



T.C.  
ULUDAĞ ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ

**AKILLI KARTLARDA SALDIRILARA KARŞI TEDBİR YÖNTEMLERİNİN  
ARAŞTIRILMASI**

**Zümrüt MÜFTÜOĞLU**

Prof. Dr. Eldar MUSA  
(Danışman)

YÜKSEK LİSANS TEZİ  
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

BURSA – 2011

**Her Hakkı Saklıdır**

## TEZ ONAYI

Zümrüt MÜFTÜOĞLU tarafından hazırlanan “**Akıllı Kartlarda Saldırlara Karşı Tedbir Yöntemlerinin Araştırılması**” adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Elektronik Mühendisliği Anabilim Dalı’nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

**Danışman** : Prof. Dr. Eldar MUSA

<b>Başkan :</b>	İmza
.. Ü. ....Fakültesi, .....Anabilim Dalı	
<b>Üye :</b>	İmza
.. Ü. ....Fakültesi, .....Anabilim Dalı	
<b>Üye :</b>	İmza
.. Ü. ....Fakültesi, .....Anabilim Dalı	
<b>Üye :</b>	İmza
.. Ü. ....Fakültesi, .....Anabilim Dalı	
<b>Üye :</b>	İmza
.. Ü. ....Fakültesi, .....Anabilim Dalı	

**Yukarıdaki sonucu onaylarım**

**Prof. Dr. Kadri ARSLAN**  
**Enstitü Müdürü**  
.././....

**U.Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmada;**

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

**beyan ederim.**

...../...../.....

**İmza**

**Adı Soyadı**

## ÖZET

Yüksek Lisans Tezi

### AKILLI KARTLARDA SALDIRILARA KARŞI TEDBİR YÖNTEMLERİNİN ARAŞTIRILMASI

**Zümrüt MÜFTÜOĞLU**

Uludağ Üniversitesi  
Fen Bilimleri Enstitüsü  
Elektronik Mühendisliği Anabilim Dalı

**Danışman:** Prof. Dr. Eldar MUSA

Özellikle son yıllarda kullanım alanı giderek artan akıllı kartlar için saklanılan verilerin güvenliği önem kazanmaktadır. Akıllı kartlarda veri güvenliği DES,AES,3DES gibi şifreleme algoritmaları ile sağlanmaktadır. Ancak nitelikli algoritmaların geliştirilmesi akıllı kartlara karşı saldırılara engel olmak için yeterli değildir. Özel bir donanımla karta müdahale edilmesi, yazılımsal bir takım müdahalelerin yapılmasının yanı sıra, veri güvenliğini sağlayan şifreleme algoritmaları yürütülürken istemsiz çıkışlar sızdırmaktadır. Bu çıkışlar (zaman,elektromanyetik yayılım,güç tüketimi,gürültü,ses..gibi) bir şekilde gizli bilgi ile ilişkili olduğunda, yan-kanal bilgisi olarak adlandırılmaktadır.

Bu tez çalışmasında, akıllı kartlara karşı saldırı ve karşı tedbir yöntemleri araştırılmıştır. RFID uygulama kiti üzerinde bir uygulama gerçekleştirilmiştir. Bu uygulamada el yapımı antenler yardımıyla, kartın okutulduğu sırada sistemin elektromanyetik yayılım ve güç tüketimi davranışlarının gözlemlenmesi amaçlanmıştır. Gözlemlerin yorumlanması için istatistiksel tekniklerden faydalanılmıştır. Yapılan ölçümler neticesinde, kartın okuyucuya gönderilen komutlara karşılık osilokoptaki işaretle oluşan değişiklikler gözlemlenmiştir.

**Anahtar kelimeler:** Akıllı kartlar, akıllı kartların güvenliği, yan kanal analizi, şifreleme algoritmaları

**2011,x+59 sayfa**



## **ABSTRACT**

MSc. Thesis

### **SEARCHING THE COUNTERMEASURE METHODS OF ATTACKS AGAINST SMARTCARDS**

**Zümrüt MÜFTÜOĞLU**

Uludag University  
Graduate School of Natural and Applied Sciences  
Department of Electronics Engineering

**Danışman:** Prof. Dr. Eldar MUSA

For the smartcards , whose using field increase by time especially in recent years, data security becomes importance. The data security of smartcards are ensured by cryptographic algorithms like DES, AES, 3DES. But sometimes well-qualified algorithms are not enough to prevent attacks on smartcards. In addition to tampering cryptographic device with a special physical device or software manipulates, the cryptographic device leak some unintentional outputs while they are runned. When these outputs (as electromagnetic radiation, power consumption, acustic,timing or noise) are somehow related with secret data, they are called side channel information.They threaten the security of data as well.

In this work, information about attacks on smartcards and countermeasures of them are investigated with details.An implementation was performed on a RFID evaluation kit. It is aimed to observe power consumption and electromagnetic radiation behaviours of system through this application. For this aim some self made antennas and statiscal methods were used to interpret the results of observation. As result of experiments, observable changes were seen when we sent commands to reader.

**Key words :** Smartcards, security of smartcards,side channel analysis, cryptographic algorithms

**2011,x+59 pages**

## **TEŞEKKÜR**

Tez çalışmalarımnda emeđi geen danıřman hocam Sayın Prof.Dr.Eldar MUSA' ya deđerli katkılarından dolayı teřekkür ederim.

Tezin geliřimindeki yardımlarından dolayı Sayın Yrd. Do.Dr. Halil YEŐILİMEN' e, Elektronik Yüksek Mühendisi Sayın Bayazıt DİRİM'e, TARGE Elektronik AR-GE Mühendisi Sayın Vahit GEMİCİ' ye; maddi ve manevi desteđinden dolayı Burulař Genel Müdürü Sayın Dr. Ali KAYA' ya, desteđiyle beni motive eden Burulař Bilet Sistemleri Müdürü Sayın Nur KÖSE ve Sayın Dr. Sibel GÜLER YENİKAYA' ya teřekkürü bor bilirim.

Bugünlere gelmemin en büyük mimarı olan deđerli anne ve babama sonsuz teřekkürlerimi sunarım.

Zümrüt MÜFTÜOĐLU

06/04/2011

## İÇİNDEKİLER

	<b>Sayfa</b>
ÖZET.....	i
ABSTRACT.....	ii
ÖNSÖZ VE TEŞEKKÜR.....	iii
SİMGELER VE KISALTMALAR DİZİNİ.....	vi
ŞEKİLLER DİZİNİ.....	viii
1. GİRİŞ.....	1
2. KAYNAK ARAŞTIRMASI.....	2
2.1 Akıllı Kart Teknolojileri.....	2
2.2 Akıllı Kartların Sınıflandırılması.....	3
2.2.1 Temashlı akıllı kartlar.....	3
2.2.2 Temassız akıllı kartlar.....	4
2.3 Akıllı Kartlarda Veri Güvenliđi.....	5
2.3.1 Şifreleme(Kriptografi).....	5
2.3.2 Şifreleme algoritmalarının sınıflandırılması.....	6
2.3.2.1 Asimetrik şifreleme algoritmaları.....	7
RSA algoritması.....	7
2.3.2.2 Simetrik şifreleme algoritmaları.....	8
2.4 Blok Şifreleme Algoritmaları.....	11
2.4.1 DES algoritması.....	12
2.4.2 3DES algoritması.....	15
2.4.3 AES algoritması.....	15
2.4.3.1 AES tur dönüşümü.....	17
2.4.3.2 Bayt deđiştirme.....	17
2.4.3.3 Satırları kaydırma.....	19
2.4.3.4 Sütunları karıştırma.....	20
2.5 Akıllı Kartlara Karşı Saldırı Yöntemleri.....	21
2.5.1 Fiziksel saldırılar.....	21
2.5.2 Algoritmaya yönelik saldırılar.....	21
2.5.2.1 Temel saldırılar.....	21

2.5.2.2 Gelişmiş saldırılar .....	22
Doğrusal kriptanaliz .....	22
Farksal kriptanaliz .....	23
2.5.3 Yazılıma yönelik saldırılar .....	23
2.5.4 Yan-kanal analizi saldırıları .....	23
2.5.4.1 Aktif saldırılar .....	24
Hata indüklenme saldırısı .....	26
Ölçüm saldırıları .....	26
2.5.4.2 Pasif saldırılar.....	26
Zamanlama analizi saldırıları .....	26
Güç analizi saldırıları .....	28
Basit güç analizi saldırıları .....	30
Farksal güç analizi saldırıları.....	33
Elektromanyetik analizi saldırıları .....	38
2.6 Karşı Tedbir Yöntemleri .....	39
2.6.1 Maskelenmiş AES algoritması örneği.....	42
3 MATERYAL VE YÖNTEM .....	45
3.1 Materyal .....	45
3.1.1 Mifare temassız akıllı kartlar .....	45
3.2 Yöntem.....	47
3.2.1 Ortalamaların farkı testi yöntemi .....	48
3.2.2 T-Test yöntemi .....	49
3.2.3 Korelasyon yöntemi .....	49
3.3 Uygulama Düzenegi.....	49
4 BULGULAR VE SONUÇ .....	56
KAYNAKLAR .....	57
ÖZGEÇMİŞ .....	59

## SİMGELER VE KISALTMALAR DİZİNİ

<b>Simgeler</b>	<b>Açıklama</b>
$R$	En sağdaki register
$L$	En soldaki register
$K$	Döngü anahtarı
$F$	Döngü fonksiyonu
$n$	Blok genişliği
$d$	Döngü sayısını
$w$	Kelime genişliği
$N_k$	Anahtar uzunluğu
$N_b$	Blok uzunluğu
$N_r$	Döngü sayısı
$\Delta$	Farksal değer
$A$	Ortalama değer
$var$	Varyans
$D$	Seçme fonksiyonu
$c$	Korelasyon katsayısı

<b>Kısaltmalar</b>	<b>Açıklama</b>
AES	Advanced Encryption Standard
ALU	Arithmetic Logic Unit
CMOS	Complementary Metal Oxide Semiconductor
DEMA	Differential EM Analysis
DES	Data Encryption Standard
DOM	Distance of Mean
DPA	Differential Power Analysis
EEPROM	Electrically Erasable Programmable Read-Only Memory
EM	ElectroMagnetic
EXOR	Exclusive OR

FIPS	Federal Information Processing Standards
GF	Galois Field
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
SEMA	Simple EM Analysis
SPA	Simple Power Analysis
TDES	Triple Data Encryption Standart

## ŞEKİLLER DİZİNİ

	<b>Sayfa</b>
Şekil 2.1 Kontaklı akıllı kart mimarisi	3
Şekil 2. 2 Temaslı akıllı kart kontak noktaları	4
Şekil 2.3 Temassız akıllı kart	4
Şekil 2.4 Şifre biliminin sınıflandırılması	5
Şekil 2.5 Asimetrik şifreleme algoritması gösterimi	7
Şekil 2.6 RSA şifreleme ve şifre çözme işlemi gösterimi	9
Şekil 2.7 Simetrik algoritmada şifreleme ve şifre çözme işlemi	10
Şekil 2.8 DES şifreleme algoritmasının Feistel yapısı	13
Şekil 2.9 F fonksiyonu gösterimi	14
Şekil 2.10 3DES yapısı	15
Şekil 2.11 AES blok diyagramı	16
Şekil 2.12 AES algoritmasına ait anahtar uzunluğu-tur sayısı-blok boyutu ilişkisi	16
Şekil 2.13 4x4 durum matrisi	17
Şekil 2.14 Sekizli bayt değiştirme dönüşümü	18
Şekil 2.15 Onaltılık durum için S-kutusu çıkışları	19
2.16 Satırları kaydırma dönüşümü	19
2.17 Sütunları karıştırma dönüşümü	20
Şekil 2.18 Doğrusal kriptanaliz blok şeması	22
Şekil 2.19 Akıllı karttan sızan yan-kanal bilgileri	24
Şekil 2.20 Sıcak nitrik asit çipe zarar vermeden plastiğin eritilmesi sağlar	24
Şekil 2.21 Çıkarılan akıllı kart işlemcisi test paketine monte edilir	25

Şekil 2.22 Soldaki şekilde aynı odaklı mikroskoptan alınan CMOS AND görülüyor.Sağdaki şekilde ise aynı kapının metal tabaka çıkarıldıktan sonraki görünümü bulunuyor	25
Şekil 2.23 Akıllı kart güç tüketimi	28
Şekil 2.24 CMOS devresinde güç tüketimi	29
Şekil 2.25 CMOS kapısının durum değiştirmesi sırasında çektiği akım	29
Şekil 2.26 Güç tüketimi ölçüm devre düzeneği	30
Şekil 2.27 DES turlarını gösteren güç ölçümü	31
Şekil 2.28 Akıllı kartın güç tüketimi	33
Şekil 2.29 Farksal güç analizi	34
Şekil 2.30 CMOS evirici	38
Şekil 2.31 Gizleme ve maskeleye karşı tedbir yöntemlerinin genel gösterimi	40
Şekil 2.32 AES maskeleye işlemi gösterimi	44
Şekil 3.1 Mifare temassız akıllı kart	45
Şekil 3.2 Üretici bloğuna ait gösterim	46
Şekil 3.3 Mifare 1K(1024 bayt) hafıza haritası gösterimi	47
Şekil 3.4 Anten 1 ( n=400, r=3mm)	50
Şekil 3.5 Anten 2 ( n=800, r=3mm)	50
Şekil 3.6 Anten 3 (n=50, r = 35mm)	51
Şekil 3.7 Anten 4 (Ferrite nuve, n=1000)	51
Şekil 3.8 Devre düzeneğinden bir görünüm	52
Şekil 3.9 Uygulama düzeneğinden bir görünüm	52
Şekil 3.10 Taşıyıcı frekansı 13,56MHz olan sinüs sinyali	53
Şekil 3.11 Kart okutulduğu esnada osiloskopta gözlenen işaret	53
Şekil 3.12 Değiştirilmiş Miller kodu gösterimi	54
Şekil 3.13 Doğru anahtar girilmesi durumunda elde edilen işaret	54





## 1. GİRİŞ

Akıllı kartların kullanımı gelişen teknoloji ile birlikte artarken, üst seviyede güvenlik ihtiyacı da doğurmaktadır. Özellikle elektronik cüzdan ve ön ödemeli sistemlerin uygulamalarında yaygın olarak kullanılan akıllı kartlar için zaman içerisinde saldırı teknikleri ve bunlara karşı tedbir yöntemleri geliştirilmiştir.

Kart sahiplerinin işlemlerini daha güvenilir bir şekilde gerçekleştirebilmesi için şifreleme algoritmaları geliştirilmiştir. Bu algoritmalar içerdikleri kriptografik anahtarlar sayesinde güvenliği sağlamaktadırlar. Şifreleme algoritmaları asimetrik ve simetrik algoritmalar olarak ikiye ayrılmaktadır. Simetrik algoritmalar şifreleme ve şifre çözme işlemleri için tek bir anahtar kullanırken, asimetrik algoritmalar bu iki işlem için iki farklı anahtar kullanmaktadırlar.

Ancak yapılan çalışmalar neticesinde, kullanılan şifreleme algoritması ne kadar güçlü olursa olsun, bir akıllı kartın algoritmayı yürüttüğü esnada yan-kanal bilgisi olarak adlandırılan istem dışı çıkışlar ürettiği saptanmıştır. Sızdırılan bu bilginin gizli anahtarla ilişkilendirilmesi gizli bilgiye erişilmesine neden olabilmektedir. Bu bilgi zaman, elektromanyetik yayılım, güç tüketimi veya ısı şeklinde olabilir. İlk olarak 1995 yılında Paul Kocher tarafından keşfedilen pasif yan-kanal analizi saldırıları üzerinde çalışmalar özellikle son dönemde yoğunluk kazanmıştır. Bu çalışmalarda, bir takım karşı tedbir yöntemleri geliştirilerek sızan bilginin gizli anahtarla olan ilişkisinin zayıflatılması amaçlanmaktadır.

## 2. KAYNAK ARAŞTIRMASI

### 2.1. Akıllı Kart Teknolojileri

Akıllı kartı ilk bulan kişiler, Fransa'dan Roland Moreno, Almanya'dan Jergen Dethloff ve Japonya'dan Arimura olarak gösterilmektedir. Akıllı kartın ilk patenti 1974 yılında Roland Moreno tarafından hafıza kartları olarak alınmıştır. İlk mikroişlemcili akıllı kart ise 1977 yılında Michel Ugon tarafından keşfedilmiştir. 1984 yılında ilk başarılı akıllı kart uygulaması, Fransa'da telefon ödemelerinde "Telekart" ismiyle kullanılarak hayata geçirilmiştir. Bankacılık sektöründe gerçekleşen ve en önemli akıllı kart uygulaması olan *elektronik cüzdan uygulaması*, 1990'ların ortasından itibaren Avrupa'da pilot olarak uygulanmaya başlanmıştır. Bu denemeler Almanya, Belçika, Hollanda, İsviçre, İsveç, İngiltere ve Danimarka'da gerçekleştirilmiştir. 1990' lı yıllarda Avrupa'da GSM telefonlarında SIM (Subscriber Identity Module-Abone Kimlik Modülü) kart kullanımının başlamasıyla, akıllı kart kullanımındaki en büyük çalışma gerçekleşmiştir. Dünyanın en büyük kredi üreticileri olan Mastercard, Visa ve Europay akıllı kartları kredi kartı olarak geliştirmek amacıyla 1993 yılında birlikte çalışma başlatmışlardır. Özellikle 2005 yılından itibaren EMV standardına geçilmesiyle akıllı kart kullanımı daha yaygın hale gelmiştir. Haberleşme alanında, cep telefonlarında kullanılan SIM kartlar birer akıllı karttır. Bunun dışında günümüzde akıllı kartların en yaygın kullanıldığı alanları özetlersek (Rankl ve ark. 2003);

*Personel otomasyonu:* Özellikle vardiya sisteminin bulunduğu fazla personele sahip şirketler için çok büyük kolaylık sağlamaktadır. Akıllı kart ile personel takibinde çalışanın imza atmak yerine okuyucuya kartını okutması yeterli olmaktadır. Böylelikle hem giriş kapılarındaki uzun kuyruklar sona ermekte, hem de personele ait verilerin daha güvenli bir şekilde depolanması mümkün olmaktadır.

*Kimlik (e-kimlik kartı, pasaport,..):* Kimlik kartlarında akıllı kart uygulamasına geçilmesiyle, kart sahiplerine erişim daha kolay ve güvenilir hale gelmiştir. Özellikle sağlık sektöründe kullanımı büyük kolaylık sağlamaktadır.

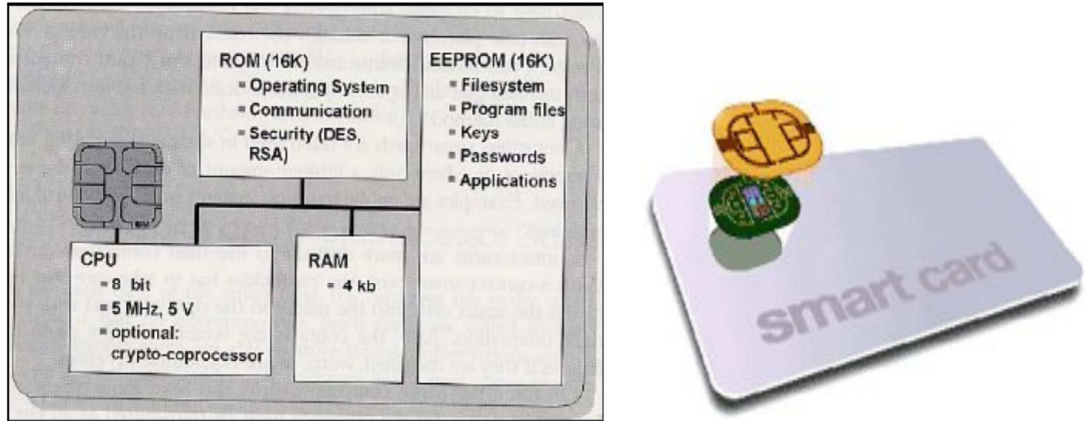
*Kent kart uygulamaları:* Kent kart uygulaması, Türkiye için en güncel projelerden biri olmaktadır. Birçok ilde pilot uygulaması bulunmaktadır. Kent kart uygulamasında amaç, kişinin sahip olduğu tek bir akıllı kart ile şehir içinde ulaşım, tiyatro, sinema, kütüphane, hayvanat bahçesi, otopark gibi hizmetlerden faydalanmasını sağlamaktır.

## 2.2. Akıllı Kartların Sınıflandırılması

Akıllı kartları üzerlerinde bulunan yongaya göre *temaslı akıllı kartlar* ve *temassız akıllı kartlar* olarak sınıflandırılmaktadır:

### 2.2.1. Temaslı akıllı kartlar:

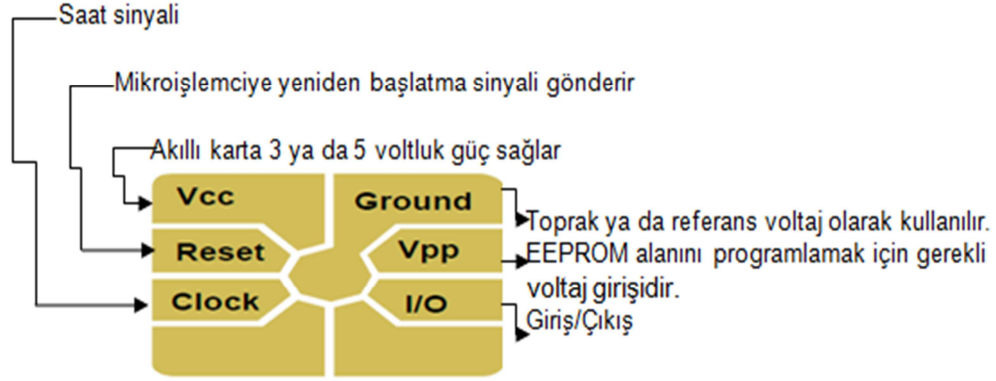
Adından da anlaşıldığı gibi temaslı akıllı kartların kullanımı sırasında okuyucu terminal ile temas etmesi gerekmektedir. Böylece kart yüzeyindeki iletken bölge ile doğrudan bağlantı kurulup, enerji ve veri alışverişi bu temas noktalarıyla sağlanmaktadır. Üzerinde işletim sistemi bulunan bir mikroişlemci ile, belleklerinde bulunan veri üzerinde işlem yaparlar.



Şekil 2.1 Kontaklı Akıllı Kart Mimarisi

Akıllı kart standartları ISO (International Organization for Standardization-Uluslararası Standardizasyon Organizasyonu) ve IEC (International Electrotechnical Commission-

Uluslararası Elektroteknik Komisyonu) tarafından belirlenmiştir. ISO/IEC 7810 ve ISO/IEC 7816 standartları, temaslı akıllı kartların standartlarını belirler. Bu standartlar, kartın fiziksel özellikleri, fiziksel karakteristikleri, kontak yerleşimi, kontak noktalarının ölçüleri, elektronik sinyaller ve iletişim protokolleri gibi standartları içerir.

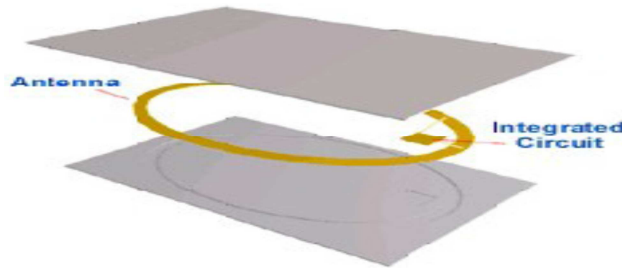


Şekil 2. 2 Temaslı Akıllı Kart Kontak noktaları

Temaslı kartların uygulama alanı olarak, cep telefonlarında kullanılan SIM kartlar ve banka işlemlerinde kullanılan kredi kartları örnek olarak verilebilir.

### 2.2.2. Temasız akıllı kartlar

Temaslı akıllı kartların aksine temasız akıllı kartlar, iletişim için kart okuyucu terminal ile fiziksel temasa ihtiyaç duymazlar. Gerek kart ve gerekse okuyucu ünite üzerinde birer anten bulunur. Böylece kartın okuyucu yuvasına sokulması gerekmez. Kart, okuyucuya belli bir mesafe yaklaştırıldığında, çalışması için gerekli olan enerji ve veri aktarımı kablosuz olarak radyo dalgalarıyla gerçekleşir. Temasız akıllı kartlarda bulunan anten sayesinde kartın her iki tarafı da kullanılabilir.



Şekil 2.3 Temasız Akıllı kart

ISO14443 protokolüne göre yakın mesafede çalışan kontaklız kartlar ile okuyucu terminal arasındaki haberleşme 13,56 MHz frekansta gerçekleşir. Kart ile okuyucu terminal arasında şifreli bir haberleşme gerçekleştirilerek işlemler yapılmaktadır.

Bu aşamada, RSA,3DES,AES, DES gibi güçlü şifreleme algoritmaları kullanılarak verinin güvenliği sağlanır.

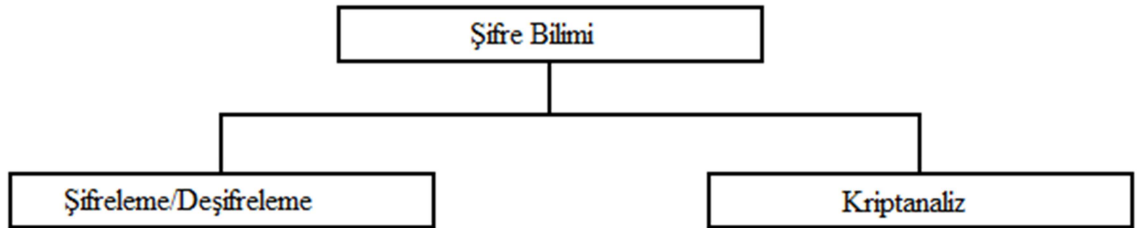
Temassız akıllı kartlarda, ISO/IEC 14443 ve ISO/IEC 15693 standartları uygulanmaktadır. Bu standartlar, kartın fiziksel özellikleri, RF ara yüzü, iletişim protokolleri gibi özellikleri içermektedir.

Başlıca kullanım alanı olan toplu geçişlerin olduğu otobüs ve turnikelerde ise zaman kaybını önleyerek yığılmaların önüne geçen bu sistem, ayrıca mekanik hiç bir parçasının bulunmaması nedeniyle uzun ömürlüdür.

## 2.3. Akıllı Kartlarda Veri Güvenliği

### 2.3.1. Şifreleme (Kriptografi)

Yunanca *krypto's* (gizli) ve *lo'gos* (sözcük) kelimelerinin birleşiminden meydana gelen kriptoloji (şifre bilimi), iletişimde gizlilik olarak değerlendirilmektedir. Bir sistemin içerisindeki verinin güvenli bir şekilde iletilmesinden emin olmak için gönderilen verinin şifrelenmesi gerekmektedir. Şifreleme, bir kısım bilgiyi anlaşılabilir şekilde dönüştürme sürecidir.



Şekil 2.4 Şifre biliminin sınıflandırılması

Şifre bilimi kriptografi (şifreleme/deşifreleme) ve kriptanaliz olmak üzere iki bölümde incelenmektedir. Gönderilmek istenen mesajın orijinal haline *açık mesaj*, bu mesajın şifrelenmiş şekli ise *şifreli metin* olarak adlandırılmaktadır.

Bir mesajın gizliliğini sağlamak amacıyla şifreleme yönteminin yanı sıra *stenografi* tekniği de kullanılabilir. *Şifreleme*, mesajın belirli bir teknikle anlaşılabilir bir biçime dönüştürülmesi iken, stenografi mesajın yine bir belirli bir tekniğe göre kısaltılması yöntemidir.

Akıllı kartlarda verinin güvenliğini sağlamak amacıyla, açık metinden şifreli metin oluşturmak için şifreleme algoritmaları kullanılmaktadır. Bu algoritmalar genellikle mesaj ve gizli anahtar olmak üzere iki giriş parametresine sahip matematiksel fonksiyonlardır (Schneier 1994).

### **2.3.2. Şifreleme algoritmalarının sınıflandırılması**

Bir şifreleme işleminin güvenli bir şekilde gerçekleştirilebilmesi için şifreleme sırasında kullanılan tüm bilgi ve yöntemlerin gizliliği esastır. Şifreleme anahtarı yardımıyla iletişim güvenliği artırılarak, şifreleme işlevlerinin bir şekilde açığa çıkarılması önlenmektedir. Bir şifreleme sistemi;

- Şifreleme Algoritması
- Açık Metin
- Şifreli Metin
- Anahtar

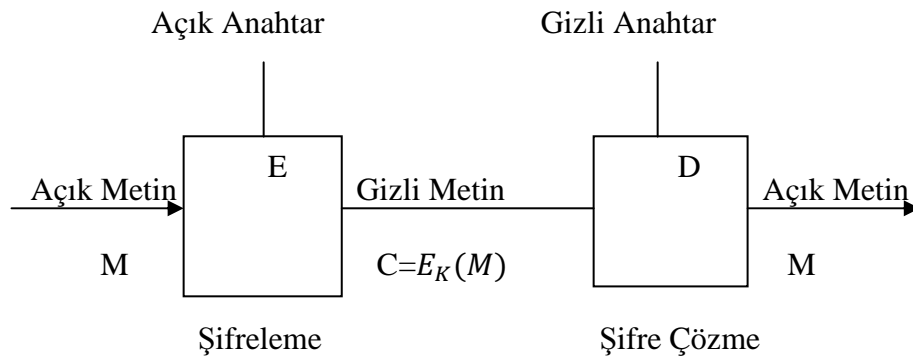
öğelerinden oluşmaktadır.

Modern şifreleme algoritmaları genellikle Kerchoff prensibine dayanmaktadır. Auguste Kerchoff tarafından bulunan bu prensibe göre, verinin güvenliği kullanılan algoritmanın değil anahtarın gizliliğine bağlı olmalıdır. Algoritma gizliliğinin esas olduğu sistemlerde ise güvenlik, saldırganın sistemin nasıl çalıştığını keşfetmediği sürece tehdit altında değildir. Günümüzde geçerliliği nadir de olsa bulunan bu tür sistemler çok eski sistemlerdir ve veri güvenliğinin gerektiği durumlarda kesinlikle tek başına tercih edilmemelidir.

Şifreleme algoritmaları kullanılan anahtara göre asimetrik ve simetrik şifreleme algoritmaları olmak üzere iki başlık altında incelenmektedir. *Simetrik şifreleme algoritmalarında*, şifreleme işlemi ve şifre çözme işlemi için aynı anahtar kullanılırken, *asimetrik şifreleme algoritmalarında* farklı iki anahtar kullanılmaktadır (Schneier 1994).

### 2.3.2.1. Asimetrik şifreleme (açık anahtar) algoritmaları

İlk olarak, 1976 yılında Whitfield Diffie ve Martin E. Hellman adlı araştırmacılar iki farklı anahtara dayalı algoritma düşüncesini geliştirmişlerdir. Bu anahtarlardan biri açık diğeri ise gizli anahtardır. Şifreleme ve şifre çözme işlevleri için farklı anahtarlar kullanılmaktadır. Şifreleme için *açık anahtar* kullanılırken, şifre çözme işlemi için *gizli anahtar* kullanılır. Açık anahtardan gizli anahtarın üretilmesi pratik olarak mümkün olmamaktadır.



Şekil 2.5 Asimetrik şifreleme algoritması gösterimi

#### ***RSA algoritması***

Ronald L. Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiş bir *açık anahtar* algoritmasıdır. Büyük tamsayı aritmetiğine dayalı basit bir işletim esasına göre çalışmaktadır. Gizli ve açık anahtar, iki büyük asal sayıdan üretilir.



Şifreleme ve şifre çözme süreçleri matematiksel olarak aşağıdaki gibi ifade edilebilir:

$$\text{şifreleme} = y = x^e \bmod n$$

$$\text{şifre çözme} = x = y^d \bmod n$$

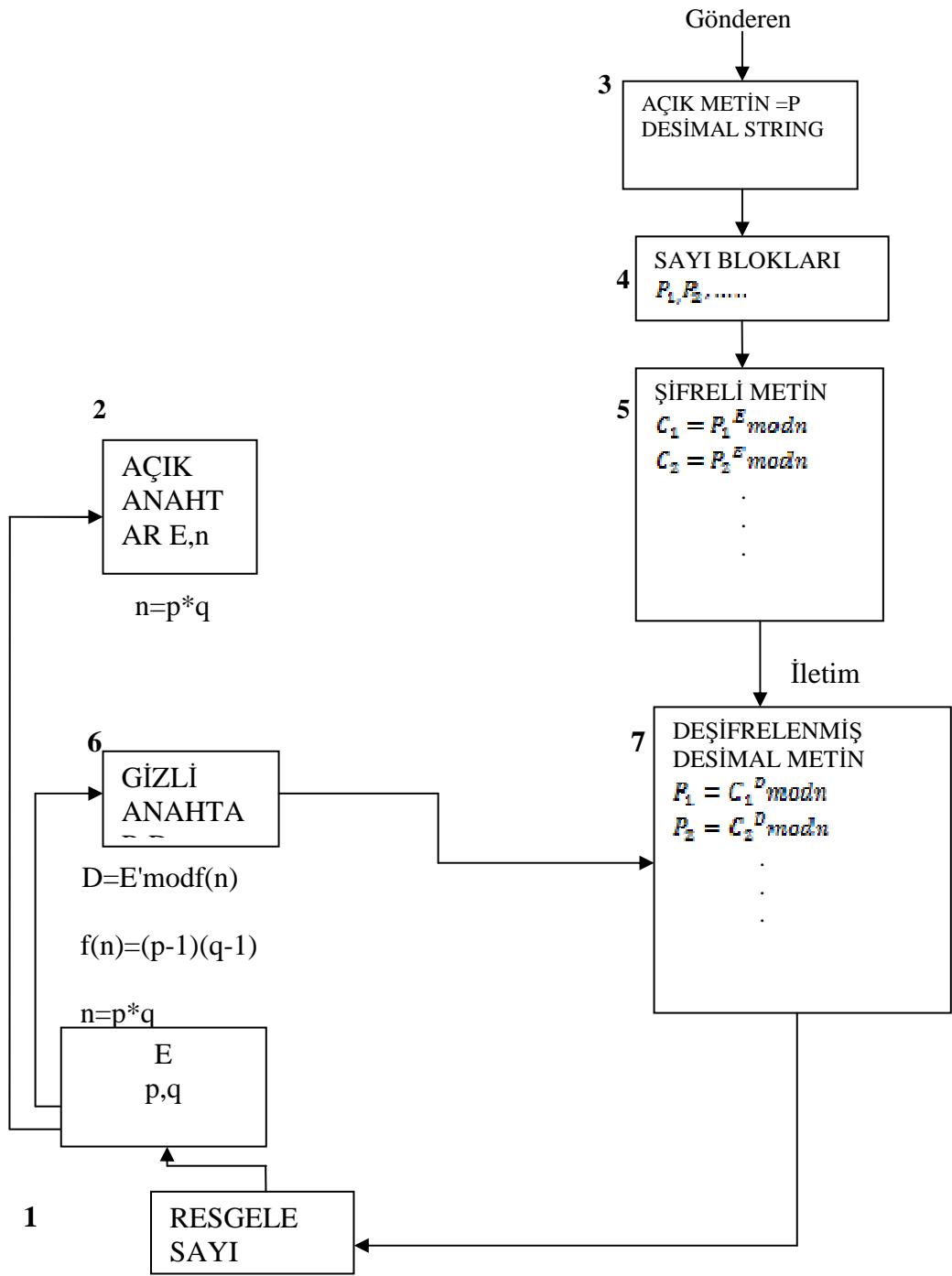
Burada  $x$ , şifresiz metni;  $y$ , şifreli metni;  $e$ , açık anahtarı;  $d$ , gizli anahtarı;  $n$ , açık modülü ifade eder. Ayrıca  $p$  ve  $q$  gizli asal sayılarının çarpımı açık modülü verir ( $n=p.q$ ).

Kodlamadan önce, şifresiz metin uzunluğu, RSA algoritmasında kullanılan anahtar uzunluğuna göre değişen uygun uzunluklardaki bloklar haline dönüştürülmelidir. Şifreleme, modül işleminin takip ettiği şifresiz metnin üs alma işlemiyle gerçekleşir.

Algoritmada ancak gizli anahtar biliniyorsa şifresiz metin elde edilebilir. Algoritmanın gösterimine şekli 2.6 da detaylı olarak yer verilmektedir.

### **2.3.2.2. Simetrik şifreleme algoritmaları**

Simetrik şifreleme algoritmaları, blok ve akan şifreleme algoritmaları olarak ikiye ayrılmaktadır. Akan şifreleme algoritmasında, metnin tek seferde sadece 1 bit ya da 1 baytı şifrelenirken; blok şifreleme algoritmasında bu işlem blok olarak adlandırılan kümeler halinde yapılmaktadır. Akan şifrelemeye örnek olarak Enigma, RC-4, A5 algoritmaları gösterilebilir. Akıllı kart teknolojilerinde kullanılan AES ve DES algoritmaları blok şifrelemeye örnektir. Blok şifreleme algoritmalarının gücünün ölçülmesinde; algoritmada kullanılan S kutuları, döngü sayısı, anahtarların XOR işlemine sokulması, blok uzunluğu, anahtarın uzunluğu ve niteliği önemlidir. Shannon' a göre bir şifreleme algoritmasının güçlü olması için blok uzunluğunun en azından anahtar uzunluğuna eşit olması gerekmektedir. Ayrıca anahtarın rastlantısal olması da gerekmektedir.



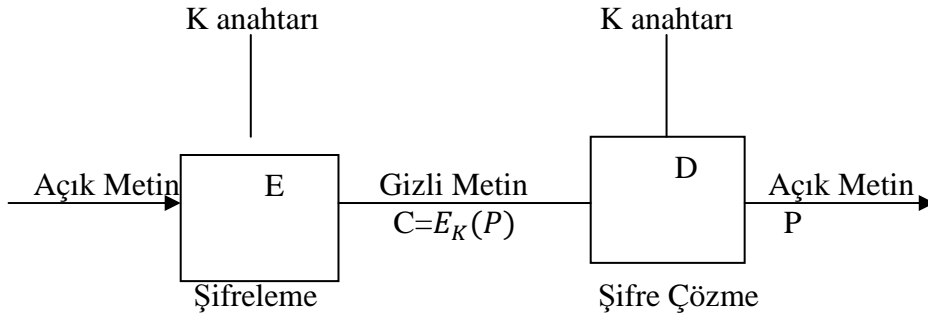
Şekil 2.6 RSA Şifreleme ve Şifre çözme işlemi Gösterimi

Simetrik algoritmalar şifreleme ve şifre çözme işleminde aynı gizli anahtarı kullanmaktadır. Bu algoritmalar *gizli anahtar algoritmaları* olarak da adlandırılır. Haberleşmeye başlamadan önce alıcı ve verici taraf bir anahtar belirler. Simetrik algoritmaların güvenliği tamamıyla bu gizli anahtara bağlıdır. Bu anahtarın bir şekilde ele geçirilmesi demek, mesajın da ele geçirilmesi anlamına gelmektedir.  $P$  açık metni,  $C$  şifreli metni,  $E$  ve  $D$  simgelerinin şifreleme ve şifre çözme işlevlerini temsil ettiği bir ifadede, simetrik algoritma için şifreleme ve şifre çözme işlemlerinin gösterimi aşağıdaki gibidir:

$$E_K(P) = C$$

$$D_K(C) = P$$

Her iki ifadede de  $K$  şifreleme anahtarını temsil etmektedir. Burada  $K$  anahtarını kullanmanın amacı, eğer  $P$  açık metni sadece  $E$  kriptoloji ile şifrelenirse gizliliği sağlayacak olan tek parametre şifreleme algoritması olacaktır. Bu durumda, iletişim güvenliğini arttırmak için alıcı tarafın her yeni şifreleme işlevi için farklı bir kriptoloji algoritmasını bilmesi gerekmektedir. Başka bir deyişle,  $K$  anahtarı mesajın şifreleme algoritması bilinse de ikinci bir güvenlik parametresi olduğundan iletişim güvenliğini arttırmaktadır.



Şekil 2.7 Simetrik algoritmada şifreleme ve şifre çözme işlemi

Eğer mesajın şifrelediği  $E$  işlevi kaybolursa olursa, yeni bir algoritma tasarlanmak durumundadır. Bu durumda zaman kaybı da göz önüne alınacak olursa oldukça pahalı bir yöntemdir.

## 2.4. Blok Şifreleme Algoritmaları

Blok şifreler, Shannon'un önerdiği karıştırma(confusion) ve yayılma(diffusion) tekniklerine dayanmaktadır. Karıştırma tekniğinde şifreli metin ile açık metin arasındaki ilişkiyi gizlemek amaçlanırken, yayılma tekniği açık metindeki izlerin şifreli metinde sezilmemesini amaçlar. Karıştırma, yerdeğiştirme işlemleriyle(S-Box yapısı); yayılma, doğrusal dönüşüm işlemleriyle gerçekleşmektedir. Blok şifreleme yapısı Feistel ve yerdeğiştirme-permutasyon ağı olmak üzere ikiye ayrılır. Her iki mimari de doğrusal dönüşüm ve yer değiştirme işlemlerini kullanır.

Blok şifreleme birden fazla şifreleme işleminin gerçekleşmesiyle oluşur. Bu durum aynı şifreleme işleminin tekrarlanması anlamına gelir. Her şifreleme adımına **döngü** denir. Her döngüde kullanılan anahtar genellikle farklıdır. Bir döngüde birden fazla şifreleme işlemi de yapılabilmektedir. Şifreleme işlemi yapılırken, açık metin bloklara bölünür ve her blok bir bütün olarak şifrelenir. Blok şifrelemede güvenliği sağlamak amacıyla çeşitli şifreleme modları bulunmaktadır. Blok şifrelerin çoğunluğu iteratif yapıdadır ve her bir döngünün çıkışı, bir sonraki döngünün girişi olarak tanımlanır.

Akıllı kartlarda veri güvenliğinin sağlanması için kullanılan en yaygın algoritmalar, dinamik yapısı sebebiyle blok şifreleme algoritmalarıdır. Bu bölümde blok şifreleme algoritmalarında kullanılan çeşitli terimler hakkında kısa bilgi verilecektir.

### **Anahtar**

Anahtar uzunluğu ya da bit sayısı temel bir saldırı olan geniş anahtar arama saldırısına karşı dayanıklı olmalıdır. Örnek olarak DES algoritması 56-bit anahtar kullanır. Buna karşılık AES daha güvenli bir şekilde 128,192,256 bit anahtar seçeneklerini kullanır. Anahtar rastgele olmalıdır. Birbiriyle ilişkili üretilen anahtarlar, saldırılar için zayıflık gösterirler.

### **Döngü sayısı**

Lineer dönüşüm ve yer değiştirme işlemlerinin algoritmaya yeterli gücü sağlaması bakımından seçilen döngü sayısı büyük önem taşımaktadır. Lars Knudsen' e göre döngü sayısı en kaba haliyle

$$r \geq dn/w \quad (2.1)$$

şeklinde olmalıdır. Burada  $r$  döngü sayısını,  $n$  blok genişliğini,  $d$  yer değiştirme durumuna bir word ü almak için gerekli olan en fazla döngü sayısını,  $w$  ise tüm şifrede yer değiştirme durumuna giriş olan en az kelime genişliğini temsil eder. Döngü sayısı iyi seçilmek zorundadır. Çünkü lineer dönüşüm ve yer değiştirme operasyonlarının bu seçilen değerle algoritmaya yeterli gücü vermesi gerekmektedir.

### ***S kutuları (S-box )***

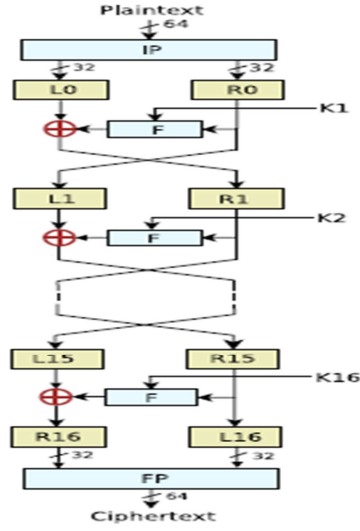
Blok şifreleme algoritmasında en önemli öğedir. Algoritmadaki tek non-lineer yapı olması sebebiyle algoritmanın gücünü de belirler. S kutularının genişliği kriptanaliz saldırıları açısından önemlidir. Büyük sayıda giriş ve çıkış bitleri, özellikle farksal ve doğrusal saldırılardan korunmak için önemlidir. Blok şifreleme algoritmasının en önemli adımıdır. S kutuları için 3 önemli nokta vardır. Bunların belirlenmesinde doğrusal kriptanaliz, farksal kriptanaliz ve Davies saldırıları etkili olmuştur. Bunlar; SAC(Strict Avalanche Criteria), S kutularının genişliği ve çıkış dağılımlarının Davies saldırılarına karşı dayanıklılığı noktalarıdır. SAC kriterine göre 1 bit giriş değişimi sonucunda her çıkış bitinin değişme olasılığı  $\frac{1}{2}$  olmaktadır.

### **2.4.1. DES (Data Encryption Standard) algoritması**

DES algoritması en önemli modern simetrik şifreleme algoritmasıdır. Sivil güvenlikle ilgili verilerde kullanılmak için Amerika Birleşik Devletleri tarafından 1977 yılında yayınlanmıştır.

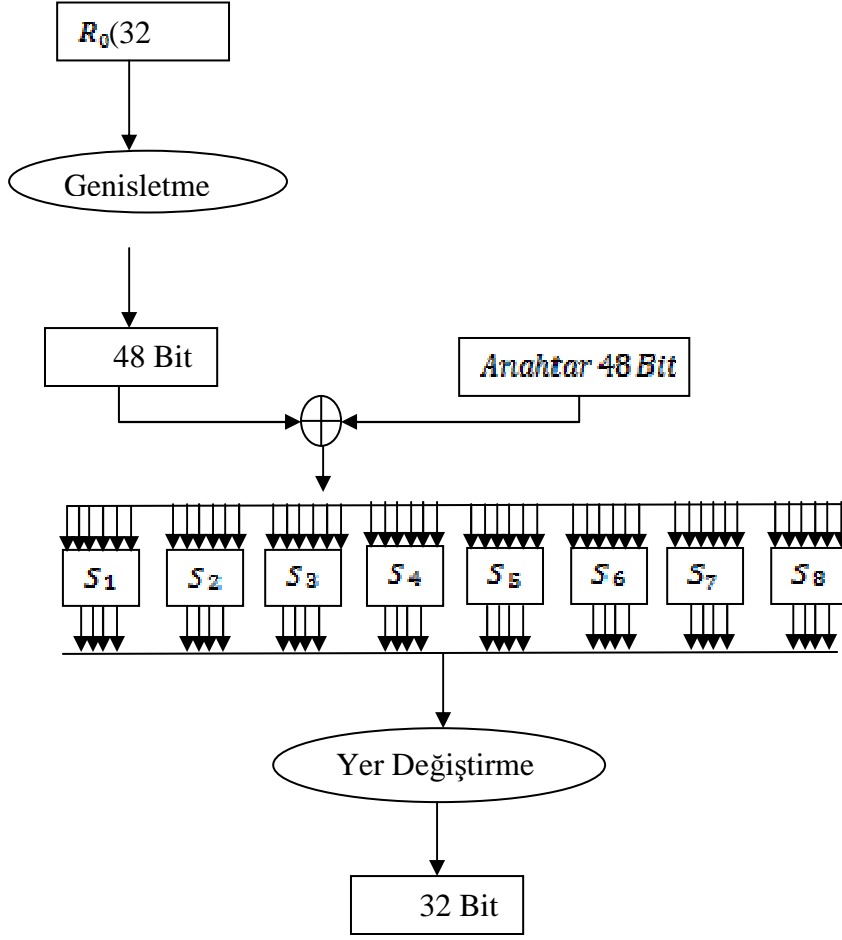
DES algoritması, 64 bitlik veri bloklarını, 56 bit uzunluğunda anahtar kullanarak şifreleme işlemini gerçekleştirmektedir.  $2^{56}$  adet olası anahtar kullanılabilir. Gerçekte anahtar uzunluğu 64 bit olarak ifade edilir, ancak diğer 8 bit eşlik biti olarak kullanılır ve ihmal edilir. Şifreleme ve şifre çözme için aynı anahtar kullanılır.

Algoritmanın genel yapısı şekil 2.8' de görüldüğü gibi başlangıç permütasyonu(IP),her biri döngü olarak adlandırılan 16 özdeş katman ve başlangıç permütasyonunun tersi olan bitiş permütasyonundan(FP) oluşmaktadır.



Şekil 2.8 DES şifreleme algoritmasının feistel yapısı

Başlangıç permütasyonundan sonra blok 32 bit uzunluğunda iki eşit parçaya ayrılır. Her bir döngüde anahtar bitler kaydırılır, anahtarın 56 bitinin içinden 48 bit seçilir. Genişletme permutasyonu ile sağ yarım bit 48 bite genişletilir. Kaydırılan ve yer değiştirilen anahtarın 48 biti XOR uygulanarak birleştirilip, 32 yeni bit üreten 8 adet S-kutusuna gönderilir ve yeniden yer değiştirme uygulanır. Bu 4 işlem  $F$  fonksiyonunu oluşturur.  $F$  fonksiyonuna ait gösterim Şekil 2.9’ da görülmektedir. Bu  $F$  fonksiyonun çıkışı XOR işlemi ile sol yarım bit ile birleştirilir. Bu işlemin sonucunda yeni sağ yarım oluşmuş olur. Eski sağ yarım olduğu gibi yeni sol yarımı oluşturur.



Şekil 2.9 F fonksiyonu gösterimi

Bu işlem adımları 16 döngü boyunca tekrarlanır. Son olarak 16. döngünün sonunda ayrı olan bölümler birleşir ve bitiş permütasyonu uygulanır. Bitiş permütasyonu, başlangıç permütasyonunun tersidir. Böylece algoritma tamamlanır.

$i$ .inci iterasyonun sağ ve sol yarım bitleri sırasıyla  $R_i$  ve  $L_i$  şeklinde ve  $K_i$ ,  $i$  döngüsü için 48 bit anahtar olarak ifade edilirse F fonksiyonunun ifadesi

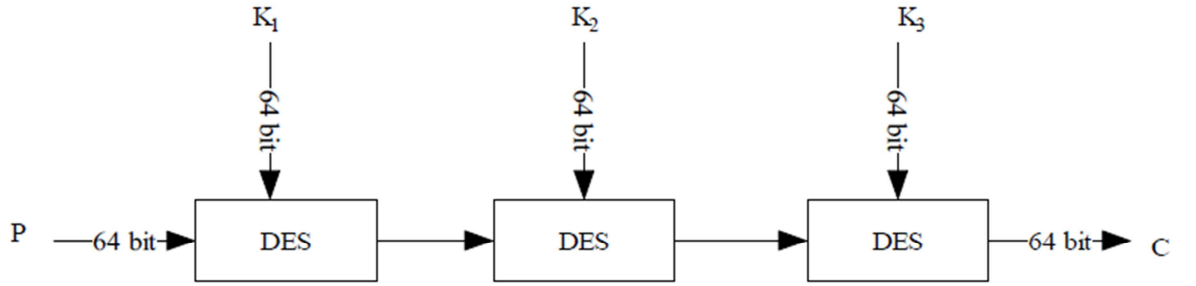
$$L_i = R_{i-1} \quad (2.2)$$

$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \quad (2.3)$$

şeklinde olmaktadır. DES algoritması en yaygın kullanılan şifreleme algoritmalarından biridir.

### 2.4.2. 3DES algoritması

Gelişen bilgisayar teknolojisi karşısında DES şifreleme algoritmasının zayıf kalmasına karşın 3DES(TripleDES) şifreleme algoritması geliştirilmiştir. Bu algoritma ard arda üç adet DES şifreleme algoritmasının gerçekleştirilmesinden oluşmaktadır. Böylece anahtar uzunluğu  $56 \times 3 = 168$  bit olduğu için deneme-yanılma ile anahtar bulma günün teknolojisi ile imkânsız hale gelmektedir.

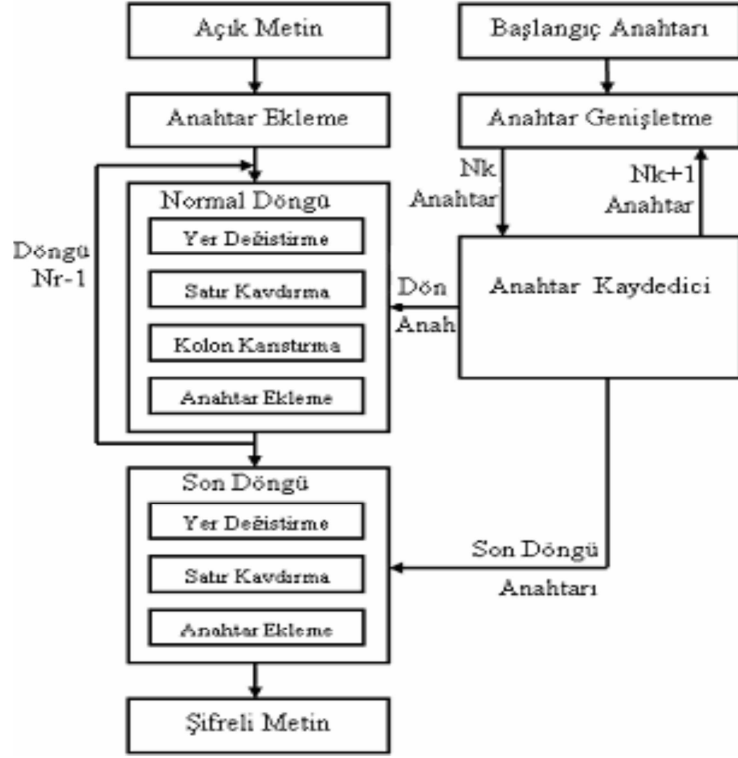


Şekil 2.10 3DES yapısı

### 2.4.3. AES (Advanced Encryption Standard) algoritması

Gelişmiş şifreleme standardı (AES) ,Kasım 2001’de elektronik verinin saklanması için kullanılmak üzere Federal Bilgi İşleme Standardı (FIPS) olarak Amerikan ulusal standartlar ve teknoloji enstitüsü (NIST) tarafından yayınlanmıştır. AES algoritması, 128,192 veya 256 anahtar bit kullanarak veriyi 128 bitlik bölümler halinde kodlayan bir simetrik blok şifreleme algoritmasıdır. Şekil 2.11 AES algoritmasının blok diyagramını göstermektedir.





Şekil 2.11 AES blok diyagramı

Döngü sayısı, anahtar uzunluğu ve metin uzunluğuna göre değişiklik göstermektedir. Şekil 2.12 bulunan tabloda anahtar uzunluğuna ve metin uzunluğuna göre döngü sayıları gösterilmektedir.

	Anahtar Uzunluğu( $N_k$ )	Blok Boyutu( $N_b$ )	Döngü Sayısı( $N_r$ )
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Şekil 2.12 AES algoritmasına ait anahtar uzunluğu-tur sayısı-blok boyutu ilişkisi

AES algoritmasında mesaj ilk olarak 4x4 bayt matrisine dönüştürülür. Sonra sırasıyla baytların yer değiştirmesi, satır kaydırma, sütun karıştırma ve anahtar ekleme işlemleri gerçekleşir. Eklenen anahtar o döngü için belirlenmiştir ve ekleme XOR işlemiyle gerçekleştirilir. AES algoritması 128 bit veri bloklarını 128,192 ve 256 bit anahtar

seçenekleri ile şifreler. Bu özelliği ile şu ana kadar kullanılan şifreleme algoritmaları arasında en güçlü olanıdır.

#### 2.4.3.1. AES tur dönüşümü

Bu bölümde AES şifreleme algoritmasına ait bir tur döngüsündeki işlemler anlatılacaktır. Bahsedildiği gibi AES şifreleme algoritması ‘adım’ adı verilen, birbirini izleyen dört adımdan oluşmaktadır;

- a) Bayt değiştirme,
- b.) Satırları kaydırma,
- c) Sütunları Karıştırma,
- d) Tur anahtarının eklenmesi.

Her adım, bir önceki adımın çıktısını giriş durumu olarak alır. Son turda ise ‘Sütunları Karıştırma’ adımı atlanır ve ‘*Tur anahtarının eklenmesi*’ adımı, *Satırları kaydırma* adımının çıktısı kullanılır. AES turunun adımlarının her biri, ters-dönüşümü olan işlemlerdir.

#### 2.4.3.2. Bayt değiştirme

Bayt değiştirme işleminde 128 bit veri, her biri 8 bit olan 16 bloğa ayrılarak şekil 2.12 ‘de gösterildiği gibi 4x4 boyutunda bir durum matrisi oluşturulur.

S <sub>0</sub>	S <sub>4</sub>	S <sub>8</sub>	S <sub>12</sub>
S <sub>1</sub>	S <sub>5</sub>	S <sub>9</sub>	S <sub>13</sub>
S <sub>2</sub>	S <sub>6</sub>	S <sub>10</sub>	S <sub>14</sub>
S <sub>3</sub>	S <sub>7</sub>	S <sub>11</sub>	S <sub>15</sub>

Şekil 2.13 4x4 durum matrisi

Bayt değiştirme işlemi algoritma içerisindeki tek doğrusal olmayan dönüşüm işlemidir. Bu dönüşüm ‘S Kutusu(S-Box)’ adı verilen bir değiştirme tablosu kullanılarak gerçekleştirilir.

Ayrılan her 8 bit için iki aşamadan oluşan bir matematiksel dönüşüm uygulanır:

1) Giriş sekizlisi,  $GF(2^8)$  uzayında bir polinom olarak ele alınır ve matematiksel olarak terslenir. Hex{00} elemanı yine kendisine atanır.

2) Birinci dönüşümün sonunda elde edilen değere, afin dönüşüm uygulanır.  $b_i$  afin dönüşüm girişindeki sekizlinin  $i$ 'inci biti olmak üzere, afin dönüşümü aşağıdaki gibi ifade edilebilir:

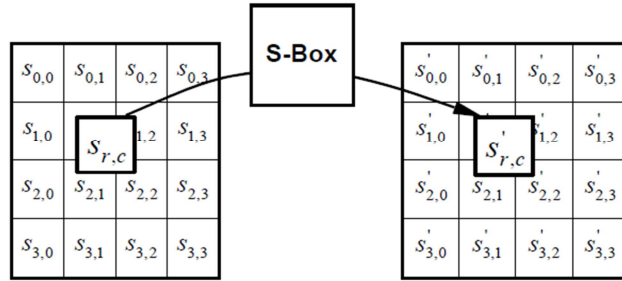
$$\bar{b}_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \quad (2.4)$$

Burada  $c_i$ , Hex{63} değerinin  $i$ 'inci bitidir.

Afin Dönüşüm kısmının, matris formuyla ifadesi aşağıda verilmektedir.

$$\begin{bmatrix} \bar{b}_0 \\ \bar{b}_1 \\ \bar{b}_2 \\ \bar{b}_3 \\ \bar{b}_4 \\ \bar{b}_5 \\ \bar{b}_6 \\ \bar{b}_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Şekil 2.13' de afin dönüşümünün gerçekleşmesi görülmektedir.



Şekil 2.14 Sekizli bayt değiştirme dönüşümü

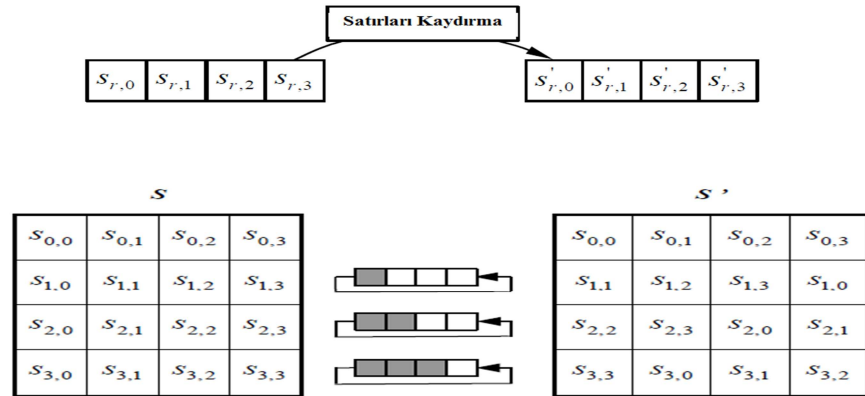
Şekil 2.14' de onaltılık form için yer değiştirme tablosu yer almaktadır. Örneğin  $s_{1,1} = \{53\}$  olsun. Bu durumda 5 numaralı satır ile 3 numaralı sütunun kesişme noktası yer değiştirme değerini belirlemektedir. Sonuç olarak  $s'_{1,1} = \{ed\}$  olur.

	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

Şekil 2.15 Onaltılık durum için S-kutusu çıkışları

### 2.4.3.3. Satırları kaydırma

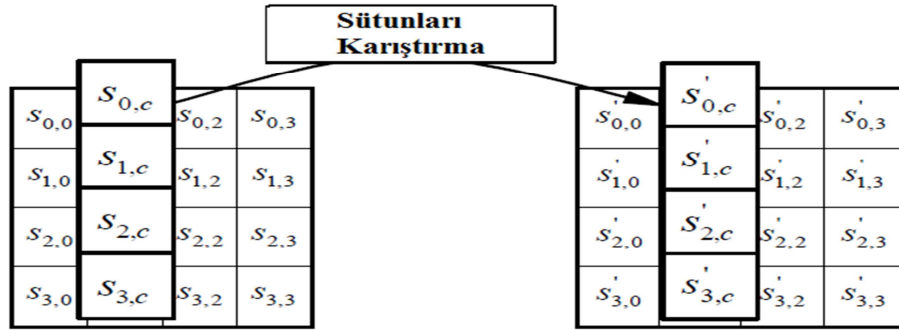
Bayt değiştirme işleminde elde edilen 128 bit veri, yine 8 bitlik 16 parçaya ayrılarak durum matrisi elde edilir. Satırları kaydırma, adından da anlaşılacağı gibi, bu matrisin satırları üzerinde işlem yapar. İlk satır aynı bırakılır. İkinci satır sağdan sola doğru bir pozisyon değiştirecek şekilde, döngüsel olarak kaydırılır. Döngüsel kaydırma nedeniyle, 1. sütuna gelen eleman kaydırıldığında 4.sütuna geçer. Üçüncü satır benzer şekilde iki pozisyon, dördüncü satır da üç pozisyon döngüsel olarak kaydırılır. Bu işlemler sonucunda yeni bir 128 bitlik veri elde edilir. Şekil 2.15’ de satırları kaydırma işleminin blok diyagramı bulunmaktadır.



2.16 Satırları kaydırma dönüşümü

#### 2.4.3.4. Sütunları karıştırma

Sütunları karıştırma dönüşümünde, 4x4'lük durum matrisinin sütunları üzerinde işlem yapılmaktadır. Giriş durum matrisinin her sütunu, sütunları karıştırma dönüşümünden geçirilerek, çıkışta yeni bir durum matrisi elde edilir. GF(2) için doğrusal bir işlem olan sütunları karıştırma, algoritmaya yayılım (diffusion) özelliği kazandırmaktadır.



2.17 Sütunları karıştırma dönüşümü

Durum matrisinin her bir sütunu, katsayıları GF(2<sup>8</sup>)'in birer elemanı olan üçüncü dereceden birer polinom olarak ele alınır.

Bu polinomlar  $a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$  olarak verilen bir  $a(x)$  polinomu ile, modülo  $x^4 + 1$ 'de çarpılarak sütunları karıştırma dönüşümü gerçekleştirilir. Sütunları kaydırma dönüşümüne ait blok diyagram şekil 2.16' da verilmektedir.

## 2.5. Akıllı Kartlara Karşı Saldırı Yöntemleri

Kriptografik cihazlara karşı yapılan saldırılar genellikle sistemdeki zayıf noktalara dayanmaktadır. Bu tür sistemler açık ve gizli anahtara sahiptirler. Saldırıların kaynağında da bu iki anahtar yatmaktadır. Saldırıların da çeşitleri vardır. Akıllı kartlarda saldırı yöntemleri Fiziksel (invasive tampering attack), algoritmaya yönelik, yan-kanal analizi saldırıları olmak üzere 3 başlıkta incelenecektir.

### 2.5.1. Fiziksel saldırılar:

Karta fiziksel olarak, özel bir donanımla müdahale edilmek suretiyle gerçekleştirilen saldırılardır. Laboratuvar ortamında ve çok uzun bir süreci kapsayan ataklardır. Kartın plastiği tamamen çıkartılıp, direk yonga üzerinde çalışmalar yürütülmektedir. Fiziksel saldırılar için akıllı kartlar hakkında başlangıç seviyesinde bilgi sahibi olmak yeterli olmaktadır. Örneğin EEPROM da saklanan bilginin UV ışın v.b. Yöntemlerle silinmesi ve akıllı kart üzerindeki yongadan microprobing yöntemiyle bilgi çalınması fiziksel saldırıdır. Genel olarak fiziksel saldırılar, çok zaman alıcı ve yıkıcı ataklar olmaktadır.

### 2.5.2. Algoritmaya yönelik saldırılar

Verilen şifrenin çözülmesi ya da şifrenin çözülmesi için kullanılan kriptografik algoritmaya yönelik saldırılardır. Genel olarak saldırılar için üç parametre önemlidir: veri, veri alanı ve zaman. Temel ve gelişmiş saldırılar olarak iki ana başlıkta incelenebilmektedir.

**2.5.2.1. Temel saldırılar:** Temel saldırılar sözlük saldırısı, kod kitabı saldırısı ve gelişmiş anahtar saldırısı olmak üzere 3 grupta incelenmektedir. Uzunluğu  $n$  bit ve anahtar uzunluğu  $k$  bit olan bir blok şifresi için en temel saldırı *sözlük saldırısı*dır. Sözlük saldırısında, saldırgan  $k$  bitlik bir anahtar kullanarak açık metni mümkün olan  $2^k$  anahtarla şifreler. Şifrelenen metinleri sıralı bir sözlükte tutar. Saldırgan gizli anahtarla şifreli seçilmiş bir açık metni elde eder ve uygun eşleşmeyi oluşturduğu sözlükten kontrole eder. Saldırı için  $2^k$  tane  $n$ -bit kelime belleği gerekir.

*Kod kitabı saldırısında*, saldırgan olası  $2^n$  açık metnin gizli bir anahtar ile şifrelenmiş metinlerini elde ederek kod kitabı olarak adlandırılan bir tabloya depolar. Elde ettiği şifreli metni tablodakiler ile karşılaştırarak açık metni elde eder. Saldırı için  $2^n$  açık metin ve  $2^n$  kelime belleği gerektirdiğinden pahalı bir saldırdır.

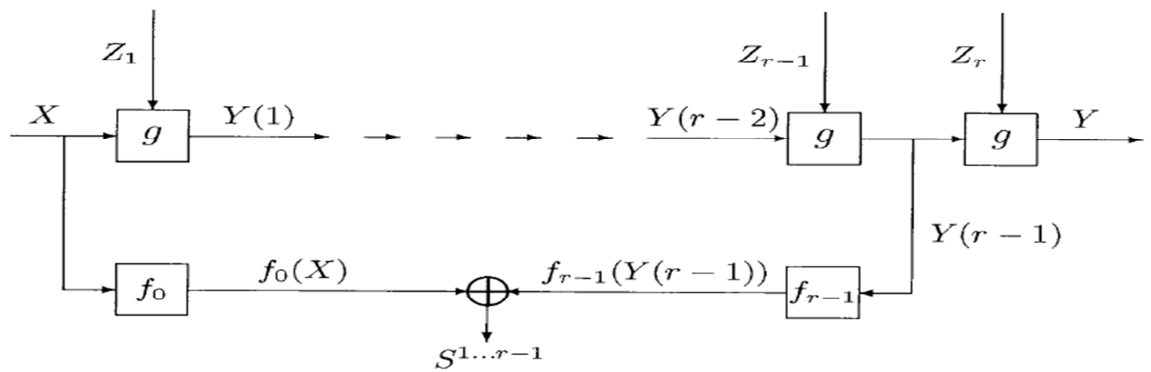
*Geniş anahtar arama saldırısında* mümkün olan  $2^k$  anahtar, şifreli metinden anlamlı bir açık metin elde edilinceye kadar denir. Eğer kriptanaliz saldırısında, bir geniş anahtar arama saldırı tekniğinde harcanandan daha az güç harcayarak blok şifre kırılırsa, bu saldırı başarılı bir saldırı olarak düşünülebilir.

### 2.5.2.2. Gelişmiş saldırılar:

Doğrusal kriptanaliz ve farksal kriptanaliz olmak üzere ikiye ayrılmaktadır:

#### *Doğrusal kriptanaliz*

Doğrusal kriptanaliz, tüm blok şifrelere uygulanabilen bir *bilinen açık metin* saldırı türüdür. Doğrusal kriptanaliz ilk olarak FEAL algoritmasına uygulanmış, fakat asıl ilk olarak 1993 yılında Matsui tarafından teorik bir saldırı olarak keşfedilmiştir. Bu saldırıda, saldırganın algoritmayı bildiği (Kerchoffs Kuralı) ve belli sayıda açık metin ve şifreli metinlere sahip olduğu varsayılmaktadır. Lineer kriptanaliz, şifreli metin bitleriyle açık metin bitleri arasındaki yüksek olasılıklı lineer ifadelerin meydana gelme avantajını kullanmaktadır. Küçük S-kutularının tasarımı lineer kriptanalizin uygulanmasını engelleyici yöndedir.



Şekil 2.18 Lineer kriptanaliz blok şeması

### ***Farksal kriptanaliz***

Farksal kriptanaliz ilk olarak 1991 yılında Biham ve Shamir tarafından yayınlanmıştır. Farksal kriptanaliz, açık metin çiftlerindeki belirli farklılıkların, oluşan şifreli metin farkları üzerindeki etkiyi analiz eden bir yöntemdir. Farkın algoritmada ilerlemesi istatistiksel olarak hesaplanır ve çıkışta bu istatistiksel özellik gözlenir. İstatistiksel olmasının nedeni algoritmada yer alan ve lineer olmayan yapıdaki S-Kutularıdır. Kısaca farksal kriptanaliz çok sayıda blok şifreleme sistemine uygulanmış bir *seçilmiş açık metin saldırısıdır* ve açık metin farklarının algoritma içerisinde ilerlemesine dayanmaktadır.

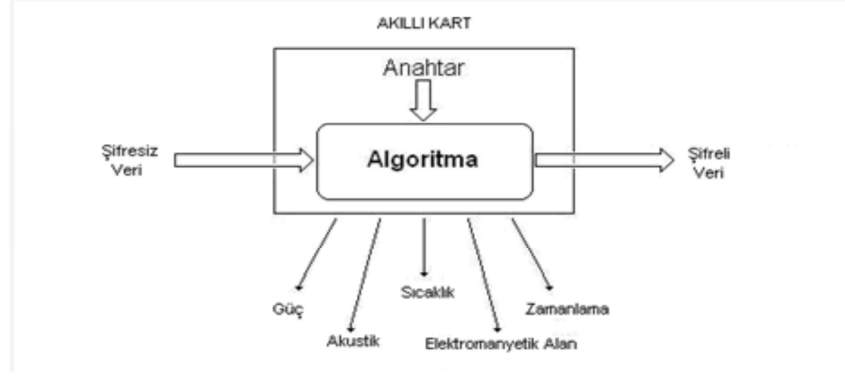
#### **2.5.3. Yazılıma yönelik saldırılar:**

Yazılım saldırıları kartın haberleşme ara yüzündeki uygulama zayıflıklarından faydalanır. Bu tip saldırılar arabellek taşmalarını sömürmeyi ve değişik yazılımlar aracılığıyla kasıtlı olarak yongaya kötü niyetli kod yerleştirmeyi içermektedir.

#### **2.5.4. Yan kanal analizi saldırıları**

Akıllı kartların kriptografik algoritmanın gerçekleşmesi sırasında ürettiği istem dışı gibi kriptografik algoritmaların gerçeklemeleri olan cihazlar istem dışı bazı çıkışlar yan kanal bilgisi olarak adlandırılmaktadır. Bu çıkışlar, kartın tasarımından kaynaklanan zayıflıkların sebep olduğu fiziksel karakteristikler tarafından sızdırılmaktadır. Bu ekstra bilgi kartın yaptığı işlem veya işlenen veriye bağlı olarak zaman, güç veya elektromanyetik sızıntı şeklinde olabilmektedir. Çok güçlü matematiksel algoritmaların kullanılması durumunda bile tasarımdan kaynaklanan zayıflıklarla güçsüz hale getirilebilir.





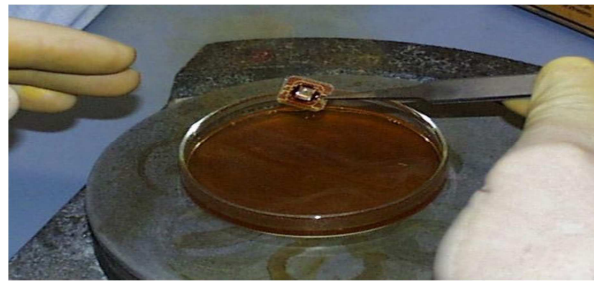
Şekil 2.19 Akıllı karttan sızan yan-kanal bilgileri

Yan kanal saldırıları aktif ve pasif saldırılar olmak üzere ikiye ayrılmaktadır.

#### 2.5.4.1. Aktif saldırılar

Kurcalama saldırısı olarak da adlandırılan aktif saldırılarda, karta fiziksel olarak müdahale gerekmektedir. Saldırgan kriptografik sistemin iç devresine ulaşmayı hedeflemektedir. Laboratuvar ortamında ve haftalarca süren bir çalışma gerektirmesi sebebiyle sabır istemektedir. Aktif saldırılar ölçüm ve hata oluşturma saldırıları olarak ikiye ayrılmaktadır.

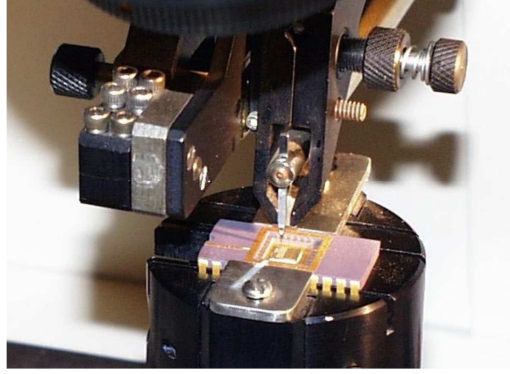
Kömmerling ve Kuhn akıllı kart yongası üzerinde kurcalama saldırısı gerçekleştirmek amacıyla çalışmalar yapmışlardır. Kurcalama saldırılarına, kimyasalla kartın plastiğinin eritilmesiyle başlanmaktadır.



Şekil 2.20 Sıcak nitrik asit çipe zarar vermeden plastiğin eritilmesi sağlar

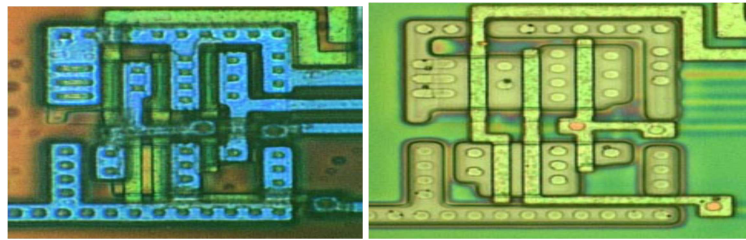
Devrenin iç kısmındaki veri yollarına ve hafıza alanlarına sensor yardımıyla bakılarak yapılmaktadır. Amaç bellek bölgelerini okuyarak ya da veri iletim hatlarını gözleyerek

gizli bilgiye erişmektir. Ölçüm saldırıları *prob saldırısı* olarak da anılır. Yukarıdaki şekilde plastiğin eritilmesi işleminden bir kare bulunmaktadır.



Şekil 2.21 Çıkarılan akıllı kart işlemcisi test paketine monte edilir

Bundan sonraki aşama, akıllı kartın işlemcisinin haritasını oluşturmaktır. Çip yüzeyinin yüksek çözünürlüklü fotoğraflarının üretilmesi için CCD kamera sahip bir optik mikroskop kullanılmaktadır. Veri ve adres hatları gibi temel yapılar hemen tanımlanabilir (ROM, RAM, EEPROM, ALU...) . Tüm işlem modülleri ana veri yoluna genellikle kolayca ayırt edilebilir mandal ve veri yolu sürücüleriyle bağlanır. Saldırgan CMOS VLSI tasarım teknikleri ve mikroişlemci mimarileri hakkında bilgiye sahip olmalıdır. Çip üzerindeki işlemcinin haritası bir CCD kameralı optik mikroskop yardımıyla çıkarılabilmektedir.



Şekil 2.22 Soldaki şekilde aynı odaklı mikroskoptan alınan CMOS AND görülüyor. Sağdaki şekilde ise aynı kapının metal tabaka çıkarıldıktan sonraki görünümü bulunuyor.

### ***Hata indükleme saldırısı***

Hata indükleme ya da hata oluşturma atağında ise devre çalışır vaziyette iken belirli noktalara dışarıdan müdahale edilip devrenin davranışını değiştirerek hata yaptırmak suretiyle yapılır. Örneğin tüm devreye hata ürettirecek şekilde bağlantı yollarında açık-devre veya kısa-devre oluşturmak suretiyle müdahale edilerek saldırı düzenlenebilmektedir. Bu saldırı türü genellikle lazer istasyonlar yardımıyla yapılmaktadır. Nitelikli hatalar yaptırılarak gizli anahtar bilgisine ulaşılmaya çalışılır. Yongaya hata yaptırmak veya kartın anormal davranmasına neden olmak bazen saldırganın güvenlik engellerini aşmasında veya gizli bilgiye erişimde yardımcı olacak ilave bir bilgiye ulaşmaya yardımcı olabilir.

### ***Ölçüm saldırıları***

Saldırgan cihaz içerisindeki bellek bölgelerine mikroprob analiz yöntemiyle erişip okuyarak veya veri iletim hatlarını gözleyerek doğrudan gizli bilgiye erişmeye çalışır.

#### **2.5.4.2. Pasif saldırılar**

Pasif saldırılarda cihazın çalışmasına müdahale edilmez. Saldırıcıyı yapan kişi kriptografik sistemin standart işlevlerini kullanır. Bu işlemler sırasında devreden alınan fiziksel ya da elektriksel davranışları saldırı için kullanır. Bu davranışlar istemsiz sızan davranışlardır ve gizli anahtar ile ilgili bilgi verebilirler. Yayıdıkları yan kanal bilgisine göre pasif saldırılar da gruplara ayrılır: Zamanlama Analizi Saldırıları, Güç Analizi Saldırıları, Elektromanyetik Analiz Saldırıları ve Akustik Analiz Saldırıları. Kart sahibinin saldırıcıyı fark etmesi mümkün olmadığından aktif saldırılara göre daha tehlikelidir. Bu tip saldırıları gerçekleştirmek için hem yazılım hem de işlemci hakkında detaylı bilgiye sahip olmak gerekmektedir.

### ***Zamanlama analizi saldırıları***

Kripto sistemler önbellek işlemleri, sabit bir zaman almayan komutların yürütülmesi, dallanmalar ve şartlı komutlar gibi faktörlerden dolayı, farklı girişleri işlemek için farklı

zaman harcarlar. Bu saldırıya zamanlama bilgisini kullanarak algoritmada yürütülen işlemi tespit edebilme olanağı sağlamaktadır. Örnek olarak, RSA algoritmasında gizli anahtar işleminde  $R = y^x \text{mod} n$  hesaplanmaktadır. Bu ifadede  $n$  açık anahtar,  $y$  ise bulunabilen bir değerdir. Saldırının hedefi  $x'$  i bulmaktır. Bu noktada, Kocher zamanlama analizi saldırıları üzerine yaptığı çalışmada [13] basit modülo üs alıcılarının kriptanalizini tanımlamaktadır. Aşağıda  $R = y^x \text{mod} n$  değerini hesaplayan modülo üs alma algoritması verilmektedir.

$$S_0 = 1$$

$0 \leq k \leq w - 1$  için;

Eğer  $x_k = 1$  ise ;

$$R_k = (S_k * y) \text{mod} n$$

Değilse,

$$R_k = S_k$$

$$S_{k+1} = R_k^2 \text{mod} n$$

$$\text{Sonuç} = R_{w-1}$$

Burada  $x$ ,  $w$ -bit uzunluğundadır. Kocher'in önerdiği saldırıda  $y^x \text{mod} n$  değeri, farklı  $k$  adet değer için hesaplatılır ve kaydedilir. İşlemlerin süresi, saldırgan tarafından, girişlerin hedeflenen cihaza ulaşmasıyla çıkışın üretilmesi arasında geçen zamana bakarak ölçülebilir.

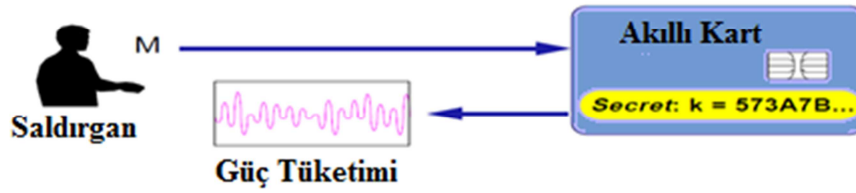
Önerilen saldırıya göre üssün ilk  $(b-1)$ . biti  $(0,1,\dots,b-1)$  biliniyorsa,  $b$ . bit bulunabilir. İlk  $b$  bitin değeri bilindiği için,  $S_b$  değerini hesaplamak için algoritmanın ilk  $b$  döngüsü hesaplanır. Sonraki adımda ilk bilinmeyen bit hesaplanır. Eğer bu bit  $1$  ise  $R_b$  hesaplanır, eğer  $0$  ise bu işlem atlanır. Saldırı bu dallanmadan faydalanır. Eğer  $R_b$  hesaplanırken, döngü için toplam modülo üs alma işlemi daha hızlı olması  $b$  bitinin değerinin  $0$  olduğu

anlamına gelmektedir. Böylece her iki başlangıç değerinden birisi kullanılarak anahtarın tüm bitleri bulunur.

Zamanlama saldırısı kartın algoritmayı yürüttüğü zaman bilgisinin gizli anahtar bilgisine bağlı olduğu durumlarda geçerlidir. Algoritma sürecindeki küçük zaman değişikliklerinin (saat darbe sayısı gibi) ölçülüp analiz edilmesiyle saldırgan gizli bilgi hakkında bilgi edinebilir. Zamanlama saldırılarında sabit veri işleme zamanına sahip olmayan algoritmaların sızdırdığı yan kanal bilgisinden faydalanılır. Yan kanal bilgisinin bir saldırı kaynağı olmasının sebebi, algoritmada yürütülen adımlardan birinde işlem süresinin gizli anahtara bağlı olmasıdır. Bu saldırı tekniği özellikle asimetrik anahtarlı algoritmalar için geçerlidir. Simetrik anahtarlı algoritmaların zamanlama karakteristikleri gizli anahtara o kadar bağlı olmadığı için zamanlama saldırılarına karşı daha güçlüdürler.

### ***Güç analizi saldırıları***

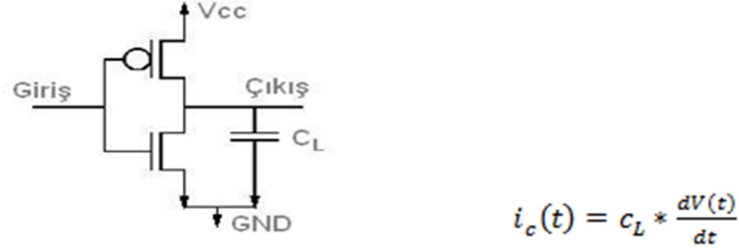
Modern kriptografik cihazlar, transistörlerin oluşturduğu yarı iletken mantık kapılarından meydana gelmektedir. Cihaz kriptografik algoritmayı yürüttüğü sırada, bu kapılarda güç tüketimi ve manyetik yayınımlar oluşur. Güç analizi saldırıları, kartın algoritmayı yürüttüğü sırada tükettiği güç miktarının analiziyle, sızdırdığı bilgi arasındaki korelasyonu kullanmaktadır.



Şekil 2.23 Akıllı kart güç tüketimi

Akıllı kartlar gibi tüm devre tasarımlarında da en yaygın kullanılan teknoloji metal oksitli yarı iletken transistörlerdir (CMOS: complementary metal oxide semiconductor). Bu teknolojinin çekirdek donanımı olan transistörlerin geçitinde (gate) oluşan gerilim

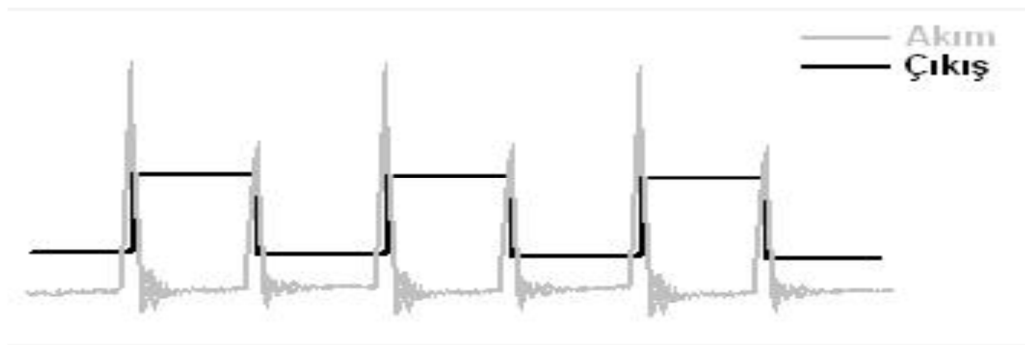
farklılıkları üzerlerinden akım geçmesini sağlar. Böylelikle transistörlerin üzerinde güç tüketimi olur ve bir elektromanyetik alan oluşur. CMOS transistörlerin oluşturduğu lojik kapılarda en fazla güç tüketimi durum geçişlerinde olmaktadır. Şekil 2.24' de görüldüğü üzere transistörün sürdüğü yük kapasitesinin akımı ( $C_L$  üzerinden geçen akım), üzerindeki gerilimin değişimine bağlıdır.



Şekil 2.24 CMOS devresinde güç tüketimi

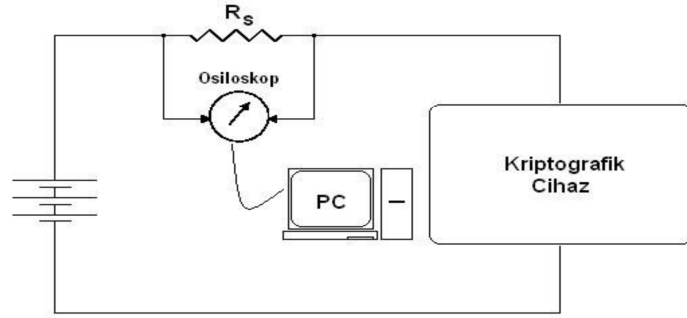
Akıllı kart kriptografik algoritmayı yürütürken, elde edilen güç eğrisinden işlenen '1' lerin sayısı (Hamming Weight) ya da durum geçiş sayısı (Hamming Distance) elde edilerek, algoritma hakkında ayrıntıya ulaşmak mümkün olabilir.

Şekil 2.25' de 0-1 geçişlerindeki tüketilen güç miktarının, 1-0 geçişlerinde tüketilen güç miktarına oranla daha yüksek olduğu görülmektedir. Bir lojik kapının güç tüketimi giriş değerleriyle doğrudan ilişkilendirilebilir. Bu nedenle CMOS kapıların güç tüketimi, kapı girişleri gizli bilgiye bağlı ise yan kanal bilgisi olarak kullanılabilir. Farklı işlemlerin farklı güç tüketim karakteristiğine sahip olması, ayırt edicilik sağlamasından dolayı saldırının başarısını artırır.



Şekil 2.25 CMOS kapısının durum değiştirmesi sırasında çektiği akım(Ordu 1999)

Kriptografik algoritmanın yürütüldüğü esnada cihazın tükettiği güç miktarı, hedef tümleşik devrenin toprak ile arasına yerleştirilen bir direnç yardımıyla ölçülür. Akıllı kart devresi plastik bir kılıfla kaplandığından ölçüm yapılabilecek herhangi bir elektriksel bağlantı yoktur. Bu nedenle direk yonga üzerinden güç tüketimini ölçmek zordur. Kriptografik bir cihaz üzerindeki güç tüketimini ölçmek amacıyla devre ile kaynak arasına yerleştirilen küçük değerli bir direncin(örneğin 50 ohm) her iki ucundaki gerilimlerin farkından yararlanılarak çekilen akım elde edilir.



Şekil 2.26 Güç tüketimi ölçüm devre düzeni

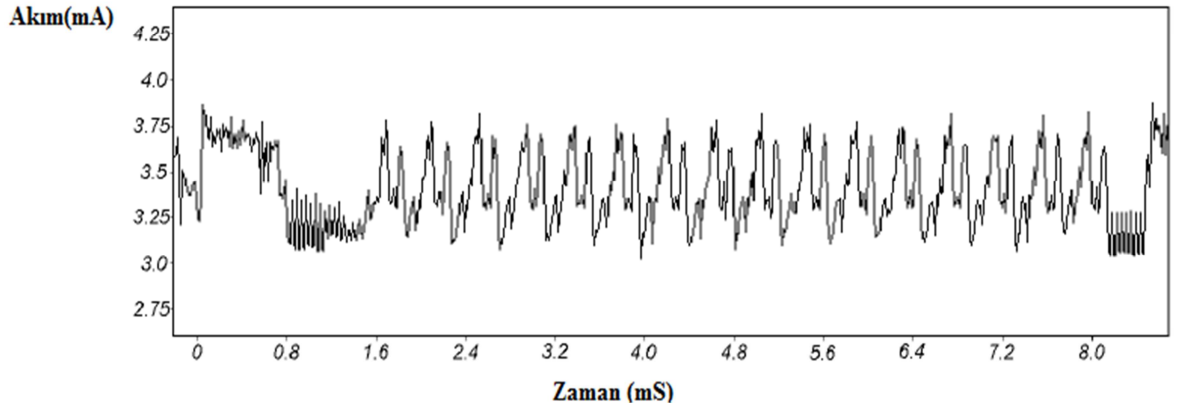
Güç analizi saldırıları, ilk olarak Paul Kocher tarafından 1998 yılında kriptoloji cihazının güç tüketimini bilgi kanalı gibi kullanmak amaçlı bir yöntem olarak tanıtılmıştır. Güç analizi saldırıları farksal güç analizi ve basit güç analizi olmak üzere ikiye ayrılmaktadır.

### Basit güç analizi saldırıları

Basit güç analizi ilk geliştirilmiş ancak en zayıf saldırı tekniğidir. Kriptografik işlemler süresince elde edilen güç tüketim değerlerini doğrudan yorumlayarak gerçekleştirilmektedir. Yürütülmekte olan işlemle tüketilen güç arasında ilişki kurularak gizli bilgiye ulaşılmaya çalışılmaktadır. Örneğin, bütünleşmiş devreler çapma ve toplama gibi işlemler yürütürken farklı miktarlarda güç tüketirler. Bu farklılıkları genelde bir koddaki dallanmalar oluşturmaktadır. DES, AES veya RSA işlemleri gibi büyük algoritma blokları, bu blokların adımlarının gerçekleştirilmesi sırasında, yürütülen farklı işlemlerde tüketilen gücün de farklılık göstermesi sebebiyle, güç tüketimleri kolaylıkla gözlemlenebilmektedir.

Mesages' a göre veri hattındaki aktiviteden oluşan iki tip bilgi mevcuttur: Hamming ağırlık bilgisi ve Hamming uzaklığı bilgisi. Hamming ağırlık bilgisi, veri içerisindeki '1' bitlerinin sayısını ifade etmektedir. Hamming uzaklığı ise, verideki 1-0 ve 0-1 durum geçişlerinin sayısını ifade etmektedir.

Basit güç analizi saldırısını ilk olarak uygulayan Kocher, Jaffe ve Jun, DES in kriptografik işlemi süresince alınan güç tüketim ölçümlerinden alınan değerlerin oluşturduğu güç ölçüm değerlerinde DES in 16 döngüsünü netlikle gözlemişlerdir. Şekil 3.10' da DES algoritmasının yürütüldüğü bir akıllı karta ait güç tüketim ölçümü görülmektedir.



Şekil 2.27 DES turlarını gösteren güç ölçümü

Basit güç analizi tek bir güç ölçümünden yorumlanabilmektedir. Genelde bu tek bir ölçüm yerine, ölçme gürültüsünü düşürmek nedeniyle birkaç ölçüm değerinin ortalaması da kullanılabilir. Bu yaklaşımın başarısı ve bu saldırıda kullanılan teknikler, kriptografik algoritmanın uygulamasına ve algoritmada kullanılan işlemlere bağlıdır. Bir basit güç analizi saldırısı yürütülen işlemler dizisini açığa çıkarabilir ve bundan dolayı işlenen verinin gizli bilgiye bağlı olduğu kriptografik bir algoritmanın kırılmasında kullanılabilir. Bu bölümde Kocher in saldırılarda önerdiği zayıf noktalardan bahsedilecektir.



*DES anahtar planlama:* DES anahtar planlaması dönüşümlü 28 bit anahtarı kapsamaktadır. Rotasyonlar genellikle bir bit kaydırarak ve “0” eklenerek yapılır. Eğer kaydırılan bit “1” ise o halde eklenen “0” evrilir. Bu şartlı işlem tüketilen güç adımlarında gözlenebilir.”1”ve “0” bitlerinin farklı karakteristiklere sahip olacağı gözlemlenebildiğinden, güç eğrisinde ayırt edilebilmektedir.

*DES permutasyonu:* DES uygulamaları bit permutasyonlarını içermektedir. Yazılımdaki şartlı dallanmalar, “1” ve “0” bitleri için ayırt edilebilir güç tüketim farklarına neden olmaktadır.

*Karşılaştırmalar:* Hafıza veya dizgi karşılaştırma işlemleri yürütülürken, bir uyumsuzluk yakalandığında şartlı dallanma gerçekleşmektedir. Basit güç analizi ve zamanlama zayıflıklarına neden olabilmektedir.

*Çoğaltıcılar:* Modüler çoğalma devreleri işledikleri veri hakkında birçok bilgiyi sızdırmaya eğilimlidirler. Bu sızıntının niteliği, çoğaltıcının tasarımına bağlı olarak farklılık göstermektedir. Fakat zayıflıklar genellikle değişkenler ve Hamming ağırlıklarıyla ilişkilidir.

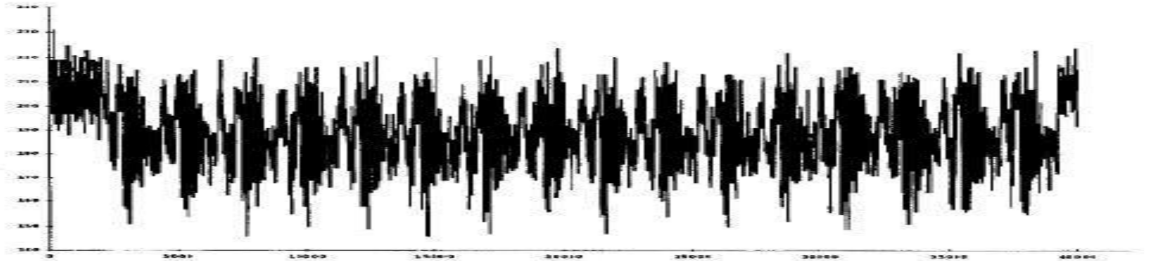
*Üs Alıcılar:* Basit bir modülo üs alma fonksiyonu her bir iterasyonda kare alma işlemi ve ek olarak üssün her bir 1 bit değeri için ek çoğullama işlemi uygulayarak katsayıyı soldan sağa taramak için kullanılmaktadırlar. Eğer kare alma ve çarpma işlemleri farklı güç işaretlerine sahip ise, üs alma işlemi güç analizi bakımından bilgi sızdırabilir. Zamanlama için de aynı analiz geçerlidir.

Güç tüketiminin kriptografik cihazda yürütülen işlemlerle arasındaki korelasyonunu kullanmanın yanı sıra basit güç analizi, güç tüketimi ile işlenmiş veri arasındaki korelasyonu da kullanabilir. Güç tüketimi genellikle işlenmiş verinin Hamming ağırlığı ile ilişkilidir. Hamming ağırlığı binary verideki “1” lerin sayısını temsil eder. Bu tip korelasyon güç tüketiminin, “1” lerin değişimine bağlı olarak değiştiği durumlarda ortaya çıkar.

Tipik bir akıllı kart mikroişlemcisinde, güç yitiminin büyük kısmı iç veri yoluna bağlı kapılarda oluşmaktadır. Messerges’in makalesinde belirttiğine göre veri ve adres hatlarındaki etkinlik, güç tüketiminin en baskın nedenidir .

## Farksal güç analizi saldırıları

Farksal güç analizi saldırıları prensipte basit güç analizine dayalı olan ancak kıyasla daha güçlü olan saldırı çeşitleridir. Kocher'in araştırmasına göre farksal güç analizi saldırısı en çok tehdit eden saldırı şeklidir. Bunun en önemli sebebi saldırıyı uygulamak için saldırganın uygulanan algoritma hakkında çok detaylı bir bilgi bilmesine gerek yoktur. Bu saldırıda gizli anahtarın açığa çıkarılması hata düzeltme algoritmaları ve istatistiksel analiz tekniklerine dayanır. Ortalama tüketimin iki serisi üzerindeki farklılıklar hesaplanır ve alışık olmayan bir durum ortaya çıkarsa o zaman anahtar bitler buradaki farklılıklardan yola çıkarak bulunabilir. Beklenti dışı oluşan bu durumun nedeni veri değerleriyle oynanması olabilir. Sonuca ulaşmak için istatistiksel fonksiyonlar kullanılır. Asimetrik işlemlerden sızan işaretler simetrik işlemlerden sızan işaretlerden daha güçlüdür. Sebebi; asimetrik işlemlerde kullanılan çarpma işlemlerinin karışık işlemler olmasıdır.



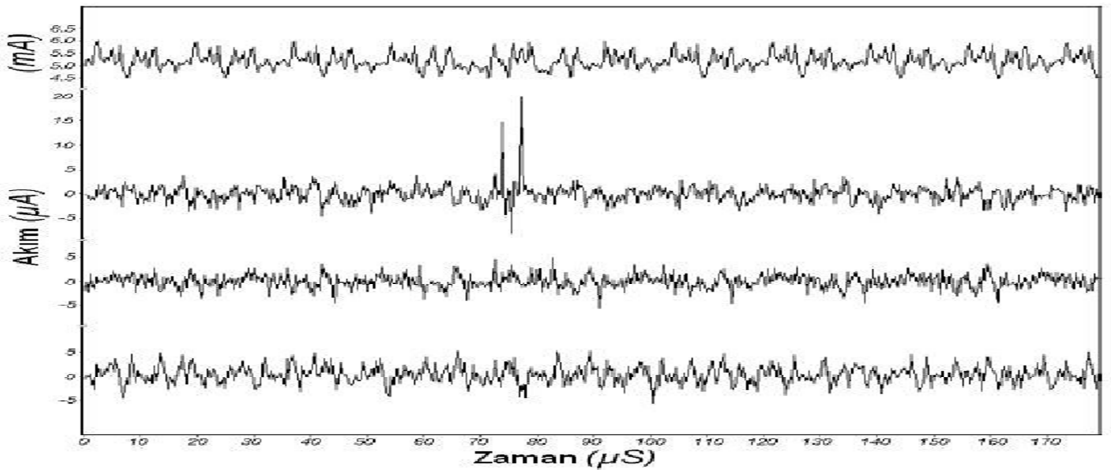
Şekil 2.28 Akıllı kartın güç tüketimi

Kriptografik algoritmanın yürütüldüğü bir cihaza farksal güç analizi saldırısı uygulamak için birkaç güç tüketim eğrisi elde edilir. Bu eğrilerin gizli anahtar hakkında, istatistiksel yöntemlerle ulaşılabilecek bilgiyi içermesi gerekmektedir. Farksal güç analizi saldırıları için öngörülen varsayım, algoritmanın işlediği sürece var olan bir ara değişkenin olduğu ve bu ara değişkenin değerinin gizli anahtarın kolay erişilebilir altkümelerine ve bilinen şifreli/deşifreli metne bağlı olmasıdır. Bu durumda ilgili anahtar bitleri, seçilen ara değere göre güç eğrisini parçalara ayırarak ve hesaplanmış ortalama eğrileri karşılaştırarak yeniden yapılandırılabilir. İki ortalama eğrisi arasında bir veya daha fazla

noktada farklılık varsa, bu saldırının başarılı olduğunu gösterir. Birçok algoritmanın öngörülen varsayıma uygun olması, bu saldırının da güç olmasını kılar.

Bir farksal güç analizi saldırısının detaylarına incek olursak; aynı anahtar ve farklı girişler kullanan bir algoritmanın kullanıldığı kriptografik bir cihazda, toplanan güç ara ölçüm değerleri  $T_1, T_2, T_3, \dots, T_n$  olarak ifade edilsin. Her bir ara ölçüm değeri  $k$  sayıda güç tüketim ölçümlerinin bir dizilimidir ve her bir kriptografik işlem boyunca tüketilen gücü temsil eder. Genel varsayım ; güç tüketimi hesaplanan özel bitin ( $b$ ) 1 ya da 0 olmasına bağlı olarak farklılık gösterir. Bu özel bit ( $b$ ), şifreye bağlı olan bir seçme fonksiyonu ( $D$ ) tarafından belirlenir. Kocher, DES algoritmasının daha yaygın kullanımından dolayı bu algoritma üzerinde çalışmıştır. Önceden bahsedildiği gibi, DES algoritmasında her 16 döngüde bir 8 adet S-Kutusu işlemi uygulanır. Her bir S-Kutusu 6 bit girişe karşılık 4 bit veri üretir. DES algoritması ile ilgili bölüm 2.4.1' de detaylı bilgi yer almaktadır.

Şekil 2.29' da yapılan üç farklı anahtar tahmini için  $\Delta(j)$  değerlerinin grafikleri verilmiştir [32]. En üstteki DES turu ortalama güç eğrisine aittir. İkinci grafik doğru anahtar ( $K_s$ ) tahmini için elde edilen farksal güç ölçümünü göstermektedir. Son iki grafik ise yanlış anahtar tahminleri için elde edilmiş farksal ölçüm değeri grafiklerini göstermektedir.



Şekil 2.29 Farksal güç analizi (Kocher 1996)

Eğer saldırgan, şifresiz metin ile ilgili bilgiye sahipse seçme fonksiyonu ( $D$ ),  $R_1$  registerının ilk biti olarak belirlenebilir:

$$R_1 = L_0 \oplus F(R_0, K_1) \quad (2.5)$$

Bu ifadede;

$R_1$ - ilk dönüşüm döngüsünün sonuçlarının en sağdaki 32 bitini içeren register

$L_0$ -şifresiz metnin başlangıç permutasyonunun sonuçlarının en soldaki 32 bitini içeren register (saldırgan tarafından bilinen değer )

$R_0$ -şifresiz metnin başlangıç permutasyonu sonuçlarının en sağdaki 32 bitini içeren register(saldırgan tarafından bilinen bir değer)

$K_1$ -ilk döngü anahtarı

F-döngü fonksiyonu anlamına gelir.

Yukarıdaki eşitlikte bilinmeyen tek değer  $K_1$  döngü anahtarının değeridir. Döngü fonksiyonu ve S-kutularının uygulamalarından hareketle,  $R_1$  in ilk biti  $K_1$  in sadece 6 bitinden etkilenir. Saldırgan bu bitleri bilemez ancak  $2^6$  olasılığın arasından kaba kuvvet arama (brute force search) yöntemiyle bu değerlere ulaşabilir.

Genel bir ifade ile her bir anahtar tahmini için( $K_s$ ) ,kriptografik işlem süresince  $D$  fonksiyonunu kullanılarak hesaplanan  $b$  bitinin ara değerine göre güç tüketim eğrileri aşağıdaki gibi iki gruba ayrılır :  $T_0$  ve  $T_1$  güç tüketim eğrilerinin iki bölümünü temsil etsin;

$$T_0 = \{T_i : b = 0\}$$

$$T_1 = \{T_i : b = 1\}$$

Ara ölçüm değerlerinin ortalaması  $j=1, \dots, k$  ve  $|T_0| + |T_1| = n$  için aşağıdaki gibi hesaplanır :

$$A_0[j] = \frac{1}{|T_0|} \sum_{T_i \in T_0} T_i[j] \quad (2.6)$$

$$A_1[j] = \frac{1}{|T_1|} \sum_{T_i \in T_1} T_i[j] \quad (2.7)$$

Sonraki adımda saldırgan farksal gücü ( $\Delta$ ) hesaplar:

$$\Delta[j] = A_1[j] - A_0[j] \quad (2.8)$$

Eğer  $K_s$  anahtarı yanlış tahmin edildiyse, D fonksiyonu kullanılarak hesaplanan bit şifresiz metnin yarısı için gerçek hedef bitten farklı olacaktır. Bu nedenle seçme fonksiyonu, cihazda fiilen neyin hesaplandığı ile bağlantılı değildir. Bu durumda D fonksiyonu tüm güç örnekleri serisini iki alt gruba bölmek için kullanılan bir fonksiyondur ve :

$$\lim_{n \rightarrow \infty} \Delta(j) = 0$$

şeklinde dir. Uygulamada bu farksal güç ölçümü tamamen yatay olmayabilir. Hatta doğru anahtar tahmini için güç ölçümü ile çok ince bir ilişki olabilir.

Diğer taraftan eğer anahtar tahmini doğru olsaydı, seçme fonksiyonunun değeri kriptografik cihazda hesaplanan değer ile eşit olmalıydı. Bu nedenle seçme fonksiyonu ile cihazda kurcalanan değer ve güç tüketimi arasında bir ilişki vardır. Eğer  $b$  biti  $j'$  anlarında kurcalanırsa, o zaman güç için beklenen fark aşağıdaki şekilde olmalıdır :

$$E[T_i[j']|b = 1] - E[T_i[j']|b = 0] = \varepsilon > 0 \quad (2.9)$$

$j \neq j'$  olduğu zaman, güç kaybı  $b$  bitinin değerinden bağımsızdır. Yukarıdaki eşitlikte verilen fark "0" olmalıdır:

$$E[T_i[j]|b = 1] - E[T_i[j]|b = 0] = 0, \forall j \neq j' \quad (2.10)$$

Güç ölçümlerinin sayısı arttığından,  $A_1[j]$  ve  $A_0[j]$  değerleri sırasıyla  $E[T_i[j]|b = 1]$  ve  $E[T_i[j]|b = 0]$  ifadelerine yakınsar. Yukarıdaki eşitliklere göre:

$$\lim_{n \rightarrow \infty} \Delta[j] = \lim_{n \rightarrow \infty} (A_1[j] - A_0[j]) = \begin{cases} \varepsilon, & j = j' \\ 0, & j \neq j' \end{cases} \quad (2.11)$$

2.9 ve 2.11 denklemlerine göre; eğer yeterli şifresiz metin örnekleri kullanılırsa,  $j'$  zamanında  $\Delta[j]$  farksal gücü  $\varepsilon$  kadar bir sapma gösterir ve diğer tüm zamanlarda “0” olur. S-Kutusu çıkışlarındaki küçük istatistiksel sapmalar olmasından dolayı, 3 numaralı denklem tamamıyla doğru değildir ve uygulamada  $\Delta[j]$  hiçbir zaman “0” olmayacaktır. Fakat  $j'$  zamanında daha büyük sapma oluşacaktır. Eğer kriptografik işlem için kullanılan anahtar doğru ise, kurcalanan bit değerinin seçme fonksiyonu ile ilişkisi olduğu bir yerde sapma ortaya çıkacaktır.

Özetle bir farksal güç analizi şu şekilde gelişir; her bir tahmin için saldırgan güç ölçümleri ve yeni bir farksal ölçüm ( $\Delta[j]$ ) için yeni bir bölüntü yapılandırır. Eğer uygun seçme fonksiyonu seçildiyse, fonksiyon tarafından tanımlanan bit kurcalandığında farksal ölçüm sapmalar gösterir. Bu yöntemle saldırgan ilk döngü anahtarının ( $K_1$ ) 6 bitini belirleyebilir. Bu yaklaşımın diğer 7 tane S-kutusu için uygulanmasıyla saldırgan ilk döngü anahtarının tüm 48 bitini öğrenebilir. DES anahtarının kalan 8 biti kaba kuvvet (brute force) saldırılarıyla keşfedilebilir.

Saldırı DES kriptolamasının son döngüsünde de uygulanabilir. Bu saldırı ilk döngüye uygulanan saldırıya benzer ancak bu sefer saldırgan şifreli metni bilmelidir. Son döngü saldırısında seçme fonksiyonu,  $L_{15}$  registerının ilk biti larak tanımlanabilir ve aşağıdaki gibi hesaplanır:

$$R_{16} = L_{15} \oplus F(R_{15}, K_{16}) \quad (2.12)$$

$$L_{16} = R_{15} \quad (2.13)$$

Buradan,

$$R_{16} = L_{15} \oplus F(L_{16}, K_{16}) \quad (2.14)$$

$$L_{15} = R_{16} \oplus F(L_{16}, K_{16}) \quad (2.15)$$

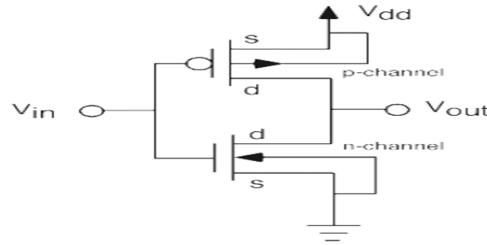
elde edilir. Yukarıda F fonksiyonunun seçilme sebebi, DES şifrelemesi süresince bazı noktalarda belirtilen bitin hesaplanması gerekliliğinden doğmaktadır. Böyle bir durum olduğunda, tüketilen güç miktarında bu bitin “0” ya da “1” e eşit olmasına göre farklılık olacaktır.

Farksal güç analizi kurcalanan veri ile yan kanal uygulaması arasındaki ilişkiyi saptamaktadır. Bu analizin diğer bir özelliği ise uygulanan algoritma ile ilgili çok detaylı bilgiye sahip olmayı gerektirmemesidir.

### **Elektromanyetik analiz saldırıları**

Farksal güç analizine çok benzer. Kart çalışırken sızdırdığı elektromanyetik yayını kullanır. Genelde Farksal Elektromanyetik Analizi (DEMA) olarak adlandırılır. Çipe çok yakın bir şekilde konumlandırılan yakın-alan problemleri yardımıyla ölçülebilir.

Önceki bölümlerde de değinildiği gibi yan kanal bilgi sızıntısının sebebi, akıllı kartın yapısında kullanılan CMOS teknolojisidir. Kartın yongasında çok sayıda transistörden oluşan kapılar bulunmaktadır.



Şekil 2.30 CMOS evirici

Şekildeki evirici bir açma kapama anahtarı olarak düşünülebilir. Yüksek giriş, toprak seviyesinde çıkış verir. Bir bit seviye değiştiğinde, cihazın *n* ve *p* transistörleri anlık olarak *açık* konuma geçerler. Bu durumda güç tüketiminde anlık değişimler gözlenir. Oluşan bu anlık akım darbeleri elektromanyetik yayınımda da değişikliklere neden olur.

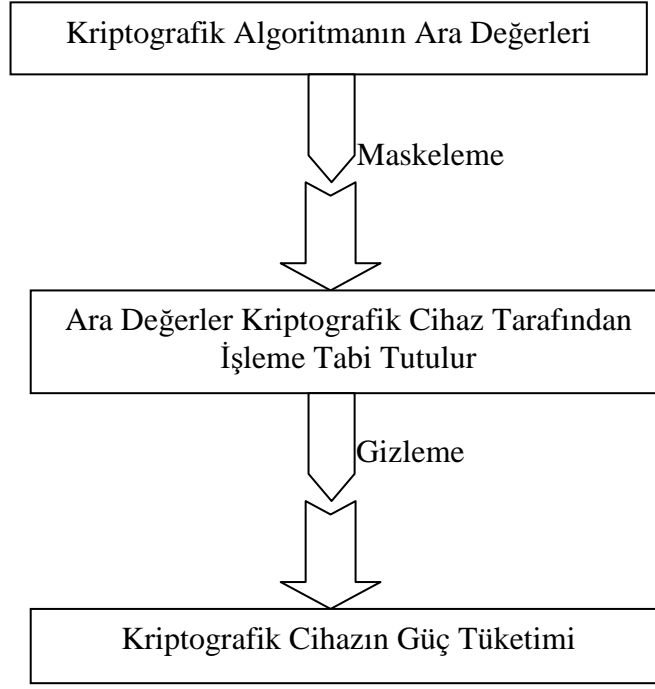
## 2.6. Karşı Tedbir Yöntemleri

Bu bölümde, daha büyük risk taşınması bakımından, özellikle pasif yan kanal analizi saldırılarına karşı tedbir yöntemlerinden bahsedilecektir. Daemen ve Rijmen, algoritmanın yürütüldüğü sırada sızan zamanlama bilgisi üzerine çalışmışlardır. Bu çalışmada sızan zaman bilgisinin gizleme anahtarından bağımsız olmasını sağlayarak, kriptografik uygulamalarını zamanlama saldırılarına karşı korumayı önermişlerdir. gerek duyulan yerlere işlevsiz kodlar ( NOP= No Operation) getirilerek bu tüm işlemlerin aynı zamanı alması sağlanabilir. Zamanlama saldırılarını önlemek için önerilen bir diğer yaklaşım da uygulamaya rastgele gecikmeler eklemektir. Böylece zaman bilgisine hiçbir zaman sağlıklı bir şekilde ulaşamayacaktır.

Kocher zamanlama analizi saldırılarına karşı tedbir olarak kör imza uygulaması için kullanılan tekniklere dayanan bir yöntem tanımlanmaktadır. Bu çalışmadaki yaklaşıma göre, rastgele bir  $(v_i, v_f)$  çifti seçilir. Bu çiftin arasında  $v_f^{-1} = v_i^x \text{mod} n$  ilişkisi bulunmaktadır. Modülo üs alma işleminden önce, giriş mesajı  $v_i(\text{mod} n)$  ile çarpılır. Daha sonra tekrar  $v_f(\text{mod} n)$  ile çarpılarak düzeltilir. Rastgele seçilen çiftler saldırı riskine karşılık yeniden kullanılmamalıdır. Her bir modülo üs alma adımına başlamadan önce  $v_i$  ve  $v_f$  değerlerinin güncellenmesi gerekmektedir. Sonuç olarak, eğer  $(v_i, v_f)$  değerleri gizliyse, saldırganın modülo üs alıcı girişinde faydalı bir bilgiye sahip olması mümkün olmayacaktır.

Güç analizi saldırılarında karşı tedbir yöntemlerinin amacı, kriptografik cihazın güç tüketimini algoritmanın ara değerlerinden bağımsız hale getirmektir. Böylece tüketilen güç miktarının bir anlamı kalmayacaktır. Özellikle farksal güç analizi saldırılarında gizleme ve maskeleyme olmak üzere iki tip karşı tedbir yöntemi kullanılmaktadır.





Şekil 2.31 Gizleme ve maskeleye karşı tedbir yöntemlerinin genel gösterimi

*Gizleme yönteminin* temeli, güç tüketiminin veri bağımlılığını ortadan kaldırmaktır. Bu, algoritmanın uygulamasının rastsallaşması veya cihazın güç tüketim karakteristiklerinin değiştirilmesi anlamına gelir. Güç tüketimi iki yöntemle değiştirilir : kriptografik cihaz her işlem yaklaşık olarak aynı miktarda enerji gerektirecek şekilde ya da güç tüketimi daha rastsal olacak şekilde yapılandırılır. İki durumda da güç tüketimi ile işlenen veri arasındaki ilişki önemli şekilde azalır. Fakat pratikte bu ilişkinin tamamen yok edilmesi mümkün değildir. *Gizleme yöntemi* ile korunan uygulamalarda, korumasız uygulamalarla aynı ara değer sonuçlarının işleme tabi tutulduğuna dikkat edilmelidir. Güç analizi saldırıları, sadece güç tüketim karakteristikleri değiştirilerek önlenir.

*Maskeleye yönteminin* amacı ise, kriptografik cihaz tarafından işlenen ara değerleri rastsallaştırmaktır. Bu adımın arkasındaki yaklaşım, rastsal ara değerlerin işlenmesi için gereken enerjinin gerçek ara değerler için gerekenden bağımsız olmasıdır. Maskeleye yönteminin büyük bir avantajı; cihazın güç tüketim karakteristiklerinin değiştirilmesine gerek yoktur. İşlenen ara değerler rasgele seçilerek maskelendiği için güç tüketimi hala

veriye bağılı olabilir. Bu yaklaşımın avantajı; kriptografik cihazın güç tüketim karakteristiklerini deęiřtirmeden algoritma seviyesinde uygulamasıdır.

Bir maskeleme uygulamasında, her bir ara deęer  $v$ , maske olarak adlandırılan bir  $m$  deęeri tarafından gizli hale getirilir ve  $v_m = v * m$  řeklinde ifade edilir. Maske( $m$ ), kriptografik cihazın ięerisinde üretilir ve uygulamaya göre deęiřiklik gösterir. Bu nedenle saldırgan tarafından bilinmez. Genellikle “\*” iřlemi, kriptografik algoritmada kullanılan iřlemlere göre tanımlanır. Bu nedenle bu iřlem genelde Boolean X-OR fonksiyonu( $\oplus$ ), modüler toplam (+) veya modüler çarpım (x) řeklinde dir. Modüler çarpma ve modüler toplama olması durumunda, katsayı algoritmaya göre seçilir.

Çoęunlukla, maske řifresiz metin ya da anahtara uygulanır. Maskelenmiř ara deęeri iřlemek ve maskelerin izini kaybetmemek ięin algoritmanın uygulanmasında küçük çaplı deęiřiklikler gerekmektedir. Ayrıca veri řifrelemenin sonucu da maskelenir. Bundan dolayı, řifreli metni elde etmek ięin hesaplamaların sonunda maskeler kaldırılmalıdır.

Güvenlik aęısından her ara deęerin maskelenmesi önemlidir. Bu durum ayrıca bir önceki ara deęerlere dayalı olarak hesaplanan ara deęerler ięin de önem tařır. Örneęin iki maskelenmiř deęere XOR fonksiyonu uygulanırsa, sonucun da maskeli olduęuna emin olmalıyız. Bu nedenle, farklı ara deęerler farklı maskeler tarafından gizlenir. Maskelerinin sayısının performansı düşürmesi sebebiyle her bir ara deęer ięin yeni bir maske kullanılması tavsiye edilmez. Sonuç olarak, uygun performans elde etmek ięin

Farksal güç analizi saldırılarına kıyasla basit güç analizi saldırılarını önlemek daha kolaydır. Amaç, her karřı tedbir yönteminde olduęu gibi sızdırılan güç sinyalinin azaltılarak saldırganın uygulama hakkında bilgi almasını önlemektir. Şartlı dallanma iřlemleri ięin gizli anahtar veya ara deęerlerin kullanımının engellenmesiyle her türlü basit güç analizi karakteristięinin maskelenmesi saęlanacaktır. Gizli ara deęer veya anahtar bilgisi kullanılarak yapılan kořullu dallanmalardan sakınılmasıyla da, basit güç analizi karakteristiklerinin birçoęu maskelenebilir. Dallanmaların şart olduęu durumlarda, algoritmanın geręeklenmesi adımı nda güç tüketimini dengeleme yöntemleri kullanılabilir. Bu amaçla güç tüketiminin düşük olduęu dallarda, önceden bahsedildięi

gibi algoritmanın işleyişine etkisi olmayacak gereksiz işlemler eklenebilir. Amaç, tüketilen güç miktarını arttırarak, tüketimin yüksek olduğu dallardan ayırt edilmesini engellemektir.

Diferansiyel güç analizi saldırılarında, güç tüketimiyle işlenen veriler dolayısıyla da gizli bilgiler arasında ilişki kurulur. Bu nedenle, karşı tedbirler gizli bilgiyle güç tüketimi arasındaki ilişkiyi zayıflatmayı veya güç ölçümlerini zorlaştırmayı hedefler.

Elektromanyetik analiz saldırılarına önlem olarak, TEMPEST standartlarına uyulması ve manyetik radyasyonu engelleyici kaplama yapılması, elde edilecek yan-kanal bilgisinin zayıflatılmasını sağlamak için en temel karşı tedbirlerdendir. Ancak cihazın saldırganın eline geçmesi durumunda bu tedbirler, koruyucu yapıların çıkarılmasıyla, etkisiz hale getirilebilir. Bunun dışında, güç analizi saldırıları için yukarıda bahsedilen karşı tedbir yöntemleri, elektromanyetik analiz saldırılarını da önleyici nitelikte olacaktır.

### **2.6.1. Maskelenmiş AES algoritması örneği**

Bu bölümde maskeli AES algoritmasının akıllı kart uygulama örneğinden bahsedilecektir. Sadece Boolean maske kullanılmış ve AES yazılımına uyarlanmıştır. Yöntemde anahtar tablosu da maskelenmiştir. Bu durum, şifreleme işleminin başlangıcında bazı maskelerin şifresiz metin ile bazı diğer maskelerin de ilk döngü anahtarı ile XOR işlemine sokulduğu anlamına gelir.

Aşağıda ilk olarak AES döngü dönüşümünün ilk 4 işleminin nasıl maskelendiği anlatılmaktadır. Daha sonra maskeleme planı tümüyle tarif edilmektedir.

*Tur anahtarı ekleme* : “*k*” döngü anahtar baytları “*m*” ile maskelendiğinden, AddRoundKey adımında “*d*” bilgi baytlarının durumu otomatik olarak maskelenir:

$$d \oplus (k \oplus m) = (d \oplus k) \oplus m$$

Döngü anahtarlarını maskeleme basit güç analizi saldırılarını önlemek açısından önemlidir.

*Yer deęiřtirme:* AES algoritmasındaki doęrusal olmayan tek iřlem yer deęiřtirme iřlemidir. Mikro denetleyici üzerindeki yazılım uygulamalarında, yer deęiřtirme iřlemi genellikle tabloya bařvurma řeklinindedir. Bundan dolayı, bu iřlem iin maskelenmiř bir S-Kutu tablosu kullanılır.

*Satırları kaydırma:* Bu adım baytların durumunu farklı konumlara tařımaktadır. Yöntemde, tüm durum baytları algoritmanın bu adımında aynı maske ile maskelenir. Bu nedenle, algoritmada bu ařama maskelemeyi etkilemez.

*Sütunları karıřtırma:* Bu adım dięerlerine göre daha fazla dikkat gerektirir. ünkü bu ařama bir sütunun farklı sıralarındaki baytları karıřtırır. Bu nedenle, sütunları karıřtırma iřlemi en az iki maskeleme gerektirmektedir. Eęer bir sütunun baytları iin iki maske kullanılmıřsa, o zaman sütunları karıřtırma iřlemi tüm ara deęerlerin maskeli olduęundan her bir sıranın ayrı bir maske ile maskelenmesi daha etkilidir.

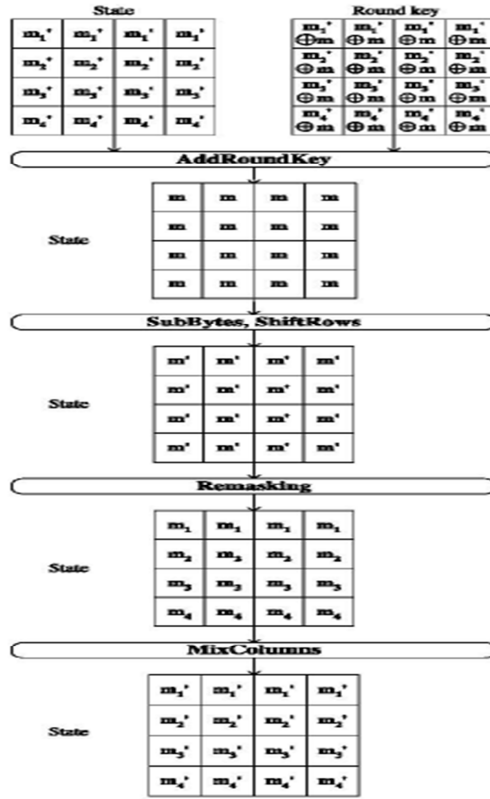
Sonuç olarak örnek AES maskelemesinde, 6 adet baęımsız maske kullanılmaktadır. ilk iki maske ,  $m$  ve  $m'$ , maskelenmiř SubByte iřlemi iin giriř ve ıkıř maskeleridir. Kalan 4 maske;  $m_1, m_2, m_3$  ve  $m_4$ ; sütunları karıřtırma iřleminin giriř maskeleridir. Her bir AES řifrelemesinin bařlangıcında iki adet ön hesaplama yer almaktadır.

İlk olarak S-Kutu tablosuna bařvurularak,  $S_m$ , hesaplanmaktadır:

$$S_m(x \oplus m) = S(x) \oplus m'$$

İkinci olarak, bu iřlem dięer maskelere uygulanarak sütunları karıřtırma iřleminin ıkıř maskeleri hesaplanır. Bu ıkıř maskeleri  $m'_1, m'_2, m'_3, m'_4$  řeklinde gösterilmektedir.

Maskelenmiř bir AES dngüsünde, her bir dngünün bařında řifresiz metin  $m'_1, m'_2, m'_3, m'_4$  ile maskelenir. Sonra dngü anahtarı eklenerek,  $m$  ile maskelenir. Maskeleme iřlemi sonrasında uygulanan  $S_m$  fonksiyonu ile yeni maske ( $m'$ ) bulunur. Satırları kaydırma adımı tüm durum baytları aynı  $m'$  maskesi ile maskelendięi iin etkisiz bir role sahiptir.



Şekil 2.32 AES Maskeleye işlemi gösterimi

Sütun karıştırmadan önce,  $m'$  maskesi, ilk sırada  $m_1$ , ikinci sırada  $m_2$ , üçüncü sırada  $m_3$  ve dördüncü sırada  $m_4$  olarak değişmiştir. En son döngünün bitişinde maskeler çıkarılır.

### 3. MATERYAL VE YÖNTEM

#### 3.1. Materyal

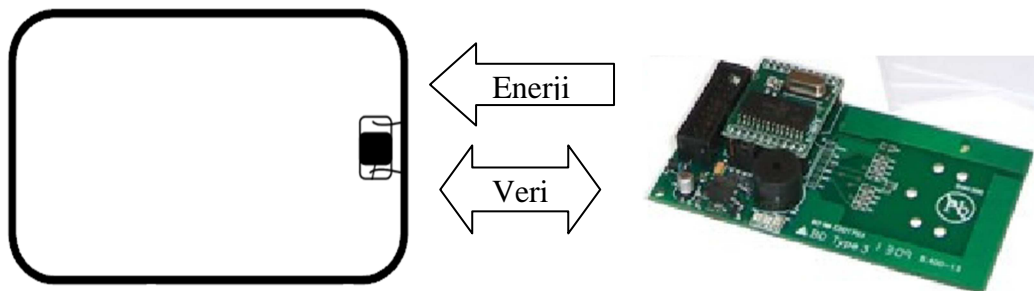
Bu tez çalışmasında uygulamalar için SonMicro firmasından satın alınan SMX-1300 uygulama kiti kullanılmıştır. Bu uygulama kitinin bilgisayar bağlantısı RS32 ile sağlanmaktadır. Kit üzerinde PCB anten, giriş/çıkış pinleri, ikaz LED' leri, I2C ve UART gibi bağlantı pinleri bulunmaktadır. Kitin harici beslemesi 9V adaptör ile sağlanmıştır. Haberleşme hızı olarak 9600bps - 115200bps aralığını destekleyen cihazda, uygulamamız için UART/Seri haberleşmesi 19200bps hızı tercih edilmiştir. Uygulama için gerekli olan yazılım, SDK ve ActiveX komponenti set ile birlikte gelmiştir.

Çalışmada 1K mifare temassız kart kullanılmıştır. Kart üzerindeki bloklara yapılan okuma/yazma gibi işlemlerde sistem davranışı incelenerek yorumlanmıştır.

Kartın okunması sırasında elde edilen işaretlerin gözlemlenmesi Tetronix TDS 220 marka, 100 MHz frekansta çalışan osiloskop kullanılmıştır. Ancak süreç kaydı alabilmek için bu osiloskop yetersiz kaldığından TARGE Elektronik tarafından sağlanan, bilgisayar uyumlu OWON marka osiloskop kullanılmıştır.

##### 3.1.1. Mifare temassız akıllı kartlar

Tez çalışmamız içerisinde mifare temassız kart üzerinde uygulamalar gerçekleştirildiğinden, bu bölümde bu kartlar hakkında detaylı bilgi verilecektir. Mifare temassız akıllı kartlara ISO 14443/IEC A standardı uygulanır.



Şekil 3.1 Mifare temassız akıllı kart

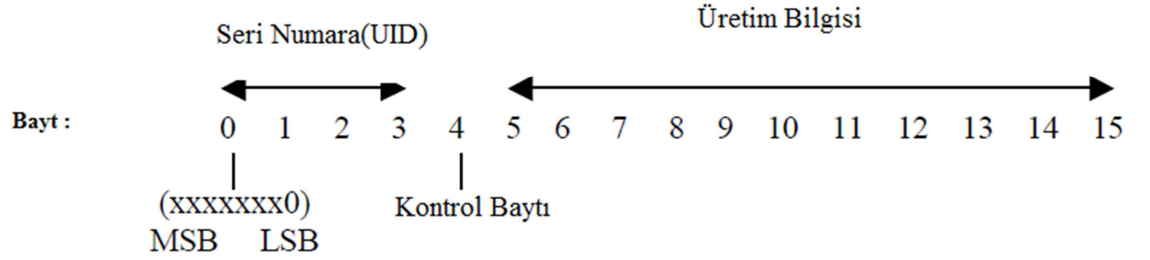
Çalışmalarda kullanılan mifare kart 1K hafızasına sahiptir. Kartın sahip olduğu yonga

1 Kbyte EEPROM, RF ara yüz ve dijital kontrol ünitesinden oluşmaktadır. Haberleşme bu yonga ile bağlantılı birkaç döngüden oluşan bir anten vasıtasıyla sağlanmaktadır.

### ***1K Mifare temassız kart hafıza yapısı***

1K Mifare temassız kartlara ait hafıza yapısının gösterimi şekil 2.5 ' de yer almaktadır. 1024 bayt hafıza 16 adet sektöre ayrılmaktadır. Sektörler, her biri 16 bayt uzunluğunda 4 adet bloktan oluşmaktadır.

İlk sektörde (Sektör 0) bulunan ilk veri bloğu (Blok 0) sadece okunabilir bir alandır ve seri numarası(UID-Unique Identifier) ile üretim bilgileri içermektedir. Bu blok “*üretici blok*” olarak adlandırılmaktadır.

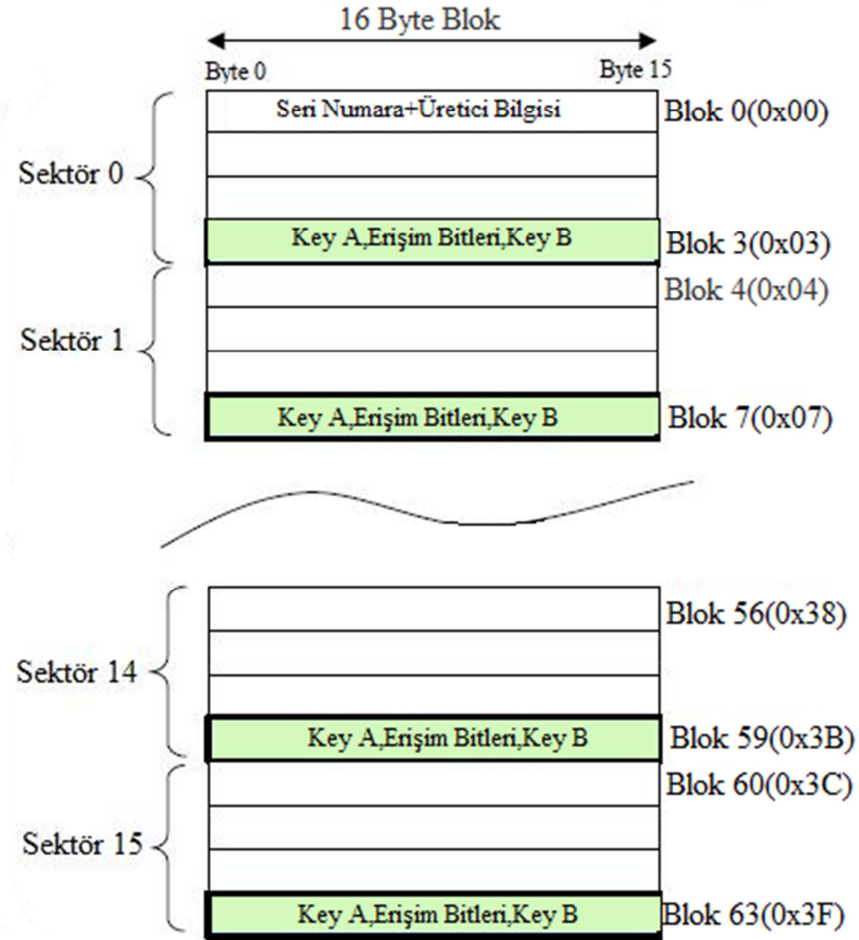


Şekil 3.2 Üretici bloğuna ait gösterim(IB technology 2006)

Her bir sektördeki son blok “*Trailer Bloğu*” olarak adlandırılır ve iki tip anahtar kodu ile (Key A ve Key B) erişim bitlerini içermektedir. Erişim bitleri sektöre nasıl ulaşılabilceğini tanımlamaktadır. Üretici bilgilerinin bulunduğu blok ve trailer bloğu göz önünde bulundurulduğunda 752 bayt hafıza, kullanıcının bilgilerini depolamak için kullanılmaktadır. Mifare kart hafızası onaltılık formattaki blok numarası tarafından adreslenir.

Her bir sektörde iki adet veri bloğu bulunmaktadır. Veri blokları, özel elektronik cüzdan uygulamaları için *değer blokları* olarak veya standart okuma/yazma hafızası olarak düzenlenebilir. Değer blokları, veri alanını kontrol etmek amacıyla “arttır/azalt”

komutlarını kullanabilirler. ayrıca deęer blokları yedek yönetimi ve hata bulma/düzeltilme özelliklerine imkan veren uygun bir veri formatına sahiptirler.



Şekil 3.3 Mifare 1K(1024 bayt) hafıza haritası gösterimi (IB technology 2006)

## 3.2. Yöntem

### 3.2.1. Ortalamaların farkı testi yöntemi

Paul Kocher tarafından kullanılan [4] bu test, iki grubun ortalama deęerler arasındaki farkını hesaplamaktadır. Algoritma N adet gelişigüzel metin için çalıştırılır. Herbir metin için saldırı noktasındaki deęerler tahmin edilir. Bu deęerler bir ayrıştırma



fonksiyonu yardımı ile iki gruba ayrılır. Ortalama değeri hesaplanan bu her iki grubun farkı alınır.

$$\Delta_{D_{oM}}(ks, t) = \overline{P_{0,k}(t)} - \overline{P_{1,k}(t)} \quad (3.1)$$

$P_{0,k}$  ve  $P_{1,k}$  gruplarının tanımı ;  $P_{0,k} = \{P(x_n, t) | D(x_n, b, k) = 0\}$

$$P_{1,k} = \{P(x_n, t) | D(x_n, b, k) = 1\}$$

şeklindedir. Yukarıdaki ifadede bulunan  $D(x_n, b, k)$  için;  $D(x_n, b, k) = d$  olan eş gruplarının sayısı  $n_{d,k}$  olarak tanımlanırsa ifade ;

$$\overline{P_{d,k}(t)} = \frac{1}{n_{d,k}} \sum_{i=1}^{n_{d,k}} P_{x_i, t}$$

(3.2)

olur. Fark işlemi her bir anahtar olasılığı için ayrı ayrı hesaplanır. En yüksek farkın elde edildiği anahtar, kullanılan anahtar bilgisini vermektedir.

### 3.2.2. T-test yöntemi

Bu yöntem Manfred Aigner ve Elisabeth Oswald tarafından bulunmuştur [22]. İki serinin varyansını da içine alan ve önceki bölümde bahsedilen ortalamaların farkı testinin genişletilmiş şeklidir.

$$\Delta_{ks,t} = \frac{\overline{P_{0,k}(t)} - \overline{P_{1,k}(t)}}{S_P} \sqrt{\frac{n_{0,k} \cdot n_{1,k}}{n_{0,k} + n_{1,k}}} \quad (3.3)$$

Bu ifadede  $n_{0,k}$  ve  $n_{1,k}$  eş gruptaki elementlerin sayısını sembolize eder.

$$S_P(k, t) = \sqrt{\frac{(n_{0,k}-1)var_0(k,t) + (n_{1,k}-1)var_1(k,t)}{n_{0,k} + n_{1,k} - 2}} \quad (3.4)$$

Son olarak varyans,

$$var_d(k, t) = \frac{1}{n_{d,k-1}} \sum (P(x_n, t) - \overline{P_{d,k}(t)})^2 \quad (3.5)$$

şeklinde hesaplanır. Bu test, ölçüm sırasında güç tüketim verisinin varyansının farklı noktalarda, önemli derecede değişim göstermesi durumunda tercih edilmektedir.

### 3.2.3. Korelasyon metodu yöntemi

Bu yöntem de çeşitli istatistik kitaplarında yer alan ve yine Manfred Aigner ve Elisabeth Oswald tarafından güç analizi çalışmalarında kullanılan bir yöntemdir.

Korelasyon katsayısı  $c(k, t)$ ,  $t$  zamanında açık metnin( $x_n$ ) bir fonksiyonudur.  $D$  seçme fonksiyonu ile ilişkilidir.  $D(x_n, b, k)$  ifadesinde yer alan  $k$  anahtar varsayımı bu ilişkiyi kurmaktadır.

$$c(k, t) = \frac{\sum_n (D(x_n, b, k) - \overline{D(x_n, b, k)}) (P(x_n, t) - \overline{P(x_n, t)})}{\sqrt{\sum_n (D(x_n, b, k) - \overline{D(x_n, b, k)})^2} \sqrt{\sum_n (P(x_n, t) - \overline{P(x_n, t)})^2}} \quad (3.6)$$

Yukarıdaki ifadede  $P(x_n, t)$  güç tüketim değerlerini sembolize eder. Korelasyon katsayısı, bağımsız değişkenler arasındaki bağlantının büyüklüğünü ve yönünü belirten bir katsayıdır. Korelasyon katsayısı -1 ile +1 arasında bir değer almaktadır. İki işaret arasında herhangi bir ilişki yoksa  $c(k, t) = 0$  olacaktır. Korelasyon katsayı değerinin -1 olması d, anahtar varsayımının doğru olduğu anlamına gelir ancak bu durumda gözlenen bit konumu ile güç tüketimi arasındaki ilişki modeli orantısızdır.

### 3.3. Uygulama Düzenegi

Devrenin elektromanyetik analizini yapmak amacıyla aşağıdaki şekillerde fotoğrafı bulunan 4 adet el yapımı basit anten yapılmıştır. Şekil 3.4, Şekil 3.5 ve Şekil 3.6' da görülen antenler ile ilgili çalışmalarda Dario Carluccio' nun çalışmalarından esinlenilmiş ve bu çalışmalardan yola çıkarak 30 mm iç çapa sahip olan ferrite nüve üzerine sarım yapılarak bir anten oluşturulup, kart okuyucuya gönderilen çeşitli komutlara karşılık oluşan işaretler gözlemlenmiştir. İşaretin sağlıklı gözlenebilmesi için gerekli olan tetikleme, kartın başarılı şekilde doğrulanması durumunda yanıp sönen LED' den sağlanmıştır.

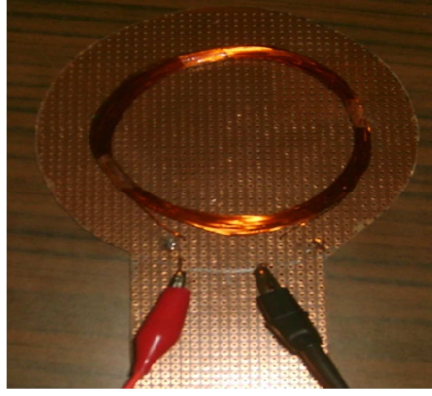
Bu anten tipleri sarım sayısına baęlı olarak alanın manyetik kısmını almaktadırlar ve manyetik alan yuvarlak tarafından kapsanan alandan geçmektedir. Çevrelenmiş alan üzerindeki manyetik alanın  $H(r)$  sarım sayısı ile çarpımı, sonucu dâhil edilerek hesaplanabilir. Alınan güç daha büyük çaplar ve daha fazla sarıma baęlı olarak artacaktır.



Şekil 3.4 Anten 1 (  $n=400$ ,  $r=3\text{mm}$ ) (Carluccio 2005)



Şekil 3.5 Anten 2 (  $n=800$ ,  $r = 3\text{mm}$ ) (Carluccio 2005)

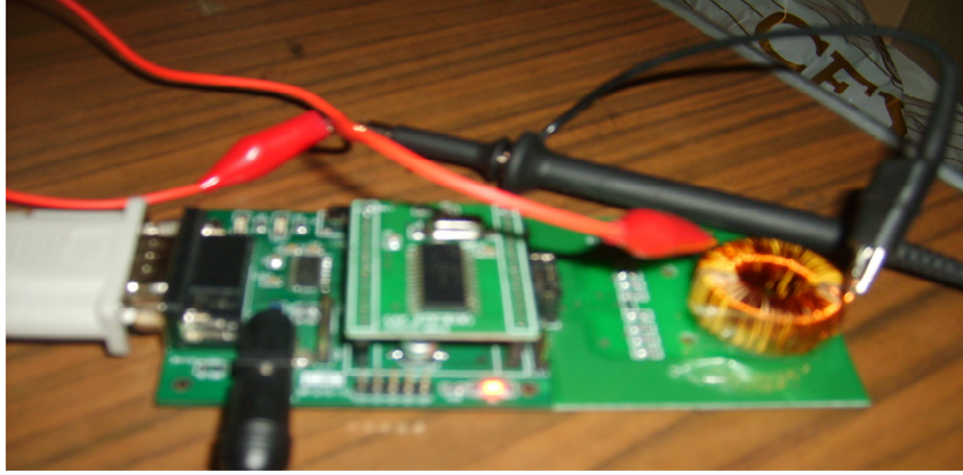


Şekil 3.6 Anten 3 (n=50, r=35mm)

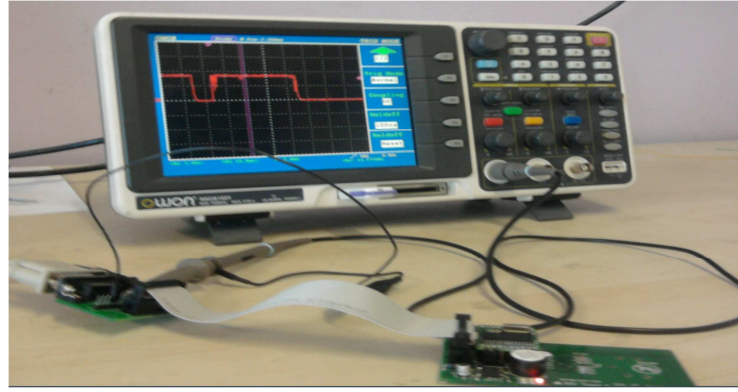


Şekil 3.7 Anten 4 (Ferrite nüve, n=100)

Şekil 3.7' de ferrite nüve sarım uçlarından elde edilen işaretin gözlenmesi için kurulmuş devre düzeneği görülmektedir. Amaç, veri alışverişinin süregeldiği zaman aralığında toroid üzerinde indüklenen gerilimde oluşan değişiklikleri gözlemleyebilmektir. Ölçümlerin, cihazın gözlemlenen işlemi hesapladığı zaman noktasının her ölçümün aynı örnekleme noktası  $P(x_n, t_0)$  olacak biçimde eş zamanlı olarak gerçekleşmesi esastır.



Şekil 3.8 Devre düzeneğinden bir görünüm

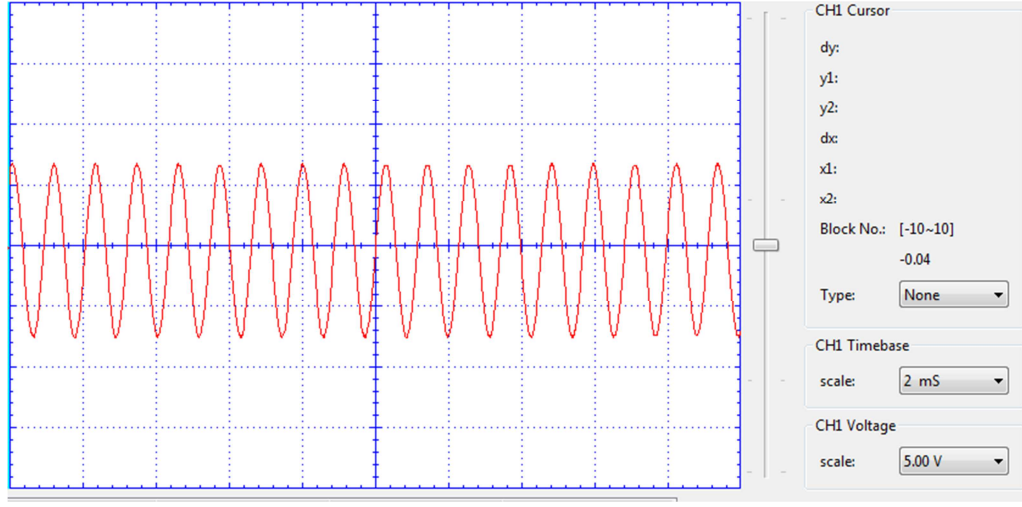


Şekil 3.9 Uygulama düzeneğinden bir görünüm

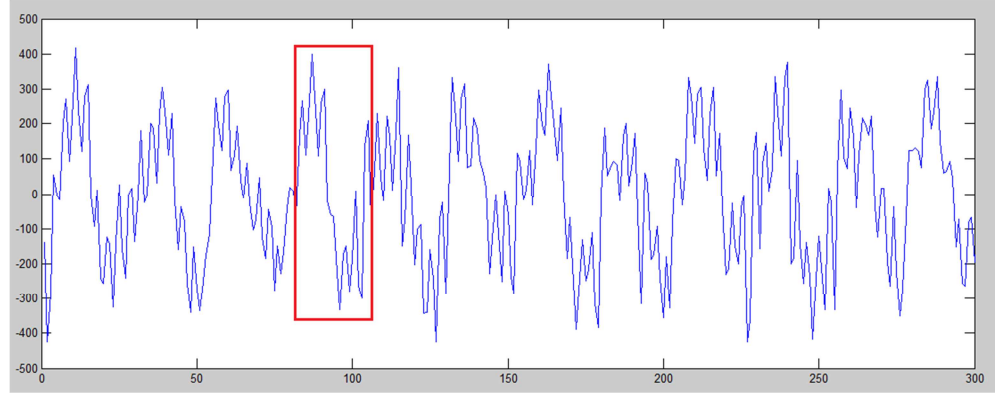
Okuyucu 13,56 MHz frekansta bir *sinüs* sinyali oluşturmaktadır. Bu sinyal karta enerji aktarmak ve cihaza bir saat sistemi sağlamak için kullanılmaktadır. Dolayısıyla, cihaz saati okuyucudan oluşan sinyal ile eş zamanlıdır. Okuyucudan karta veri aktarımı şekil 3.10'de gösterilen değiştirilmiş Miller Kodu ile tanımlanmaktadır. Karartma boşluğu sadece 2-3µs almakta ve dolayısıyla cihazın gönderim sırasında sürekli güç beslemesinde kalmasını sağlamaktadır.

Bu haberleşmeyi denetleyebilme bağlamında, işlem sırasında anten sinyalinin kaydedilebilmesi için okuyucu antenin çıkış sinyaline bir osiloskop bağlanarak yapılandırılmıştır. Şekil 3.10' da RF alanın aktif olduğu durumda anten uçlarındaki işaret görülürken, Şekil 3.11'de okuyucunun karta gönderdiği osiloskop sinyali görülmektedir. Bu sinyal kartın RF alana girdiği anda kaydedilmiştir. Veri alışverişinin

sağlandığı zamanlarda, 13,56 MHz taşıyıcı frekansa sahip olan sinüs işarette faz modülasyonunun gerçekleştiği görülmektedir.

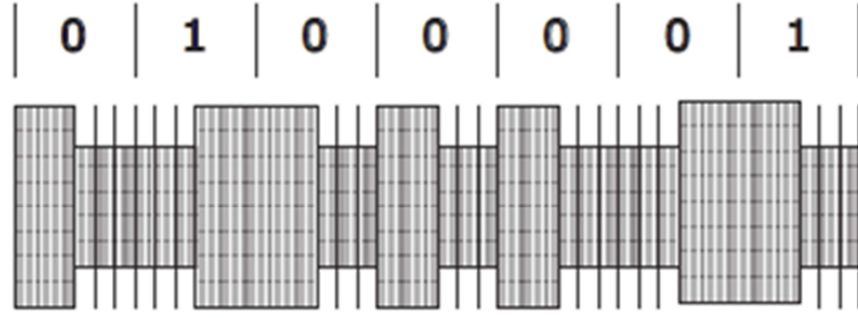


Şekil 3.10 Taşıyıcı frekansı 13,56MHz olan sinüs sinyali



Şekil 3.11 Kart okutulduğu esnada osiloskopta gözlenen işaret

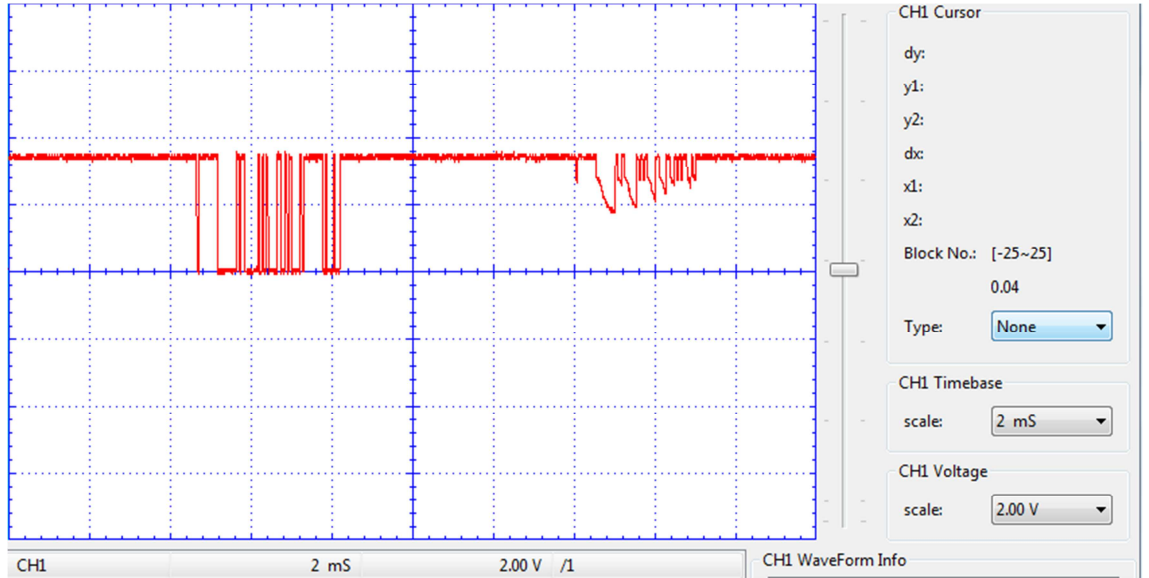
Uygulama düzeneği ile Doğrula(AUTH) komutu esnasındaki haberleşme birçok kez denetlenmiştir. Komut, doğrulamanın başarısız olacağı biçimde kart ve okuyucuya farklı anahtarlar kullanılarak verilmiştir. En iyi sonuçlar ve en küçük SNR değeri, anten yonganın en yakınında konumlandırıldığı elde edebilmektedir.



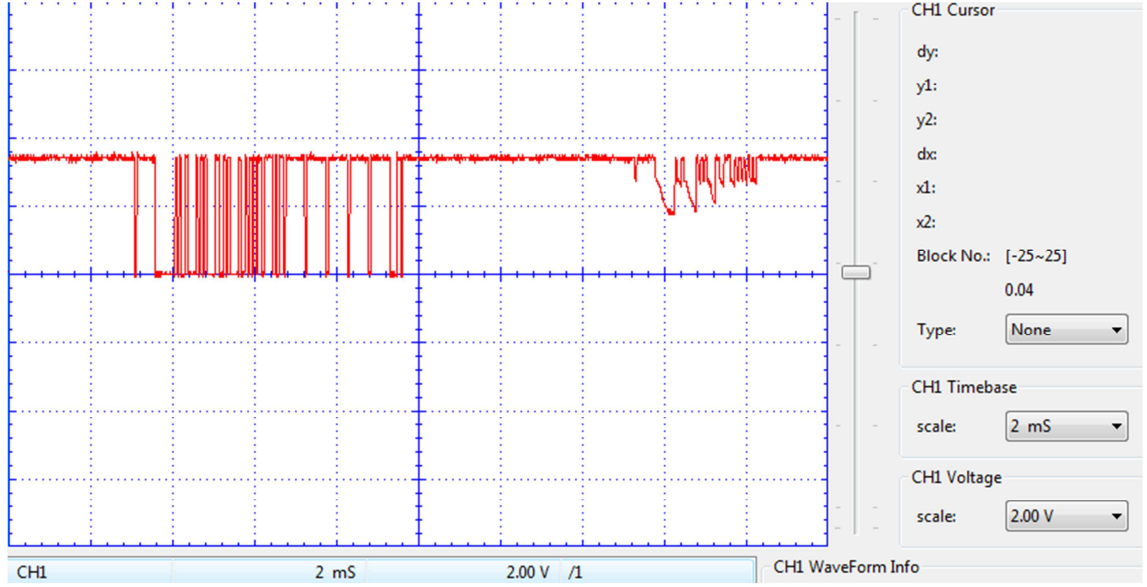
Şekil 3.12 Değiştirilmiş Miller kodu gösterimi

Cihazın DES işlemini hesapladığı zaman noktasında sinyal değişiminin yüksek olduğu gözlenmiştir. Ayrıca, EM radyasyonu ortalama değeri DES'in hesaplandığı zaman noktasında farklı olabilecektir.

Uygulamada gizli anahtar olarak "AB81CDFF4612" değeri atanmıştır. Doğru ve yanlış anahtar girilmesi durumunda elde edilen işaretler kaydedilmiştir.



Şekil 3.13 Doğru anahtar girilmesi durumunda elde edilen işaret



Şekil 3.14 Yanlış anahtar girilmesi durumunda elde edilen işaret



#### **4. BULGULAR VE SONUÇ**

Elektromanyetik radyasyon, örneğin RFID cihazları veya FPGA'lar gibi şifreleme cihazlarında güç tüketimini ölçmek pratik değilse bir yan kanal seçeneği olmaktadır.

Bu çalışmada elektromanyetik radyasyon kaynağı ve bu radyasyonu almak için kullanılacak anten tiplerine ilişkin teorik bir giriş verilmektedir. Ayrıca, yan kanal ölçümleri için bant genişliği, parazit ve durağan dalga oranları ilişkisi de açıklanmıştır.

Bazı elektriksel ve manyetik antenler yapılmış ve bir mifare temassız akıllı kartın üzerinde iyi bilinen basit DES uygulaması ile farksal elektromanyetik analiz gerçekleştirilebileceği gösterilmiştir.

Mifare kart için ölçüm düzeneği kurulmuş ve kartı doğrulama işlemi gerçekleştirilmiştir. Dolayısıyla gerek elektromanyetik analiz gerekse güç analizi için seçilen düz şifrelenmemiş metin analizi için elektromanyetik ve güç ölçümlerinin yapılmasının mümkün olduğu gözlenmiştir.

Ancak yapılan çalışmada elektromanyetik analizin mifare kartın şifre anahtarını riske atmak bağlamında tek başına başarılı olamadığı ortaya çıkmıştır.

## KAYNAKLAR

- Alptekin Bayam ,K. 2007** *Power Analysis Resistant Hardware Implementation of The RSA Cryptosystem.Yüksek Lisans Tezi*, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul
- Biham E., Shamir A.1993.** Differential Cryptanalysis of the full 16-round DES. Advances in Cryptology- CRYPTO'92, 16-20 Ağustos 1992, New York.
- Biham, E., Shamir, A.1990.** Differential Cryptanalysis of DES-like Cryptosystems. Advances in Cryptology- CRYPTO'91,11-15 Ağustos 1991,California.
- Biham, E. , Shamir, A. 1991.** Differential Cryptalysis of FEAL and N-Hash, Advances in Cryptology-EUROCRYPT'91,8-11 Nisan 1991, Brighton.
- Carluccio D. 2005.** Electromagnetic Side Channel Analysis for Embedded Crypto Devices, Ruhr University-Bochum
- Hess, E. , Janssen N. , Meyer B. , Schütze, T.2000.** Information Leakage Attacks Against Smart Card Implementations of Cryptographic Algorithms and Countermeasures. EUROSMART Security Conference.
- Karakoç,F. 2008** Kripto Analizde Melez Bir Yöntem: Çakışma Saldırısı.*Yüksek Lisans Tezi*,İstanbul Teknik Üniversitesi,Fen Bilimleri Enstitüsü,Bilgisayar Mühendisliği Anabilim Dalı, İstanbul
- Kocher, P.,Jaffe, J., Jun, B.,1998.** Introduction to Differential Power Analysis and Related Attacks. <http://www.cryptography.com/public/pdf/DPATechInfo.pdf> - (Erişim tarihi: 26.02.2011)
- Kocher, P.1996.** Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems. *Lecture Notes in Computer Science*, 1109:104–113.
- Koçak,A. 2006** Akıllı Kartlar Kullanarak Sayısal Araç Ruhsatı İçin Web Tabanlı Bir Prototip Geliştirilmesi. *Yüksek Lisans Tezi*, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Elektronik-Bilgisayar Dersi Eğitimi Anabilim Dalı, Ankara
- Kommerling, O. ve Kuhn, M.G.,1999.** Design Principles for Tamper Resistant Smart Card Processors. <http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf> - (Erişim tarihi: 26.02.2011)
- Matsui, M.** Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology-EUROCRYPT'93, 23-27 Mayıs, Lofthus.
- Messerges, T.S., Dabbish, E. A., Sloan, R.H. 1999** Investigations of power analysis attacks on smartcards,*Proceedings of USENIX Workshop on SmartcardTechnology*, pp. 15(161) : 1-12.

**Rankl, W., Effing, W., 2003.** Smart Cards: Smart Card Handbook , Editör : Cox, K. s. 18-23.

**Rankl, W., Effing, W., 2003.** SmartCards in Payment Systems: Smart Card Handbook , Editör : Cox, K. s. 673-721.

**Schneier, B., 1994.** Data Encryption Systems(DES): Applied Cryptography , Editörler: Riordan, M.,Merkle,R., s. 226-279.

**Şahin, A. , Buluş, E. , Sakallı, M.T.2005.** Modern Blok Şifreleme Algoritmalarının Gücünün İncelenmesi. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, 17-19 Kasım 2005, İstanbul.

**Yerlikaya,T. , Buluş E. , Buluş N.2006.** Kripto Algoritmaların Gelişimi ve Önemi. Akademik Bilişim Konferansı, Şubat 2006, Denizli.

**Yerlikaya,T. , Buluş E. , Buluş N.2006.** Asimetrik Şifreleme Algoritmalarında Anahtar Değişim Sistemleri. Akademik Bilişim Konferansı, Şubat 2006, Denizli.

## ÖZGEÇMİŞ

Adı Soyadı  
Doğum Yeri ve Tarihi

: Zümrüt MÜFTÜOĞLU  
: İstanbul-06.04.1982

Eğitim Durumu  
Lise  
Lisans

: Fenerbahçe Anadolu Lisesi (1996-2000)  
: Niğde Üniversitesi (2000-2004)

Çalıştığı Kurum ve Yıl  
İletişim(e-posta)

: BursaRay (02.01.2006-Halen)  
: [zumrutmuftuoglu@burulas.com](mailto:zumrutmuftuoglu@burulas.com)  
: [zumrutmuftuoglu@gmail.com](mailto:zumrutmuftuoglu@gmail.com)

## ULUDAĞ ÜNİVERSİTESİ

## TEZ ÇOĞALTMA VE ELEKTRONİK YAYIMLAMA İZİN FORMU

Yazar Adı Soyadı	Zümrüt MÜFTÜOĞLU
Tez Adı	Akıllı Kartlarda Saldırlara karşı Tedbir Yöntemlerinin Araştırılması
Enstitü	Fen Bilimleri Enstitüsü
Anabilim Dalı	Elektronik Mühendisliği
Tez Türü	Yüksek Lisans
Tez Danışman(lar)ı	Prof.Dr. Eldar MUSA
Çoğaltma (Fotokopi Çekim) izni	<input checked="" type="checkbox"/> Tezimden fotokopi çekilmesine izin veriyorum  <input type="checkbox"/> Tezimin sadece içindekiler, özet, kaynakça ve içeriğinin % 10 bölümünün fotokopi çekilmesine izin veriyorum  <input type="checkbox"/> Tezimden fotokopi çekilmesine izin vermiyorum
Yayımlama izni	<input checked="" type="checkbox"/> Tezimin elektronik ortamda yayımlanmasına izin Veriyorum  <input type="checkbox"/> Tezimin elektronik ortamda yayımlanmasının ertelenmesini istiyorum  1 yıl <input type="checkbox"/> 2 yıl <input type="checkbox"/> 3 yıl <input type="checkbox"/>  <input type="checkbox"/> Tezimin elektronik ortamda yayımlanmasına izin vermiyorum

Hazırlamış olduğum tezimin belirttiğim hususlar dikkate alınarak, fikri mülkiyet haklarım saklı kalmak üzere Uludağ Üniversitesi Kütüphane ve Dokümantasyon Daire Başkanlığı tarafından hizmete sunulmasına izin verdiğimi beyan ederim.

Tarih :08.04.2011

İmza :