreteçleri birden fazla doğrusal geri beslemeli öteleyici saklayıcının bir boole fonksiyonu ile birleşiminden meydana gelirken, Doğrusal Olmayan Filtre Yaklaşımında bir tane doğrusal geri beslemeli saklayıcı kullanılır. Diğer yandan Doğrusal Olmayan Filtre Yaklaşımı, F_{2^w} genişletilmiş cismini kullanan ve yazılım yoluyla tasarlanan akan şifrelerde tasarım için etkin bir yoldur. Bunun nedeni olarak F_{2^w} üzerine tanımlanan maksimum uzunluklu doğrusal geri beslemeli öteleyici saklayıcıları ötelenmesinin yazılımda oldukça maliyetli olması gösterilebilir [15]. Yine doğrusal geri beslemeli öteleyici saklayıcı temelli akan şifrelerin diğer bir kategorisi de saat kontrollü üreteçlerdir. Bu tür şifrelerdeki tasarım felsefesinde saat vuruşlarının sayısını düzensiz sinyaller kullanarak kontrol etme fikri vardır. Saat besleme sinyali bir doğrusal geri beslemeli öteleyici saklayıcı olabileceği gibi şifrenin diğer içsel bir yapısı da olabilir. Bu metotla doğrusal geri beslemeli saklayıcıların çıkışındaki doğrusallığın yok edilmesi amaç edinilir.

Diğer tasarım mekanizmalarından biri de doğrusal olmayan durum kullanan mekanizmalardır. Bu mekanizmalardan RC4 rastlantısal olarak karıştırma temellidir. Bununla beraber doğrusal geri beslemeli saklayıcı temelli doğrusal olmayan güncellemeye sahip şifrelere örnek olarak E0 (Bluetooth da kullanılan akan şifre) [16] verilebilir. Bu tür şifrelerin tasarımında doğrusal geri beslemeli saklayıcının doğrusallığını yok etmek için doğrusal olmayan bir bellek eklenir. Doğrusal geri beslemeli saklayıcı tabanlı fakat doğrusal olmayan durum güncellemesine sahip olan diğer mekanizmalara örnek saat kontrollü üreteçler verilebilir. GSM de kullanılan A5 şifresi [17], alternatifli adım üreteci ve eSTREAM adaylarından Decim [18], Mickey [19] ve POMARANCH [20] bu mekanizmalardandır. Bu tasarım mekanizmaları dışında doğrusal geri beslemeli saklayıcıların cebirsel saldırılar gibi saldırılar karşısında zayıf düşmesinin bir sonucu olarak kullanılan doğrusal olmayan geri beslemeli saklayıcıları (Nonlinear Feedback Shift Registers) kullanan şifreler de mevcuttur. Bu şifrelere örnek olarak eSTREAM adaylarından HC–256 [7] ve Trivium [6][21] verilebilir. Bu şifrelerden HC–256 yazılım tabanlı bir şifre iken Trivium donanım tabanlı bir şifredir

Akan şifrelerin ayrıldığı diğer bir kategori de bu şifrelerin word tabanlı ya da bit tabanlı olup olmamaları ile ilgilidir. Yukarıdaki örnek verilen şifrelerden HC–256 word tabanlı iken Trivium bit tabanlı bir akan şifredir.

1.2. Kriptanaliz

Kriptanaliz açık metni veya anahtarı elde etme bilimidir. Kısacası şifre kırma bilimidir. Kriptoloji içerisinde oldukça önemli bir yere sahiptir. Ortaya sürülen bir şifreleme sisteminin zayıf ve güçlü yönlerini ortaya çıkarmak için kullanılabileceği gibi kötü niyetli olarak bir şifrenin kırılıp açık metne ulaşmak içinde kullanılabilir. Bilinen kayıtlı ilk kriptanaliz açıklaması 9.yy da Matematikçi olan Ebu Yusuf Yakup tarafından yazılan "A Manuscript on Deciphering Cryptographic Messages" eserinde yer almıştır. Bu yöntem frekans analizine dayanmaktadır [22]. İkinci dünya savaşı ile beraber kriptanalizin önemi daha çok ortaya çıkmıştır. Bu şekilde Almanların Enigma şifresi kırılmış ve savaşın yönü büyük oranda değişmiştir.

Kriptanalizde düşmanın saldırı yapılan kripto sistemi bildiği kabul edilir (Kerckhoffs'un prensibi) ve bu koşul altında düşman kripto sistemin en önemli öğesi olan şifreleme algoritmasına saldırı gerçekleştirir. Düşmanın bir kripto sisteme saldırabilmesi için sahip olması gereken veriler vardır. Bu sahip olduğu verilere göre saldırı modellerinden birini seçebilir. Bu saldırı modellerinden en yaygın olanları şunlardır [23]:

- Sadece şifreli metin saldırısı; Düşman şifreli metin dizisine sahiptir,
- Bilinen açık metin saldırısı; Düşman açık metin dizisine ve bunların şifreli metin dizisine sahiptir,
- Seçilmiş açık metin saldırısı; Düşman bir açık metin dizisini seçebilir ve bunların şifreli metinlerini oluşturabilir,
- Seçilmiş şifreli metin saldırısı; Düşman bir şifreli metin dizisi seçebilir ve bunların açık metinlerini oluşturabilir.

Blok şifrelerin kırılması, zaaflarının ve güçlü yanlarının anlaşılması için birden fazla kriptanaliz yöntemi kullanılabilir. Bunlardan en önemlileri doğrusal ve diferansiyel kriptanalizdir. Bu saldırılar, şifrenin doğrusal olmayan tek yapısı olan S-kutularını hedef alır. Örneğin AES şifresi doğrusal ve diferansiyel saldırılara karşı dayanıklı olması amacıyla geliştirilmiş bir şifredir.

1.2.1. Doğrusal Kriptanaliz

1993 yılında Matsui [24] tarafından teorik bir saldırı olarak keşfedilmiştir. Daha sonra DES algoritmasına karşı başarı ile uygulanmıştır. Modern sifreleme algoritmalarının tasarımında dikkate alınması gereken önemli bir unsurdur.

Doğrusal kriptanaliz, S-kutularının doğrusal ifadelere dönüştürülmesi ve doğrusal ifadeleri birleştirerek bilinmeyen anahtar bitlerini elde etme prensibine dayanır. Doğrusal kriptanaliz, şifreli metin bitleri ile açık metin bitleri arasındaki yüksek olasılıkta doğrusal ifadelerin meydana gelme avantajını kullanır. Bunun yolu da S-kutularından geçer. Saldırganın algoritmayı bildiği (Kerchoffs kuralı) ve belli sayıda açık metin ve şifreli metinlere sahip olduğu varsayılır. S-kutularının büyüklüğü, aktif S-kutularının (doğrusal ifade içinde olan) sayısının artışı ve doğrusal sapması küçük S-kutularının tasarımı doğrusal kriptanalizin uygulanmasını engelleyici faktörlerdir. Bu işlem için son döngüde yerine getirilen yer değiştirmelerden önceki durum bitleri ile açık metin bitleri arasında doğrusal bir ilişki bulunması gereklidir. Bu doğrusal ifade olası tüm anahtar bitleri ile test edilir ve anahtar bitlerinin sapması teorik olarak elde edilen sapma değeri ile karşılaştırılır. En yüksek sapma ($\frac{1}{2}$ den + yada -) değerine sahip anahtar aranılan hedef anahtardır. Eğer hedef anahtar yanlış ise sapma 0 değerine yakın olacaktır.

1.2.2. Diferansiyel Kriptanaliz

1991 yılında Biham [25] tarafından keşfedilmiş bir kriptanaliz yöntemidir. Doğrusal kriptanalize benzemekle beraber seçilmiş açık metin saldırısı modeline

dayanmaktadır. Yani açık metin çiftlerindeki özel farkların sonuçlanan şifreli metinlerde oluşturduğu farkın etkisini analiz eder. Bu farklar mümkün olan anahtarların olasılıklarını ve en yüksek mümkün anahtarı ortaya koymak için tayin edilir. Kısacası bu saldırıda birçok sayıda açık metin ve şifreli metin çiftlerini üretilir. Bu çiftler arasındaki özel farklara karşılık şifreleme algoritmasının son döngüsündeki S-kutusundan önceki durum bitleri farkı bulunur. Bu farka göre her açık ve şifreli metin çiftleri için olası anahtar değerleri denenir ve eğer uygun bir değer yakalanır ise sayaç değeri bulunan anahtar değeri için 1 arttırılır. Yüksek olasılığı yakalayan anahtar değeri aranan hedef anahtar olarak kabul edilir.

İki saldırı yönteminde de S-kutularının önemi açıktır. Eğer şifreleme algoritması için kriptografik özellikler açısından iyi S-kutuları seçilirse hem doğrusal hem de diferansiyel saldırılara karşı daha dayanıklı ve güvenli şifreleme algoritmaları tasarlanabilir.

Bu iki kriptanaliz yöntemlerinin dışında imkânsız diferansiyel kriptanaliz [26], çokluset saldırıları [27], interpolasyon saldırısı [28] gibi cebirsel saldırılar, boomerang saldırısı [29], kare (rectangular) saldırısı [30], yan kanal saldırıları [31] gibi çeşitli saldırı teknikleri mevcuttur.

BÖLÜM 2

2. Matematiksel Altyapı

Kriptolojide kullanılan karmaşık şifreleme algoritmaları matematiğin bazı teorilerinin birleşmesi ile ortaya çıkmıştır. Bunların en önemlileri sonlu cisimler teorisi, sayı teorisi ve kodlama teorisidir.

Bu bölümde tez esnasında kullanılan ve tezin anlaşılması açısından önemli olan bazı matematiksel tanım ve teorilere yer verilecektir. Bu tanım ve teorilerin ispatlarına [32] [33] ve [34]'den elde edilebilir.

2.1. Sonlu Cisim Teorisi

Aritmetik mod m işlemi: Z_m toplama ve çarpma işlemi ile birlikte $\{0,1,....,m-1\}$ seti olacak şekilde tanımlanır. Z_m'de toplama ve çarpma işlemi sonucu modulo m'e indirgenir.

Tanım 2.1: Cisim, toplama ve çarpma işlemleri ile aşağıdaki aksiyomları sağlayan elemanları boş olmayan bir Z setidir.

1. Toplamada kapalılık özelliği;
   $a,b \in Z_m \rightarrow a+b \in Z_m$
2. Çarpmada kapalılık özelliği;
   $a,b \in Z_m \rightarrow a.b \in Z_m$
3. Toplamada değişme özelliği;
   $a,b \in Z_m \rightarrow a+b=b+a$
4. Çarpmada değişme özelliği;
   $a,b \in Z_m \rightarrow a.b=b.a$

5. Toplamada geçişme özelliği;
   $a,b,c \in Z_m \rightarrow (a+b)+c = a+(b+c)$
6. Çarpmada geçişme özelliği;
   $a,b,c \in Z_m \rightarrow (a.b).c = a.(b.c)$
7. Çarpmada dağılma özelliği;
   $a,b,c \in Z_m \quad \rightarrow \quad (a.b).c = a.(b.c)$
   $a.(b+c) = a.b + a.c$

İki farklı birim elemanı (identity) 0 ve 1 (sırası ile toplamaya ve çarpmaya göre) aşağıdakileri sağlayan Z_m'in içinde olmak zorundadır.

8. $a+0 = a, \forall a \in Z_m$
9. $a.1 = a$ ve $a.0 = 0, \forall a \in Z_m$
10. $a \in Z_m$ için a nın toplamaya göre tersi $m-a$ dır.
11. $a \in Z_m$ için a nın çarpmaya göre tersi a^{-1} dir ve $a^{-1}.a = 1$ olmalıdır.

Tanım 2.2: Eğer Z_m seti yukarıdaki 1, 2, 5, 6 ve 7 numaralı aksiyomları sağlıyor ise toplama ve/veya çarpma işlemlerine göre gruptur denir. Buna ek olarak 3 ve 4 numaralı aksiyomlar da sağlanıyor ise abelyan grup adı verilir.

Tanım 2.3: Eğer Z_m seti yukarıdaki aksiyomlardan 1'den 9'a kadar olan aksiyomları sağlıyor ise bu sete halka denir. Örneğin tam sayılar ve reel sayılar birer halkadır.

Tanım 2.4: Eğer Z_m seti yukarıdaki aksiyomların hepsini sağlıyor ise cisim olarak adlandırılır. Sonlu elemana sahip cisimlere sonlu cisim adı verilir.

Örnek 2.1: Z_4'ü ele alalım. Sonlu bir cisim olup olmadığını inceleyelim. $Z_4 = \{0,1,2,3\}$ elemanlarına sahip bir set olduğuna göre çarpma ve toplama işlemlerine göre Cayley tabloları aşağıdaki gibi elde edilebilir.

+	**0**	**1**	**2**	**3**
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	**0**	**1**	**2**	**3**
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Yukarıda görüldüğü gibi Z_4 seti aksiyomlardan 1, 2, 5, 6 ve 7 yi sağlamaktadır ve dolayısı ile bir gruptur. Aynı zamanda 3 ve 4 numaralı aksiyomları da sağlamaktadır. Bu yüzden bir ableyan gruptur. Z_4 setinin halka olduğu söylenebilir çünkü 1'den 9'a kadar olan aksiyomları da sağlamaktadır. Fakat Z_4 seti bir cisim değildir. Bunun nedeni çarpma işlemine göre 2 elemanının tersi yoktur.

Teorem 2.1: Eğer p asal sayı ise Z_p bir cisimdir.

Teorem 2.2: Eğer p asal sayı ise Z_p^*[1] çevrimsel bir gruptur.

Tanım 2.5: Z_p cisiminin 0 olmayan bir elemanı olan α'nın derecesi $\alpha^k = 1$ olmak üzere en küçük k değeridir.

Tanım 2.6: $\bmod p$'ye göre $(p-1)$ derecesine sahip bir α elemanına asal eleman denir.

Tanım 2.7: p asal ve α $\bmod p$'ye göre asal eleman olsun. Herhangi bir $\beta \in Z_p^*$, $\beta = \alpha^i (0 < i < p-2)$ olmak üzere yazılabilir. $\beta = \alpha^i$'nin derecesi

[1] Z_p^*: 0 elemanı hariç Z_p seti.

$\frac{p-1}{OBEB(p-1,i)}$'dir. Böylece eğer $OBEB(p-1,i)=1$ ise β asal bir elemandır. Dolayısıyla $\bmod p$'ye göre asal elemanların sayısı $\varphi(p-1)$'dir (bakınız Tanım 2.10).

Teorem 2.3: p asal ve $\alpha \in Z_p^*$ olsun. Eğer $(p-1)$'i bölen tüm asal q değerleri için $\alpha^{\frac{p-1}{q}} (\bmod p) \neq 1$ ise o zaman α $\bmod p$'ye göre asaldır.

2.2. Bölünebilirlik

$a \neq b$ şeklinde a ve b iki tamsayı tamsayı olsun. $a.c = b$ olacak şekilde bir c tamsayısı düşünelim. O zaman a, b'yi böler ya da b, a ile bölünebilir diyebiliriz ve $a|b$ şeklinde yazılır. Aynı şekilde b'ye a'nın katıda diyebiliriz.

Eğer a, b'yi bölmez ise $a \nmid b$ şeklinde gösterilir.

- Eğer $a|b$ ve $b|c$ ise $a|c$ olur

  $3 \mid 6 \quad 6 \mid 12 \rightarrow 3 \mid 12$

- $a|b$ her hangi bir x için $a|bx$ olur
- $a|b$ ve $a|c$ ise $a|b+c$ ve $a|b-c$ olur
- $1|a$ ise $a = \mp 1$ dir.

2.3. Asal Sayılar

Tanım 2.8: p > 1 olmak üzere pozitif bir tamsayının bölenleri ∓ 1 ve $\mp p$ ise o zaman p asal sayıdır.

Teorem 2.4: n bir tamsayı ve $n > 1$ olmak üzere, n tam sayısı asal sayıların bir ürünü olarak yazılabilir ve (2.1)'deki gibi gösterilebilir. m_i'ler pozitif ve $P_1 < P_2 < \ldots < P_r$ olacak şekildedir.

$$n = P_1^{m1}.P_2^{m2}.P_3^{m3}.....P_r^{mr} \qquad (2.1)$$

Örnek 2.2: $60 = 2^2.3^1.5^1$

2.4. Ortak Bölenlerin En büyüğü (Greater Common Divisior - GCD)

a ve b sıfır olmayan tamsayılar olsun. Eğer tamsayı d, d|a ve d|b şeklinde ise d'ye a ve b'nin ortak böleni denir. gcd(a,b) , a ve b nin en büyük ortak böleni olarak adlandırılır.

Teorem 2.5: ax+by formunun en küçük tam sayısı d olsun. O zaman d=gcd(a,b) olarak yazılabilir.

Örnek 2.3: 540 ile 168'in en büyük ortak böleni aşağıdaki gibi bulunabilir.

a'yı ve b ye bölerek ve tekrar tekrar her kalanı, sıfır kalan elde edene kadar bölünene bölünür.

gcd(540,168) =

168 | 36	36 | 24	24 | 12	540 | 168
144 | 4	24 | 1	24 | 2	504 | 3
24	12	0	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.

Tanım 2.9: 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.

Teorem 2.6: $ab \equiv ac \pmod{m}$ ve $\gcd(a,m)=1$ olsun. O zaman $b \equiv c \pmod{m}$ olur.

Teorem 2.7: $ab \equiv ac \pmod{m}$ ve $\gcd(a,m)=d$ olsun. O zaman $b \equiv c \pmod{m/d}$ olur.

Önerme 2.1: p asal sayı olmak üzere 1 den p ye kadar tam sayılar p ye göre asaldır. Böylece $ab \equiv ac \pmod{p}$ ve $a \not\equiv b \pmod{p}$ ise o zaman $b \equiv c \pmod{p}$ dir.

Tanım 2.10: $a \geq 1$ ve $m \geq 1$ olsun. Eğer $\text{OBEB}(a,m)=1$ ise a ve m için aralarında asal denir. Z_m de m ile aralarında asal olan tamsayıların sayısı genellikle $\varphi(m)$ ile tanımlanır ve bu fonksiyona Euler Phi Fonksiyonu denir.

Teorem 2.8: $\varphi(m)$, 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 $\varphi(m)$ (2.2) ifadesindeki gibi gösterilebilir.

$$m = \prod_{i=1}^{n} p_i^{e_i}, \qquad \varphi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i - 1}). \tag{2.2}$$

Örnek 2.4: $\varphi(98)$ değerini bulalım. Yani 98'den küçük 98 ile aralarında asal olan tamsayıların sayısını bulalım.

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

Önerme 2.2: $d = \gcd(a,b)$ ise ve c|a ve c|b ise c|d dir. Bunu aşağıdaki örnekte açık olarak görebiliriz.

gcd(6,12) =6 3|6 2|6

2.5. Euclidean Algoritması

a ve b tamsayılar gcd(a,b) ifadesini bulmak için Euclidean algoritması kullanılabilir. Euclidean algoritması Algoritma 1.1'deki gibidir.

Euclidean(a,b) →

$r_0 \leftarrow a$
$r_1 \leftarrow b$
$m \leftarrow 1$
while($r_m \neq 0$)
$\left\{ \begin{array}{l} q_m \leftarrow \left\lfloor \frac{r_{m-1}}{r_m} \right\rfloor \\ r_{m+1} \leftarrow r_{m-1} - q_m r_m \\ m \leftarrow m+1 \end{array} \right\}$
$m \leftarrow m-1$
return$(q_1, q_2 ... q_m, r_m)$
r_m=gcd(a,b)

Algoritma 1.1 Euclidean Algoritması

Örnek 2.5: 12 ve 16 sayılarının ortak bölenlerinin en büyüğünü Euclidean algoritmasını kullanılarak elde edilmesi aşağıdaki gibidir.

Euclidean(a,b) →

$r_0 = 12$
$r_1 = 16$
$m = 1$

1.döngü	2.döngü	3.döngü	döngü çıkış
$q_1 = 0$	$q_2 = 1$	$q_3 = 3$	$m = 3$
$r_2 = 12$	$r_2 = 4$	$r_2 = 0$	
$m = 2$	$m = 3$	$m = 4$	

Buna göre $r_3 = 4 = \gcd(12,16)$ şeklinde olacaktır.

2.5.1. Extended Euclidean Algoritması

Euclidean algoritması sadece a ve b tamsayılarının d = gcd(a,b) ifadesinde sadece d'yi hesaplarken Extended Euclidean Algoritması bu değerin yanında ax+by = d denklemindeki a ve b katsayılarını da bulmak için olanak vermektedir. Extended Euclidean Algoritması Algoritma 1.2'de verilmiştir.

Extended_Euclidean(a,b) →

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

Algoritma 2.1 Extended Euclidean Algoritması

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

Örnek 2.6: 28 ve 75 tamsayılarının Extended Euclidean algoritmasını kullanarak ax+by = d formunda elde edilmesi aşağıdaki gibidir.

Extended_Euclidean(75,28) =

$a_0 = 75$	$temp = -2$	$temp = 3$	$temp = 8$
$b_0 = 28$	$t_0 = 1$	$t_0 = -2$	$t = -8$
$t_0 = 0$	$t = -2$	$t = 3$	$temp = 3$
$t = 1$	$temp = 1$	$temp = -1$	$s_0 = -1$
$s_0 = 1$	$s_0 = 0$	$s_0 = 1$	$s = 3$
$s = 0$	$s = 1$	$s = 1$	$a_0 = 9$
$r = 19$	$a_0 = 28$	$a_0 = 19$	$b_0 = 1$
$q = 2$	$b_0 = 19$	$b_0 = 9$	$q = 0$
	$q = 1$	$q = 2$	$r = 0$
	$r = 9$	$r = 1$	

Döngü çıkışında $r = 1, s = 3, t = -8$ değerleri elde ederiz ve ax+by = d formunda aşağıdaki gibi gösterilebilir:

$$3 \times 75 + (-8) \times 28 = 1.$$

2.6. Cebirsel Yapılar

2.6.1. Yarı Gruplar (Semi Groups)

Tanım 2.11: S, boş olmayan bir küme ve *, S üzerinde tanımlı bir işlem olsun. (S, *) yapısı S üzerinde * işlemi birleştirme özelliğine sahip ise yarı gruptur. Eğer işlem hem birleştirme hem de değişme özelliğine sahip ise (S, *) yapısı değişken yarı grup adını alır. Eğer yarı grupların birleşme özelliğine ek olarak etkisiz eleman varlığı söz konusu ise bu yapılara monoid denir. Bir monoid etkisiz elemana sahip bir (S, *) yarı gruptur.

Tanım 2.12: Her bir elemanın tersinin olduğu monoide (S, *) grup denir. Yani (S, *) çifti üç şartı sağlar:

- *, S üzerinde birleşme özelliğine sahiptir.

- Bir etkisiz eleman mevcuttur.
- S'in her bir elemanının tersi vardır.

Tanım 2.13: Herhangi bir (G,*) grubunun sahip olduğu eleman sayısı yada derecesi (order) G kümesinin kardinalitesidir ve |G| şeklinde gösterilir.

Teorem 2.9: (G,*) bir grup ise sol ve sağ sadeleşme kuralı uygulanabilir. Yani a,x,y ∈ G ise

1. ax = ay ifadesinin anlamı x = y (sol sadeleştirme)
2. xa = ya ifadesinin anlamı x = y (sağ sadeleştirme)

şeklinde ifade edilebilir.

Tanım 2.14: (G,*) bir grup ve a,b ∈ G ise

a) ax = b denkleminin $x = a^{-1}b$ şeklinde tek bir çözümü vardır
b) ya = b denkleminin $y = ba^{-1}$ şeklinde tek bir çözümü vardır

Tanım 2.15: Eğer (G,*) sonlu bir grupsa, bu grubun cayley tablosunda G'nin her elemanı her bir satır ve sütunda sadece bir kez yer alır.

Tanım 2.16: En az bir üretece sahip gruplara cyclic denir.

Tanım 2.17: (G,*) grubu, n bir tamsayı olmak üzere her bir g ∈ G için a ∈ G elemanı mevcut ise halkadır denir. (G,*) grubu a tarafından üretilmiştir denir ve a, (G,*) grubunun üretecidir.

Örnek 2.7: Pozitif tamsayılar kümesi N^+

$(N^+,+)$ → birleşme (yarı grup)
$(N^+,*)$ → birleşme (yarı grup)
$(N^+,*)$ → etkisiz elemana sahip (1) (Monoid)
$(N^+,+)$ → etkisiz eleman yok (Monoid değil)

Örnek 2.8 : 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 modoid 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.

2.6.2. Permütasyon Gruplar

Tanım 2.18: S boş olmayan bir küme olsun. S'in bir permütasyonu S'ten S'e bir bijeksiyondur.

Bir bijeksiyon tanımlamak için kullanılan yol genellikle S'in tüm elemanlarının eşleşmelerinin etkilerini göstermektir [35].

Örnek 2.9: S={1,2,3,4} ise şu şekilde p_1 bijeksiyonu tanımlanabilir.

$p_1(1) = 2,\ p_1(2) = 4,\ p_1(3) = 3,\ p_1(4) = 1$

$p_1 = \begin{vmatrix} 1\,2\,3\,4 \\ 2\,4\,3\,1 \end{vmatrix}$ şeklinde gösterilebilir.

Örnek 2.10: A = {1,2,3} kümesini düşünelim olası tüm permütasyonlar S_3 kümesi P_1, $P_2 \ldots P_6$ olsun

$$p_1 = \begin{vmatrix} 1\,2\,3 \\ 1\,2\,3 \end{vmatrix} \quad p_2 = \begin{vmatrix} 1\,2\,3 \\ 2\,3\,1 \end{vmatrix} \quad p_3 = \begin{vmatrix} 1\,2\,3 \\ 3\,1\,2 \end{vmatrix} \quad p_4 = \begin{vmatrix} 1\,2\,3 \\ 1\,3\,2 \end{vmatrix} \quad p_5 = \begin{vmatrix} 1\,2\,3 \\ 3\,2\,1 \end{vmatrix} \quad p_6 = \begin{vmatrix} 1\,2\,3 \\ 2\,1\,3 \end{vmatrix}$$

Bu küme üzerinde birleşme P_iP_j ($P_i\,P_j \in S_3$) olmak üzere bileşke olarak tanımlansın

$p_{35} = \begin{vmatrix} 1\,2\,3 \\ 3\,1\,2 \end{vmatrix} \begin{vmatrix} 1\,2\,3 \\ 3\,2\,1 \end{vmatrix} \Rightarrow \begin{vmatrix} 1\,2\,3 \\ 1\,3\,2 \end{vmatrix}$ olarak bulunur.

O zaman (S_3,*) için cayley tablosu aşağıdaki gibi olmaktadır.

*	p_1	P_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_3	p_1	p_5	p_6	p_4
p_3	p_3	p_1	p_2	p_6	p_4	p_5
p_4	p_4	p_6	p_5	p_1	p_3	p_2
p_5	p_5	p_4	p_6	p_2	p_1	p_3
p_6	p_6	p_5	p_4	p_3	p_2	p_1

2.7 İzomorfizm

3 elemanlı bir kümenin D_3 dihedral grubu ve S_3 permütasyon grubu için cayley tablosu aşağıdaki gibi olsun.

*	r_0	r_1	r_2	m_1	m_2	m_3
r_0	r_0	r_1	r_2	m_1	m_2	m_3
r_1	r_1	r_2	r_0	m_2	m_3	m_1
r_2	r_2	r_0	r_1	m_3	m_1	m_2
m_1	m_1	m_2	m_3	r_0	r_1	r_2
m_2	m_2	m_3	m_1	r_1	r_2	r_0
m_3	m_3	m_1	m_2	r_2	r_0	r_1

Tablolar karşılaştırıldığında ilginç bir şekilde her iki tablonun isimlendirmeler dışında aynı olduğunu görmekteyiz. İlk tabloda r_2 olduğu yerde p_3; m_3 ün olduğu yerde p_6 vardır. p_1, p_2, …, p_6 dönüşümleri yerine sırası ile r_0, r_1, r_2, m_1, m_2, m_3 kullanırsak tablo iki sonlu grup bu şekilde ilişkilendirilmiş ise izomorfik olarak adlandırılır. izomorfik olmak grupların aynı olmasına denk değildir. Örneğimizde iki küme elemanları nasıl etiketlendirilirse etiketlendirilsin farklı ve ikili işlemleri aynı değildir. Öte yandan, izomorfik gruplar arasında çok yakın ilişki vardır öyle ki elemanları aynı olmasa da yapıları aynıdır ve bu şekilde bu ilişkiyi matematiksel olarak tanımlanabilir.

Cayley tablolarının isimlendirilmesi dışında aynı olması demek D_3 elemanları ve S_3 elemanları arasında birebir eşleşme olması demektir. Bu birebir eşleşme grup özelliğini muhafaza etme özelliğine sahip bir bijektif fonksiyondur. Bu tip fonksiyonlara izomorfik fonksiyonlar denir.

Daha doğru bir ifade ile : (G,*) ve (G',○) şeklinde verilmiş iki grup varsa bir izomorfizm bijektif bir f: G → G' fonksiyonudur. Öyle ki; g_1*g_2'nin görüntüsü G' nin elemanıdır ve ○ işleminin g_1 ve g_2'nin görüntüleme uygulaması işleminin sonucudur.

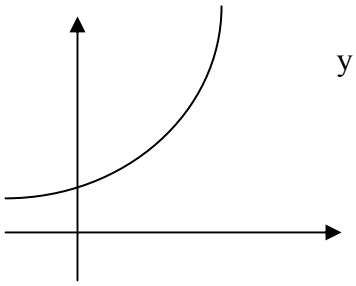
$$\begin{array}{ccc} G & & G' \\ g_1, g_2 & \xrightarrow{f} & f(g_1), f(g_2) \\ \downarrow & & \downarrow \\ g_1 * g_2 & & f(g_1) \circ f(g_2) \\ & \xrightarrow{f} & f(g_1 * g_2) \end{array}$$

$$f(g_1 * g_2) = f(g_1) \circ f(g_2)$$

Örnek 2.11: (R,+) ve (R^+,*) f : R → R^+ $f(x) = 2^x$ fonksiyonunun (R, +) dan (R^+, *) ya izomorfizmim tanımlandığını aşağıdaki gibi gösterilebilir :

İzomorfizm için

1. f fonksiyonunun bijektif olması gerekir
2. x, y ∈ R olmak üzere f(x+y) = f(x)*f(y) olması gerekir

1.  $y = 2^x$

   Her elemanın karşılığı olduğu için bijektiftir.

2. $2^{x+y} = 2^x.2^y$
   $2^{x+y} = 2^{x+y}$ izomorfik

Aslında iki grubun izomorfik olup olmadığını belirlemek grupların derecesi (order) büyük ise zaman alır.

Örnek 2.12: Z_4 te toplama ve S=(1,3,7,9) seti için Z_{10} da çarpma işlemi aşağıdaki tablolardaki gibi tanımlansın.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	1	0
3	3	0	1	2

*	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

f: Z_4 → S olmak üzere

f(0) = 1		0 → 1
f(1) = 3		1 → 3
f(2) = 7	şeklinde fonksiyon tanımlanırsa	2 → 9
f(3) = 9	izomorfizm gösterilebilir	3 → 7

f(1+3) = f(1)*f(3)	f(3+2) = f(3)*f(2)
f(0) = 3*7	f(1) = 7*9
1 = 1.	3 = 3.

2.8. Sonlu Cisimde Polinomlar

Tanım 2.19: Z_m bir cisim olmak üzere set $Z_m[X] := \left\{ \sum_{i=0}^{n} a_i X^i : a_i \in Z_m, n \geq 0 \right\}$, Z_m üzerine bir polinom halka olarak isimlendirilir. $Z_m[X]$'in bir elemanı Z_m üzerine polinom olarak isimlendirilir. Pozitif dereceli bir polinom $f(X) = \sum_{i=0}^{n} a_i X^i$ için $\text{derece}(g(X)) < \text{derece}(f(X))$, $\text{derece}(h(X)) < \text{derece}(f(X))$ ve $f(X) = g(X)h(X)$ şartlarını sağlayacak şekilde iki polinom varsa $f(X)$ polinomu Z_m üzerine indirgenebilir aksi takdirde pozitif dereceli $f(X)$ polinomu Z_m üzerine indirgenemez polinom olarak tanımlanabilir.

Örnek 2.13: $f(X) = X^4 + X^3 + 1$ polinomu 4. dereceden bir polinomdur ve katsayıları $Z_2[X]$'in elemanıdır.

Teorem 2.10: $f(X)$, derecesi 1'den büyük Z_m cisimi üzerine bir polinom olmak üzere $Z_m[X]/f(X)$ sadece ve sadece $f(X)$ indirgenemez ise cisimdir.

Örnek 2.14: $Z_2[X]/(X^2+X+1)$ halkasının sonlu bir cisim olup olmadığını incelenmek istendiğinde toplama ve çarpma işlemlerini ele alınmalıdır.

+	**0**	**1**	**X**	**1+X**
0	0	1	X	1+X
1	1	0	1+X	X
X	X	1+X	0	1
1+X	1+X	1	1	0

.	**0**	**1**	**X**	**1+X**
0	0	0	0	0
1	0	1	X	1+X
X	0	X	1+X	1
1+X	0	1+X	1	X

$Z_2[X]/(X^2+X+1)$ polinom halkası sonlu bir cisim oluşturur. Teorem 2.10 gereği $f(X)=(X^2+X+1)$ polinomu $Z_2[X]$ üzerine indirgenemez bir polinomdur. Ayrıca şekilde gösterilen toplama ve çarpma işlemleri bunu doğrulamaktadır.

Yukarıdaki Tanım 2.19 ve Teorem 2.10'u biraz açarsak, p asal ve $n \geq 1$ (n, $f(X)$ polinomunun derecesi) olmak üzere $q=p^n$ elemana sahip bir sonlu cisim vardır diyebiliriz. Diğer bir ifade ile $Z_m[X]/f(X)$ sonlu cisim ise bu sonlu cisim F_{p^n} ya da $GF(p^n)$ şeklindeki ifade ile tanımlanabilir ve bu özel sonlu cisim $GF(p)$ cisminin n. dereceden genişletilmiş cismi olarak adlandırılır. Örneğin $GF(2^3)$, $GF(2)$ cisminin 3. dereceden genişletilmiş cismi olarak isimlendirilir ve $GF(2)$ cismine, $GF(2^3)$ cisminin taban cismi adı verilir.

Tanım 2.20: Asal polinom (pirimitive polynomial) taban cisiminden genişletilmiş cisimin tüm elemanlarını üretebilen polinomdur.

Tanım 2.21: Asal eleman x, genişletilmiş cisim $GF(p^n)$'de $x^{p^n-1}=1$ olacak şekilde derecesi p^n-1 olan elemandır.

Teorem 2.11: Herhangi bir asal ya da asal üs q ve pozitif n için GF(q) üzerine n. dereceden bir asal polinom vardır ve bu asal polinomların sayısı $s_q(n) = \frac{\phi(q^n - 1)}{n}$ şeklinde bulunabilir.

Örnek 2.15: $Z_2[X]/(X^3 + X + 1)$ bir sonlu cisim olmak üzere bu sonlu cisimin eleman sayısı 8 dir ve F_{2^3} şeklinde gösterilebilir. Aşağıda 0 haricindeki F_{2^3}'ün elemanları gösterilmektedir.

$$X^1 = X$$
$$X^2 = X^2$$
$$X^3 = X + 1$$
$$X^4 = X^2 + X$$
$$X^5 = X^2 + X + 1$$
$$X^6 = X^2 + 1$$
$$X^7 = 1$$

Tanım 2.22: Daha önce bahsedildiği gibi Z_p^* (p asal) derecesi $(p-1)$ olan çevrimsel bir gruptur. Aynı şekilde $F_{p^n} \setminus \{0\}$ da derecesi $(p^n - 1)$ olan çevrimsel bir gruptur.

Örnek 2.16: $GF(2^8)$ sonlu cisimi için 8. dereceden asal polinomların sayısını bulalım.

$$s_q(n) = \frac{\phi(q^n - 1)}{n} \Rightarrow s_{2^4}(8) = \frac{\phi(2^8 - 1)}{8} = \frac{\phi(255)}{8} = \frac{(17^1 - 17^0).(5^1 - 5^0).(3^1 - 3^0)}{8} = 16.$$

Örnek 2.17: $Z_2[X]/(X^4 + X + 1)$ sonlu cisimine göre $f(X) = (X^4 + X + 1)$ polinomu $Z_2[X]$ üzerine indirgenemez hatta asal polinomdur.) $(0100) = (4)_{hex}$ değerinin tersinin $(1101) = (D)_{hex}$ olduğunu aşağıdaki gibi gösterilebilir:

$$(4)_{hex}.(D)_{hex} \bmod (X^4+X+1) \stackrel{?}{=} 1$$
$$(X^2).(X^3+X^2+1) \bmod (X^4+X+1) \stackrel{?}{=} 1$$
$$(X^5+X^4+X^2) \bmod (X^4+X+1) \stackrel{?}{=} 1$$
$$(X^2+X+X+1+X^2) \bmod (X^4+X+1) \stackrel{?}{=} 1$$
$$1 = 1$$

2.9. Sonlu cisimde İşlemler

2.9.1. 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 toplamıdır denilebilir.

Örnek 2.18: 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 bulunacaktır.

2.9.2. 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.

Örnek 2.19: $a = 1101$ 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.

2.9.3. 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 2.20: $GF(2^4)$ 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.

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

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)	1
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

Örnek 2.20'de n (örnek için 4) küçük olduğu için tablo kolay bir şekilde elde edilmiştir. Örneğin n = 8 için $GF(2^8)$ sonlu cisminde 0 elemanı ile birlikte 256 adet eleman mevcuttur. Bu cisim için hesaplamalar tablo ile yapılabilir. Bu tezde tablo yöntemi kullanılarak cisim elemanları $P(X) = X^8 + X^4 + X^3 + X + 1$ indirgenemez polinomu kullanılarak elde edilmiştir. Sonlu cisimde ters alma işlemi için ikinci yöntem ise ikili Euclidean algoritmasını kullanmaktır. Sonlu cisimde ters alma işlemi için ikili Euclidean algoritması Algoritma 2.1 de gösterilmiştir.

Giriş:	$a \in GF(2^m), a \neq 0$.
Çıkış:	$a^{-1} \bmod f$.
Adım 1:	$u \leftarrow a, v \leftarrow f, g_1 \leftarrow 1, g_2 \leftarrow 0$.
Adım 2:	X, u'yu tam böldüğü sürece aşağıdaki işlemleri gerçekle.
	Adım 2.1: $u \leftarrow u/X$.
	Adım 2.2: Eğer x, g_1'i tam bölerse $g_1 \leftarrow g_1/X$ yap aksi taktirde $g_1 \leftarrow (g_1 + f)/X$ yap.
Adım 3:	Eğer $u = 1$ ise (g_1) değerini döndür.
Adım 4:	Eğer derece (u) < derece(v) ise $u \leftrightarrow v, g_1 \leftrightarrow g_2$ yap.
Adım 5:	$u \leftarrow u + v, g_1 \leftarrow g_1 + g_2$.
Adım 6:	Adım 2'ye git.

Algoritma 2.1. Ters Alma İşlemi için İkili Euclidean Algoritması [23]

Algoritma 2.1 de gösterilen ikili Euclidean algoritması (1110)'ın tersini Örnek 2.20'de gösterildiği gibi $P_1(X) = X + 1$ yada (0011) şeklinde bulacaktır. Bu sonuç, derece$(P_1(X))$ < 4 ve derece$(P_2(X))$ < 3 olmak üzere $P_1(X).(X^3 + X^2 + X) + P_2(x).(X^4 + X + 1) = 1$ ifadesinde $P_1(X)$, $(X^3 + X^2 + X)$ polinomunun çarpmaya göre tersi olacak şekilde gösterilebilir. Yukarıdaki ifadede $P_1(X)$ ve $P_2(X) \in Z_2[X]$'tir.

$a \leftrightarrow b$: a'nın b'ye, b'nin a'ya atanması anlamındadır (swap).

BÖLÜM 3

3. S- Kutularının Kriptografik Özellikleri

S-kutuları simetrik şifreleme algoritmalarının temel bileşenlerindendir. Blok şifreleme algoritmalarında karıştırma işlemi yapan elemandır. Şifreleme algoritmasında doğrusal olmayan tek eleman S-kutularıdır. Şifreleme algoritmasına yapılan saldırılardan doğrusal ve diferansiyel saldırılara karşı blok şifreleme algoritması güvenli kılmak için kriptografik özellikleri iyi olan S-kutuları seçilmelidir.

S-kutuları vektörel fonksiyonlar olarak ifade edilebilir ve $f_0, f_1, ..., f_{m-1}$ ile temsil edilebilir. f_i boole fonksiyonları F_2^n'den F_2'ye tanımlanır ve S-kutusunun çıkış fonksiyonları olarak isimlendirilir.

S-kutuları tasarlanırken aşağıdaki çeşitli yöntemler kullanılmaktadır [36]:

- Pseudo-random üretim
- Sonlu cisimde ters alma
- Sonlu cisimde üs alma tekniği
- Heuristic teknikler

Bu yöntemlerin en çok kullanılanları sonlu cisimde ters alma ve üssel fonksiyon tekniğidir. Nitekim AES algoritmasında kullanılan S-kutusu sonlu cisimde ters alma yöntemi ile oluşturulmuş bir S-kutusudur. Bu tezde sonlu cisimde üs alma tekniği ile tasarlanan 8 bit giriş ve 8 bit çıkışlı S-kutuları üzerine odaklanılmıştır. Buna ek olarak bu tez AES S-kutusunda olduğu gibi kriptografik özellikleri iyi ve AES S-kutusunun

cebirsel ifadesindeki terim sayısından daha fazla terim sayısına sahip olan üs haritalama tabanlı S-kutuları tasarımı üzerinedir.

Bir S-kutusunun kriptografik özellikleri statik özellikler ve dinamik özellikler başlıkları altında işlenebilir. Statik özellikler açık metin, şifreli metin ve anahtar arasındaki ilişkiler ile ilgilidir. Örneğin doğrusal olmaması bir statik özelliktir. S-kutusunun karakteristik yapısının saklandığı kriptografik özellikler dinamik olanlardır. S-kutuları için kriptografik özellikler aşağıdaki gibi sıralanabilir:

- Bütünlük (Completeness) kriteri,
- Çığ (Avalanche) kriteri,
- Katı çığ kriteri (Strict Avalanche Criterion),
- Bit bağımsızlık kriteri (Bit Independence Criterion),
- MOSAC ve MOBIC özellikleri,
- Doğrusal olmama kriteri,
- S-kutularının doğrusal yaklaşım tablosu,
- S-kutularının XOR tablosu (Fark Dağılım Tablosu),
- S-kutularında doğrusal eşitlik.

3.1 Bütünlük (Completeness) Kriteri

Kam ve Davida'nın tarafından belirlenmiştir [37]. S-kutuları vektörel bir fonksiyondur ve bir fonksiyonun bütünlük özelliği taşıması için gerekli olan kurallar aşağıdaki gibi olmalıdır.

$f:\{0,1\}^n \rightarrow \{0,1\}^n$ olsun. i ve j $\in \{1,2,....n\}$ olmak üzere f fonksiyonun en az bir tane $X \in \{0,1\}^n$ olmalı ki f(X) ve $f(X \oplus \Delta X_i)$ bir j de farklılaşıyorsa bütünlük özelliği sağlanmış olur. Kısacası her çıkış biti giriş bitlerinin tümüne bağlıdır.

Bir S-kutusunun çığ (avalanche) vektörü (3.1) denklemindeki gibidir. [38][39][40].

$$\begin{aligned}\Delta Y^{\Delta X_i} &= f(X) \oplus f(X \oplus \Delta X_i) \\ &= [a_1^{\Delta X_i}\ a_2^{\Delta X_i} \ldots\ldots\ldots a_n^{\Delta X_i}]\end{aligned} \tag{3.1}$$

$\Delta Y^{\Delta X_i}$, çığ vektörü, giriş şeridinden sadece bir biti (i. bit) değiştirilerek elde edilmiş fark şeridir. O zaman (3.2) ifadesi avalance vektöründeki toplam değişmeyi verecektir.

$$wt\,(a_j^{\Delta X_i}) = \sum_{\substack{\text{her X} \\ \text{için}}} a_j^{\Delta X_i} \tag{3.2}$$

(3.2) ifadesinin maksimum değeri 2^n dir. Dolayısıyla $0 \le wt(a_j^{\Delta X_i}) \le 2^n$ dir. ΔX_i vektörü (3.3) teki gibi ifade edilebilir.

$$\begin{aligned}\Delta X_1 &= [1,0,0,....,0] \\ \Delta X_2 &= [0,1,0,....,0] \\ &\vdots \\ \Delta X_n &= [0,0,0,....,1]\end{aligned} \tag{3.3}$$

Eğer $wt(a_j^{\Delta X_i}) = 0$ ise yani çıkış bitleri giriş bitlerinden etkilenmiyorsa bütünlük yoktur denir. Bunun yanında eğer $wt(a_j^{\Delta X_i}) = 2^n$ ise giriş bitinin değili alındığında çıkış bitinin doğrudan etkilendiği anlamına gelir ki bu da istenmeyen bir özelliktir. Bunun dışındaki tüm durumlar için S-kutusu bütünlük ölçütünü sağlayacaktır. Yani avalance vektöründeki toplam değişme (3.4) deki gibi olmalıdır.

$$0 < \frac{1}{2^n} wt(a_j^{\Delta X_i}) < 1 \tag{3.4}$$

3.2 Çığ (Avalanche) Kriteri

Çığ ölçütü (avalance criterion) (AVAL) Feistel [41] tarafından S-kutuları ve SPN tabanlı blok şifreler için tanımlanmıştır.

Bir $f:\{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu için giriş bitinin bir biti değiştiğinde çıkış bitlerinin yarısı değişecektir. Yani (3.2) deki avalance vektöründeki toplam değişme, i giriş ve j çıkış bitleri için $i, j \in \{0,1,2,..\}$ olmak üzere tüm i değerleri için (3.5) deki gibi olur ise AVAL [38][39][40] kriteri sağlanmış olur.

$$\frac{1}{2^n}\sum_{j=1}^{n} wt(a_j^{\Delta X_i}) = \frac{n}{2} \tag{3.5}$$

(3.5) ifadesini $k_{AVAL}(i)$ parametresini elde etmek için tekrar düzenlenir ise (3.6) ifadesi elde edilir.

$$k_{AVAL}(i) = \frac{1}{n.2^n}\sum_{j=1}^{n} wt(a_j^{\Delta X_i}) = \frac{1}{2} \tag{3.6}$$

(3.6) ifadesine göre $k_{AVAL}(i)$ parametresi [0,1] aralığında değerler almaktadır ve herhangi bir i değeri için $\frac{1}{2}$ değerinden farklı bir değer alırsa S-kutusu AVAL kriterini sağlamayacaktır.

3.3 Katı Çığ Kriteri (Strict Avalanche Criterion)

Webster ve Tavares [42] bütünlük ve çığ özelliklerini bileştirerek katı çığ özelliğini (Strict Avalanche Criterion) (SAC) tanımlamışlardır. Buna göre $f:\{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu için i ve j $\in$ {0, 1, 2,..., n) olmak üzere eğer giriş biti i'yi

değiştirmek çıkış biti j'nin kesinlikle $\frac{1}{2}$ olasılığında değişiyor ise SAC özelliği sağlanmaktadır. Matematiksel olarak tüm i ve j değerleri için (3.7) doğrulanır ise S-kutusunda katı çığ kriteri vardır denir [38][39][40].

$$\frac{1}{2^n} \mathrm{wt}(a_j^{\Delta X_i}) = \frac{1}{2} \tag{3.7}$$

(3.7) ifadesi (3.8) şeklinde değiştirilerek $k_{SAC}(i, j)$ tipinde bir SAC parametresi tanımlamak mümkündür.

$$k_{SAC}(i, j) = \frac{1}{2^n} \mathrm{wt}(a_j^{\Delta X_i}) \tag{3.8}$$

Eğer ki $k_{SAC}(i, j)$ parametresi [0,1] aralığında değerler alır ve herhangi bir (i, j) kombinasyonu için $\frac{1}{2}$ değerinden farklı ise o zaman S-kutusu SAC kriterini sağlamaz. İfadelerden de görülebileceği gibi S-kutusu çığ ve bütünlük kriterlerinin ikisini de sağlıyor ise o zaman SAC ölçütünü de sağlar demek mümkündür.

3.4 Bit Bağımsızlık Kriteri (Bit Independence Criterion)

Bit bağımsızlık ölçütü (Bit Independence Criterion - BIC) yine Webster ve Tavares [42] tarafından tanımlanmıştır.

$f : \{0,1\}^n \rightarrow \{0,1\}^n$ için $i, j, k \in \{1,2....n\}$ ve $j \neq k$ olmak üzere, tüm i, j, k parametreleri için, giriş biti i'nin tersini almak j ve k çıkış bitlerinin bağımsız olarak değişebiliyor ise BIC sağlanmıştır denir.

BIC değerini ölçmek için çığ verktörü ile j ve k bitleri arasındaki korelasyon katsayısı gereklidir. İki değişken (v,w) arasındaki korelasyon (3.9) ifadesi gibi hesaplanabilir

$$\mathrm{corr}(v,w) = \frac{E(vw) - E(v)E(w)}{\sqrt{(E(v^2) - E(v)^2)(E(w^2) - E(w)^2)}} \tag{3.9}$$

(3.10)'de E(v) ya da E(w) çığ vektörü v ya da w'nın ortalama değerini verecektir.

$$E(v) = \frac{1}{2^n} \sum_{\text{tüm X için}} v(X) \tag{3.10}$$

Bir S-kutusunun çığ vektöründeki bitler $\left[a_1^{\Delta X_i} a_2^{\Delta X_i} .....a_n^{\Delta X_i}\right]$ olmak üzere i. giriş bitinin çığ vektörünün j. ve k. bitlerindeki etkisi ile ilgili BIC parametresi (3.11) ile verilebilir.

$$BIC(a_j, a_k) = \left|\mathrm{corr}(a_j^{\Delta X_i}, a_k^{\Delta X_i}\right| \tag{3.11}$$

Eğer bir f fonksiyonu için BIC, bit bağımsızlık kriteri, düşünülürse tüm $1 \leq i, j, k \leq n$ için (3.12) ifadesi bize bunu verecektir.

$$BIC(f) = \max_{\substack{1\le i,j,k\le n \\ j\neq k}} BIC(a_j, a_k) = \max_{\substack{1\le i,j,k\le n \\ j\neq k}} \left|\mathrm{corr}(a_j^{\Delta X_i}, a_k^{\Delta X_i}\right| \tag{3.12}$$

Dolayısı ile BIC(f), [0,1] aralığında olmak üzere mümkün olabildiğince 0'a yakın olması gereklidir. Böylelikle $\Delta Y^{\Delta X_i}$ çığ vektörünün iki biti arasındaki korelasyon küçük olabilir. En kötü korelasyon değeri 1 dir ve bu da i giriş bitini değiştirildiğinde j. ve k. çıkış bitleri arasında maksimum korelasyona denk düşer [38] [39] [40].

Bütünlük, çığ, katı çığ gibi özelliklerin temsilini ve anlaşılmasını kolaylaştırmak amacı ile çığ vektörlerinin toplamı kullanılarak $n \times n$ boyutunda kare bir fark matrisi (D) oluşturulabilir. Bu matris (3.13) ve (3.14) de gösterilmektedir [39].

$$D = \frac{1}{2^n} \sum_{\text{tümXiçin}} \begin{bmatrix} \Delta Y^{\Delta X_1} \\ \Delta Y^{\Delta X_2} \\ ------ \\ \Delta Y^{\Delta X_n} \end{bmatrix} \tag{3.13}$$

$$D = \begin{bmatrix} d_{11} \; . \; . \; . \\ d_{21} \; . \; . \; . \\ . \quad . \quad . \quad . \\ . \quad . \quad . \; d_{nn} \end{bmatrix}_{nxn} \tag{3.14}$$

(3.14) ifadesindeki d_{ij} parametreleri ise (3.15) de belirtilmiştir.

$$d_{ij} = \frac{1}{2^n} wt(a_j^{\Delta X_i}) \quad (1 \le i, j, k \le n) \tag{3.15}$$

(3.15) ifadesindeki d_{ij} parametresinden faydalanarak $k_{SAC}(i,j)=d_{ij}$ ve $k_{AVAL}(i) = \sum_{j=1}^{n} d_{ij}$ olarak belirtilebilir. Buna benzer olarak çığ vektörünün j. ve k. bitleri için korelasyon katsayılarının oluşturacağı bir B matrisi (3.16) de gösterilmiştir. Bu matrise bit bağımsızlık parametreler matrisi adı verilir.

$$B = \begin{bmatrix} b_{1,12} \ldots . b_{1,1n} & b_{1,23} \ldots . b_{1,2n} & \ldots . & b_{1,(n-1)n} \\ b_{2,12} \ldots . b_{2,1n} & b_{2,23} \ldots . b_{2,2n} & \ldots . & b_{2,(n-1)n} \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots . & \ldots\ldots\ldots \\ b_{n,12} \ldots . b_{n,1n} & \ldots\ldots\ldots\ldots & \ldots . & b_{n,(n-1)n} \end{bmatrix}_{n \; x \binom{n}{2}} \tag{3.16}$$

B matrisinin indisleri (3.17) deki ifadeden bulunabilir.

$$b_{\substack{i,jk \\ 1 \le i,j,k \le n}} = BIC(a_j^{\Delta X_i}, a_k^{\Delta X_i}) \tag{3.17}$$

3.5 Doğrusal Olmama Kriteri

Doğrusal olmama (nonlinearity) S-kutuları için oldukça önemlidir. Şifrede kullanılan S-kutularının doğrusal olmaması istenir. Böylelikle açık metnin tahmini veya bulunması imkansız hale gelir.

Bir şifrenin doğrusal olmama parametresi $NLM_f(z)$'dir. $f : Z_2^n \rightarrow Z_2^m$ ve $z = (a,w,c) \in Z_2^{n+m+1}$ olmak üzere, tüm giriş değerleri için $P \in Z_2^n$ doğrusal fonksiyon $(w.P \oplus c)$ ve sıfır haricindeki doğrusal kombinasyonları $(a.f(P))$ birbirinden farklılaşması doğrusal olmama olarak tanımlanır. Burada $a \in Z_2^m, w \in Z_2^n$ ve $c \in Z_2$ dir. Buna göre doğrusal olmama ölçüsü, $NLM_f(z)$, (2.18) ve (2.19) deki gibi tanımlanabilir [38][43].

$$NLM_f(z) = \#\{P \mid a.f(P) \neq w.P \oplus c\} \tag{3.18}$$

$$NLM_f = \min_z NLM_f(z) \tag{3.19}$$

NLM_f değerinin alabileceği maksimum değer $2^{n-1} - 2^{\frac{n}{2}-1}$ dir. Şifrenin doğrusal olmaması ve doğrusal kriptanalize karşı başarılı olması için NLM_f değerinin bu maksimum değere yakın olması gerekir. NLM_f değerinin 0'a yakın olması istenmeyen bir özelliktir. Bu gibi durumlarda şifrenin doğrusal kriptanaliz ile kırılması olasıdır.

3.6 MOSAC ve MOBIC özellikleri

Eğer f fonksiyonunun bir ya da daha fazla giriş biti değiştiğinde çıkış biti $\frac{1}{2}$ olasılık ile değişiyor ise MOSAC (Maximum Order SAC) [44] [45] özelliği sağlanmış olur. (3.20) bu denkliği göstermektedir.

$$wt(a_j^{\Delta X}) = 2^{n-1} \quad \forall \Delta X \text{ ve } j. \tag{3.20}$$

(3.20) ye göre $\Delta X \neq (0,0,0,0....0)$ olmak üzere tüm ΔX vektörleri için çığ vektörü bitlerinin tümünün Hamming ağırlığının 2^{n-1} olması gerekir. MOBIC (Maximum Order BIC) ölçütü (3.21) ifadesi ile tanımlanabilir.

$$MOBIC(a_j, a_k) = \max_{\Delta X \in \{0,1\}^n, \neq \{0,....0\}} \left| corr(a_j^{\Delta X}, a_k^{\Delta X}) \right| \tag{3.21}$$

Bir f fonksiyonunun maksimum dereceden bit bağımsızlığı aynı çıkış bitleri haricindeki $MOBIC(a_{j,} a_k)$ değerlerinin maksimumudur. Bu ifade de (3.22) de gösterilmektedir.

$$MOBIC(f) = \max_{j \neq k} MOBIC(a_j, a_k) \tag{3.22}$$

MOBIC ölçütünü sağlayan f fonksiyonu için MOBIC(f) = 0 olması gerekmektedir.

3.7 Doğrusal Yaklaşım Tablosu

Doğrusal yaklaşım tablosu (Lineer Approximation Table) (LAT) [46] [47] [48] doğrusal kriptanalize karşı S-kutularının gücünü test etmeye yarayan önemli bir ölçüttür. Şifreleme algoritması için doğrusal yaklaşım tablosunda bulunan maksimum değerin küçük olması doğrusal saldırıların başarımını zorlaştıracaktır.

$S : GF(2^n) \rightarrow GF(2^n)$ 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 $N_L(\Gamma_a, \Gamma_b)$, 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 (3.23) ifadesindeki gibi gösterilebilir [42]. S için (3.23) de Γ_a ve Γ_b değerleri sırasıyla giriş maskesi ve çıkış maskesi olarak isimlendirilir. (3.24)'te herhangi bir giriş ve çıkış maskesi değerine göre LAT tablosu değerinin nasıl elde edileceği verilmiştir.

$$N_L(\Gamma_a,\Gamma_b) = \#\left\{x \in GF(2^n) \mid \Gamma_a \bullet x = \Gamma_b \bullet S(x)\right\}^2 \tag{3.23}$$

$$LAT(\Gamma_a,\Gamma_b) = \#\left\{x \in GF(2^n) \mid \Gamma_a \bullet x = \Gamma_b \bullet S(x)\right\} - 2^{n-1} \tag{3.24}$$

Diğer yandan bir S-kutusu için doğrusal olmama ölçüsü NLM_S değeri LAT değeri ile ilişkili olarak (3.25)'te verilmiştir.

$$NLM_S = 2^{n-1} - \text{maks}\left|LAT_S(\Gamma_a,\Gamma_b)\right| \tag{3.25}$$

Örnek 3.1 Tablo 3.1 de 4 × 4 boyutunda bir S-kutusu gözükmektedir. Bu S-kutusu $X^4 + X + 1$ indirgenemez polinomu ve $X \to X^7$ üs haritalama fonksiyonu ile üretilmiştir. S-kutusunun doğrusal yaklaşım tablosu Tablo 3.2 deki gibi olacaktır.

Hex Giriş	0 0000	1 0001	2 0010	3 0011	4 0100	5 0101	6 0110	7 0111	8 1000	9 1001	A 1010	B 1011	C 1100	D 1101	E 1110	F 1111
Çıkış Hex	0011 3	1101 D	1010 A	0010 2	0001 1	0111 7	1011 B	0101 5	1100 C	1110 E	1111 F	0110 6	1001 9	1000 8	0000 0	0100 4

Tablo 3.1 4 × 4 Boyutundaki Bir S-kutusu

[2] $x \bullet y$ nokta ürün olarak isimlendirilir, $\#\psi$: Set ψ'deki eleman sayısını ifade eder.

Giriş Maskesi (Γ_a) \ Çıkış Maskesi (Γ_b)	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	-2	0	2	4	-2	0	-2	-2	0	2	0	2	0	2	4
2	0	-2	2	0	0	-2	2	0	-2	-4	-4	2	2	0	0	-2
3	0	0	2	-2	0	-4	-2	-2	4	0	-2	-2	0	0	-2	2
4	0	2	-4	-2	-2	0	-2	0	-2	0	-2	0	4	-2	0	2
5	0	0	0	4	-2	2	-2	-2	0	-4	0	0	-2	-2	-2	2
6	0	0	2	2	-2	-2	-4	4	0	0	2	2	2	2	0	0
7	0	2	-2	4	2	0	0	2	2	0	-4	-2	0	2	2	0
8	0	-4	-2	-2	2	2	-4	0	2	-2	0	0	0	0	2	-2
9	0	2	-2	0	2	-4	0	2	0	-2	2	0	-2	-4	0	-2
A	0	-2	0	2	-2	0	2	0	4	2	0	2	2	-4	2	0
B	0	0	0	0	2	2	2	2	2	-2	2	-2	4	0	-4	0
C	0	2	2	0	4	2	-2	0	0	2	-2	4	0	-2	-2	0
D	0	0	-2	-2	0	0	2	2	2	-2	0	4	-2	2	0	4
E	0	-4	0	0	0	0	0	4	-2	2	-2	-2	-2	-2	-2	2
F	0	-2	-4	2	0	-2	0	-2	0	2	0	2	0	2	-4	-2

Tablo 3.2 Doğrusal Yaklaşım Tablosu (LAT)

Örnek olarak LAT(7,C) değerinin elde edilişi aşağıda gösterilmektedir.

$(0111)\cdot(0000) = (1100)\cdot(0011) \rightarrow 0=0$ *
$(0111)\cdot(0001) = (1100)\cdot(1101) \rightarrow 1\neq 0$
$(0111)\cdot(0010) = (1100)\cdot(1010) \rightarrow 1=1$ *
$(0111)\cdot(0011) = (1100)\cdot(0010) \rightarrow 0=0$ *
$(0111)\cdot(0100) = (1100)\cdot(0001) \rightarrow 1\neq 0$
$(0111)\cdot(0101) = (1100)\cdot(0111) \rightarrow 0\neq 1$
$(0111)\cdot(0110) = (1100)\cdot(1011) \rightarrow 0\neq 1$
$(0111)\cdot(0111) = (1100)\cdot(0101) \rightarrow 1=1$ *
$(0111)\cdot(1000) = (1100)\cdot(1100) \rightarrow 0=0$ *
$(0111)\cdot(1001) = (1100)\cdot(1110) \rightarrow 1\neq 0$
$(0111)\cdot(1010) = (1100)\cdot(1111) \rightarrow 1\neq 0$
$(0111)\cdot(1011) = (1100)\cdot(0110) \rightarrow 0\neq 1$
$(0111)\cdot(1100) = (1100)\cdot(1001) \rightarrow 1=1$ *
$(0111)\cdot(1101) = (1100)\cdot(1000) \rightarrow 0\neq 1$
$(0111)\cdot(1110) = (1100)\cdot(0000) \rightarrow 0=0$ *
$(0111)\cdot(1111) = (1100)\cdot(0100) \rightarrow 1=1$ *

(3.23) ifadesine göre LAT(7,C) için eşitliği sağlayan (* ile işaretlenmiş olanlar) 8 değer bulunmaktadır. (3.24) teki ifadeyi kullanarak $\mathrm{LAT}(7,C) = 8 - 2^{4-1} = 8 - 8 = 0$

şeklinde elde edilir. S-kutusunun (3.25) ifadesine göre NLM_S değeri ise tüm LAT elemanlarının en büyük mutlak değeri göz önüne alınarak $NLM_S = 2^{4-1} - 4 = 4$ şeklinde elde edilir.

3.8 Fark Dağılım Tablosu (Difference Distribution Table)

Diferansiyel kriptanaliz bir blok şifreleme algoritmasına karşı kullanılan bir saldırı yöntemidir [25]. S-kutularının fark dağılım tablosu (XOR tablosu veya DDT) bu saldırıya karşı şifrenin gücü ile ilgili fikirler vermektedir. n × m boyutunda bir S-kutusu için XOR tablosu [25] [48] $2^n \times 2^m$ matrise denk düşer.

$S : GF(2^n) \to GF(2^n)$ olmak üzere n bit giriş ve n bit çıkışa sahip bir S-kutusu olmak üzere herhangi verilen $a, b \in GF(2^n)$ için $XOR(a,b)$, herhangi $a \setminus 0$ ve b için $S(x) + S(x+a) = b$ denklemindeki b değerlerinin sayısını tanımlar ve (3.26)'daki gibi gösterilebilir [49]. S için denklem (3.26) da a ve b değerleri sırasıyla giriş farkı ve çıkış farkı olarak isimlendirilir.

$$XOR(a,b) = \#\left\{x \in GF(2^n) \mid S(x) + S(x+a) = b\right\} \tag{3.26}$$

GF(q), q elemanlı sonlu bir cisim ve q, p^n olacak şekilde asal bir sayının üssü olmak üzere, $f : GF(q) \to GF(q)$ olan fonksiyonlar ele alınsın. $a, b \in GF(q)$ olmak üzere (3.27) ile hesaplanan $\nabla_f(q)$ değeri q değerinden az ise fonksiyon için doğrusal değildir denir.

$$\nabla_f(q) = maks\left\{XOR(a,b) : a, b \in GF(q), a \neq 0\right\} \tag{3.27}$$

Örnek 3.2: Örnek 3.1 de kullanılan S-kutusunun XOR tablosu Tablo 3.3 teki gibidir.

		Çıkış Farkı (b)															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Giriş Farkı (a)	**0**	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
	2	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
	3	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
	4	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
	5	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
	6	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
	7	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
	8	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
	9	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
	A	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
	B	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
	C	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0
	D	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
	E	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
	F	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0

Tablo 3.3 Fark Dağılım Tablosu (XOR tablosu)

(3.26) ifadesi gereği elde edilen $XOR_S(8,F) = 4$ aşağıda verilmektedir.

$S(0) \oplus S(8) = 3 \oplus C \rightarrow F$ *
$S(1) \oplus S(9) = D \oplus E \rightarrow 3$
$S(2) \oplus S(A) = A \oplus F \rightarrow 5$
$S(3) \oplus S(B) = 2 \oplus 6 \rightarrow 4$
$S(4) \oplus S(C) = 1 \oplus 9 \rightarrow 8$
$S(5) \oplus S(D) = 7 \oplus 8 \rightarrow F$ *
$S(6) \oplus S(E) = B \oplus 0 \rightarrow B$
$S(7) \oplus S(F) = 5 \oplus 4 \rightarrow 1$
$S(8) \oplus S(0) = C \oplus 3 \rightarrow F$ *
$S(9) \oplus S(1) = E \oplus D \rightarrow 3$
$S(A) \oplus S(2) = F \oplus A \rightarrow 5$
$S(B) \oplus S(3) = 6 \oplus 2 \rightarrow 4$
$S(C) \oplus S(4) = 9 \oplus 1 \rightarrow 8$
$S(D) \oplus S(5) = 8 \oplus 7 \rightarrow F$ *
$S(E) \oplus S(6) = 0 \oplus B \rightarrow B$
$S(F) \oplus S(7) = 4 \oplus 5 \rightarrow 1$

Yukarıdaki işlemlerden de görüldüğü gibi $S(x) + S(x+8) = F$ eşitliğini sağlayan (* ile işaretli olanlar) 4 durum vardır.

BÖLÜM 4

4. Üs Haritalama Tabanlı S-kutularının Sınıflandırılması

Üs haritalama yöntemi ile doğrusal olmama ölçüsü yüksek ve diğer kriptografik özellikleri iyi S-kutuları elde edilebilir. Bu bölümün sonlarına doğru 8 bitlik S-kutuları bazı kriterlere göre sınıflandırılacak ve bu sınıflar hakkında çeşitli değerlendirmeler yapılacaktır.

Cebirsel Hazırlık

Tanım 4.1. $f(x) = x^d$ fonksiyonu $GF(p^n)$ üzerine bir fonksiyon olsun. $\nabla_f = 2$ şeklindeki haritalara APN (Almost Perfect Nonlinear- Hemen Hemen Kusursuz Doğrusal Olmayan) denir.

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. Bu alanda yapılan ve literatürde yer alan çeşitli çalışmalar [50][51][52][53][54][55][56] şeklinde verilebilir. Bu tezde $GF(2^8)$'de üs fonksiyonlarının sınıflandırılması yapılacağından dolayı $p = 2$ olacak şekilde düşünülmektedir. Bu fonksiyonlar diferansiyel kriptanalize karşı simetrik şifre tasarımında dayanıklılık sundukları için özel ilgi gösterilen fonksiyonlardır.

Diğer yandan bijektif (birebir ve örten) S-kutuları her ne kadar zorunlu olmasa da kriptografik özellikleri için tercih edilen S-kutularıdır. Ancak fonksiyon $X \to X^d$, $OBEB(d, 2^n - 1) = 1$ 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. Nitekim AES şifresinin tasarımcıları byte yapısındaki şifre tasarım felsefesinden ödün vermeden Nyberg'in [14] önerdiği ters haritalama tabanlı ve APN fonksiyon dağılımına yakın sonuç veren S-kutusunu şifrelerinde kullanmışlardır. Bilinen bazı APN fonksiyonları Tablo 4.1 ve Tablo 4.2'de gösterilmektedir.

Fonksiyonun Adı	d	Ref.
Gold fonksiyonu	$2^i+1 \Rightarrow (i,n)=1, 1\le i\le m$	[50][51]
Kasami fonksiyonu	$2^{2i}-2^i+1 \Rightarrow (i,n)=1, 2\le i\le m$	[52]
Ters alma	2^n-2	[14]
Welch fonksiyonu	2^m+3	[53][54]
Niho fonksiyonu	m tek ise $\Rightarrow 2^m+2^{m/2}-1$ m çift ise $\Rightarrow 2^m+2^{(3m+1)/2}-1$	[54]
Dobbertin fonksiyonu	Eğer $n=2m \Rightarrow 2^{4i}+2^{3i}+2^{2i}+2^i-1$	[55]

Tablo 4.1 $n=2m+1$ olmak üzere $GF(2^n)$ de bilinen X^d haritalamasına göre bilinen APN fonksiyonları

Fonksiyonun Adı	d	Ref.
Gold fonksiyonu	$2^i+1 \Rightarrow (i,n)=1, 1\le i\le m$	[51]
Kasami fonksiyonu	$2^{2i}-2^i+1 \Rightarrow (i,n)=1, 2\le i\le m$	[52]
Dobbertin fonksiyonu	Eğer $n=5i \Rightarrow 2^{4i}+2^{3i}+2^{2i}+2^i-1$	[55]

Tablo 4.2 $n=2m$ olmak üzere $GF(2^n)$ de bilinen X^d haritalamasına göre bilinen APN fonksiyonları

Tanım 4.2. $a,b \in GF(p^n)$ 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 [56]. Dolayısı ile f ve g fonksiyonları ile oluşturulmuş S-kutularının fark dağılım tablosu aynı ise bu S-kutuları denktir.

Tanım 4.3. Bir tamsayı d 'i içeren mod N 'e göre cyclotomic koset

$$C_d = \{d, dp, ..., dp^{n-1}\} \pmod{N} \tag{4.1}$$

şeklinde bir settir ve d $dp^n \equiv d \pmod{N}$ olacak şekilde en küçük tamsayıdır [57].

Teorem 4.1. $f(x) = x^d$ fonksiyonu için cyclotomic koset üzerindeki $XOR(a,b)$ sabittir [56].

$$\begin{aligned} &\{dp^i : i = 0,1,..., n-1\} \\ &(XOR_{dp^i}(a,b) = XOR(a,b) \quad i = 0,1,..., n-1 \text{ için}) \end{aligned} \tag{4.2}$$

İspat.

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

Teorem 4.2. $a \neq 0$ için $XOR(a,b) = XOR(1, ba^{-d})$ dir [56].

Önerme 4.1. $x \in GF(2^n)$ ve n çift olmak üzere $GF(2^n)$ cisminde ters haritalama işlemi $f(x) = x^{-1}$, $f(0) = 0$ fark dağılımına göre 4 uniformdur [14].

Önerme 4.2. $x \in GF(2^n)$ 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 4.1'e göre $(x^{2^n-2})^{2^i \bmod(2^n-1)}$ fonksiyonuda Önerme 4.1 deki gibi aynı fark dağılımını verecektir. Dolayısıyla

$$(x^{2^n-2})^{2^i \bmod(2^n-1)} = (x^{2^n-1-1})^{2^i \bmod(2^n-1)} = x^{(-2^i)\bmod(2^n-1)} \tag{4.3}$$

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

Teorem 4.2'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 4.1 gereği $GF(2^8)$ de ters haritalama işlemi ya da $X \to X^{254}$ üs haritalama işlemi 4 uniform dağılım göstermektedir. Teorem 4.1, Önerme 4.1 ve Önerme 4.2 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 fonksiyonları ile tasarlanan S-kutuları da aynı kriptografik özellikleri barındıracaklardır. Yani bu üs haritalama yöntemi ile tasarlanacak S-kutuları fark dağılım tablosu açısından 4 uniform dağılım göstereceklerdir. Bu üs haritalama fonksiyonları aynı cyclotomic kosette olduklarından denk fonksiyonlardır ve aynı sınıfa incelenebilir [58][59].

Bu bölümde $GF(2^8) \to GF(2^8)$ şeklindeki cebirsel haritalamalar için üs fonksiyonları incelenmiştir. Bunun için bir indirgenemez polinom seçilmelidir. Çalışmada kullanılan indirgenemez polinom AES S-kutusunun kullandığı $x^8 + x^4 + x^3 + x + 1$ polinomudur. Bu polinomun α kökü ilkel eleman olmadığı için yani bütün sonlu cisim elemanlarını üretmediği için $\beta = \alpha + 1$ ilkel elemanı kullanılarak (4.4) ifadesindeki gibi cismin elemanları elde edilmiştir. Elde edilen cismin elemanları EK A'da üretilen S-kutuları ise EK B'de verilmiştir.

$$(\beta^1 = "03", \beta^2 = "05", ..., \beta^{254} = "F6", \beta^{255} = "01") \quad (4.4)$$

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)

Tablo 4.3: Tek satır DDT ve LAT dağılımlarına göre $GF(2^8)$ de tüm üs fonksiyonlarının sınıflandırılması.

Tezde, üretilen cisim ve Tablo 4.3'teki sınıflardan herhangi bir üs fonksiyonu kullanılarak S-kutusu oluşturulmuştur. Oluşturulan S-kutusunun DDT ve LAT değerlerinin herhangi bir satırının dağılımları elde edilmiştir ve buna göre Tablo 4.3 oluşturulmuştur.

Tablo 4.3'te ∇_S, $|N_{Lmaks}|$ olarak belirtilen doğrusal yaklaşım tablosunun maksimum mutlak değeri ve doğrusal olmama değeri yani NLM_S bütün sınıflar için hesaplanarak gösterilmektedir

Tablo 4.3'te belirtilen sınıflardan 3, 9, 39, 5, 21, 95, 111, 25, 63, 55, 15, 45, 27, 85 olanları bijektif S-kutuları değildir. Yani $\gcd(d,2^8-1)\neq 1$. Bunun yanında 3 (Gold), 9 (Gold) , 39 (Kasami) sınıfları APN fonksiyonlardır. 5, 21, 95 ve 127 sınıfları diferansiyel fark dağılımı için 4 uniformdur. Ancak bunlardan 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 olmayan diğer bir sınıf olan 63, 156 tane 0, 86 tane 2 ve 14 tane 6 içermektedir.

$S: GF(2^n) \rightarrow GF(2^n)$ şeklindeki bir S-kutusu için maksimum doğrusal olmama değeri NLM_{Smaks} değeri $2^n - 2^{\frac{n}{2}-1}$ (n çift) olarak daha önce verilmişti. Dolayısıyla herhangi bir S-kutusu için elde edilecek NLM_S değerinin NLM_{Smax} değerine oranı yüzde olarak o S-kutusunun doğrusal olmama değerini verecektir. Tablo 4.3'te % değerleri bu şekilde elde edilmiştir.

Tablo 4.3 oluşturulurken, sınıfların fark dağılımları göz önüne alınmıştır. Buna göre Tablo 4.4'te sınıfların bir satır için DDT dağılımları gösterilmektedir. Teorem 4.1'e göre aynı cyclotomic kosette bulunan sınıfların dağılımlarının değerleri aynı olacaktır.

d (Sınıf)	x değerlerinin sayısı																		
-	0	2	4	6	10	12	14	16	18	22	24	26	28	30	50	52	60	84	256
3	128	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	128	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	128	128	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	192	0	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	152	80	24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	156	72	28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
111	140	104	12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
127	129	126	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	157	84	1	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	172	48	28	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	157	84	1	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	156	86	0	14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	165	66	21	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	165	66	21	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	149	102	1	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0
55	152	96	4	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0
59	149	102	1	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0
15	134	121	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
45	134	121	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
17	240	0	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0	0	0
19	159	72	24	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
23	165	60	30	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
31	135	120	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
47	159	72	24	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
53	155	96	0	0	0	4	0	1	0	0	0	0	0	0	0	0	0	0	0
61	165	60	30	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0

Tablo 4.4: Sınıfların DDT dağılımları

Tablo 4.4'e benzer olarak sınıfların LAT dağılımları incelenmiştir. Buna göre üretilen S-kutularının LAT dağılımları Tablo 4.5'te verilmektedir.

d	|x| değerlerinin sayısı														
(Sınıf)	|0|	|2|	|4|	|6|	|8|	|10|	|12|	|14|	|16|	|20|	|24|	|32|	|40|	|48|	|128|
3	65	0	0	0	170	0	0	0	21	0	0	0	0	0	0
9	65	0	0	0	170	0	0	0	21	0	0	0	0	0	0
39	65	0	0	0	170	0	0	0	21	0	0	0	0	0	0
5	49	0	0	0	204	0	0	0	0	0	0	3	0	0	0
21	113	0	0	0	106	0	0	0	37	0	0	0	0	0	0
95	62	0	96	0	36	0	32	0	30	0	0	0	0	0	0
111	49	0	88	0	58	0	40	0	21	0	0	0	0	0	0
127	17	48	36	40	34	24	36	16	5	0	0	0	0	0	0
7	105	0	0	0	120	0	0	0	30	0	0	1	0	0	0
25	115	0	0	0	108	0	0	0	32	0	0	1	0	0	0
37	105	0	0	0	120	0	0	0	30	0	0	1	0	0	0
63	41	0	104	0	72	0	16	0	13	8	2	0	0	0	0
11	101	0	0	0	132	0	0	0	18	0	4	1	0	0	0
29	165	66	21	0	0	4	0	0	0	0	0	0	0	0	0
13	101	0	0	0	132	0	0	0	18	0	4	1	0	0	0
55	99	0	0	0	136	0	0	0	16	0	4	1	0	0	0
59	101	0	0	0	132	0	0	0	18	0	4	1	0	0	0
15	1	0	24	84	85	52	10	0	0	0	0	0	0	0	0
45	1	0	24	84	85	52	10	0	0	0	0	0	0	0	0
17	16	0	0	0	240	0	0	0	0	0	0	0	0	0	0
19	88	0	0	0	152	0	0	0	8	0	8	0	0	0	0
23	90	0	0	0	144	0	0	0	20	0	0	2	0	0	0
31	120	0	0	0	96	0	0	0	40	0	0	0	0	0	0
47	88	0	0	0	152	0	0	0	8	0	8	0	0	0	0
53	60	0	0	0	192	0	0	0	0	0	0	4	0	0	0
61	90	0	0	0	144	0	0	0	20	0	0	2	0	0	0
91	120	0	0	0	96	0	0	0	40	0	0	0	0	0	0
119	16	0	128	0	80	0	0	0	32	0	0	0	0	0	0
27	117	0	0	0	118	0	0	0	16	0	4	0	0	1	0
43	109	0	0	0	136	0	0	0	8	0	0	1	0	2	0
87	109	0	0	0	136	0	0	0	8	0	0	0	2	1	0
51	16	0	64	96	0	64	16	0	0	0	0	0	0	0	0
85	64	0	0	128	0	64	0	0	0	0	0	0	0	0	0
1	255	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Tablo 4.5: Sınıfların LAT dağılımları

3, 9, 39 APN fakat bijektif olmayan fonksiyonlar için bir satır LAT dağılımı aynıdır. Yani 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 tanedir. 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.

Elde edilen sınıflar içerisinde kriptografik özellikler açısından en iyi sonuçları veren fonksiyonların APN fonksiyonlar olduğu söylenebilir. Bu fonksiyonlar 2 uniform dağılıma sahiptirler. Diğer yandan bijektif S-kutuları açısından ise 127 sınıfı her iki kriptografik özellik açısından iyi sonuçlar vermektedir. 127 sınıfına dahil olan 254 haritalaması AES S-kutusu tasarımında kullanılmıştır. 4 uniform bir dağılıma sahiptir. Doğrusal olmama oranı % 93'tür. Dikkat edilir ise APN fonksiyonların bulunduğu sınıfların da % 93 oranda doğrusal olmadığı görülebilir. Bunların yanında 7 ve 37 sınıfları da kriptografik özellikler açısından kötü sonuçlar vermemektedir. Dolayısı ile bir şifre için gerekli S-kutusu tasarımında kullanılabilirler.

BÖLÜM 5

5. S-kutularının Cebirsel Olarak İncelenmesi

F_2^n'de bir f boole fonksiyonunu cebirsel olarak temsil etmek için iki yöntem kullanılabilir. Bunlardan biri cebirsel gösterim biçimi (Algebraic Normal Form-ANF) diğeri polinomsal gösterimdir. Tezin ilerleyen kısmında S-kutuları incelenirken polinomsal gösterim yöntemi tercih edilmiştir.

5.1. Cebirsel gösterim biçimi (Algebraic Normal Form - ANF)

F_2^n'de bir f boole fonksiyonunu temsil etmek için cebirsel gösterim biçimi kullanılabilir. Aşağıdaki gibi gösterilebilir [60] [61].

$$f(x) = f(x_1, x_2, ..., x_n) = \sum_{u \in F_2^n} a_u \left(\prod_{i=1}^{n} x^{u_i} \right) = \sum_{u \in F_2^n} a_u x^u \; ; \quad a_u \in F_2$$
$$= a_0 \oplus a_1 x_1 \oplus ... \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus ... \oplus a_{(n-1)n} x_{(n-1)} x_n \qquad (5.1)$$
$$\oplus a_{123} x_1 x_2 x_3 \oplus ... \oplus a_{123...n} x_1 x_2 x_3 ... x_n$$

Algoritma 5.1: ANF Algoritması [61]

1. $g(x_1, ..., x_n) = f(0, 0, .., 0)$ değerini ata.
2. $k = 1$ den $2^n - 1$ değerine kadar, yap.

   a- Tamsayı k'nın ikili temsilini kullan. $(k = b_1 + b_2 2 + b_3 2^2 + ... + b_n 2^{n-1})$

   b- Eğer $g(b_1, b_2, ..., b_n) \neq f(b_1, b_2, ..., b_n)$ ise

   $g(x_1, ..., x_n) = g(x_1, ..., x_n) \oplus \prod_{i=1}^{n} (x_i)^{b_i}$ değerini ata.
3. $ANF(f) = g(x_1, ..., x_n)$.

Örnek 5.1: Bir boole fonksiyonu olan $f(x_3, x_2, x_1) = \{0,0,1,0,1,1,0,1\}$ için Algoritma 2.1 de gösterildiği gibi ANF gösteriminin elde edilmesini adım adım gösterimi aşağıdaki gibidir.

k	**b_3**	**b_2**	**b_1**	**$f(b_1, b_2, b_3)$**	**$g(b_1, b_2, b_3)$**
	0	0	0	0	0
1	0	0	1	0	0
2	0	1	0	1	x_2
3	0	1	1	0	$x_2 \oplus x_1x_2$
4	1	0	0	1	$x_2 \oplus x_1x_2 \oplus x_3$
5	1	0	1	1	$x_2 \oplus x_1x_2 \oplus x_3$
6	1	1	0	0	$x_2 \oplus x_1x_2 \oplus x_3$
7	1	1	1	1	$x_2 \oplus x_1x_2 \oplus x_3$

Örnek 5.2: $f(X) = X^3 + X + 1$ polinomu kullanılarak $GF(2^3)$ te $g : X \to X^{-1}$ haritalamasını aşağıdaki gibi oluşturulabilir.

Bu cismin üreteci $\beta = 010 = \alpha$ dır dolayısı ile cisim aşağıdaki gibi üretilebilir.

k	β^k
0	$\beta^0 = 001 = 1$
1	$\beta^1 = 010 = \alpha$
2	$\beta^2 = 100 = \alpha^2$
3	$\beta^3 = 011 = \alpha + 1$
4	$\beta^4 = 110 = \alpha^2 + \alpha$
5	$\beta^5 = 111 = \alpha^2 + \alpha + 1$
6	$\beta^6 = 101 = \alpha^2 + 1$
7	$\beta^7 = 001 = 1$

Bu cisme göre $X \to X^{-1}$ haritalama fonksiyon tablosu aşağıdaki gibi gösterilebilir

X				X^{-1}		
x_3	x_2	x_1		f_3	f_2	f_1
0	0	0	$\to$	0	0	0
0	0	1	$\to$	0	0	1
0	1	0	$\to$	1	0	1
0	1	1	$\to$	1	1	0
1	0	0	$\to$	1	1	1
1	0	1	$\to$	0	1	0
1	1	0	$\to$	0	1	1
1	1	1	$\to$	1	0	0

ANF algoritması kullanılarak X^{-1} haritalaması çıkışındaki f_1 koordinatının ANF formundaki cebirsel açılımı aşağıdaki tabloda gösterildiği gibi elde edilebilir.

k	b_3 x_3	b_2 x_2	b_1 x_1	$f = (b_{1,} b_{2,}, b_3)$	$g = (x_1, x_2, x_3)$
0	0	0	0	0	0
1	0	0	1	1	x_1
2	0	1	0	1	$x_1 \oplus x_2$
3	0	1	1	0	$x_1 \oplus x_2$
4	1	0	0	1	$x_1 \oplus x_2 \oplus x_3$
5	1	0	1	0	$x_1 \oplus x_2 \oplus x_3$
6	1	1	0	1	$x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3$
7	1	1	1	0	$x_1 \oplus x_2 \oplus x_3 \oplus x_2 x_3$

5.2. Cebirsel derece (Algebraic Degree)

Bir f boole fonksiyonunun cebirsel derecesi deg(f) ya da kısaca d ile tanımlanır. f boole fonksiyonunun ANF formundaki $x_0^{a0} \ldots x_{n-1}^{a_{n-1}}$ terimlerinden değişken sayısı maksimum olan değer f boole fonksiyonunun cebirsel derecesidir.

Örnek 5.3: $f(x_3, x_2, x_1) = x_1 \oplus x_1x_2 \oplus x_1x_2x_3$ boole fonksiyonunun cebirsel derecesi 3'tür.

5.3. Cebirsel dayanıklılık (Algebraic Immunity)

İki boole fonksiyonunun, f, g den elde edilen boole fonksiyonunun doğruluk tablolarının ürünü $f.g$ (iki vektör arasında elde edilen nokta ürünü değil) ile temsil edilsin. F_2^n üzerinde tanımlanmış bir boole fonksiyonunun cebirsel dayanıklılığı (Algebraic Immunity) (AI) $f.g = \overline{0} = (0,0,...,0)$ ya da $(f \oplus \overline{1}).g = \overline{0}$ yapan F_2^n den F_2 ye tanımlı g fonksiyonunun en düşük derecesidir. $f.g = \overline{0} = (0,0,...,0)$ olacak şekilde fonksiyon g'ye f'in bir bozucusu (annihilator) denir. $An(f)$, f'in tüm bozucularının setini tanımlar [60] [61] [62].

Örnek 5.4: Fonksiyon $f(x) = f(x_3, x_2, x_1) = \{0,0,0,1,1,1,0,1\}$ şeklindeki boole fonksiyonunun $An(f)$ fonksiyonu aşağıda gösterilmiştir. "$*$" yerine istenen 0 ya da 1 değeri konabilir.

x_3	x_2	x_1	f (x)	an (f)
0	0	0	0	*
0	0	1	0	*
0	1	0	0	*
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	0	*
1	1	1	1	0

Tanım 5.1: Bir $f(x)$ boole fonksiyonu eğer $f(x) = x \bullet w \oplus c$ formunda temsil ediliyorsa bu fonksiyona affine fonksiyonu denir. Ayrıca $c = 0$ ise $f(x)$ boole fonksiyonu

doğrusaldır denir. $x \bullet w = \bigoplus_{i=1}^{n} x_i.w_i = x_1.w_1 \oplus x_2.w_2 \oplus .....\oplus x_n.w_n$ nokta ürünü $x, w \in F_2^n$ olmak üzere ikili değere sahip vektörleri ile tanımlanır.

Tanım 5.2: {0,1} lerden oluşan vektör sıranın Hamming ağırlığı wt(α) = α'daki 1'lerin sayısını temsil eder.

Tanım 5.3: $f(x), g(x): F_2^n \to F_2$ iki boole fonksiyon olmak üzere bu fonksiyonların arasındaki Hamming uzaklığı $d_H(f,g), (f(x) \oplus g(x))$'in doğruluk tablosunun Hamming ağırlığı olarak tanımlanır. Diğer bir deyişle Hamming uzaklığı aşağıdaki gibi tanımlanabilir.

$$d(f,g) = \sum_{x \in F_2^n} f(x) \oplus g(x) = 2^{n-1} - \frac{1}{2} \sum_{x \in F_2^n} \hat{f}(x)\hat{g}(x) \qquad (5.2)$$

Bir boole fonksiyonunun Hamming ağırlığı ise f_0 sabit sıfır fonksiyonuna olan uzaklık olarak tanımlanır. Hamming ağırlığı $w_h(x) = \#\{i \mid x_i \neq 0\}$ şeklinde gösterilebilir.

5.4. Polinomsal Gösterim

Tezin devamında S-kutuları polinomsal gösterim biçimi ile temsil edileceklerdir. Bunun için α, $GF(2^n)$ sonlu cismini üretmek için kullanılan ilkel eleman olmak üzere;

$$b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + ... + b_0 \ , \ b_i \in \{0,1\} \qquad (5.3)$$

sonlu cisim elemanı $(b_{n-1}, b_{n-2}, ..., b_0)$ bitlerini içeren hexadecimal sayı olarak temsil edilebilir. Dolayısı ile bir S-kutusu katsayıları hexadecimal sayılar olmak üzere cebirsel bir ifade şeklinde yazılarak ifade edilebilir.

5.4. İz (Trace) Fonksiyonu

$F = GF(p)$, $K = GF(p^n)$ ve $\lambda \in K$ olsun. O zaman alt cisim F'in λ'ya göre trace (iz) fonksiyonu

$$Tr_F^K(\lambda) = \lambda + \lambda^p + \lambda^{p^2} + ... + \lambda^{p^{n-1}} \tag{5.4}$$

şeklinde ifade edilebilir ve karışıklığın olmayacağı durumlarda Tr_F^K ifadesindeki alt ve üst indisler göz ardı edilebilir.

Trace fonksiyonu kullanarak aşağıda verilen tanımlar ile cebirsel bir S-kutusunun (sonlu cisimde ters alma ya da sonlu cisimde üs haritalama tabanlı) cebirsel ifadesi elde edilebilir.

$\{\alpha_0 ..... \alpha_{n-1}\}$, $GF(2)$ üzerine $GF(2^n)$'in herhangi bir tabanı olmak üzere; $\{\beta_0 ..... \beta_{n-1}\}$ buna karşı gelen dual taban ve $f(x_0, x_1, ..., x_{n-1}) = (f_0(x), ..., f_{n-1}(x))$ ise $GF(2^n)$ üzerine bir permütasyon olsun. O zaman $g(x) = \sum_{i=0}^{n-1} \alpha_i f_i(x_0, ...x_{n-1})$ de $GF(2^n)$ üzerine bijektif bir haritadır. $f(x)$'in her çıkış koordinatı, $x = \sum_{i=0}^{n-1} x_i \alpha_i$ olmak üzere, (5.5) ifadesindeki gibi verilebilir [57][64].

$$f_i(x) = Tr(g(x)\beta_i) \tag{5.5}$$

Buna ek olarak (5.5) ifadesinde β_i dual taban değerleri (5.6) ifadesinde gösterildiği gibi hesaplanabilir [57][64].

$$\beta_i = \sum_{k=0}^{n-1} b_{ki} \alpha_k \tag{5.6}$$

Denklem (5.6) da $B = \left[b_{ij} \right] = A^{-1}$ ve $A = \left[a_{ij} \right]$ olmak üzere $n \times n$ boyutundaki A matrisi elemanları

$$a_{ij} = Tr(\alpha_i \alpha_j), \qquad 0 \le i, j \le n-1 \tag{5.7}$$

ifadesindeki gibi gösterilebilir. $A = \left[a_{ij} \right]$ şeklindeki A matrisi (5.8) ifadesinde açık biçimde gösterilmiştir.

$$A = \begin{bmatrix} Tr(\alpha_0\alpha_0) & Tr(\alpha_0\alpha_1) & ..... & Tr(\alpha_0\alpha_{n-1}) \\ Tr(\alpha_1\alpha_0) & Tr(\alpha_1\alpha_1) & ..... & Tr(\alpha_1\alpha_{n-1}) \\ & . & & \\ & . & & \\ Tr(\alpha_{n-1}\alpha_0) & Tr(\alpha_{n-1}\alpha_1) & .... & Tr(\alpha_{n-1}\alpha_{n-1}) \end{bmatrix} \tag{5.8}$$

Böylece giriş bitlerine uygulanacak ters haritalama işleminden sonraki çıkış koordinatları ya da giriş bitlerine uygulanacak doğrusal dönüşüm işleminden sonraki çıkış koordinatları (5.9) ifadesi ile gösterilebilir.

$$f_i, \quad 0 \le i \le n\text{-}1 \tag{5.9}$$

Örnek 5.5: Bu bölümdeki tanım ve matematik alt yapıyı kullanarak AES S-kutusunun cebirsel ifadesinin elde edilişi aşağıda göstermektedir. (5.10) ifadesindeki doğrusal dönüşüm AES S-kutusunun tasarımında kullanılan doğrusal dönüşümdür.

$$\begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{5.10}$$

AES S-kutusunun tasarımında kullanılan ve (5.10) ifadesinde verilen doğrusal dönüşüm düşünülerek $P(X) = X^8 + X^4 + X^3 + X + 1$ indirgenemez polinomu ile oluşturulan sonlu cisimde doğrusal dönüşümün cebirsel ifadesi bulunmaya çalışılsın. α, $P(X)$ polinomunun bir kökü olsun. $\beta = \alpha + 1$ ise ilkel eleman olsun (α, tüm cisim elemanlarını üretmemektedir). O zaman x_i giriş biti değerleri β değerlerine bağlı olarak bu bölümde verilen tanımlara göre;

$$\begin{aligned} x_0 &= \mathrm{Tr}(\beta^{228}X) \\ x_1 &= \mathrm{Tr}(\beta^{204}X) \\ x_2 &= \mathrm{Tr}(\beta^{179}X) \\ x_3 &= \mathrm{Tr}(\beta^{2}X) \\ x_4 &= \mathrm{Tr}(\beta^{73}X) \\ x_5 &= \mathrm{Tr}(\beta^{48}X) \\ x_6 &= \mathrm{Tr}(\beta^{23}X) \\ x_7 &= \mathrm{Tr}(\beta^{253}X) \end{aligned} \tag{5.11}$$

ifadesindeki gibi elde edilebilir. Doğrusal matris çıkışı koordinatlar $f_0, f_1, ..., f_7$ ise (5.10) ifadesinde verilen ikili matrisi kullanılarak (5.12) ifadesindeki gibi elde edilebilir.

$$\begin{aligned} f_0 &= \mathrm{Tr}(\beta^{166}X) + 1 \\ f_1 &= \mathrm{Tr}(\beta^{53}X) + 1 \\ f_2 &= \mathrm{Tr}(\beta^{36}X) \\ f_3 &= \mathrm{Tr}(\beta^{11}X) \\ f_4 &= \mathrm{Tr}(\beta^{72}X) \\ f_5 &= \mathrm{Tr}(\beta^{76}X) + 1 \\ f_6 &= \mathrm{Tr}(\beta^{51}X) + 1 \\ f_7 &= \mathrm{Tr}(\beta^{26}X) \end{aligned} \tag{5.12}$$

Doğrusal matris çıkış koordinatlarını kullanarak doğrusal dönüşümün cebirsel ifadesi polinom taban değerlerinin $\{1, \alpha, \alpha^2, ..., \alpha^7\}$ olduğu bilgisinden yola çıkarak AES S-kutusunda kullanılan doğrusal dönüşümün cebirsel ifadesi $A(X)$,

$$A(X) = f_0 + \alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + ... + \alpha^7 f_7 \tag{5.13}$$

şeklinde yazılabilir. Bunun yanında

$$\alpha = \beta^{25}, \alpha^2 = \beta^{50}, \alpha^3 = \beta^{75}, \alpha^4 = \beta^{100}, \alpha^5 = \beta^{125}, \alpha^6 = \beta^{150}, \alpha^7 = \beta^{175} \tag{5.14}$$

şeklinde verilen polinom taban değerleri (bakınız EK A) $A(X)$ ifadesinde yerine konursa

$$\begin{aligned} A(X) = {} & (\beta^{166}X + (\beta^{166})^2 X^2 + ... + (\beta^{166})^{128} X^{128}) \\ & + \beta^{25}(\beta^{53}X + (\beta^{53})^2 X^2 + ... + (\beta^{53})^{128} X^{128}) \\ & + \beta^{50}(\beta^{36}X + (\beta^{36})^2 X^2 + ... + (\beta^{36})^{128} X^{128}) \\ & + \beta^{75}(\beta^{11}X + (\beta^{11})^2 X^2 + ... + (\beta^{11})^{128} X^{128}) \\ & + \beta^{100}(\beta^{72}X + (\beta^{72})^2 X^2 + ... + (\beta^{72})^{128} X^{128}) \\ & + \beta^{125}(\beta^{76}X + (\beta^{76})^2 X^2 + ... + (\beta^{76})^{128} X^{128}) \\ & + \beta^{150}(\beta^{51}X + (\beta^{51})^2 X^2 + ... + (\beta^{51})^{128} X^{128}) \\ & + \beta^{175}(\beta^{26}X + (\beta^{26})^2 X^2 + ... + (\beta^{26})^{128} X^{128}) + "63". \end{aligned} \tag{5.15}$$

$A(X)$ ifadesindeki X teriminin katsayısı A_0 ise

$$\begin{aligned} & \beta^{166}, \beta^{(53+25) \bmod 255}, \beta^{(50+36) \bmod 255}, \beta^{(75+11) \bmod 255}, \\ & \beta^{(100+72) \bmod 255}, \beta^{(125+76) \bmod 255}, \beta^{(150+51) \bmod 255}, \\ & \beta^{(175+26) \bmod 255} \end{aligned} \tag{5.16}$$

değerlerinin toplamı şeklinde ifade edilebilir. Dolayısıyla

$$\begin{aligned} A_0 &= \beta^{166} + \beta^{78} + \beta^{86} + \beta^{86} + \beta^{172} + \beta^{201} + \beta^{201} + \beta^{201}, \\ A_0 &= \text{"2A"+"78"+"DC"+"DC"+"7A"+"2D"+"2D"+"2D"}, \\ A_0 &= \text{"05"} \end{aligned} \tag{5.17}$$

şeklinde elde edilir. Diğer terimlerin katsayıları da aynı şekilde elde edildikten sonra sonuçlanan cebirsel ifade (5.18) deki gibi elde edilir.

$$A(X) = \text{"63"+"05"X+"09"}X^2 + \text{"f9"}X^4 + \text{"25"}X^8 + \text{"f4"}X^{16} + \text{"01"}X^{32} + \text{"b5"}X^{64} + \text{"8f"}X^{128} \tag{5.18}$$

5.5. Lagrange İnterpolasyonu

Lagrange interpolasyonu, n noktadan geçen $n-1$ dereceli polinomu bulmak için kullanılır. Dolayısı ile $(x_0, y_0), (x_1, y_1), ..., (x_{n-1}, y_{n-1})$ değerleri biliniyor ise (5.19) ifadesi ile polinomun cebirsel açılımı bulunabilir.

$$P(X) = \sum_{j=0}^{n} y_j \ell_j(X) \tag{5.19}$$

(5.19)'daki $\ell_j(X)$ değerinin açılımı (5.20) deki gibidir.

$$\ell_j(X) = \prod_{i=0, i\neq j}^{k} \frac{X - x_i}{x_j - x_i} = \frac{X - x_0}{x_j - x_0} \cdot \cdots \cdot \frac{X - x_{j-1}}{x_j - x_{j-1}} \cdot \frac{X - x_{j+1}}{x_j - x_{j+1}} \cdot \cdots \cdot \frac{X - x_k}{x_j - x_k} \tag{5.20}$$

(5.21) ifadesi lagrange interpolasyonunun nasıl hesaplandığını açık şekilde göstermektedir.

$$
\begin{aligned}
P(X) = {} & \frac{(X-x_2)(X-x_3)(X-x_4)...(X-x_n)}{(x_1-x_2)(x_1-x_3)(x_1-x_4)...(x_1-x_n)} y_1 + \\
& \frac{(X-x_1)(X-x_3)(X-x_4)...(X-x_n)}{(x_2-x_1)(x_2-x_3)(x_2-x_4)...(x_2-x_n)} y_2 + \\
& \frac{(X-x_1)(X-x_2)(X-x_4)...(X-x_n)}{(x_3-x_1)(x_3-x_2)(x_3-x_4)...(x_3-x_n)} y_3 + \\
& \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \\
& \frac{(X-x_1)(X-x_2)(X-x_4)...(X-x_{n-1})}{(x_n-x_1)(x_n-x_2)(x_n-x_4)...(x_n-x_{n-1})} y_n
\end{aligned}
\tag{5.21}
$$

Lagrange interpolasyonu ile bir S-kutusunun cebirsel ifadesinin açılımı bulunabilir. Fakat bu yapılır iken sonlu cisim aritmetiği dikkate alınmalıdır ve Galois cismi üzerinde işlem yapıldığı unutulmamalıdır. Buna ek olarak lagrange interpolasyonu kaba bir hesaplama yöntemidir. Dolayısı ile çalışmamızda S-kutularının cebirsel ifadesinin incelenmesinde sonlu cisim aritmetiği kullanılmıştır.

5.5. Doğrusal Dönüşüm (Affine Dönüşüm)

Bir S-kutusu, gerek sonlu cisimde ters alma işlemi ile üretilsin gerekte üs haritalama yöntemi ile üretilsin istenmeyen bir özellik olan doğrusal fazlalığın (linear redundancy) oluşumu bu tür cebirsel yapılarda gerçekleşir. Sonlu cisim aritmetiği kullanılarak AES S-kutusuna benzer olarak tasarlanan S-kutuları için bu istenmeyen özellik gösterilebilir. Sonlu cisimde ters haritalama ya da üs haritalama yöntemini kullanarak elde edilen yapıların üzerine doğrusal dönüşüm uygulamak S-kutusunun kriptografik özellikleri (DDT, LAT gibi) üzerinde bir değişiklik yapmaz iken cebirsel ifadesini daha karmaşık hale getirmektedir.

Tanım 5.4: Bir doğrusal dönüşüm f'den g'ye $g(x) = f(Dx \oplus a) \oplus b.x \oplus c$ (D n x n tersi olan bir matris ve $a \in F_2^n, b \in F_2^n, c \in F_2$) olacak şekilde bir haritadır.

Örnek 5.6: GF(2) de aşağıdaki

$$M=\begin{bmatrix}1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\\1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\end{bmatrix}$$ matrisi ve $v=\begin{bmatrix}1\\1\\0\\0\\0\\1\\1\\0\end{bmatrix}$ vektörü ile doğrusal dönüşümüne

uygulanır ise yani $\{a'\}=M\{a\}+\{v\}$ değeri aşağıdaki gibi hesaplanır.

$$\begin{aligned}
a'_0 &= a_0 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus 1 = 0\oplus 0\oplus 0\oplus 1\oplus 1\oplus 1 = 1\\
a'_1 &= a_0 \oplus a_1 \oplus a_5 \oplus a_6 \oplus a_7 \oplus 1 = 0\oplus 1\oplus 0\oplus 1\oplus 1\oplus 1 = 0\\
a'_2 &= a_0 \oplus a_1 \oplus a_2 \oplus a_6 \oplus a_7 \oplus 0 = 0\oplus 1\oplus 0\oplus 1\oplus 1\oplus 0 = 1\\
a'_3 &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_7 \oplus 0 = 0\oplus 1\oplus 0\oplus 1\oplus 1\oplus 0 = 1\\
a'_4 &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus 0 = 0\oplus 1\oplus 0\oplus 1\oplus 0\oplus 0 = 0\\
a'_5 &= a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus 1 = 1\oplus 0\oplus 1\oplus 0\oplus 0\oplus 1 = 1\\
a'_6 &= a_2 \oplus a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus 1 = 0\oplus 1\oplus 0\oplus 0\oplus 1\oplus 1 = 1\\
a'_7 &= a_3 \oplus a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus 0 = 1\oplus 0\oplus 0\oplus 1\oplus 1\oplus 0 = 1
\end{aligned}$$

Sonuç olarak $\{a'\}=\{11101101\}$ ve polinomsal gösterimi ile $a'(X)=X^7+X^6+X^5+X^3+X^2+1$ şeklinde ifade edilebilir.

Tanım 5.5: Eğer Tanım 5.4 de gösterildiği gibi f ve g fonksiyonları bir doğrusal dönüşüm ile ilişkili ise bu fonksiyonlara denk fonksiyonlar ya da aynı denk sınıftaki fonksiyonlar denir.

Literatürde doğrusal dönüşümün S-kutusu tasarımı sırasında kullanımında çeşitli farklılıklar gözlenmiştir. Örneğin AES S-kutusu tasarımında ters haritalama işleminden sonra ikili bir doğrusal dönüşüm kullanılırken, Camellia'da ters haritalama işleminden önce ve sonra ikili doğrusal dönüşüm kullanılmaktadır. Bu da ortaya doğrusal dönüşümün kullanılacağı yere ilişkin olarak üç farklı durumu işaret etmektedir:

- Durum 1: İkili doğrusal dönüşümü ters haritalama işleminden sonra kullanmak (AES),

- Durum 2: İkili doğrusal dönüşümü ters haritalama işleminden önce kullanmak,

- Durum 3: İkili doğrusal dönüşümü ters haritalama işleminden hem önce hem de sonra kullanmak (Camellia).

Tezin bu bölümünde sonlu cisimde üs alma yöntemi ile tasarlanan bir S-kutusunun cebirsel ifadesindeki terim sayısı, belirtilen üç durum için incelemiştir ve 8 bit girişli ve 8 bit çıkışlı cebirsel tabanlı S-kutularının cebirsel ifadelerindeki terim sayısında iyileştirme yapılıp yapılamayacağı üzerine odaklanılmıştır.

Tanım 5.7: $GF(2^n)$ üzerinde β_i katsayılarına sahip olan $L(X)=\sum_{i=0}^{t}\beta_i X^{2^i}$ şeklinde yazılabilen polinomlara doğrusallaşmış polinom adı verilir.

Önerme 5.1: A, $GF(2^n)$ üzerinde doğrusal bir harita olsun. O zaman $A(X), X \in GF(2^n)$ olmak üzere $GF(2^n)$ üzerinde doğrusallaşmış polinom olarak terimlerine (5.22) ifadesinde gösterildiği gibi açılabilir.

$$A(X)=\sum_{i=0}^{n-1}\beta_i X^{2^i} \tag{5.22}$$

Önerme 5.2: $\alpha_1,\alpha_2,...\alpha_t$ $GF(2^n)$'in elemanları olsun. O zaman (5.23)'teki ifade yazılabilir.

$$(\alpha_1+\alpha_2+...+\alpha_t)^{2^k}=\alpha_1^{2^k}+\alpha_2^{2^k}+....+\alpha_t^{2^k} \tag{5.23}$$

Bu tanım ve önermelerden yola çıkarak Teorem 5.1 durum 1 için cebirsel tabanlı bir S-kutusunun cebirsel ifadesindeki terim sayısı ve cebirsel ifadedeki derece hakkında bilgi vermektedir.

Teorem 5.1: $GF(2^n)$'in bir fonksiyonu $F(X) = X^d$ olsun ve bu $F_2^{(n)}$ üzerinde $f(x_1....x_n) = (f_1(x)....f_n(x))$ boole fonksiyonuna karşılık gelsin. O zaman $f(x_1....x_n)$'nin çıkış koordinatlarına uygulanan doğrusal bir dönüşüm ile elde edilen boole fonksiyonuna karşılık gelen $G(X)$ aşağıdaki şekilde ifade edilir [57].

$$G(X) = \sum_{i=0}^{2^n-1} b_i X^i \qquad b_i = 0 \forall i \notin C_d \pmod{2^n - 1} \tag{5.24}$$

İspat: Önerme 5.1 kullanılarak $G(X)$ aşağıdaki gibi açılabilir.

$$\begin{aligned} G(X) = \sum_{i=0}^{n-1} (a_i F(X))^{2^i} &= \sum_{i=0}^{n-1} (a_i X^d)^{2^i} \\ &= \sum_{i=0}^{n-1} a_i {}^{2^i} X^{d2^i}. \end{aligned} \tag{5.25}$$

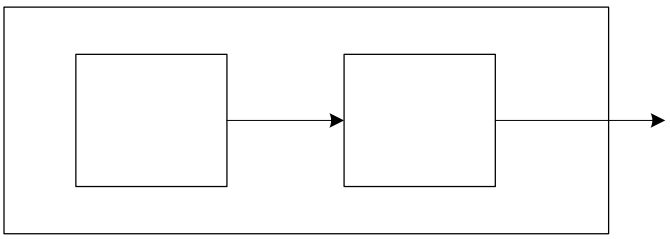
Teoremde $X^{d2^i} = X^{(d2^i) \bmod (2^n - 1)}$ olarak alınmıştır. $F(X) = \sum_{i \in I} a_i X^i$ ise o zaman diyebiliriz ki $G(X) = \sum_{j \in J} b_j X^j$ dir ve J ise set I'ya karşılık gelen $\bmod 2^n - 1$'e göre cyclotomic kosetlerdir.

AES S-kutusu tasarımda durum 1 deki gibi doğrusal ikili bir dönüşüm uygulanmıştır. Yani giriş bitleri önce sonlu cisimde ters haritalama işlemine daha sonra ters haritalama çıkışındaki koordinatlara doğrusal dönüşüm uygulanmıştır. Daha önceki bölümlerde AES şifresinin ters haritalama tabalı S-kutusuna sahip olduğunu belirtilmişti. Ters haritalama tabanlı bu S-kutusuna doğrusal dönüşüm uygulanarak tek terimli olan basit cebirsel ifade dokuz terime çıkartılmıştır. Ters haritalama işleminden

sonra (5.10) ifadesindeki doğrusal dönüşüm kullanılarak elde edilen AES S-kutusunun cebirsel ifadesi, A(X) ifadesinde X yerine X^{-1} veya X^{254} konarak

$$S(X) = "63" + "05" X^{254} + "09" X^{253} + "f9" X^{251} + "25" X^{247} + "f4" X^{239} + "01" X^{223} + "b5" X^{191} + "8f" X^{127}. \quad (5.26)$$

(5.26)'daki gibi elde edilebilir. Bu ifade AES S-kutusunun cebirsel açılımıdır. Terim sayısı 9 ve herhangi bir üssün derecesinin Hamming ağırlığı 7 dir. Durum 1 ve Teorem 5.1, Şekil 5.1'de gösterilmiştir.



Şekil 5.1: Durum 1'e göre S-kutusu üretimi

Teorem 5.2: $GF(2^n)$'in bir fonksiyonu $F(X) = X^d$ olsun ve bu $F_2^{(n)}$ üzerinde $f(x_1,....,x_n) = (f_1(x),....,f_n(x))$ boole fonksiyonuna karşılık gelsin. G(X) ise $f(x_1,....,x_n)$ sabitlenirken $x_1,....,x_n$ giriş bitlerine doğrusal bir dönüşüm uygulanarak elde edilen bir boole haritasına karşılık gelen bir fonksiyon olsun. O zaman $G(X)$,

$$G(X) = \sum_{i=0}^{2^n-1} b_i X^i \qquad wt(i) > wt(d) \text{ için } b_i = 0 \quad (5.27)$$

şeklinde ifade edilir [57].

İspat: Önerme 5.1 kullanılarak G(X) aşağıdaki gibi ifade edilebilir.

$$X \rightarrow X^{254}$$

$$G(X) = \left(\sum_{i=0}^{n-1} c_i X^{2^i} \right)^d \tag{5.28}$$

Burada $d = \sum_{j=0}^{n-1} d_j 2^j$ ve J'de $s = wt(d)$ olmak üzere $\{j_1, ..., j_s\}$ olan bir set olduğu düşünülür ise o zaman

$$\begin{aligned} G(X) &= \prod_{j \in J} \left(\sum_{i=0}^{n-1} c_i X^{2^{i+j}} \right) \\ &= \left(\sum_{i_1=0}^{n-1} c_{i_1} X^{2^{i_1+j_1}} \right) \left(\sum_{i_2=0}^{n-1} c_{i_2} X^{2^{i_2+j_2}} \right) \cdots \left(\sum_{i_1=0}^{n-1} c_{i_s} X^{2^{i_1+j_s}} \right) \\ &= \sum_{i_1, i_2, ..., i_s} c_{i_1} c_{i_2} \ldots c_{i_s} X^{2^{i_1+j_1} + 2^{i_2+j_2} + \ldots + 2^{i_s+j_s}} \end{aligned} \tag{5.29}$$

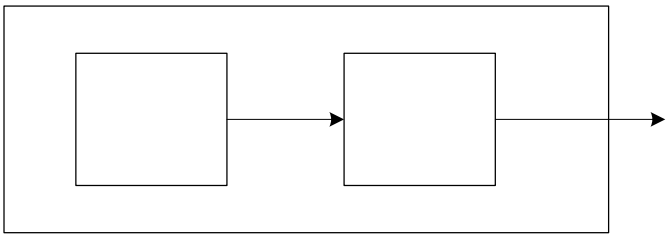
olarak yazılabilir.

Teoremde $wt(2^{i_1+j_1} + 2^{i_2+j_2} + \ldots + 2^{i_s+j_s}) = s \le wt(d)$ dir. O zaman $W = \underset{i \in I}{maks}\, wt(i)$ olsun. Eğer $F(X) = \sum_{i \in I} a_i X^i$ ise $G(X) = \sum_{j \in J} b_j X^j$ şeklindedir ve J, W 'dan küçük Hamming ağırlığına sahip elemanların setidir.

Teorem 5.2 gereği durum 2'ye göre tasarlanan cebirsel S-kutularının ifadesindeki terim sayısı için (5.30) da gösterilen formül verilebilir.

$$T.S = 1 + C\binom{n}{1} + C\binom{n}{2} + ... + C\binom{n}{r} \tag{5.30}$$

(5.30) da verilen r, S-kutusu tasarımında kullanılan üs fonksiyonunun hamming ağılığını temsil etmektedir.



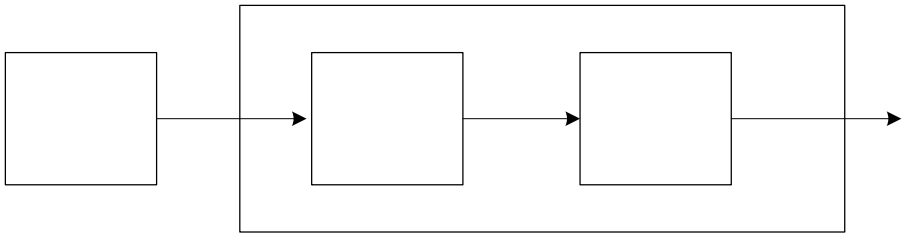
Şekil 5.2: Durum 2'ye göre S-kutusu üretimi

Şekil 5.2 durum 2 kullanılarak tasarlanan bir S-kutusunu temsil etmektedir. Durum 2 de S-kutusunun cebirsel ifadesini A(X) formundaki doğrusal dönüşümün $S(X) = A(X)^{254}$ şeklinde 254. kuvvetini alarak elde edilebilir. Bu alınan üs fonksiyonunun Hamming ağırlığı 7 olduğu için (5.30)'da verilen formül gereğince durum 2'ye göre tasarlanan bir S-kutusunun cebirsel ifadesindeki terim sayısı

$$T.S = 1 + C\binom{8}{1} + C\binom{8}{2} + ... + C\binom{8}{7} = 1 + 8 + 28 + 56 + 70 + 56 + 28 + 8 = 255$$

şeklinde verilebilir.

Birinci durumda doğrusal dönüşüm haritalama işleminden sonra, ikinci durumda doğrusal dönüşüm haritalama işleminden önce kullanılmaktadır. Üçüncü durumda ise doğrusal dönüşüm haritalama işleminden hem önce hem de sonra kullanılmaktadır. Bu işlem Şekil 5.3'de gösterilmektedir ve tezde durum 3 olarak isimlendirilmiştir



Şekil 5.3: Durum 3'e göre S-kutusu üretimi

Şekil 5.3'te görüldüğü gibi giriş bitlerine önce bir doğrusal dönüşüm (L_{A1}) uygulanmış daha sonra haritalama işlemi yapılmıştır. Buradan çıkan bitler, tekrar bir doğrusal dönüşüme (L_{A2}) tabi tutulmuşlardır. Böylelikle S-kutusu oluşturulmuştur.

Bunun yanında durum 2 için (5.30) da verilen terim sayısı formülü durum 3 ile aynı olacaktır. Örneğin 8 bit giriş ve 8 bit çıkışlı bir S-kutusu düşünelim ve bu S-kutusu sonlu cisimde ters haritalama yöntemine göre ve durum 3'e göre tasarlanmış olsun. Buna ek olarak Şekil 5.3'te gösterilen L_{A2}, AES S-kutusu tasarımında kullanılan doğrusal dönüşüm olsun. Dolayısı ile durum 3 için cebirsel ifadenin hesaplanmasında AES S-kutusunun cebirsel ifadesinden faydalanılabilir. Yani durum 3 ile tasarlanacak bir S-kutusu için cebirsel ifade AES S-kutusundaki cebirsel ifade de X yerine $L_{A1}(X)$ konarak elde edilebilir.

$$\begin{aligned} S(X) = {} & "63" + "05"\left[L_{A1}(X)\right]^{254} + "09"\left[L_{A1}(X)\right]^{253} + "f9"\left[L_{A1}(X)\right]^{251} + "25"\left[L_{A1}(X)\right]^{247} \\ & + "f4"\left[L_{A1}(X)\right]^{239} + "01"\left[L_{A1}(X)\right]^{223} + "b5"\left[L_{A1}(X)\right]^{191} + "8f"\left[L_{A1}(X)\right]^{127} \end{aligned} \tag{5.31}$$

(5.31) ifadesinde AES S-kutusunun girişine uygulanacak bir doğrusal dönüşüm olan L_{A1}'in cebirsel ifadedeki etkisi gösterilmektedir. (5.31) ifadesinde gözlenen her üs aynı cyclotomic kosette olduğunda sonuçlanan cebirsel ifadedeki terim sayısı 255 olacaktır. Hatta (254, 253, 251, 247, 239, 223, 191, 127) üs fonksiyonları aynı cyclotomic kosette olduğu için bu üs fonksiyonlarının herhangi biri ile tasarlanacak S-kutusunun cebirsel ifadesi de 255 terime sahip olacaktır. Yani $\left[L_{A1}(X)\right]^{254}$, $\left[L_{A1}(X)\right]^{253}$, $\left[L_{A1}(X)\right]^{251}$, $\left[L_{A1}(X)\right]^{247}$, $\left[L_{A1}(X)\right]^{239}$, $\left[L_{A1}(X)\right]^{223}$, $\left[L_{A1}(X)\right]^{191}$, $\left[L_{A1}(X)\right]^{127}$ ifadelerinin ayrı ayrı açılımları da 255 terim içerecektir ve sonuçlanan cebirsel ifade 255 terimden meydana gelecektir.

BÖLÜM 6

6. Cebirsel Olarak Güçlendirilmiş S-kutusu Önerisi

Tezin bu bölümünde 5. bölümde anlatılan durum 3'e göre $X \to X^{254}$, $X \to X^{127}$ ve $X \to X^{7}$ $X \in GF(2^8)$ olmak üzere 8 bit giriş ve 8 bit çıkışlı cebirsel açıdan geliştirilmiş üç S-kutusunun tasarımı gerçekleştirilecektir. Bu üç S-kutusunun tasarım yapısı aşağıdaki gibi verilebilir:

$$\begin{aligned} &\text{Adım1. } P = L_{A1}(x) = L_{A1(n\times n)}.(x_0, x_1, ..., x_{n-1})^T \oplus L_{A_{S1}}. \\ &\text{Adım 2. } K = (P)^7,\ K = (P)^{127} \text{ veya } K = (P)^{254}. \\ &\text{Adım3. } S(x) = L_{A2(n\times n)}.(K_0, K_1, ..., K_{n-1})^T \oplus L_{A_{S2}}. \end{aligned} \tag{6.1}$$

(6.1) ifadesindeki adımlarda P ve K ara adımlardaki 8-bit değerleri L_{A1} ve L_{A2} ikili doğrusal dönüşümlerindeki ikili doğrusal matrisleri, $L_{A_{S1}}$ ve $L_{A_{S2}}$ ise doğrusal dönüşümdeki ikili doğrusal sabitleri temsil etmektedir. İndirgenemez polinom olarak AES'te de kullanılan $P(X) = X^8 + X^4 + X^3 + X + 1$ polinomu kullanılmıştır. Bu polinom kullanılarak önce $GF(2^8)$ cismi üretilmiştir. Üretilen bu cisim EK A'da verilmektedir. S-kutusu oluşturulurken giriş bitlerine önce L_{A1} dönüşümü uygulanmıştır. Daha sonra $X \to X^7$, $X \to X^{127}$, $X \to X^{254}$ gibi üs haritalama işlemleri adımlarda belirtilen şekilde uygulanmış ve en son olarak L_{A2} dönüşümü üs haritalama çıkış koordinatlarına uygulanarak S-kutuları elde edilmiştir.

6.1 $X \to X^{254}$ Üs Haritalaması için S-kutusu Tasarımı

$X \to X^{254}$ üs haritalaması için kullanılan doğrusal dönüşümler (6.2) ve (6.3) ifadelerindeki gibidir. Bu doğrusal dönüşümler tersi alınabilir ikili dönüşümlerdir. 8 bit giriş 8 bit çıkışlı bir S-kutusu üretilmek istendiğinden dolayı 8×8 'lik doğrusal dönüşüm kullanılmıştır. Dönüşümlerdeki $x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7$ değerleri ikili biçimde yazılmış bitlerdir. Doğrusal dönüşümdeki matris çarpımına eklenen değer ise doğrusal dönüşüm sabitidir. Doğrusal dönüşümlerin sabitleri sırası ile L_{AS1} ="33" ve L_{AS1} ="63" şeklindedir. Bu değerler hexadecimal notasyonda gösterilmiştir. Tezde herhangi bir S-kutusu tasarlanırken AES'te olduğu gibi sabit nokta içermemesine önem verilmiştir.

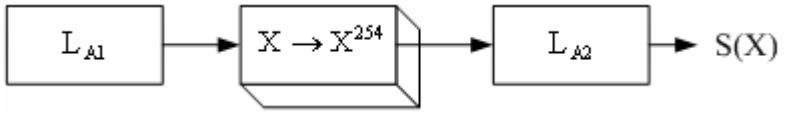
$$L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{6.2}$$

$$L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{6.3}$$

L_{A1} doğrusal dönüşümünün cebirsel açılımı Bölüm 5.4 te verilen tanım ve teorilerin ışığı altında (6.4) teki gibi verilebilir.

$$L_{Al}(X) = "33" + "52"X + "77"X^2 + "13"X^4 + "E0"X^8 + "FE"X^{16} + "9E"X^{32} + "96"X^{64} + "27"X^{128} \quad (6.4)$$

$X \to X^{254}$ haritalaması ile $X \to X^{127}$ haritalaması aynı cyclotomic kosetteki üslere sahiptir. Bu iki üs Tablo 4.3'te verilen 127 sınıfının iki elemanıdır. Bölüm 4'te verilen tanım ve teoriler gereği 127, 254, 253, 251, 247, 239, 223, 191 üsleri kullanılarak tasarlanacak S-kutuları aynı kriptografik özellikleri barındıracaktır. Diğer bir deyişle $X \to X^{254}$ ve $X \to X^{127}$ haritalamaları ile tasarlanacak S-kutuları aynı kriptografik özelliklere sahiptir. Bunun ötesinde yukarıda verilen üsler tabanlı ve herhangi bir duruma göre tasarlanacak S-kutusu da AES S-kutusunun sahip olduğu kriptografik özellikler ile aynı özelliklere sahip olacaktır. Ancak Durum 2 ve durum 3'e göre 127 sınıfı kullanılarak tasarlanacak S-kutularının cebirsel ifadesinde 9'dan 255'e artan cebirsel açıdan bir iyileştirme mümkün olacaktır. Buna ek olarak durum 1 ile elde edilecek cebirsel derece 254 değişmeyecektir.



Şekil 6.1: Durum 3'e göre $X \to X^{254}$ haritalaması ile S-kutusu tasarımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	C3	18	27	80	15	34	FD	F7	2B	FE	6B	77	F0	CA	D4	72
1	1A	1B	E3	D6	CF	6A	D1	B1	21	10	9D	40	85	D0	F9	9F
2	66	48	C1	57	8A	E8	78	B4	E9	CE	D9	98	68	8C	99	BB
3	0A	49	95	AC	08	6C	C8	4E	14	DE	2A	4F	17	CD	A7	19
4	89	E6	B0	0F	28	1E	E1	94	74	BD	1C	2E	F6	3E	61	9E
5	13	97	64	3D	0B	EE	60	88	F4	7A	8D	6D	24	32	C2	79
6	C9	59	9C	AF	AB	01	63	C5	E5	D8	36	26	05	C7	07	75
7	AA	4D	50	7F	F3	B6	51	F5	BE	4C	20	ED	5A	83	52	84
8	E7	A9	AE	56	91	62	3A	06	C4	73	44	0C	22	DC	B8	5E
9	BA	C6	8B	DD	86	B9	B5	03	41	16	42	A1	69	11	87	55
A	53	5B	58	CB	29	B3	2C	6E	45	A8	33	EF	92	8F	DA	FF
B	B7	CC	31	A5	EB	E2	23	96	AD	C0	47	82	F2	7B	67	D7
C	A3	38	D2	BC	3C	02	FB	43	3B	2F	A0	09	FC	00	39	4A
D	7C	6F	76	30	A4	A2	7D	FA	12	B2	9A	04	3F	93	F1	71
E	81	90	DB	46	5D	7E	EC	5F	D3	E4	5C	E0	D5	37	EA	65
F	F8	8E	DF	9B	54	2D	0D	BF	35	1D	0E	70	A6	25	1F	4B

Tablo 6.1: (6.2) ve (6.3) dönüşümleri kullanılarak $X \to X^{254}$ haritalamasına göre üretilen S-kutusu

Tablo 6.1'deki S-kutusunun cebirsel ifadesi (5.31) deki gibidir. Terim sayısı 255'tir. AES S-kutusunun terim sayısı 9 dur. Dolayısı ile durum 3'e göre 127 sınıfı elemaları kullanılarak tasarlanacak bir S-kutusu cebirsel ifadedeki terim sayısını 9'dan 255'e arttıran bir iyileştirme sunacaktır.

Tablo 6.1'deki S-kutusunun DDT dağılım 256×256 boyutlu bir tablo olacaktır. Bu tablonun bütününü incelemek çok zordur. Fakat Teorem 4.2 düşünüldüğünde bu tablonun 1×256'lık bölümünü incelemek yeterlidir. Zira diğer bölümler aynı dağılımı göstereceklerdir. Buna göre Fark Dağılım Tablosunun (DDT) 01 numaralı satırı için dağılımı Tablo 6.2'deki gibidir. Bu dağılımda 129 adet 0, 126 adet 2 ve 1 adet 4 vardır. 4 uniform dağılım göstermektedir.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	2	0	0	0	0	2	0	2	2	2	0	0	0	0	0
1	2	2	0	2	2	0	2	0	0	0	0	0	2	2	0	0
2	0	2	2	2	0	2	0	2	2	0	0	0	0	0	2	2
3	0	2	2	2	0	2	2	2	0	2	2	0	2	2	2	2
4	0	2	2	2	2	2	2	0	2	0	0	0	0	0	2	0
5	0	0	0	0	2	2	2	2	0	2	0	0	0	0	0	0
6	2	0	2	0	2	2	2	0	0	0	0	0	0	2	2	2
7	0	0	2	2	0	2	2	0	2	2	0	2	2	0	2	0
8	2	0	0	2	2	0	2	2	0	2	0	0	0	0	2	2
9	2	0	0	2	2	0	2	0	0	0	2	2	0	2	2	0
A	2	0	0	0	2	2	4	2	0	2	2	0	2	0	0	0
B	2	0	2	2	0	2	2	2	2	0	0	2	2	0	2	2
C	0	0	2	0	0	2	0	0	2	2	2	0	2	2	0	0
D	0	0	2	0	0	2	2	0	0	2	2	2	2	2	0	0
E	2	0	2	2	2	2	2	2	2	0	0	0	0	2	0	0
F	0	0	2	2	0	0	0	0	2	0	0	0	2	0	2	2

Tablo 6.2: Tablo 6.1'deki S-kutusunun "01" giriş farkı için DDT dağılımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	-8	8	0	16	-4	-16	-12	10	-10	-2	2	-14	-6	6	-2
1	0	-12	-8	4	4	-4	12	4	6	-2	2	10	-14	6	6	-14
2	-8	-8	0	-16	-4	16	-12	-16	2	-2	6	-6	6	-2	-14	-6
3	-12	0	4	-8	-12	4	12	12	-6	2	-2	-10	-6	-2	-2	-6
4	2	-2	-14	-10	-10	14	-2	6	-12	-12	8	8	-8	12	12	8
5	10	10	2	2	2	-2	-6	14	-8	12	-4	8	0	-8	12	-12
6	-2	-6	6	-6	-10	-2	-2	6	-8	0	-12	-4	-8	4	12	0
7	2	-14	-6	-6	6	2	6	10	-8	-12	12	0	-12	4	8	8
8	-2	10	2	14	-6	2	-2	-2	4	-4	-4	-4	0	-4	0	-4
9	2	2	6	-2	10	6	6	2	4	0	4	0	-4	12	-4	-12
A	-2	10	-6	6	-10	14	-6	10	4	-12	4	12	4	8	4	-8
B	-10	-10	-6	-14	-14	-2	-10	2	-8	-4	8	-4	-4	4	4	4
C	12	-12	-8	8	12	-8	-8	-12	-6	-2	2	-10	2	2	-14	10
D	-8	12	12	0	4	12	0	0	-14	-14	-6	2	6	2	-2	-6
E	-8	8	-12	12	-12	8	8	12	-2	2	6	10	-6	-6	-14	-6
F	8	4	4	0	8	-8	4	12	-6	10	-6	2	10	-10	2	-2

Tablo 6.3: Tablo 6.1'deki S-kutusunun "01" giriş maskesi için LAT dağılımı

Tablo 6.1'deki S-kutusunun LAT dağılım DDT'ye benzer şekilde 256×256 'lık bir tablo olacaktır. $2^8 \times 2^8$ boyutunda LAT tablosu değerleri yerine $\mathrm{LAT}(1,\Gamma_b)$ değerlerinin elde edilmesi yeterli olacaktır. Diğer satırlarda aynı dağılımı vermektedir. Buna göre Doğrusal Yaklaşım Tablosunun (LAT) 01 numaralı satırı için dağılımı Tablo 6.3'deki gibidir. Bu tabloda 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 şeklindedir. Dolayısı ile S-kutusunun $|\mathrm{N}_{\mathrm{Lmaks}}| = 16$ 'dır ve aynı zamanda bu sınıf, %93 doğrusal olmama oranındadır. Dikkat edilirse 127 ve 254 aynı özellikleri yansıtmaktadırlar.

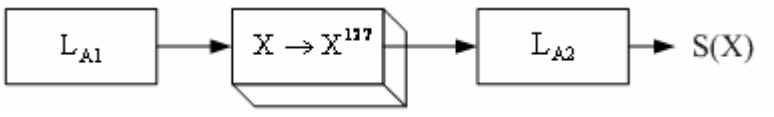
6.2 $X \rightarrow X^{127}$ Üs Haritalaması için S-kutusu Tasarımı

Bu haritalama için kullanılan doğrusal dönüşümler (6.5) ve (6.6) ifadelerindeki gibidir ve doğrusal dönüşümlerin sabitleri sırası ile $L_{A_{S1}} = "A9"$ ve $L_{A_{S1}} = "63"$ şeklindedir.

$$L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{6.5}$$

$$L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \tag{6.6}$$

Buna göre $X \rightarrow X^{127}$ haritalamasına göre S-kutusu tasarım yapısı Şekil 6.2'de gösterilmiştir. Üretilen S-kutusu Tablo 6.4'te gösterilmektedir.



Şekil 6.2: Durum 3'e göre $X \rightarrow X^{127}$ haritalaması ile S-kutusu tasarımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	F4	1A	95	20	ED	AC	1B	7A	22	3C	EC	DA	FF	5F	02	DC
1	8F	7E	43	5E	B8	FB	5D	92	4C	49	D6	6D	8D	E3	0A	BE
2	8E	C0	A1	30	76	42	AD	F8	E8	C7	9E	F7	FD	61	05	8A
3	15	F6	07	78	B4	75	3E	34	7C	41	47	DF	9B	82	16	6F
4	93	B9	96	4B	1F	23	86	3F	FE	E6	AF	98	D9	9C	89	2B
5	E9	C9	B0	6B	77	0F	59	CE	A6	EB	B5	F1	71	03	E2	25
6	F3	17	F9	60	88	9F	CD	B6	53	D3	A0	AE	56	09	E4	5B
7	A9	2F	E0	CB	58	5C	3B	E7	EE	D0	19	F5	51	A7	85	0B
8	70	A5	C6	B2	12	BA	31	0E	BB	C5	1E	CA	F0	28	63	99
9	D4	E1	AB	68	8C	01	94	72	9A	8B	B7	35	1D	CC	DD	04
A	64	9D	14	AA	4D	DE	40	3D	3A	39	D5	29	B3	37	4A	06
B	6E	65	00	62	91	FC	EA	2C	7F	4F	10	97	13	21	2A	50
C	52	C8	CF	24	32	6A	4E	84	33	DB	A3	C4	73	38	46	EF
D	0C	BC	90	A8	45	81	D2	44	79	B1	6C	83	5A	08	D1	C2
E	FA	55	7B	2D	54	F2	87	7D	80	2E	D8	48	66	E5	1C	27
F	C1	36	74	C3	18	BD	26	57	0D	67	69	A4	A2	11	D7	BF

Tablo 6.4: (6.5) ve (6.6) dönüşümleri kullanılarak $X \to X^{127}$ haritalamasına göre üretilen S-kutusu

$X \to X^{127}$ için de durum 3'e göre tasarlanacak S-kutusunun cebirsel ifadesi $X \to X^{254}$ 'te olduğu gibi 255 terim içerecektir. Çünkü bu üsler aynı cyclotomic kosette üslerdir yani 127 sınıfının elemanlarıdır.

Tablo 6.4'te gösterilen S-kutusu Fark Dağılım Tablosu açısından 4 uniform dağılıma sahiptir. Bu S-kutusu için $\left|N_{Lmaks}\right| = 16$ 'dır ve bu S-kutusu % 93 doğrusal olmama değerine sahiptir. Bijektif olan bu S-kutusu kriptografik özellikler açısından iyi sonuçlar vermektedir.

S-kutusunun bir satırı için DDT dağılımı Tablo 6.5'te, bir satırı için LAT dağılımı ise Tablo 6.6'da gösterilmektedir.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	0	0	2	2	2	0	0	0	0	2	2	0	0	2	0
1	0	2	0	2	0	0	0	2	2	2	0	0	0	2	2	0
2	2	0	0	0	0	0	0	0	0	0	2	2	0	0	0	2
3	2	0	2	0	2	2	2	2	2	0	0	2	2	2	2	2
4	0	2	0	2	2	2	0	0	0	0	0	2	2	2	2	0
5	0	0	2	0	0	2	2	0	2	0	0	0	0	0	0	2
6	0	2	2	0	0	0	0	2	2	2	2	0	0	2	2	0
7	0	2	2	0	2	0	0	0	2	2	2	2	0	2	2	2
8	2	0	2	2	2	0	2	2	0	0	0	0	0	2	2	2
9	2	2	0	2	0	0	2	2	2	2	2	0	2	0	0	0
A	2	0	2	0	0	2	2	0	2	2	0	0	0	0	2	2
B	2	0	0	2	2	2	0	2	0	2	0	2	0	0	2	2
C	0	2	0	2	2	0	2	2	2	0	2	0	0	2	0	2
D	0	2	0	0	2	2	0	0	2	2	0	2	2	2	2	0
E	0	0	0	2	2	0	2	0	2	0	0	2	2	0	2	2
F	0	2	0	0	0	0	2	2	0	2	4	0	2	0	0	0

Tablo 6.5: Tablo 6.4'deki S-kutusunun "01" giriş farkı için DDT dağılımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	6	2	-8	0	-6	-2	8	8	10	-6	12	4	-6	2	8
1	-14	8	0	-10	-14	12	4	-2	-10	0	-12	-2	10	8	12	10
2	12	-2	10	-12	-16	14	2	8	4	-6	-6	-8	-4	-2	6	0
3	-6	-12	-4	14	-10	12	4	2	-2	-12	8	6	6	8	12	6
4	0	-2	-10	4	8	10	-6	12	4	-2	10	-12	0	14	2	0
5	2	-8	4	-6	2	12	8	-14	2	12	-12	-2	-2	-4	4	2
6	16	10	10	12	-12	-6	2	0	-12	2	6	12	4	14	-6	12
7	-2	8	12	-2	2	8	-4	-6	-2	-12	-12	2	-10	8	-8	-14
8	-2	8	-12	-2	2	-8	-12	-6	2	-8	-8	-2	2	4	4	6
9	-12	6	-2	0	-8	6	-10	4	12	-14	6	12	-12	6	2	4
A	14	4	8	6	6	16	-12	6	-6	4	-4	14	6	4	-4	2
B	8	-2	-2	-4	8	2	-6	-4	8	-6	6	0	4	10	14	-4
C	-10	8	0	-14	2	16	-8	-10	-10	4	0	-2	6	0	-4	-10
D	-12	6	2	4	8	6	-6	-8	8	-2	6	-4	-8	-6	10	-4
E	2	-16	8	14	-6	-4	4	-2	10	12	-8	-14	-2	4	0	-2
F	-12	-6	-10	-12	12	-10	-6	-4	0	2	10	4	12	-14	2	0

Tablo 6.6: Tablo 6.4'deki S-kutusunun "01" giriş maskesi için LAT dağılımı

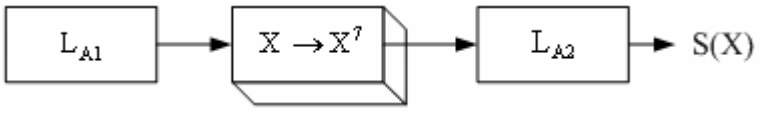
6.3 $X \rightarrow X^7$ Üs Haritalaması için S-kutusu Tasarımı

$X \rightarrow X^7$ üs haritalaması için kullanılan doğrusal dönüşümler (6.7) ve (6.8) ifadelerindeki gibidir. Bu sabit L_{A1} doğrusal dönüşümü için $L_{A_{S1}}$ ="A5" ve L_{A2} doğrusal dönüşümü için ise $L_{A_{S1}}$ ="36" olarak seçilmiştir.

$$L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} \tag{6.7}$$

$$L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{6.8}$$

$X \rightarrow X^7$ tabanlı S-kutusu tasarlanırken önce giriş bitlerine L_{A1} doğrusal dönüşümü, daha sonra $X \rightarrow X^7$ haritalaması doğrusal dönüşüm çıkış koordinatları üzerine uygulanmış ve devamında L_{A2} dönüşümü haritalama çıkışındaki koordinatlara uygulanmıştır. Bu durum Şekil 6.3 ile gösterilmiştir. Buna göre üretilen S-kutusu Tablo 6.7'de gösterilmektedir.



Şekil 6.3: Durum 3'e göre $X \rightarrow X^7$ Haritalaması ile S-kutusu Tasarımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	68	C4	22	04	2B	D8	D5	11	4D	AD	8F	AC	9F	E8	81	88
1	CA	4E	7B	6A	FD	7A	5F	F0	C3	09	59	4F	86	87	67	07
2	8B	EC	7C	3E	5D	CC	C7	CE	49	1F	E3	D9	17	7F	B8	01
3	12	96	ED	53	E5	CB	D0	79	63	D4	62	A6	FF	2A	5C	47
4	28	69	1B	39	08	61	FB	4C	41	3C	26	71	EA	77	25	2F
5	21	31	14	78	4A	2E	18	BD	03	2D	C1	DA	00	92	CD	D7
6	65	30	3A	A3	E6	32	A0	05	89	9D	57	C6	98	C5	37	52
7	54	9B	FE	E2	C9	DB	DD	A1	6C	E0	E4	F2	80	19	DE	60
8	58	D1	2C	7E	38	A8	EB	1D	B3	F3	45	97	23	B2	1A	A4
9	15	10	13	D2	3D	7D	3B	02	8D	43	AA	E9	B6	F5	F9	8A
A	16	74	94	82	48	9A	B4	AF	BB	6D	6E	85	0C	A2	CF	E1
B	B9	9C	BA	F4	FA	33	20	3F	F8	6B	0F	BE	B1	06	F7	DF
C	73	5E	29	36	35	76	BC	70	42	D6	46	A9	EE	DC	51	A5
D	8E	56	5B	AE	BF	55	1E	64	AB	C8	83	84	93	0A	A7	E7
E	8C	95	F1	75	C2	1C	B5	4B	99	44	6F	66	24	F6	B0	0B
F	90	B7	91	34	FC	40	50	D3	0E	EF	27	0D	72	C0	9E	5A

Tablo 6.7: (6.7) ve (6.8) dönüşümleri kullanılarak $X \to X^7$ haritalamasına göre üretilen S-kutusu

$X \to X^7$ üs haritalaması kullanılarak Bölüm 5'te bahsedilen tüm üç durum için S-kutusu tasarlanabilir. Bu durumlardan durum 1 kullanılarak tasarlanan S-kutularının cebirsel ifadesi AES S-kutusunda olduğu gibi 9 terim içerecektir ve cebirsel ifadelerindeki terimlerin üsleri sırası ile 7'nin cyclotomic koset elemanları olacaktır. Bunlarda 7, 14, 28, 56, 112, 224, 193, 131 şeklindedir. Örnek olarak durum 1'e göre tasarlanacak olan S-kutusunun cebirsel ifadesi (6.8)'deki gibi olacaktır.

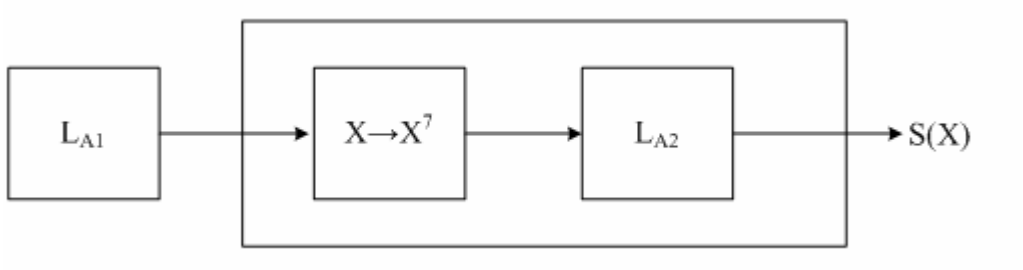
$$S(X) = "a"X^{224} + "b"X^{193} + "c"X^{131} + "d"X^{112} + "e"X^{56} + "f"X^{28} + "g"X^{14} + "h"X^{7} + "i"^{3} \qquad (6.9)$$

Durum 2 düşünüldüğünde ise cebirsel ifade Bölüm 5'teki Teorem 5.2'ye göre verilen formül gereği 93 terim içerecektir. Ayrıca bu terimlerin üsleri 1'den 3'e kadar Hamming ağırlığına sahip üsler olacaktır.

[3] a,b,c, ….., i $GF(2^8)$ 'de cisim elemanlarını temsil etmektedir.

Durum 3 düşünüldüğünde Şekil 6.3'e göre kabaca cebirsel ifade (6.10)'daki ifade gibi olacaktır. Dolayısı ile $[L_{A1}(X)]^{224}$, $[L_{A1}(X)]^{193}$, $[L_{A1}(X)]^{131}$, $[L_{A1}(X)]^{112}$, $[L_{A1}(X)]^{56}$, $[L_{A1}(X)]^{28}$, $[L_{A1}(X)]^{14}$, $[L_{A1}(X)]^{7}$ ifadelerinin her biri durum 2 gibi düşünülebilir ve cebirsel ifadede 93 terim içereceklerdir. Sonuçlanan cebirsel ifade yine 93 terim içerecektir. Cebirsel ifadedeki cebirsel derece ise 224 olacaktır.

$$S(X) = "a"[L_{A1}(X)]^{224} + "b"[L_{A1}(X)]^{193} + "c"[L_{A1}(X)]^{131} + "d"[L_{A1}(X)]^{112} + "e"[L_{A1}(X)]^{56} + "f"[L_{A1}(X)]^{28} + "g"[L_{A1}(X)]^{14} + "h"[L_{A1}(X)]^{7} + "i" \quad (6.10)$$



Şekil 6.3 $X \rightarrow X^7$ Haritalaması ile S-kutusu Tasarımı

$X \rightarrow X^7$ üs haritalaması ile üretilen S-kutusunun bir satırı için DDT dağılımı Tablo 6.5'te, bir satırı için LAT dağılımı ise Tablo 6.6'da gösterilmektedir. Bu üretilen S-kutusu Tablo 4.4'te gösterildiği gibi bir satırı için 6 uniform DDT dağılımı göstermektedir. Yani bir satırda 14 tane 6, 1 tane 4, 84 tane 2 ve 157 tane 0 içermektedir. Bu S-kutusunun bir satırı için LAT dağılımı ise $|32|$ sayısı 1 tane, $|16|$ sayısı 30 tane, $|8|$ sayısı 120 tane ve 0 sayısı 105 tane olacak şekildedir. Buna ek olarak LAT dağılımındaki maksimum mutlak değer göz önüne alındığında bu S-kutusunun doğrusal olmama ölçüsü $NLM_S = 128 - 32 = 96$ olarak elde edilir. Bu da bu S-kutusunun % 80 oranında doğrusal olmama özelliğine sahip olduğunu gösterir.

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	2	0	0	0	2	0	2	0	6	2	0	0	0	0	0
1	2	2	2	0	2	0	6	0	0	2	2	6	2	0	0	4
2	0	0	2	2	0	2	2	2	2	0	2	0	0	2	6	0
3	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0
4	6	2	2	6	0	0	0	0	0	0	0	0	0	0	2	0
5	0	0	2	0	0	2	2	2	0	0	0	0	0	2	0	0
6	2	0	2	2	2	2	0	2	2	2	0	0	2	0	0	0
7	0	0	0	2	0	0	0	2	0	0	2	0	2	2	0	0
8	0	0	0	2	6	0	0	2	0	2	0	0	2	0	0	0
9	2	6	2	2	2	0	0	0	0	6	0	0	0	2	0	0
A	0	0	0	0	0	6	0	0	0	2	0	0	2	0	2	2
B	0	2	2	0	0	0	0	6	0	2	0	2	2	0	6	0
C	0	2	0	0	6	0	0	0	0	2	2	0	2	0	2	2
D	0	0	6	0	2	2	2	0	2	0	0	0	0	2	2	0
E	2	2	0	0	0	0	0	0	0	0	2	2	0	0	0	2
F	0	0	0	2	2	2	2	0	0	0	0	0	0	0	2	0

Tablo 6.8: Tablo 6.7'deki S-kutusunun "01" giriş farkı için DDT dağılımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	-8	0	8	8	0	0	8	-8	-8	0	0	0	0	0	0
1	0	0	-8	-8	0	0	0	0	8	0	-8	0	8	0	0	8
2	0	0	8	-8	0	0	16	0	0	8	0	8	16	-8	-8	0
3	0	-8	0	-8	8	0	0	-8	-16	0	-8	-8	8	-8	8	8
4	8	8	0	16	8	-8	8	8	8	0	8	0	-8	0	0	8
5	-8	0	8	16	0	-8	8	0	-8	8	0	0	16	16	16	0
6	0	8	-16	8	-8	-16	0	8	-8	-8	0	0	16	0	-16	0
7	0	0	8	8	-16	0	0	16	-8	0	8	0	8	0	0	8
8	0	8	0	8	0	8	-8	0	8	-8	-16	-16	-8	8	-8	-8
9	8	8	16	0	0	0	16	0	0	-8	0	-8	8	0	-16	8
A	8	8	0	0	0	0	0	0	-8	0	8	0	-16	-8	8	0
B	-32	8	0	-8	0	8	-8	16	0	0	8	8	0	0	0	0
C	0	0	-8	-8	-8	8	-8	8	0	-8	0	8	-8	0	0	-8
D	8	0	8	16	8	-16	0	-8	8	8	0	0	8	-8	-8	8
E	-16	8	-16	8	0	8	-8	0	8	-8	0	0	8	8	-8	8
F	-8	-8	0	16	0	16	16	-16	-16	-8	0	8	8	0	0	-8

Tablo 6.9: Tablo 6.7'deki S-kutusunun "01" giriş maskesi için LAT dağılımı

SONUÇLAR

Bu tezde sonlu cisim $GF(2^8)$'de üs alma yöntemi ile elde edilen S-kutuları incelenmiştir. Üs alma yöntemi ile tasarlanacak tüm S-kutuları iki önemli kriptografik özellik olan DDT ve LAT dağılımlarına göre sınıflandırılmıştır. Tez çalışmasında görülmüştür ki AES S-kutusu tasarımında kullanılan ters haritalama yöntemi ya da üs fonksiyonu olarak $X \to X^{254}$ haritalaması DDT ve LAT dağılımları açısından gayet iyi sonuçlar vermektedir. Ancak bu S-kutusunun tasarımında kullanılan doğrusal dönüşümün yeri şifre tasarımda olduğu gibi doğrusal olmayan bir yapıdan sonra doğrusal bir dönüşüm gelecek şekildedir. Aslında bu mimari şifre düşünüldüğünde doğrusal ve diferansiyel kriptanalizi zorlaştırmak amacı gütmektedir. Ancak S-kutusu tasarımında bir doğrusal dönüşüm kullanılmasının amacı interpolasyon saldırıları gibi cebirsel saldırıları engelleyici bir amaç gütmektedir. Dolayısı ile ters haritalama işleminden sonra kullanılan doğrusal dönüşüm cebirsel ifadeyi daha karmaşık hale getirmektedir. Fakat bu cebirsel ifade doğrusal dönüşümün ters haritalama işleminden önce kullanılması ya da ek bir doğrusal dönüşümün ters haritalama işleminden önce kullanılması ile geliştirilebileceği bu tezde sonlu cisim teorisi kullanılarak gösterilmiştir. Buna ek olarak bu tezde cebirsel ifadedeki terim sayısının, üs haritalama yöntemi ile durum 2 ve durum 3'e göre tasarlanacak S-kutularının kullanılan üs fonksiyonunun Hamming ağırlığına bağlı olduğu da belirtilmiştir. Örneğin literatürde bulunan $GF(2^7)$'de $X \to X^{81}$ ve $GF(2^9)$'da $X \to X^5$ üs haritalama tabanlı olarak tasarlanmış Misty 1 [65] ve Kasumi [66] S-kutuları düşük Hamming ağırlığına sahip üs fonksiyonlarına sahiptir. Kendi cisimlerinde bu üs fonksiyonları ile beraber durum 2 veya durum 3 S-kutusu tasarımında kullanılsa dahi o cisimde bu S-kutularının cebirsel ifadesinde maksimum terim sayısı mümkün olmayacaktır.

Bu tezde bütün sınıflar için cebirsel ifadesi iyi ve sabit nokta içermeyen 8 bit girişli ve 8 bit çıkışlı S-kutuları $P(X) = X^8 + X^4 + X^3 + X + 1$ polinom tabanlı oluşturulan cisim $GF(2^8)$ de üs haritalama yöntemi kullanılarak elde edilmiş ve bu üretilen S-kutuları Ek B'de verilmiştir.

KAYNAKLAR

[1] FIPS 46-3, *Data Encryption Standard*, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

[2] B. Schneier, *Applied Cryptography - Protocols, Algorithms, and Source code in C*, John Wiley & Sons, Inc., 2nd edition, 1996.

[3] J. Daemen, L. Knudsen, V. Rijmen, *The Block Cipher Square*. Fast Software Encryption (FSE) 1997, Volume 1267 of Lecture Notes in Computer Science: 149–165, Haifa, Israel: Springer-Verlag. Retrieved on 2007-02-15.

[4] FIPS 197, *Advanced Encryption Standard*, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.

[5] Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: *Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis*. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001)

[6] C. De Cannière and B. Preneel, *The Stream Cipher Trivium*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[7] H. Wu, *The Stream Cipher HC-256*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[8] N. Koblitz, (1987). *Elliptic curve cryptosystems.* Mathematics of Computation, 48 (177), 203–209.

[9] H. Dobbertin, A. Bosselaers, and B. Preneel (1996). *RIPEMD-160: A strengthened version of RIPEMD,* Fast Software Encryption, LNCS, vol. 1039, ed. D. Gollmann. Springer-Verlag, Berlin, 71–82.

[10] C.E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, No. 30, pp. 50-64, 1949.

[11] L. Keliher, *Linear Cryptanalysis of Substitution-Permutation Networks*, PHd Thesis, 2003.

[12] L. R. Knudsen, *The Number of Rounds in Block Ciphers*, Public Reports of Nessie Project, May 12,2000.

[13] H. Heys, S. Tavares, *Substitution Permutation Networks Resistant to Differential and LinearCryptanalysis*, JOURNAL OF CRYPTOLOGY ,Vol 9, No 1, pp 1-19, 1996.

[14] K. Nyberg, *Differentially uniform mappings for cryptography, Advances in Cryptology*–EUROCRYPT'93, Springer-Verlag pp. 55-64, 1994.

[15] P. Ekdahl, *On LFSR Based Stream Ciphers*, PHd Thesis, November 2003.

[16] Bluetooth S.I.G, *Specification of Bluetooth System*, v.1.2, 2003. available at: http://www.bluetooth.org/spec.

[17] R. Anderson, *A-5 - the GSM encryption algorithm*, sci-crypt post, 1994.

[18] C. Berbain, O. Billet, A. Canteaut, N. Courtois, B. Debraize, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin and H. Sibert, *The Stream Cipher DECIM*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[19] S. Babbage, M. Dodd, *The Stream Cipher MICKEY*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[20] C. Jansen and A. Kolosha, *The Stream Cipher POMARANCH*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[21] C. De Cannière and B. Preneel, *A Stream Cipher Construction Inspired by Block Cipher Design Principles*, eSTREAM, the ECRYPT Stream Project., 2005, available at: http://www.ecrypt.eu.org/stream.

[22] B. Örencik, *Matematiksel Kriptanaliz*, http://www3.itu.edu.tr/~orencik/

[23] M. T. Sakallı, *Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi*, Doktora tezi, 2006.

[24] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology- EUROCRYPT' 93, Springer-Verlag, pp. 386-397, 1994.

[25] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol 4, No 1 pp. 3-72, 1991.

[26] R.C.-W. Phan, *Impossible Differential Cryptanalysis of 7-round Advanced Encryption Standard (AES)*, Information Processing Letters, Vol. 91, Issue 1, pp. 33-38, 2004.

[27] M. T. Sakallı, E. Buluş, A. Şahin, F. Büyüksaraçoğlu, *Bir Blok Şifreleme Algoritmasına karşı Square Saldırısı*, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, ABG-2005, Istanbul-Türkiye, Haziran-2005

[28] T. Jakobsen, L. Knudsen, *The interpolation attack on block ciphers*, In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 28–40. Springer, Heidelberg (1997)

[29] D. Wagner, *The boomerang attack*, In Lars Ramkilde Knudsen, editor, Proceedings of Fast Software Encryption – FSE'99, number 1636 in Lecture Notes in Computer Science, pages 156–170. Springer-Verlag, 1999.

[30] E. Biham, O. Dunkelman, and N. Keller, *The rectangle attack – rectangling the Serpent* in Proceedings of Eurocrypt'01 (B. Pfitzmann, ed.), no. 2045 in LNCS, pp. 340–357, Springer-Verlag, 2001

[31] J. Kelsey, B. Schneier, D. Wagner, and C. Hall (1998). *Side channel cryptanalysis of product ciphers,* Proc. of ESORICS'98, LNCS, vol. 1485, eds. Quisquater, Deswarte, Meadows, and Gollmann. Springer-Verlag, Louvain la Neuve, Belgium, 97–110.

[32] D. R. Stinson, *Cryptography: Theory and Practice*, Second Edition, CRC Press, 2002.

[33] S. Ling, C. Xing, *Coding Theory: A First Course*, Cambridge University Pres, 2004.

[34] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Revised edition, Cambridge University Press, 1994.

[35] Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü *Ayrık Matematik Ders Notları* http://www.bilmuh.gyte.edu.tr/BIL211/bolum1.pdf

[36] M. T. Sakallı, E. Buluş, F. Büyüksaraçoğlu, A. Şahin, *S-kutularında Doğrusal Eşitlik-Affine equivalence in S-boxes*, IEEE Sinyal işleme ve İletişim Uygulamaları Kurultayı, Antalya-Türkiye, 2006.

[37] J.B. Kam and G.I. Davida, *Structured Design of Substitution Permutation Encryption Networks*, IEEE Transactions on Computers, Vol. C-28, No.10 pp. 747-753, 1979.

[38] S.Kavut and M. D. Yücel, *On Some Cryptographic Properties of Rijndael*, Lecture Notes in Computer Science: Information Assurance in Computer Networks, Methods, Models and Architectures for Network Security, Editors: V.

I. Gorodetski, V. A. Skormin, L. J. Popyack, LNCS Vol.2052, Springer-Verlag, pp.300-311, May 2001.

[39] I. Vergili, *Statistics on Satisfaction of Security Criteria for Randomly Generated S-boxes*, M.S. Thesis, Middle East Technical University, Ankara, Türkiye, 2000.

[40] E. Aras, *Analysis of Security Criteria for Block Ciphers*, M.S. Thesis, Middle East Technical University, Ankara, Türkiye, 1999.

[41] H. Feistel, *Cryptography and Computer Privacy*, Scientific American, Vol. 228, No. 5, pp.15-23, 1973.

[42] A. F. Webster and S.H. Tavares, *On the Design of S-boxes*, Advances in Cryptology: Proceedings of CRYPTO'85, Springer Verlag, New York, pp. 523-534, 1986.

[43] W. Meier and O. Staffelbach, *Nonlinearity Criteria for Cryptographic Functions*, Advances in Cryptology, Proc. EUROCRYPT'89, Springer Verlag, pp. 549-562, 1989.

[44] E. Aras and M. D. Yücel, *Performance Evaluation of Safer K-64 and S-Boxes of Safer Family,* Turkish Journal of Electrical Eng. & Computer Sciences , Vol.9, No. 2, pp.161-175, August 2001.

[45] S. Mister and C. M. Adams, *Practical S-Box Design*, SAC'96- Third Annual Workshop on Selected Areas in Cryptography, Queen's Univ., Kingston, Ontario, Canada, pp. 61-76, August 1996.

[46] M. Matsui, *The First Experimental Cryptanalysis of the Data Encryption Standard*, Advances in Cryptology, CRYPTO'94, Lecturer Notes in Computer Science, Springer-Verlag, pp. 1-11, 1994.

[47] S. Çeçen, *Nonlinearity and Propagation Characteristics of Substitution Boxes,* M.S. Thesis, Middle East Technical University, Ankara, Türkiye, 2001.

[48] H. Heys, *A Tutorial on Linear and Differential Cryptanalysis*, Cryptologia, Vol 26, No 3 pp. 189-221, 2002.

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

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

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

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

[53] 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.

[54] 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.

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

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

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

[58] B. Aslan, M. T. Sakallı, E. Buluş, *Üs Haritalama Tabanlı Cebirsel 8-bit giriş 8-bit çıkışlı S-kutularının Sınıflandırılması*, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, ABG-2008, Girne-Kıbrıs, 2008.

[59] B. Aslan, M. T. Sakallı, E. Buluş, *Classifying 8-Bit to 8-Bit S-Boxes Based on Power Mappings from the Point of DDT and LAT Distributions*, International Workshop on the Arithmetic of Finite Fields, WAIFI 2008, Lecture Notes in Computer Science, Siena-Italy, Springer-Verlag, 2008

[60] A. Braeken, *Cryptographic Properties of Boolean Functions and S-Boxes*, PHd Thesis, March 2006.

[61] T-79.503 *Fundamentals of Cryptology,* available at: http://www.tcs.hut.fi/Studies/T-79.503/handout3.pdf

[62] W. Meier, E. Pasalic, and C.Carlet, *Algebraic Attacks and Decomposition of Boolean Functions*, Eurocrypt 2004, Lecturer Notes in Computer Science, Vol. 3027, Springer-Verlag, pp. 474-491, 2004.

[63] E. Pasalic, *Boolean functions, Definitions, Cryptographic criteria*, avaliable at:

http://www2.mat.dtu.dk/people/E.Pasalic/LecturesPdf/Lectures_BoolDefin.pdf

[64] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Revised Edition, 1994.

[65] M. Matsui, *New Block Encryption MISTY*. In: Biham, E. (ed.) FSE 1997. LNCS, vol. 1267, pp. 54–68. Springer, Heidelberg (1997)

[66] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: Kasumi Specification, V.3.1.1 (2001)

KISALTMALAR

AES	: Advanced Encryption Standard
GF	: Galois Field
DDT	: Difference Distribution Table (Fark Dağılım Tablosu)
LAT	: Lineer Approximation Table (Doğrusal Yaklaşım Tablosu)
DES	: Data Encryption Standard
IDEA	: International Data Encryption Algorithm
SPN	: Substitution-Permutation Network (Yerdeğiştirme-Permütasyon Ağları)
GCD	: Greatest Common Divisor (Ortak Bölenlerin En Büyüğü)
AVAL	: Avalance Criterion (Çığ Ölçütü)
SAC	: Strict Avalanche Criterion (Katı Çığ Ölçütü)
BIC	: Bit Independence Criterion (Bit Bağımsızlık Ölçütü)
NLM	: Nonlinearity Measure (Doğrusal Olmama Parametresi)
MOSAC	: Maximum Order SAC
MOBIC	: Maximum Order BIC
APN	: Almost Perfect Nonlinear (Hemen Hemen Kusursuz Doğrusal Olmayan)
ANF	: Algebraic Normal Form (Cebirsel Gösterim Biçimi)
Tr	: Trace (İz) Fonksiyonu
TS	: Terim Sayısı

ÖZGEÇMİŞ

Bora ASLAN, 12 Eylül 1980 yılında Sarıkamış'ta doğdu. 1998 yılında Trakya Üniversitesi Bilgisayar Mühendisliği kazandı. 2002 yılında mezun oldu. 2003 yılında Lüleburgaz Meslek Yüksekokulunda Bilgisayar Teknolojileri ve Programlama programında öğretim görevlisi olarak göreve başladı. Halen Kırklareli Üniversitesinde öğretim görevlisi olarak çalışmaktadır.

EK A: Tez Esnasında Kullanılan Sonlu Cisim

Tez esnasında birçok S-kutusu oluşturulmuştur. Bu S-kutuları için AES S-kutusunda da kullanılan $p(x) = x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu seçilmiştir. Bu polinomun üreteci $\beta = \alpha + 1$ dir. Buna göre üretilen cismin elemanları aşağıdaki gibi olacaktır.

Üreteç	Binary	Polinom Değeri	Hex.
β^0	00000001	1	01
β^1	00000011	$\alpha+1$	03
β^2	00000101	α^2+1	05
β^3	00001111	$\alpha^3+\alpha^2+\alpha^1+1$	0F
β^4	00010001	α^4+1	11
β^5	00110011	$\alpha^5+\alpha^4+\alpha^1+1$	33
β^6	01010101	$\alpha^6+\alpha^4+\alpha^2+1$	55
β^7	11111111	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	FF
β^8	00011010	$\alpha^4+\alpha^3+\alpha^1$	1A
β^9	00101110	$\alpha^5+\alpha^3+\alpha^2+\alpha^1$	2E
β^{10}	01110010	$\alpha^6+\alpha^5+\alpha^4+\alpha^1$	72
β^{11}	10010110	$\alpha^7+\alpha^4+\alpha^2+\alpha^1$	96
β^{12}	10100001	$\alpha^7+\alpha^5+1$	A1
β^{13}	11111000	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3$	F8
β^{14}	00010011	$\alpha^4+\alpha^1+1$	13
β^{15}	00110101	$\alpha^5+\alpha^4+\alpha^2+1$	35
β^{16}	01011111	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	5F
β^{17}	11100001	$\alpha^7+\alpha^6+\alpha^5+1$	E1
β^{18}	00111000	$\alpha^5+\alpha^4+\alpha^3$	38
β^{19}	01001000	$\alpha^6+\alpha^3$	48
β^{20}	11011000	$\alpha^7+\alpha^6+\alpha^4+\alpha^3$	D8
β^{21}	01110011	$\alpha^6+\alpha^5+\alpha^4+\alpha^1+1$	73
β^{22}	10010101	$\alpha^7+\alpha^4+\alpha^2+1$	95
β^{23}	10100100	$\alpha^7+\alpha^5+\alpha^2$	A4
β^{24}	11110111	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha^1+1$	F7
β^{25}	00000010	α^1	02
β^{26}	00000110	$\alpha^2+\alpha^1$	06
β^{27}	00001010	$\alpha^3+\alpha^1$	0A
β^{28}	00011110	$\alpha^4+\alpha^3+\alpha^2+\alpha^1$	1E
β^{29}	00100010	$\alpha^5+\alpha^1$	22
β^{30}	01100110	$\alpha^6+\alpha^5+\alpha^2+\alpha^1$	66
β^{31}	10101010	$\alpha^7+\alpha^5+\alpha^3+\alpha^1$	AA
β^{32}	11100101	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+1$	E5
β^{33}	00110100	$\alpha^5+\alpha^4+\alpha^2$	34

β^{34}	01011100	$\alpha^6+\alpha^4+\alpha^3+\alpha^2$	5C
β^{35}	11100100	$\alpha^7+\alpha^6+\alpha^5+\alpha^2$	E4
β^{36}	00110111	$\alpha^5+\alpha^4+\alpha^2+\alpha^1+1$	37
β^{37}	01011001	$\alpha^6+\alpha^4+\alpha^3+1$	59
β^{38}	11101011	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^1+1$	EB
β^{39}	00100110	$\alpha^5+\alpha^2+\alpha^1$	26
β^{40}	01101010	$\alpha^6+\alpha^5+\alpha^3+\alpha^1$	6A
β^{41}	10111110	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	BE
β^{42}	11011001	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+1$	D9
β^{43}	01110000	$\alpha^6+\alpha^5+\alpha^4$	70
β^{44}	10010000	$\alpha^7+\alpha^4$	90
β^{45}	10101011	$\alpha^7+\alpha^5+\alpha^3+\alpha^1+1$	AB
β^{46}	11100110	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+\alpha^1$	E6
β^{47}	00110001	$\alpha^5+\alpha^4+1$	31
β^{48}	01010011	$\alpha^6+\alpha^4+\alpha^1+1$	53
β^{49}	11110101	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	F5
β^{50}	00000100	α^2	04
β^{51}	00001100	$\alpha^3+\alpha^2$	0C
β^{52}	00010100	$\alpha^4+\alpha^2$	14
β^{53}	00111100	$\alpha^5+\alpha^4+\alpha^3+\alpha^2$	3C
β^{54}	01000100	$\alpha^6+\alpha^2$	44
β^{55}	11001100	$\alpha^7+\alpha^6+\alpha^3+\alpha^2$	CC
β^{56}	01001111	$\alpha^6+\alpha^3+\alpha^2+\alpha^1+1$	4F
β^{57}	11010001	$\alpha^7+\alpha^6+\alpha^4+1$	D1
β^{58}	01101000	$\alpha^6+\alpha^5+\alpha^3$	68
β^{59}	10111000	$\alpha^7+\alpha^5+\alpha^4+\alpha^3$	B8
β^{60}	11010011	$\alpha^7+\alpha^6+\alpha^4+\alpha^1+1$	D3
β^{61}	01101110	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha^1$	6E
β^{62}	10110010	$\alpha^7+\alpha^5+\alpha^4+\alpha^1$	B2
β^{63}	11001101	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+1$	CD
B^{64}	01001100	$\alpha^6+\alpha^3+\alpha^2$	4C
β^{65}	11010100	$\alpha^7+\alpha^6+\alpha^4+\alpha^2$	D4
β^{66}	01100111	$\alpha^6+\alpha^5+\alpha^2+\alpha^1+1$	67
β^{67}	10101001	$\alpha^7+\alpha^5+\alpha^3+1$	A9
β^{68}	11100000	$\alpha^7+\alpha^6+\alpha^5$	E0
β^{69}	00111011	$\alpha^5+\alpha^4+\alpha^3+\alpha^1+1$	3B
β^{70}	01001101	$\alpha^6+\alpha^3+\alpha^2+1$	4D
β^{71}	11010111	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+\alpha^1+1$	D7
β^{72}	01100010	$\alpha^6+\alpha^5+\alpha^1$	62
β^{73}	10100110	$\alpha^7+\alpha^5+\alpha^2+\alpha^1$	A6
β^{74}	11110001	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+1$	F1
β^{75}	00001000	α^3	08
β^{76}	00011000	$\alpha^4+\alpha^3$	18
β^{77}	00101000	$\alpha^5+\alpha^3$	28
β^{78}	01111000	$\alpha^6+\alpha^5+\alpha^4+\alpha^3$	78
β^{79}	10001000	$\alpha^7+\alpha^3$	88

β^{80}	10000011	$\alpha^7+\alpha^1+1$	83
β^{81}	10011110	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	9E
β^{82}	10111001	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+1$	B9
β^{83}	11010000	$\alpha^7+\alpha^6+\alpha^4$	D0
β^{84}	01101011	$\alpha^6+\alpha^5+\alpha^3+\alpha^1+1$	6B
β^{85}	10111101	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	BD
β^{86}	11011100	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2$	DC
β^{87}	01111111	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	7F
β^{88}	10000001	α^7+1	81
β^{89}	10011000	$\alpha^7+\alpha^4+\alpha^3$	98
β^{90}	10110011	$\alpha^7+\alpha^5+\alpha^4+\alpha^1+1$	B3
β^{91}	11001110	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha^1$	CE
β^{92}	01001001	$\alpha^6+\alpha^3+1$	49
β^{93}	11011011	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^1+1$	DB
β^{94}	01110110	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha^1$	76
β^{95}	10011010	$\alpha^7+\alpha^4+\alpha^3+\alpha^1$	9A
β^{96}	10110101	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+1$	B5
β^{97}	11000100	$\alpha^7+\alpha^6+\alpha^2$	C4
β^{98}	01010111	$\alpha^6+\alpha^4+\alpha^2+\alpha^1+1$	57
β^{99}	11111001	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	F9
β^{100}	00010000	α^4	10
β^{101}	00110000	$\alpha^5+\alpha^4$	30
β^{102}	01010000	$\alpha^6+\alpha^4$	50
β^{103}	11110000	$\alpha^7+\alpha^6+\alpha^5+\alpha^4$	F0
β^{104}	00001011	$\alpha^3+\alpha^1+1$	0B
β^{105}	00011101	$\alpha^4+\alpha^3+\alpha^2+1$	1D
β^{106}	00100111	$\alpha^5+\alpha^2+\alpha^1+1$	27
β^{107}	01101001	$\alpha^6+\alpha^5+\alpha^3+1$	69
β^{108}	10111011	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^1+1$	BB
β^{109}	11010110	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+\alpha^1$	D6
β^{110}	01100001	$\alpha^6+\alpha^5+1$	61
β^{111}	10100011	$\alpha^7+\alpha^5+\alpha^1+1$	A3
β^{112}	11111110	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	FE
β^{113}	00011001	$\alpha^4+\alpha^3+1$	19
B^{114}	00101011	$\alpha^5+\alpha^3+\alpha^1+1$	2B
β^{115}	01111101	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	7D
β^{116}	10000111	$\alpha^7+\alpha^2+\alpha^1+1$	87
β^{117}	10010010	$\alpha^7+\alpha^4+\alpha^1$	92
β^{118}	10101101	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+1$	AD
β^{119}	11101100	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2$	EC
β^{120}	00101111	$\alpha^5+\alpha^3+\alpha^2+\alpha^1+1$	2F
β^{121}	01110001	$\alpha^6+\alpha^5+\alpha^4+1$	71
β^{122}	10010011	$\alpha^7+\alpha^4+\alpha^1+1$	93
β^{123}	10101110	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+\alpha^1$	AE
β^{124}	11101001	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+1$	E9
β^{125}	00100000	α^5	20

β^{126}	01100000	$\alpha^6+\alpha^5$	60
β^{127}	10100000	$\alpha^7+\alpha^5$	A0
β^{128}	11111011	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^1+1$	FB
β^{129}	00010110	$\alpha^4+\alpha^2+\alpha^1$	16
β^{130}	00111010	$\alpha^5+\alpha^4+\alpha^3+\alpha^1$	3A
β^{131}	01001110	$\alpha^6+\alpha^3+\alpha^2+\alpha^1$	4E
β^{132}	11010010	$\alpha^7+\alpha^6+\alpha^4+\alpha^1$	D2
β^{133}	01101101	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$	6D
β^{134}	10110111	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha^1+1$	B7
β^{135}	11000010	$\alpha^7+\alpha^6+\alpha^1$	C2
β^{136}	01011101	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$	5D
β^{137}	11100111	$\alpha^7+\alpha^6+\alpha^5+\alpha^2+\alpha^1+1$	E7
β^{138}	00110010	$\alpha^5+\alpha^4+\alpha^1$	32
β^{139}	01010110	$\alpha^6+\alpha^4+\alpha^2+\alpha^1$	56
β^{140}	11111010	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^1$	FA
β^{141}	00010101	$\alpha^4+\alpha^2+1$	15
β^{142}	00111111	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	3F
β^{143}	01000001	α^6+1	41
β^{144}	11000011	$\alpha^7+\alpha^6+\alpha^1+1$	C3
β^{145}	01011110	$\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	5E
β^{146}	11100010	$\alpha^7+\alpha^6+\alpha^5+\alpha^1$	E2
β^{147}	00111101	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	3D
β^{148}	01000111	$\alpha^6+\alpha^2+\alpha^1+1$	47
β^{149}	11001001	$\alpha^7+\alpha^6+\alpha^3+1$	C9
β^{150}	01000000	α^6	40
β^{151}	11000000	$\alpha^7+\alpha^6$	C0
β^{152}	01011011	$\alpha^6+\alpha^4+\alpha^3+\alpha^1+1$	5B
β^{153}	11101101	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+1$	ED
β^{154}	00101100	$\alpha^5+\alpha^3+\alpha^2$	2C
β^{155}	01110100	$\alpha^6+\alpha^5+\alpha^4+\alpha^2$	74
β^{156}	10011100	$\alpha^7+\alpha^4+\alpha^3+\alpha^2$	9C
β^{157}	10111111	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	BF
β^{158}	11011010	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^1$	DA
β^{159}	01110101	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+1$	75
β^{160}	10011111	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	9F
β^{161}	10111010	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^1$	BA
β^{162}	11010101	$\alpha^7+\alpha^6+\alpha^4+\alpha^2+1$	D5
β^{163}	01100100	$\alpha^6+\alpha^5+\alpha^2$	64
β^{164}	10101100	$\alpha^7+\alpha^5+\alpha^3+\alpha^2$	AC
β^{165}	11101111	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha^1+1$	EF
β^{166}	00101010	$\alpha^5+\alpha^3+\alpha^1$	2A
β^{167}	01111110	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	7E
β^{168}	10000010	$\alpha^7+\alpha^1$	82
β^{169}	10011101	$\alpha^7+\alpha^4+\alpha^3+\alpha^2+1$	9D
β^{170}	10111100	$\alpha^7+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	BC
β^{171}	11011111	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	DF

β^{172}	01111010	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^1$	7A
β^{173}	10001110	$\alpha^7+\alpha^3+\alpha^2+\alpha^1$	8E
β^{174}	10001001	$\alpha^7+\alpha^3+1$	89
β^{175}	10000000	α^7	80
β^{176}	10011011	$\alpha^7+\alpha^4+\alpha^3+\alpha^1+1$	9B
β^{177}	10110110	$\alpha^7+\alpha^5+\alpha^4+\alpha^2+\alpha^1$	B6
β^{178}	11000001	$\alpha^7+\alpha^6+1$	C1
β^{179}	01011000	$\alpha^6+\alpha^4+\alpha^3$	58
β^{180}	11101000	$\alpha^7+\alpha^6+\alpha^5+\alpha^3$	E8
β^{181}	00100011	$\alpha^5+\alpha^1+1$	23
β^{182}	01100101	$\alpha^6+\alpha^5+\alpha^2+1$	65
β^{183}	10101111	$\alpha^7+\alpha^5+\alpha^3+\alpha^2+\alpha^1+1$	AF
β^{184}	11101010	$\alpha^7+\alpha^6+\alpha^5+\alpha^3+\alpha^1$	EA
β^{185}	00100101	$\alpha^5+\alpha^2+1$	25
β^{186}	01101111	$\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha^1+1$	6F
β^{187}	10110001	$\alpha^7+\alpha^5+\alpha^4+1$	B1
β^{188}	11001000	$\alpha^7+\alpha^6+\alpha^3$	C8
β^{189}	01000011	$\alpha^6+\alpha^1+1$	43
β^{190}	11000101	$\alpha^7+\alpha^6+\alpha^2+1$	C5
β^{191}	01010100	$\alpha^6+\alpha^4+\alpha^2$	54
β^{192}	11111100	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	FC
β^{193}	00011111	$\alpha^4+\alpha^3+\alpha^2+\alpha^1+1$	1F
β^{194}	00100001	α^5+1	21
β^{195}	01100011	$\alpha^6+\alpha^5+\alpha^1+1$	63
β^{196}	10100101	$\alpha^7+\alpha^5+\alpha^2+1$	A5
β^{197}	11110100	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2$	F4
β^{198}	00000111	$\alpha^2+\alpha^1+1$	07
β^{199}	00001001	α^3+1	09
β^{200}	00011011	$\alpha^4+\alpha^3+\alpha^1+1$	1B
β^{201}	00101101	$\alpha^5+\alpha^3+\alpha^2+1$	2D
β^{202}	01110111	$\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha^1+1$	77
β^{203}	10011001	$\alpha^7+\alpha^4+\alpha^3+1$	99
β^{204}	10110000	$\alpha^7+\alpha^5+\alpha^4$	B0
β^{205}	11001011	$\alpha^7+\alpha^6+\alpha^3+\alpha^1+1$	CB
β^{206}	01000110	$\alpha^6+\alpha^2+\alpha^1$	46
β^{207}	11001010	$\alpha^7+\alpha^6+\alpha^3+\alpha^1$	CA
β^{208}	01000101	$\alpha^6+\alpha^2+1$	45
β^{209}	11001111	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+\alpha^1+1$	CF
β^{210}	01001010	$\alpha^6+\alpha^3+\alpha^1$	4A
β^{211}	11011110	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	DE
β^{212}	01111001	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+1$	79
β^{213}	10001011	$\alpha^7+\alpha^3+\alpha^1+1$	8B
β^{214}	10000110	$\alpha^7+\alpha^2+\alpha^1$	86
β^{215}	10010001	$\alpha^7+\alpha^4+1$	91
β^{216}	10101000	$\alpha^7+\alpha^5+\alpha^3$	A8
β^{217}	11100011	$\alpha^7+\alpha^6+\alpha^5+\alpha^1+1$	E3

β^{218}	00111110	$\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha^1$	3E
β^{219}	01000010	$\alpha^6+\alpha^1$	42
β^{220}	11000110	$\alpha^7+\alpha^6+\alpha^2+\alpha^1$	C6
β^{221}	01010001	$\alpha^6+\alpha^4+1$	51
β^{222}	11110011	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^1+1$	F3
β^{223}	00001110	$\alpha^3+\alpha^2+\alpha^1$	0E
β^{224}	00010010	$\alpha^4+\alpha^1$	12
β^{225}	00110110	$\alpha^5+\alpha^4+\alpha^2+\alpha^1$	36
β^{232}	10001111	$\alpha^7+\alpha^3+\alpha^2+\alpha^1+1$	8F
β^{233}	10001010	$\alpha^7+\alpha^3+\alpha^1$	8A
β^{234}	10000101	$\alpha^7+\alpha^2+1$	85
β^{235}	10010100	$\alpha^7+\alpha^4+\alpha^2$	94
β^{236}	10100111	$\alpha^7+\alpha^5+\alpha^2+\alpha^1+1$	A7
β^{237}	11110010	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^1$	F2
β^{238}	00001101	$\alpha^3+\alpha^2+1$	0D
β^{239}	00010111	$\alpha^4+\alpha^2+\alpha^1+1$	17
β^{240}	00111001	$\alpha^5+\alpha^4+\alpha^3+1$	39
β^{241}	01001011	$\alpha^6+\alpha^3+\alpha^1+1$	4B
β^{242}	11011101	$\alpha^7+\alpha^6+\alpha^4+\alpha^3+\alpha^2+1$	DD
β^{243}	01111100	$\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2$	7C
β^{244}	10000100	$\alpha^7+\alpha^2$	84
β^{245}	10010111	$\alpha^7+\alpha^4+\alpha^2+\alpha^1+1$	97
β^{246}	10100010	$\alpha^7+\alpha^5+\alpha^1$	A2
β^{247}	11111101	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^3+\alpha^2+1$	FD
β^{248}	00011100	$\alpha^4+\alpha^3+\alpha^2$	1C
β^{249}	00100100	$\alpha^5+\alpha^2$	24
β^{250}	01101100	$\alpha^6+\alpha^5+\alpha^3+\alpha^2$	6C
β^{251}	10110100	$\alpha^7+\alpha^5+\alpha^4+\alpha^2$	B4
β^{252}	11000111	$\alpha^7+\alpha^6+\alpha^2+\alpha^1+1$	C7
β^{253}	01010010	$\alpha^6+\alpha^4+\alpha^1$	52
β^{254}	11110110	$\alpha^7+\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha^1$	F6
β^{255}	00000001	1	01

EK B: Çeşitli S-kutuları

Durum 3'e göre tez çalışması esnasında $GF(2^8)$'de üs haritalama yöntemi ile üretirilen S-kutuları aşağıda verilmektedir. Bu S-kutuları tasarlanırken önce giriş bitlerine L_{A1} doğrusal dönüşümü, daha sonra sonlu cisimde üs haritalama doğrusal dönüşüm çıkış koordinatları üzerine ve son olarak L_{A2} dönüşümü haritalama çıkışındaki koordinatlara uygulanmıştır. L_{A1} doğrusal dönüşümü için $L_{A_{S1}}$ ="33" doğrusal dönüşüm sabiti kullanılmıştır. L_{A2} doğrusal dönüşümü için $L_{A_{S2}}$ doğrusal dönüşüm sabiti için her S-kutusunda farklı bir değer kullanılmıştır. Böylelikle sabit nokta içermeyen S-kutuları üretilmiştir.

$$L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + L_{A_{S1}}$$

$$L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + L_{A_{S2}}$$

$X \rightarrow X^3$ Üs Haritalaması $L_{A_{S2}}$ ="47"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	36	FA	C6	31	2D	4C	5D	07	E1	77	12	BF	C9	F2	BA	BA
1	E1	9D	46	01	50	81	77	9D	98	BE	3C	21	1A	91	3E	8E
2	14	42	D3	BE	07	FC	40	80	7D	71	B9	8E	5D	FC	19	83
3	6A	8C	FA	27	D3	98	C3	B3	AD	11	3E	B9	27	36	34	1E
4	3F	CE	3E	F4	5B	07	DA	BD	0A	A1	08	98	5D	5B	DF	E2
5	D8	99	8E	F4	16	FA	C0	17	43	58	16	36	BE	08	6B	E6
6	9D	F6	AB	FB	F1	37	47	BA	16	27	23	29	49	D5	FC	5B
7	D3	08	B2	52	15	63	F4	B9	F6	77	94	2E	03	2F	E1	F6
8	71	CE	91	15	23	31	43	6A	23	C6	C0	1E	42	0A	21	52
9	1A	15	AD	99	E2	40	D5	4C	E6	B3	52	3C	2D	D5	19	DA
A	C3	E6	14	0A	99	11	CE	7D	2F	50	FB	BF	46	94	12	FB
B	01	94	81	2F	F1	C9	F1	F2	43	8C	C0	34	80	E2	83	DA
C	03	81	12	AB	2E	01	BF	AB	B3	6B	A1	42	AD	D8	3F	71
D	58	6A	1E	17	DF	40	19	BD	46	2E	03	50	F2	37	37	C9
E	31	29	17	34	14	A1	B2	3C	3F	7D	1A	63	29	C6	8C	58
F	C3	6B	B2	21	4C	49	BD	83	63	91	11	D8	DF	80	2D	49

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
1	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
2	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
3	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
4	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
5	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
6	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
7	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
8	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
9	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
A	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
B	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
C	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
D	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0
E	2	0	0	2	0	2	2	0	0	2	2	0	2	0	0	2
F	0	2	2	0	2	0	0	2	2	0	0	2	0	2	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	-8	0	0	0	-8	8	8	8	-8	8	16	-16	-8	8
1	0	-8	8	8	0	0	-8	16	8	-8	-8	8	0	-8	8	0
2	8	0	-16	8	0	-8	-8	0	8	8	-8	8	-8	-8	0	16
3	-8	0	-8	8	8	0	8	8	8	-8	8	-8	0	8	-8	0
4	0	16	-8	-8	0	8	-16	0	-8	16	-8	0	-8	8	-8	0
5	-8	-16	8	0	-8	0	-8	8	-8	0	-8	8	8	-8	0	0
6	-8	8	8	-8	8	-8	8	-16	0	0	8	-8	-16	8	0	0
7	-8	-8	0	0	-8	0	8	-8	-8	0	8	-8	8	8	-8	-8
8	8	8	-8	-8	-8	-8	-8	8	-8	8	-8	8	-8	-8	-8	8
9	-8	-8	-8	8	0	-8	0	8	16	-8	-8	-8	8	0	0	0
A	8	0	8	-16	0	-8	0	-8	8	0	-8	0	-8	-8	8	-8
B	0	-8	-16	8	-8	-8	8	8	-8	-8	8	0	8	0	-8	8
C	16	-8	0	8	16	-8	0	0	0	0	8	8	16	-8	-8	8
D	-8	0	8	8	8	0	-16	8	8	-8	0	0	8	8	8	0
E	8	16	0	8	8	0	-8	-8	8	16	-8	0	0	8	-8	8
F	-8	-8	8	0	-8	8	8	8	-8	-8	8	8	16	8	0	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^9$ Üs Haritalaması $L_{A_{S2}}$ ="C5"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	70	9B	D2	02	5D	0C	51	3B	D9	58	2F	95	88	B3	D0	D0
1	D9	CE	83	AF	AC	01	58	CE	31	4C	3F	79	38	FF	98	64
2	A3	3D	E9	4C	3B	1F	DF	C0	B5	41	AB	64	51	1F	E1	94
3	29	4B	9B	C2	E9	31	F5	16	7E	76	98	AB	C2	70	8A	03
4	A5	44	98	42	60	3B	F3	93	E8	63	81	31	51	60	96	9C
5	A1	BC	64	42	3C	9B	57	CB	AD	DA	3C	70	4C	81	73	85
6	CE	5A	1B	B4	BE	90	C5	D0	3C	C2	BD	78	30	74	1F	60
7	E9	81	C4	97	C1	13	42	AB	5A	58	23	1A	0E	B6	D9	5A
8	41	44	FF	C1	BD	02	AD	29	BD	D2	57	03	3D	E8	79	97
9	38	C1	7E	BC	9C	DF	74	0C	85	16	97	3F	5D	74	E1	F3
A	F5	85	A3	E8	BC	76	44	B5	B6	AC	B4	95	83	23	2F	B4
B	AF	23	01	B6	BE	88	BE	B3	AD	4B	57	8A	C0	9C	94	F3
C	0E	01	2F	1B	1A	AF	95	1B	16	73	63	3D	7E	A1	A5	41
D	DA	29	03	CB	96	DF	E1	93	83	1A	0E	AC	B3	90	90	88
E	02	78	CB	8A	A3	63	C4	3F	A5	B5	38	13	78	D2	4B	DA
F	F5	73	C4	79	0C	30	93	94	13	FF	76	A1	96	C0	5D	30

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
1	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
2	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
3	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
4	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
5	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
6	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
7	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
8	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
9	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
A	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
B	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
C	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
D	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
E	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
F	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	8	-16	-16	0	8	8	-8	-8	-8	8	0	0	-8	-8
1	0	-8	-8	8	0	0	-8	0	8	8	8	8	0	-8	-8	16
2	-8	0	0	8	0	-8	8	0	8	8	-8	8	-8	-8	0	0
3	-8	16	-8	8	-8	0	-8	8	-8	-8	8	8	0	8	-8	0
4	0	16	-8	8	0	8	0	16	-8	0	-8	0	8	-8	-8	0
5	8	-16	-8	0	-8	0	-8	8	8	0	8	8	8	8	0	0
6	-8	8	-8	-8	8	-8	8	0	0	0	8	-8	0	8	0	0
7	8	-8	0	0	8	-16	8	-8	-8	0	-8	8	8	8	8	-8
8	-8	8	-8	8	-8	8	8	-8	-8	-8	8	-8	8	8	8	-8
9	-8	8	-8	-8	0	8	16	8	-16	8	8	-8	-8	0	0	0
A	8	-16	8	-16	0	8	0	8	8	0	8	16	8	8	8	-8
B	0	8	0	-8	8	-8	8	8	-8	-8	-8	0	-8	0	-8	8
C	0	8	16	8	0	-8	0	-16	0	0	8	-8	-16	8	-8	8
D	8	0	-8	-8	-8	0	16	-8	-8	8	16	0	8	-8	8	-16
E	-8	0	0	-8	-8	0	-8	8	-8	0	8	16	0	8	-8	-8
F	8	8	8	0	-8	8	-8	8	8	-8	-8	-8	-16	-8	0	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{39}$ Üs Haritalaması $L_{A_{S2}}$ ="C5"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C0	B6	13	95	79	98	D9	97	CE	58	E8	C4	57	3D	DF	DF
1	CE	BC	96	A3	FF	3B	58	BC	90	9B	01	B3	C2	0E	A5	38
2	70	30	60	9B	97	1B	63	CB	4B	41	C1	38	D9	1B	8A	AB
3	5A	42	B6	23	60	90	F5	2F	29	3C	A5	C1	23	C0	3F	85
4	16	E1	A5	4C	0C	97	F3	94	74	1F	93	90	D9	0C	B4	64
5	1A	BD	38	4C	78	B6	44	83	73	DA	78	C0	9B	93	9C	D0
6	BC	AC	A1	02	03	88	C5	DF	78	23	31	AD	AF	D2	1B	0C
7	60	93	5D	51	E9	81	4C	C1	AC	58	7E	B5	76	BE	CE	AC
8	41	E1	0E	E9	31	95	73	5A	31	13	44	85	30	74	B3	51
9	C2	E9	29	BD	64	63	D2	98	D0	2F	51	01	79	D2	8A	F3
A	F5	D0	70	74	BD	3C	E1	4B	BE	FF	02	C4	96	7E	E8	02
B	A3	7E	3B	BE	03	57	03	3D	73	42	44	3F	CB	64	AB	F3
C	76	3B	E8	A1	B5	A3	C4	A1	2F	9C	1F	30	29	1A	16	41
D	DA	5A	85	83	B4	63	8A	94	96	B5	76	FF	3D	88	88	57
E	95	AD	83	3F	70	1F	5D	01	16	4B	C2	81	AD	13	42	DA
F	F5	9C	5D	B3	98	AF	94	AB	81	0E	3C	1A	B4	CB	79	AF

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	0	0	2	2	0	2	2	2	0	2	2	2	0	0	0
1	2	0	0	0	0	2	2	2	2	0	2	0	0	0	2	0
2	0	2	2	2	0	2	2	0	0	2	0	2	2	0	0	2
3	0	2	0	2	0	2	0	2	2	0	0	0	0	0	2	2
4	2	2	0	2	2	0	0	0	0	2	2	0	2	2	2	0
5	2	0	0	0	2	0	0	2	2	0	0	2	2	2	0	0
6	0	0	2	0	2	2	0	2	2	2	2	2	0	0	0	2
7	0	0	2	0	2	0	2	0	0	2	0	2	0	2	0	2
8	2	2	0	0	0	2	2	0	0	2	0	2	2	2	0	2
9	0	0	0	0	2	2	2	0	2	0	0	2	2	2	0	0
A	2	0	0	2	2	0	0	2	2	2	2	2	0	0	0	2
B	0	0	2	2	0	2	0	0	2	0	2	0	2	0	2	0
C	0	2	2	0	2	0	2	2	2	0	0	2	2	0	2	0
D	2	0	0	0	0	2	2	2	0	0	2	0	0	2	0	2
E	0	2	2	2	2	0	0	2	2	2	2	0	0	0	2	0
F	2	0	0	2	2	0	0	2	0	2	0	2	0	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	8	-16	0	0	8	8	8	8	-8	8	-16	0	-8	8
1	0	8	-8	8	0	16	-8	0	-8	-8	8	8	0	8	-8	0
2	-8	0	-16	-8	-16	-8	-8	0	-8	8	-8	8	8	-8	0	0
3	8	0	-8	8	8	0	-8	-8	8	-8	8	8	0	-8	-8	0
4	-16	0	-8	-8	0	-8	0	-16	8	0	8	0	-8	-8	8	0
5	8	-16	8	0	8	0	-8	8	-8	0	-8	8	-8	8	0	16
6	8	8	-8	8	8	8	8	16	0	0	-8	-8	0	-8	16	16
7	-8	-8	0	16	8	0	-8	-8	-8	0	8	8	8	-8	8	-8
8	8	-8	8	8	8	-8	8	8	8	8	-8	8	8	-8	8	8
9	-8	-8	8	8	0	-8	0	-8	0	8	8	8	-8	0	0	0
A	-8	0	8	16	-16	8	-16	8	8	0	8	0	-8	-8	-8	-8
B	0	-8	0	8	8	-8	8	8	8	-8	-8	0	-8	-16	-8	8
C	0	-8	0	-8	0	-8	0	0	0	-16	-8	-8	0	8	-8	-8
D	8	0	-8	8	8	0	0	8	-8	8	-16	0	8	-8	-8	0
E	8	0	0	8	8	0	8	8	8	0	-8	0	0	8	-8	8
F	-8	-8	-8	-16	-8	8	-8	8	8	-8	8	-8	16	8	0	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^5$ Üs Haritalaması L_{AS2} ="A9"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	97	A7	F9	35	15	7D	38	AC	42	B6	42	4A	26	8A	65	35
1	FA	D8	11	CF	07	7D	AF	29	4A	AC	CF	D5	51	EF	97	D5
2	1C	F5	82	97	97	26	4A	07	82	AF	72	A3	EF	9A	5C	D5
3	1C	E7	07	00	E8	4B	B0	EF	E7	D8	92	51	F5	92	C3	58
4	A7	8A	AC	7D	E7	92	AF	26	D8	31	BD	A8	7E	CF	58	15
5	51	6E	DF	1C	6E	09	A3	38	4B	B0	AB	AC	92	31	31	6E
6	58	AC	A3	AB	11	BD	A9	F9	6C	5C	F9	35	C3	AB	15	81
7	C3	25	BD	A7	F5	4B	C8	8A	92	B0	82	5C	42	38	11	97
8	B6	72	38	00	65	F9	A8	C8	35	35	D5	29	00	58	A3	07
9	8A	5C	81	AB	26	A8	6E	1C	6C	7E	09	E7	26	6C	00	B6
A	B6	AB	C8	29	6C	29	51	E8	7E	A7	6E	4B	42	C3	11	6C
B	E7	E8	1C	EF	42	15	FA	51	4A	81	DF	E8	09	9A	DF	B0
C	11	C8	FA	DF	00	81	A8	D5	38	25	BD	5C	CF	8A	09	B0
D	B6	7D	D8	EF	D8	4B	F5	9A	FA	F5	FA	09	72	25	31	9A
E	65	65	7E	82	7D	25	25	81	07	C3	72	4A	F9	65	CF	AF
F	AF	BD	31	DF	C8	82	15	A3	A8	7E	58	72	29	A7	9A	E8

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4
1	0	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0
2	0	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0
3	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4
4	0	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0
5	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4
6	4	0	0	0	0	0	0	4	4	0	0	0	0	0	0	4
7	0	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0
8	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4	0
9	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0
A	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0
B	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4	0
C	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0
D	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4	0
E	0	4	0	0	0	0	4	0	0	4	0	0	0	0	4	0
F	0	0	0	4	4	0	0	0	0	0	0	4	4	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	-8	-8	8	0	8	-8	8	0	-8	0	8	-8	-8	-8
1	-8	8	0	0	-8	8	-8	8	8	8	-8	8	8	8	-8	8
2	8	-8	8	8	0	8	8	0	8	8	-8	-8	8	8	-8	-8
3	8	8	-8	0	0	8	-8	-8	-8	0	-8	0	-8	8	-8	8
4	-8	-8	8	8	-8	-8	8	8	0	8	-8	-8	8	-8	0	-8
5	-8	8	-8	8	8	8	8	8	-8	8	8	8	-8	-8	-8	8
6	8	-8	8	0	-8	-8	-8	0	8	-8	8	0	-8	32	8	8
7	-8	-8	0	8	-8	-8	0	8	-8	8	-8	8	-8	8	8	-8
8	8	8	0	0	8	0	8	-8	8	-8	8	-8	8	0	8	-8
9	8	8	-8	0	-8	8	-8	-8	-8	0	-8	0	0	0	8	0
A	8	-8	8	-32	8	8	-8	-8	8	-8	8	8	-8	-8	0	8
B	-8	8	0	0	8	0	8	-8	8	8	-8	8	8	8	-8	0
C	8	0	0	8	8	-8	0	-8	-8	-8	8	8	0	-8	32	0
D	-8	-8	-8	8	-8	-8	0	8	8	0	0	0	-8	8	8	-8
E	8	-8	8	0	0	-8	8	0	-8	-8	8	-8	0	-8	-8	8
F	8	-8	8	0	8	8	8	8	-8	0	8	8	-8	-8	-8	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{21}$ Üs Haritalaması $L_{A_{S2}}$ ="93"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F9	5A	55	C0	C3	E3	0C	28	FA	17	CD	E2	FB	0B	BE	BE
1	FA	A9	96	6B	57	75	17	A9	6A	36	94	92	DE	6D	1D	C6
2	66	2F	F7	36	28	45	22	F5	FD	0E	49	C6	0C	45	32	35
3	DC	97	5A	01	F7	6A	A5	1A	B7	07	1D	49	01	F9	6E	40
4	14	CA	1D	BF	4C	28	A3	89	E0	84	86	6A	0C	4C	9D	67
5	C5	58	C6	BF	8F	5A	25	26	EA	8C	8F	F9	36	86	EB	79
6	A9	69	D7	D5	F3	2E	93	BE	8F	01	20	98	E5	E8	45	4C
7	F7	86	54	7F	4D	D3	BF	49	69	17	12	C2	C1	CE	FA	69
8	0E	CA	6D	4D	20	C0	EA	DC	20	55	25	40	2F	E0	92	7F
9	DE	4D	B7	58	67	22	E8	E3	79	1A	7F	94	C3	E8	32	A3
A	A5	79	66	E0	58	07	CA	FD	CE	57	D5	E2	96	12	CD	D5
B	6B	12	75	CE	F3	FB	F3	0B	EA	97	25	6E	F5	67	35	A3
C	C1	75	CD	D7	C2	6B	E2	D7	1A	EB	84	2F	B7	C5	14	0E
D	8C	DC	40	26	9D	22	32	89	96	C2	C1	57	0B	2E	2E	FB
E	C0	98	26	6E	66	84	54	94	14	FD	DE	D3	98	55	97	8C
F	A5	EB	54	92	E3	E5	89	35	D3	6D	07	C5	9D	F5	C3	E5

S-kutusu

0	2	0	2	2	0	0	4	2	2	2	0	2	0	4	0	2
1	0	0	0	0	0	0	0	0	2	0	4	2	0	0	0	0
2	4	0	2	0	2	2	2	0	0	0	2	4	0	2	2	2
3	0	0	0	0	0	2	2	4	0	0	0	0	0	0	0	0
4	2	0	0	0	0	2	0	0	2	4	0	4	0	0	2	0
5	2	0	0	2	4	0	0	0	2	0	0	2	2	0	0	2
6	0	0	0	2	4	2	4	0	2	0	0	0	0	2	0	0
7	0	2	2	0	0	2	2	0	0	4	0	0	0	2	2	0
8	0	0	0	0	2	0	2	0	0	0	0	0	0	0	2	2
9	0	2	4	4	0	2	4	0	0	2	0	0	0	4	2	0
A	0	0	2	2	0	0	0	0	0	2	0	2	0	0	0	0
B	4	0	0	2	2	0	0	0	2	0	0	4	2	0	4	4
C	4	2	2	0	2	0	2	0	0	0	0	0	0	2	0	2
D	2	0	0	0	0	4	0	2	0	0	0	2	2	2	2	0
E	2	0	2	0	0	0	0	0	0	2	0	2	2	4	0	2
F	2	2	0	2	0	0	2	0	4	0	2	0	0	2	0	0

"01" Giriş Farkı için DDT Dağılımı

0	0	0	0	0	-8	0	-8	0	8	0	0	8	8	-16	8	0
1	-8	-8	8	0	0	8	0	0	0	-8	8	-16	0	0	0	16
2	0	-8	8	0	-8	-16	0	8	-16	16	0	0	16	-16	-8	-8
3	0	-8	-16	16	16	8	0	-16	0	-16	-16	0	8	0	0	-8
4	8	-8	16	0	-8	16	-8	8	0	8	0	-8	0	16	0	8
5	0	8	0	8	0	8	0	0	0	-8	16	0	0	16	-8	8
6	0	8	-8	0	-8	0	0	0	-8	0	-8	0	0	-16	8	16
7	-8	16	-8	0	0	0	8	-16	-8	8	0	-8	0	8	-8	0
8	-8	16	16	8	0	-8	-8	0	8	16	0	-8	0	8	-8	0
9	0	8	-8	0	0	0	8	8	8	-8	-8	0	-8	8	8	16
A	0	8	0	8	-8	0	-8	-16	0	-8	0	8	-16	0	0	0
B	-8	16	-8	-16	0	0	0	0	-16	0	0	-8	0	8	0	0
C	8	0	8	0	8	0	-8	-8	-8	-8	0	16	8	0	0	0
D	0	-8	16	0	0	-8	-8	0	0	0	-8	8	0	0	16	8
E	0	0	16	0	-8	-8	0	8	0	0	-8	-8	0	0	0	-8
F	8	0	0	0	0	-8	-8	0	8	0	-16	-8	8	-8	0	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{95}$ Üs Haritalaması L_{AS2} ="27"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2D	DF	22	1C	74	A8	7B	51	0C	38	0C	89	CC	E2	19	1C
1	4D	41	66	BF	04	A8	21	0F	89	51	BF	A7	E0	D2	2D	A7
2	9B	EB	C5	2D	2D	CC	89	04	C5	21	25	D6	D2	9F	77	A7
3	9B	AB	04	BB	C4	87	3E	D2	AB	41	5B	E0	EB	5B	26	69
4	DF	E2	51	A8	AB	5B	21	CC	41	61	F0	29	8E	BF	69	74
5	E0	92	56	9B	92	FC	D6	7B	87	3E	F3	51	5B	61	61	92
6	69	51	D6	F3	66	F0	27	22	46	77	22	1C	26	F3	74	33
7	26	B6	F0	DF	EB	87	14	E2	5B	3E	C5	77	0C	7B	66	2D
8	38	25	7B	BB	19	22	29	14	1C	1C	A7	0F	BB	69	D6	04
9	E2	77	33	F3	CC	29	92	9B	46	8E	FC	AB	CC	46	BB	38
A	38	F3	14	0F	46	0F	E0	C4	8E	DF	92	87	0C	26	66	46
B	AB	C4	9B	D2	0C	74	4D	E0	89	33	56	C4	FC	9F	56	3E
C	66	14	4D	56	BB	33	29	A7	7B	B6	F0	77	BF	E2	FC	3E
D	38	A8	41	D2	41	87	EB	9F	4D	EB	4D	FC	25	B6	61	9F
E	19	19	8E	C5	A8	B6	B6	33	04	26	25	89	22	19	BF	21
F	21	F0	61	56	14	C5	74	D6	29	8E	69	25	0F	DF	9F	C4

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	0	0	0	0	4	0	0	0	2	0	0	2	0	0	0
1	0	0	0	0	0	2	0	0	2	0	0	4	0	4	2	0
2	4	0	2	0	2	2	0	0	0	0	4	0	0	0	4	2
3	2	4	2	0	2	0	0	2	2	0	2	4	0	4	4	0
4	0	0	0	2	0	0	0	2	0	4	0	4	2	2	0	2
5	0	2	0	0	0	0	0	2	0	0	0	2	0	2	0	0
6	0	0	0	2	0	2	0	0	2	0	0	0	2	0	2	2
7	2	0	4	0	2	0	0	2	2	0	0	0	0	0	0	0
8	0	0	0	2	0	4	0	2	2	0	4	0	0	2	2	0
9	4	0	2	4	0	2	2	0	0	0	0	0	0	0	2	0
A	0	0	4	0	0	0	2	2	2	0	0	0	4	4	0	0
B	2	2	2	0	0	0	0	0	0	2	2	2	0	0	0	2
C	4	0	2	0	0	0	2	0	2	0	0	2	0	4	0	0
D	4	4	4	0	0	2	0	0	2	4	0	0	2	0	0	0
E	0	2	0	0	2	2	0	0	2	0	2	0	2	2	0	0
F	2	0	2	4	0	0	2	0	0	2	0	0	0	0	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	4	16	-12	0	-12	-8	12	-8	12	0	-4	-8	4	16	4
1	16	-4	0	-12	-8	-12	0	4	0	-4	-8	-4	16	-4	8	12
2	0	4	0	-4	0	-4	-8	12	0	-12	-16	12	0	4	0	-4
3	0	4	16	4	0	12	-8	-12	-16	-4	0	-12	16	4	0	-4
4	-4	0	4	0	12	0	-12	-16	4	0	4	0	4	8	-12	-8
5	-4	16	4	0	-4	-16	-12	0	-4	0	4	0	4	8	-4	8
6	4	16	4	0	4	-16	4	0	4	0	4	0	-4	0	-4	0
7	-4	8	4	16	-4	-8	4	0	-4	-8	-4	0	-12	0	4	8
8	16	4	0	-4	-8	4	0	-4	8	12	-16	-4	-8	-12	0	-4
9	16	4	8	-4	-8	-4	0	-4	8	-12	-16	4	0	4	16	-12
A	0	-4	0	12	-8	4	-8	-4	-8	4	8	12	8	4	0	-4
B	-8	4	16	4	0	-12	-16	4	0	-4	0	4	0	-4	16	-4
C	-4	0	12	8	-4	8	12	-8	4	-16	-4	0	-12	8	12	0
D	4	0	-4	16	4	0	-12	0	-4	-16	-4	0	4	16	-4	0
E	-4	0	-4	0	4	-16	-4	0	4	-8	4	0	4	0	-4	8
F	-4	16	-4	0	-4	0	-4	-8	4	0	-12	-16	-4	16	12	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{111}$ Üs Haritalaması L_{AS2} ="47"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	F2	27	52	80	DF	C0	7D	D8	8C	C3	3C	17	1E	31	50	50
1	8C	F4	01	2D	15	AB	C3	F4	2F	1A	FC	FB	C6	D3	CE	D5
2	21	BF	37	1A	D8	11	91	42	6B	DA	23	D5	7D	11	40	99
3	83	E2	27	63	37	2F	71	34	BD	4C	CE	23	63	F2	A1	6A
4	19	BA	CE	8E	C9	D8	77	9D	81	03	E1	2F	7D	C9	14	0A
5	29	BE	D5	8E	3E	27	E6	49	B3	58	3E	F2	1A	E1	12	F6
6	F4	B9	16	36	AD	F1	47	50	3E	63	FA	3F	B2	07	11	C9
7	37	E1	46	2E	98	5D	8E	23	B9	C3	08	43	5B	94	8C	B9
8	DA	BA	D3	98	FA	80	B3	83	FA	52	E6	6A	BF	81	FB	2E
9	C6	98	BD	BE	0A	91	07	C0	F6	34	2E	FC	DF	07	40	77
A	71	F6	21	81	BE	4C	BA	6B	94	15	36	17	01	08	3C	36
B	2D	08	AB	94	AD	1E	AD	31	B3	E2	E6	A1	42	0A	99	77
C	5B	AB	3C	16	43	2D	17	16	34	12	03	BF	BD	29	19	DA
D	58	83	6A	49	14	91	40	9D	01	43	5B	15	31	F1	F1	1E
E	80	3F	49	A1	21	03	46	FC	19	6B	C6	5D	3F	52	E2	58
F	71	12	46	FB	C0	B2	9D	99	5D	D3	4C	29	14	42	DF	B2

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	2	0	2	2	0	0	2	0	2	2	0	0	0	0	0
1	0	2	0	0	0	2	0	2	2	2	0	2	0	0	2	2
2	2	2	2	2	0	2	2	0	0	0	2	2	2	2	0	2
3	2	0	0	0	0	4	0	4	0	0	0	0	0	0	2	2
4	2	0	2	0	2	2	0	2	2	0	0	4	0	2	2	2
5	0	2	0	0	0	0	2	0	0	0	0	2	2	2	2	0
6	2	2	0	2	0	2	0	0	2	0	0	0	2	4	2	0
7	0	0	4	0	0	0	0	0	2	0	4	0	0	0	0	0
8	0	2	2	0	0	2	0	2	0	0	0	0	2	0	2	0
9	0	2	0	0	2	0	0	2	0	0	0	4	2	0	2	0
A	2	0	0	2	0	2	0	0	2	0	0	0	0	2	0	2
B	0	2	0	2	2	2	0	0	0	0	4	0	2	2	2	2
C	2	0	2	2	0	4	0	2	0	2	0	2	2	0	2	2
D	0	2	4	2	0	4	2	0	4	2	0	2	0	2	0	0
E	0	0	0	0	2	0	0	0	2	0	2	2	0	2	2	2
F	2	2	2	0	0	0	2	0	0	0	0	2	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	4	-4	-16	-8	4	4	-4	4	0	0	4	-4	16	0
1	0	16	4	-12	-8	0	12	4	12	4	0	-16	-4	-4	8	0
2	-4	4	-8	8	-4	-12	8	-8	0	16	12	-12	-8	8	-4	4
3	12	4	0	-8	-4	4	0	8	0	-16	-4	4	8	0	12	-4
4	-4	-4	16	8	4	-4	-16	-8	0	-8	-12	4	8	8	-4	-4
5	-4	-12	8	-8	12	4	-8	-16	-8	0	12	-12	8	-8	4	-4
6	-8	0	12	-4	8	0	-4	-12	-4	4	0	0	-4	-4	-8	8
7	0	-8	-4	12	-8	-8	-4	-4	-4	-4	-8	-8	4	12	0	0
8	4	-4	16	0	12	-12	8	-8	8	0	12	-4	0	8	4	-12
9	-12	-4	0	0	12	12	8	0	16	0	12	-4	8	-8	4	4
A	0	-8	4	4	8	0	-4	12	4	12	0	16	-12	-12	0	8
B	8	0	-4	-4	-8	8	12	4	4	4	0	0	12	4	8	0
C	0	8	-4	-4	0	-8	12	-12	-4	-4	8	0	-4	4	-8	0
D	0	-8	-4	-12	8	-16	-4	12	12	-4	8	-16	4	-12	8	-8
E	4	-12	16	-8	-4	-4	0	0	0	16	-4	4	16	-16	-12	-12
F	-4	4	-16	-8	-4	4	0	0	-8	-16	4	4	0	16	-4	-4

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{127}$ Üs Haritalaması L_{AS2} ="A9"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4A	E4	12	82	AC	2F	D6	ED	30	9F	B1	E7	9E	38	4D	B7
1	C7	AD	A3	6E	68	DB	1D	75	0B	FC	BE	09	D2	77	EC	9D
2	F9	11	69	0E	B9	F2	8C	25	98	02	05	EE	F8	A0	84	4E
3	B3	7B	A6	49	90	C2	1B	08	C6	76	5A	62	8F	4B	18	8E
4	F0	F3	1F	E3	79	FD	80	CC	AE	57	DE	60	87	14	8A	F7
5	B5	85	DA	5D	D9	EB	E0	9A	A4	AF	CA	A8	5B	36	20	E6
6	71	0F	D4	00	3A	E2	A9	53	BA	6F	0C	78	D8	70	FB	C4
7	50	41	7D	FF	D7	06	17	CE	1E	2B	61	A2	46	CB	5E	B8
8	99	19	6A	64	9C	C3	2E	91	39	DD	33	AA	42	55	07	7C
9	24	1A	D3	3F	9B	6D	4F	C1	63	E5	2A	01	92	96	F1	2D
A	34	2C	65	52	13	56	43	E1	59	73	5C	81	D5	E9	4C	F5
B	6C	21	7F	3B	BB	C9	28	EF	23	03	7A	A1	BD	C5	93	04
C	22	0D	54	3D	37	AB	CF	40	44	0A	6B	FA	BC	88	67	32
D	B6	8B	8D	15	51	48	DC	A5	DF	3C	CD	B2	7E	BF	F4	FE
E	E8	F6	26	10	35	95	C8	16	3E	D0	5F	EA	27	66	D1	B0
F	86	83	1C	A7	47	29	C0	74	45	B4	89	94	72	31	97	58

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	2	2	2	0	0	0	0	2	2	0	0	2	0
1	0	2	0	2	0	0	0	2	2	2	0	0	0	2	2	0
2	2	0	0	0	0	0	0	0	0	0	2	2	0	0	0	2
3	2	0	2	0	2	2	2	2	2	0	0	2	2	2	2	2
4	0	2	0	2	2	2	0	0	0	0	0	2	2	2	2	0
5	0	0	2	0	0	2	2	0	2	0	0	0	0	0	0	2
6	0	2	2	0	0	0	0	2	2	2	2	0	0	2	2	0
7	0	2	2	0	2	0	0	0	2	2	2	2	0	2	2	2
8	2	0	2	2	2	0	2	2	0	0	0	0	0	2	2	2
9	2	2	0	2	0	0	2	2	2	2	2	0	2	0	0	0
A	2	0	2	0	0	2	2	0	2	2	0	0	0	0	2	2
B	2	0	0	2	2	2	0	2	0	2	0	2	0	0	2	2
C	0	2	0	2	2	0	2	2	2	0	2	0	0	2	0	2
D	0	2	0	0	2	2	0	0	2	2	0	2	2	2	2	0
E	0	0	0	2	2	0	2	0	2	0	0	2	2	0	2	2
F	0	2	0	0	0	0	2	2	0	2	4	0	2	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	6	-2	8	0	-6	2	-8	-8	-10	-6	12	-4	6	2	8
1	-14	8	0	10	-14	12	-4	2	10	0	-12	-2	-10	-8	12	10
2	12	-2	-10	12	-16	14	-2	-8	-4	6	-6	-8	4	2	6	0
3	-6	-12	4	-14	-10	12	-4	-2	2	12	8	6	-6	-8	12	6
4	0	2	-10	4	-8	-10	-6	12	4	-2	-10	12	0	14	-2	0
5	-2	8	4	-6	-2	-12	8	-14	2	12	12	2	-2	-4	-4	-2
6	-16	-10	10	12	12	6	2	0	-12	2	-6	-12	4	14	6	-12
7	2	-8	12	-2	-2	-8	-4	-6	-2	-12	12	-2	-10	8	8	14
8	2	-8	-12	-2	-2	8	-12	-6	2	-8	8	2	2	4	-4	-6
9	12	-6	-2	0	8	-6	-10	4	12	-14	-6	-12	-12	6	-2	-4
A	-14	-4	8	6	-6	-16	-12	6	-6	4	4	-14	6	4	4	-2
B	-8	2	-2	-4	-8	-2	-6	-4	8	-6	-6	0	4	10	-14	4
C	-10	8	0	14	2	16	8	10	10	-4	0	-2	-6	0	-4	-10
D	-12	6	-2	-4	8	6	6	8	-8	2	6	-4	8	6	10	-4
E	2	-16	-8	-14	-6	-4	-4	2	-10	-12	-8	-14	2	-4	0	-2
F	-12	-6	10	12	12	-10	6	4	0	-2	10	4	-12	14	2	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^7$ Üs Haritalaması L_{AS2} ="56"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	81	5D	0F	DA	AE	8B	EF	BC	FE	60	86	D9	8E	7D	14	59
1	41	80	54	53	B6	1F	E2	F2	78	4A	36	0A	D8	16	FA	45
2	58	7E	BE	6B	E6	71	A6	BD	6A	FD	99	35	E7	55	9F	69
3	25	0D	C8	DC	21	29	E4	AF	64	4C	31	ED	5B	C7	0B	1C
4	E5	C6	9D	2B	33	0C	7F	AA	3E	D7	B3	07	5E	3F	CA	89
5	AC	12	26	C2	F0	C3	C0	D6	95	50	47	10	77	AB	32	03
6	24	2D	D3	B5	FC	A1	56	1B	E1	D1	00	97	E3	13	72	5A
7	C9	4E	5C	7B	F9	BB	BF	22	DB	D4	F5	92	39	67	E9	A0
8	66	63	9E	15	D5	CE	88	62	83	C1	EC	E8	18	D0	FF	0E
9	87	BA	3A	46	76	C4	E0	6C	A4	6F	23	61	75	A5	F4	D2
A	CB	F1	F6	B8	02	6E	F3	94	1E	90	57	65	93	DF	3B	B4
B	6D	7C	85	2F	84	52	2E	3C	4B	5F	7A	1D	EE	A9	B0	FB
C	2C	CC	EB	19	73	68	EA	9C	96	B9	C5	30	08	48	28	CD
D	49	11	A2	27	06	34	3D	AD	91	B7	43	70	17	CF	38	8A
E	42	4D	A7	40	F8	44	2A	01	9B	A8	09	1A	8C	98	04	4F
F	79	DD	20	A3	B1	37	51	8F	F7	DE	74	B2	9A	05	8D	82

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	2	2	0	2	2	2	0	0	0	0	0	6
1	2	2	2	2	6	0	2	2	0	0	0	6	0	0	0	0
2	0	0	0	2	0	2	6	2	6	2	0	2	0	0	0	2
3	2	2	6	6	0	0	0	0	0	0	2	0	2	2	0	2
4	2	0	6	2	0	0	0	2	0	2	0	6	2	4	2	0
5	0	0	0	2	0	0	0	2	2	0	0	0	0	2	2	2
6	0	2	0	0	0	0	2	6	0	0	0	0	2	0	0	0
7	0	0	0	0	0	0	2	0	0	0	0	0	2	0	0	0
8	0	0	0	2	0	2	2	2	0	0	0	2	2	0	2	2
9	2	0	0	0	0	0	0	6	0	0	0	0	2	2	2	2
A	0	0	0	0	2	0	0	0	0	2	2	0	2	0	0	0
B	0	0	6	0	2	0	2	0	0	0	0	0	2	0	2	2
C	0	2	0	0	0	2	2	0	2	0	0	2	0	0	2	0
D	2	0	0	0	0	6	2	0	2	0	0	0	6	0	2	0
E	2	0	0	0	2	2	0	2	0	2	2	0	0	0	0	0
F	2	2	2	2	0	2	2	0	0	0	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	-8	0	0	-16	8	8	8	-8	0	0	-16	-8	-8	0
1	0	8	8	0	0	0	-8	-8	8	8	0	0	0	8	8	0
2	-16	-16	8	8	8	0	0	8	-8	0	0	-8	-8	8	0	-16
3	8	-8	0	0	16	8	8	0	0	8	-8	0	0	0	-8	8
4	0	8	0	-8	-8	-8	8	8	0	0	0	0	16	-8	0	-8
5	8	16	8	16	-16	0	0	0	8	-8	-8	-8	-8	0	-8	0
6	16	0	0	0	-16	8	0	-8	0	8	0	8	-8	-8	-8	8
7	0	0	0	0	0	-8	0	8	0	8	0	-8	8	-8	8	-8
8	-8	8	0	0	8	0	0	-8	0	8	-8	0	-8	-8	0	-16
9	-8	-8	0	0	8	0	0	8	0	8	8	0	8	-8	0	16
A	0	8	-8	16	-8	-8	16	-16	8	8	0	0	8	16	0	-8
B	8	-16	-16	-8	16	0	-8	-8	0	16	-8	-8	0	8	-8	0
C	8	8	8	8	16	8	0	8	-8	0	8	0	-8	8	-8	8
D	16	0	0	0	8	0	8	0	0	8	16	-8	0	0	0	16
E	-32	8	0	8	0	16	0	0	0	16	0	0	-8	0	-8	0
F	0	8	0	-8	0	0	0	0	-16	16	0	0	-8	0	8	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{25}$ Üs Haritalaması $L_{A_{S2}}$ ="D1"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	32	49	BB	FA	D4	4D	E2	D0	AD	CE	AD	9F	EA	40	90	FA
1	A7	29	DB	16	5D	4D	C8	0A	9F	D0	16	71	97	6D	32	71
2	81	69	51	32	32	EA	9F	5D	51	C8	06	7F	6D	EF	82	71
3	81	14	5D	3A	20	F9	D7	6D	14	29	33	97	69	33	A0	F2
4	49	40	D0	4D	14	33	C8	EA	29	64	05	B7	5E	16	F2	D4
5	97	24	DF	81	24	C5	7F	E2	F9	D7	78	D0	33	64	64	24
6	F2	D0	7F	78	DB	05	D1	BB	8D	82	BB	FA	A0	78	D4	D3
7	A0	B0	05	49	69	F9	1D	40	33	D7	51	82	AD	E2	DB	32
8	CE	06	E2	3A	90	BB	B7	1D	FA	FA	71	0A	3A	F2	7F	5D
9	40	82	D3	78	EA	B7	24	81	8D	5E	C5	14	EA	8D	3A	CE
A	CE	78	1D	0A	8D	0A	97	20	5E	49	24	F9	AD	A0	DB	8D
B	14	20	81	6D	AD	D4	A7	97	9F	D3	DF	20	C5	EF	DF	D7
C	DB	1D	A7	DF	3A	D3	B7	71	E2	B0	05	82	16	40	C5	D7
D	CE	4D	29	6D	29	F9	69	EF	A7	69	A7	C5	06	B0	64	EF
E	90	90	5E	51	4D	B0	B0	D3	5D	A0	06	9F	BB	90	16	C8
F	C8	05	64	DF	1D	51	D4	7F	B7	5E	F2	06	0A	49	EF	20

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	0	0	0	0	0	0	4	2	2	0	0	0	2	0	4
1	4	0	2	0	0	0	0	4	0	0	0	0	0	0	0	0
2	0	0	6	0	0	0	2	2	0	0	2	4	0	0	2	0
3	2	0	4	0	2	0	0	0	0	0	0	0	0	2	0	0
4	2	4	0	4	2	0	0	0	2	0	0	0	6	2	0	4
5	0	0	4	0	0	0	4	2	0	0	2	0	0	4	2	0
6	0	0	2	6	0	0	0	6	0	0	4	0	0	0	0	0
7	0	0	0	0	0	0	0	0	2	4	0	4	0	0	0	0
8	0	0	2	2	0	0	2	4	0	0	0	2	0	0	2	0
9	2	0	0	0	0	2	0	0	0	6	0	0	0	4	0	0
A	0	0	0	0	2	2	0	0	2	0	4	4	0	0	0	0
B	0	0	2	2	0	0	4	2	0	0	2	2	0	0	0	0
C	0	0	6	0	0	0	4	0	4	0	0	0	0	4	2	2
D	2	2	0	4	0	0	0	0	6	2	0	0	0	2	4	0
E	0	2	0	0	2	0	0	0	2	6	0	0	2	0	0	0
F	0	0	0	2	4	0	0	0	0	0	2	0	0	4	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	-8	0	-16	-8	-8	0	0	0	0	-8	-8	0	0	-16
1	0	0	8	0	0	0	8	0	8	-16	-8	8	-8	0	0	0
2	0	0	8	0	0	-8	8	8	-8	0	16	-16	0	-8	0	0
3	-16	0	-8	8	-8	0	0	8	8	-8	0	-8	8	0	-8	8
4	16	-16	8	0	-8	8	8	0	0	0	-16	16	0	-8	8	0
5	0	-16	8	0	-16	0	0	8	-8	16	0	0	8	0	8	-8
6	-8	8	8	8	0	0	8	8	16	8	0	8	8	8	0	16
7	0	0	8	-8	16	-16	0	0	-8	0	8	-8	-8	0	0	0
8	-8	8	-8	0	0	-8	0	-8	8	0	0	0	0	0	-16	16
9	-16	0	-8	8	0	-16	0	-8	0	0	8	-32	-8	0	-16	-8
A	0	0	0	0	-8	8	0	8	16	-8	-16	0	8	0	8	-16
B	0	0	-8	0	0	8	-8	0	0	8	0	0	0	8	8	0
C	0	8	8	-8	8	-8	-8	8	0	8	0	-16	0	0	-8	-8
D	0	0	0	-8	0	0	0	0	0	0	-8	8	0	8	-8	8
E	8	-8	0	0	-8	0	0	0	-8	16	0	0	-8	8	0	0
F	16	0	8	8	0	16	16	8	16	0	-8	8	16	8	0	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{37}$ Üs Haritalaması $L_{A_{S2}}$ ="53"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D3	2B	AE	59	39	2D	21	E2	43	65	16	88	66	87	41	C0
1	17	05	B1	15	29	26	E7	86	8F	2A	B9	1D	DA	49	93	D9
2	00	68	8E	62	EA	B7	50	51	2E	F8	BB	5E	85	4D	33	10
3	95	6E	F9	3F	B4	8B	E1	3B	A5	89	6A	CC	61	A2	80	11
4	EE	18	AA	C6	FF	5B	7A	9C	0A	1C	6C	57	F7	98	47	DD
5	AD	02	D4	58	8D	81	38	CF	73	55	90	22	1B	B5	23	C1
6	D0	13	B2	60	A1	E9	53	D2	4E	0D	3D	D8	5D	BE	A9	34
7	69	8A	0F	44	36	AF	CD	24	DB	D1	14	01	42	19	07	9B
8	63	45	71	5F	CA	25	8C	B3	A4	B6	F1	5C	6D	9D	7B	EC
9	79	3A	DE	2C	0C	77	F2	E0	A3	BD	FB	E3	12	1F	04	D7
A	CE	31	B8	C4	7D	92	0E	BA	ED	46	EF	70	B0	20	A0	DC
B	84	67	7E	A7	F4	F6	06	E6	AC	72	9A	C9	96	82	BF	FE
C	E4	0B	E5	97	5A	C2	AB	76	D5	30	99	56	28	91	83	C8
D	4C	75	1E	03	CB	74	64	27	52	08	F5	3C	32	C5	7F	C3
E	2F	BC	9F	1A	EB	D6	FA	09	3E	C7	F0	A8	37	4B	4F	4A
F	7C	40	A6	35	9E	FD	E8	FC	54	6B	48	6F	DF	94	78	F3

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	2	2	0	0	2	0	0	0	0	2	0	2	2	0	2
1	0	0	6	0	6	2	2	0	2	0	0	0	0	2	2	0
2	0	0	0	2	0	0	6	2	0	0	0	0	2	0	2	0
3	0	0	0	0	0	0	0	0	0	2	0	2	2	2	0	6
4	0	2	0	6	0	0	0	0	2	0	2	6	0	0	0	0
5	0	0	0	2	0	0	0	0	2	0	2	2	0	2	0	0
6	0	2	0	2	0	0	0	0	2	0	0	0	2	0	0	2
7	0	0	2	0	0	0	0	0	0	0	0	2	6	0	0	0
8	0	4	0	0	0	2	0	0	0	0	0	2	2	0	0	0
9	2	2	0	6	0	0	0	2	2	2	2	0	2	2	2	2
A	0	0	0	0	6	2	2	0	0	0	0	2	0	2	2	2
B	0	0	2	0	2	0	0	0	0	2	0	0	2	0	0	2
C	0	0	0	6	0	0	2	0	2	2	0	0	0	0	0	2
D	0	0	2	2	0	0	2	0	0	2	2	0	0	2	2	0
E	2	2	2	6	0	6	2	0	0	2	0	0	2	0	0	6
F	2	0	2	2	0	0	2	6	2	2	0	2	0	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	-8	0	0	-8	0	0	-8	0	16	16	8	-8	-8	0
1	0	0	8	0	-16	-8	0	0	-8	-16	0	0	8	-8	8	0
2	-16	16	-16	8	-16	8	-8	8	8	0	8	8	8	8	0	8
3	0	0	0	8	0	8	8	-8	-8	0	-8	-8	8	8	0	-8
4	0	8	0	0	-8	-8	16	8	8	8	-8	0	0	8	-8	8
5	8	0	8	8	0	0	-8	0	0	0	16	8	8	0	0	16
6	8	0	0	0	-16	0	0	-8	0	0	8	0	-8	0	8	8
7	0	8	8	8	-8	8	-8	0	8	8	0	8	0	-8	0	0
8	-8	8	-8	0	0	-8	8	-8	0	-8	-32	0	8	-8	0	-8
9	0	0	0	8	8	0	16	-16	8	0	8	-8	0	0	-8	16
A	8	8	0	8	0	8	0	-16	16	8	8	-8	-8	8	8	-16
B	16	0	-8	0	-8	0	8	8	-8	-16	0	0	0	0	0	8
C	-8	0	-16	0	-8	8	8	0	0	0	8	0	-16	8	0	-16
D	-8	0	0	0	8	8	8	0	-16	0	8	0	0	-8	0	0
E	0	8	0	0	0	-16	-8	0	-8	8	8	0	-8	0	16	0
F	0	8	0	-16	0	0	-8	0	8	8	-8	16	-8	0	16	16

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{63}$ Üs Haritalaması $L_{A_{S2}}$ ="B4"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2C	15	70	D2	BA	E1	D0	6E	6B	84	90	01	C7	E7	58	58
1	6B	C4	4C	E4	E5	12	84	C4	3D	ED	AE	F2	99	DA	F9	5E
2	B5	C5	CC	ED	6E	8E	2B	08	09	82	BF	5E	D0	8E	F4	A8
3	F0	DC	15	05	CC	3D	30	35	62	98	F9	BF	05	2C	A1	52
4	26	72	F9	02	40	6E	29	20	FB	DD	E6	3D	D0	40	41	67
5	07	3A	5E	02	11	15	CF	C2	E9	AB	11	2C	ED	E6	D4	0F
6	C4	E2	7F	DE	B3	EA	B4	58	11	05	33	7D	73	4E	8E	40
7	CC	E6	B1	6A	CD	4A	02	BF	E2	84	A3	4D	B0	49	6B	E2
8	82	72	DA	CD	33	D2	E9	F0	33	70	CF	52	C5	FB	F2	6A
9	99	CD	62	3A	67	2B	4E	E1	0F	35	6A	AE	BA	4E	F4	29
A	30	0F	B5	FB	3A	98	72	09	49	E5	DE	01	4C	A3	90	DE
B	E4	A3	12	49	B3	C7	B3	E7	E9	DC	CF	A1	08	67	A8	29
C	B0	12	90	7F	4D	E4	01	7F	35	D4	DD	C5	62	07	26	82
D	AB	F0	52	C2	41	2B	F4	20	4C	4D	B0	E5	E7	EA	EA	C7
E	D2	7D	C2	A1	B5	DD	B1	AE	26	09	99	4A	7D	70	DC	AB
F	30	D4	B1	F2	E1	73	20	A8	4A	DA	98	07	41	08	BA	73

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	2	0	0	2	2	0	0	0	2	0	2	0	6	0	0
1	2	0	0	0	2	0	0	2	2	2	0	0	0	0	0	2
2	2	2	0	2	0	0	6	0	0	2	2	0	2	2	2	2
3	0	0	0	0	0	2	0	0	0	2	2	0	0	6	2	2
4	2	0	2	6	0	0	2	2	0	2	0	0	2	0	6	0
5	0	0	0	0	6	2	0	0	2	2	0	6	6	0	2	0
6	0	0	0	2	0	2	2	0	2	0	2	0	0	0	2	2
7	2	0	0	0	2	0	0	2	0	0	0	2	0	0	2	0
8	0	2	0	0	0	0	0	2	2	2	0	2	0	0	0	0
9	6	2	2	0	0	0	0	0	2	0	0	0	0	2	0	2
A	0	2	6	0	2	0	0	2	2	2	0	0	2	0	0	6
B	0	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0
C	0	0	0	0	2	0	0	0	0	2	0	0	0	0	2	0
D	2	0	0	2	2	0	0	0	0	0	0	6	0	2	0	2
E	2	6	0	0	2	0	0	0	0	0	0	0	2	0	2	6
F	2	2	0	2	2	0	0	2	0	2	2	2	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-4	12	8	12	-16	8	-4	8	4	4	0	4	0	8	20
1	-16	4	-12	0	-12	0	-8	-4	-16	4	-12	-24	4	0	0	-4
2	-8	-4	4	8	-4	0	8	-4	-8	-4	4	-8	12	0	16	4
3	8	4	4	8	-4	-8	-8	-4	0	-20	4	0	4	-8	0	4
4	8	4	-4	-8	4	8	0	12	16	-4	4	16	4	-8	8	4
5	-24	4	-4	-8	-20	8	0	4	0	4	-4	8	-20	-8	0	-4
6	-8	-4	4	-8	4	-8	0	-4	-16	12	-4	8	-12	8	-8	-12
7	0	-4	-4	8	20	8	-8	20	8	4	4	8	4	8	0	4
8	-8	4	-12	0	-4	-8	-8	4	8	-4	-4	-16	4	-8	8	-20
9	16	4	4	-8	4	0	-8	4	16	4	4	0	-4	0	0	-4
A	0	-4	12	-8	-4	-8	-8	-12	0	-12	4	8	-4	-8	0	-4
B	-16	4	4	8	4	0	8	4	0	4	-4	8	4	16	0	4
C	-8	4	-4	8	-4	-8	16	4	-8	4	-4	8	4	-8	-8	4
D	0	4	-4	-8	-4	0	0	4	-8	-4	4	8	-4	0	0	12
E	0	4	-4	0	4	8	-8	4	0	-4	12	-8	4	0	8	-4
F	0	4	-4	8	-4	0	-8	-4	-8	20	-4	8	4	8	-8	4

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{11}$ Üs Haritalaması $L_{A_{S2}}$ ="B2"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7E	F6	C2	1B	07	C8	25	DA	FE	36	AF	F3	C5	1C	08	24
1	13	4F	81	C3	15	DF	1F	AA	7D	64	4B	89	26	FF	8A	E9
2	75	23	52	16	5C	F9	87	51	EA	00	86	BB	EB	A4	79	80
3	CA	BA	A2	8F	94	C6	06	68	FA	33	90	C1	93	2E	01	45
4	14	6F	A8	0D	3A	34	29	98	D6	7B	BF	09	7C	F2	B8	4C
5	61	B5	E0	A5	96	E6	BE	3E	AC	AB	B1	E2	C0	35	76	B6
6	57	46	E5	69	CD	1D	B2	9E	95	AE	54	37	E1	4D	EF	7A
7	74	38	9A	04	3F	63	1A	F5	F8	9B	2C	58	42	67	5F	0C
8	2F	55	BD	44	8D	47	48	60	6B	D1	D7	2B	65	39	8C	F7
9	CF	C9	83	49	70	17	6D	A7	6A	A9	41	8B	66	92	1E	82
A	84	6E	77	5D	4E	A0	88	C7	31	E7	4A	99	3D	B9	71	91
B	43	27	0F	E4	9C	2D	E3	BC	56	0B	DB	CC	50	8E	EC	19
C	D0	62	6C	D2	02	32	D8	85	73	97	D9	F4	CB	FB	05	9D
D	AD	18	DC	2A	C4	22	D5	11	0E	E8	20	40	12	F1	5E	5A
E	EE	78	A6	7F	B0	10	FC	72	A3	9F	5B	ED	FD	A1	03	B4
F	30	53	D4	B7	DD	59	3B	DE	3C	F0	21	28	CE	B3	D3	0A

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	2	0	2	2	0	2	0	0	0	0	2	0
1	0	2	0	0	0	0	0	2	0	2	0	0	0	0	0	0
2	0	0	0	0	0	2	0	0	2	0	2	0	4	4	0	0
3	4	0	0	0	0	0	0	0	0	0	0	2	2	2	0	0
4	0	0	2	0	4	2	0	0	0	0	0	0	2	0	0	4
5	0	2	2	4	0	0	2	0	0	0	0	0	10	4	0	2
6	2	0	0	10	2	0	0	2	0	0	0	0	0	0	2	0
7	4	0	0	0	2	0	0	0	0	0	2	4	0	2	0	0
8	2	0	0	0	4	0	0	0	2	0	0	0	2	0	4	0
9	0	0	0	0	0	2	2	0	2	0	0	0	2	0	2	0
A	2	0	0	0	0	4	0	0	0	0	0	0	2	2	0	0
B	0	4	2	0	0	4	4	2	0	0	2	0	0	2	2	0
C	2	0	2	2	2	0	0	0	2	2	10	0	2	0	0	2
D	2	0	0	2	2	0	4	0	0	10	0	0	0	0	2	0
E	2	0	0	2	2	2	4	0	0	0	4	2	0	0	2	2
F	0	0	0	0	4	4	2	0	0	4	0	0	2	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	0	0	-8	0	-8	8	0	-8	8	-8	16	-8	8	8
1	0	-8	-8	-8	8	0	0	0	0	-8	0	-16	0	-8	0	0
2	8	8	-16	8	0	0	-8	0	16	0	0	8	-16	0	-16	-8
3	0	0	0	-8	8	8	8	0	-8	-8	0	8	8	-8	0	-24
4	-8	0	0	0	0	8	8	-8	8	0	-8	-8	8	-16	-8	8
5	8	0	8	8	-16	-8	16	0	8	0	-32	0	-8	0	0	0
6	0	0	0	-8	-8	-8	-8	0	8	-24	0	8	-8	-8	0	8
7	8	-8	0	8	0	0	8	0	0	0	0	-8	0	0	16	-8
8	0	-8	-8	-8	0	-8	8	-8	8	0	8	-8	0	8	0	0
9	-8	0	8	-8	8	0	8	8	0	-8	-8	-8	-8	0	0	0
A	-8	8	-24	0	8	8	8	0	-8	-8	0	-8	16	0	-24	-16
B	8	-8	0	8	8	-8	0	8	8	-8	-8	0	0	0	0	8
C	0	-8	0	0	0	8	0	0	-8	0	16	0	0	8	-8	8
D	8	0	0	0	-8	0	16	0	16	8	16	0	8	16	-8	8
E	8	-8	0	-8	-8	8	0	8	8	8	-8	0	0	0	-16	-8
F	-8	8	-8	0	-8	8	-8	0	-8	8	0	-8	0	0	8	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{29}$ Üs Haritalaması $L_{A_{S2}}$ ="A3"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2F	7D	6A	8B	AD	F7	30	EE	A0	3E	7F	C2	4A	1B	29	AE
1	87	EC	80	F3	4E	51	11	26	9F	79	57	74	10	5E	76	0F
2	A2	52	1C	62	AC	97	00	90	D9	0E	FB	C4	22	E4	DA	13
3	15	9B	60	63	0B	61	08	CD	4D	45	20	8E	9A	B7	DB	B0
4	F2	36	F5	14	07	E1	21	39	8F	FD	94	5D	B1	75	FF	99
5	65	59	68	05	18	BE	82	A9	D4	BA	D7	3B	B8	C3	CA	2D
6	69	FA	2E	88	83	F8	A3	24	6C	5A	67	0C	64	33	D0	D1
7	B4	F4	98	31	AB	E8	B2	D6	6D	8C	CE	E3	58	28	84	34
8	27	3D	46	1A	86	C5	3C	E6	42	C8	9E	C0	23	19	32	C1
9	DD	12	25	BD	44	2A	06	E7	FC	3A	53	1D	03	96	92	95
A	93	72	40	35	47	7A	A8	CC	4C	02	C9	77	78	1E	7B	E2
B	6F	73	F6	C7	5C	37	7C	F0	4B	81	BF	71	2C	7E	49	17
C	5F	04	A7	D8	6B	3F	16	55	54	AF	91	D2	CB	85	8D	8A
D	BC	50	D3	D5	56	89	EB	EA	5B	2B	A4	EF	48	AA	F1	DE
E	ED	E0	DF	09	41	CF	9D	E9	DC	B6	6E	B5	4F	01	B9	A5
F	38	C6	A6	E5	B3	A1	70	F9	FE	BB	9C	43	0A	1F	0D	66

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	4	0	2	0	0	2	4	2	0	0	0	0	2	0	0
1	0	0	2	0	0	2	0	0	2	0	2	0	4	0	0	2
2	0	0	0	2	0	0	0	0	0	0	0	2	0	4	0	2
3	0	2	0	0	0	0	2	2	0	0	2	2	2	2	0	2
4	2	0	0	10	0	2	0	0	0	0	0	2	0	0	10	0
5	0	2	4	0	2	0	0	2	0	0	2	2	2	0	4	0
6	0	0	0	0	4	0	4	0	0	0	4	10	0	2	4	0
7	4	0	2	2	2	2	0	0	0	2	0	4	0	0	2	2
8	0	0	0	0	0	0	0	4	0	2	2	0	2	0	4	0
9	2	0	0	2	0	2	0	0	2	2	0	0	0	0	2	0
A	0	0	0	0	0	0	4	0	0	2	0	0	0	0	2	0
B	2	0	0	0	0	0	0	0	0	0	0	0	0	2	2	0
C	0	0	0	0	4	2	4	0	0	4	2	0	0	0	2	2
D	0	0	0	0	0	0	2	2	0	0	2	2	0	0	2	4
E	0	10	2	0	0	0	4	2	0	0	0	0	4	0	0	0
F	2	0	0	2	0	0	0	0	0	0	0	2	0	0	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	0	24	0	0	0	0	-8	8	-8	-8	8	0	8	0
1	8	-8	-8	-8	0	8	0	8	0	8	0	24	-8	8	8	-8
2	8	0	-8	0	0	0	0	0	0	0	0	16	-8	-16	8	0
3	-8	8	-8	-8	8	0	8	0	0	8	0	-8	0	0	0	0
4	0	8	8	0	8	8	0	0	24	-8	-16	0	16	-8	-8	0
5	8	-8	-16	16	-8	0	0	8	16	8	-8	0	0	0	8	8
6	-8	0	0	-8	-8	8	0	16	0	0	8	-8	0	-8	8	0
7	-8	-8	0	16	0	8	-8	0	0	8	-8	16	-8	-8	0	0
8	8	8	8	8	0	8	16	8	0	-8	0	-8	-8	8	8	8
9	32	-8	0	-8	0	0	0	-16	-8	-8	8	8	8	0	-8	0
A	0	0	0	0	0	-8	0	8	8	0	-8	-16	-8	-8	8	-8
B	0	8	0	8	8	8	-8	8	-8	8	-8	8	0	-8	16	-8
C	-24	-8	0	-16	8	0	0	8	0	-8	8	0	0	16	8	8
D	-16	-8	-8	0	8	-8	0	0	-8	-8	0	0	0	-8	-8	0
E	0	0	8	8	8	0	0	8	-8	0	0	8	-16	0	8	8
F	0	8	-8	0	0	0	-8	8	-8	-8	0	0	-8	0	0	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{13}$ Üs Haritalaması $L_{A_{S2}}$ ="D4"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	11	BC	F0	0F	B2	E5	C5	C1	CF	E4	96	88	D9	EA	28	2F
1	0E	0A	58	87	70	1C	7F	C9	C7	69	12	00	B4	90	06	9F
2	A5	7A	E9	04	BB	7B	EB	18	78	60	8F	C2	72	97	A7	16
3	65	AA	3A	4E	F5	B7	79	81	A1	85	7E	86	9D	D6	AF	39
4	20	B8	AC	14	41	AE	FB	35	46	6F	CA	A4	63	DF	E7	1D
5	BD	B0	89	2D	BA	52	77	37	42	D2	4D	13	B9	2E	71	29
6	17	C3	3C	A8	43	05	D4	D3	23	07	0B	08	92	C6	38	4A
7	C8	30	FF	CE	A9	51	ED	DD	6B	4F	64	EE	57	91	15	7C
8	E2	E6	C4	3D	F4	2C	F8	DC	2B	D7	FE	98	74	B6	B5	EC
9	83	40	8C	3B	BF	32	55	AD	31	26	F6	F2	FC	47	E0	49
A	50	CC	25	24	5F	FA	8A	B3	27	02	A2	7D	C0	3E	DB	DE
B	6C	8E	94	62	1A	53	8D	D1	6E	19	5D	59	48	76	2A	66
C	01	5C	99	4B	33	3F	21	A3	73	E1	A0	DA	F9	D8	9E	56
D	CB	6D	75	D5	68	0D	93	F1	4C	09	82	A6	EF	8B	5A	5E
E	F7	0C	36	22	54	1B	95	34	6A	1F	E3	1E	D0	F3	67	CD
F	FD	44	BE	61	9C	03	10	E8	9B	80	AB	B1	5B	84	9A	45

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	2	0	2	12	2	0	4	0	0	0	0	2	2	0	0
1	0	0	2	0	2	0	0	2	2	0	2	2	0	0	2	0
2	0	2	0	2	12	2	0	0	0	2	0	2	0	0	0	0
3	2	2	0	2	0	0	0	0	0	2	0	0	0	0	2	0
4	2	0	2	0	0	2	2	0	0	2	0	2	2	2	0	2
5	0	0	0	0	2	0	0	2	2	2	0	0	2	2	2	0
6	0	0	2	0	2	2	2	0	0	2	0	0	2	0	2	0
7	0	0	2	0	2	2	0	2	0	0	2	0	0	0	0	0
8	0	0	2	0	0	0	0	0	0	0	2	0	0	2	0	0
9	2	0	2	0	2	0	2	2	2	2	0	0	2	0	0	2
A	2	2	0	0	2	2	2	0	0	2	2	0	0	2	2	0
B	0	2	0	0	0	0	2	2	2	2	0	2	2	0	0	0
C	2	0	2	2	0	0	2	0	2	0	0	0	0	0	2	2
D	0	0	2	0	2	0	0	0	2	0	0	0	0	0	0	12
E	0	0	2	0	0	2	0	0	2	0	0	0	0	2	0	2
F	0	0	0	2	0	0	2	0	12	2	2	2	2	2	2	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	0	8	8	8	-8	0	0	0	8	0	-8	8	0	0
1	-8	-8	-8	8	8	0	0	0	0	-8	-8	-8	8	0	8	0
2	-16	8	0	-8	0	0	-8	0	0	8	0	0	0	-8	8	0
3	0	8	0	-8	-8	-8	8	0	-8	0	-8	-8	8	-16	-8	0
4	-8	0	-8	-24	8	-8	-8	-8	0	-8	0	-8	8	0	8	8
5	0	-8	8	8	0	0	16	0	0	8	8	0	0	8	0	0
6	8	0	-8	-8	-8	-8	0	0	0	0	-8	8	8	8	-8	0
7	-16	0	-8	0	0	-8	-8	0	-16	8	0	8	0	-8	0	0
8	-8	8	0	0	8	0	8	8	16	-32	0	-8	0	-16	8	-8
9	0	8	0	-8	-8	-24	-8	16	-8	0	0	0	-8	0	0	-8
A	0	-8	0	-8	-8	8	8	0	0	16	0	-8	8	8	8	-8
B	-8	0	0	-8	8	-24	8	0	8	8	-16	-8	16	0	0	0
C	-16	0	0	8	8	0	16	8	8	0	8	0	-8	0	16	0
D	8	-8	-8	0	0	8	0	8	0	8	16	8	-8	0	-8	-8
E	-8	0	0	0	0	0	8	-8	8	0	24	0	-8	16	-8	-8
F	8	8	0	8	-16	-8	0	8	-8	-8	8	-8	-16	0	8	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{55}$ Üs Haritalaması $L_{A_{S2}}$ ="74"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	35	12	27	9F	24	DD	15	1E	4F	6B	4F	85	E8	F8	CC	9F
1	71	7A	4A	8C	3A	DD	6D	D4	85	1E	8C	96	EC	C1	35	96
2	81	47	08	35	35	E8	85	3A	08	6D	60	97	C1	B8	C8	96
3	81	57	3A	FB	7E	F4	72	C1	57	7A	5F	EC	47	5F	02	DA
4	12	F8	1E	DD	57	5F	6D	E8	7A	B3	76	05	A0	8C	DA	24
5	EC	32	75	81	32	5C	97	15	F4	72	A3	1E	5F	B3	B3	32
6	DA	1E	97	A3	4A	76	74	27	E5	C8	27	9F	02	A3	24	AF
7	02	B1	76	12	47	F4	28	F8	5F	72	08	C8	4F	15	4A	35
8	6B	60	15	FB	CC	27	05	28	9F	9F	96	D4	FB	DA	97	3A
9	F8	C8	AF	A3	E8	05	32	81	E5	A0	5C	57	E8	E5	FB	6B
A	6B	A3	28	D4	E5	D4	EC	7E	A0	12	32	F4	4F	02	4A	E5
B	57	7E	81	C1	4F	24	71	EC	85	AF	75	7E	5C	B8	75	72
C	4A	28	71	75	FB	AF	05	96	15	B1	76	C8	8C	F8	5C	72
D	6B	DD	7A	C1	7A	F4	47	B8	71	47	71	5C	60	B1	B3	B8
E	CC	CC	A0	08	DD	B1	B1	AF	3A	02	60	85	27	CC	8C	6D
F	6D	76	B3	75	28	08	24	97	05	A0	DA	60	D4	12	B8	7E

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	0	0	0	2	0	0	2	2	0	0	12	2	2	0	0
1	2	0	0	0	0	0	0	0	2	0	2	2	0	0	2	0
2	2	2	0	0	2	0	0	2	0	2	2	0	2	12	2	0
3	2	2	0	0	2	0	2	0	2	0	0	0	2	2	0	0
4	2	0	2	0	0	2	0	0	0	0	0	0	0	2	0	0
5	0	0	0	4	2	0	0	0	0	0	2	0	0	0	2	0
6	0	0	2	0	2	2	0	0	0	0	0	2	2	0	2	0
7	0	0	0	2	2	0	0	0	0	2	0	0	0	0	0	2
8	0	2	2	0	0	2	2	0	0	0	2	2	0	0	2	0
9	2	0	2	2	0	0	0	0	0	0	0	2	0	2	0	0
A	0	2	0	2	2	2	0	0	2	0	0	0	0	2	0	2
B	0	0	2	12	0	0	2	0	4	2	2	2	0	2	2	2
C	2	2	0	2	2	0	12	0	2	2	2	0	0	0	0	0
D	2	2	0	0	0	0	2	0	2	0	0	0	0	2	2	0
E	0	2	0	0	2	2	0	2	0	0	2	4	2	2	2	0
F	0	0	0	0	2	0	0	2	0	2	0	0	2	0	2	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	0	0	0	8	-8	-8	0	-8	8	0	-8	8	16	16
1	16	16	0	0	-8	8	0	0	-8	8	0	0	0	0	-8	-8
2	0	0	-8	8	0	8	0	-8	-8	-8	0	0	0	0	-8	8
3	8	-8	-16	-8	-8	0	-8	-8	0	8	8	0	8	-8	0	16
4	-8	8	16	0	0	0	-8	8	8	0	-8	8	-8	8	-8	-16
5	0	0	8	-8	8	-8	16	0	8	-8	0	-16	0	0	8	-8
6	0	-16	24	0	8	-8	0	8	8	-8	0	-8	0	-8	8	-8
7	8	8	-8	0	0	0	0	8	0	0	-8	-8	8	8	-16	0
8	24	-8	8	8	0	8	8	-8	0	0	8	-8	-8	-32	0	0
9	0	0	-24	0	8	8	0	0	-8	0	0	8	8	8	-8	0
A	0	0	-8	0	-8	8	0	0	-8	8	0	0	0	0	0	8
B	8	8	8	-8	16	8	8	-8	0	-16	8	-8	-8	-8	0	-8
C	-8	0	-8	0	0	0	0	8	0	0	-8	-8	0	8	-8	8
D	0	0	8	8	-8	-8	-8	0	8	0	-8	8	0	0	-8	-8
E	-16	0	8	0	0	-8	0	8	8	8	0	0	-8	0	8	8
F	-8	8	0	-8	0	0	-8	8	0	8	-8	8	8	24	0	-16

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{59}$ Üs Haritalaması L_{AS2} ="36"

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	D4	EC	93	77	33	92	C6	63	A5	AB	C1	1E	3F	E1	E7	69
1	B7	12	4A	F1	F8	88	84	11	D7	90	4E	98	FD	97	62	EB
2	66	DD	3E	81	C4	5A	3B	22	BE	9B	6C	D1	A4	04	3D	7F
3	5E	4C	2D	48	8F	13	9D	67	5B	31	26	DC	FB	D5	4F	C9
4	60	0B	72	0E	89	91	B4	61	32	BF	20	F2	54	21	ED	5F
5	4D	79	0C	2C	D0	F7	DF	B9	75	2F	09	37	27	6B	A9	46
6	35	80	02	6A	D9	0A	36	B8	EF	85	CC	F9	47	8C	68	9E
7	87	7D	57	7B	6E	94	14	86	73	19	0F	F0	D3	2B	24	C5
8	B2	17	7A	43	28	5C	DA	B0	D2	03	4B	16	8E	EA	96	74
9	9A	1B	E6	FC	3A	B1	1A	E0	55	49	39	9C	08	A0	A3	00
A	06	25	AA	EE	B3	CA	2A	FE	F5	6F	C3	78	3C	CF	AF	9F
B	34	F6	C2	E8	BD	64	52	70	99	59	A2	07	BA	53	E5	82
C	2E	7C	58	45	10	F3	50	71	18	41	95	65	8B	C0	E3	1F
D	29	D8	E9	8A	CE	BC	A8	01	40	D6	CB	A1	A7	F4	C8	6D
E	1D	42	05	7E	FA	1C	E2	E4	B5	76	51	5D	8D	A6	23	30
F	AD	DE	83	38	44	C7	56	AC	FF	DB	CD	BB	15	AE	0D	B6

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	2	0	0	0	0	0	2	0	2	0
1	0	0	2	2	0	0	0	0	2	2	2	0	2	2	0	0
2	2	2	2	2	2	2	0	2	0	0	2	2	2	0	2	0
3	2	0	0	0	2	2	0	0	2	2	0	0	0	0	2	0
4	0	0	2	0	2	0	0	2	0	0	0	2	2	0	0	0
5	0	0	2	2	0	0	0	0	0	2	2	0	0	2	0	2
6	0	0	0	2	2	2	2	2	2	0	12	2	0	0	0	0
7	2	0	2	2	2	2	2	0	0	2	0	2	2	0	0	0
8	0	2	0	2	0	0	2	0	0	2	0	2	0	2	4	0
9	0	0	2	0	0	2	2	0	0	0	2	0	2	0	2	0
A	2	2	0	2	0	12	0	0	2	2	0	0	0	0	0	0
B	0	0	2	0	0	2	0	0	0	0	0	12	0	2	0	2
C	2	0	2	2	0	0	0	0	0	0	0	2	0	0	0	0
D	0	2	2	2	2	2	2	0	0	2	0	0	0	0	2	2
E	0	2	2	2	2	0	2	0	0	2	0	0	0	0	0	2
F	2	2	0	2	0	0	2	0	2	0	12	0	2	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	0	-8	-8	-8	16	-16	8	0	8	-8	16	-8	-8	-16	0
1	8	0	0	8	-8	-8	16	0	-8	8	-16	0	8	0	0	-8
2	0	0	8	8	0	-8	8	0	0	8	8	0	0	0	8	-8
3	0	-8	-8	0	-8	-8	-16	0	-16	0	8	-8	8	0	0	-8
4	8	-8	8	-8	-8	0	-8	0	-8	0	-8	16	-8	-8	-8	8
5	0	-8	0	8	8	8	8	-8	0	0	0	0	-8	0	-8	0
6	-24	-8	8	-8	0	8	0	8	-8	0	-8	-16	0	0	0	16
7	8	0	-8	0	-8	-8	8	-8	8	8	-8	-8	8	16	-8	0
8	0	24	8	0	0	0	8	8	0	0	8	-8	0	8	8	0
9	-8	8	0	0	0	8	8	0	-8	0	0	8	0	0	8	8
A	0	-8	8	0	-8	24	0	0	0	0	8	-8	-8	0	0	-8
B	0	-16	-8	-8	0	8	-8	-16	0	8	-8	0	0	0	-8	24
C	8	0	8	0	0	0	0	0	-8	8	-8	-8	0	-8	0	8
D	0	0	0	-16	0	-8	0	8	16	-8	-16	-8	0	0	0	0
E	-8	16	8	0	8	8	-8	-8	8	-8	-8	-8	8	0	-8	0
F	8	8	8	-8	0	-8	0	8	-8	0	-8	-32	0	0	0	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{15}$ Üs Haritalaması $L_{A_{S2}}$ ="47"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	BF	B2	49	49	36	31	2D	BF	21	58	21	01	36	17	49	49
1	21	F2	21	FB	B2	31	58	F2	01	BF	FB	80	17	2D	BF	80
2	31	46	DF	BF	BF	36	01	B2	DF	58	17	80	2D	36	46	80
3	31	FB	B2	46	DF	01	58	2D	FB	F2	BF	17	46	BF	DF	F2
4	B2	17	BF	31	FB	BF	58	36	F2	14	14	01	2D	FB	F2	36
5	17	42	80	31	42	B2	80	2D	01	58	42	BF	BF	14	14	42
6	F2	BF	80	42	21	14	47	49	42	46	49	49	DF	42	36	FB
7	DF	14	14	B2	46	01	31	17	BF	58	DF	46	21	2D	21	BF
8	58	17	2D	46	49	49	01	31	49	49	80	F2	46	F2	80	B2
9	17	46	FB	42	36	01	42	31	42	2D	B2	FB	36	42	46	58
A	58	42	31	F2	42	F2	17	DF	2D	B2	42	01	21	DF	21	42
B	FB	DF	31	2D	21	36	21	17	01	FB	80	DF	B2	36	80	58
C	21	31	21	80	46	FB	01	80	2D	14	14	46	FB	17	B2	58
D	58	31	F2	2D	F2	01	46	36	21	46	21	B2	17	14	14	36
E	49	49	2D	DF	31	14	14	FB	B2	DF	17	01	49	49	FB	58
F	58	14	14	80	31	DF	36	80	01	2D	F2	17	F2	B2	36	DF

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	14	0	0	2	2	0	0	2	0	2	0	0	2	2	2	0
1	2	0	0	0	0	2	2	2	0	0	2	2	2	0	2	0
2	2	2	2	0	2	2	2	0	0	0	0	0	2	2	0	0
3	2	0	2	0	0	2	2	2	0	2	2	0	0	0	0	2
4	2	0	0	2	2	0	0	2	0	2	0	0	2	2	0	2
5	0	2	2	0	0	2	2	0	0	2	0	0	0	0	0	2
6	2	0	0	2	0	0	0	2	0	2	0	2	0	2	2	2
7	2	0	2	2	2	2	0	2	0	2	0	2	0	0	0	0
8	0	2	0	2	2	0	0	2	0	2	0	0	0	0	2	0
9	0	0	2	2	2	0	0	2	0	2	0	0	0	2	2	2
A	0	2	0	2	0	2	2	0	2	0	2	2	0	2	0	0
B	2	2	0	2	2	0	2	0	0	2	0	0	0	2	2	0
C	0	0	2	2	2	0	2	0	2	0	2	2	0	2	0	0
D	0	0	0	2	0	0	2	0	2	0	2	0	0	0	2	2
E	0	0	0	0	0	2	2	2	0	2	2	0	2	0	2	2
F	2	0	2	2	2	0	0	0	0	2	2	0	0	2	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	8	-6	6	-8	6	-6	6	-12	8	-4	6	-6	8	-6
1	10	-8	4	-4	6	-6	8	-10	8	-8	8	-10	6	-8	6	-10
2	-8	6	-10	6	-8	8	-10	8	-8	8	-8	6	-6	8	-6	6
3	-10	6	-6	12	-12	10	-8	8	-10	4	-8	12	-10	6	-8	6
4	6	-6	6	-8	10	-8	6	-6	4	-6	6	-10	6	-6	4	-6
5	8	-6	6	-10	6	-10	8	-10	10	-6	6	-8	6	-8	6	-6
6	-6	8	-8	4	-8	8	-6	8	-10	10	-10	4	-6	4	-10	10
7	-8	8	-8	6	-8	6	-12	8	-8	10	-10	10	-10	10	-8	6
8	6	-8	4	-4	8	-4	6	-8	6	-6	10	-8	10	-4	6	-6
9	6	-6	10	-4	6	-8	10	-6	10	-12	8	-4	4	-8	10	-8
A	-10	6	-6	8	-10	8	-6	10	-8	6	-6	10	-6	6	-4	10
B	-6	8	-8	12	-8	12	-10	8	-8	8	-8	10	-8	10	-8	4
C	6	-4	8	-8	10	-6	8	-6	6	-6	6	-8	8	-6	4	-4
D	10	-6	6	-8	8	-10	8	-8	10	-4	8	-8	6	-6	8	-6
E	-6	10	-6	4	-4	6	-8	12	-8	10	-10	6	-8	8	-6	8
F	-6	8	-8	8	-10	10	-8	6	-8	12	-8	10	-6	8	-10	10

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{45}$ Üs Haritalaması $L_{A_{S2}}$ ="55"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	05	54	A0	A0	E0	92	CD	05	E9	4A	E9	3F	E0	5B	A0	A0
1	E9	23	E9	24	54	92	4A	23	3F	05	24	50	5B	CD	05	50
2	92	13	06	05	05	E0	3F	54	06	4A	5B	50	CD	E0	13	50
3	92	24	54	13	06	3F	4A	CD	24	23	05	5B	13	05	06	23
4	54	5B	05	92	24	05	4A	E0	23	33	33	3F	CD	24	23	E0
5	5B	AD	50	92	AD	54	50	CD	3F	4A	AD	05	05	33	33	AD
6	23	05	50	AD	E9	33	55	A0	AD	13	A0	A0	06	AD	E0	24
7	06	33	33	54	13	3F	92	5B	05	4A	06	13	E9	CD	E9	05
8	4A	5B	CD	13	A0	A0	3F	92	A0	A0	50	23	13	23	50	54
9	5B	13	24	AD	E0	3F	AD	92	AD	CD	54	24	E0	AD	13	4A
A	4A	AD	92	23	AD	23	5B	06	CD	54	AD	3F	E9	06	E9	AD
B	24	06	92	CD	E9	E0	E9	5B	3F	24	50	06	54	E0	50	4A
C	E9	92	E9	50	13	24	3F	50	CD	33	33	13	24	5B	54	4A
D	4A	92	23	CD	23	3F	13	E0	E9	13	E9	54	5B	33	33	E0
E	A0	A0	CD	06	92	33	33	24	54	06	5B	3F	A0	A0	24	4A
F	4A	33	33	50	92	06	E0	50	3F	CD	23	5B	23	54	E0	06

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	14	0	0	2	2	0	0	2	0	2	0	2	2	0	0	2
1	2	2	0	0	0	2	2	2	0	0	2	2	2	0	2	0
2	2	2	2	0	2	2	2	0	0	0	0	0	2	2	0	0
3	2	0	0	0	0	2	2	2	0	2	2	0	0	0	0	2
4	0	0	0	2	2	0	0	2	2	0	0	0	2	2	0	2
5	0	2	2	0	0	2	2	0	0	2	0	0	0	2	2	2
6	2	0	0	2	2	0	0	2	2	2	0	2	0	0	2	2
7	2	0	2	2	2	2	0	2	2	2	0	2	0	0	0	2
8	0	2	0	0	0	0	0	2	0	2	0	0	0	0	2	0
9	0	0	2	0	2	0	2	2	0	2	0	0	0	2	2	0
A	0	2	0	2	0	0	0	0	2	0	2	2	0	2	0	0
B	2	2	2	0	2	0	2	0	0	2	0	2	0	2	2	0
C	0	0	2	2	2	0	2	0	2	2	2	2	0	2	0	0
D	0	0	0	2	0	0	2	0	2	0	2	0	0	0	2	2
E	0	0	0	0	0	2	2	2	0	2	0	0	2	0	2	2
F	0	0	2	2	0	2	2	0	0	2	2	0	0	2	2	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	8	-10	6	-8	10	-10	-10	4	-8	4	-10	10	-8	6
1	6	-8	4	-4	10	-10	8	-10	-8	8	-8	6	-6	8	-10	6
2	-8	6	-6	10	-8	8	-6	8	8	-8	8	-6	10	-8	6	-6
3	-6	10	-6	12	-4	6	-8	8	10	-4	8	-4	10	-6	8	-10
4	-10	10	-6	8	-6	8	-6	6	4	-6	10	-6	6	-6	12	-10
5	-8	6	-10	6	-6	10	-8	6	6	-10	6	-8	10	-8	6	-6
6	10	-8	8	-4	8	-8	6	-8	-10	10	-6	12	-6	4	-6	6
7	8	-8	8	-10	8	-6	4	-8	-8	6	-10	10	-6	6	-8	6
8	-10	8	-4	4	-8	12	-6	8	6	-6	6	-8	10	-4	10	-10
9	-6	6	-6	12	-6	8	-6	10	6	-4	8	-4	12	-8	10	-8
A	6	-10	6	-8	6	-8	6	-10	-8	6	-10	6	-6	6	-12	6
B	6	-8	8	-4	8	-12	6	-8	-8	8	-8	10	-8	6	-8	4
C	6	-4	8	-8	10	-6	8	-10	-10	10	-6	8	-8	10	-4	4
D	6	-10	6	-8	8	-6	8	-8	-10	4	-8	8	-6	6	-8	10
E	-6	10	-10	12	-4	6	-8	4	8	-6	10	-6	8	-8	6	-8
F	-10	8	-8	8	-6	6	-8	6	8	-12	8	-6	6	-8	6	-6

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{17}$ Üs Haritalaması $L_{A_{S2}}$ ="C5"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C3	41	58	DC	DA	77	5E	F5	5E	F3	77	DC	5E	DC	68	EC
1	F5	F5	DC	DA	71	5E	47	6E	6E	41	F5	DC	F3	F3	77	71
2	DA	C3	77	68	5E	68	EC	DC	68	5E	77	47	F5	EC	F5	EA
3	F3	68	EC	71	EA	5E	EA	58	47	F3	EA	58	47	DC	F5	68
4	58	6E	58	68	77	6E	68	77	58	41	EA	F5	6E	58	C3	F3
5	41	F5	F3	41	F3	68	5E	C3	47	DC	47	DA	EC	58	F3	41
6	5E	F3	68	C3	EC	6E	C5	41	71	F3	F5	71	DA	77	41	EA
7	58	77	DC	F5	77	77	EC	EA	71	71	47	41	47	68	6E	47
8	F5	5E	47	EA	5E	DA	F3	71	6E	EA	6E	EC	DC	77	C3	6E
9	71	58	71	5E	47	41	58	58	EC	EA	5E	5E	C3	EA	6E	41
A	58	68	DC	EA	6E	71	F5	EC	EC	F3	DA	C3	C3	F3	EA	DC
B	C3	71	F5	41	68	F5	41	DA	71	EC	F5	6E	C3	71	58	EC
C	71	6E	58	41	EC	DC	DA	EC	77	47	EC	DA	F3	EC	77	6E
D	DA	47	41	DA	DA	68	5E	EA	DA	68	F3	47	C3	5E	F5	6E
E	C3	47	DC	5E	C3	68	C3	6E	EA	41	47	EA	F3	77	41	C3
F	77	71	DA	DA	EA	C3	58	77	58	71	47	68	DC	DA	DC	DC

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	16
2	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	16
3	16	0	0	0	0	0	16	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	16	0	16	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	16	0	16	0	0
A	0	0	0	0	0	0	0	0	0	0	0	16	0	16	0	0
B	0	0	16	0	16	0	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	-8	8	-8	8	-8	8	8	0	-8	8	-8	8	-8	8
1	-8	-8	-8	8	-8	-8	-8	-8	8	8	-8	8	8	8	8	8
2	8	8	-8	8	8	8	8	8	-8	-8	-8	8	-8	-8	-8	-8
3	8	0	-8	8	-8	8	-8	8	0	-8	-8	8	-8	8	-8	8
4	0	8	8	-8	8	-8	8	-8	-8	0	8	-8	8	-8	8	-8
5	8	8	8	-8	8	8	8	8	-8	-8	8	-8	-8	-8	-8	-8
6	-8	-8	8	-8	-8	-8	-8	-8	8	8	8	-8	8	8	8	8
7	-8	0	8	-8	8	-8	8	-8	0	8	8	-8	8	-8	8	-8
8	-8	8	-8	8	-8	8	0	-8	-8	8	-8	8	-8	8	8	0
9	-8	-8	-8	-8	-8	8	-8	-8	8	8	8	8	-8	8	8	8
A	8	8	8	8	-8	8	8	8	-8	-8	-8	-8	-8	8	-8	-8
B	-8	8	-8	8	-8	8	8	0	-8	8	-8	8	-8	8	0	-8
C	8	-8	8	-8	8	-8	0	8	8	-8	8	-8	8	-8	-8	0
D	8	8	8	8	8	-8	8	8	-8	-8	-8	-8	8	-8	-8	-8
E	-8	-8	-8	-8	8	-8	-8	-8	8	8	8	8	8	-8	8	8
F	8	-8	8	-8	8	-8	-8	0	8	-8	8	-8	8	-8	0	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{19}$ Üs Haritalaması $L_{A_{S2}}$ ="E8"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	50	A8	B9	67	1D	58	3A	E3	A2	75	9A	E2	6D	A6	2B	F5
1	1C	BD	24	E6	D1	D5	C7	1A	7B	2E	7C	C3	04	55	9D	9C
2	AE	89	DF	CE	7D	8B	63	19	DA	C1	83	27	90	FB	16	78
3	23	AF	60	9F	BF	FA	73	FF	35	5E	B0	21	00	03	BA	F9
4	59	CD	C5	1E	A1	76	5C	7E	AC	37	34	69	42	3B	0B	0E
5	6F	A5	53	93	B1	20	0C	2D	F0	EE	26	BB	08	EC	EF	32
6	4F	5B	B7	FC	D0	EB	E8	36	7F	77	7A	A4	ED	6B	98	72
7	88	30	33	91	FE	71	65	4A	25	5A	8D	61	6E	87	56	96
8	6C	09	38	A3	8A	54	15	8F	18	C6	F6	5F	3C	F8	A9	A0
9	AB	B5	0F	AA	31	8C	BE	02	29	57	D9	95	41	3D	2A	DE
A	D8	F3	79	BC	E7	1B	2C	84	92	11	70	94	74	81	4C	64
B	46	E4	F4	FD	CA	A7	F2	8E	0D	DC	12	E1	68	D7	4D	6A
C	06	C9	3E	66	C2	48	9E	39	40	14	17	5D	D2	62	51	45
D	F7	44	4E	2F	E9	07	D4	52	B8	4B	80	28	C0	CF	CC	22
E	DB	05	EA	B3	3F	C8	CB	01	E0	B6	47	1F	49	97	9B	F1
F	43	13	10	82	B2	D3	C4	DD	86	85	AD	E5	0A	99	B4	D6

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	2	0	4	2	2	0	0	2	4	0	0	0	0	0	2
1	0	2	0	0	4	0	0	0	0	2	0	2	0	0	4	0
2	0	2	2	0	0	0	0	4	2	0	0	2	0	0	0	2
3	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
4	0	0	0	2	0	4	0	0	2	0	2	2	2	0	0	0
5	2	2	0	0	2	2	2	0	4	2	0	0	0	2	0	0
6	0	4	2	0	0	2	0	0	0	0	2	4	0	2	2	0
7	0	0	0	0	0	0	0	0	2	2	2	0	4	0	2	2
8	0	0	0	2	0	0	4	0	0	0	2	0	4	0	0	2
9	0	4	2	2	2	0	0	0	0	0	2	4	0	2	0	0
A	0	2	4	0	2	2	0	2	4	2	0	0	0	0	0	0
B	2	0	0	2	0	0	0	0	2	0	0	0	2	2	0	4
C	4	0	2	0	2	2	0	0	0	0	4	2	0	0	0	2
D	0	2	0	0	0	0	0	4	0	2	0	2	0	4	16	0
E	0	0	0	0	4	0	0	0	0	2	2	0	2	0	4	0
F	0	0	0	4	2	2	2	2	2	0	0	0	2	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	16	8	8	8	8	0	0	-8	8	0	8	8	0	8	8
1	0	-8	0	0	-8	0	-8	8	-8	0	-8	0	0	0	8	8
2	0	8	0	0	8	8	0	8	8	8	-8	-8	0	0	16	0
3	8	8	-8	8	-8	0	0	-8	8	0	8	8	0	-8	0	0
4	0	8	0	-8	0	0	-8	8	-8	-8	0	-8	-8	-8	0	-8
5	-8	0	0	0	8	-24	-8	0	0	16	0	0	-8	-8	8	8
6	-8	8	0	8	-8	24	0	24	-8	8	-8	8	0	-8	8	0
7	0	0	8	8	8	8	16	0	-8	-8	8	0	0	-24	-8	8
8	8	-8	8	8	-16	-16	-8	8	0	-8	-8	-8	8	-8	0	24
9	8	8	-8	0	0	0	8	0	0	8	8	0	0	0	-8	-8
A	0	0	0	-8	-8	0	24	-8	8	8	-16	0	8	8	8	-8
B	8	-8	0	0	8	0	0	-8	-24	8	8	0	8	-8	0	-8
C	0	8	0	8	-8	8	-8	-8	8	0	8	-8	-24	0	0	0
D	0	0	0	8	8	0	-8	-8	-8	8	8	8	-16	0	8	8
E	8	0	8	8	0	8	-8	-8	-8	8	8	-8	0	8	0	-8
F	-8	8	0	0	-8	-8	-8	8	0	-8	8	-8	8	8	0	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{23}$ Üs Haritalaması $L_{A_{S2}}$ ="33"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7D	AC	4A	B3	32	2D	5F	B4	07	03	DA	F6	84	00	0A	F3
1	40	48	9D	C6	25	E2	A8	C5	5C	DF	43	27	62	53	16	B0
2	59	39	30	70	B9	C0	E3	52	C8	B1	C3	E6	6D	76	57	71
3	96	0C	DB	AA	14	49	1A	61	89	D9	D2	A1	C4	1B	EC	54
4	CD	F0	F7	47	F9	3E	81	C1	2F	5B	79	26	01	7C	A2	77
5	92	F5	65	88	1E	44	F2	0D	8C	2A	6B	55	9C	C7	E5	80
6	BE	FA	A4	D8	EE	11	33	CA	46	5D	73	8A	CB	AD	85	B6
7	17	8D	AF	BA	A0	99	FC	51	58	98	EF	CE	A9	3F	74	91
8	05	2E	64	21	BB	42	24	06	FB	02	28	9F	4F	12	BF	90
9	4C	B2	A5	D3	67	8E	38	C9	4D	68	19	20	D1	A6	DC	AE
A	B7	FE	72	0E	15	83	ED	CF	56	6E	60	31	93	37	4E	8B
B	6F	EB	BD	5A	D4	95	09	8F	9B	EA	E9	13	E7	23	7E	1C
C	7A	6C	A7	6A	2B	9A	F4	FD	3A	97	B5	45	1F	DE	F1	87
D	2C	A3	F8	36	75	5E	B8	94	3D	D6	E0	78	BC	0B	29	22
E	C2	3B	08	CC	18	DD	FF	50	0F	34	1D	E1	82	7B	D5	35
F	9E	41	63	AB	D7	E8	66	3C	4B	04	69	7F	E4	86	D0	10

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	2	0	0	0	2	2	0	2	0	0	0	0
1	0	0	0	0	0	2	4	0	0	0	0	4	0	0	0	2
2	0	2	4	0	0	4	2	0	0	0	0	4	4	0	0	2
3	0	2	0	2	0	0	0	0	2	4	0	2	0	2	2	2
4	4	2	0	0	2	2	0	0	0	2	0	0	0	0	0	2
5	2	2	0	0	0	0	0	0	0	0	4	4	0	4	0	2
6	2	0	4	0	2	2	2	2	0	0	0	0	0	2	0	0
7	0	4	2	2	2	0	4	2	0	4	0	2	4	2	0	0
8	0	0	0	2	4	0	2	0	0	0	0	0	0	0	0	2
9	0	0	0	0	0	0	4	0	2	0	4	0	0	0	0	0
A	0	0	0	0	2	0	4	0	0	0	0	0	0	4	0	2
B	2	4	0	0	0	0	0	4	2	0	0	0	0	0	0	0
C	4	2	0	0	4	4	0	4	2	0	0	0	0	2	2	0
D	0	2	0	0	0	2	0	0	0	0	0	0	0	0	0	4
E	2	0	0	0	0	2	0	2	0	2	0	4	0	2	0	0
F	2	2	0	0	0	0	0	0	0	16	2	0	2	0	2	4

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	8	8	-8	8	-8	-8	-8	8	-8	0	-8	8	-16	0
1	0	-8	8	8	0	0	0	0	8	8	8	0	0	0	-8	8
2	-8	8	-8	-8	0	-8	0	0	0	-8	0	-8	0	-8	16	0
3	-8	0	0	-8	16	0	-8	0	-8	-8	0	0	8	-8	0	-8
4	-8	0	8	-8	0	8	8	0	-8	-8	0	-8	-8	0	-8	0
5	-8	0	16	0	8	0	8	-32	8	-8	8	-16	-16	8	-8	0
6	8	-8	0	-16	-8	-8	0	-8	8	0	0	8	0	0	-8	0
7	0	-8	8	0	0	8	8	-8	8	-8	0	0	0	8	8	8
8	0	0	-8	-8	0	8	8	8	-8	0	0	8	-8	-16	0	16
9	8	-8	-8	8	0	-8	0	0	-8	0	8	-16	0	8	16	0
A	8	-8	0	8	-16	8	32	-8	-16	-8	0	0	-8	0	0	8
B	0	8	-8	-8	8	8	-8	8	8	-8	8	16	16	0	8	8
C	0	0	8	8	8	8	0	-8	0	-8	8	0	-8	-8	0	-8
D	-8	-8	0	0	-8	-8	0	8	-16	-8	-8	0	0	0	-8	0
E	8	-8	0	-8	0	16	0	0	8	0	8	8	-16	0	-8	-8
F	-8	0	-8	8	16	8	8	0	8	8	-16	-8	0	-8	0	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{31}$ Üs Haritalaması L_{AS2} ="71"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D8	D4	0A	E0	B6	51	DE	97	99	F5	D2	9A	A1	93	C1	2B
1	EE	18	A5	07	6F	8D	58	7D	BC	5D	8C	BD	24	B5	12	CF
2	89	65	B2	E7	A8	D9	29	5A	0E	5E	60	3B	9D	CE	28	49
3	55	E8	E1	7E	6C	0F	F3	F6	63	23	62	D7	33	2D	D0	46
4	FF	82	01	A9	9E	4E	DA	1E	2F	C0	F9	C2	32	15	4A	09
5	35	4B	85	75	E5	44	F7	59	E4	77	0C	84	CB	31	08	A2
6	14	3E	03	DF	3A	48	71	9B	98	3C	BA	50	CD	36	66	FA
7	AF	B9	80	CA	6A	57	AD	C6	BB	DC	13	27	4D	1A	06	F4
8	EC	34	90	B0	DD	37	7A	72	16	FC	9F	26	FD	43	ED	05
9	83	AB	E2	AC	A3	5C	02	AE	EB	FB	BE	69	B4	45	E6	41
A	47	38	AA	1D	96	78	C7	5F	D3	8B	7F	C9	10	E3	5B	D1
B	0D	81	76	B8	67	CC	2C	70	EF	86	19	3D	30	DB	6B	EA
C	B3	8A	F8	A7	A4	7B	22	D5	7C	40	79	E9	F0	25	2E	C3
D	6E	56	11	17	74	04	BF	0B	C4	F2	8F	95	92	B1	88	1C
E	A6	4C	3F	9C	52	C8	F1	94	A0	20	D6	91	6D	87	1F	68
F	C5	39	00	21	8E	42	64	53	B7	54	2A	61	4F	1B	73	FE

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	2	2	0	2	0	0	0	2	0	0	0
1	2	0	0	0	0	0	2	0	0	0	2	0	0	0	2	0
2	2	2	0	2	2	2	0	2	2	0	2	0	0	0	0	0
3	0	2	2	0	2	0	2	2	2	2	0	2	2	2	0	0
4	2	0	0	2	0	0	0	2	2	2	2	2	0	0	2	0
5	2	0	0	2	2	2	0	2	2	0	0	2	2	0	0	2
6	0	2	0	2	0	2	0	2	0	2	0	2	2	0	0	0
7	2	2	2	2	0	0	0	2	0	0	0	0	0	2	2	2
8	2	2	0	0	0	0	0	0	2	0	2	0	2	2	0	0
9	2	2	0	2	2	0	2	0	2	0	2	0	2	0	0	2
A	0	2	2	2	2	0	0	2	2	0	2	2	2	0	2	0
B	0	0	0	0	2	2	2	2	0	2	0	0	0	2	2	0
C	0	0	0	0	2	0	0	0	0	0	0	0	2	0	2	0
D	2	0	0	0	0	2	0	2	2	0	0	0	2	2	0	2
E	0	2	2	2	0	0	0	2	2	0	16	2	2	2	2	2
F	2	2	2	2	0	0	2	2	0	0	2	2	2	0	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	-8	0	0	8	0	0	0	8	0	0	16	-16	-8	8
1	8	0	8	0	-16	0	-8	0	-8	-8	8	0	0	0	8	-8
2	-16	0	8	-8	8	8	8	16	0	0	-8	0	0	8	0	-8
3	-8	-16	0	8	0	0	0	-8	0	-16	0	8	0	0	8	8
4	8	16	0	0	8	0	8	0	0	0	0	0	8	0	-16	16
5	0	8	16	0	16	0	8	8	-8	-16	-8	0	0	-8	-8	8
6	16	0	8	0	0	-16	16	0	0	8	-8	0	16	0	0	8
7	8	16	-16	0	0	0	-16	16	0	-8	0	-8	8	16	0	0
8	-8	8	-8	0	8	0	-8	-16	0	0	0	0	0	0	0	8
9	8	16	-16	0	0	8	8	0	-16	0	-16	16	8	0	8	-8
A	0	-8	0	0	0	0	0	0	8	0	0	-8	0	-8	8	-8
B	0	8	0	-16	0	8	0	8	0	0	0	0	8	-16	8	8
C	0	0	8	-8	8	0	0	0	8	0	0	0	8	0	0	-8
D	0	8	0	-8	-8	-16	-8	-8	-8	0	0	-16	-8	8	0	-16
E	16	8	-8	0	0	-16	-8	0	16	0	0	8	0	-16	16	0
F	0	-8	8	0	8	16	0	16	8	0	0	0	0	0	8	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{47}$ Üs Haritalaması $L_{A_{S2}}$ ="95"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	97	61	92	B6	F3	AC	C1	82	40	A3	02	3C	37	AE	96	B2
1	C3	C4	81	C6	B7	9D	17	EA	03	ED	B8	F4	CB	33	F8	36
2	E4	35	F2	3F	2A	B0	10	09	B4	0E	99	BF	D1	74	46	7D
3	D5	0B	DF	D2	39	2F	BA	23	75	4B	45	FC	A1	50	7F	65
4	FD	A2	28	DD	58	3D	38	D6	34	6F	5A	B9	85	26	1A	12
5	C7	FB	1C	EC	F1	2B	DE	77	86	8C	1E	52	47	2E	1B	14
6	BB	80	57	9F	D7	A0	95	B1	7A	E6	91	B5	D3	70	51	EB
7	5E	E1	D4	43	72	AA	A4	F0	FA	21	18	01	54	67	16	EF
8	A5	C2	22	48	49	6D	E5	5D	4D	69	83	F7	3B	D9	41	E7
9	A7	AF	B3	62	1F	DA	68	6C	87	D0	31	CD	DB	8D	DC	11
A	08	06	15	78	0C	56	F5	A8	32	8F	E3	C9	19	EE	5B	E9
B	7E	63	24	C0	9A	5C	D8	90	F6	00	C8	25	59	98	0A	BC
C	8E	2C	CC	6B	E8	2D	60	A9	66	44	71	9B	53	CE	7B	3E
D	8A	1D	07	94	29	5F	0F	3A	0D	7C	4F	AD	AB	05	30	FE
E	4E	6A	76	CF	64	8B	BE	E0	13	89	F9	4C	4A	6E	9E	93
F	27	CA	FF	20	55	04	79	E2	73	84	88	9C	A6	C5	BD	42

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	2	0	0	2	4	0	2	0	0	4	2	2
1	0	0	0	0	2	0	2	0	0	4	2	0	0	2	0	0
2	0	0	2	0	16	0	2	0	0	0	4	0	0	0	0	0
3	0	0	0	2	0	2	0	0	0	0	0	4	2	0	4	0
4	0	0	0	2	0	2	0	2	2	0	0	0	4	0	0	0
5	0	2	0	0	2	0	2	2	0	0	2	2	0	2	2	4
6	0	0	0	2	0	2	0	2	0	2	2	0	0	2	0	0
7	0	2	0	0	2	0	2	2	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	2	0	0	0	4	0	4	4	2	2	2	0	0
A	0	0	2	4	0	2	2	2	0	2	0	0	0	0	2	0
B	0	0	2	0	0	2	2	0	2	4	4	0	0	2	0	2
C	0	2	0	0	0	4	2	0	2	2	0	0	0	4	4	0
D	0	4	0	0	0	0	0	0	2	0	2	2	0	0	2	2
E	0	0	4	4	2	0	0	0	0	0	2	0	0	4	4	2
F	2	2	0	0	0	2	4	4	2	2	0	0	2	2	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	-8	-8	0	8	0	8	0	8	-24	0	0	-24	-8	-8	-8
1	-24	8	8	8	-8	8	0	0	8	0	-8	0	0	-8	8	0
2	16	-8	-8	0	-8	0	8	0	-8	-24	0	0	8	8	8	8
3	8	-8	-8	-8	8	8	0	0	-8	0	-8	0	16	-8	8	0
4	0	8	-8	0	0	8	0	-8	0	0	-8	8	-8	8	8	-8
5	8	-8	-8	-8	0	0	-8	-8	0	-8	0	-8	0	-8	-8	0
6	0	8	-8	-16	0	8	0	8	0	0	-8	-8	8	-8	-8	24
7	-8	8	8	24	0	0	-8	8	0	-8	0	8	0	-8	-8	-16
8	8	8	0	0	8	8	8	-8	-8	16	0	8	0	8	0	8
9	0	8	0	-8	-8	16	0	-8	-8	8	-8	8	8	-8	0	0
A	8	-8	0	0	-8	8	-8	8	-8	0	0	8	0	-8	0	8
B	0	-8	0	-8	-8	0	0	-8	8	8	8	-8	8	8	0	0
C	0	0	8	24	8	8	-8	-8	-8	0	-16	-8	8	0	-8	0
D	-8	0	-8	0	8	0	-16	-8	-8	-8	-8	8	0	0	-8	-8
E	0	0	-8	24	-8	-8	-8	8	-8	0	0	-8	8	0	8	0
F	-8	0	8	0	8	0	0	-8	8	8	-8	-8	0	0	8	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{53}$ Üs Haritalaması L_{AS2} ="A6"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4D	5F	34	95	53	87	DC	60	9E	96	18	DA	B5	8E	EA	4B
1	BC	00	3A	A8	1F	2B	3D	B7	49	15	D5	E7	6F	B1	38	93
2	E0	72	AF	6B	46	99	BE	26	AA	24	83	36	B3	7F	2F	42
3	4C	41	66	B0	FD	2D	8F	DE	3C	E2	33	62	ED	1E	F8	55
4	DF	AB	AD	C1	4F	80	14	6C	F3	A1	81	C2	C9	32	44	8A
5	4A	7C	03	6D	F0	9F	77	A4	51	BF	73	F5	D8	82	A2	FF
6	11	8B	D2	2A	20	86	A6	07	25	FB	78	D9	A3	A9	40	DB
7	F4	A5	85	E6	64	35	0A	47	D3	0D	F1	39	02	CB	84	FE
8	90	2C	19	9A	BB	1A	C8	16	65	C4	F9	E3	C7	54	8D	6E
9	CD	58	EF	67	1C	5B	EB	BA	68	74	2E	92	FA	E4	05	3B
A	22	31	71	01	BD	B6	21	C3	76	17	3E	AC	6A	C6	EC	B2
B	06	91	DD	1B	48	D6	CE	C0	3F	7B	28	94	57	30	5C	89
C	D4	50	52	1D	4E	08	D0	69	0C	7A	5A	13	75	09	EE	12
D	B9	FC	10	61	A7	43	8C	23	F6	D1	70	AE	E8	59	79	C5
E	29	88	63	CA	37	5D	7D	E1	97	CF	04	B4	F7	56	9C	A0
F	0B	7E	5E	CC	9B	98	E9	B8	27	0E	F2	E5	45	D7	0F	9D

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	2	0	0	0	0	2	0	2	2	0	2	2	0
1	0	0	2	2	0	0	0	2	0	0	2	0	2	0	2	0
2	0	0	0	0	0	0	0	2	0	2	0	0	0	0	0	0
3	0	0	2	0	2	0	2	0	0	0	0	2	2	0	2	0
4	0	0	0	2	2	2	2	2	0	2	0	0	0	2	0	2
5	0	12	2	0	0	0	0	0	2	0	2	0	2	2	2	0
6	0	2	0	2	0	0	0	2	0	0	2	0	2	2	2	2
7	2	2	0	0	2	2	2	0	2	0	2	0	2	0	0	0
8	0	0	0	2	2	0	2	0	2	0	2	0	0	0	2	0
9	0	0	12	2	0	2	0	2	2	0	2	2	2	0	2	0
A	0	16	0	0	0	0	2	0	0	2	0	2	2	2	0	2
B	2	2	0	0	0	2	0	0	0	2	0	0	12	0	0	0
C	0	0	2	0	2	0	2	0	2	2	0	0	2	0	2	2
D	2	0	0	2	2	2	2	0	0	0	0	0	0	0	12	2
E	0	0	2	2	2	0	0	0	0	0	0	0	0	0	2	0
F	0	0	0	2	0	0	0	0	2	0	0	2	2	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	8	8	-8	8	0	0	-8	-8	-8	8	8	-8	-8	8
1	0	0	-8	-8	-8	8	0	0	-8	8	8	-8	-8	-8	-8	8
2	-8	8	8	8	-8	-8	-8	-8	0	0	8	-8	8	8	0	0
3	8	-8	8	-8	-8	-8	-8	8	0	0	-8	8	-8	-8	0	0
4	-8	-8	-8	8	-8	-8	-8	-8	0	0	8	-8	8	8	0	0
5	8	-8	-8	-8	8	8	-8	-8	32	0	-8	-8	8	-8	0	0
6	0	0	8	8	8	-8	0	0	8	8	8	-8	-8	-8	8	8
7	0	0	-8	8	-8	-8	-32	0	-8	-8	8	-8	8	-8	-8	8
8	8	8	0	0	0	0	8	-8	8	-8	8	-8	-8	-8	-8	8
9	8	8	0	0	0	0	-8	8	8	8	8	-8	-8	8	-8	8
A	8	8	-8	-8	8	-8	-8	-8	-8	8	0	0	0	0	8	8
B	8	8	-8	8	-8	8	-8	8	-8	8	0	0	0	0	8	8
C	8	8	8	8	8	8	8	-8	-8	8	0	0	0	0	-8	-8
D	-8	-8	-8	-8	8	-8	8	8	-8	-8	0	0	0	32	8	-8
E	-8	-8	0	0	0	0	-8	8	8	8	-8	-8	-8	-8	-8	8
F	-8	8	-32	0	0	0	-8	-8	8	-8	-8	8	-8	-8	8	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{61}$ Üs Haritalaması L_{AS2} ="95"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	E9	91	CB	AB	C6	56	4C	68	5A	11	CA	35	EB	97	A2	C2
1	2E	79	BE	0D	96	78	BC	D6	72	FB	CC	64	ED	DA	7A	DD
2	29	09	84	0C	8D	E0	0F	4E	85	BA	FA	A4	73	CD	FD	1D
3	07	16	49	2B	22	48	17	E5	D7	51	1E	80	DF	9F	23	FE
4	4A	F8	F1	EA	8E	70	3E	B3	12	7F	18	AF	AA	4F	BD	9E
5	82	0A	EC	C4	6B	4D	55	3C	E8	93	A9	E3	62	EE	89	C8
6	3A	14	2C	F4	05	F2	95	F5	57	61	FC	9C	94	36	B8	54
7	33	63	04	92	B7	D2	BB	EF	06	38	32	43	71	03	E1	87
8	08	45	10	AD	F0	90	01	65	99	F9	AC	37	59	98	15	6E
9	3F	8F	9A	7D	00	46	1C	4B	DE	86	69	5B	2D	BF	7B	A5
A	A3	83	1A	1F	E2	B0	28	C1	2F	B1	20	3B	D4	C0	44	41
B	81	67	34	B9	A0	26	30	52	7C	40	6C	66	B6	0B	D5	0E
C	8B	D9	1B	24	31	19	9B	9D	F6	A8	CF	C5	D8	2A	B5	27
D	8A	F7	5C	60	F3	DC	13	75	FF	E7	6F	B2	50	39	5E	58
E	AE	CE	C9	D0	A6	25	42	02	6A	D1	47	A1	C7	A7	C3	8C
F	21	B4	D3	E4	88	76	53	5D	E6	5F	74	3D	DB	6D	7E	77

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	4	4	0	0	2	4	0	0	0	2	0
1	0	2	0	0	2	0	0	0	2	2	0	4	0	0	0	0
2	4	0	0	2	2	0	2	0	4	0	0	0	0	0	2	2
3	0	0	2	0	0	0	2	4	0	0	0	0	4	0	2	4
4	4	4	0	0	0	0	2	0	0	2	2	2	0	2	0	2
5	2	0	4	0	2	0	0	4	2	0	0	0	0	0	4	0
6	16	0	4	0	2	2	4	0	0	4	4	0	0	4	0	0
7	0	2	2	0	0	0	0	0	2	0	0	4	2	2	0	0
8	0	0	0	2	0	0	4	0	4	2	0	0	2	4	0	0
9	2	0	4	0	0	2	2	0	0	0	0	2	0	0	4	0
A	0	0	2	0	0	0	0	2	2	0	0	0	0	0	0	0
B	2	0	2	2	0	0	2	2	0	2	0	2	0	4	2	0
C	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	2	0	0	2	0	4	2	0
E	2	0	0	0	0	2	4	2	0	2	0	0	2	0	2	0
F	0	0	4	0	0	0	0	2	0	0	0	0	0	0	4	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	-8	0	8	-8	-8	-8	-8	-8	0	0	0	8	0	8
1	0	0	8	-8	8	0	8	-16	-8	16	-16	-8	0	0	0	0
2	0	-8	0	8	-8	8	0	0	8	-8	8	8	-32	8	-8	0
3	0	0	0	0	-8	0	0	-8	8	0	8	0	0	-16	8	-8
4	8	8	8	-8	0	8	8	16	8	0	8	0	0	0	-8	-8
5	8	0	8	0	0	0	8	8	8	-8	8	8	16	-8	-8	0
6	0	0	8	-8	8	0	-8	0	0	8	8	-16	-8	-8	8	-8
7	0	-8	8	0	-8	8	8	8	0	0	8	-8	-8	0	-8	-16
8	0	8	0	8	8	8	0	-16	8	-8	8	8	16	8	-8	0
9	-8	-8	8	8	-16	8	8	0	0	8	0	-8	-8	-8	0	0
A	0	8	8	0	-8	8	8	8	8	-8	-16	0	0	8	16	8
B	-8	8	0	0	0	-8	0	-8	16	8	8	0	-8	-8	-8	-8
C	8	-8	0	16	0	8	16	8	8	0	0	-8	16	-16	0	0
D	0	-8	8	0	-8	-8	8	8	0	0	-8	-8	-8	0	8	0
E	0	0	-16	16	-8	0	0	8	0	-8	0	-8	-8	8	0	0
F	-8	0	-8	0	0	0	8	-8	8	8	8	8	0	-8	8	32

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{91}$ Üs Haritalaması $L_{A_{S2}}$ ="59"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	71	04	19	A8	58	06	3C	B5	84	DD	1E	5B	1C	D6	E0	51
1	63	92	F9	AC	9B	96	70	3E	34	90	BF	D5	CB	0B	54	56
2	33	25	79	32	F6	49	E6	8D	81	76	9A	1B	30	0D	A4	98
3	A3	CF	12	CA	A6	89	DB	07	DC	45	D3	87	4B	17	5E	E9
4	D0	15	DE	6C	3A	1A	F2	48	22	8F	61	E4	55	29	8E	0C
5	08	EA	14	FC	52	4F	97	62	8B	5F	CC	3F	FB	43	AD	74
6	F5	9D	DA	E1	C3	B7	59	E8	C7	D8	A0	11	A1	7F	1D	4A
7	86	7B	95	C6	B6	36	C9	44	7C	F4	7E	37	24	6E	BE	B8
8	C4	B4	02	D2	99	28	21	47	60	D1	CE	03	53	AF	4D	2E
9	A9	3D	93	27	FE	4E	9F	D7	01	35	B1	80	BA	B9	BC	69
A	6F	2C	72	D4	94	78	F8	85	0E	A7	0A	9C	F7	7D	6D	B2
B	F0	5A	E2	39	10	EF	8A	E5	F3	E3	00	A2	38	AB	83	C2
C	B0	2D	2A	0F	AE	05	9E	8C	6B	13	FD	2F	16	77	FA	EB
D	46	BD	B3	5C	1F	F1	41	EE	57	C0	CD	65	6A	DF	31	AA
E	D9	68	67	A5	18	2B	C5	66	73	5D	3B	23	20	91	75	40
F	ED	E7	09	C1	88	7A	FF	42	4C	50	64	26	C8	EC	BB	82

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	2	2	0	0	2	0	0	0	2	0	0	2	0	0
1	2	2	2	0	0	0	2	0	2	0	0	0	2	2	0	2
2	2	0	0	0	2	2	0	0	0	0	0	0	0	0	2	2
3	0	2	0	2	2	2	0	0	0	2	0	2	2	2	0	0
4	0	2	2	2	0	2	0	0	2	2	2	2	0	0	2	0
5	0	0	0	2	2	2	0	2	0	2	0	0	2	0	2	0
6	0	2	0	2	0	0	2	0	2	0	2	2	2	0	0	2
7	2	0	0	0	2	2	0	0	2	0	0	0	2	2	0	0
8	2	2	2	0	0	2	0	0	2	2	2	0	0	2	0	0
9	0	0	0	2	2	0	2	2	0	2	0	2	0	2	0	0
A	0	0	2	2	2	0	2	0	2	2	2	2	0	2	0	2
B	2	16	2	0	2	2	0	2	2	0	2	0	0	2	0	2
C	2	0	2	0	0	2	0	0	2	0	2	0	0	2	0	0
D	2	0	2	0	2	2	0	0	2	2	0	2	2	0	2	2
E	0	0	2	0	0	0	0	0	2	0	0	0	2	0	2	2
F	0	2	2	2	0	2	0	2	0	0	0	2	2	2	0	2

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	0	0	16	-16	0	8	0	0	8	16	8	0	0	0
1	-16	0	8	-8	0	0	0	0	8	8	0	0	0	-16	16	-16
2	0	0	0	0	-8	-8	0	0	-16	-8	-8	0	-16	8	-16	-8
3	8	0	0	0	8	-8	0	8	-8	-16	0	-16	0	0	8	0
4	0	16	0	0	8	-8	8	-8	0	0	16	0	0	-16	0	0
5	0	8	0	-16	16	0	8	0	8	-8	0	8	0	8	-16	0
6	8	0	-8	-8	0	16	8	0	0	8	0	0	0	0	-8	0
7	-8	8	-8	8	16	0	0	0	0	-8	8	0	0	-8	8	0
8	-8	8	16	0	8	8	0	-16	8	0	0	-8	8	0	0	-8
9	0	-8	-16	0	8	8	0	-8	-8	0	16	0	0	0	16	8
A	0	8	0	-16	-8	8	16	8	0	16	-16	-8	8	0	0	0
B	-16	0	8	-8	8	-8	0	0	0	0	0	0	8	8	8	8
C	0	16	8	0	8	16	0	0	-8	8	-8	0	0	8	0	0
D	-8	0	0	-8	0	8	0	-8	8	-8	0	0	0	16	-16	0
E	8	0	8	0	0	-8	8	0	-8	0	0	8	16	8	0	8
F	16	-16	0	8	0	8	0	0	0	-8	0	16	-16	0	-16	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{119}$ Üs Haritalaması L_{AS2} ="B4"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B2	82	84	AD	AB	2F	19	30	19	29	2F	AD	19	AD	36	00
1	30	30	AD	AB	9B	19	06	9D	9D	82	30	AD	29	29	2F	9B
2	AB	B2	2F	36	19	36	00	AD	36	19	2F	06	30	00	30	1F
3	29	36	00	9B	1F	19	1F	84	06	29	1F	84	06	AD	30	36
4	84	9D	84	36	2F	9D	36	2F	84	82	1F	30	9D	84	B2	29
5	82	30	29	82	29	36	19	B2	06	AD	06	AB	00	84	29	82
6	19	29	36	B2	00	9D	B4	82	9B	29	30	9B	AB	2F	82	1F
7	84	2F	AD	30	2F	2F	00	1F	9B	9B	06	82	06	36	9D	06
8	30	19	06	1F	19	AB	29	9B	9D	1F	9D	00	AD	2F	B2	9D
9	9B	84	9B	19	06	82	84	84	00	1F	19	19	B2	1F	9D	82
A	84	36	AD	1F	9D	9B	30	00	00	29	AB	B2	B2	29	1F	AD
B	B2	9B	30	82	36	30	82	AB	9B	00	30	9D	B2	9B	84	00
C	9B	9D	84	82	00	AD	AB	00	2F	06	00	AB	29	00	2F	9D
D	AB	06	82	AB	AB	36	19	1F	AB	36	29	06	B2	19	30	9D
E	B2	06	AD	19	B2	36	B2	9D	1F	82	06	1F	29	2F	82	B2
F	2F	9B	AB	AB	1F	B2	84	2F	84	9B	06	36	AD	AB	AD	AD

S-kutusu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	22	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	16	0	0	0	0	0	16
2	0	0	0	0	0	0	0	0	0	22	0	0	0	0	0	16
3	16	0	0	0	0	0	4	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	10	0	16	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	16	0	16	0	0
A	0	0	0	0	0	0	0	0	0	0	0	22	0	16	0	0
B	0	0	22	0	10	0	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	0	8	8	8	4	-4	4	-4	8	0	8	8	-4	4	-4	4
1	4	-4	-4	4	-16	-16	8	8	-4	4	4	-4	-16	-16	8	8
2	-4	4	4	-4	-16	-16	8	8	4	-4	-4	4	-16	-16	8	8
3	8	0	8	8	-4	4	-4	4	0	8	8	8	4	-4	4	-4
4	0	8	8	8	4	-4	4	-4	8	0	8	8	-4	4	-4	4
5	4	-4	-4	4	-16	-16	8	8	-4	4	4	-4	-16	-16	8	8
6	-4	4	4	-4	-16	-16	8	8	4	-4	-4	4	-16	-16	8	8
7	8	0	8	8	-4	4	-4	4	0	8	8	8	4	-4	4	-4
8	4	-4	4	-4	8	8	0	8	-4	4	-4	4	8	8	8	0
9	8	8	-16	-16	-4	4	4	-4	8	8	-16	-16	4	-4	-4	4
A	8	8	-16	-16	4	-4	-4	4	8	8	-16	-16	-4	4	4	-4
B	-4	4	-4	4	8	8	8	0	4	-4	4	-4	8	8	0	8
C	4	-4	4	-4	8	8	0	8	-4	4	-4	4	8	8	8	0
D	8	8	-16	-16	-4	4	4	-4	8	8	-16	-16	4	-4	-4	4
E	8	8	-16	-16	4	-4	-4	4	8	8	-16	-16	-4	4	4	-4
F	-4	4	-4	4	8	8	8	0	4	-4	4	-4	8	8	0	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{27}$ Üs Haritalaması L_{AS2} ="53"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	25	77	3A	56	00	F2	7F	3D	F6	65	E8	5D	7E	94	01	01
1	F6	9A	39	CB	8C	02	65	9A	80	D2	05	22	46	23	AE	13
2	EF	03	E5	D2	3D	58	C7	AB	06	63	EE	13	7F	58	85	AA
3	8D	1E	77	49	E5	80	CE	B5	89	D4	AE	EE	49	25	17	97
4	54	44	AE	C1	0A	3D	D7	E0	BF	4F	98	80	7F	0A	35	95
5	2B	0E	13	C1	DA	77	E2	A6	20	4C	DA	25	D2	98	28	AD
6	9A	37	2A	E6	A9	B9	53	01	DA	49	33	0D	52	CC	58	0A
7	E5	98	15	57	3B	69	C1	EE	37	65	F5	A7	DD	1C	F6	37
8	63	44	23	3B	33	56	20	8D	33	3A	E2	97	03	BF	22	57
9	46	3B	89	0E	95	C7	CC	F2	AD	B5	57	05	00	CC	85	D7
A	CE	AD	EF	BF	0E	D4	44	06	1C	8C	E6	5D	39	F5	E8	E6
B	CB	F5	02	1C	A9	7E	A9	94	20	1E	E2	17	AB	95	AA	D7
C	DD	02	E8	2A	A7	CB	5D	2A	B5	28	4F	03	89	2B	54	63
D	4C	8D	97	A6	35	C7	85	E0	39	A7	DD	8C	94	B9	B9	7E
E	56	0D	A6	17	EF	4F	15	05	54	06	46	69	0D	3A	1E	4C
F	CE	28	15	22	F2	52	E0	AA	69	23	D4	2B	35	AB	00	52

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	0	0	0	0	0	0	0	0	2	0	0	0	0	2	0
1	6	0	0	0	0	0	0	0	6	0	0	0	0	0	2	0
2	0	0	0	0	0	2	0	6	0	0	0	0	0	2	0	6
3	0	2	0	0	0	0	0	12	0	0	0	0	0	2	12	0
4	2	0	6	0	2	0	0	0	0	0	6	0	2	0	0	0
5	2	2	26	0	0	0	0	0	0	0	0	2	0	2	0	0
6	0	0	0	2	0	12	0	0	0	0	0	0	12	0	0	2
7	0	0	0	0	0	6	0	2	0	0	0	2	0	6	0	0
8	2	0	0	0	0	2	0	2	0	0	0	0	0	0	2	0
9	2	0	0	6	0	0	0	0	0	0	0	0	0	2	6	0
A	6	0	2	0	0	0	0	0	0	0	0	0	0	6	0	0
B	0	2	0	0	0	2	0	0	0	0	0	2	2	2	0	0
C	0	6	2	0	0	0	0	2	0	0	0	0	6	0	0	0
D	0	0	2	0	0	0	0	2	0	0	2	0	0	0	0	2
E	0	0	0	0	0	0	2	0	0	0	2	0	2	0	0	0
F	2	0	6	0	0	2	0	0	0	0	0	0	0	2	0	6

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	8	-8	0	0	8	8	0	8	8	0	0	0	-16	16
1	0	8	0	0	0	8	16	0	0	0	0	0	0	16	-8	-8
2	-8	0	0	-8	0	0	-8	8	0	0	8	8	-8	0	8	0
3	0	0	-8	0	0	-8	8	8	8	0	-8	0	-8	0	0	8
4	-8	-8	16	0	8	-8	8	0	8	0	0	8	0	24	-8	8
5	0	0	8	8	0	-8	8	-8	-8	8	8	16	0	0	8	8
6	0	-8	0	8	0	16	0	-8	0	8	0	-24	-8	0	0	0
7	8	-8	8	8	8	8	-16	-8	0	-8	0	0	-8	0	-8	0
8	-8	0	8	16	0	0	0	0	16	8	8	0	0	0	8	8
9	-16	16	-8	8	0	0	8	8	0	8	-8	8	8	-8	48	-8
A	0	8	0	8	0	0	0	0	8	0	0	-8	-8	0	0	-8
B	8	-8	0	0	8	8	0	0	-8	0	-8	-8	8	0	-8	8
C	8	0	8	0	0	16	0	8	0	0	0	0	0	0	0	8
D	-8	8	0	24	0	8	0	-8	0	8	8	0	16	0	0	-8
E	-8	8	0	0	0	8	0	0	-16	0	8	8	8	0	8	-8
F	-8	8	0	8	0	-24	8	0	0	0	0	16	8	8	-8	0

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{43}$ Üs Haritalaması $L_{A_{S2}}$ ="C5"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	A4	AC	BD	C7	5D	24	82	4C	33	F5	F8	09	DE	CF	15	A8
1	BE	03	54	AF	92	C8	6E	25	FD	5A	4B	4A	AB	16	F9	EB
2	A3	E6	40	2D	66	0B	2B	FB	1C	71	D7	BA	B6	52	1A	35
3	0C	0A	C9	19	0F	E7	68	51	F0	E8	07	44	1D	11	B5	BB
4	97	4E	3B	6A	21	EF	EA	87	CE	73	37	DF	F1	3F	7D	93
5	38	85	94	29	74	A0	06	6B	B7	C3	7C	70	B2	90	81	3C
6	E3	98	28	45	A2	72	C5	78	CD	C1	D0	7A	30	F4	9C	DB
7	8A	62	27	9B	E2	8F	86	56	8E	5E	53	C2	75	18	48	D3
8	F3	2A	8C	C6	AA	02	13	67	BF	6F	D8	08	1E	50	F6	A9
9	32	E1	55	0D	46	AD	BC	01	FC	2C	F7	9A	D1	8D	3A	58
A	41	05	8B	5B	4D	9D	A1	FA	22	A5	B4	59	12	E9	E4	34
B	84	7F	42	FF	69	1F	0E	B3	61	B1	1B	D6	FE	10	57	77
C	9F	4F	D9	64	3E	EE	95	89	B8	D5	36	3D	60	20	9E	47
D	DA	AE	76	CB	96	43	E5	CA	83	39	2F	F2	B9	D4	63	04
E	00	6D	65	A6	ED	80	26	14	CC	23	5C	7B	D2	17	7E	DC
F	EC	91	C4	79	E0	6C	88	A7	31	5F	B0	DD	2E	C0	49	99

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	2	0	0	0	0	2	0	2	0	0	2	6	0	2	0
1	0	2	2	0	0	0	0	0	2	0	0	0	2	0	0	0
2	2	0	2	0	0	0	0	2	0	0	0	0	0	0	0	6
3	0	0	2	0	0	0	0	0	0	2	0	0	0	0	0	0
4	2	0	0	2	2	2	0	2	0	0	2	2	0	0	2	0
5	0	2	0	0	0	0	0	0	2	0	2	2	2	0	0	2
6	0	0	2	0	0	0	0	2	0	0	0	0	0	30	2	0
7	0	0	0	0	6	0	2	0	0	2	2	2	0	2	0	0
8	0	0	0	0	0	0	0	2	0	0	0	0	2	0	0	0
9	0	2	0	0	0	0	0	0	0	0	0	2	0	0	0	0
A	0	0	2	0	0	0	0	2	2	0	2	0	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	2	0	2	28	0	0
C	0	0	0	2	2	2	2	0	0	0	0	0	0	2	6	0
D	30	0	0	2	2	2	0	0	0	6	0	0	0	2	0	0
E	0	0	0	0	2	0	0	0	6	0	0	2	0	2	6	2
F	0	2	0	0	0	0	0	0	0	0	0	6	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	16	0	-8	-8	-8	0	8	8	-8	-8	0	8	8	0	-8
1	-8	0	0	0	16	-8	0	0	0	8	8	-8	0	-8	0	0
2	-8	0	0	0	-8	0	-8	-8	-8	0	0	0	0	8	0	0
3	8	8	8	0	-8	-8	16	8	-8	8	-8	0	0	0	8	0
4	8	8	-32	8	0	0	0	-8	0	0	8	-16	0	0	0	-8
5	-8	0	-8	8	0	-8	8	-8	0	-8	0	0	0	-8	8	-8
6	0	8	0	0	-16	-8	-8	8	0	-8	0	0	8	0	0	16
7	8	8	0	8	8	8	8	0	8	-8	0	8	0	0	0	8
8	-8	-8	-8	0	0	0	8	16	0	0	0	-8	0	0	8	0
9	8	0	0	0	0	8	48	0	0	8	-8	-8	0	8	0	0
A	0	-8	8	8	0	8	-16	0	0	8	-8	8	8	0	8	8
B	-8	8	-8	0	8	8	0	-8	8	8	8	0	0	0	8	0
C	0	0	-8	0	8	8	8	0	-8	-8	0	8	8	8	8	0
D	-8	0	8	8	-48	8	-8	-8	0	8	0	0	0	8	-8	8
E	-8	0	8	-8	-8	0	0	0	-8	0	8	8	0	8	-8	8
F	-8	-8	0	8	-8	-8	8	0	8	-8	0	8	0	0	0	8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{87}$ Üs Haritalaması L_{AS2} ="93"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C0	EA	32	2F	66	58	84	BE	45	A5	FB	E5	BF	F5	01	01
1	45	D7	C3	9D	D3	79	A5	D7	FD	98	40	F9	14	86	20	1D
2	D5	26	FA	98	BE	DC	12	E2	C1	A3	7F	1D	84	DC	CE	28
3	E8	07	EA	1A	FA	FD	0E	2E	E0	35	20	7F	1A	C0	F3	C6
4	6A	5A	20	8F	A9	BE	17	75	25	B7	94	FD	84	A9	92	E3
5	57	C5	1D	8F	49	EA	36	54	F7	8C	49	C0	98	94	4C	DE
6	D7	55	69	0B	67	97	93	01	49	1A	C2	4D	96	CA	DC	A9
7	FA	94	6B	22	0C	6E	8F	7F	55	A5	CD	6D	89	EB	45	55
8	A3	5A	86	0C	C2	2F	F7	E8	C2	32	36	C6	26	25	F9	22
9	14	0C	E0	C5	E3	12	CA	58	DE	2E	22	40	66	CA	CE	17
A	0E	DE	D5	25	C5	35	5A	C1	EB	D3	0B	E5	C3	CD	FB	0B
B	9D	CD	79	EB	67	BF	67	F5	F7	07	36	F3	E2	E3	28	17
C	89	79	FB	69	6D	9D	E5	69	2E	4C	B7	26	E0	57	6A	A3
D	8C	E8	C6	54	92	12	CE	75	C3	6D	89	D3	F5	97	97	BF
E	2F	4D	54	F3	D5	B7	6B	40	6A	C1	14	6E	4D	32	07	8C
F	0E	4C	6B	F9	58	96	75	28	6E	86	35	57	92	E2	66	96

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	2	0	2	0	0	0	2	0	0	0	0	2	0	2	0
1	2	0	0	0	0	0	0	2	2	0	0	0	0	2	2	2
2	2	0	0	0	0	2	0	0	2	0	2	2	0	2	0	0
3	2	0	0	0	0	2	0	0	2	0	2	0	0	2	2	2
4	0	0	2	0	0	0	0	0	0	2	2	0	0	0	0	0
5	2	0	0	2	0	0	0	0	2	0	2	0	2	2	2	2
6	0	0	30	0	2	2	0	0	0	2	0	0	0	0	2	0
7	2	2	2	0	0	2	0	0	0	0	2	2	0	0	0	2
8	2	0	2	0	0	0	0	0	0	2	2	2	2	0	0	2
9	0	2	26	0	0	0	0	0	0	0	0	2	0	0	0	0
A	2	0	0	2	0	0	0	2	0	0	2	2	2	0	2	2
B	0	0	0	0	0	0	0	2	0	2	0	2	0	0	0	0
C	0	0	0	0	0	2	0	0	0	2	0	0	0	0	2	0
D	2	0	0	0	0	2	0	0	2	2	2	2	0	0	0	0
E	2	0	0	0	0	0	2	0	2	0	0	0	0	2	2	2
F	30	2	0	2	0	0	0	0	0	2	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	8	-8	0	8	-8	0	0	8	8	8	8	-8	8	0	0
1	8	0	0	0	0	0	8	0	0	0	0	16	0	8	-8	0
2	0	-8	8	-16	0	-8	-8	0	0	0	0	0	8	8	-48	0
3	8	0	-8	-8	0	-8	0	0	-8	-8	-8	8	-8	0	-16	-8
4	-8	8	16	0	0	-8	0	0	0	8	0	8	8	-8	-8	0
5	-8	0	8	0	0	8	0	0	-8	0	8	8	0	0	8	-8
6	8	8	-8	8	0	0	0	-8	0	0	8	8	-8	0	8	-8
7	0	0	8	-8	-8	0	8	8	0	8	0	0	-8	-8	8	8
8	0	0	0	0	-8	-8	8	8	0	0	0	0	-8	-8	8	8
9	8	-8	-8	-8	8	16	-8	0	0	-8	8	-8	-16	8	8	8
A	-8	0	8	0	-8	0	8	0	-8	0	8	0	0	0	0	0
B	-8	0	8	-16	-8	8	8	8	0	0	0	-8	8	0	-8	8
C	0	8	0	8	-8	0	8	8	0	0	8	8	8	0	0	0
D	-16	8	0	0	8	0	0	8	0	0	-8	8	40	8	-8	0
E	0	8	-8	0	-8	0	-8	8	0	-8	0	-8	0	-8	-8	-8
F	8	8	-40	0	0	0	0	0	-8	-8	-8	-8	8	0	8	-8

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{51}$ Üs Haritalaması L_{AS2} ="A9"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	B6	99	9F	B6	B6	9F	34	34	34	2D	9F	B6	34	B6	99	99
1	34	34	B6	B6	2D	34	2D	34	34	99	34	B6	2D	2D	9F	2D
2	B6	B6	9F	99	34	99	99	B6	99	34	9F	2D	34	99	34	9F
3	2D	99	99	2D	9F	34	9F	9F	2D	2D	9F	9F	2D	B6	34	99
4	9F	34	9F	99	9F	34	99	9F	9F	99	9F	34	34	9F	B6	2D
5	99	34	2D	99	2D	99	34	B6	2D	B6	2D	B6	99	9F	2D	99
6	34	2D	99	B6	99	34	A9	99	2D	2D	34	2D	B6	9F	99	9F
7	9F	9F	B6	34	9F	9F	99	9F	2D	2D	2D	99	2D	99	34	2D
8	34	34	2D	9F	34	B6	2D	2D	34	9F	34	99	B6	9F	B6	34
9	2D	9F	2D	34	2D	99	9F	9F	99	9F	34	34	B6	9F	34	99
A	9F	99	B6	9F	34	2D	34	99	99	2D	B6	B6	B6	2D	9F	B6
B	B6	2D	34	99	99	34	99	B6	2D	99	34	34	B6	2D	9F	99
C	2D	34	9F	99	99	B6	B6	99	9F	2D	99	B6	2D	99	9F	34
D	B6	2D	99	B6	B6	99	34	9F	B6	99	2D	2D	B6	34	34	34
E	B6	2D	B6	34	B6	99	B6	34	9F	99	2D	9F	2D	9F	99	B6
F	9F	2D	B6	B6	9F	B6	9F	9F	9F	2D	2D	99	B6	B6	B6	B6

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	50	0	0	0	0	0	24	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	18	0	0	0	0	0	24
3	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	18	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	18	0	0	0	0
A	0	0	0	0	0	0	0	0	0	0	0	18	0	24	0	0
B	0	0	18	0	24	0	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	6	-6	6	-12	6	-6	6	6	0	6	-6	6	-12	6	-6
1	4	-10	10	-10	10	-4	4	-4	-10	4	-10	10	-4	10	-4	4
2	-10	4	-10	10	-4	10	-4	4	4	-10	10	-10	10	-4	4	-4
3	6	0	6	-6	6	-12	6	-6	0	6	-6	6	-12	6	-6	6
4	0	6	-6	6	-12	6	-6	6	6	0	6	-6	6	-12	6	-6
5	4	-10	10	-10	10	-4	4	-4	-10	4	-10	10	-4	10	-4	4
6	-10	4	-10	10	-4	10	-4	4	4	-10	10	-10	10	-4	4	-4
7	6	0	6	-6	6	-12	6	-6	0	6	-6	6	-12	6	-6	6
8	6	-6	12	-6	6	-6	0	-6	-6	6	-6	12	-6	6	-6	0
9	-4	4	-10	4	-10	10	-4	10	4	-4	4	-10	10	-10	10	-4
A	4	-4	4	-10	10	-10	10	-4	-4	4	-10	4	-10	10	-4	10
B	-6	6	-6	12	-6	6	-6	0	6	-6	12	-6	6	-6	0	-6
C	6	-6	12	-6	6	-6	0	-6	-6	6	-6	12	-6	6	-6	0
D	-4	4	-10	4	-10	10	-4	10	4	-4	4	-10	10	-10	10	-4
E	4	-4	4	-10	10	-10	10	-4	-4	4	-10	4	-10	10	-4	10
F	-6	6	-6	12	-6	6	-6	0	6	-6	12	-6	6	-6	0	-6

"01" Giriş Maskesi için LAT Dağılımı

$X \rightarrow X^{85}$ Üs Haritalaması L_{AS2} ="17"

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0E	08	08	11	08	0E	0E	08	0E	08	0E	11	0E	11	0E	11
1	08	08	11	08	11	0E	0E	11	11	08	08	11	08	08	0E	11
2	08	0E	0E	0E	0E	0E	11	11	0E	0E	0E	0E	08	11	08	11
3	08	0E	11	11	11	0E	11	08	0E	08	11	08	0E	11	08	0E
4	08	11	08	0E	0E	11	0E	0E	08	08	11	08	11	08	0E	08
5	08	08	08	08	08	0E	0E	0E	0E	11	0E	08	11	08	08	08
6	0E	08	0E	0E	11	11	17	08	11	08	08	11	08	0E	08	11
7	08	0E	11	08	0E	0E	11	11	11	11	0E	08	0E	0E	11	0E
8	08	0E	0E	11	0E	08	08	11	11	11	11	11	11	0E	0E	11
9	11	08	11	0E	0E	08	08	08	11	11	0E	0E	0E	11	11	08
A	08	0E	11	11	11	11	08	11	11	08	08	0E	0E	08	11	11
B	0E	11	08	08	0E	08	08	08	11	11	08	11	0E	11	08	11
C	11	11	08	08	11	11	08	11	0E	0E	11	08	08	11	0E	11
D	08	0E	08	08	08	0E	0E	11	08	0E	08	0E	0E	0E	08	11
E	0E	0E	11	0E	0E	0E	0E	11	11	08	0E	11	08	0E	08	0E
F	0E	11	08	08	11	0E	08	0E	08	11	0E	0E	11	08	11	11

S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	84	0	0	0	0	0	60	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0	0	0	60	0	0	0	0	0	52
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
D	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
E	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
F	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

"01" Giriş Farkı için DDT Dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
1	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
2	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
3	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
4	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
5	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
6	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
7	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
8	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
9	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
A	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
B	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
C	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
D	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10
E	0	10	-6	6	-6	6	0	10	-10	0	-6	6	-6	6	-10	0
F	10	0	6	-6	6	-6	10	0	0	-10	6	-6	6	-6	0	-10

"01" Giriş Maskesi için LAT Dağılımı