Önemli Blok Şifrelerde Kullanılan Doğrusal Dönüşümlerin İncelenmesi

Füsun Yavuzer ASLAN
Kırklareli Üniversitesi
M. Tolga SAKALLI
Trakya Üniversitesi
Bora ASLAN
Kırklareli Üniversitesi

Taslak

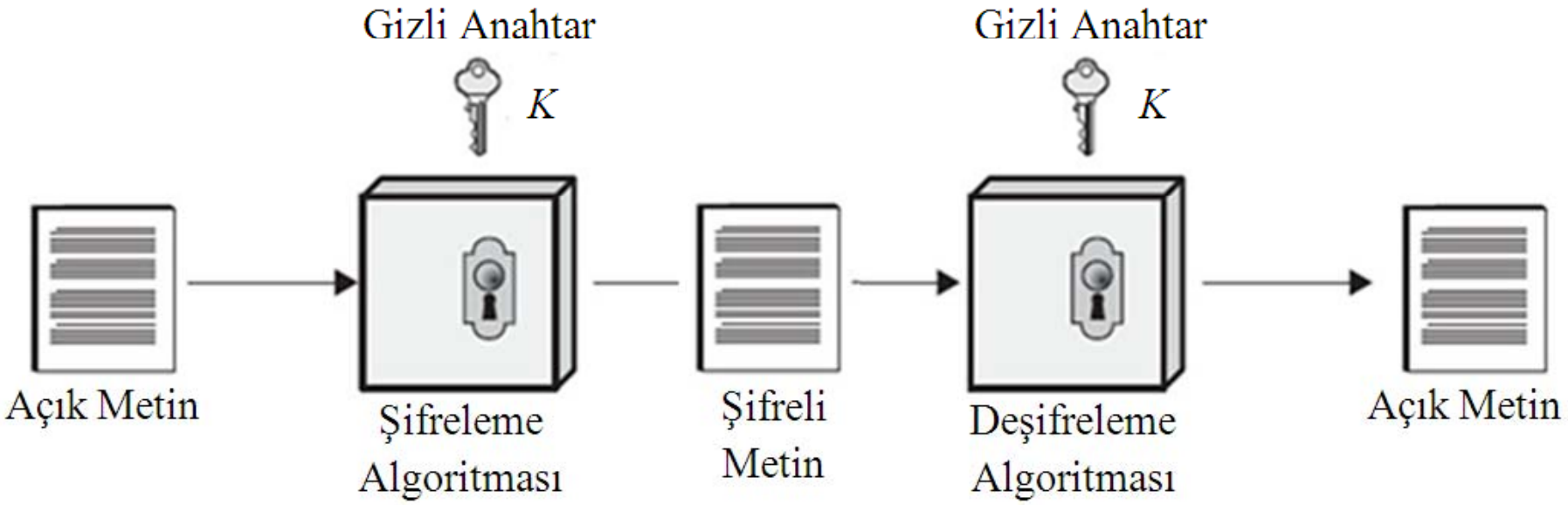
- Giriş
- Blok Şifreler
- Örnek Bir Blok Şifre : AES
- Matematiksel Altyapı
- Doğrusal Dönüşümler
- AES, Khazad, Camellia,Aria Doğrusal Dönüşümleri
- Sonuçlar

Kriptografi

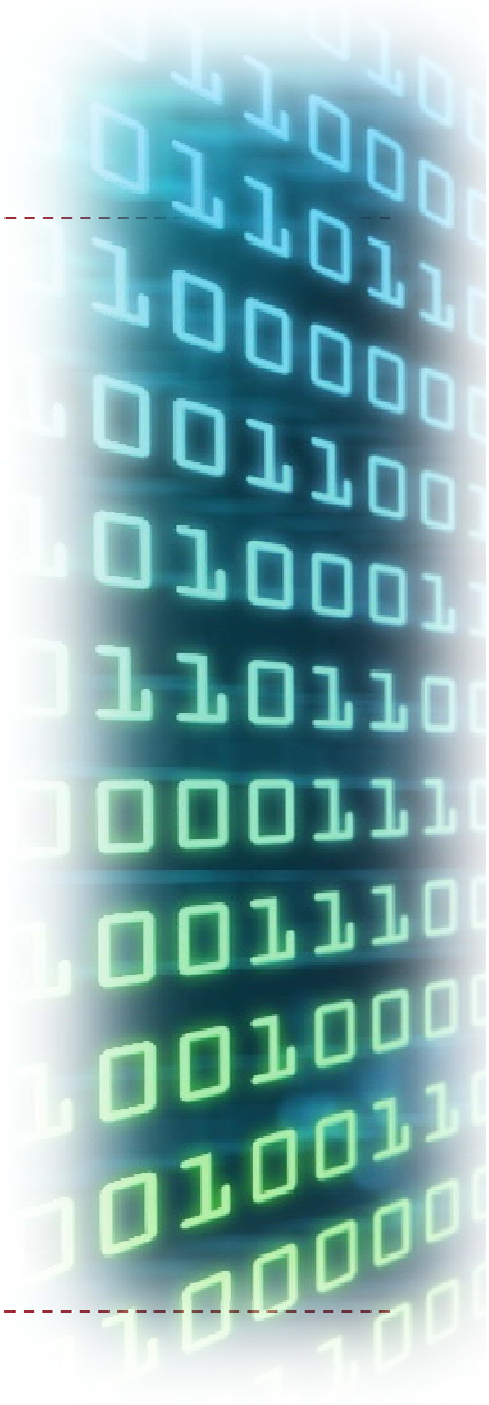
- “kryptos” + “graphien”= gizli yazı
- Kriptografi anlaşılır bir mesajı anlaşılmaz hale dönüştürme ve tekrar anlaşılmaz mesajı anlaşılır hale geri dönüştürme işlemlerinin bütünüdür.
- Kriptografi ile ilgilenen bilim adamlarına kriptograf adı verilir.
- Kriptanaliz ise ele geçirilen şifreli metinleri bazı teknikler kullanılarak açık metinleri elde etme işlemidir.
- Kriptanaliz ile ilgilenen kişilere kriptanalist denir.
- Kriptografi + Kriptanaliz = Kriptoloji

Bir Kriptosistemin Bileşenleri

- Şifreleme algoritması
- Açık metin
- Şifreli metin
- Anahtar



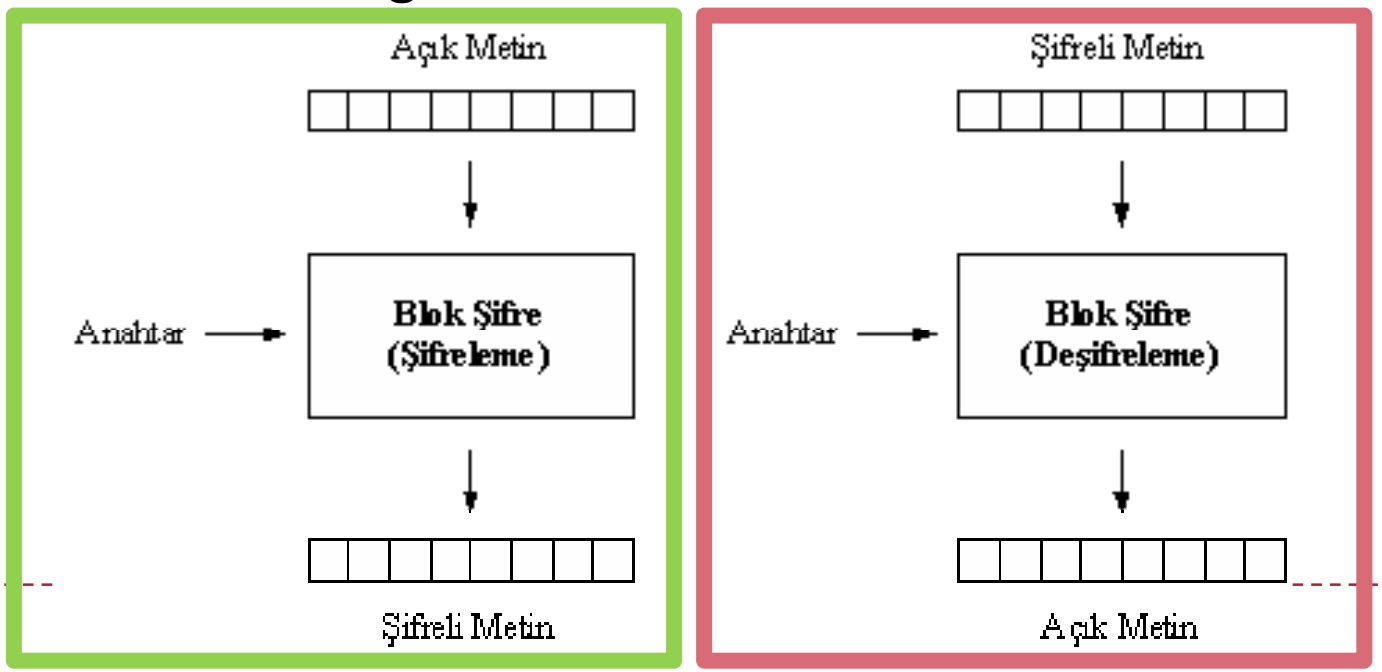
- Şifreleme algoritmaları
  - Simetrik Şifreleme Algoritmaları
    - Blok Şifreler
    - Akan Şifreler
  - Asimetrik Şifreleme Algoritmaları
  - Hash Algoritmalar



Simetrik Şifreleme Algoritmaları		Asimetrik Şifreleme Algoritmaları	Hash Algoritmaları
Blok Şifreler	Akan Şifreler		
-DES -IDEA -Square -AES -Camellia -ARIA -Khazad	-RC4 -Trivium - HC-256	- RSA - ElGamal - ECC	- MD4 - MD5 - SHA -RIPEMD-160

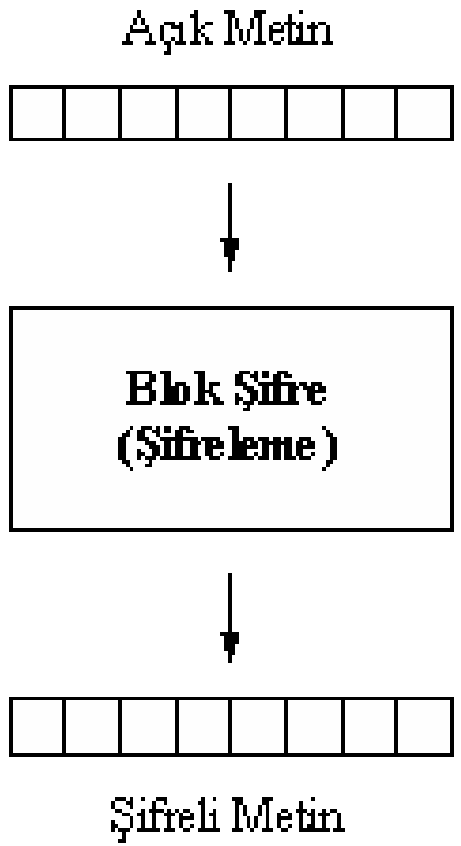
Blok Şifreler

- 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.



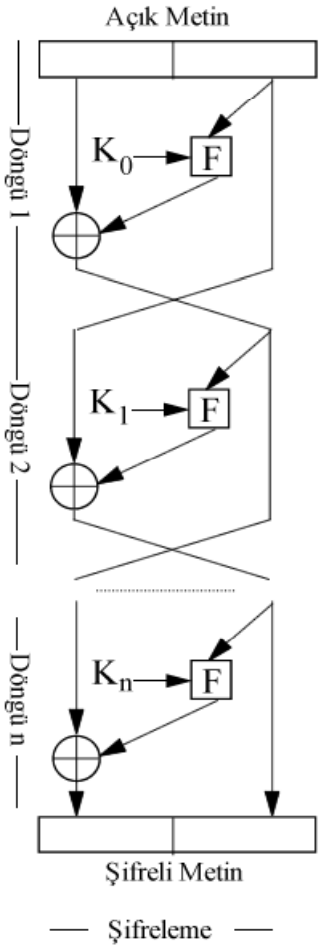
Blok Şifreler

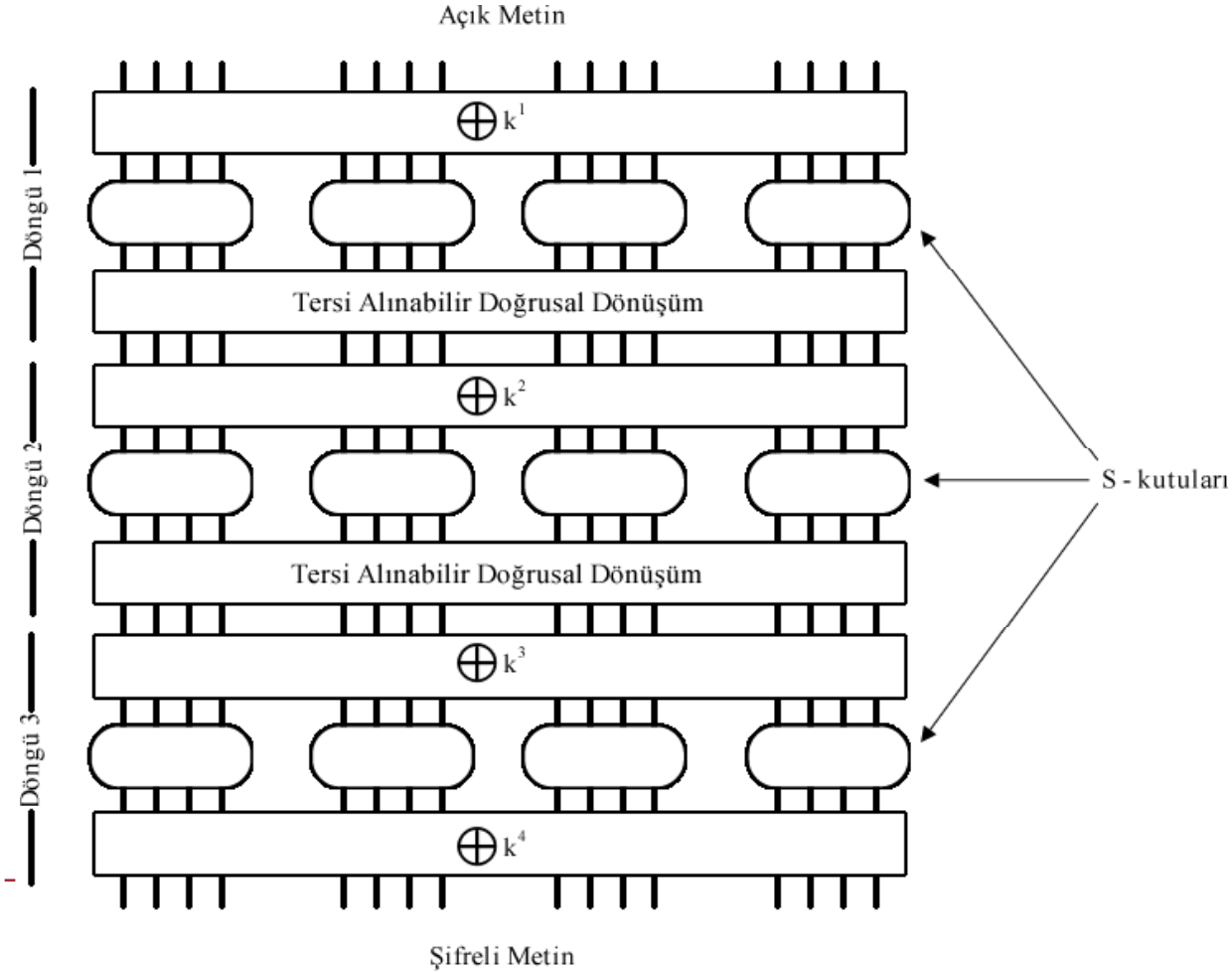
- Blok şifreler, Shannon'un önerdiği karıştırma (confusion) ve yayılma (diffusion) teknikleri üzerine kuruludur.
- Karıştırma, şifreli metin ve açık metin arasındaki ilişkiyi gizlemeyi amaçlarken; yayılma, açık metindeki izlerin şifreli metinde sezilmemesini sağlamak için kullanılır.
- Karıştırma yer değiştirme işlemi ile gerçekleştirilirken yayılma ise doğrusal dönüşüm işlemleri ile gerçeklenir.



Blok Şifreler

- Blok şifresi iki mimari üzerine kuruludur. Bunlar Feistel ağları ve Yer değiştirme-Permütasyon ağlarıdır (SPN).





Blok Şifreler

- Blok Şifrelerin gücünü belirleyen faktörler
  - Anahtar Büyüklüğü
  - S-kutuları (Yer değiştirme Kutuları)
  - Doğrusal dönüşümler

- Anahtar Büyüklüğü
  - Saldırılara karşı güçlü seçilmelidir

Blok Şifreler	Anahtar Uzunluğu
DES	56-bit
IDEA	128-bit
AES	128, 192, 256-bit
Camellia	128, 192, 256-bit
ARIA	128-bit
Khazad	128-bit

S-Kutuları (Substitution-boxes)

- Blok şifreleme algoritmalarının en önemli elemanı S-kutularıdır ve karıştırma işlevini üstlenirler.
- Algoritmanın tek doğrusal olmayan elemanıdır.
- Bu yüzden iyi bir S-kutusu seçimi şifrenin karmaşıklığını doğrudan etkiler.
- S-kutuları şifre içerisinde bit bloklarının yer değiştirmesinde kullanılır. Bit blokları S-kutusundan geçirilerek farklı bit bloklarına haritalanır.

Doğrusal Dönüşümler

- Blok şifrelerin önemli bir özelliği olan yayılma işlemini sağlayan yapılar doğrusal dönüşümlerdir.
- Doğrusal dönüşümler sabit uzunluktaki bir giriş bloğunu doğrusal olarak karıştırarak aynı uzunlukta bir çıkış bloğu elde etmeyi sağlar.

Örnek bir Blok Şifre: AES(Advanced Encryption Standart)

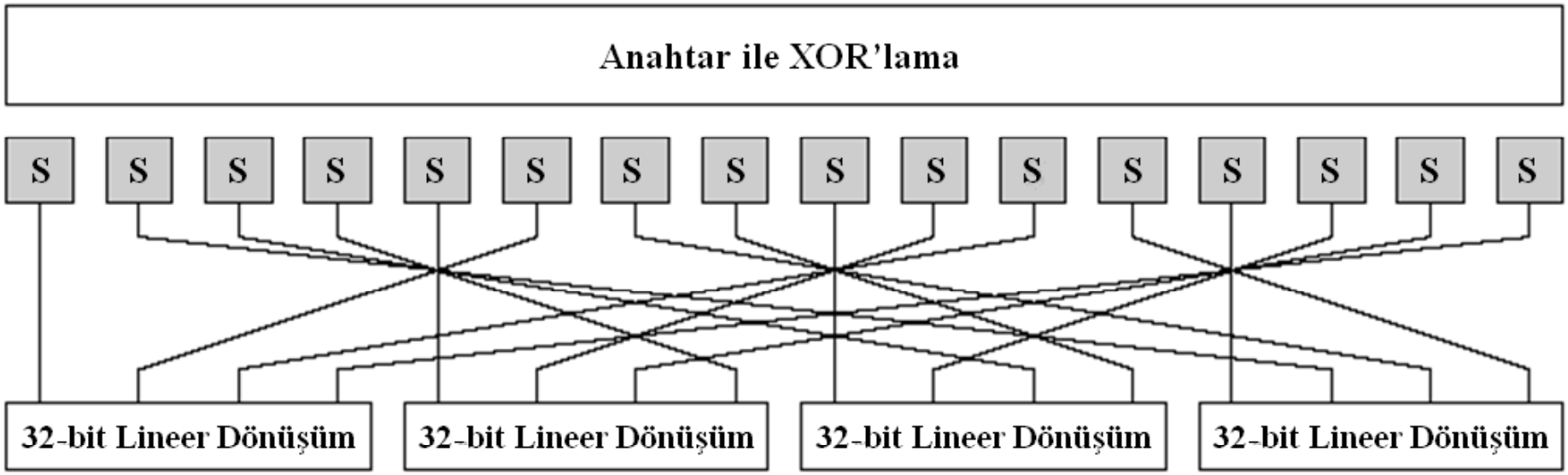
- 1990'lı yıllara gelindiğinde DES(Data Encryption Standart) güvenli bir şifreleme algoritması olarak görülmekteydi.
- 1991 yılında Biham ve Shamir tarafından yapılan diferansiyel saldırı ile DES sorgulanmaya başlandı.
- 1993 yılında Mitsuri Matsui doğrusal Kriptanaliz yöntemini keşfetti ve DES'in kırılabileceğini gösterdi.
- 2001 yılında Rijndael şifreleme algoritması AES (Advanced Encryption Standard- Gelişmiş Şifreleme Standardı) adıyla yeni şifreleme standardı olarak kabul gördü.
- Günümüzde AES hala bütün dünyada yaygın olarak kullanılan güvenli bir şifreleme algoritmasıdır.

Örnek bir Blok Şifre: AES(Advanced Encryption Standart)

- 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 10 döngü
  - 192 bit anahtar 12 döngü
  - 256 bit anahtar 14 döngü

Örnek bir Blok Şifre: AES(Advanced Encryption Standart)

- Her döngü dört adım içerir:
  - SubBytes (Byte Yerdeğiştirme),
  - ShiftRows (Satırları Öteleme),
  - MixColumns (Sütünları Karıştırma),
  - AddRoundKey (Döngü Anahtarı Ekleme).



Örnek bir Blok Şifre: AES(Advanced Encryption Standart)

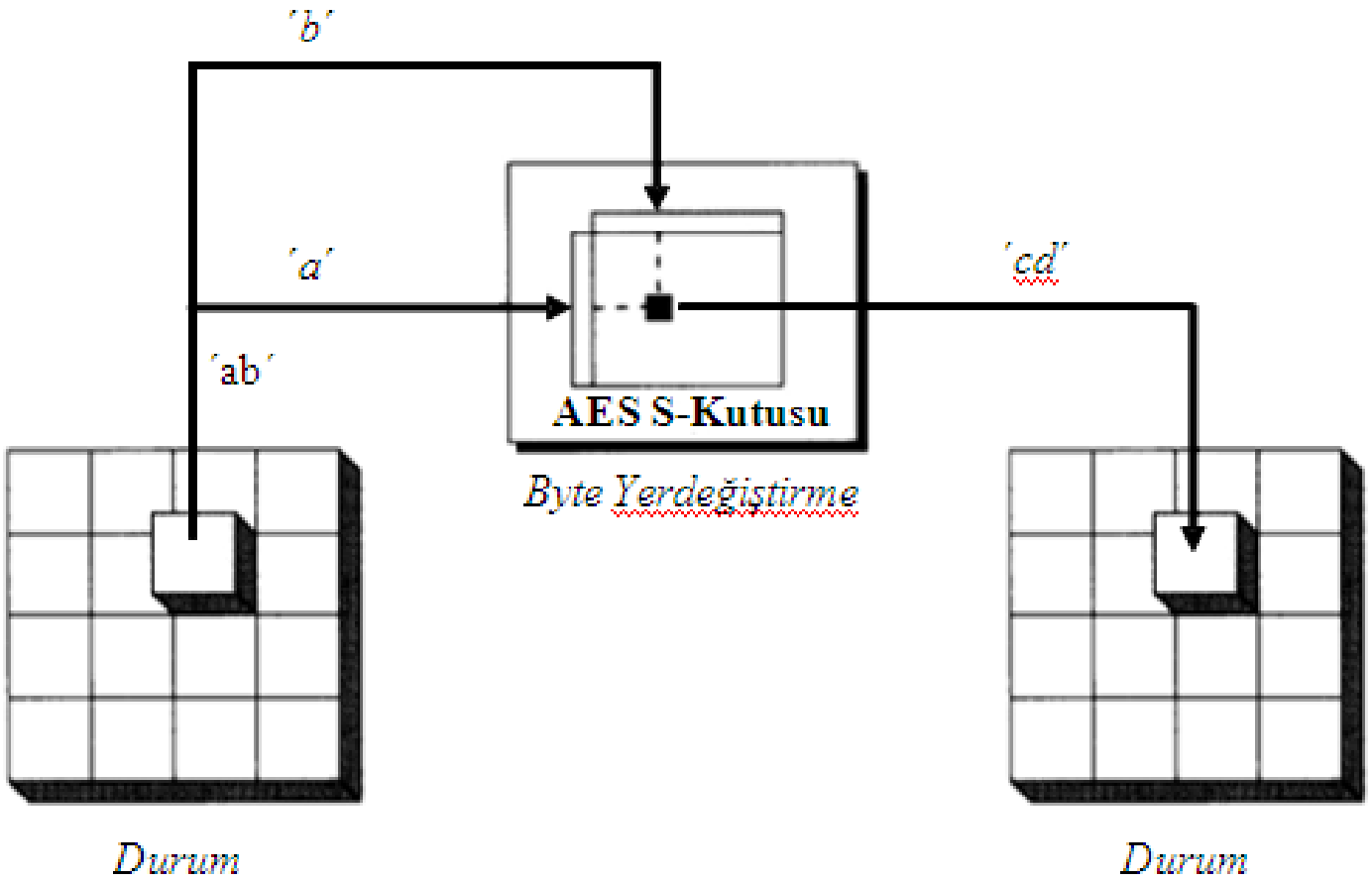
- Her döngüde tersi alınabilir dönüşümler kullanır,
- Son döngü hariç her döngüde SubBytes, ShiftRows, MixColumns ve AddRoundKey dönüşümleri kullanır. Sadece son döngüde MixColumns dönüşümü kullanılmaz,
- Anahtar planlama evresinde gizli anahtar kullanılarak döngü sayısı kadar farklı anahtar üretilir.
- Deşifreleme kısmında ters dönüşümler kullanılır: InvSubByte, InvShiftRows, InvMixColumns ve AddRounKey (tersi kendisidir- XOR işlemi).

SubBytes (Byte Yerdeğiştirme) Dönüşümü

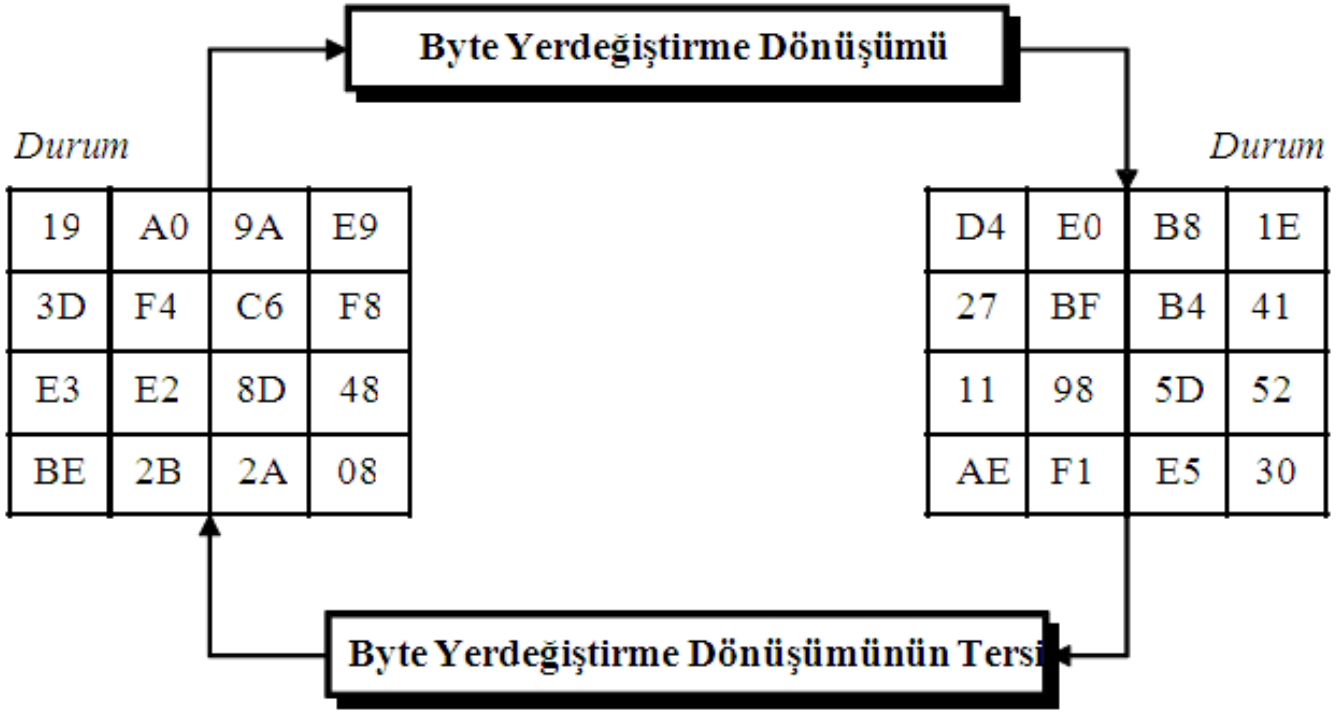
- AES şifresi her byte (8-bit) değere karşılık farklı bir byte değerine dönüşümü yapan ve şifreye doğrusal olmama özelliğini katan bir S-kutusu kullanır.

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

SubBytes (Byte Yerdeğiştirme) Dönüşümü

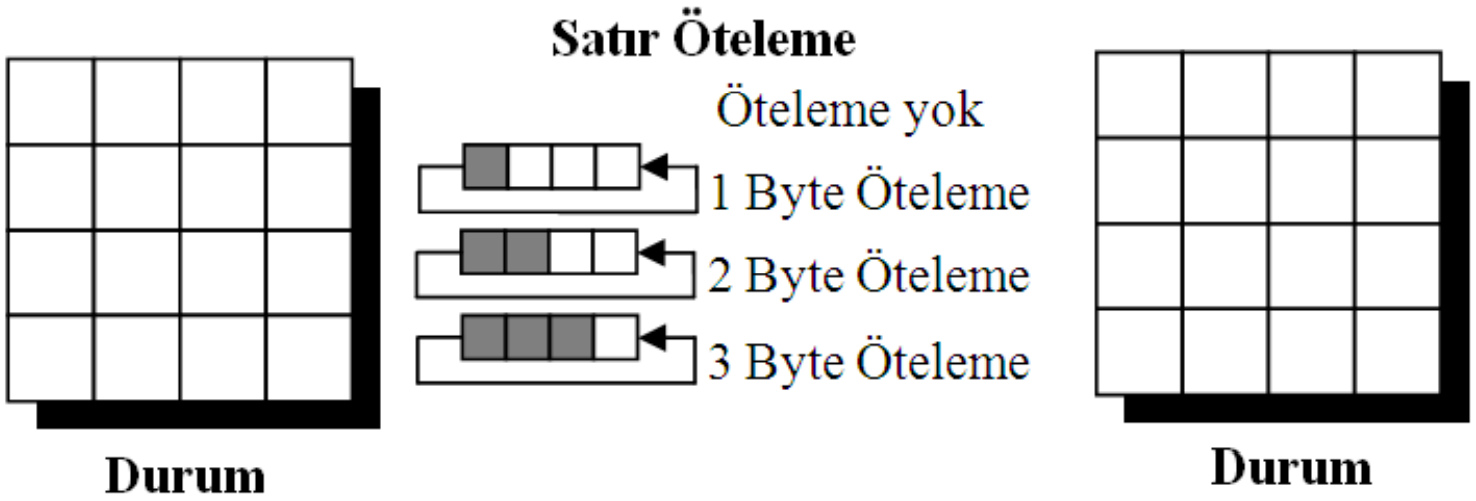


Örnek. ´19´,´3D´,´E3´,´BE´,´A0´,´F4´,´E2´,´2B´,´9A´,´C6´,´8D´,´2A´,´E9´,´F8´,´48´,´08´ 128 bitlik değerinin SubByte ve InvSubByte işlemleri aşağıdaki gibi gösterilebilir.

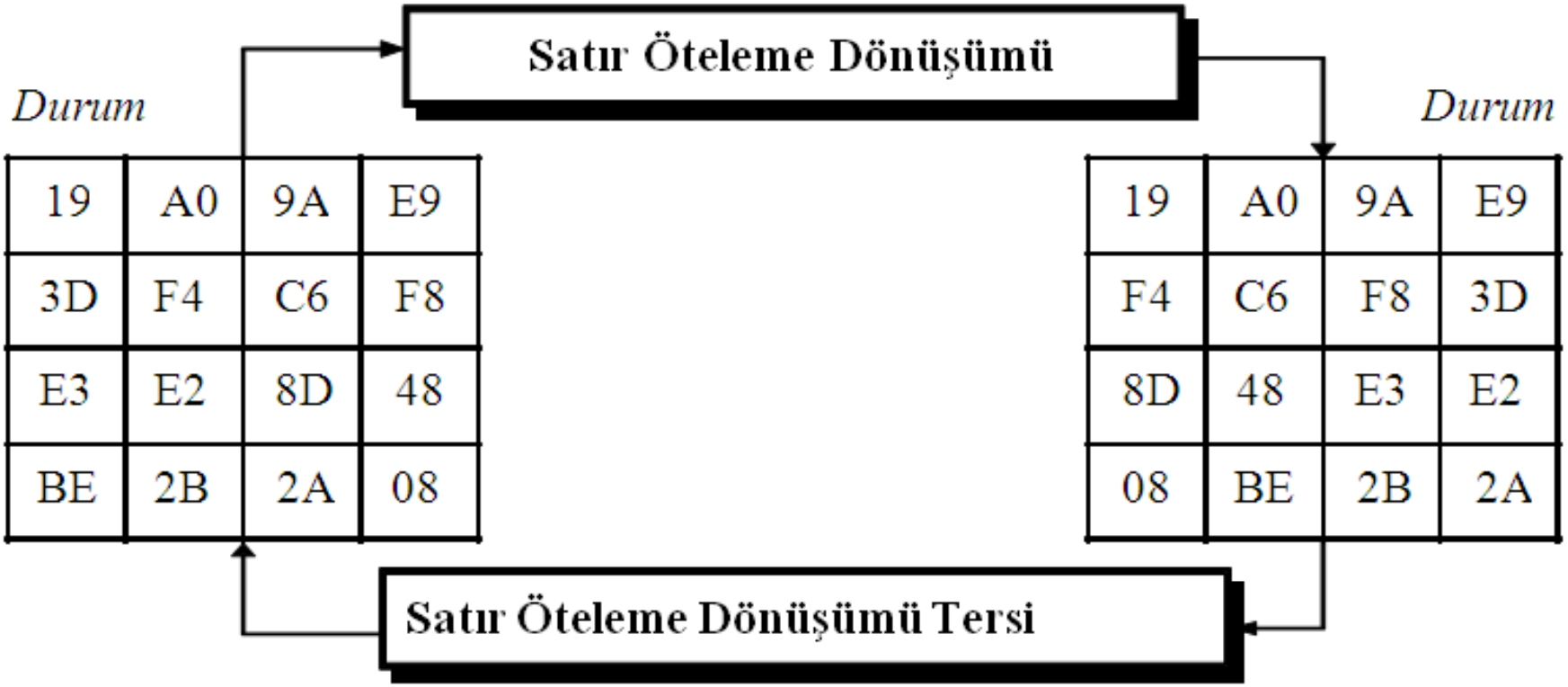


ShiftRows (Satırları Öteleme) Dönüşümü

- AES şifresi 4×4 boyutunda bir durum matrisi şeklinde değerlendirilirse satırları öteleme dönüşümü byte değerlerinin sola öteleme işlemidir.
- İlk satırda sola öteleme yapılmaz iken ikinci, üçüncü ve dördüncü satırlar sırasıyla 1 defa, 2 defa ve 3 defa sola ötelenir.



ShiftRows (Satırları Öteleme) Dönüşümü



MixColumns (Sütunları Karıştırma) Dönüşümü

- AES şifrenin içyapısında 32-bitten 32 bite dönüşüm yapan bir doğrusal dönüşüm içerir ve bu dönüşüm MixColumns (sütunları karıştırma) olarak isimlendirilir.
- Bu dönüşüm doğrusal ve diferansiyel kriptanalizi zorlaştırıcı etki yapma amacındadır ve sonlu cisimde çarpma tabanlıdır.

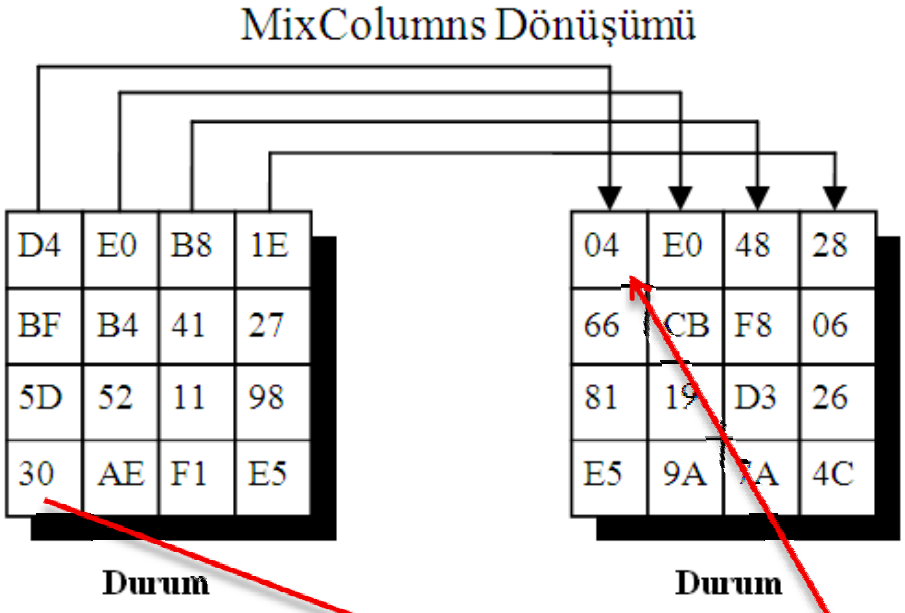
$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Şifreleme

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 0E_h & 0B_h & 0D_h & 09_h \\ 09_h & 0E_h & 0B_h & 0D_h \\ 0D_h & 09_h & 0E_h & 0B_h \\ 0B_h & 0D_h & 09_h & 0E_h \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Deşifreleme

Örnek. ´D4´,´BF´,´5D´,´30´,´E0´,´B4´,´52´,´AE´,´B8´,´41´,´11´,´F1´,´1E´,´27´,´98´,´E5´ 128 bit değeri şifreleme yapılırken MixColumns aşamasında aşağıdaki gibi işleme sokulur.



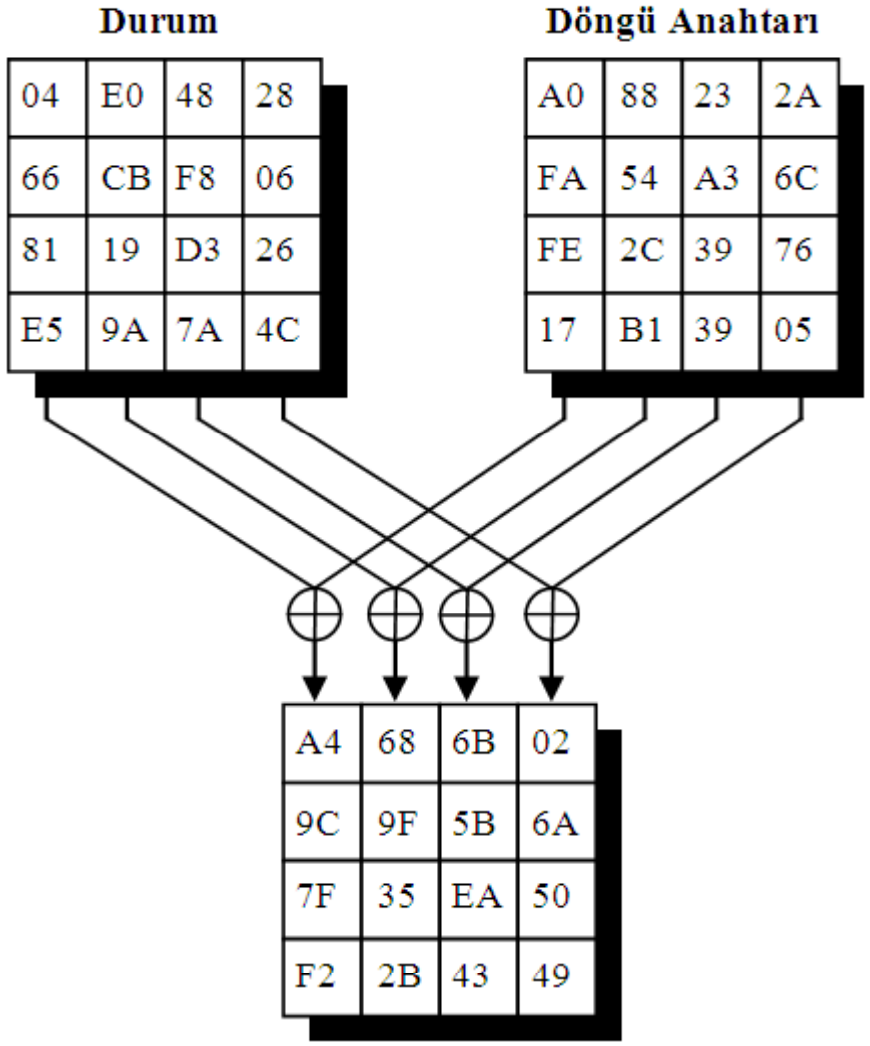
$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \begin{bmatrix} D4_h \\ BF_h \\ 5D_h \\ 30_h \end{bmatrix} = \begin{bmatrix} 04_h \\ 66_h \\ 81_h \\ E5_h \end{bmatrix}$$

AddRoundKey (Döngü Anahtarı Ekleme)

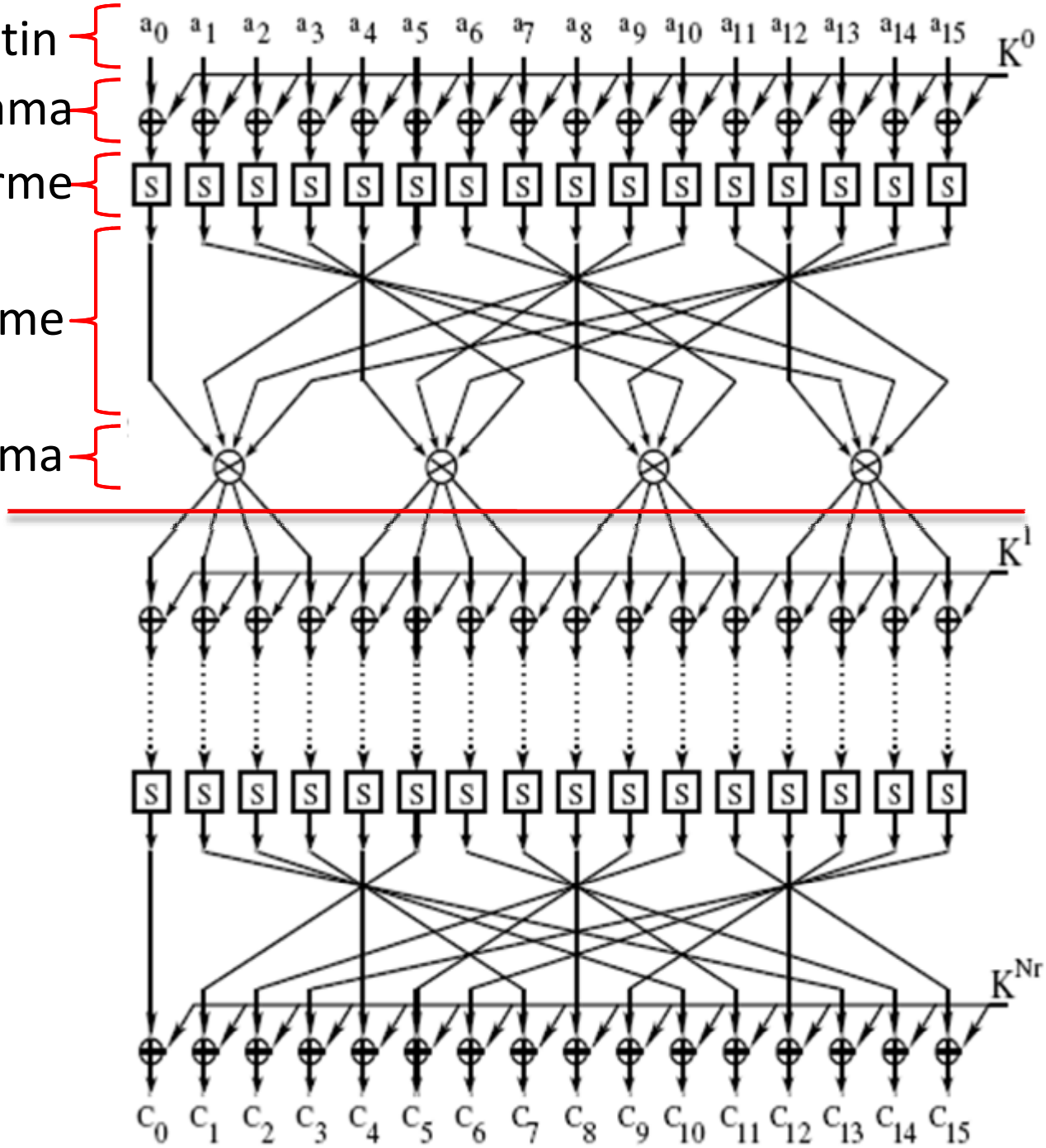
- Anahtar planlama aşamasında gizli anahtar kullanılarak her döngü için farklı bir anahtar üretilir.
- AddRoundKey aşamasında döngü anahtarı ile MixColumns dönüşümünden çıkan durum matrisi XOR işlemine tabi tutulur.
- Bu işleme beyazlatma (whitening) adı da verilir.
- Bu işlem şifrede güvenliğin artırılması amacıyla uygulanır.

AddRoundKey (Döngü Anahtarı Ekleme)

- ´04´,´66´,´81´,´E5´,´E0´,´CB´,´19´,´9A´,´48´,´F8´,´D3´,´7A´,´28´,´06´,´26´,´4C´ 128 bit değeri şifreleme yapılırken MixColumns dönüşümünün çıkışı olsun ve anahtar planlama evresinden ´A0´,´FA´,´FE´,´17´,´88´,´54´,´2C´,´B1´,´23´,´A3´,´39´,´39´,´2A´,´6C´,´76´,´05´ 128 bit değeri ilgili döngü için oluşturulmuş olsun. Bu durumda AddRoundKey işlemi aşağıdaki gibi özetlenebilir.



- Açık metin
- Anahtar XOR lama
- Byte Değiştirme
- Satır Öteleme
- Sütun Karıştırma
- Döngü 1



Doğrusal Dönüşümler

- Doğrusal dönüşümler bir blok şifreye yayılım eklemek için kullanılan elemanlardır.
- Blok şifre mimarilerinin (Feistel ve SPN) her ikisinde de kullanılabilirler.
- Doğrusal dönüşümler sabit uzunluktaki bir giriş bloğunu doğrusal olarak karıştırarak aynı uzunlukta bir çıkış bloğu elde etmeyi sağlar .
- Doğrusal dönüşümlerin sağladığı yayılımın ölçülmesi için var olan teknikler aşağıdaki gibi sıralanabilir:
  - Çığ Etkisi (Avalanche ciriterion)
  - Katı çığ etkisi (Strict avalance criterion)
  - Bütünlük (Completeness)
  - Dallanma sayısı (Branch number)
  - Sabit noktaların sayısı (Fixed points)

Doğrusal Dönüşümler

- Çığ ve katı çığ etkisi, tek bit değişimlerin çıkıştaki bitlerdeki değişimleri ölçer.
- Bütünlük kriteri çıkış bitlerinin giriş bitleri üzerindeki bağımlılığını ölçer.
- Dallanma sayısı bir blok şifrede iki ardışık döngüde aktif S-kutularının minimum sayısını temsil eder. Bu sayı, bir blok şifreye karşı uygulanacak doğrusal ve diferansiyel saldırıların başarımını ölçmek için kullanılır.
- Son olarak sabit noktaların sayısı kriteri bir doğrusal dönüşümün çıkış bloğunu üretirken giriş bloğunun değerini ne kadar etkin bir şekilde değiştirdiği ile ilişkilidir.

Doğrusal Dönüşümler için Matematiksel Altyapı

Yayılım elemanları doğrusal dönüşümlerdir ve matrisler ile temsil edildiklerinden bir doğrusal dönüşüm $A:(\{0,1\}^m)^n \rightarrow (\{0,1\}^m)^n$ ifadesindeki aşağıdaki gibi tanımlanabilir.

$$A(x) = A \,.\, x^T = \begin{pmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{pmatrix} . \begin{pmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{pmatrix}$$

Doğrusal Dönüşümler için Matematiksel Altyapı

$n \times n$ bir matris A'nın dallanma sayısı ifade aşağıdaki gibi tanımlanabilir.

$$\beta(A) = \min\{wt(x) + wt(A.x^T) \mid x \in (\{0,1\}^m)^n, x \neq 0\}$$

Bir kod kelimesinin Hamming ağırlığı $wt(c)$ olarak temsil edilebilir ve c kod kelimesinin 0 olmayan elamanlarının sayısı olarak tanımlanır. Buna ek olarak $(GF(2^m))^n$ vektör uzayından n boyutlu iki vektör arasındaki Hamming uzaklığı da vektörlerin farklılaştığı pozisyon sayısı olarak tanımlanır.

Doğrusal Dönüşümler için Matematiksel Altyapı

Bir $GF(2^m)$ üzerine bir $[n,k,d]$ kod, vektör uzayı $(GF(2^m))^n$'in k boyutlu bir alt uzayıdır ve n elemanlı iki vektör arasındaki Hamming uzaklığı minimum d dir. Bu özellik ile d en büyük değerdir. Doğrusal bir $[n,k,d]$ kod C için bir G üreteç matris satırları C için bir taban oluşturan $k \times n$ boyutunda bir matristir. Doğrusal $[n,k,d]$ kodlar Singleton sınırı olan $d \leq n-k+1$ eşitsizliğini sağlar.

Eğer bir $[n,k,d]$ hata düzeltme kodu üreteç matris $G = [I_{k\times k} \mid A]$ ile birlikte, $I_{k\times k}$ $k \times k$ birim matris ve A bir $k \times (n-k)$ matris olmak üzere, A singular (tekil) değilse (A'nın tüm alt kare matrislerinin determinantı 0'dan farklı ise) o zaman A matrisi MDS dir.

Doğrusal Dönüşümler için Matematiksel Altyapı

- Literatürde MDS matris tasarımları için
  - Dairesel (circulant) matrislerin kullanılması,
  - Hadamard matrislerin kullanılması

$A = circ(a_1, a_2, \ldots, a_n)$ notasyonu A matrisinin dairesel ve her satırının sağa 1 pozisyon hareket ettirilerek elde edildiğini ifade eder. Dolayısıyla $n \times n$ boyutlu A matrisi aşağıdaki gibi verilebilir.

$$A = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ a_n & a_1 & \ldots & a_{n-1} \\ . & . & \ldots & . \\ a_2 & a_3 & \ldots & a_1 \end{bmatrix}_{n \times n}$$

Doğrusal Dönüşümler için Matematiksel Altyapı

$A = Had\,(a_1, a_2, \ldots, a_n)$ notasyonu A matrisinin bir Hadamard matris olduğunu ifade etmektedir. 4×4 boyutlu A matrisi aşağıdaki gibi verilebilir.

$$A = Had(a_1, a_2, a_3, a_4) = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_2 & a_1 & a_4 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_4 & a_3 & a_2 & a_1 \end{bmatrix}$$

Doğrusal Dönüşümler için Matematiksel Altyapı

A bir doğrusal dönüşüm ve x bu doğrusal dönüşüme giriş bloğu olmak üzere $A(x)=x$ ise x sabit noktadır. Bir başka deyişle A doğrusal dönüşümü giriş bitlerini aynı çıkış bitlerine haritalıyor ise bir sabit nokta oluşmuş olur.

Bir doğrusal dönüşüm için sabit nokta sayısı (FPN), I birim matris olmak üzere aşağıdaki şekilde bulunabilir [27].

$$FPN = 2^{b(rank(A)-rank(A-I))}$$

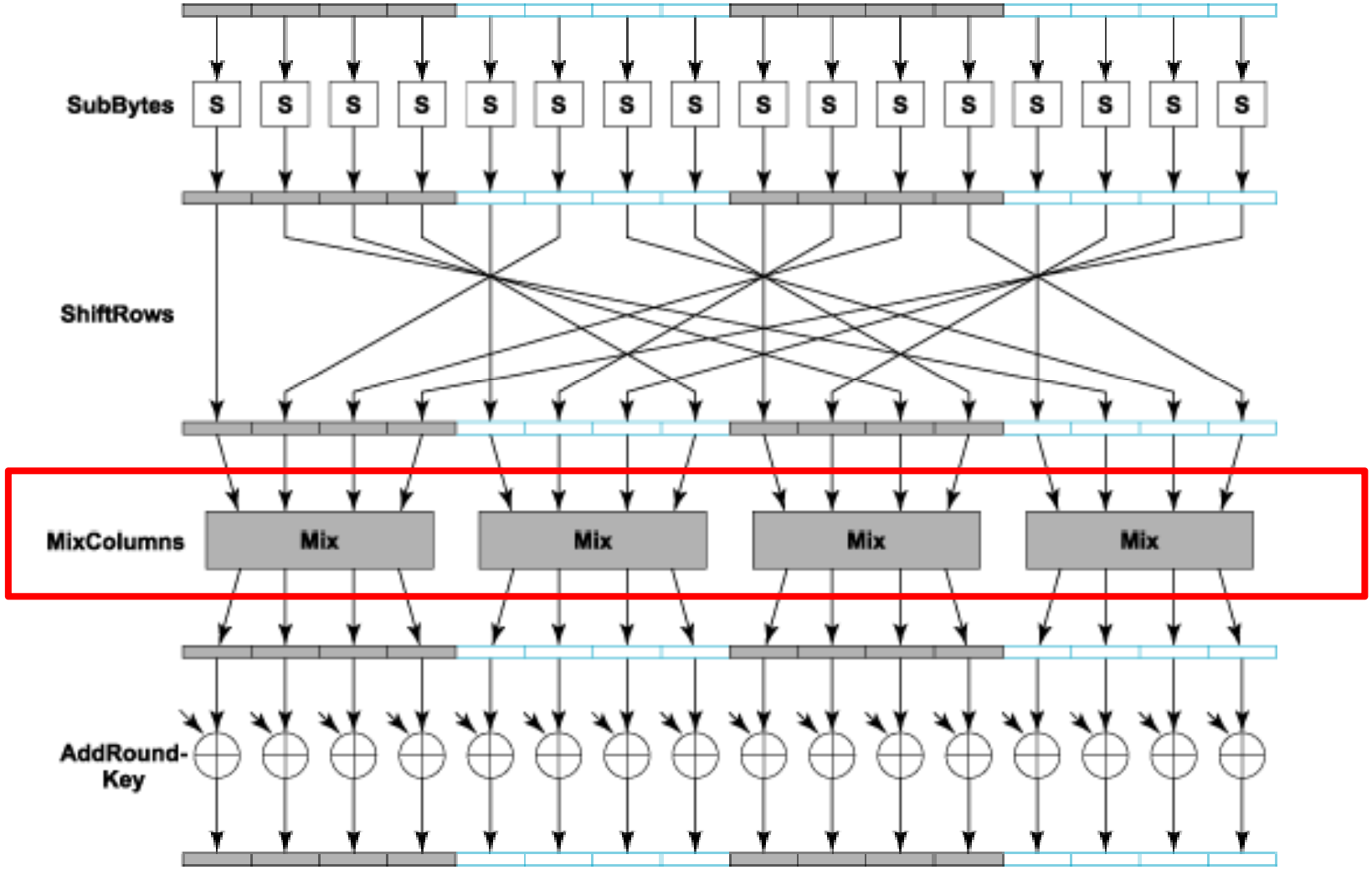
- Çalışmanın bu kısmında AES, ARIA, Khazad ve Camellia blok şifreleme algoritmalarında kullanılan doğrusal dönüşümler, dallanma sayısı ve sabit nokta sayısı kriterlerine göre incelenecektir.

AES Şifresinde Kullanılan Doğrusal Dönüşüm

AES şifresi 32-bitten 32-bite dönüşüm yapan bir doğrusal dönüşüm içerir. Bu dönüşüm doğrusal ve diferansiyel kriptanalizi zorlaştırıcı etki yapma amacındadır ve sonlu cisimde çarpma tabanlıdır. $GF(2^8)$ de elemanlar içeren AES matrisi çarpma işlemleri sonucunda indirgeme işlemleri için $x^8 + x^4 + x^3 + x + 1$ polinomunu kullanmaktadır. Bir MDS matris tabanlı olan bu doğrusal dönüşüm, şifreleme işlemi için aşağıdaki matrisi kullanmaktadır.

$$A_{AES} = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \qquad A_{AES}^{-1} = \begin{bmatrix} 0E_h & 0B_h & 0D_h & 09_h \\ 09_h & 0E_h & 0B_h & 0D_h \\ 0D_h & 09_h & 0E_h & 0B_h \\ 0B_h & 0D_h & 09_h & 0E_h \end{bmatrix}$$

AES Şifresinde Kullanılan Doğrusal Dönüşüm



AES Şifresinde Kullanılan Doğrusal Dönüşüm

$$A_{AES} = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \qquad A_{AES}^{-1} = \begin{bmatrix} 0E_h & 0B_h & 0D_h & 09_h \\ 09_h & 0E_h & 0B_h & 0D_h \\ 0D_h & 09_h & 0E_h & 0B_h \\ 0B_h & 0D_h & 09_h & 0E_h \end{bmatrix}$$

AES'in dairesel formda tasarlanan MDS matrisinin dallanma sayısı 5'tir. Dolayısı ile giriş değerlerinden 1 byte'ın değişmesi sonucunda minimum 4 byte bu durumdan etkilenecektir. Kullanılan doğrusal dönüşüm matrisi involutif değildir. Dolayısı ile deşifreleme işlemi için farkı bir matris kullanılmaktadır. Sütunları karıştırma dönüşümünün $(A-I)$ matrisinin rank değeri 3 olduğundan $2^{b(rank(A)-rank(A-I)} = 2^{8(4-3)} = 2^8$ adet sabit nokta içerir.

Khazad Şifresinde Kullanılan Doğrusal Dönüşüm

- KHAZAD şifresi 128-bit anahtarla çalışan 64-bit bir blok şifredir.
- Doğrusal yayılım katmanı birkaç döngüden sonra tüm çıkış bitlerinin tüm giriş bitlerine bağımlı olmasını sağlarken doğrusal olmayan katman ise karmaşıklığı ve doğrusal olmamayı sağlar.
- KHAZAD şifresinin doğrusal dönüşüm katmanı GF(2^8) de MDS olarak Hadamard formunda tasarlanmıştır.

$$A=\begin{bmatrix} 01_h & 03_h & 04_h & 05_h & 06_h & 08_h & 0B_h & 07_h \\ 03_h & 01_h & 05_h & 04_h & 08_h & 06_h & 07_h & 0B_h \\ 04_h & 05_h & 01_h & 03_h & 0B_h & 07_h & 06_h & 08_h \\ 05_h & 04_h & 03_h & 01_h & 07_h & 0B_h & 08_h & 06_h \\ 06_h & 08_h & 0B_h & 07_h & 01_h & 03_h & 04_h & 05_h \\ 08_h & 06_h & 07_h & 0B_h & 03_h & 01_h & 05_h & 04_h \\ 0B_h & 07_h & 06_h & 08_h & 04_h & 05_h & 01_h & 03_h \\ 07_h & 0B_h & 08_h & 06_h & 05_h & 04_h & 03_h & 01_h \end{bmatrix}$$

KHAZAD için tasarlanan bu doğrusal dönüşüm matrisinin dallanma sayısı 9 olmakla beraber involutif olarak tasarlanmıştır. Bu sebeple şifreleme ve deşifreleme işlemlerinde aynı matris kullanılmaktadır. Böylelikle bu işlemler arasındaki fark kaldırılmış olur. Bu matrisin, $(A-I)$ matrisinin rank değeri 4 olduğundan FPN değeri aşağıdaki gibi hesaplanabilir.

$$2^{b(rank(A)-rank(A-I)} = 2^{8(8-4)} = 2^{32}$$

Camellia Şifresinde Kullanılan Doğrusal Dönüşüm

- Camellia,128-bit veri bloklarını 128, 192 veya 256-bit anahtar seçenekleri ile şifreleyen bir şifreleme algoritmasıdır.
- 2000 yılında NTT(Nippon Telegraph And Telephone Corporation) ve Mitsubishi Electric Corporation tarafından ortak geliştirilmiştir.
- Camellia şifresinde kullanılan doğrusal dönüşüm matrisi MDBL (Maximal Distance Binary Linear) kod olarak tasarlanmıştır.

Camellia Şifresinde Kullanılan Doğrusal Dönüşüm

MDBL (Maximal Distance Binary Linear) kod olarak tasarlanmıştır. Dallanma sayısı 5 olan dönüşüm aşağıda gösterilmiştir. Camellia doğrusal dönüşümünün $(A-I)$ matrisinin rank değeri 7 olduğundan $2^{8(8-7)}=2^8$ adet sabit nokta içerir.

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

ARIA Şifresinde Kullanılan Doğrusal Dönüşüm

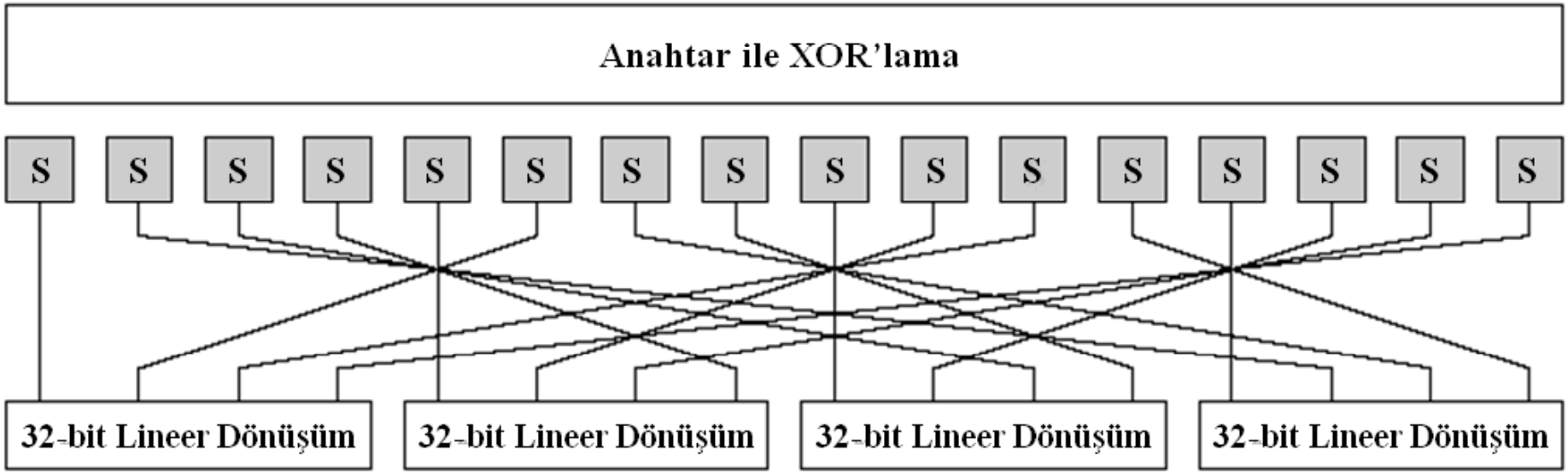
- ARIA blok şifresi Güney Koreli araştırmacılar tarafından 2004'de tasarlanmıştır ve Kore Teknoloji Ajansı tarafından standart şifreleme tekniği olarak seçilmiştir.
- ARIA, verileri 128 bit bloklarla 128, 192 ve 256-bit anahtar seçenekleri ile şifreleyen bir şifreleme algoritmasıdır.
- Döngü sayıları anahtar uzunluğuna göre 10, 12 ya da 14 tür.
- ARIA şifresi yayılım katmanı olarak 16×16 boyutunda giriş değerlerini byte değerler olarak alan involutif ve MDBL kod olarak tasarlanmış bir ikili matris kullanır.

ARIA Şifresinde Kullanılan Doğrusal Dönüşüm

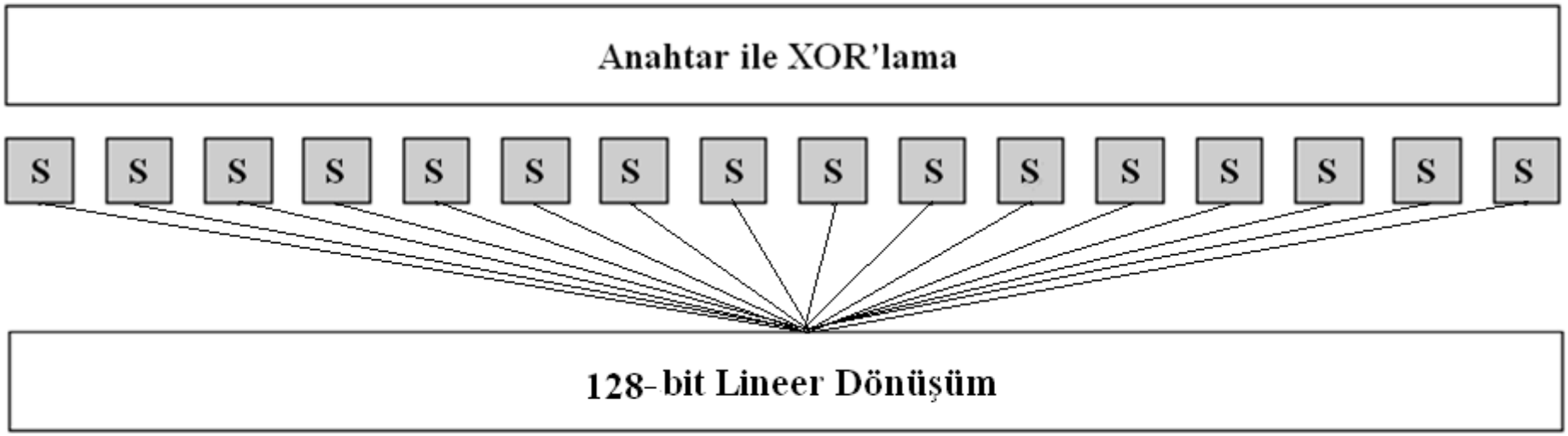
$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{pmatrix}$$

- MDBL kod
- Dallanma sayısı 8
- 2^{72} sabit nokta

AES


Anahtar ile XOR'lama
S S S S S S S S S S S S S S S S
32-bit Lineer Dönüşüm
32-bit Lineer Dönüşüm
32-bit Lineer Dönüşüm
32-bit Lineer Dönüşüm

ARIA


Anahtar ile XOR'lama
S S S S S S S S S S S S S S S S
128-bit Lineer Dönüşüm

Sonuçlar

- Literatürde bulunan önemli blok şifrelerin kullandığı doğrusal dönüşümler incelenmiştir.
- Kullanılan doğrusal dönüşümler genellikle MDS ve MDBL kod tabanlıdır.
- Camellia ve ARIA şifresinde optimal dallanma sayısına sahip ikili matrisler kullanılmıştır.
- İkili matris kullanılması bu dönüşümlerin uygulamada sadece XOR işlemi tabanlı olarak gerçekleştirilmesini sağlamaktadır.
- İncelenen doğrusal dönüşümlerin sabit nokta sayılarının oldukça yüksek olduğu gözlenmiştir.

	ÖZELLİK	BN	FPN
AES	GF(2^8) üzerine 4×4 boyutunda MDS matris	5	2^8
KHAZAD	GF(2^8) üzerine 8×8 boyutunda involutif MDS matris	9	2^{32}
CAMELLIA	GF(2^8) üzerine 8×8 boyutunda MDBL matris	5	2^8
ARIA	GF(2^8) üzerine 16×16 boyutunda involutif MDBL matris	8	2^{72}

Dinlediğiniz İçin Teşekkürler

Bora Aslan