Raspberry Pi Üzerinde AES Algoritmasına Yan Kanal Analizi ve Ölçüm İyileştirme

Bu tez Bilgi Güvenliği Mühendisliği'nde
Tezli Yüksek Lisans Programının bir koşulu olarak

Elif BÜYÜKKAYA
tarafından

Fen Bilimleri Enstitüsü'ne
sunulmuştur.

İSTANBUL
ŞEHİR
ÜNİVERSİTESİ

Bu tezi okuduk, kapsam ve nitelik açısından Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans derecesi için tümüyle uygun olduğu görüşüne vardık.

ONAYLAYANLAR:

Prof. Dr. Ensar Gül .....
(Tez Danışmanı)

Necati Ersen Şişeci .....
(Tez Eş-danışmanı)

Doç. Dr. Gökhan Bora Esmer .....

Yrd. Doç. Dr. Ali Çakmak .....

Bu tez İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü tarafından belirlenen tüm koşullara uygundur.

ONAY TARİHİ: 25.08.2015

MÜHÜR/İMZA:

Yazarlık Beyanı

Ben, Elif BÜYÜKKAYA, başlığı, 'Raspberry Pi Üzerinde AES Algoritmasına Yan Kanal Analizi ve Ölçüm İyileştirme' olan tezin ve içinde sunulan bilgilerin şahsıma ait olduğunu beyan ederim. Ayrıca:

- Bu çalışmanın bütünü veya esası bu üniversitede Yüksek Lisans derecesi elde etmek üzere çalıştığım süre içinde gerçekleştirilmiştir.
- Daha önce bu tezin herhangi bir kısmı başka bir derece veya yeterlik almak üzere bu üniversiteye veya başka bir kuruma sunulduysa bu açık biçimde ifade edilmiştir.
- Başkalarının yayımlanmış çalışmalarına başvurduğum durumlarda bu çalışmalara açık biçimde atıfta bulundum.
- Başkalarının çalışmalarından alıntıladığımda kaynağı her zaman belirttim. Tezin bu alıntılar dışında kalan kısmı tümüyle benim kendi çalışmamdır.
- Esaslı yardım aldığım bütün kaynaklara teşekkür ettim.
- Tezde başkalarıyla birlikte gerçekleştirilen çalışmalar varsa onların katkısını ve kendi yaptıklarımı tam olarak açıkladım.

İmza: _____

Tarih: 25.08.2017

“Yaşamak için bir "neden" i olan, her türlü "nasıl" a dayanabilir."

Friedrich Nietzsche

“’Hayatta başarı A ise, A eşittir x artı y artı z. Çalışmak x; eğlenmek y; z ise çeneni tutmaktır."

Albert Einstein

Raspberry Pi Üzerinde AES Algoritmasına Yan Kanal Analizi ve Ölçüm İyileştirme

Elif Büyükkaya

Öz

Bilginin, güvenliğinin sağlanması için kullanılan bir çok yöntem mevcuttur. Bu yöntemlerden en etkili olanlarının birisi de şifrelemedir. Şifreleme işlemi yapmak için kullanılabilecek bir çok algoritma mevcuttur. AES (Advanced Encryption Standard) algoritması, Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yayınlanmış algoritmalardan biridir. Aynı zamanda AES algoritması, veriyi şifrelemek ve çözmek için aynı şifreleme anahtarını kullanan simetrik blok şifreleme algoritmasıdır.

AES algoritmasının matematik alt yapısının güçlü olması onu bilindik kriptoanalize karşı dayanıklı kılmıştır. Bununla birlikte algoritmanın matematiksel yapısı ile ilgilenmeyen yan kanal saldırıları olarak adlandırılan farklı bir saldırı tekniği mevcuttur. Bu yan kanal saldırılarından, pasif yan kanal saldırılarında, kriptografik sisteme fiziksel olarak herhangi bir müdahalede bulunulmaz. Atak yapacak olan kişi, sistemin çalışması sırasında istemsiz olarak ürettiği verileri kullanır/analiz eder. Atak için kullanılacak olan bu veriler gizli anahtara ulaşmayı sağlıyorsa, yan kanal bilgisi olarak adlandırılır. Yan kanal bilgisi, sistemin çalışması sırasında tükettiği güç, yaydığı elektromanyetik dalga, çıkardığı ses, kriptografik işleminin tamamlama süresi olabilir.

Pasif yan kanal ataklarında kullanılan iki temel inceleme yöntemi mevcuttur. Bunlar basit yan kanal analizi ve farksal yan kanal analizidir [27]. Basit yan kanal analizi yöntemi bir ölçüm kullanılarak gerçekleştirilirken, farksal yan kanal analizi yönteminde birden fazla ölçüm kullanılır.

Bu tez çalışmasında Raspberry Pi üzerinde çalışan AES algoritmasına farksal yan kanal analizi yöntemlerinden birisi olan DEMA (Differential Electromagnetic Analysis) saldırısı yapılmıştır. Raspberry Pi nin işletim sistemi basit bir işletim sistemi değildir. Mini bir bilgisayar olması nedeniyle Raspberry Pi de bir işlem yapılırken işletim sistemine özgü işler de eşzamanlı olarak yapılmaktadır. İşletimin sisteminin rutin işlerinin çıkarmış olduğu gürültü, AES ile şifreleme veya çözme işlemi yapılırken işlem süresinin göstermiş olduğu değişkenlik izlenmiştir. Şifreleme süresinin değişkenlik göstermesi ve işletim sisteminin kendine has yaptığı rutin işlemler alınan ölçümleri analiz edilebilecek hale getirmeyi zorlaştırmıştır. Bu çalışma kapsamında Raspberry Pi platformunun kullanılmasının, direk yan kanal analizine karşı bir önlem olup olmadığı incelenmiştir.

Analiz işlemi sonunda algoritmanın yan kanal saldırısına bu haliyle direnemeyeceği gizli anahtarın elde edilmesiyle görülmüştür. AES algoritmasında yapılacak olan yazılımsal bir önlem ya da Raspberry Pi ye eklenecek yazılımsal/donanımsal bir önlem ile çözüm getirilmesi önerilmiştir.

Anahtar Sözcükler: Yan kanal analizi, DEMA, farksal elektromanyetik analiz,

Saygıdeğer aileme ve sevgili dostlarıma ...

Teşekkür

Tez çalışmam boyunca anlayış göstererek yardımcı olan, motivasyonum için desteğini esirgemeyen ve yol gösteren danışmanım Necati Ersen Şişeci' ye teşekkür ederim.

Maddi, manevi desteklerini sürekli gördüğüm, gerektiğinde benimle çareler arayan, değerli dostlarım eski çalışma arkadaşlarıma teşekkür ederim.

Anlayış ve sabırlarından dolayı aileme ve yardımları için kardeşime teşekkürlerimi sunarım.

İçindekiler

Şekil Listesi

Tablo Listesi

Kısaltmalar

AES	**A**dvanced **E**ncryption **S**tandard
DEMA	**D**ifferential **E**lectromagnetic **A**nalysis
DES	**D**ata **E**ncryption **S**tandard
DPA	**D**ifferential **P**ower **A**nalysis
EM	**E**lectromagnetic
EMA	**E**lectromagnetic **A**nalysis
FPGA	**F**ield **P**rogrammable **G**ate **A**rray
GF	**G**alois **F**ield
NIST	**N**ational **I**nstitute of **S**tandards and **T**echnology
RMS	**R**oot **M**ean **S**quare
RSA	**R**ivest **S**hamir **A**dleman
PA	**P**ower **A**nalysis
PCI	**P**ayment **C**ard **I**ndustry
SCA	**S**ide **C**hannel **A**nalysis
TA	**T**iming **A**nalysis
SEMA	**S**ingle **E**lectromagnetic **A**nalysis
SPA	**S**ingle **P**ower **A**nalysis

Bölüm 1

Giriş

Güvenli haberleşmenin, bilgi güvenliğinin, önemi ve farkındalığı gün geçtikçe artmaktadır. Paylaşılan bir çok verinin elektronik ortama aktarılması ve paylaşılması, bu işlemin güvenli bir şekilde sağlanması gerekliliğini doğurmuştur. Güvenli haberleşmenin sağlanması için geliştirilen savunma mekanizmaları aynı zamanda saldırı tekniklerinin de gelişmesine neden olmuştur.

Güvenli haberleşmenin sağlanması için alınan önlemler, kullanılan mekanizmalar M.Ö ki yüzyıllara dayanmaktadır. Kriptografik algoritmaların kullanılması güvenli haberleşmenin temelini oluşturan en önemli bileşenlerden biridir. Modern kriptolojiden önce güvenliğin sağlanması için algoritmaların gizliliği/saklanması önem arz etmekteydi. Kerchhoff ile geçilen modern kriptolojide ise algoritmanın gizliliği değil, algoritmada kullanılan anahtarın güvenliğinin sağlanması önemlidir [18]. Gizli anahtarın güvenliğini sağlamak bilginin gizliliğini sağlamaktır. Bu nedenle modern kriptolojiye geçilmesiyle yapılan saldırılar anahtarı ele geçirmeye yönelik olan saldırılar olmuştur.

Kriptolojide gerçekleştirilen saldırılar, matematiksel saldırılar ve tasarıma yönelik olan saldırılardır. Matematiksel saldırılarda sistemin dayandırıldığı matematiksel zorluk aşılmaya çalışılır. Tasarıma yönelik olan saldırılarda ise kriptografik sistemin doğası gereği ürettiği çıkışlar kullanılır. Bunlara örnek verilecek olursa sistemin kriptografik işlem gerçekleştirdiği esnada çıkarmış olduğu ses, yaymış olduğu elektromanyetik dalga, elektronik devreden çekilen güçtür. Bu saldırı tekniğine yan kanal saldırısı denir. Yan kanal saldırısı tekniği 1996 yılında yayınlanan, zamanlama analizi ile ilk defa Kocher tarafından gerçeklenmiştir [24]. Başarılı olmasıyla birlikte yan kanal saldırısı artık temel bir tehdit

olarak görülmeye başlamıştır. Yan kanal saldırıları pasif yan kanal saldırısı, yarı pasif yan kanal saldırısı ve aktif yan kanal saldırıları olmak üzere üç kısma ayrılır.

Pasif yan kanal saldırıları için kullanılan araçların maliyeti diğer yan kanal saldırılarında kullanılanlara göre daha düşüktür. Kriptografik işlem yapan cihaza/sisteme zarar vermeden gerçekleştirilir. Bu nedenle saldırı yapıldığı anlaşılmaz.

Günümüzde bilgisayarın ve mobil cihazların kullanımının oldukça yaygınlaşması saldırı yapılacak alanların da genişlemesini beraberinde getirmiştir. Kullandığımız bilgisayarlarda bulunan, matematiksel alt yapısı güçlü olan algoritmalar, yan kanal saldırılarına karşı önlem alınmadan tasarlanmışsa gizli anahtar ele geçirilebilir. 2016 yılında Tel Aviv Üniversitesi Laboratuvarı'nda yapılan bir çalışmada cep telefonunda bulunan eliptic-curve gizli anahtarı yan kanal saldırısı ile elde edilmiştir [48].

Yan kanal saldırısı için önlemler genelde kriptografik cihazlarda/sistemlerde alınmaktadır. Örneğin akıllı kartlar, HSM ler, güvenli işlemciler. Bu BT ürünleri genelde yan kanal saldırılarına karşı belirli seviyede güvenlik sağladıklarına dair sertifikalar alırlar. Örneğin akıllı kartlarda EAL4 ve üzeri güvenlik seviyesinde Common Criteria (CC) sertifikası alınır.

Akıllı kartlarda kullanılan işletim sisteminden daha gelişmişine sahip olan bir sistemde, bir bilgisayarda yan kanal saldırısının başarısını etkileyecek olan gürültü daha fazladır. İşletim sistemi şifreleme işlemi yapılırken sadece o işlemi değil başka işlemleri de gerçekleştirdiği için şifreleme süresi sabit kalmayacaktır. Bu tez çalışması kapsamında bilgisayar, cep telefonu gibi cihazlar düşünülerek Raspberry Pi üzerinde önlem alınmadan gerçeklenmiş bir AES algoritmasının yan kanal saldırısına karşı gösterebileceği direnç incelenmiştir.

Çalışmanın daha iyi ifade edilebilmesi için farklı başlıklar altında gerekli ön bilgiler verilmiş ve gerçekleştirilen işlemler anlatılmıştır. Bölüm 2 de gerekli matematiksel kavramlar ve kriptolojinin genel bir özetinden bahsedilmiştir. Bölüm 3 de yan kanal analizi saldırıları ve tez çalışmasında kullanılmış olan Elektromanyetik Analiz Saldırısına değinilmiştir. Bölüm 4 de saldırının gerçekleştirildiği Rapsberry Pi ve işletim sisteminin kurulu olduğu BCM2835 hakkında bilgi verilmiştir. Bölüm 5 te DEMA saldırısını gerçekleştireceğimiz AES algoritması ve özellikleri anlatılmıştır. Bölüm 6 da Raspberry Pi nin şifreleme işlemi yaparken etrafa yaydığı EM dalgaları kaydetmek için nasıl bir

ortam hazırlandığı ve alınan verilerin matlab ortamına aktarılması anlatılmıştır. Bölüm 7 de hangi analiz yöntemlerinin kullanılarak anahtarın bulunmaya çalışıldığı, kaydedilen ölçümlerin analize tabi tutulabilmesi için ne tür işlemlerden geçirildiği anlatılmıştır. Son bölüm olan 8 de ise alınan sonuçlar ve geleceğe yönelik olan çalışmalara yer verilmiştir.

Bölüm 2

Genel Bilgiler

Bu bölümde tezin anlatılması suresince konuya dahil olacak matematiksel kavramlar anlatılmıştır. Bununla birlikte kısaca kriptografik algoritmalar konusundan bahsedilmiştir.

2.1 Matematiksel Kavramlar

AES algoritmasında kullanılan sonlu alanlar kümesinin bir altkümesi olan Galois Alanları' nı anlamak için bilinmesi gereken bazı matematiksel tanımlar aşağıda verilmiştir.

2.1.1 Abelian Grubu

Abelian Grubu, $< G, + >$, bir G kümesi ve bu kümenin elemanları üzerinde tanımlanmış olan bir '+' işleminden oluşur [2],[3]. Öyle ki,

$$+ : GXG \longrightarrow G : (a, b) \rightarrow a + b \tag{2.1}$$

$<$ G, $+$ $>$ grubunun Abelian Grubu olabilmesi için, '+' işleminin aşağıda sıralanan koşulları sağlaması gerekir:

1. Kapalılık

$$\forall a, b \in G : (a + b) \in G \tag{2.2}$$

2. Birleşme

$$\forall a, b, c \in G : (a + b) + c = a + (b + c) \tag{2.3}$$

3. Değişme

$$\forall a, b \in G : a + b = b + a \tag{2.4}$$

4. Etkisiz Eleman

$$\exists 0 \in G, \forall a \in G : a + 0 = a \tag{2.5}$$

5. Ters Eleman

$$\forall a \in G, \exists b \in G : a + b = 0 \tag{2.6}$$

Örneğin; Tamsayılar kümesi ve 'toplama' işlemi, $< \mathrm{Z}, + >$, bir Abelian Grubu oluşturmaktadır. Benzer şekilde 0'dan n -1' e kadar olan tamsayıların oluşturduğu küme ve 'modülo n toplama' işlemi, $<Z_n, + >$, de bir Abelian Grubu oluşturmaktadır.

2.1.2 Halka

R boş kümeden farklı bir küme aynı zamanda "+" ve "*" işlemi bu küme üzerinde tanımlı olan ikili işlemler olsun. Eğer; (R,+) kümesi değişmeli bir küme, (R,*) kümesi sadece birleşme özelliğini sağlayan bir küme ve "*" işlemi "+" işlemi üzerine sağdan ve soldan dağılmalı ise (R,+,*) kümesine halka denir. Eğer "*" işlemi değişme özelliğine sahipse, (R,+,*) halkası 'Değişmeli Halka' olarak adlandırılır. "+" işleminin birim elemanı 0, "*" işleminin birim elemanı ise 1'dir [2].

2.1.3 Alan

Bir F kümesi, üzerinde tanımlı "+"ve "*" işlemleriyle birlikte aşağıda belirtilen koşullar sağlanmışsa bir 'Alan' oluşur.

(F,+) ve (F,*) bir Abelian grubu olmalıdır, bununla birlikte sadece 0 elemanı için ters eleman olmayabilir. "*" işleminin "+" işlemi üzerine dağılma özelliği olmalıdır [2].

2.1.4 Sonlu Alan

Sonlu sayıda elemanlara sahip alanlardır. Aynı matematiksel yapıya sahip olup sadece eleman gösterimlerinde farklılıklar vardır.

2.1.5 Galois Alanları

P sayısı asal olmak üzere $\{0, 1, 2 \ldots, p-1\}$ elemanlarından oluşan ve üzerinde modülo p toplama "+" ve modülo p çarpma "*" işlemleri tanımlı alana 'Galois Alanı' denir ve "$GF(p)$" olarak gösterilir. P sayısı 'Galois Alanının Karakteristiği' olarak adlandırılır [4].

Başka bir ifadeyle, p bir asal sayı olmak üzere, p sayısınca elemanı olan sonlu bir alan 'Galois Alanı' olarak adlandırılır. Galois Alanı $GF(p)$ ile gösterilir.

$GF(p^n)$, $GF(p)$ 'nin Genişletilmiş Sonlu Alanı' nı ifade etmektedir. $GF(p^n)$ 'nin eleman sayısı $GF(p)$ sonlu alanının elaman sayısının n katıdır. $GF(p^n)$ 'de yapılan "+" ve "*" işlemlerinin alan içerisinde kalmasını sağlamak için n. dereceden polinoma ihtiyacı vardır. Kullanılan n. dereceden polinomun çarpanlarına ayrılamaması gerekmektedir. Bu polinomun "İndirgenemez Polinom" olması gerekmektedir [4].

2.1.5.1 $GF(2^n)$ Galois Alan

Karakteristiği 2 ve eleman sayısı 2^n olan Galois Alanları' dır. "İkili Sonlu Alanlar" olarak adlandırılmaktadır. Eleman gösterimi $\{0, 1\}$ in yan yanan yazılmasıyla gösterilir. Bu nedenle matematiksel işlemlerin gerçekleştirilmesini kolaylaştırmaktadır. Dolayısıyla yazılım, donanım ve kriptografik algoritmaların gerçeklenmesinde yaygın bir kullanıma sahiptir.

Farklı baz vektörlerinin kullanımı nedeniyle farklı gösterimlere sahiptir. En yaygın gösterim şekli polinomsal gösterimidir. $\left\{x^{n-1}, x^{n-2}, x^{n-3}, \ldots, x^2, x, 1\right\}$ İkili sonlu alanlar için polinomsal baz kümesinden oluşur. $GF(2^n)$ nin bir elemanının polinomsal baz gösterimi, polinomsal baz vektörünün her bir elamanının $GF(2)$ 'ye ait bir elemanla çarpılması ile elde edilir. Örneğin, $GF\left(2^8\right)$ 'in bir elemanı olan $\{11101011\}$'in polinomsal baz olarak gösterimi aşağıdaki gibidir.

$a(x) = x^7 + x^6 + x^5 + x^3 + x + 1$

2.1.5.2 $GF(2^n)$ Galois Alanları' nda Matematiksel İşlemler

Toplama İşlemi

$GF(2^n)$ Galois Alanları' nda toplama ve çıkarma işlemi, verilen polinomların toplandıktan sonra elde edilen polinomun katsayılarının modülo 2 olarak düzenlenmesiyle elde edilir. Bir örnekle gösterilecek olursa $a, b, c \in GF\left(2^7\right)$ olmak üzere;

$a(x) = x^6 + x^5 + x^3 + x + 1$

$b(x) = x^6 + x^4 + x + 1$

$c(x) = a(x) + b(x) = 2x^6 + x^5 + x^4 + x^3 + 2x + 2$

Katsayıların modülo 2 deki değeri alındığı zaman

$c(x) = x^5 + x^4 + x^3$

Buradan hareketle toplama sonucu elde edilen polinomun modülosunu almak aynı zamanda bu polinomu bit bit xor işlemine tabi tutmaktır. Yukarıda verilen örneği xor yaparak tekrardan matematiksel işleme tabi tutulacak olursa [1];

$c(x) = a(x) \oplus b(x)$

$= \{1101011\} \oplus \{1010011\} = \{0111000\}$

$c(x) = x^5 + x^4 + x^3$ olarak aynı sonucun bulunduğu görülür.

Çarpma İşlemi

İkili sonlu alanda tanımlı iki polinomun çarpılması, aritmetik olarak iki polinomun çarpımı ile aynıdır. Bununla birlikte bu çarpımdan elde edilen polinomun derecesi sonlu alanın derecesinden daha büyük olabilir. Bu durumda elde edilen polinom sonlu alan içerisindeki bir polinoma karşılık gelecek şekilde indirgeme işleminin yapılması gerekir. Bu işlem n. dereceden bir indirgeme polinomu ile modülünün alınmasıyla yapılır. Bir örnekle gösterilecek olursa $a, b, c \in GF\left(2^8\right)$ olmak üzere;

$a(x) = x^6 + x^5 + x^3 + x + 1$

$b(x) = x^6 + x^4 + x + 1$

$c(x) = a(x) + b(x) = \left(x^6 + x^5 + x^3 + x + 1\right) \cdot \left(x^6 + x^4 + x + 1\right)$

$c(x) = x^{12} + x^{11} + x^{10} + 2x^9 + 3x^7 + 3x^6 + 2x^5 + 2x^4 + x^3 + x^2 + 2x + 1$

Elde edilen polinomun derecesi 8 den büyük olduğu için indirgeme polinomu ile modülü alınarak sonlu alan içerisinde tanımlı bir polinoma denk getirmek gerekir. İndirgeme polinomu olarak $x^8 + x^4 + x^3 + x + 1$ kullanılırsa;

$c(x) = x^7 + x^5 + x^3 + x^2 + x$ olarak bulunur.

2.2 Kriptoloji

Kriptografi, verinin güvensiz (herkese açık) ortamda gizliliğini sağlamak, erişilebilirliğinden emin olmak, inkaredemezlik asıllama ya da değiştirilmeden iletmesi gibi bilgi güvenliği problemlerine çözüm amacı ile kullanılan bir bilimdir. Şifreleme olarak da adlandırılan kriptografide kullanılan yöntemlerin güvenliği bazı matematiksel teorilerin çözülmesinin zorluğundan/karmaşıklığından ya da bir bilgisayarla/sistemle uzun yıllar alacak çalışmalar aracılığıyla çözülmesine dayanmaktadır. Kriptoanaliz, kriptografide kullanılan matematik teorilerinin zorluklarının aşılması ya da teknolojinin gelişmesi vb. sebeplerle kullanılan yöntemlerin geçersiz kılınmasıdır. Kriptoanaliz ile şifrelemede kullanılan algoritmalar bazı yöntemlerle kırılmaya çalışılır.

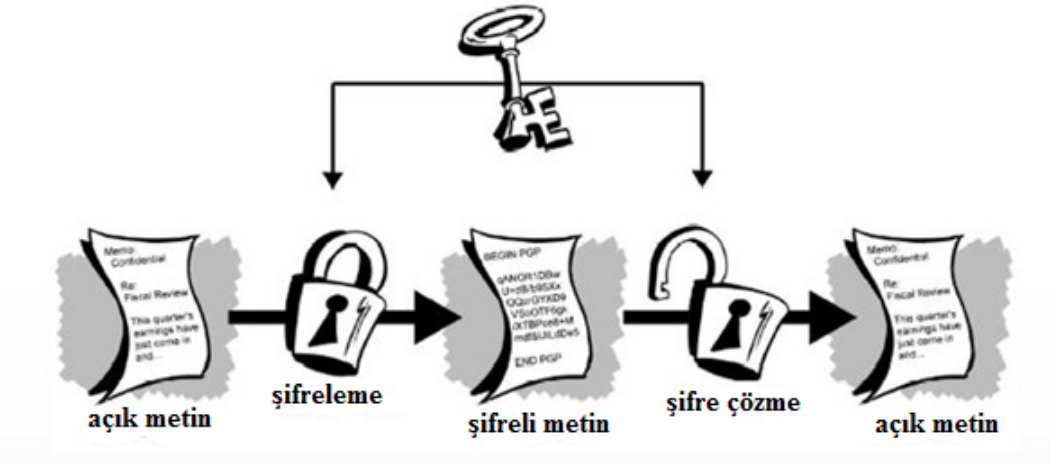
Kriptografi ve kriptoanalizin birleşimi kriptolojiyi oluşturur. Kriptolojinin temelleri M.Ö ki yüzyıllara dayanır.

Günümüzde şifreleme algoritmaları simetrik ve asimetrik şifreleme algoritmaları olmak üzere ikiye ayrılır.

2.2.1 Simetrik Şifreleme

Simetrik şifrelemede açık veriyi şifrelemek ve bu şifrelenmiş kapalı veriyi çözmede aynı anahtar kullanılır (bkz. Şekil 2.1). Bu anahtar sadece gönderici ve alıcı tarafından bilinir. Verinin üçüncü kişiler tarafından okunamaması için anahtarın gizliliği önemlidir. Bu anahtara gizli anahtar da denir.

Simetrik şifreleme asimetrik şifrelemeye göre daha hızlıdır. Gerçeklenmeleri de daha kolaydır. Çünkü asimetrik şifrelemede büyük sayılarla işlem yapılması gerekir. Yine



Şekil 2.1: Simetrik şifreleme

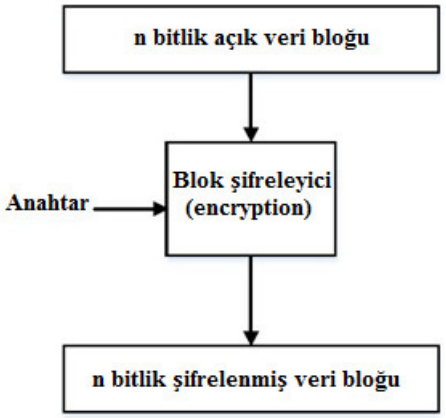
asimetrik şifrelemeye göre anahtar boyu daha küçüktür. Simetrik şifreleme algoritmalarına örnek olarak DES, AES, Blowfish, 3DES, IDEA, RC4, A5/1, A5/2, E0 verilebilir [15], [16]. Donanımsal olarak gerçeklenmesi kolaydır. Özel olarak hazırlanmış olan donanımlar yazılımlardan daha hızlı işlem yapabilmektedir [6]. Simetrik şifreleme algoritmaları veriyi işleyiş biçimlerine göre blok şifreleme ve dizi şifreleme olmak üzere iki kısımda incelenebilir.

2.2.2 Blok Şifreleme

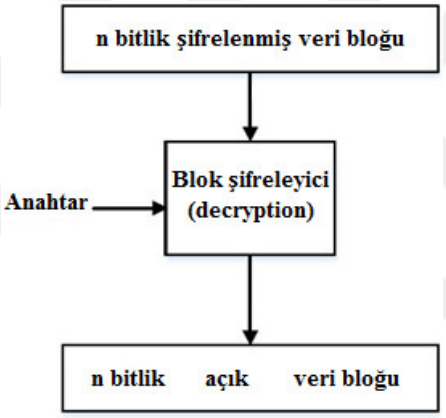
Blok şifreleme algoritmaları, Shannon'un [9] karıştırma ve yayılma tekniklerine dayanır [10]. Karıştırma şifreli veri ve açık veri arasındaki bağlantıyı saklarken, yayılma açık verideki izlerin şifreli veride sezilmemesini sağlamak için kullanılır. Karıştırma ve yayılma, sırasıyla yer değiştirme ve doğrusal dönüşüm işlemleri ile gerçeklenir. Feistel ağları ve Yer değiştirme-Permütasyon ağları olmak üzere iki ana blok şifreleme mimarisi vardır [11]. Her ikisi de yer değiştirme ve lineer dönüşümü kullanır [7]. Blok şifrelerde yer değiştirme S kutuları ile sağlanır. Yayılma bayt veya bit bazında gerçekleştirilen doğrusal dönüşümler aracılığıyla sağlanmaktadır. S kutuları doğrusal olmayan yapılardır ve doğrusal olmama (nonlinearity) bu tip şifrelerin tasarımındaki en önemli ölçütlerden biridir [21].

Şifrelenecek olan veriyi bit grubu halinde alır. Bu bit gruplarına blok denir. Bloklar genel olarak 32,64 ya da 128 bit olarak alınır [17]. Şifreleme esnasında açık veri bloklara bölünür. Bu bloklar birbirinden bağımsız olarak şifrelenir [5]. Şifrelenen blok yine açık veri ile aynı boyuttadır. Şifre çözme işlemi ise yine sabit uzunlukta alınan şifrelenmiş

bloğun ters dönüşümden geçirilerek bloklar halindeki açık veriye dönüşüdür. Genel yapısı Şekil 2.2 ve Şekil 2.3 deki gibidir.



Şekil 2.2: Blok şifreleme (şifreleme işlemi)



Şekil 2.3: Blok şifreleme (şifre çözme işlemi)

Blok şifreleme büyük boyutlu verilerin şifrelenmesinde yaygın olarak kullanılır. Bunlara örnek olarak 64 bitlik DES ve 128 bitlik AES algoritması verilebilir [18] [20].

2.2.3 Dizi Şifreleme

Dizi şifreleme algoritması veriyi küçük boyutlarda (1 bit veya 8 bit) işler. Dizi şifreleyiciler bir anahtar dizisi üretirler. Şifreleme veya çözme işlemi, üretilen bu anahtar dizisinin algoritma girişindeki veri dizisiyle etkileştirilmesiyle (genellikle karşılıklı bitlerin xor' lanması şeklinde olur) gerçekleştirilir [1]. Dizi şifrelemenin genel yapısı Şekil 2.4 ve Şekil 2.5 deki gibidir.

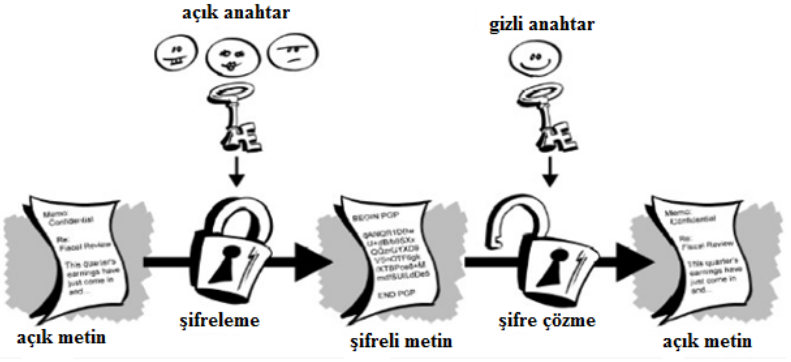
ŞEKIL 2.4: Dizi şifreleme (şifreleme işlemi)

ŞEKIL 2.5: Dizi şifreleme (şifre çözme işlemi)

Blok şifrelemeye göre daha hızlıdır ve daha az yer kaplar. Daha az donanıma ihtiyaç duyar. Bununla birlikte dizi şifrelemede eş zamanlılık için ek mekanizma gerekli. Güvenlik riski daha yüksektir. Riski azaltmak için kayan anahtarı bir kez kullanmak ve kayan anahtarın rastgeleliğini sağlanmak alınabilecek bir önlemdir [5].

2.2.4 Asimetrik Şifreleme

Asimetrik şifrelemede, şifreleme anahtarı ve şifrelenmiş veriyi çözme için iki farklı anahtar kullanılır. Bu anahtar çiftinden birisi açık anahtar (public key) diğeri ise gizli anahtardır (private key). Açık anahtarın üçüncü kişilerden saklanmasına ihtiyaç yoktur. Önemli olan gizli anahtarın simetrik şifrelemede olduğu gibi üçüncü kişilerden saklanmasıdır. Asimetrik şifrelemenin genel yapısı Şekil 2.6 deki gibidir. Asimetrik şifreleme algoritmaları ile, kullanıcılara güvenli olmayan bir iletişim hattında, güvenli bir iletişim kurma imkanı sağlanmaktadır [8].



ŞEKIL 2.6: Asimetrik şifreleme

Simetrik şifrelemeye göre daha yavaştır. Gizli anahtarların karşı tarafa aktarılması gerekmediğinden anahtar dağıtma problemi bu şifreleme türünde görülmez. Veri gönderilecek kişi sayısı arttıkça veriyi gönderecek olan kişideki açık anahtar sayısı da artacaktır. Bu sorun ise sayısal sertifika ile çözülmektedir [13].

Günümüzde yaygın olarak kullanılan asimetrik şifreleme algoritmalarına örnek olarak RSA (Rivest-Shamir-Adleman), El-Gamal, Eliptik Eğri [12]. Asimetrik şifreleme algoritmalarının en büyük avantajı, veri şifreleme ve şifre açma işlemleri ile gizlilik sağlamasının yanında kimlik doğrulama (authentication), bütünlük(integrity), inkar edememezlik (non-repudiation) gibi prensipleri de sağlayabilmesidir [14].

Bölüm 3

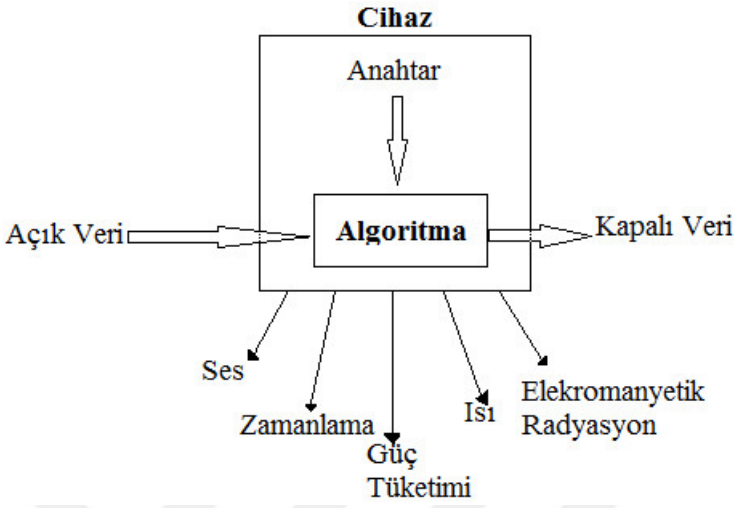
Yan Kanal Analizi Saldırıları

Gelişen teknolojiyle birlikte insanlığın güvenli haberleşme yöntemleri de değişmiş ve gelişmiştir. M.Ö ki yüzyıllara bakıldığında güvenli haberleşmeyi sağlamak amacıyla bazı şifreleme algoritmaları oluşturulmuş ve sadece haberleşmek istenilen kişilerle paylaşılmıştır. Bununla birlikte şifreleme algoritmasının üçüncü bir kişi tarafından öğrenilmesi/ele geçirilmesi ile haberleşmenin güvenliği ortadan kalkmış oluyordu.

Kerckhoff prensibi ile temeli atılan modern şifreleme algoritmaları geliştirilmeden önce haberleşmenin güvenliği algoritmanın gizliliğine dayanıyordu [22]. Modern şifreleme algoritmalarının geliştirilmesiyle birlikte bu sorun yerini şifreleme anahtarının gizliliğine bırakmıştır. Tek başına şifreleme anahtarı demek yine yetersiz olur. Çünkü algoritmanın sağlamlığı yine bir problem olarak karşımızdadır. Bir kripto sistemini kırmak: belirlenmiş bir hesaplama gücüne karşı sağlandığı iddia edilen bir kripto hizmetinin daha az hesaplama gücüyle korunması durumunun aşılmasıdır. Bölüm 2 de bahsedilen kriptoanaliz kripto sistemlerini kırma çalışmalarının bütünüdür [5].

Modern şifreleme algoritmalarından DES kriptoanaliz ile kırılmıştır. Nedenlerinden birisi algoritmasındaki S kutularının zayıflığıydı. DES algoritmasının kırılmasında diferansiyel atak [25] ve doğrusal atak [26] uygulanmıştır [22]. Kriptoanaliz yöntemleri sadece algoritmanın matematiksel sağlamlığına bakmaz. Örneğin algoritma çok güçlü kırılamıyor. Bu haberleşmede %100 güvenlik sağlar mı? Bu sorularımızın yanıtı yan kanal bilgisi ile cevap buluyor. Sistemin doğrudan ürettiği sonuçları kullanmak yerine onların yaydıkları

elektromanyetik dalga, çıkardığı ses, tükettiği güç [23], zamanlama farkı vb. bilgileri kullanılarak gizli bilgiye ulaşılmaktadır. Sistemlerin istem dışı verdikleri yan kanal bilgisi aşağıdaki şekilde verilmiştir.



Şekil 3.1: Sistem tarafından dışarıya verilen yan kanal bilgileri

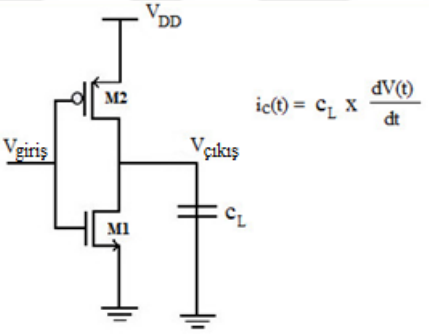
Yan kanal analizi saldırıları Aktif, Yarı Aktif ve Pasif olmak üzere üç grupta incelenir. Aktif yan kanal analizi saldırılarında atağın yapıldığı çoğu kere anlaşılır. Çünkü saldırılar için cihazın içine [27],[28] (devreye, yongaya vb.) ulaşılması gerekir ve müdahale sırasında hasar görebilir. Çip soyma veya problama [29] aktif yan kanal saldırılarına örnek olarak verilebilir. Diğer saldırı yöntemlerine göre ilgili yere ulaşımı daha zordur. Aynı zamanda aktif yan kanal saldırılarında kullanılan cihazlar oldukça pahalıdır; örneğin lazer istasyonu, FIB istasyonu vb.

Pasif yan kanal analizi saldırılarında sistemin çalışmasına herhangi bir şekilde müdahale edilmez. Sistemin çalışması sırasında ürettiği diğer bir değişle istemeden sızdırdığı yan kanal bilgilerinden faydalanılır. Saldırı için çok pahalı cihazlara, düzeneklere ihtiyacı yoktur [18]. Yarı aktif saldırılarda ise aktif saldırılar gibi tahribat yüksek değildir. Aktif ile pasif saldırı arasında yer alır. Konsept bakımından ilk olarak Skorobogatov ve Anderson tarafından tasarlanmışıtır [19]. Pasif saldırılara nazaran uygulanması daha zordur. Aktif saldırılara göre ise daha ucuzdur [33]. Yarı aktif saldırılara örnek olarak UV Saldırıları, Fault Injection Saldırıları, Aktif Foton Problama verilebilir [34].

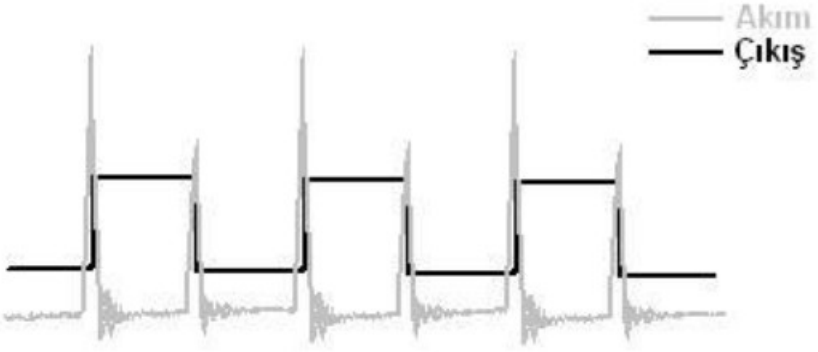
Tez çalışması kapsamında sadece pasif yan kanal saldırılarından biri olan elektromanyetik analiz saldırıları üzerinde durulmuştur.

3.1 Elektromanyetik Analiz Saldırıları

CMOS lar günümüzdeki mevcut sayısal devrelerin büyük çoğunluğunda kullanılmaktadır [30]. Kullanım nedenlerinden birisi devre açık halde iken çok az güç tüketmesidir. Devre çalışır durumda iken işledikleri verilere göre farklı güç tüketimi yapmakta ve buna bağlı olarak devreden çekilen akım da değişmektedir. Devreden çekilen akım değişimi ise elektromanyetik radyasyon yayılımında değişime sebep olur. CMOS lar da akım sadece lojik durum değişimi olduğu zaman akar [31]. Bunun için Şekil 3.2 de verilen CMOS evirici yapısına bakılabilir. Konum değişimlerinde tüketilen güce bakacak olursak Tüketilen güç miktarı değişimi devre içerisinde çekilen akımın değişimini meydana getirdiği için, devrenin yaydığı elektromanyetik radyasyonun da değişmesine neden olur. Böylelikle devre yan kanal bilgisi sızdırmış olur. Ayrıca, devre içerisinde oluşan çeşitli kuplajlar ve gerçekleştirilen modülasyonlar da elektromanyetik radyasyona, dolayısıyla yan kanal bilgisi oluşumuna neden olabilir [1]. Çekilen akımın değişmesiyle oluşan grafiğe bir örnek olarak Şekil 3.3 gösterilebilir.



Şekil 3.2: CMOS evirici yapısı



Şekil 3.3: Çekilen güç ile değişen akım grafiği

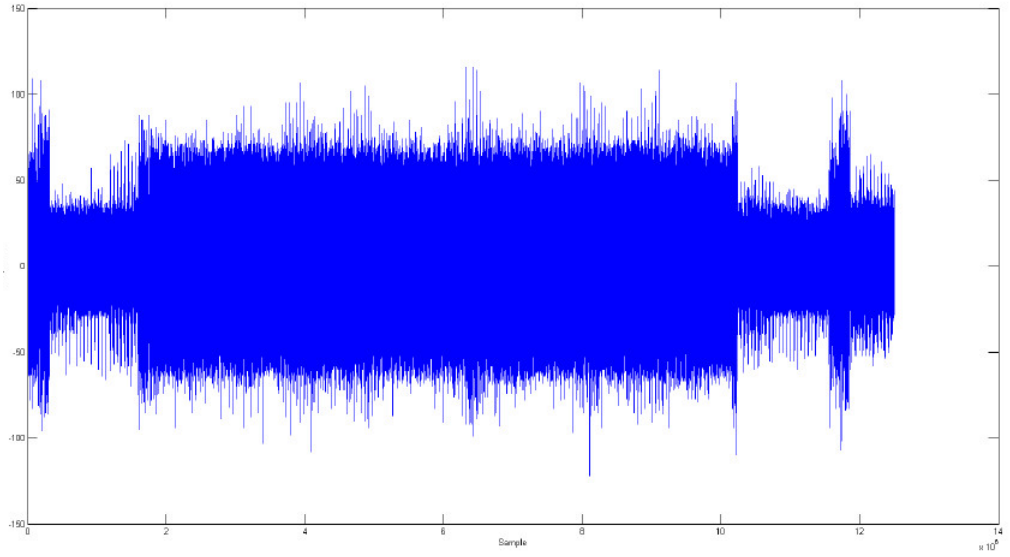
Elektromanyetik analiz saldırılarının bazı yönlerde güç saldırılarına karşı avantajları vardır. Ölçüm almak için kullanılacak olan anten aracılığıyla istenilen yere odaklanılabilir. Cihaz ile herhangi bir fiziksel bağlantı/temas yapılmasına da gerek yoktur. Belirlenen bir mesafeden ölçümler rahatlıkla alınabilir.

Elektromanyetik alan saldırılarında antenin çeşidi ve probun/antenin nereye konumlandırılacağı önemlidir. Elektromanyetik analiz saldırılarının güç analizi saldırılarından daha etkin olduğu yada daha zayıf olduğuna dair kesin bir bilgi yoktur [36].

Elektromanyetik analiz saldırılarını genel olarak iki grupta sınıflandırılabilir. Bunlar Single Electromagnetic Analysis (SEMA) ve Differential Electromagnetic Analysis DEMA saldırılarıdır.

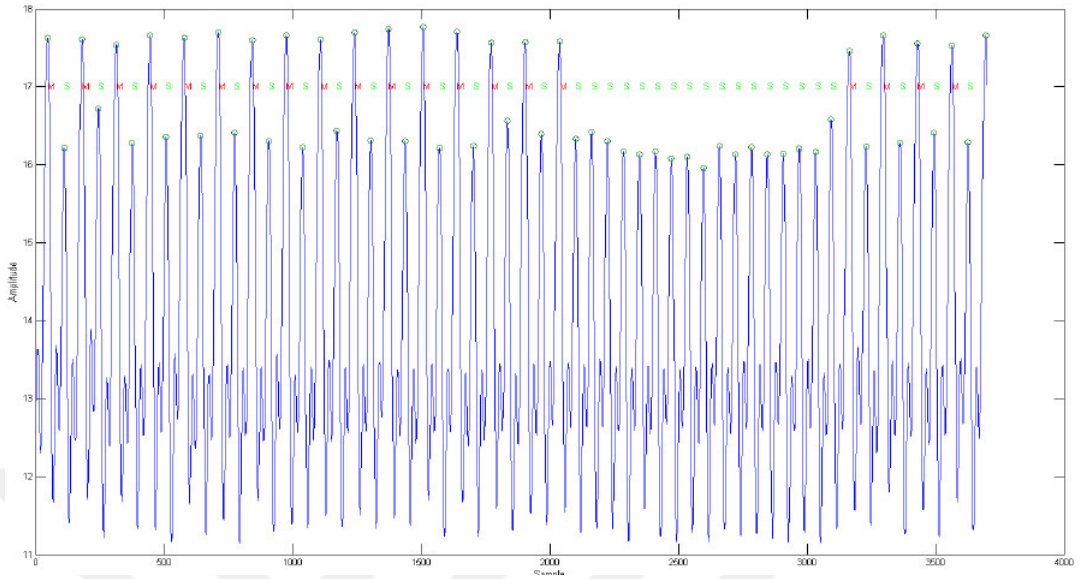
3.1.1 Basit Elektromanyetik Analiz (SEMA) Saldırıları

2000 li yıllarda elektromanyetik yan kanal bilgisi kullanılarak SEMA saldırıları gerçekleştirilmiş, [32] ardından çalışmalar hızlandırılmıştır [1]. Cihazdan alınan tek ölçümle yürütülen işlem hakkında bilgi edinilebilir. Bu işlem anahtar hakkında bilgi veriyorsa gizli anahtara ulaşılmaya çalışılır. Örneğin RSA algoritmasında kullanılan gizli anahtarı elde etmek isteyen birisi şifre çözme ya da imzalama işlemi anında cihazın yaydığı elektromanyetik dalgayı kaydederek gizli anahtara ulaşabilir. Şekil 3.4' te RSA için şifre çözme işlemi yapılırken antenle alınan bir ölçüm verilmiştir.



Şekil 3.4: Anten ile alınan tek ölçüm

Bu ölçüm için gerekli işlemler yapıldıktan sonra (filtreleme vb.) sonra gizli anahtarının bulunduğu şekil 3.5' te net bir şekilde görülmektedir.



Şekil 3.5: RSA algoritmasında anahtara göre farklı mitarda elektromanyetik alan yaymasıyla elde edilen gizli anahtar

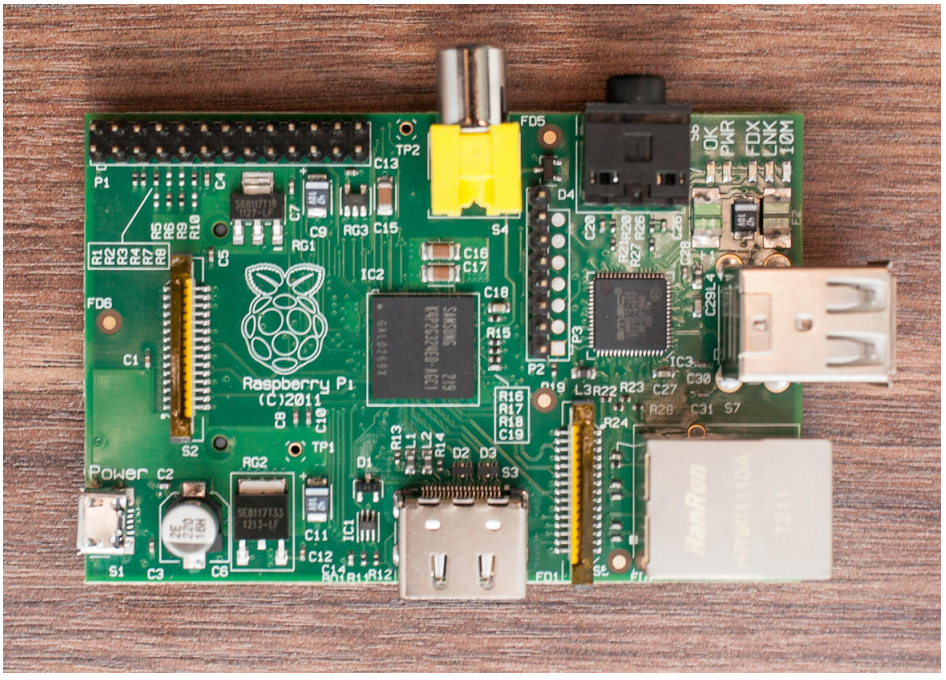
3.1.2 Farksal Elektromanyetik Analiz (DEMA) Saldırıları

DEMA saldırılarında cihazdan yayılan elektromanyetik dalga ile işlenen veri arasında bağlantı kurulmaya çalışılır. SEMA' da ki gibi tek ölçüm ya da birkaç ölçümle yetinilemez. Gürültüyü bastırmak amacıyla çok sayıda ölçüm alınır. Bu neden le gerçeklenmesi SEMA' ya göre daha zordur. Fakat daha etkilidir. SEMA' da ki gibi sistem hakkında bilgi sahibi olmak önemli değildir. DEMA saldırısının aşamaları 6. ve 7. Bölümde detaylı anlatılmıştır.

Bölüm 4

Raspberry Pi Ve Broadcom BCM2835

Raspberry Pi, Raspberry Pi Foundation tarafından 2009'da geliştirilmeye başlanmış kredi kartı büyüklüğündeki tek boardtan oluşmuş bir mini-bilgisayardır [37]. Düşük maliyeti, boyutu, güç tüketimi tercih edilme sebepleridir. SSH veya putty.exe gibi uygulamalarla istenilen yerden Raspberry Pi ye erişim sağlanabilmektedir.



Şekil 4.1: Raspberry Pi Model B

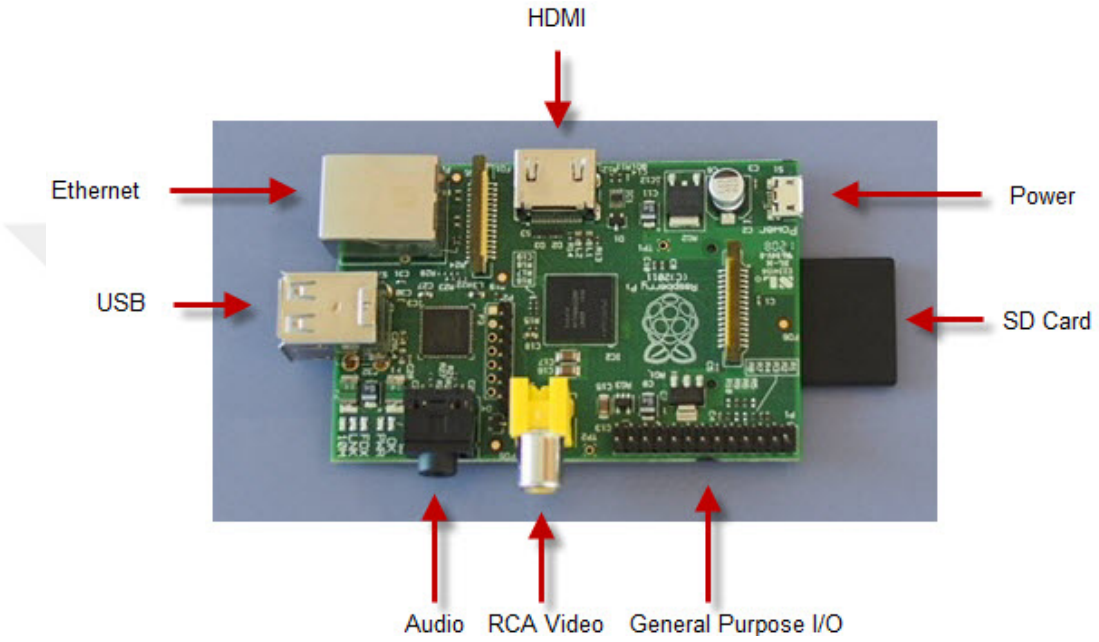
Raspberry Pi, ilk modellerinde ARM1176JZF-S 700 MHz merkezi işlem birimini içeren Broadcom BCM2835 mikroçipi üzerine kurulmuştur. Daha sonra piyasaya çıkan Raspberry Pi 2 modelinde Broadcom BCM2836 kullanmıştır. VideoCore IV GPU grafik işlem birimine sahiptir. Booting ve veri depolaması için SD kart kullanır. Üzerinde USB 2.0 portları, HDMI video çıkışı, ses çıkışı, MIPI kamera girişi, GPIO arayüzü ve 5V MicroUSB güç girişi bulunmaktadır [38]. Tez süresi boyunca Raspberry Pi Model B ve işletim sistemi olarak Raspberry Pi Foundation tarafından sağlanan Raspbian kullanılmıştır.

Raspberry Pi Model B'nin Teknik Özelliklerini sıralayacak olursak [39];

- Broadcom BCM2835 İşlemci
- 700 MHz ARM1176JZF-S tek çekirdekli CPU
- Broadcom VideoCore IV GPU
- 512 MB RAM
- 2 x USB2.0 Port
- Compozit (PAL ve NTSC), HDMI ya da Raw LCD (DSI) üzerinden video çıkışı
- 3.5mm Jack veya HDMI üzerinden ses çıkışı
- Depolama Alanı: SD/MMC/SDIO
- 10/100 Ethernet (RJ45)
- GPIO pinleri (26 adet)
- Düşük Seviyeli Çevre Birimleri:
  - 8 x GPIO
  - UART
  - SPI-2 CS ucu
  - +3.3V
  - +5V
  - Toprak

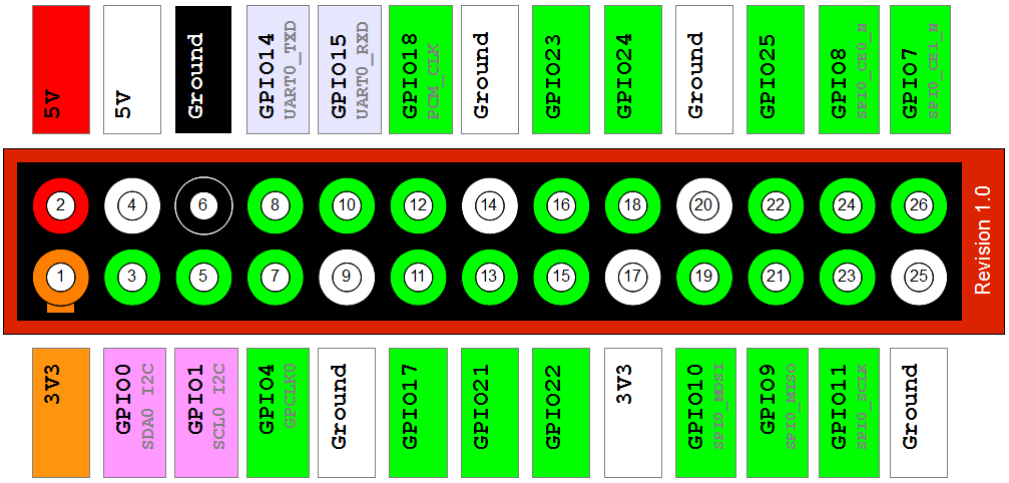
- Güç Gereksinimleri: 5V @ 700 mA, MicroUSB veya GPIO Başlığı üzerinden
- Debian GNU/Linux, Fedora, Arch Linux, RISC OS vb. işletim sistemlerini destekler.

İşletim sistemi sd karta kurulur ve buradan başlatılır. Genel amaçlı giriş çıkış pinlerinin lojik gerilim seviyesi 3.3V DC' dir. GPIO pinleri giriş veya çıkış olarak kullanılabilir.



Şekil 4.2: Raspberry Pi'nin ethernet, hdmi, usb, gpio pin, vb gösterimi

GPIO pinlerinde low durumu 0V, high durumu ise 3,3V olarak gösterilir [40].



Şekil 4.3: GPIO pin gösterimi

Tez süresi boyunca 12. pin GPIO 18 çıkış 25. pin ground olarak tanımlanmıştır.

Raspberry Pi nin sahip olduğu işlemci (BCM2835) armv6 mimarisine sahip 32 bitlik bir işlemcidir. Yapı olarak yüksek hızlı ve yüksek performanslı olması nedeniyle gömülü işlemci olarak kullanılması uygundur. Raspberry Pi ile birleştiğinde normal bir bilgisayarın yapabildiği birçok işlemi rahatlıkla yapabilmektedir. Evde sunucu olarak kullanma, yazılım geliştirme, dosya indirme platformlarında 7/24 açık tutup bir "seedbox"a dönüştürüp kullanma, 1080p videoları rahatlıkla açabildiğinden bir media center a dönüştürme için kullanmaktadır [37].

Tezi yaparken platform olarak Raspberry Pi nin kullanılmasının nedeni, karmaşık işletim sistemi ve çevre birimlerine sahip olmasıdır. Motivasyon kaynağı, bir işletim sistemi üzerinde çalışan AES algoritmasının kırılmasıdır. İşletim sistemi ile belirtilmek istenilen şey sadece belli işlemleri yapan kısıtlı bir işletim sistemi olmaması. İşletim sisteminin arka planda kendi çalışma prensibi gereği yaptığı işlemlerden kaynaklı yaydığı elektromanyetik radyasyon, giriş çıkış birimlerinin kullanılmasıyla yayılan radyasyon, tez için kullanılan programın çalışma süreci boyunca yayılan radyasyon vb. Örnekler daha da çoğaltılabilir. Örneklerin çoğaltılması işin aslında o kadar karışık ve zor olduğu gösteren bir durumdur. Bu da başlıca motivasyon kaynağıdır. Örneğin akıllı kartlarda bulunan işletim sistemleri, ya da FPGA üzerinde gerçeklenmiş bir AES algoritmasının yan kanal analizi ile kırılması -önlem alınmamışsa- çok daha kolaydır. Nedeni gürültünün az olması, kullanılan işletim sistemiyle kısıtlı işlemlerin yapılıyor olması ya da kullanılan platformun sadece şifreleme ve şifre çözme işlemi yapıyor olması gösterilebilir.

Bölüm 5

Gelişmiş Kodlama Standardı Algoritması (AES)

DES algoritması NSA tarafından değiştirilmiş ve NIST tarafından standartlaştırılmış olan bir simetrik şifreleme algoritmasıdır. DES algoritması NIST tarafından 15 Ocak 1977 tarihinde FIPS PUB 46 olarak yayınlanmıştır [41]. 20 yılı aşkın süre boyunca kullanılmıştır. DES in yaşam sürecine bakıldığında NIST tarafından 1983, 1988, 1993 ve 1999'da tekrar teyit edilmiştir [42]. Standart 1983 yılında FIPS PUB 46-1, 1993 yılında FIPS PUB 46-2 ve 1999 yılında FIPS 46-3 TDES olarak yayınlanmıştır. 19 Mayıs 2005 te FIPS PUB 46 kaldırılmıştır.

DES algoritmasının kriptoanaliz sürecine bakıldığında, karşılaşılan sorunlardan birisi diferansiyel ve doğrusal ataklara karşı zayıflığıdır. Değişen ve gelişen teknoloji ile paralel işlemcili bilgisayarların kullanılması DES in daha kısa zamanda kırılmasını mümkün hale getirmiştir [7]. 2 Ocak 1997 de NIST yine simetrik şifreleme algoritması için bir yarışma yaptı ve tartışma formu başlattı. Yapılacak olan yarışmanın sonunda çıkacak olan algoritmanın DES in yerini alması bekleniyordu. AES in standartlaşma süreci incelenecek olursa: 2 Eylül 1997 yılında 15 algoritma başvurusu gerçekleştirildi. Ağustos 1999'te finale 5 algoritma kaldı; Rijndael, Serpent, MARS, RC6, Twofish. 2 Ekim 2000 yılında NIST kazanan algoritmayı Rijndael i anons etti [22]. 26 Kasım 2001 yılında NIST Standard olarak FIPS PUB 197' yi yayınladı [43].

Tablo 5.1: Tur Sayısı ve Anahtar Uzunluğu İlişkisi

AES	Anahtar Uzunluğu (N_k Kelime)	Anahtar Uzunluğu (bit)	Blok Uzunluğu (bit)	Tur Sayısı (N_r)
AES-128	4	128	128	10
AES-192	6	192	128	12
AES-256	8	256	128	14

5.1 AES Algoritması ve Tur İşlemleri

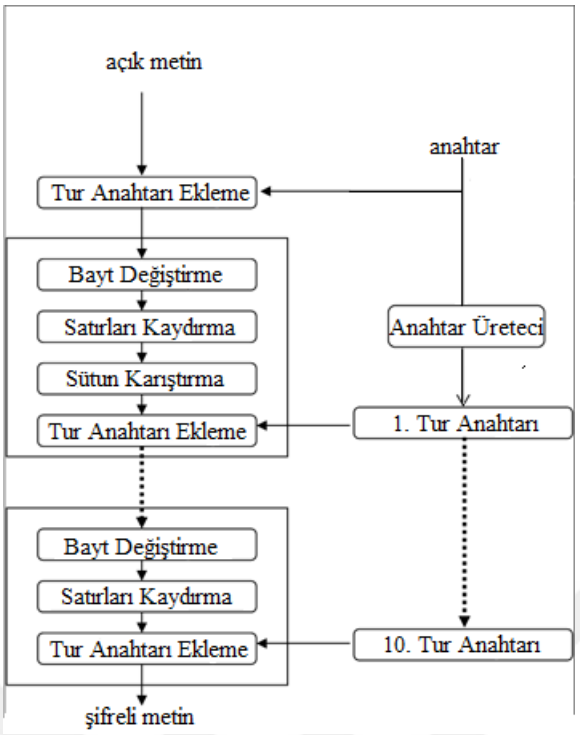
AES algoritmasında veri şifreleme ve çözme işlemi yapılırken Galois sonlu uzayı kullanmaktadır [44]. AES algoritması için kullanılan Galois Sonlu Uzayı' ndaki ($GF\left(2^8\right)$) aritmetik işlemlerden toplama ve çarpma bölüm 2.1.5 te anlatılmıştır.

AES algoritması 128, 192 ve 256 bitlik şifreleme anahtarlarını kullanarak, 128 bitlik veriyi işleyen blok şifrelemesi olan simetrik şifreleme algoritmasıdır. Kullandığı anahtar uzunluğuna göre AES-128, AES-192 ve AES-256 olmak üzere üç çeşittir [43]. Bu tezde 128 bit anahtar uzunluğuna sahip çeşidi AES-128 kullanılmıştır.

Algoritma içerisinde belirli sayılarda tekrarlanan işlemlerden oluşan turlar vardır. Bu turların tekrarlanma sayısı kullanılan anahtar uzunluğuna göre değişir. 128 bit anahtar uzunluğunun kullanıldığı AES algoritmasında şifreleme sırasında 10 tur(çevrim) yapılırken, 192 bitlik anahtar uzunluğu için 12 ve 256 bitlik anahtar uzunluğu için 14 tur yapılmaktadır. Tur sayısı, blok uzunluğu ve anahtar uzunluğunu eşleştirilmesi Tablo 5.1 de gösterilmiştir.

Algoritmada temel olarak iki süreç vardır. Bunlar şifreleme/çözme süreci ve anahtar üretme sürecidir. AES-128 şifrelemede, 10 tur işlemi yapılıyorken aynı zamanda her bir turda farklı anahtar kullanılıyor. Bu farklı anahtarlar anahtar üretme sürecinde oluşturulmaktadır. AES-128 algoritmasının genel yapısı Şekil 5.1 de verilmiştir.

Şifreleme/Şifre Çözme işlemi sırasıyla anahtar toplaması, 9 tane tur çevrimi ve son olarak da 10. tur işleminden oluşur [44]. 10. turun farklı olarak ele alınmasının nedeni diğer turlardan farklı olarak sütün karıştırma işleminin yapılmıyor oluşudur. 128 bitlik veri, ilk olarak ana anahtar ile bit bit 'xor' işlemine tabi tutulur [44]. Daha sonra her bir turda, tur işlemi olan bayt değiştirme, satır kaydırma, sütun karıştırma ve tur anahtarı ekleme işlemi yapılır. Tur anahtarı ana anahtardan oluşturulur ve bir sonraki tur anahtarı



Şekil 5.1: AES-128 algoritmasının genel yapısı

Tablo 5.2: Durum Matrisi

D_0	D_4	D_8	D_{12}
D_1	D_5	D_9	D_{13}
D_2	D_6	D_{10}	D_{14}
D_3	D_7	D_{11}	D_{15}

oluşumunda girdi olarak kullanılır. 9 tur bu şekilde gerçekleştirildikten sonra son turda sütun karıştırma işlemi yapılmadan bir önceki turlarda yapılan işlemlerin aynısı yapılır ve şifrelenmiş/kapalı veri elde edilmiş olur. AES işlemi ile şifreleme işleminin yapılabilmesi için öncelikle verinin durum matrisinin oluşturulması gereklidir. Bu durum matrisinde 16 baytlık veri 4x4 lük bir matris halini alır. Durum matrisi Tablo 5.2de verilmiştir.

Veriler durum matrisi haline getirildikten sonra tur dönüşüm işlemleri yapılabilir. Tur dönüşüm işlemleri aşağıdaki bölümlerde kısaca anlatılmıştır.

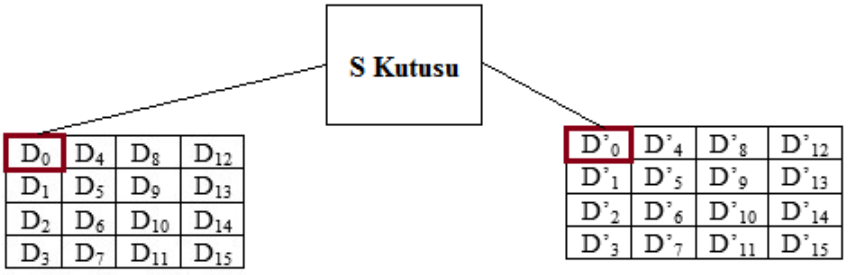
5.1.1 Bayt Değiştirme

Tur işlemlerinin ilkidir. Durum matrisi oluşturulduktan sonra 4x4 lük matris içerisinde yer alan her bir bayt Şekil 5.2 de verilen S kutusu tablosundan eşleştirme yapılarak değiştirilir. S kutusuyla bayt değiştirme işlemi AES algoritması içerisinde yapılan doğrusal olmayan (non-lineer) tek işlemdir. S kutusunda yer alan değerler, Galois Alanı'nda $GF\left(2^8\right)$, her 8 bitlik kısmın indirgeme polinomu ile çarpmaya göre ters alma işlemi yapıldıktan sonra doğrusal bir dönüşüme sokularak bulunmuş olur [7].

	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 5.2: S Kutusu

Bayt değiştirme işlemi yapılırken dönüştürülecek olan baytın hexadecimal değeri alınır. Baytın yüksek değerli 4 biti S kutusunun satırını, düşük değerli 4 biti ise sütununu gösterir. S kutusu tablosu üzerinde satır ve sütunun kesiştiği yer değiştirilecek olan baytın yerini alacak değerdir.

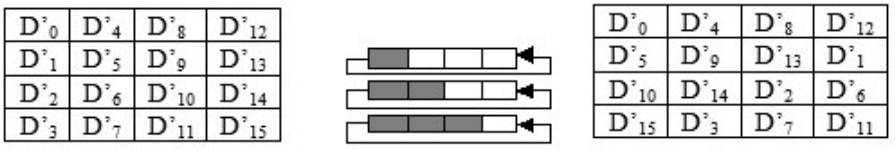


Şekil 5.3: Bayt değiştirme işlemi

Bayt değiştirme işleminin tersi alınabilir.

5.1.2 Satırları Kaydırma

Satır kaydırma işlemi bayt değiştirme adımından sonra gelen, ikinci adım işlemidir. Bayt değiştirme işleminin ardından elde edilen 4x4 lük matrisin satırlarında kaydırma işlemi yapılır. İlk satırda Şekil 5.4 de gösterildiği gibi herhangi bir kaydırma işlemi yapılmaz, sabit tutulur. İkinci satırda sağdan sola doğru olmak üzere bir adım kaydırılır. Üçüncü satırda yine sağdan sola doğru olmak üzere iki adım, son satırda ise üç adım kaydırma işlemi yapılır. Tersi işlem ise Şekil 5.5 de verildiği gibi yapılır. Yine ilk satırda herhangi bir işlem uygulanmaz. İkinci satırda bu kez soldan sağa doğru bir adım kaydırma işlemi yapılır. Üçüncü satırda soldan sağa doğru iki adım ve son satırda 3 adım kaydırma işlemi yapılır. Satır kaydırma tersi işlemi şifre çözülürken kullanılır.



Şekil 5.4: Satır kaydırma işlemi

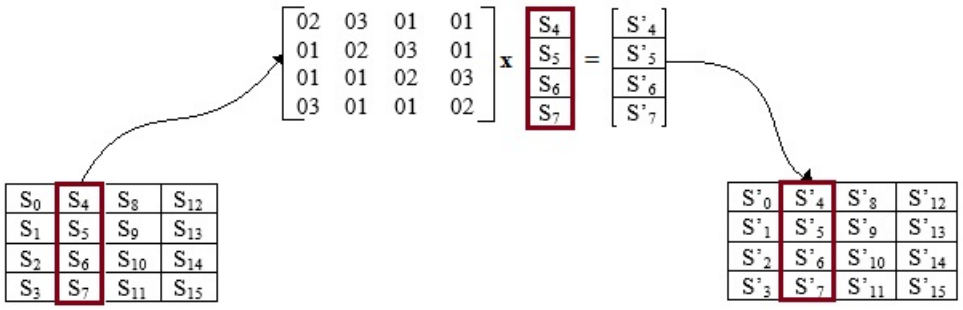
Şekil 5.5: Satır kaydırma ters işlemi

5.1.3 Sütun Karıştırma

Sütun karıştırma işlemi, satır kaydırmadan sonra yapılan üçüncü tur işlemidir. Şifre çözme işlemi sırasında sütun karıştırma işleminin tersi işlem yapılır [44]. Sütun karışma işleminde sadece sütunlar üzerinde işlem yapılır. İşlemler gerçeklenirken her bir sütun, katsayıları $GF\left(2^8\right)$ in elemanı olan üçüncü derecenden bir polinom olarak düşünülür. Polinom olarak düşünülen bu satır sabit $a\left(x\right) = \{03\}\, x^3 + \{01\}\, x^2 + (01)\, x + \{02\}$polinomu ile modülo $\left(x^4 + 1\right)$ çarpılır. İşlem sonucu elde edilen yeni polinom $S'\left(x\right)$ ve karıştırma işlemi yapmadan önceki sütunların oluşturduğu polinom da $s\left(x\right)$ olarak adlandırılacak olursa;

$$s'\left(x\right) = a\left(x\right) \cdot s\left(x\right)$$

olarak gösterilir. Sütun karıştırma işlemi Şekil 5.6 de gösterilmiştir.



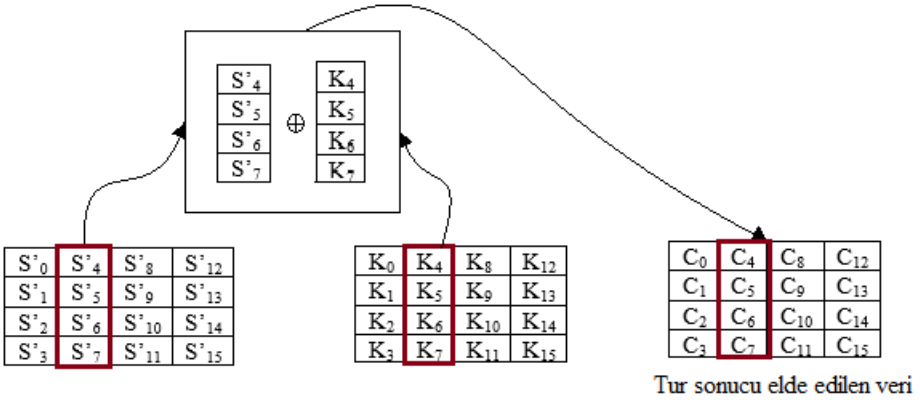
Şekil 5.6: Sütun karıştırma işlemi

Şifre çözme işlemi yapılırken sütun karıştırma işleminin tersi işlem uygulanır. Her bir sütun yine üçüncü dereceden bir polinom olarak düşünülür ve sabit bir polinom olan $b(x)$ ile modülo (x^4+1) de çarpılmaktadır. Şifre çözmede kullanılan sabit polinom $GF(2^8)$ şifrelemede kullanılan sabit polinomun çarpmaya göre tersi olarak hesaplanır.

$$b(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

5.1.4 Tur Anahtarı Ekleme

Sütun karıştırma işleminden sonra gelen tur işlemlerinin sonuncusudur. Şifreleme yaparken ve çözerken aynı dönüşüm kullanılmaktadır. Tersi kendisine eşit olan bir dönüşümdür [18]. Tur anahtarı ekleme işlemi, sütun karıştırma işlemi gerçekleştirildikten sonra elde edilen matris ile 128 bitlik tur anahtarı matrisinin 'xor' lanması ile yapılır. Şekil 5.7 da tur anahtarı ekleme işlemi gösterilmiştir.



Şekil 5.7: Tur anahtarı ekleme işlemi

TABLO 5.3: Ana üretici ilk N_k sütun

K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

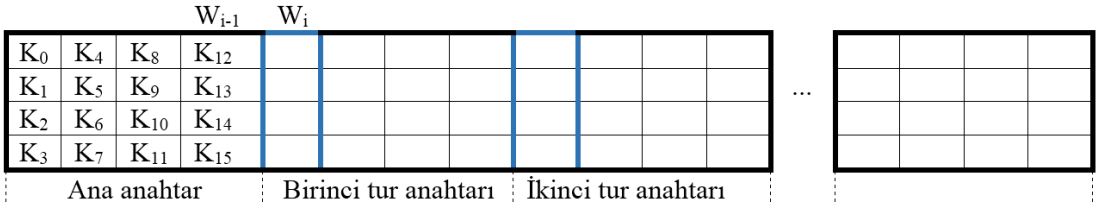
5.2 Anahtar Üretimi

Anahtar üreteci her bir turun son adımında kullanılacak olan anahtarları oluşturur. Tur sayısı kadar anahtar üretilir. Anahtarların boyu 128 bittir. Üretilen bu anahtarlar 4x4 lük matris olarak ele alınır. Tur sonunda eklenen bu anahtarlar başlangıç anahtarı olan ana anahtardan üretilirler. Üretilirken anahtar üretme fonksiyonu kullanılır.

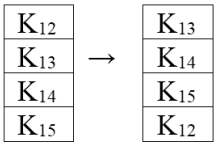
Matrisin ilk N_k sütunu ana anahtar matrisi olarak yazılır. Tablo 5.3 den ana anahtarın yazımını görülebilir.

Tur anahtarlarının oluşumunu bir dizi olarak düşünürsek [45]:

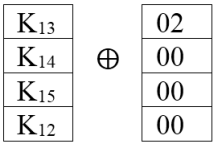
- İlk 4 sütuna ana anahtar yerleştirilir.
- Sonraki sütunları oluşturmak için, kendisinden bir önceki sütun ile NK önceki sütuna baytlar karşılıklı olacak şekilde 'xor' işlemi uygulanır.
- Xor işlemi uygulanacak olan sütün NK nın tam katı ise kendisinden bir önceki sütun bir dönüşüm işleminden geçirilir. (Örneğin Wi nin oluşturulması Şekil 5.8)
  - Dönüşümümün ilk adımında kendisinden bir önceki sütun ele alınır. Bu sütunun ilk satırında bir adım kaydırma işlemi yapılır. Bu işlem aşağıdan yukarı olmak üzere satırların bir satır yukarı kaymasıyla oluşur. Örnek olarak bkz. Şekil 5.9
  - Dönüşümün ikinci adımında ise kaydırma işlemi yapılan bu sütun bayt karıştırma işlemine tabi tutulur. Bayt karıştırma işlemi için S kutusu kullanılır. Bayt karıştırma işleminin detayları için bölüm 5.1.1 incelenebilir.
  - Dönüşümün son adımında ise elde edilen sütun tur sabiti ile baytlar karşılıklı olacak şekilde xor işlemine tabi tutulur. Bu durum için Şekil 5.10 a bakılabilir.



Şekil 5.8: Anahtar üreteci dizisi



Şekil 5.9: Sütun kaydırma işlemi



Şekil 5.10: Tur sabiti ile xor işlemi yapılması

Tablo 5.4: Anahtar üretici tur sabiti

Tur Sayısı	Tur Sabiti	Tur Sayısı	Tur Sabiti
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

Tur sabitleri bir tablo ile gösterilecek olursa Tablo 5.4 e bakılabilir.

Bölüm 6

Raspberry Pi Üzerinde Gerçeklenen AES Algoritması Ve Ölçüm Düzeneği

Bu bölümde tez süresi boyunca çalışılan sistemden bahsedilmiştir. Sistem içerisinden kullanılan yazılımlar, ölçüm alma sistemi için kullanılan araçlar, ölçüm düzeneği ve ölçüm alma anlatılmıştır.

6.1 Elektromanyetik Alan Alıcısı Sistemi

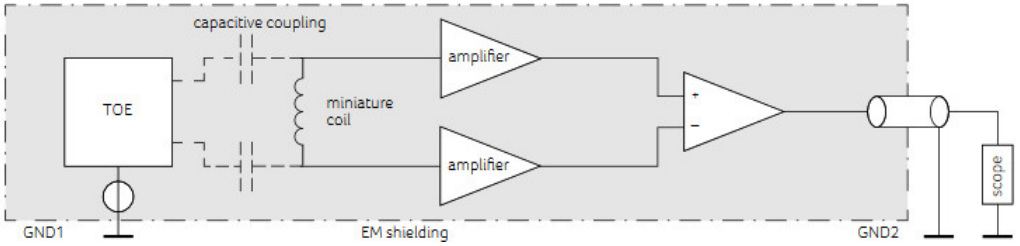
Ölçümleri almak için alıcı/anten olarak Riscure' nin "EM Probe Station" güvenlik aracının problarından yüksek hassasiyetli probu kullanılmıştır. Şekil 6.1 de yüksek hassasiyetli prob verilmiştir. Bu prob için kullanılan farksal yükselteç 15pT /$\sqrt{Hz}$@1MHz lik bir manyetik gürültüyle çalışır [46]. Yüksek hassasiyetli probun genel kullanım amacı düşük gerilimli EM sızıntılarını almaktır.

Riscure' nin bu güvenlik aracı özellikle EM yan kanal analizi için hazırlanmıştır. EM Prob İstasyonu, yapılandırma, ölçme ve daha sonra kripto analizi gerçekleştirmek için "inspector" yazılımıyla entegre olan üç donanım bileşeni, iki EM probu ve motorize bir XYZ tablosundan oluşur. Bununla birlikte, sınırlı sayıda iz ile iyi sonuçlar elde etmek için yüksek kalite (yani, düşük gürültü ve geniş bant genişliği) sağlayan ölçüm cihazı/osiloskop

Şekil 6.1: Yüksek hassasiyetli EM alan alıcısı

önemlidir. Ayrıca, Yan Kanal Analizi için elde edilen sinyalin kalitesi, analiz edilen cihaza göre probun konumuna bağlıdır.

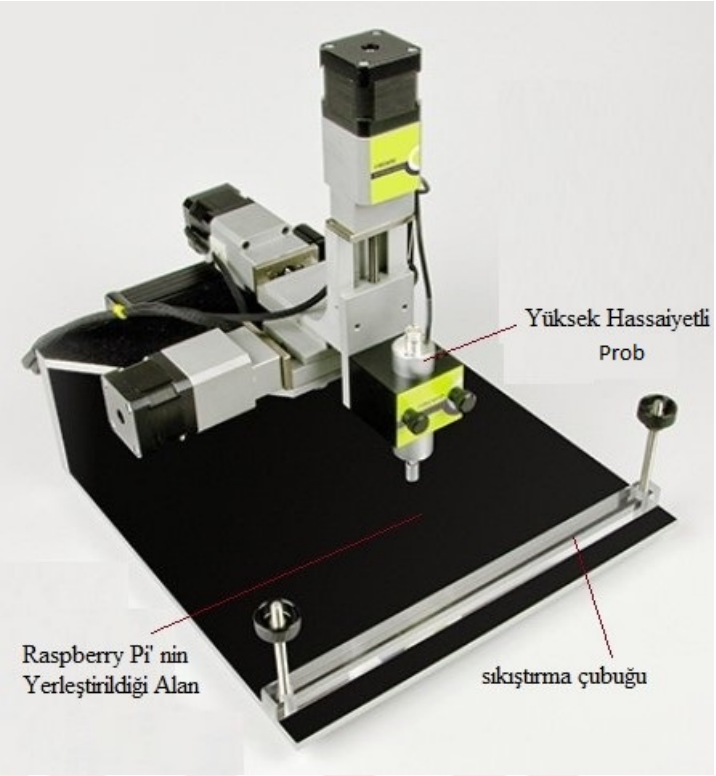
Yüksek hassasiyetli prob, çiplerdeki küçük akım döngülerinden gelen zayıf emisyonları ölçebilir ve tipik olarak en gelişmiş akıllı kart için 1V genlikli bir sinyal üretir. Düşük hassasiyetli prob, temassız kartların ve gömülü işlemcilerin güçlü emisyonlu analizleri için tasarlanmıştır. Şekil 6.2 de EM probun kavramsal özetini gösteren bir şekil verilmiştir [46].



Şekil 6.2: EM probun kavramsal özeti

Tez süresi boyunca yüksek hassasiyetli prob ve Raspberry Pi' nin ölçüm alma sırasında oynamaması için EM Prob İstasyonunun masası kullanılmıştır. Şekil 6.3 de Raspberry Pi' nin sabitlenmesi/sıkıştırılması için kullanılan EM Prob İstasyonu'nun görüntüsü verilmiştir.

Yüksek Hassasiyetli prob BNC kablo yardımıyla osiloskoba bağlanır. Raspberry Pi' nin bir kısmı sıkıştırma çubuğunun altında kalacak şekilde sıkıştırılır.



Şekil 6.3: EM Prob İstasyonu

6.2 Elektromanyetik Analiz İçin Kullanılan Yazılımlar

Bu bölümde ölçüm alma işlemi tamamlanana kadar tez boyunca kullanılmış olan yazılımlar anlatılmıştır. Ölçüm düzeneğinin ayrıntıları bölüm 6.3 de detaylı olarak verilmiştir. Bunun haricinde şifreleme için kullanılacak veriler, her satırı 16 baytlık hexadecimal formatta olacak şekilde 500 bin satırdan oluşturulmuştur. Oluşturulan bu veriler "plain.txt" olarak adlandırılmıştır. Amaç ilk etapta yaklaşık 500 bin ölçüm ile anahtarı bulmaktır.

EM Analiz için üç yazılım kullanılmıştır. Bu yazılımlardan bir tanesi Raspberry Pi üzerinde C dilinde yazılmış ve derlenmiş AES algoritmasını içeren programdır. Bu program "RAW-AES" olarak adlandırılmıştır. Program ilk derlendiğinde, Raspberry Pi nin komut satırından şifrelenecek olan veri girilerek çalıştırılıyordu. Şifreleme için kullanılacak anahtar kodun içerisinde gömülmüştür. Çalıştırılan program şifrelenmiş veriyi Raspberry Pi nin ekranına basılıyordu.

Yazılan programın doğru çalıştığının kontrolü yapıldı. Ardından osiloskoptan alınacak olan ölçümün kaydedilebilmesi için osiloskobun tetik alması işinin yapılması gerekiyordu. Raspberry Pi nin 12. pini GPIO-18, osiloskoba tetik vermek için kullanıldı. Raspberry

Pi nin bu pini ile Şekil 6.4 de gösterilen program sayesinde 3V luk çıkış alındı. Bu çıkış osiloskobun analog kanallarından bir tanesine verildi. Analog girişin 3V luk gerilimi almasıyla osiloskop tetik almıştır. Şifrelemenin başlamasıyla Raspberry Pi 3V, şifrelemenin bitmesiyle ise 0V gerilim vermiştir. Böylelikle şifrelemenin başlangıç ve bitimi belirlenmiş, osiloskobun bu süre boyunca ölçümü kaydetmesi sağlanmıştır.

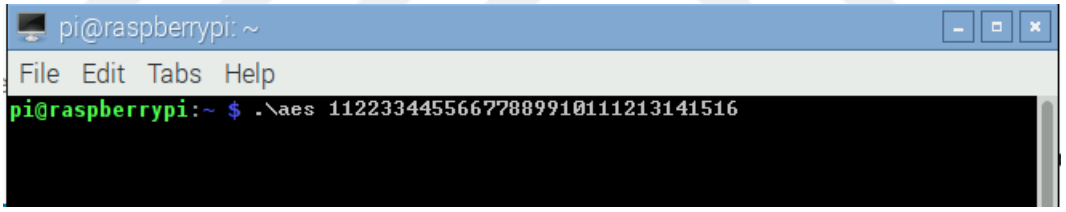
```
#define LED RPI_GPIO_P1_12
        bmc2835_gpio_fsel(LED, BCM2835_GPIO_OUTP);

                if( ! bcm2835_init() )
            return 1;

        bcm2835_gpio_clr(LED);
        bcm2835_gpio_set(LED);
...
    aes algoritması
...
        bcm2835_gpio_clr(LED);
```

ŞEKIL 6.4: Raspberry Pi nin 12. pinin tetik olarak alınmasını sağlayan program parçası

Böylelikle manuel olarak komut satırından Şekil 6.5 deki gibi şifrelenecek olan veri giriliyor, ölçüm yine elle kaydediliyor ve sonuç ekran basılıyordu.



ŞEKIL 6.5: Şifrelenecek olan verinin elle girilmesi

Sistemin otomatize edilmesi için başka yazılımlara ihtiyaç duyuldu. Bu yazılım komut satırına şifrelenecek olan veriyi otomatik olarak vermeliydi. Şifreleme sonunda ekrana basılan veriyi de başka bir yere kaydetmeliydi. Bu işlemin gerçekleştirilmesi için iki program daha yazıldı.

Sistem otomatikleştirme için kullanılan yazılımlardan birisi PC üzerinde çalışan ve "ÖLÇÜM-KODU" diye adlandırılan yazılımdır. Bu yazılım C++ dilinde yazılmıştır. Program temel olarak osiloskop ve Raspberry Pi ile bağlantı kurup veri kaydetme işlemi yapar. Bunun yanı sıra sistemin otomatik olarak ölçüm almasını sağlayacak olan programdır da denilebilir.

Genel olarak;

- Osiloskop ile bağlantı kurulur. .
- Osiloskobun yapılandırma ayarları yapılır. Bu ayar; Osiloskobun hangi analog kanallarının kullanılacağı, osiloskobun tetik ve emisyon alan kanalı vb. özelliklerin belirlenmesinden oluşur.
- Osiloskoptan kaç tane ölçüm alınacağını ve bu verinin kaç noktadan oluştuğu belirlenir.
- Raspberry Pi den gelen şifrelenmiş veriyi kaydetmek için cipher.txt dosyası oluşturulur.
- Raspberry Pi ile bağlantı kurar ve plain.txt dosyasının ilk satırından okumaya başlayarak şifrelenecek veriyi Raspberry Pi' ye gönderir.
- Osiloskoptan gelen/alınan ölçüm kaydedilir.
- Raspberry Pi den gelen şifrelenmiş veri cipher.txt dosyasına kaydedilir.

İşlemler bu şekilde istenilen ölçüm sayısına ulaşılıncaya kadar devam eder.

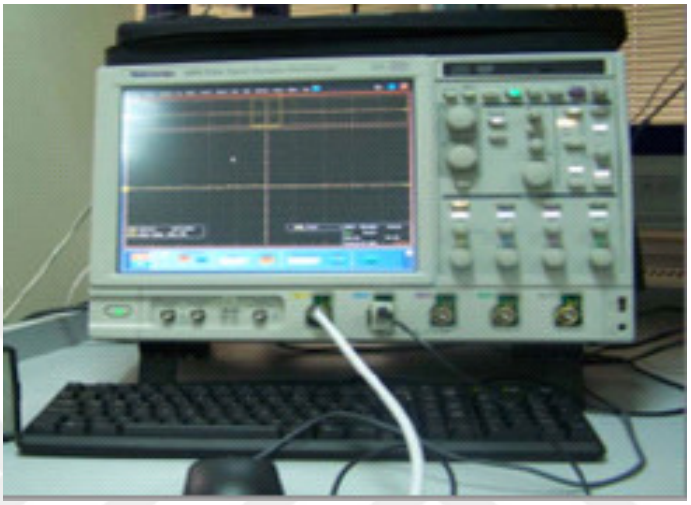
Sistemin otomatik olarak çalışması için gerekli olan son program ise C dilinde yazılmış Raspberry Pi üzerinde çalışan SERVER-KODU olarak adlandırılan programdır. Bir çeşit soket dinleme programı da diyebiliriz. Bu program ise genel olarak;

- Sürekli 5001 numaralı portu dinler.
- Porta gelen veriyi komut satırından çalıştırır.
- Komut satırına basılan sonucu kendisinden istekte bulunan ÖLÇÜM-KODU na gönderir.
- İşlem başarılı bir şekilde gerçekleştirilmişse ekrana başarılı olduğuna dair "successful" uyarısı basar.

Böylelikle sistem otomatik olarak çalışabilecek hale getirilmiş oldu.

6.3 Elektromanyetik Analiz İçin Kurulan Ölçüm Düzeneği

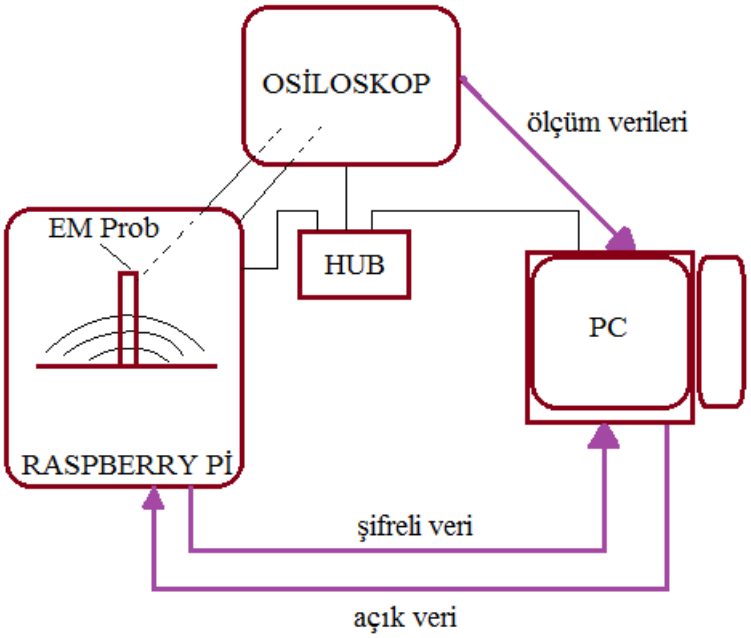
Osiloskop olarak Şekil 6.6 da verilen Tektronix marka bir osiloskop kullanılmıştır. Osiloskobun analog kanallarından bir tanesine yüksek hassasiyetli prob bağlanmıştır. Diğer analog kanallarından bir tanesine ise osiloskobun tetik almasını sağlamak için Raspberry Pi nin 12. pini bağlanmıştır.



Şekil 6.6: EM analiz için kullanılan osiloskop

Raspberry Pi nin 26. pini toprak olarak kullanılmıştır. Raspberry Pi EM Prob İstasyonu'na yerleştirilmiştir. Ölçüm alma sisteminin topolojisi Şekil 6.7 de verilmiştir. Sisteminin çalışma şeklinden bahsedilirse;

- Raspberry Pi üzerinde çalışan SERVER-KOD çalıştırılır. Böylelikle PC KOD dan gelecek olan açık veriler beklenilmeye başlanır.
- PC üzerinde çalışan ÖLÇÜM-KODU çalıştırılır.
- ÖLÇÜM-KODU osiloskopla bağlantı kurar ve gerekli olan ayarları yapar. Cipher.txt dosyasını oluşturur.
- ÖLÇÜM-KODU, SERVER-KODU ile bağlantı kurar.
- ÖLÇÜM-KODU' ndan gelen komutu (çalıştırılacak olan program ve açık veri bkz. şekil 6.5) alan SERVER-KODU, komut satırından RAW-AES' i çalıştırır.
- RAW-AES çalışır. Çalışmasıyla birlikte şifreleme işlemine başlamadan önce 12. pinini 3V a çeker. Böylelikle osiloskop tetik almış olur ve kayda başlar.



ŞEKIL 6.7: Ölçüm alma düzeneği topolojisi

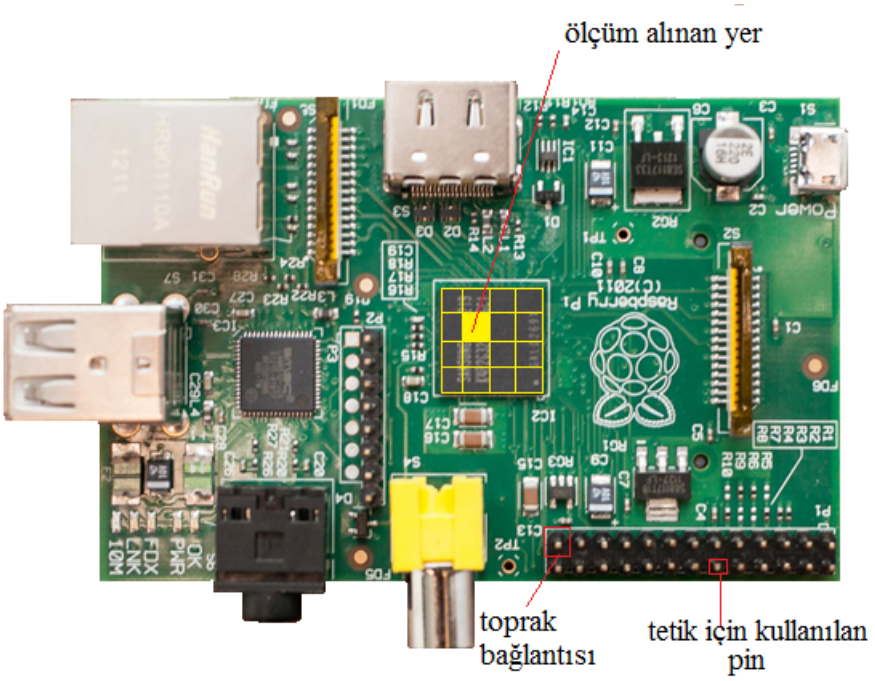
- RAW-AES şifreleme işlemini bitirir ve Raspberry Pi nin 12. pinini 0V' a çeker. Böylece osiloskop ölçümünü bitirmiş olur.
- ÖLÇÜM-KODU osiloskop ile alınan ölçümü kaydeder.
- SERVER-KOD, RAW-AES' in şifrelediği veriyi ÖLÇÜM-KODU' na gönderir.
- ÖLÇÜM-KOD şifreli veriyi cipher.txt ye kaydeder.

ÖLÇÜM-KODU' nda belirtilen sayı adedince bu işlem devam eder.

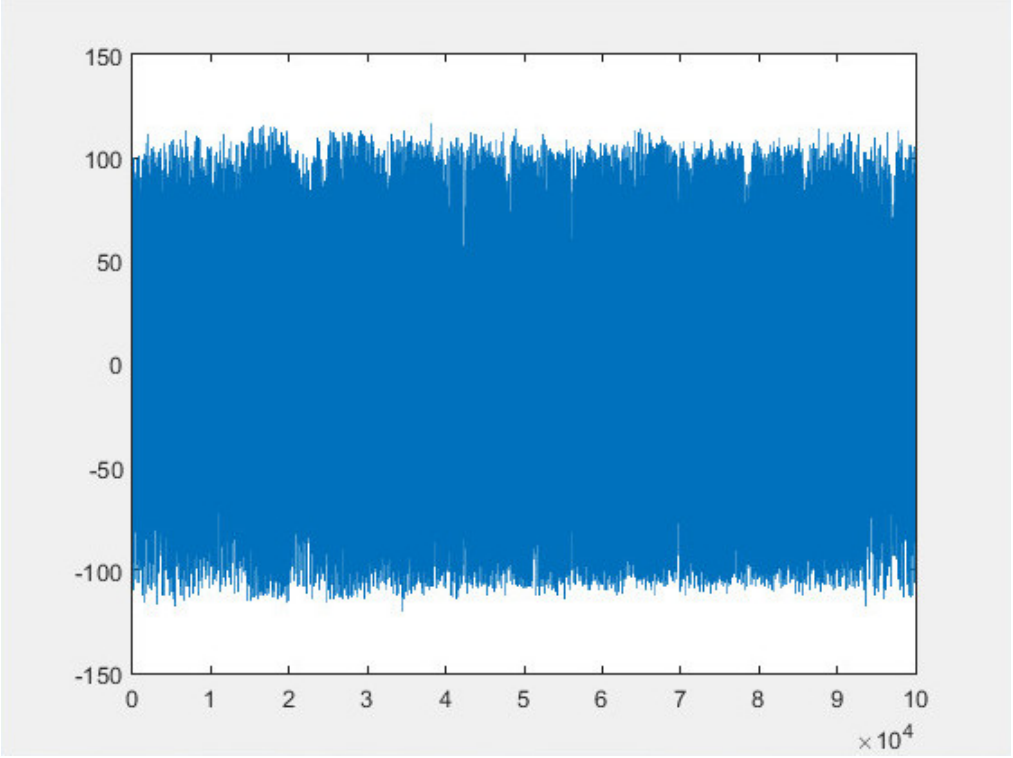
6.4 Ölçüm Alma

Bölüm 6.3' te kurulan düzeneğin ardından ölçüm alma işlemine geçilmiştir. Burada dikkat edilmesi gereken husus EM Prob' un tam olarak konumlandırılması gereken yerdir. İşlemcinin yüzeyi EM Prob' un yüzeyinden, çapından büyüktür. Bu nedenle ölçüm alınacak yerin iyi belirlenmesi gerekir. Çipin yüzeyi şekil 6.8 deki gibi 16 parçaya ayrılmıştır.

Buradan her bir alan için 1000 ölçüm alınarak en ideal yerin tespiti yapılmaya çalışılmıştır. Gürültü nedeniyle bir ölçüm üzerinden yer tespiti yapılamamıştır. Şekil 6.9 da ideal yerden alınan tek ölçüm verilmiştir.

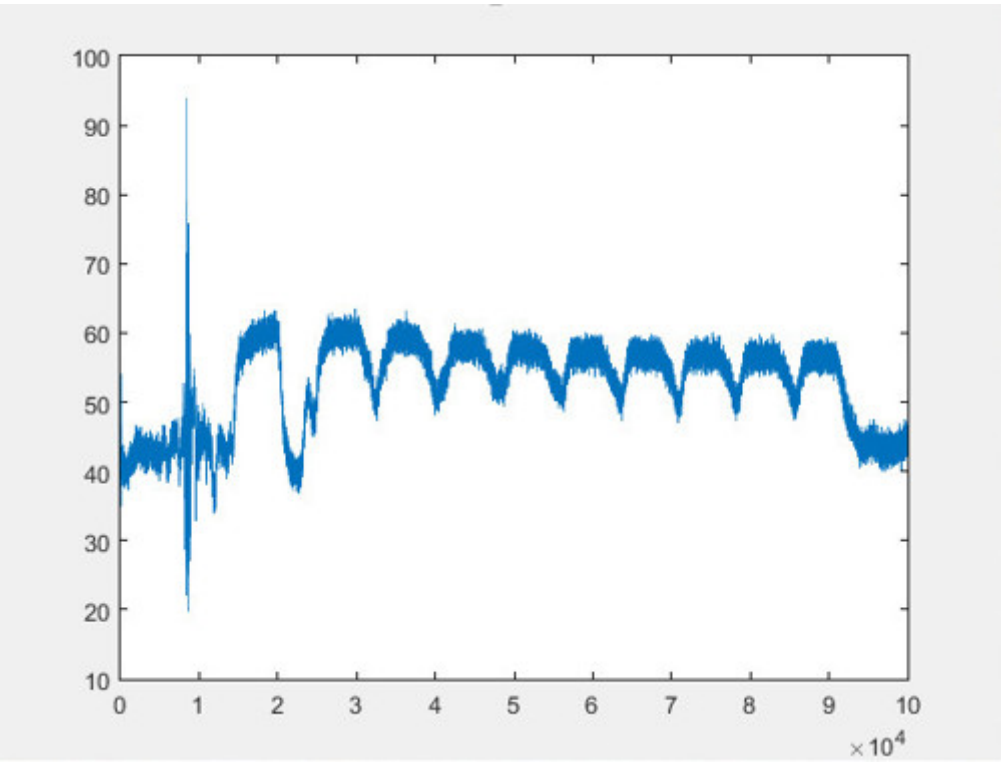


Şekil 6.8: Ölçüm alınacak yer tespiti



Şekil 6.9: İdeal yerden alınan tek ölçüm

Her bölgeden alınan 1000 ölçümün ortalaması incelendi ve uygun olan yerin Şekil 6.8 de işlemcinin sarı ile boyalı olan yerinin olduğuna karar verildi. Uygun yer için 1000 ölçümün ortalamasından elde edilen sonuç şekil 6.10 da verilmiştir. Şekilde görülen pik osiloskobun tetik aldığı yerdir.



Şekil 6.10: Bin ölçüm ile alınan ortalama

Şekil 6.10 dan da görüldüğü gibi AES' in 10 turu net bir şekilde görülmektedir. Görülen bu 10 bölümün gerçekten AES turları olduğundan emin olmak için algoritma içerisinde tur sayısı azaltılıp tekrar kontrol edilmiştir ve bölüm sayısının azaldığı görülmüştür.

Ölçüm alınacak yerin belirlenmesinin ardından 500 Msample/sn lik örnekleme frekansı ile 500 bin ölçüm alınmıştır. Her bir verinin şifrelenmesi esnasında yayılan EM dalga verisi 100.000 nokta ile kaydedilmiştir. Ölçüm sonucu elde edilen 500 bin ölçüm verisinin analiz işlemi için kullanılacağı düşünülmüş, ölçüm miktarının yetersiz kalması durumunda ölçüm sayısının artırılacağı planlanmıştır.

Bölüm 7

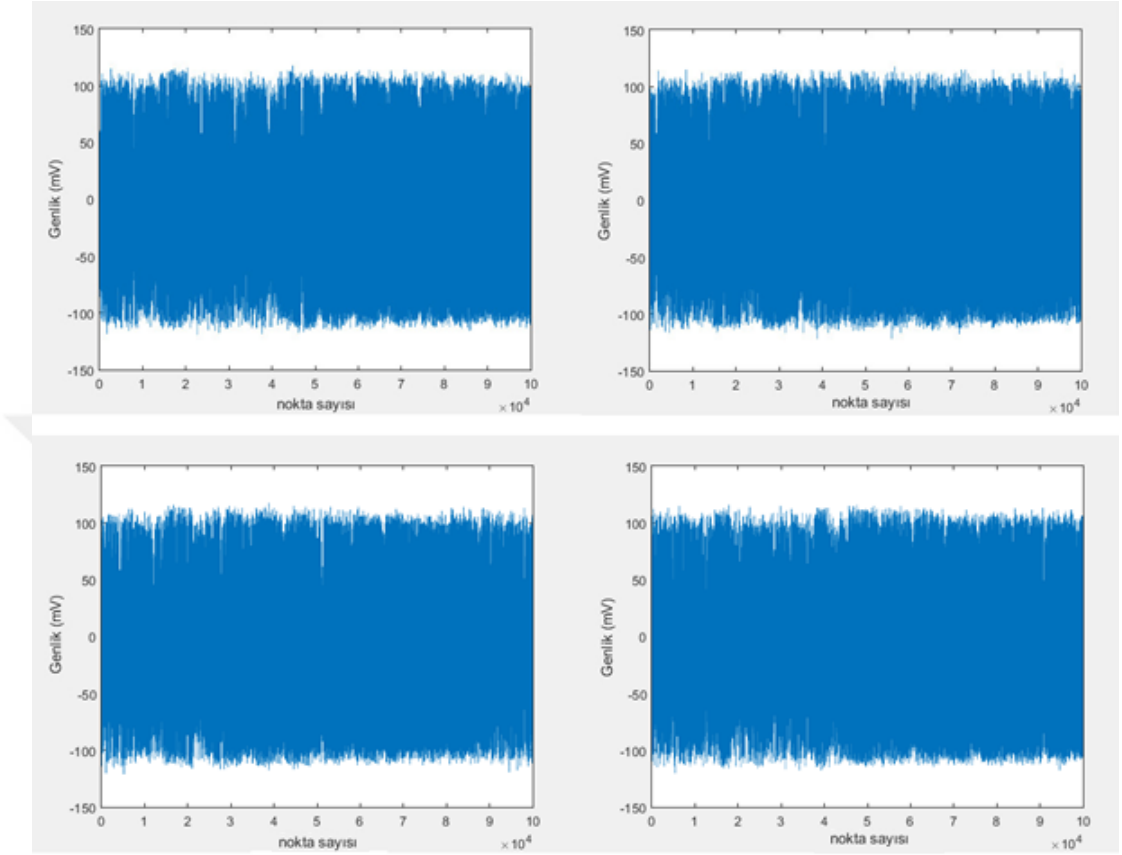
Raspberry Pi Üzerinde Gerçeklenen Elektromanyetik Analiz Saldırıları ve Ölçüm İyileştirmeler

EM yan kanal analizi saldırısının başarılı bir şekilde gerçekleştirilebilmesi için dikkat edilmesi gereken iki temel noktadan bahsedilebilir. Bunlardan birincisi alınan ölçümlerin düzgün olmasıdır. Alıcının özellikleri, alıcının konumdırılma açısı, ölçüm alınan ortamın gürültüsü vb. ölçüm kalitesini etkileyen faktörlerdir. İkinci husus ise ölçüm alındıktan sonra onları analiz için kullanılabilir hale getirmektir. Alınan ölçümün durumuna göre filtre uygulama, ortalama alma vb. işlemlerinin yapılması gerekebilir. Burada bölüm 6 da alınan ölçümlere uygulanan işlemler ve bu işlemler sonucunda yapılan analizler anlatılmıştır.

7.1 Ölçüm İyileştirme İçin Uygulanan Yöntemler

Elde edilen ölçümlerin direk analiz işleminde kullanımı özellikle algoritmanın işletim sistemi üzerinde olması nedeniyle mümkün değildir. Bu nedenle ölçümler üzerinde bir takım işlemler uygulanmıştır. Bu işlemlerden ilk olarak gürültüyü azaltmak ve ölçüm boyutunu küçültmek için her 100 noktada bir örnek alınarak rms işlemi yapılmıştır. Bu işlem yapıldıktan sonra ölçümler tekrar incelendiğinde aynı açık verinin şifrelenmesi esnasında alınan ölçümlerin farklı olduğu görülmüştür. Bu farklılık bazı ölçümlerde çok

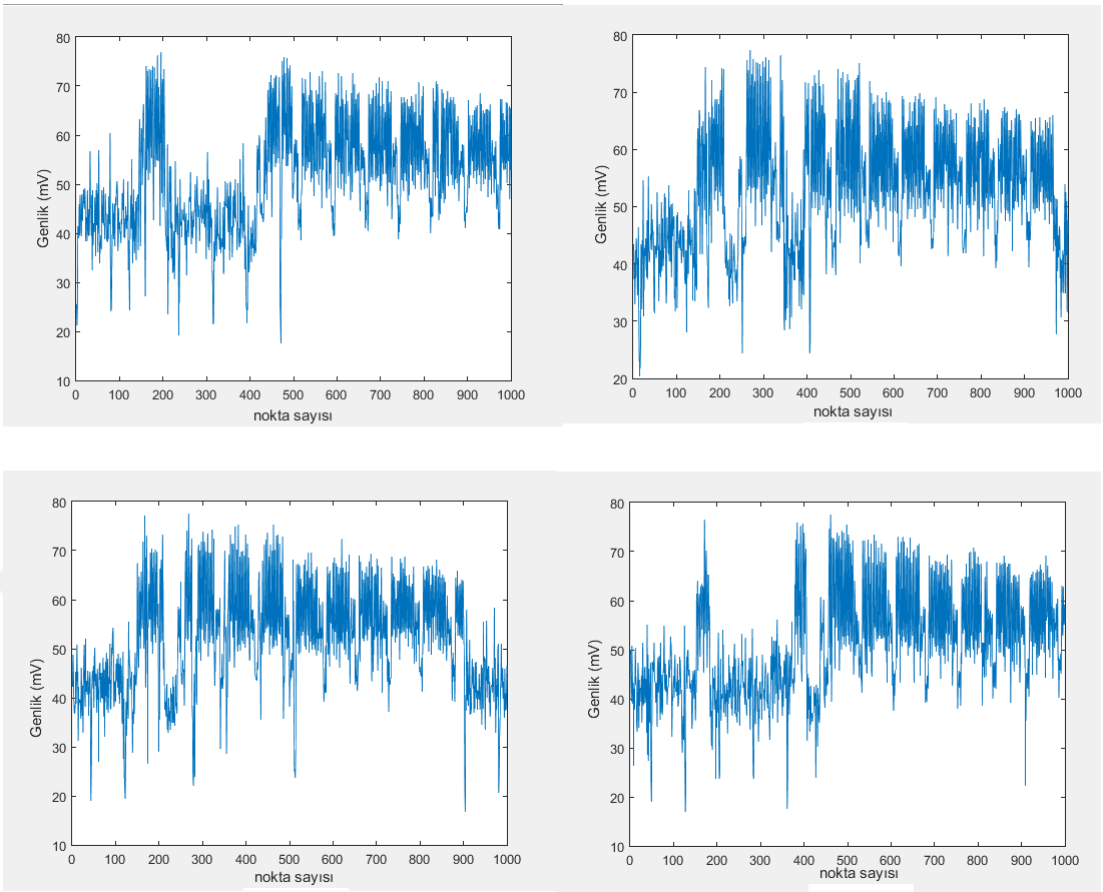
fazla bazı ölçümlerde ise azdır. Nedeni ise algoritmanın işletim sistemi üzerinde çalışıyor olmasıdır. Şekil 7.1 de aynı açık verinin kullanılmasıyla elde edilen örnek dört ölçümün rms alma öncesi ve şekil 7.2 de rms alma sonrası hali verilmiştir.



Şekil 7.1: Alınan örnek bir ölçüm

Yer belirleme işleminde AES turlarının net bir şekilde belli olduğu görülmüştü. RMS alma işleminden sonra ise ölçümler tek tek incelendiğinde turların yeri net, sayısı net olarak görünmemektedir. Çünkü ölçümlerin boyutları birbirine eşit değildir. Bazı ölçümler işletim sistemi nedeni ile istenilen sürede bitmemiş osiloskopta meydana gelen taşma nedeni ile eksik alınmıştır. Çoğunluk beklenilen boyut aralığında olduğu için yer belirlemede ihmal edilebilecek seviyede kalmıştır. RMS alma işleminden sonra elde edilen ölçümler incelenmiş ve saldırının ilk tura yapılmasının daha uygun olduğuna karar verilmiştir. Sıradaki işlem ilk tur ölçümlerinin sıralanmasıdır. Şifrelemenin başlangıç ve bitiş süreleri aynı olmadığı için hizalama işleminin yapılması gerekmektedir. Buradan sırasıyla aşağıdaki işlemler gerçekleştirilmiştir.

- RMS' i alınan ölçümlerin 100:300 arası noktalarının birinci tura geldiği tahmini ile işleme başlandı.



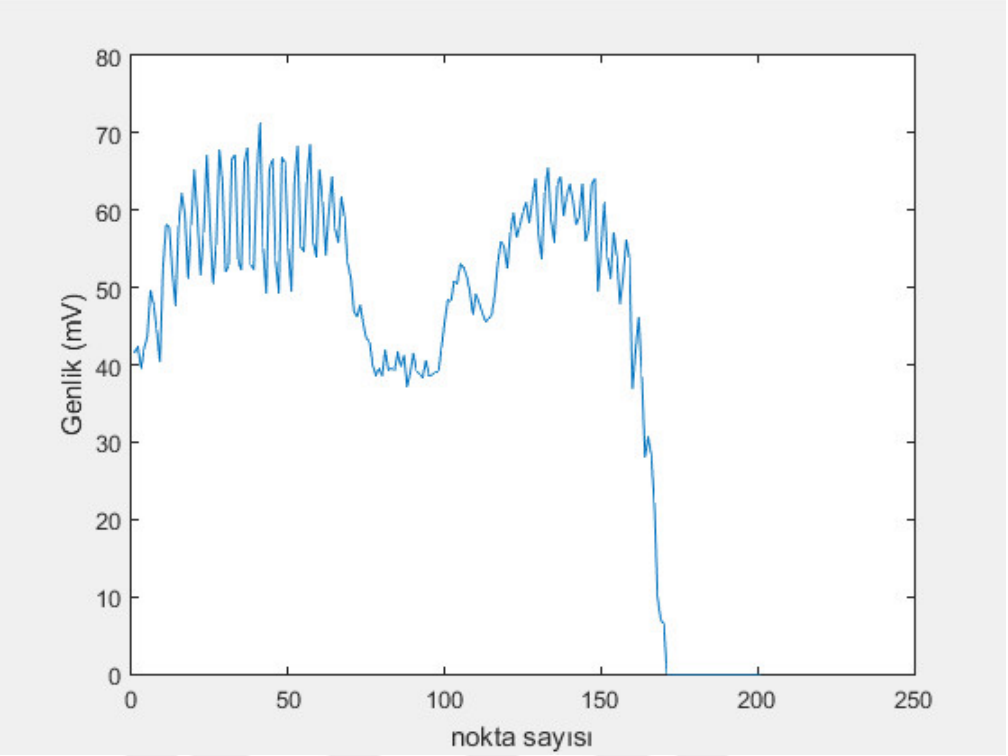
Şekil 7.2: Alınan örnek ölçümün rms i alınmış hali

- RMS' i alınan tüm ölçümlerin sadece bu kısımları ile işlem yapıldı.
- Bir ölçümün 100:300 arası noktası ilk tur olarak tahmin edilip referans ölçüm olarak kabul edildi.
- Referans olarak alınan tur diğer ölçümleri hizalamak amacıyla kullanıldı.
- Hizalama işlemi yapılırken her bir ölçümün 100:300 nokta arası referans ölçüm ile korelasyon işlemine tabi tutuldu.
- Korelasyon oranı en yüksek çıkan noktaya göre hizalama işlemi gerçekleştirildi.

Hizalama işlemi gerçekleştirilmiş bir örnek Şekil 7.3' te verilmiştir.

7.1.1 Aynı Açık Metinlerin Ortalamasının Alınması

Şifrelenecek verilerin hazırlanmasında gürültünün azaltılması amacıyla her bir veri 10 kez kullanıldı. 500 bin satırlık veri hazırlandı. Bu açık metinden oluşan dosya her 10 satır



Şekil 7.3: Hizalama işlemi gerçekleştirilmiş ölçümlerden bir örnek

da bir rastgele veriler üretilerek oluşturuldu. Aynı açık metinlerin ortalaması alınarak işlemler yapıldı. Böylelikle ölçüm boyutu 500k dan 50k ya indirgenmiş oldu. Elde edilen ölçüm boyutu 50k x 201 olmuştur. Oluşan bu matrise ölçüm matrisi 1 adı verilmiştir. Bu işlemin ardından uygulanacak olan kocher yada korelasyon analizi yöntemi ile anahtar bulma işlemine geçilmiştir.

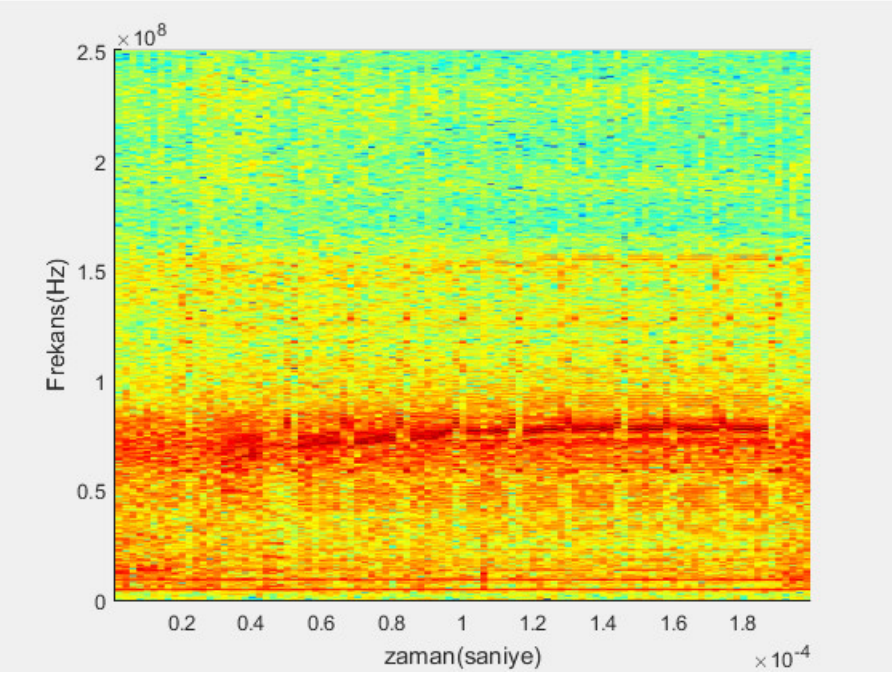
7.1.2 Ölçümlerin Filtrelenmesi

Alınan ölçümlerinin iyileştirilmesinde başka bir yöntem olarak, alınan EM dalganın spektrogramına bakılarak uygulamanın çalışma frekans aralığı bulunabilir. Daha doğrusu hangi frekans aralığında yoğun olarak EM radyasyon yaydığı bulunabilir. Spektrogram işlevi MATLAB Sinyal İşleme Araç Kutusu' nda mevcuttur ve spektrogramın çiziminin ayrıntılı hali şekil 7.4 de verilmiştir. [47].

Buradan hareketle alınan ölçümlerden birinin spektrogramı incelendi. Şekil 7.5 örnek spektrogram sonucu olarak incelenebilir. Belirli frekans aralığında dalganın daha güçlü olduğu görülmektedir.

```
Fs = 5e8 ; % örnekleme frekansı
x=(trace(91,:)); %spektrogramı alınacak olan ölçüm
WINDOW = 1000;
NOVERLAP = 0 ;
NFFT = 2^nextpow2(WINDOW) ;
[S, F, T,P]= spectrogram(x,WINDOW,NOVERLAP,NFFT, Fs ) ;
surf(T,F,10*log10(abs(P)) , 'EdgeColor', 'none' ); grid on ;
axis xy ; axis tight ; colormap( jet ) ; view (0,90);
xlabel( 'Zaman (saniye) '); ylabel( 'Frekans(Hz)') ;
```

Şekil 7.4: Spektrogram programı

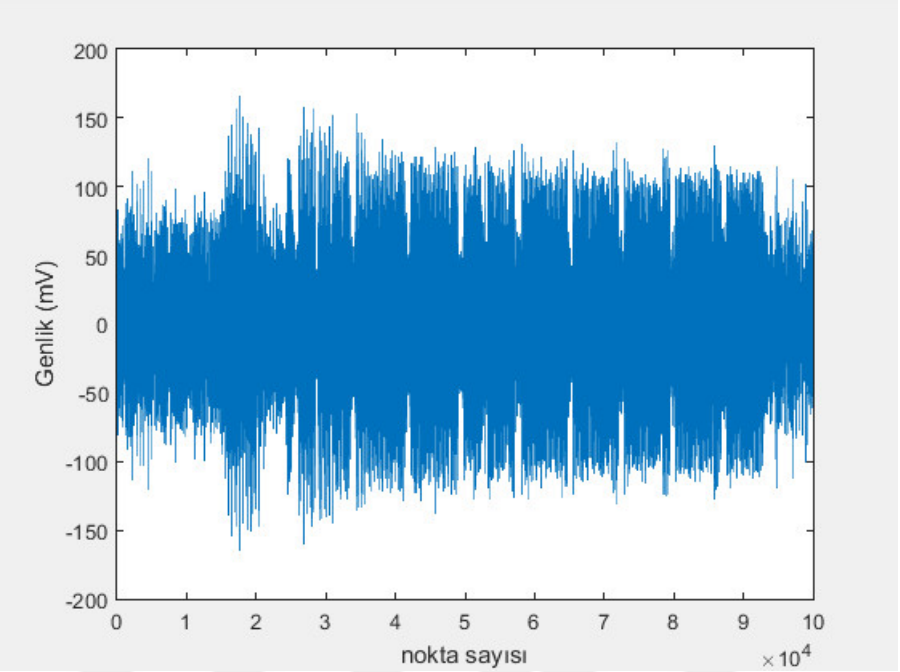


Şekil 7.5: Ölçümün spektrogramı

Gereksiz frekanslarda oluşan gürültüleri temizle işlemi yapılarak ölçüm iyileştirilmeye çalışıldı. Şekil 7.6' ten faydalanılarak sırasıyla aşağıdaki işlemler yapılmıştır.

- 58 MHz ile 89 MHz arası frekansları geçiren bir bant geçiren filtre tasarlandı ve tüm ölçümlere aynı işlem uygulandı.
- Filtreleme işlemi yapıldıktan sonra 100 noktada bir örnek alınarak rms alma işlemi yapıldı.
- RMS işleminin ardından aynı verileri şifreleyen 10 ölçümün ortalaması alındı. Toplam ölçüm boyutu 500k dan 50k ya indirildi. Ölçüm boyutu 50k x 1000 olarak ayarlanmış oldu. Elde edilen bu matrise ölçüm matrisi 2 adı verilmiştir.

- Bu işlemin ardından uygulanacak olan kocher yada korelasyon analizi yöntemi ile anahtar bulma işlemine geçilmiştir.



Şekil 7.6: Ölçümün filtrelenmiş hali

7.2 Tahmin Matrislerini Oluşturma

Kocher ve korelasyon analizinin yapılabilmesi için ölçüm değerlerinin yanında bir de tahmin matrisine ihtiyaç vardır. Bu bölümde EM analizinde kocher ve korelasyon işlemi için kullanılacak olan tahmin matrisini oluşturma anlatılmıştır. Tahmin matrisi oluşturulurken kullanılabilecek olan iki model vardır. Bunlardan birisi "Hamming Ağırlığı" diğeri ise "Hamming Uzaklığı" dır. Kocher ve korelasyon yönteminde tahmin matrisi aynı şekilde oluşturulur. Tahmin matrisi oluşturulduktan sonra analiz kısmında farklılaşırlar.

Hamming ağırlığı modeli açılanacak olursa, tahmin edilen işlem (örnek sütun karıştırma işlemi) yürütülürken kaydedicilerde bulunan bir sayısı toplanır. Hamming Uzaklığı modelinde ise yürütülen işlem sırasındaki kaydedicilerdeki 0-1 geçişlerine bakılır. Geçiş sayısının toplamı ise tahmin matrisini oluşturur. Tez çalışmasında her iki modelde kullanılmıştır. Başarı ise Hamming Distance ile elde edilmiştir.

Tahmin matrisi oluşturulmadan önce saldırının yapılacağı yere -işleme- karar verilmiştir. AES algoritmasında doğrusal olmayan tek işlem S kutusu olduğu için, S kutusunun

çıkışına saldırı gerçekleştirilmiştir. Saldırının yapılacağı yere kadar bilgisayar üzerinde AES algoritması modellenmiştir. Olası tüm anahtar değerleri açık veriler ile işleme sokulmuştur.

Anahtara bayt bayt saldırı işlemi gerçekleştirilmiştir. Bu nedenle doğru anahtarı bulabilmek amacıyla her bir bayt için 256 ayrı anahtar ile işlem gerçekleştirilmiştir. Her bir anahtar baytı için 50000x256 boyutunda bir matris elde edilmiştir. Elde edilen bu matris ile;

- S kutuna giriş ve S kutusundan çıkış işlemi sırasında yayılan manyetik dalganın farkı alınarak tahmin matrisi oluşturulmuştur. Bu matris Distance Tahmin Matrisi olarak adlandırılmıştır.
- S kutusunda işlemin yapıldığı esnada, yani bayt değiştirme işleminde kaydedicilerde bulunan bir sayısı toplanarak bir tahmin matrisi daha oluşturulmuştur. Bu tahmin matrisine ise Weight Tahmin Matrisi adı verilmiştir.

Tahmin matrisinin her bir elemanı 0-8 arasında bir değer almaktadır. Tahmin matrislerinin oluşturulmasının ardından analiz işlemlerine başlanmıştır.

7.3 Analiz Yöntemleri

Bölüm 7.1 ve 7.2 de gerçekleştirilen işlemlerin ardından elde edilen ölçüm matrisleri ve tahmin matrisleri kullanılarak analiz işlemleri gerçekleştirilmeye başlanmıştır. Ölçüm olarak hem bölüm 7.1.1 de anlatılan ölçüm matrisi 1 hem de 7.1.2 de anlatılan ölçüm matrisi 2 kullanılmıştır. Analiz işlemleri gerçekleştirilirken iki yöntem uygulanmıştır.

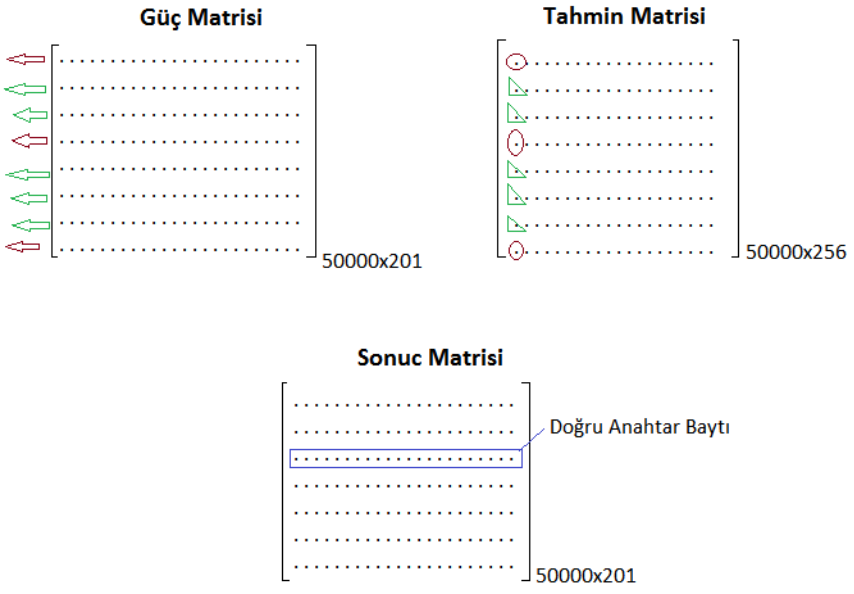
7.3.1 Kocher Yöntemi İle Analiz

Kocher yöntemi ile analiz gerçekleştirilirken;

- Distance Tahmin Matrisi' nde birinci sütunun elemanları için 4'ten büyük değerler çok yayınım yapan, 4'ten küçük değerlere ise az yayınım yapan olarak kabul edilmiştir. 4 değerleri ise analizin seyrinde yerinin tam ortada olması nedeniyle farklılık oluşturacağından işleme alınmamıştır.

- Distance Tahmin Matrisi' nde çok yayınım yapan ve az yayınım yapan olarak belirlenen değerler ölçüm matrisi 1 deki ölçümleri iki grup haline ayırmıştır.
- Ölçüm matrisi 1 deki çok yayınım yapan ölçümler kendi aralarında, az yayınım yapan ölçümler ise kendi aralarında toplanmıştır.
- Toplanan ölçüm değerlerinin farkı alınmıştır.
- Bu işlem doğru anahtar olabilecek her bir anahtar değeri için (1-256) tekrarlanmıştır.

Doğru anahtar değeri için ölçümlerinin toplamının farkında belirgin bir işaretin çıkması beklenir. Yapılan işlemler aşağıdaki resimle görselleştirilmiştir. Kırmızı daireler çok yayınım yapanları, yeşil ile gösterilenler ise az yayınım yapanları göstermektedir. Ölçüm matrisinde çok yayınım yapan ölçümler kırmızı ok ile, az yayınım yapan ölçümler ise yeşil ok ile gösterilmiştir. Sonuç matrisinde ise doğru anahtar baytı için bulunan sonuç gösterilmiştir.



Şekil 7.7: Kocher yöntemi ile analiz

Kocher yöntemi ile analiz işlemi sonucunda başarılı bir sonuç elde edilememiş, doğru anahtar değeri bulunamamıştır. Daha sonra analiz işlemi Weight Tahmin Matrisi ile tekrar yinelenmiştir. Fakat yine doğru sonuç elde edilememiştir.

Sonuç elde edilemeyince ölçüm matrisi 2 ile kocher yöntemi kullanarak analiz işlemi yapılmaya karar verilmiştir. Ölçüm matrisi 2 ile Distance Tahmin Matrisi kullanılarak analiz

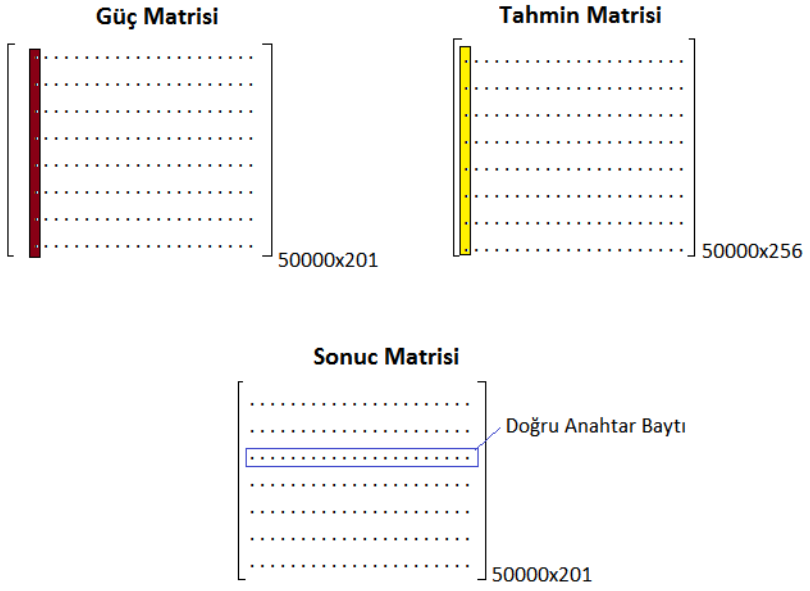
TABLO 7.1: Kocher Yöntemi İle Analiz

	Ölçüm Matrisi 1	Ölçüm Matrisi 2
Weight Tahmin Matrisi	Başarısız	Başarısız
Distance Tahmin Matrisi	Başarısız	Başarısız

işlemi gerçekleştirilmiş yine başarı elde edilememiştir. Tahmin matrisi tekrar değiştirilmiş ve Weight Tahmin matrisi kullanılarak tekrar analiz işlemi gerçekleştirilmiş ama yine başarılı olunamamıştır. Tablo 7.1 de kullanılan tahmin matrisleri ve ölçüm matrisleri kullanılarak elde edilen sonuçlar verilmiştir.

7.3.2 Korelasyon Yöntemi İle Analiz

Korelasyon Yöntemi ile yapılan analizde oluşturulan tahmin matrisinin her bir sütunu ölçüm matrisinin her bir sütunu ile tek tek korelasyon işlemine tabi tutularak sonuç matrisi elde edilir. Doğru anahtar baytı için korelasyon işleminin sonucu yüksek çıkarken yanlış anahtar tahmini için korelasyon değeri düşük çıkmaktadır. Aşağıdaki şekil ile yapılan işlem gösterilmiştir.



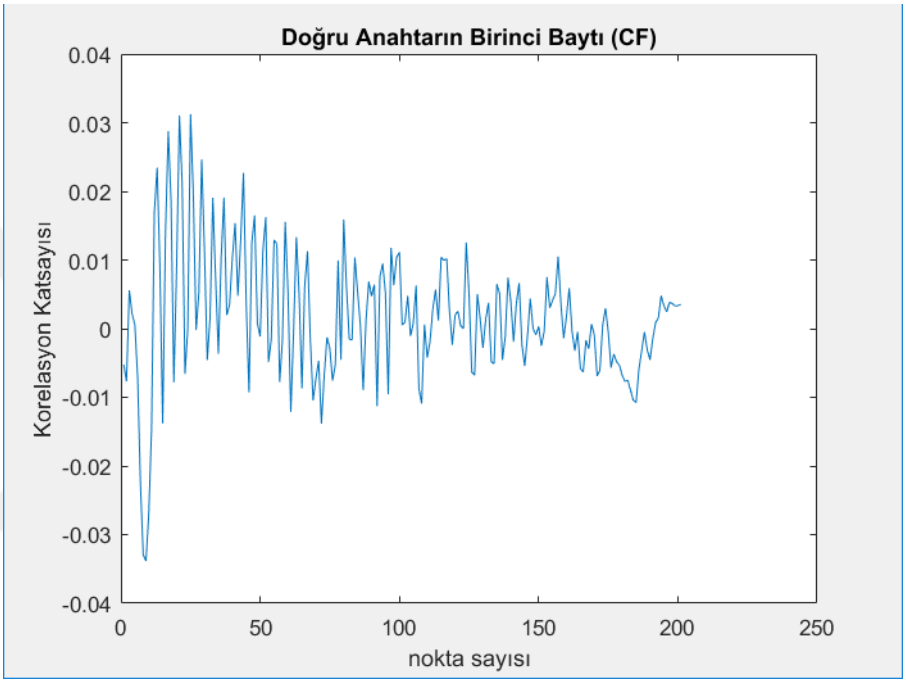
ŞEKIL 7.8: Korelasyon yöntemi ile analiz

Sırasıyla aşağıdaki işlemler gerçekleştirilmiştir.

- Weight Tahmin Matrisinin her bir sütunu ölçüm matrisi 1 ile korelasyon işlemine tabi tutulmuştur.

- İşlem sonrası oluşan sonuç matrisi ile korelasyon değeri en yüksek olan anahtar değeri için sonuç çizdirilmiştir.
- Farklı anahtar değerleri için inceleme yapılmış fakat doğru sonuç elde edilememiştir.

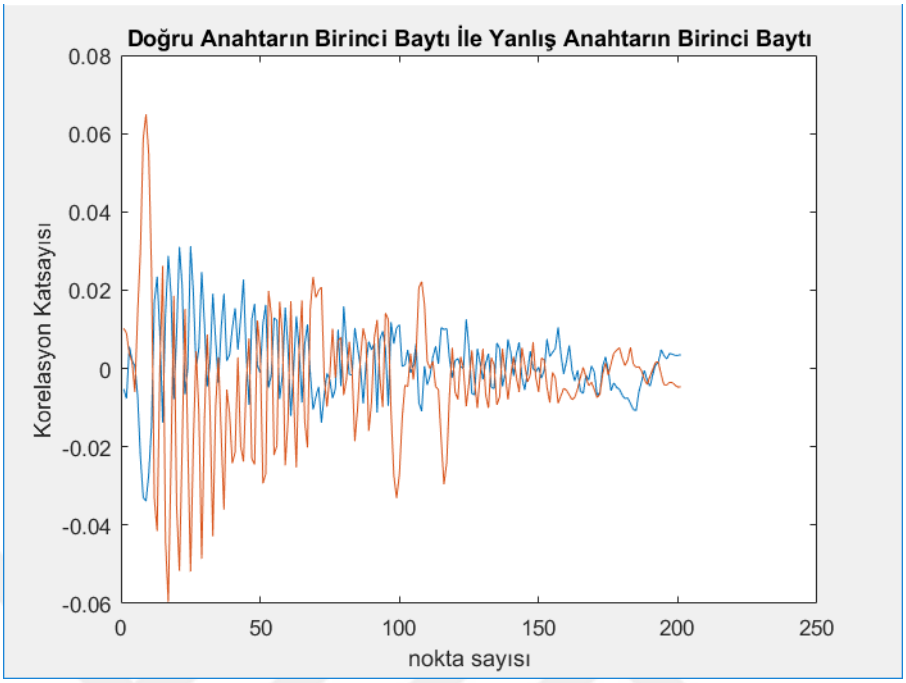
Aşağıda doğru anahtar ve yanlış anahtar baytı için örnek sonuç değerleri verilmiştir. Tez çalışmasında mavi renkli çizim doğru anahtarı kırmızı renkli çizim yanlış anahtarı göstermektedir.



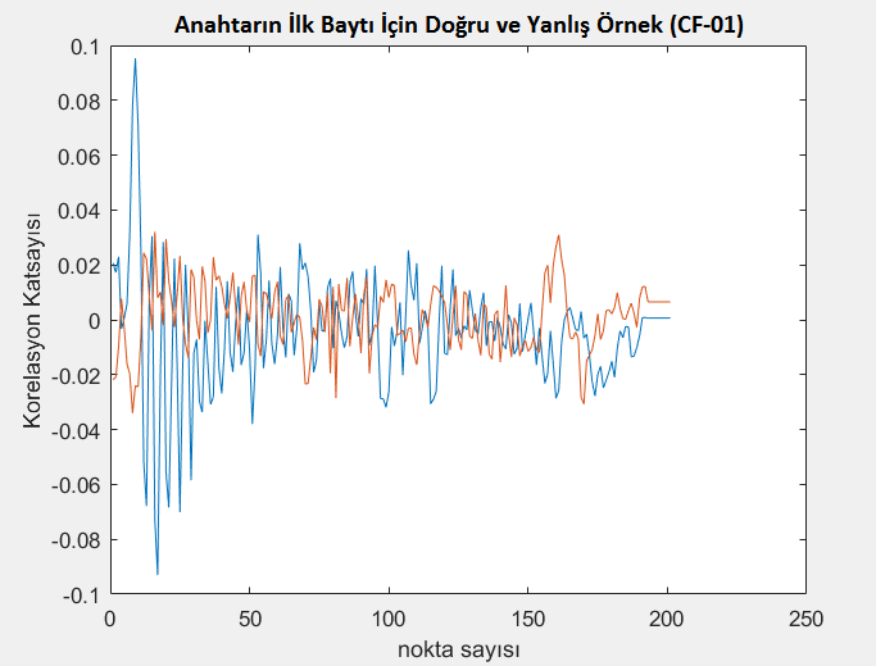
Şekil 7.9: Doğru anahtarın birinci baytı için korelasyon sonucu

Yukarıdaki şekilde görüldüğü gibi yanlış anahtar değeri için korelasyon sonucu daha fazla çıkmış ve başarılı olunamamıştır. Bu işlemin ardından tahmin matrisi değiştirilerek Distance Tahmin Matrisi korelasyon analizi için kullanılmıştır. Aynı adımlar gerçeklenmiş, Distance Tahmin Matrisi' nin her bir sütunu ölçüm matrisi 1 ile korelasyona tabi tutulmuştur. Analiz işlemi sonucunda başarıya ulaşılmış ve doğru anahtarlar bayt bayt bulunmuştur. Aşağıdaki şekillerde örnek olarak bulunan baytlar verilmiştir. Mavi ile gösterilenler doğru anahtar baytıdır. Kırmızı ile gösterilenler ise yanlış olan anahtar örnekleridir.

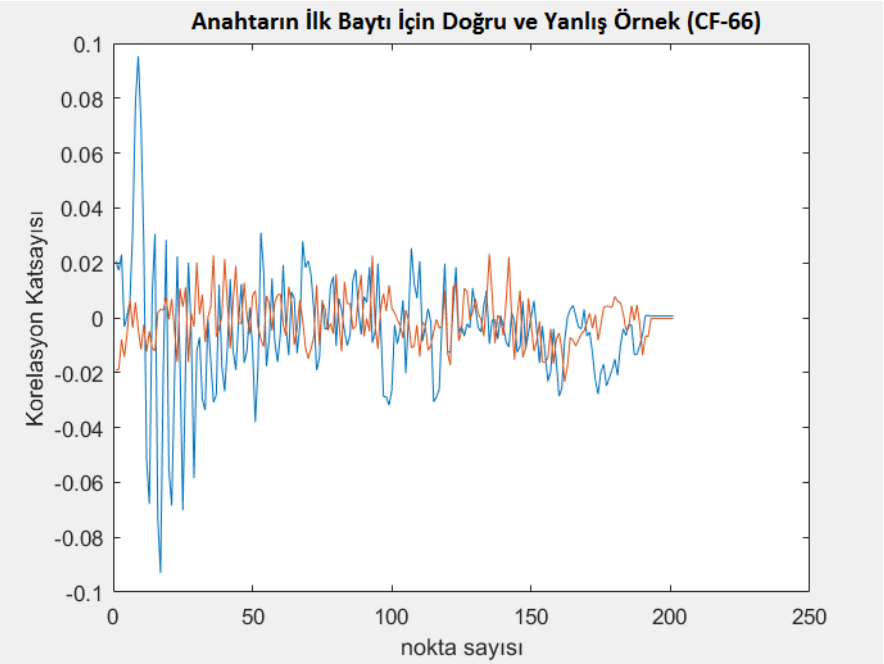
Şekil 7.11 ve şekil 7.12 den görüldüğü gibi doğru anahtar değeri olan CF nin korelasyon değeri diğer tüm anahtar tahminlerinden daha fazladır.Aynı şekilde anahtarın ikinci baytı için aynı işlemler gerçekleştirilmiş ve şekil 7.13 ve şekil 7.14 deki sonuçlar elde edilmiştir.



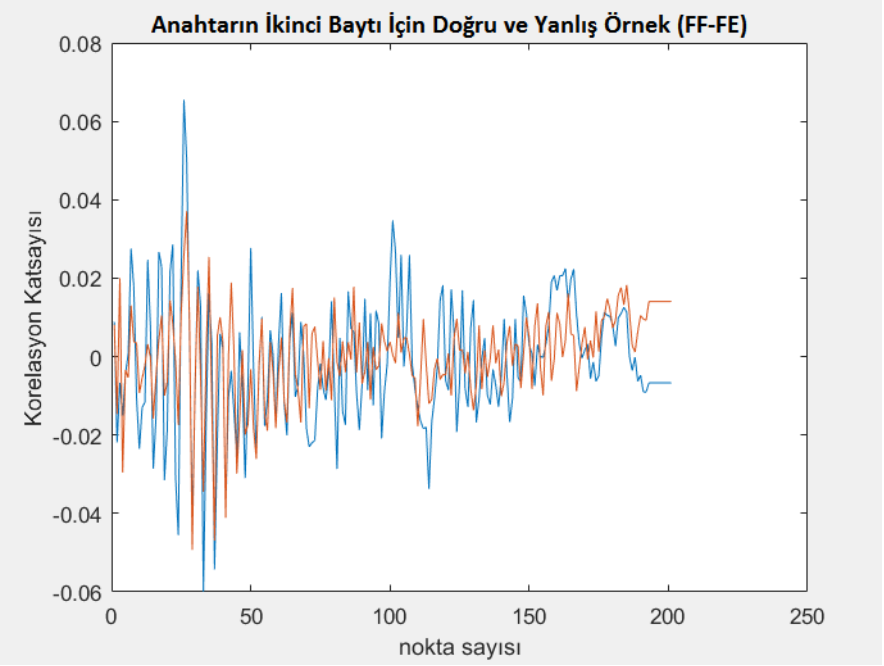
Şekil 7.10: Doğru anahtar ve yanlış anahtar arasındaki korelasyon değeri farkı



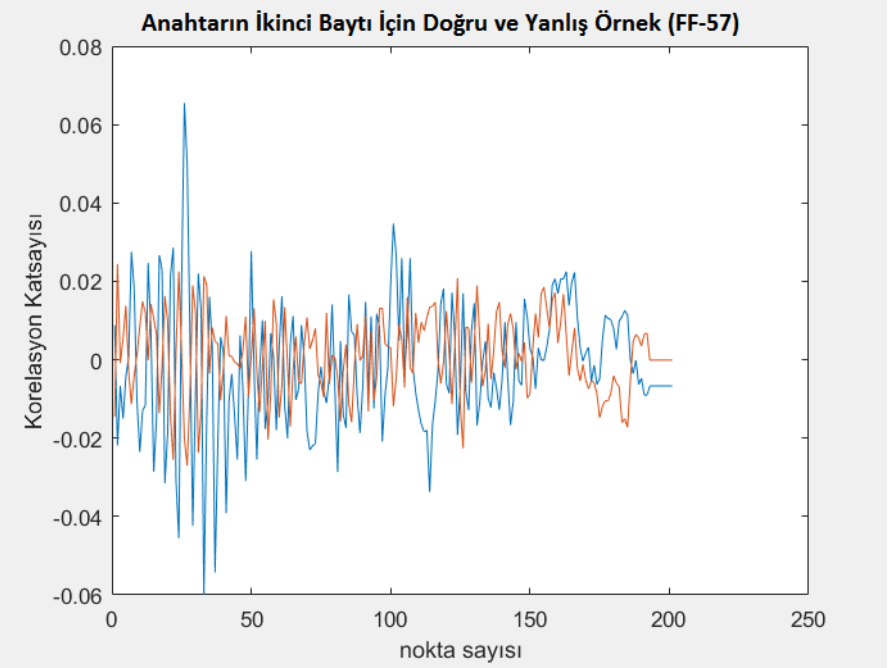
Şekil 7.11: İlk bayt değeri için anahtar tahmini



Şekil 7.12: İlk bayt değeri için anahtar tahmini

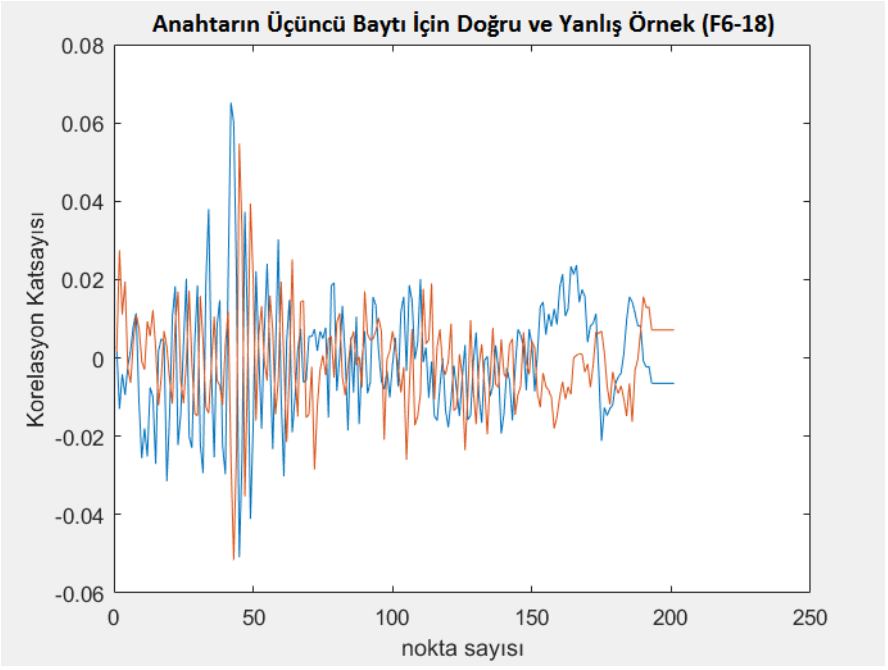


Şekil 7.13: İkinci bayt değeri için anahtar tahmini 1

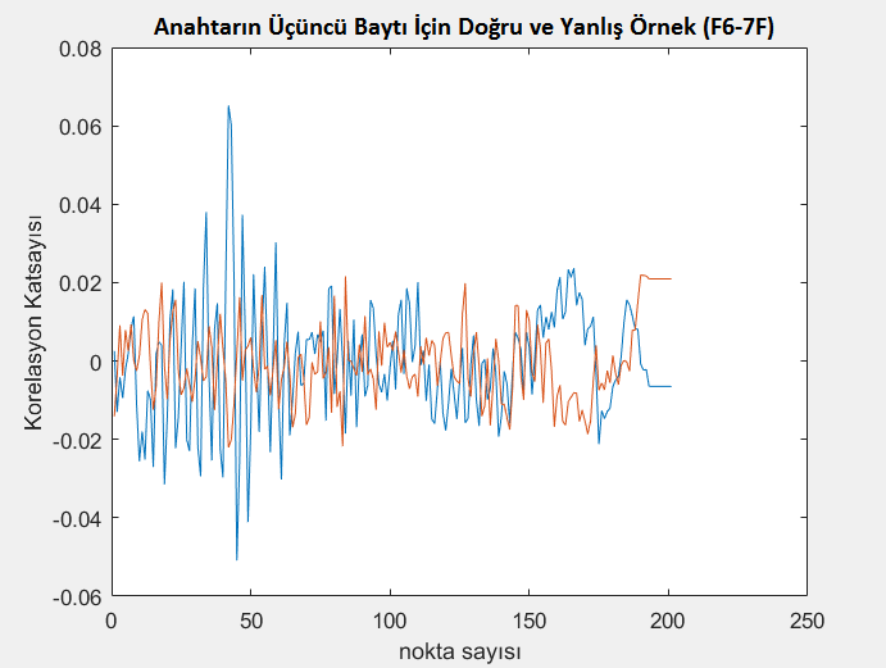


Şekil 7.14: İkinci bayt değeri için anahtar tahmini 2

Anahtarın ikinci baytı yanlış anahtar değerleri ile karşılaştırıldığında doğru anahtarın korelasyon değerinin en yüksek değer olduğu görülmüştür. Bazı bayt değerleri incelendiğinde ise korelasyon değerlerinin birbirine yakın olduğu gözlemlenmektedir. Yine de doğru anahtarın korelasyon değeri az farkla da olsa diğer değerlerden daha yüksek çıkmaktadır. Örnek olarak Şekil 7.15 incelenebilir.

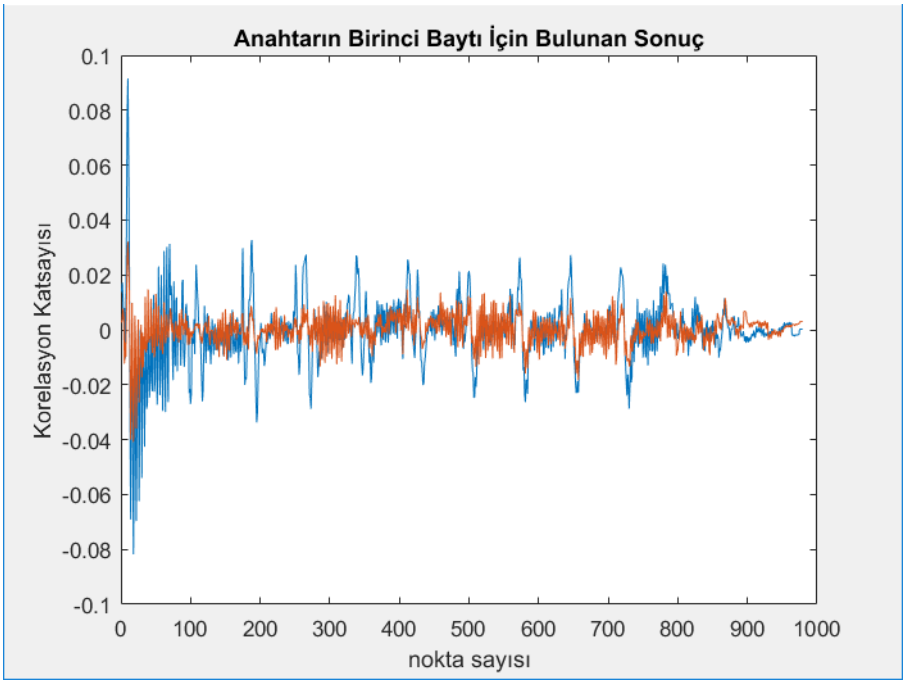


Şekil 7.15: Üçüncü bayt değeri için anahtar tahmini 1

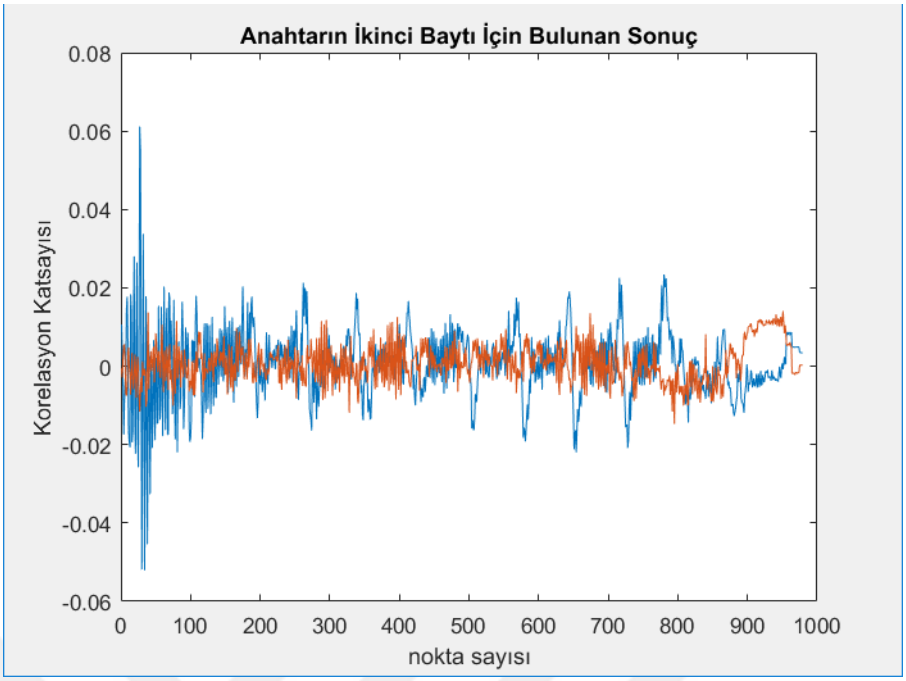


Şekil 7.16: Üçüncü bayt değeri için anahtar tahmini 2

Doğru anahtarın bulunmasının ardından ölçüm matrisi 2 ile de sonuç elde edilip edilemeyeceği incelenmiştir. Ölçüm matrisi 2 ve Distance Tahmin Matrisi kullanılarak başarılı sonuç elde edilmiş ve anahtar bulunmuştur. Şekil 7.17 ve şekil 7.18 incelenecek olursa sonucun başarılı olduğu görülecektir.

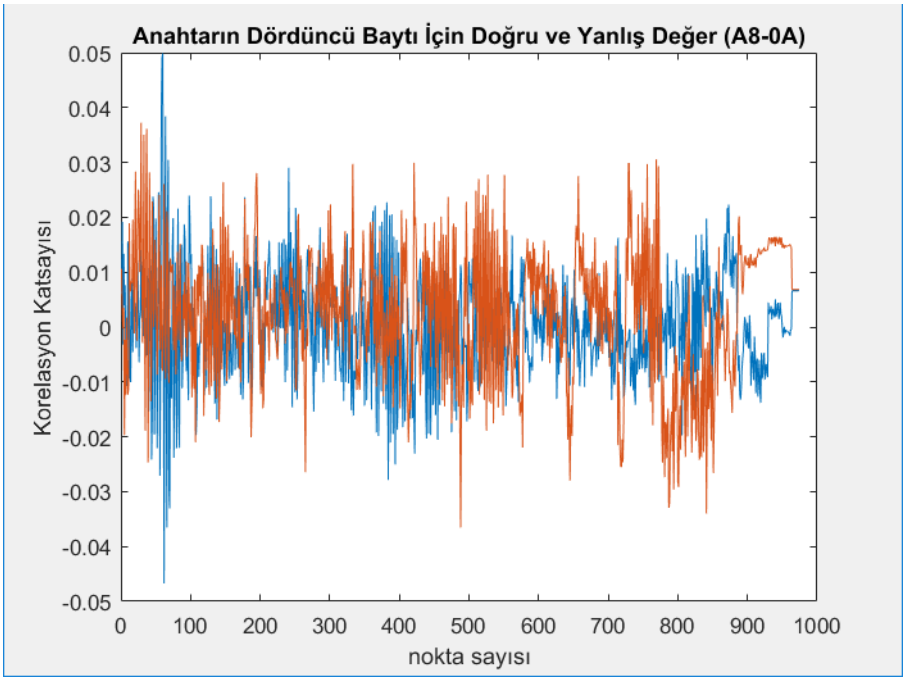


Şekil 7.17: Anahtarın birinci baytını gösteren örnek sonuç



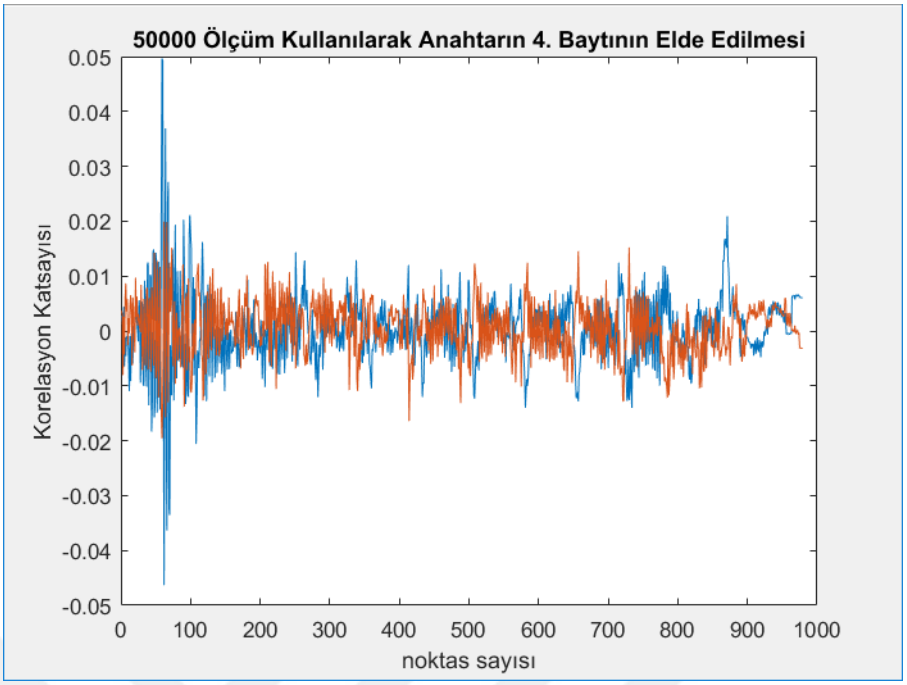
Şekil 7.18: Anahtarın ikinci baytını gösteren örnek sonuç

Bazı baytlarda anahtar değerleri için sonuçlar birbirlerine çok yakın çıkmaktadır. Aşağıdaki şekilde örnek olarak 10000 ölçüm için ve 50000 ölçüm için bulunan korelasyon katsayıları verilmiştir.



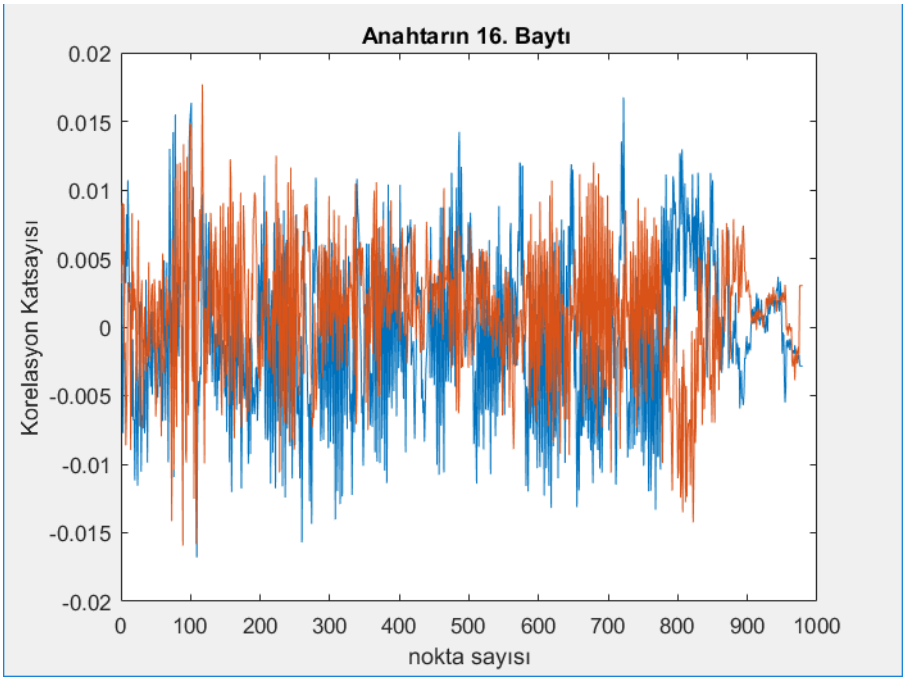
Şekil 7.19: 10000 Ölçüm kullanılarak bulunan anahtar

Anahtarların bazı baytlarının tespiti için ölçüm sayısının artırılması uygun görülmektedir. Örneğin anahtarın 15. Bayt değeri tam olarak tespit edilememektedir. Şekil 7.20



Şekil 7.20: 50000 ölçüm kullanılarak bulunan anahtar

da yapıldığı gibi ölçüm sayısının artırılmasıyla yanlış anahtarın korelasyon katsayısının düşmesi ve doğru anahtarın daha belirgin hale gelmesi beklenmektedir. Şekil 7.21 de anahtarın 16. baytı için elde edilen sonuç verilmiştir.



Şekil 7.21: Yanlış tespit edilen anahtar

Şekilde de görüldüğü gibi kırmızı ile gösterilen yanlış anahtar değerinin korelasyon katsayısı daha yüksektir. Dördüncü baytı bulmak/gürültüyü azaltmak için ölçüm sayısı 5

kat artırıldığında gürültü yaklaşık olarak %50 azalmıştır. Ölçüm sayısının yaklaşık 2 katı artırılması ile doğru anahtarın tespiti mümkün olacaktır.

Bölüm 8

Sonuç ve Öneriler

Teknolojinin gelişmesi beraberinde saldırı yüzeyinin genişlemesini getirmiştir. Hatta birçok saldırı tekniği için o saldırıya özel araçlar, yazılımlar mevcuttur. AES algoritmasının matematiksel olarak güçlü olması bilindik kriptoanalize karşı onu dirençli göstermektedir. Yan kanal saldırılarıyla birlikte AES algoritmasının farklı kriptoanalizlere karşı direnci de dikkate alınmalıdır. Bu nedenle algoritmanın kullanıldığı platform önem arz etmektedir.

Tez çalışmasında platform olarak kullanılmış olan Raspberry Pi dikkate alındığında saldırı başarılı olmuştur. Mini bir bilgisayar olarak düşünüldüğünde işletim sisteminin çalıştırmış olduğu servisler, monitör etme, haberleşme ile oluşturduğu gürültü/yaydığı dalga göz önüne alındığında AES algoritması çalışırken yaydığı dalganın tespiti engellenememiştir. Bu durum iki şeyi temel alarak önlem almayı gerektirir. Algoritmanın çalışacağı platformun yan kanal saldırılarına karşı dirençli bir platform olması ya da algoritmada yazılımsal olarak önlemler alarak yan kanal sızıntılarının önlenmesi. Yazılımsal olarak uygulama-protokol seviyesinde önlem için anahtar kullanımı sınırlandırılmalıdır. Farksal analiz saldırılarında birden fazla ölçüm alındığı için bu yöntem sıkça kullanılmaktadır [49].

Kriptografik işlemlere özel olarak tasarlanmış mikroişlemciler mevcuttur. Hatta birçoğu belirli güvenlik standartlarına (PCI, Ortak Kriterler) göre sertifikalıdır. Bu standartlarda yan kanal saldırılarına karşı olan direnci de test edilmektedir. Başka bir önlem olarak algoritmalara özel olarak kullanılan maskeleme teknikleri vardır. Bu tekniklerle

AES algoritmasının yan kanal saldırıları ile kırılmasının önüne geçilebilir. Donanımsal olarak alınabilecek olan önleme bir örnek verilecek olursa şifreleme/çözme işlemi esnasında yayılan sinyalin gücünü azaltmak için özel kalkanlar, fiziksel olarak güvenli bölgeler kullanılabilir [50].

İşletim sisteminde mevcut olarak bulunan kripto kütüphaneleri, açık kaynak kodlu kripto kütüphaneleri, ve ücretli kripto kütüphaneleri için bu konu özellikle incelenmelidir. AES gerçeklemesi yalın halde yapılmış ve hiçbir önlem alınmamışsa güvenlik açığı vardır denilebilir. Bu nedenle kullanılan kripto kütüphanelerinin güvenlik sertifikası almış olması ya da algoritmanın çalışacağı platformun sertifikalı olması tercih edilmelidir. Algoritma, kütüphane olmadan kullanılacaksa ve kullanılan platform sertifikasız ise mutlaka yazılımsal olarak yan kanal analizine karşı önlem alınması gerekir.

Kaynaklar

[1] L. Ordu. AES Algoritmasının FPGA Üzerinde Gerçeklenmesi ve Yan Kanal Analizi Saldırılarına Karsı Güçlendirilmesi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2006.

[2] R.B.J.T. Allenby. Rings, Fields and Groups, Butterworth-Heinemann, 1991.

[3] L. Fuchs. Infinite Abelian Groups, Vol. I. Pure and Applied Mathematics, Vol. 36. New York-London: Academic Press. xi+290 pp.

[4] S. Axler. Linear Algebra Done Right, 2e, Springer.. Abstract algebra theory, 1997.

[5] O. Kara. Kriptolojiye Genel Bakış, BGM 501 Kriptolojiye Giriş Ders Notları 1/14, Türkiye, 2013.

[6] F. Şahin. Modern Blok Şifreleme Algoritmaları, 2013. İstanbul Aydın Üniversitesi Dergisi (İAÜD), Yıl 5, Sayı 17, Sayfa(47-60), URL `http://iaud.aydin.edu.tr/makaleler/yil5sayi17/4FatihSahin.pdf`.

[7] K. Yıldırım. Veri Şifrelemesinde Simetrik Ve Asimetrik Anahtarlama Algoritmalarının Uygulanması (Hybrid Şifreleme)), Yüksek Lisans Tezi, Kocaeli Üniversitesi, Kocaeli, Türkiye, 2006.

[8] A. Yıldırım. Bilişim Sistemlerinde Veri Güvenliği Yaklaşımı ve Şifreleme Algoritmaları: DNA Algoritması Önerisi, Doktora Tezi, Marmara Üniversitesi, İstanbul, Türkiye, 2010.

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

[10] B. Aslan. Boole Fonksiyonları ve S-Kutularının Kriptografik Özelliklerinin İncelenmesi ve Ters Haritalama Tabanlı Cebirsel Açıdan Güçlendirilmiş Bir S-kutusu Önerisi Yüksek Lisans Tezi, Trakya Üniversitesi, Edirne, Türkiye, 2008.

[11] L. Keliher. Linear Cryptanalysis of Substitution-Permutation Networks, PHd Thesis, Queen's University, Ontario, Canada, 2003.

[12] İ. Okumuş. RSA Kriptosisteminin Hızını Etkileyen Faktörler, Doktora Tezi, Atatürk Üniversitesi, Erzurum, Türkiye, 2012.

[13] the free encyclopedia Wikipedia. Public Key Cryptography, 2015. URL `https://en.wikipedia.org/wiki/Public-key_cryptography`.

[14] A. Aksuoğlu. RSA Algoritmasının İyileştirilmesi İçin Yeni Bir Yaklaşım, Yüksek Lisans Tezi, Anadolu Üniversitesi, Eskişehir, Türkiye, 2010.

[15] B. Schneier. Applied Cryptology, Second Edition: Protocols, Algorithms, and Source Code in C, Wiley Publishing, 1996.

[16] A. Salomaa. Public-Key Cryptography, Springer Verlag, New York, 1990.

[17] İ. Ciğer. Data Şifreleme Algoritmaları ve Performans Analizi, Yüksek Lisans Tezi, İstanbul Üniversitesi, İstanbul, Türkiye, 2012.

[18] M. Öztemür. AES Algoritmasının Bir Gerçeklemesine Güç Analizi Saldırıları, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul, Türkiye, 2012.

[19] S. Skorobogatov, R. Anderson. Optical Fault Induction Attacks, URL `https://www.cl.cam.ac.uk/sps32/ches02-optofault.pdf`.

[20] J. Gallais. Microarchitectural Side-Channel Attacks, PhD Theses, Luxembourg University, The Faculty of Sciences, Technology and Communication , Luxembourg, 2013.

[21] E. Erkek. Akış Şifreleme Algoritmaları Kullanılarak Rasgele Sayı Üretilmesi Ve FPGA Ortamında Gerçekleştirilmesi, Yüksek Lisans Tezi, Fırat Üniversitesi, Elazığ, Türkiye, 2015.

[22] Y. Güven. Kriptoloji Tarihi, BGM 501 Kriptolojiye Giriş Ders Notları 3/14, Türkiye, 2014.

[23] F. Karakoç. Kripto Analizde Melez Bir Yöntem: Çakışma Saldırısı, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2008.

[24] P. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems, Advances in Cryptography: CRYPTO'96, 1109: 104-113., 1996.

[25] A. Shamir. E. Billiam. Differential Cryptanalysis of DES-like systems, Journal of Cryptography, 4: 3-72., 1993.

[26] M. Matsui. The first experimental cryptanalysis of the data encryption standard, Proceedings of CRYPTO'94, 1-11., 1994.

[27] S.B. Örs. Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks, PhD Thesis, Katholieke Universiteit Leuven, Leuven, Belgium, 2005.

[28] K. Türksoy. Differential Power Analysis Attack On A Fpga İmplementation Of Tea, Master Thesis , İstanbul Technical University, İstanbul, Türkiye, 2013.

[29] K. Alptekin Bayam. Differential Power Analysis Resistant Hardware Implementation Of The Rsa Cryptosystem, Master Thesis , İstanbul Technical University, İstanbul, Türkiye, 2007.

[30] S.M. Kang. Y. Leblebici. CMOS Digital Integrated Circuits: Analysis and Design. Mc Graw Hill, 2002.

[31] T. Chin Chi. A New Frequency-Based Side Channel Attack for Embedded Systems, Master's Thesis, Applied Science in Electrical and Computer Engineering, Waterloo University, Ontario, Canada, 2005.

[32] J. Quisquater. D. Samyde. Electromagnetic analysis (EMA): measures and countermeasures for smart cards, Proceedings of smart card programming and security, LNCS 2140, 200-210, 2001.

[33] P. Sergei. Semi-Invasive Attacks (definition), 2001. URL `http://www.cl.cam.ac.uk/~sps32/semi-inv_def.html`.

[34] P. Sergei. Semi-invasive attacks A new approach to hardware security analysis, 2005 Technical reports published by the University of Cambridge Computer Laboratory URL `https://pdfs.semanticscholar.org/2b7b/a7f2db6ae96cc7869282a1ab5d25fbe02f5b.pdf`.

[35] A. Kerckhoffs. La cryptographie militaire, Journal des sciences militaires, IX: 5–83,

[36] W. Cheuk. Analysis of DPA and DEMA Attacks, Master's Thesis and Graduate Research, San Jose State University, USA, 2012.

[37] Raspberry Pi Topluluğu, Arda. Raspberry Pi Nedir, 2014. URL `https://www.raspi-tr.com/2012/08/01/raspberry-pi-nedir/`.

[38] the free encyclopedia Wikipedia. , Raspberry Pi, 2017. URL `https://en.wikipedia.org/wiki/Raspberry_Pi`.

[39] SparkFun Electronics. , Raspberry Pi Model B, 2017. URL `https://www.sparkfun.com/products/retired/11546`.

[40] A. Volkan. , Raspberry Pi GPIO (Giriş/Çıkış) Portları, 2017. URL `http://www.volkanaktas.com/2015/02/raspberry-pi-gpio-giriscikis-portlari/`.

[41] Y. Güven. Simetrik Şifreleme Algoritmaları-Blok Şifreleme, BGM 501 Kriptolojiye Giriş Ders Notları 5/14, Türkiye, 2014.

[42] FIPS 46-3, 1999. Data Encryption Standard. National Institute of Standarts and Technology (NIST).

[43] FIPS 197, 2001. Advanced Encryption Standard. National Institute of Standarts and Technology (NIST).

[44] M. Şahinoğlu. Gelişmiş Şifreleme Standardı Algoritmasının Donanım Üzerinde Gerçeklemesine Elektromanyetik Alan Saldırısı, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, 2009.

[45] Forma Estudio. Animation of Rijndael, URL `https://www.sparkfun.com/products/retired/11546`.

[46] Riscure Security Tools. EM Probe Station, URL `http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf`.

[47] A. Do, S. Thet Ko, A. Thu Htet. Electromagnetic Side-Channel Analysis On Intel Atom Processor, A Major Qualifying Project Report, Worcester Polytechnic Institute. URL `https://web.wpi.edu/Images/CMS/ECE/MQP_Report_EM_Analysis__6.pdf`.

[48] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, Y. Yarom. ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels, 2017. URL `https://www.tau.ac.il/~tromer/mobilesc/mobilesc.pdf`.

[49] E. De Mulder. Electromagnetic Techniques and Probes for Side-Channel Analysis on Cryptographic Devices, Arenberg Doctoral School of Science, Katholieke Universiteit Leuven, Department of Electrical Engineering (ESAT), Belgium, 2010.

[50] Y. Zhou, D. Feng. Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100080, China. URL `http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper19.pdf`.