İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

AES ALGORİTMASININ FPGA ÜZERİNDE GERÇEKLEMESİNE ELEKTROMANYETİK ALAN SALDIRISI

YÜKSEK LİSANS TEZİ

Muhammet ŞAHİNOĞLU

Anabilim Dalı : Elektronik&Haberleşme Mühendisliği

Programı : Elektronik Mühendisliği

Tez Danışmanı: Doç. Dr. Müştak Erhan YALÇIN

ARALIK 2008

ÖNSÖZ

Tez çalışmalarım boyunca yol gösteren, teşvik eden danışman hocam Doç. Dr. Müştak Erhan Yalçın'a ve çalışmalarım sırasında sürekli destekleyen hocam Yrd. Doç. Dr. Sıddıka Berna Örs Yalçın'a teşekkürü bir borç bilirim.

Ayrıca tez çalışmalarım boyunca manyetik alan hakkında sorularıma usanmadan cevap vermeye çalışan hocam Doç. Dr. Selçuk Paker'e teşekkür ederim.

Laboratuarda çalışmalarım sırasında desteklerini hiçbir zaman eksik etmeyen arkadaşım Yük. Müh. Abid Üveys DANIŞ'a teşekkürlerimi sunarım.

Son olarak tüm çalışmalarım boyunca yanımda olan manevi desteğini üzerimden eksik etmeyen, motivasyonumu en üst seviyede tutmamda yardımcı olan babam Şevki ŞAHİNOĞLU'na teşekkürlerimi borç bilirim.

Tez çalışmalarım sırasında maddi destekte bulunan TÜBİTAK'a teşekkür ederim.

Aralık 2008

Muhammet ŞAHİNOĞLU
Elektronik Mühendisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

AES	: Advanced Encryption Standard
DES	: Data Encryption Standard
RSA	: Rivest-Shamir-Adleman
FPGA	: Field Programmable Gate Array
SCA	: Side-Channel Analysis
TA	: Timing Analysis
PA	: Power Analysis
SPA	: Single Power Analysis
DPA	: Differential Power Analysis
EM	: Electromagnetic
EMA	: Electromagnetic Analysis
SEMA	: Single Electromagnetic Analysis
DEMA	: Differential Electromagnetic Analysis
NIST	: National Institute of Standards and Technology
FIPS	: Federal Information Processing Standards
GF	: Galois Field

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

AES ALGORİTMASININ FPGA ÜZERİNDE GERÇEKLEMESİNE ELEKTROMANYETİK ALAN SALDIRISI

ÖZET

Gelişmiş kodlama standardı (Advanced Encryption Standard (AES)) Kasım 2001'de elektronik verinin saklanması için kullanılmak üzere federal bilgi işleme standardı (Federal Information Processing Standards (FIPS)) olarak Amerikan ulusal standartlar ve teknoloji enstitüsü (National Institute of Standards and Technology (NIST)) tarafından yayınlanmıştır [1, 2]. AES algoritması bilginin kodlanması ve kodlanmış bilginin çözülmesi için kullanılan bir simetrik blok kodlayıcıdır.

Kripto cihazlarının ana görevi kriptografi sistemlerinde sıkça kullanılan işlemleri yapmak veya bütün bir kriptografi algoritmasını gerçeklemektir [1, 3]. Bu sebeple bir kripto cihazı içinde saklanılan veya işlediği gizliliği önemli verinin öğrenilmesini engellemelidir. Yan-kanal saldırılarında kriptografi işlemlerinde kullanılan gizli parametreleri öğrenmek amacıyla gerçeklemeye özel karakterlerden yararlanılır [4, 5].

Yan-kanal atakları kriptografi alanında çalışanlar tarafından 1996'da zamanlama analizi konusunda yayınlanan ilk makale ile temel bir tehdit olarak görülmeye başlandı [6]. Bu ataklarda atak yapan kişi kripto cihazının normal fonksiyonlarını kullanır. Normal işleyişin fiziksel ve/veya elektriksel etkileri atak için kullanılır. Bu etkiler istek dışı olarak gizli anahtar hakkında bilgi veriyorlarsa verdikleri bilgilere yan-kanal bilgileri ve bu etkilere de yan-kanallar denir.

Yan-kanal atakları kullanılan etkiye göre dört gruba ayrılır. Zamanlama ataklarında bir kriptografi işleminin tamamlanma süresi kullanılır [6]. Güç harcaması ataklarında kriptografi işlemi sırasında cihazın dinamik güç harcaması kullanılır [7]. Elektromanyetik ataklarda cihazın işlem sırasında yaydığı elektromanyetik dalgalar kullanılır [8, 9]. Akustik ataklarda cihazın çalışması sırasında çıkardığı ses kullanılır [10].

Bütün yan-kanal atakları iki şekilde incelenir. Basit ataklarda atakçı gizli anahtarın bir parçasını öğrenebilmek için yan-kanal bilgisinin sadece bir ölçümünü kullanır [6]. Farksal ataklarda gürültüyü yok etmek için birden çok ölçüm kullanılır [7]. Basit ataklarda ölçüm ile işlemler arasında bir ilişki bulunmaya çalışılırken, farksal ataklarda ölçümler ile işlenen veri arasındaki ilişki bulunmaya çalışılır.

Bu tezde daha önce FPGA üzerinde gerçeklenmiş AES algoritması kullanılacaktır [11]. Ardından AES algoritmasının bu FPGA gerçeklemesine farksal elektromanyetik alan atağı uygulanacaktır. Bu atağın uygulanabilmesi için uygun bir

ölçüm düzeneğine ihtiyaç vardır. Bu sebeple üçüncü adım olarak bilgisayar, sayısal osiloskop, yakın alan alıcısı ve FPGA kartından oluşan ölçüm düzeneği kurulacaktır. Bu düzenek şu şekilde kullanılacaktır: a) Tasarımı yapılmış AES algoritmasının alınması [11], b) Yakın Alan alıcısının tasarımı, c) AES devresinin FPGA üzerinde gerçeklenmesi, d) Gerçeklemenin FPGA'e yüklenmesi, e) FPGA gerçeklemesinin farklı girişler için test edilmesi, f) FPGA'in birçok giriş ile beslenip herbiri işlenirken yaydığı elektromanyetik yayınımın yakın alan alıcısı yardımı ile ölçülmesi, g) Ölçülen elektromanyetik yayınımın istatistiksel olarak analizi yapılarak FPGA içinde saklanılan gizli anahtar ile ilgili bilgi elde edilmesi.

ELECTROMAGNETIC ANALYSIS ATTACK on FPGA IMPLEMENTATIONS of the AES ALGORITHM

SUMMARY

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data [1, 2]. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext.

The main task of cryptographic hardware is the acceleration of operations frequently used in cryptosystems or the acceleration of a complete cryptographic algorithm [1, 3]. In applications, hardware devices are also required to store secret or private keys securely. Hence, a cryptographic device must prevent the extraction of any sensitive information. A side-channel attack (SCA) takes advantage of implementation specific characteristics to recover the secret parameters involved in the computation. It is therefore less general, but often more powerful than classical cryptanalysis [4, 5].

SCAs were recognized in the cryptographic community as a major threat in 1996, when the first article about timing attacks was published [6]. In a side-channel attack, the adversary uses the standard functionality of the cryptographic device. The physical and/or electrical effects of the functionality of the device are then used for the attack. If these effects unintentionally deliver information about the key which is used inside the device, then they deliver side-channel information and are called side-channels.

SCAs are divided in four groups according to the side-channel information that they exploit. Timing analysis attacks exploit the timing information on the cryptographic hardware [6]. Power analysis attacks use the dynamic power consumption of the cryptographic hardware during the execution of the cryptographic algorithm [7]. Electromagnetic analysis attacks use the electromagnetic radiation of the cryptographic hardware during the execution of the cryptographic algorithm [8, 9]. Acoustic (sound) analysis attacks exploit the sound coming out of the cryptographic hardware during the execution of the cryptographic algorithm [10].

All the groups of the SCAs have two types . In a simple attack, an attacker uses the side-channel information from one measurement directly to determine (parts of) the secret key [6]. In differential attack, many measurements are used in order to filter out noise [7]. While a simple attack exploits the relationship between the executed

operations and the side-channel information, a differential attack exploits the relationship between the processed data and the side-channel information.

In this thesis, first AES algorithm implemented on an FPGA was used [11]. Then a differential electromagnetic analysis attack will be applied on this FPGA implementation. In order to apply this attack a suitable measurement setup is needed. Hence, as a third step a measurement setup which includes a computer, a digital oscilloscope, a close field probe and an FPGA card will be built. This measurement setup will be used as follows: a) studied on designed AES Circuit [11], b) Close Field Probe design c) FPGA implementation of the AES circuit, c) Uploading the implementation on the FPGA, d) Testing the FPGA implementation for different inputs, e) Feeding the FPGA with many inputs and measuring the electromagnetic emission during the execution of the encryption algorithm for each input, f) Finding information about the secret information inside the FPGA by using statistical analysis methods.

1. GİRİŞ

Güvenli haberleşme günümüzde çok önemli bir yere sahiptir. İhtiyaç duyulan bu güvenliği sağlayabilmek için kullanılan güvenlik sistemleri vardır. Kriptografik algoritmalar bu güvenlik sistemlerinin en önemli parçasını oluşturmaktadır. Kriptografik algoritmalarda ise güvenliği sağlayan en önemli yapı gizli anahtar kullanımıdır. Bu yüzden bir kriptografik sisteme yapılan saldırılar genellikle gizli anahtarı elde etmeye yönelik olmaktadır [6].

Kriptografik sistemlere yönelik saldırılar iki şekilde yapılabilmektedir. Bunlar matematiksel olan saldırılar ve gerçeklemeye özgü [6, 7] saldırılardır. Matematiksel saldırılarda sistem algoritma düzeyinde değerlendirmekte ve sistemdeki matematiksel yapıdan kaynaklı zayıflıklar araştırılmaktadır. Gerçeklemeye özgü saldırılarda sistemin doğrudan ürettiği sonuçları kullanmak yerine genellikle istemsiz ürettiği çıkışlar kullanılmaktadır. Bu tür saldırılar ise pasif yan kanal saldırıları ve aktif yan kanal saldırıları olmak üzere yine iki değişik şekilde değerlendirilmektedir.

Aktif yan kanal saldırıları şifreleme için kullanılan kriptografik sisteme fiziksel müdahalede bulunularak yapılan saldırılardır [12]. Bu tür saldırılarda devrenin iç yapısı sensörler yardımı ile gözlenebilmektedir, istenilen bir zamanda kaydedicilerde kayıtlı olan değerler okunabilmektedir [4]. Diğer bir aktif saldırı ise çalışan kriptografik sisteme hata yaptırmak suretiyle uygulanmaktadır [5, 13]. Bu saldırı türü ise genellikle lazer istasyonları yardımı ile yapılmaktadır. Özellikli hatalar yaptırılarak bütün saldırılarda yapıldığı gibi gizli anahtar elde edilmeye çalışılmaktadır.

Pasif yan kanal saldırıları şifreleme için kullanılan kriptografik sisteme fiziksel müdahalede bulunmaksızın yapılan saldırılardır [6, 7, 8, 9]. Tamamen devrenin istemsiz olarak ürettiği çıkışlardan faydalanılmaktadır. Sistemin verdiği istemli çıkışı şifreli veri olarak düşündüğümüzde devrenin tükettiği toplam güç profilini [7], etrafa yaydığı elektromanyetik radyasyonu [8, 9], etrafa yaydığı ses dalgalarını [10], yine devrenin sıcaklığındaki değişmeler ve son olarak şifreleme sırasındaki zaman farklılıkları istemsiz çıkışlar olarak değerlendirilmektedir [6]. Bu yüzden dolayıdır ki

pasif yan kanal saldırılarında istemsiz çıkışlar ile gizli anahtar bilgisi arasındaki ilişkinin varlığından yararlanılıp gizli anahtar elde edilmeye çalışılmaktadır. Devrenin tükettiği toplam güç profili ve etrafa yaydığı elektromanyetik radyasyon bu istemsiz çıkışlar arasında en yaygın kullanılanıdır. En yaygın kullanılmasının altında yatan sebep ise sayısal devrelerde gücün ve elektromanyetik yayınımın genel bir yapıya sahip olmasıdır. Ses ve sıcaklık ise devreden devreye farklılıklar gösterebilmektedir.

1.1 Tezin Kapsamı

Gelişmiş kodlama standardı (Advanced Encryption Standard (AES)) Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology (NIST)) tarafından Kasım 2001'de federal bilgi işleme standardı (Federal Information Processing Standards (FIPS)) olarak yayınlanmıştır [1, 2]. Gelişmiş kodlama standardı birçok güvenlik sistemleri uygulamalarında bir önceki şifreleme standardı olan Veri kodlama standardı (Data Encryption Standart (DES)) [3] yerine kullanılmaya başlanmıştır. AES yayınlanan son standart olmasına rağmen yan kanal saldırılarına karşı güvenlik problemlerinin olduğu bilinmektedir [6, 7, 8, 9, 10]. Bunun için yan kanal saldırılarına karşı güvenliği artırıcı yöntemler kullanılarak AES algoritması yan kanal saldırılarına karşı kuvvetlendirilebilmektedir [14, 15].

Diğer bütün kodlama standartlarında olduğu gibi AES için de anahtarı elde etmeye yönelik saldırı yöntemleri mevcuttur. Yan kanal saldırılarının içinden günümüzde en çok kullanılmış olanı farksal güç analizi yöntemidir (Differential Power Analysis (DPA) [7, 16]). Ancak DPA analizi için devrenin tükettiği toplam dinamik gücü ölçmek için kriptografik devre ile güç kaynağı arasına fiziksel olarak direk bağlantı kurmak gerekir. DPA'in bu tür sakıncaları göz önünde bulundurulduğunda devreye herhangi bir müdahalede bulunmaktan kaçınmak için Farksal Elektromanyetik Analizi yöntemine (Differential Electromagnetic Analysis (DEMA)) başvurulabilir. DEMA analizi için kriptografik sistem üzerinde herhangi ek bir elemana ihtiyaç duymaksızın elektromanyetik radyasyon işareti alınabilmektedir [8, 9].

Bizim çalışmamızda halihazırda en çok kullanılan Farksal Güç Analizi (Differential Power Analysis (DPA)) yöntemi yerine devrenin güç kaynağına erişiminin mümkün olmadığı sistemler düşünülerek Farksal Elektromanyetik Analizi (Differential Electromagnetic Analysis (DEMA)) yöntemi saldırılarının Sahada Programlanabilir

Kapı Dizileri (Field Programmable Gate Arrays (FPGA)) üzerinde gerçeklenmiş Gelişmiş Kodlama Standardı (AES) algoritmasına uygulanması incelenmiştir.

Elektromanyetik ölçümleri için gürültü çok önemli bir faktör olarak karşımıza çıkmaktadır [18]. Gürültünün etkisini incelemek için ise elektromanyetik işaretler alındıktan sonra istatistiksel bir ön işlemden geçirilecektir. Bizim çalışmamızda hem AES algoritmasının güvenlik önlemleri alınmamış gerçeklemesi hem de güvenlik önlemleri alınmış gerçeklemesi istatistiksel olarak ön işleme sürecinden geçirilerek sonuçları ile birlikte verilmiştir [11].

1.2 Tezin Konuya Katkısı

Literatürde FPGA üzerinde gerçeklenmiş olan güvenlik sistemleri için Farksal Elektromanyetik Analizi saldırıları hakkında kaynaklar bulunmaktadır [8, 9, 19]. Bizim çalışmamız ise FPGA üzerinde gerçeklenmiş en yaygın olarak kullanılan Gelişmiş Kodlama Standardı algoritmasının güvenlik önlemleri alınmış versiyonları için ön işleme sürecinden geçirilmiş analiz yöntemlerini içermektedir.

2. GENEL BİLGİLER

Bu bölümde tez anlatımı boyunca kullanılacak matematiksel kavramlar anlatılacaktır. Ayrıca gürültünün etkisini azaltmak için kullanılan kümülant yöntemi, EM işaretini alabilmek için anten tasarlama adımları anlatılacaktır.

2.1 Matematiksel Kavramlar

Aşağıda AES algoritmasında kullanılan *Galois Alanlarını* anlamak için bazı tanımlar verilecektir.

2.1.1 Abelian grubu

Abelian Grubu, bir G kümesi ve bu kümenin elemanları üzerinde tanımlanmış olan bir '+' işleminden oluşur [20]. Bir grubun abelian grubu olması için aşağıdaki özellikleri sağlaması gerekir.

2.1.1.1 Kapalılık özelliği

a ve b ikisi de G kümesinin elemanı olmak üzere *kapalılık özelliği* gereğince $(a+b)$' de G kümesinin elemanı olmalıdır [22].

$$\forall \text{ a, b } \in \text{ G : (a + b) } \in \text{ G} \tag{2.1}$$

2.1.1.2 Değişme özelliği

a ve b ikisi de G kümesinin elamanı olmak üzere *değişme özelliği* gereğince $(a+b) = (b+a)$ eşitliği sağlanmalıdır [23].

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

2.1.1.3 Birleşme özelliği

a ve b ikisi de G kümesinin elamanı olmak üzere *birleşme özelliği* gereğince $(a+b)+c = a+(b+c)$ eşitliği sağlanmalıdır [23].

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

2.1.1.4 Etkisiz eleman özelliği

a G kümesinin elemanı olmak üzere G kümesinde $a+0=a$ eşitliğini sağlayan bir tane *etkisiz eleman* vardır [23].

$$\exists 0 \in G, \forall a \in G : a+0=a \tag{2.4}$$

2.1.1.5 Ters eleman özelliği

a ve b G kümesinin elemanı olmak üzere öyle bir b elemanı vardır ki $a+b=0$ olsun.

$\forall a \in G, \exists b \in G : a+b=0$ [23]. (2.5)

2.1.2 Halka

R boş kümeden farklı bir küme olsun. Bu küme üzerinde "+" ve "□" ikili işlemleri tanımlı olsun. Eğer; $(R,+)$ kümesi *değişmeli bir küme*, $(R,\square)$ kümesi sadece *birleşme özelliğini* sağlayan bir küme ve "□" işlemi "+" işlemi üzerine sağdan ve soldan dağılmalı ise $(R,+,\square)$ kümesine *halka* denir. Eğer "□" işlemi *değişme özelliğine* sahipse, $(R,+,\square)$ halkası *'Değişmeli Halka'* olarak adlandırılır. "+" işleminin birim elemanı 0, "□" işleminin birim elemanı ise 1'dir [24].

2.1.3 Alan

Bir F kümesi, üzerinde tanımlanmış "+" ve "□" işlemleriyle birlikte aşağıdaki koşulları sağlıyorsa bir *'Alan'* oluşturur.

$(F,+)$ bir *abelian grubu* olmalıdır. $(F,\square)$ da bir *abelian grubu* olmalıdır, ancak sadece 0 elemanı için *ters eleman* olmayabilir. "□" işleminin "+" işlemi üzerinde *dağılma özelliği* olmalıdır [24].

2.1.4 Sonlu alan

Sonlu alan ise yukarıdaki alan tanımına uyan ancak adından da anlaşılacağı gibi sonlu sayıda elemanı olan alanlardır [25].

2.1.5 Galois alanı

p yi asal sayı olarak düşünelim. $GF(p)$; üzerinde "+" ve "□" işlemleri tanımlanmış p sayıda elemandan oluşan bir sonlu alanı temsil etmektedir. P *sonlu alanın karakteristiği* olarak adlandırılmaktadır. $GF(p^n)$ ise $GF(p)$'nin *genişletilmiş sonlu*

alanını ifade etmektedir $GF(p^n)$ ' nin p karakteristiğini gösterir. *Eleman sayısı* ise $GF(p)$ sonlu alanının elaman sayısının n katıdır. $GF(p^n)$'nin yapılan "+" ve "□" işlemlerinin alan içerisinde kalmasını sağlamak için n. dereceden bir indirgeme polinomuna ihtiyacı vardır [25].

2.1.6 GF(2^n) Galois alanı

Karakteristiği 2 olan $GF(2^n)$ sonlu alanının kriptografide kullanımı yaygındır. 2^n adet eleman içermektedir. Elemanları yan yana yazılmış bitler {0,1} olmasından dolayı kullanımı oldukça rahattır. 2 karakteristikli *Galois alanlarında* gösterim olarak polinomsal gösterim yaygın olarak kullanılmaktadır. $GF(2^n)$ için polinomsal baz, $\{x^{n-1}, x^{n-2}, ..., x^2, x, 1\}$ kümesinden oluşur. $GF(2^n)$'nin bir elemanının polinomsal gösterimi, polinomsal baz vektörünün her bir elmanının $GF(2)$'ye ait bir elemanla çarpılması ile elde edilir. Örneğin, $GF(2^8)$'in bir elemanı olan {10100111} polinomsal olarak şu şekilde gösterilir;

$$a(x) = x^7 + x^5 + x^2 + x + 1$$

Aşağıdaki bölümde GF(2^n) sonlu alanındaki toplama ve çarpma işlemleri anlatılacaktır.

2.1.6.1 GF(2^n) Galois alanında toplama işlemi

Polinomsal gösterilimde, aynı *Galois Alanı* içerisinde bulunan iki elemanın toplanması işlemi, karşı düşen iki polinomun toplanması ve daha sonra da elde edilen sonuç polinomunun katsayılarının modulo karakteristik değerlerinin bulunmasıyla gerçekleştirilir [25]. Örneğin $a, b, c \in GF(2^5)$ olmak üzere, $c = a + b$ 'yi bulmak için;

$a(x) = x^4 + x^3 + x^2 + x + 1$; $b(x) = x^4 + x^2 + x$ olsun.

$c(x) = a(x) + b(x) = 2x^4 + x^3 + 2x^2 + 2x + 1$ modulo 2'deki değerleri alındığında ise

$c(x) = x^3 + 1$ olarak bulunur.

Karakteristiği 2 olan bu *Galois sonlu alanında* toplama yapmak ve daha sonra çıkan sonucun modulosunu almak aynı zamanda bit bit x-or işlemine karşı düşmektedir. Aynı örnekten yola çıkarak

$c(x) = x^3 + 1$ olarak bulunur.

2.1.6.2 GF(2^n) Galois alanında çarpma işlemi

İki $GF(2^n)$ polinomsal elemanının çarpımı, iki polinomun aritmetik çarpımının alınmasıyla elde edilir. Ancak, bu iki polinomun çarpımı, Sonlu Alan'ın derecesinden daha yüksek dereceli bir polinom elde edilmesine neden olabilir. Bu nedenle çarpım sonucunda oluşan polinomu tekrar Sonlu Alan içerisindeki bir polinoma karşı düşürmek için polinomun n. dereceden bir polinom ile modülünün alınması gerekir. Modül alma işlemi için kullanılan bu polinom, $m(x)$, indirgeme polinomu olarak adlandırılmaktadır. Örneğin a, b, c $\in$ $GF(2^8)$ olmak üzere, $c = a \times b$ 'yi bulmak için;

$a = \{11111\} \equiv x^7 + x^5 + x^2 + x + 1$; $b = \{10110\} \equiv x^4 + x^2 + x$ olsun.

$c(x) = a(x) \times b(x) = (x^4 + x^3 + x^2 + x + 1) \times (x^4 + x^2 + x)$

$c(x) = x^{11} + 2x^9 + x^8 + x^7 + 2x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x)$

polinomların aritmetik çarpımı sonucu derecesi 7 den büyük terimler oluşmuştur. Bu terimleri yok edebilmek için $GF(2^8)$'de indirgenemez polinom olan $x^8 + x^4 + x^3 + x + 1$ polinomu kullanılarak modulo alma işlemi uygulanmalıdır. İndirgenemez polinom üzerinde çalışılan sonlu alanda iki farklı polinomun çarpımı olarak ifade edilemeyen polinomlardan seçilmektedir. Yukarıdaki c(x) polinomuna indirgenemez polinom ile modulo alma işlemi uygulanırsa aşağıdaki sonuç elde edilmektedir.

$c(x) = x^6 + x^5 + 1 \equiv \{01100001\}$ olarak bulunur.

2.2 İstatistiksel Kavramlar

Bu bölümde sırası ile *korelasyon* analizi yönteminden, *Kümülant* analizi yönteminden ve *Anova* analizi yönteminden bahsedilecektir.

2.2.1 Korelasyon analizi

Korelasyon iki değişkenin birbirleriyle ne kadar bağlantılı olduğunu gösteren istatiksel bir analiz yöntemidir. Korelasyon analizi yapılır iken genellikle katsayılar üzerinden konuşulur. *Korelasyon katsayısı* analiz işlemine giren iki değişkenin

bağlantılarının ölçüsünü ve yönünü gösterir. Farklı sistemler için farklı farklı korelasyon katsayıları kullanılmaktadır. En çok bilinen katsayı ise 'Pearson Korelasyon Katsayısı'dır [26].

$$C(X,Y) = \frac{E(X \times Y) - E(X) \times E(Y)}{\sqrt{Var(X) \times Var(Y)}} \qquad -1 \le C(X,Y) \le 1 \tag{2.6}$$

Yukarıdaki formülde $C(X,Y)$ korelasyon katsayısını, $E(X \times Y)$ $X \times Y$ 'nin beklenen değerini, $E(X)$ ve $E(Y)$ X ve Y değişkenlerinin beklenen değerlerini, var(X) ve var(Y) de X ve Y değişkenlerinin standart sapma değerlerini vermektedir.

Korelasyon katsayısı -1 ile 1 arasında değerler alabilmektedir. Katsayı değeri -1 ya da 1'e ne kadar yaklaşırsa analizi yapılan iki değişken o kadar bağıntılıdır denir. İkisi de aynı anda artan değişkenler için bağımlılık arttıkça katsayı değeri 1' yaklaşırken, birisi artan diğeri azalan değişkenler için bağımlılık arttıkça katsayı değeri -1'e yaklaşmaktadır.

2.2.2 Kümülant analizi

Moment ve *kümülantlar* işaret özelliklerini karakterize eden istatistiksel terimlerdir [27]. İşaretin olasılık yoğunluk fonksiyonunu karakterize etmek için işaretin 1. momenti (ortalama) ve işaretin 2. kümülantı (standart sapma) kullanılmaktadır. Bir işaret Gauss olasılık yoğunluk fonksiyonu özelliği gösteriyor ise o işareti 1. moment ve 2. kümülant ile tanımlamak yeterli olabilmektedir. Fakat hayatımızda karşılaşılan çoğu işaret Gauss işaret olasılık dağılımına uymaz. Bu yüzden bu işaretleri tanımlayabilmek için daha üst dereceden kümülant hesaplamalarının da işareti tanımlamak için kullanılması gerekmektedir [27].

Normal hayatta kullanılan işaretlerin içerisinde gürültü bileşeninin olduğu bir gerçektir [18]. Kümülant analizi yaparken kullanılan kabul ise bu gürültü bileşeninin Gauss olasılık yoğunluk dağılımına uygun hareket ettiğidir. Diğer bir ifade tarzı ile gürültünün 1. momenti ve 2. kümülantı ile tamamıyla tanımlanabildiği düşünülmektedir. Durum böyle olunca eğer kullanılan işaretin 3. veya daha üst mertebeden kümülantları alındığında o işaretlerde gürültüyü temsil eden bir bileşen bulunmadığından Gauss gürültüsü otomatik olarak süzülmüş olacaktır.

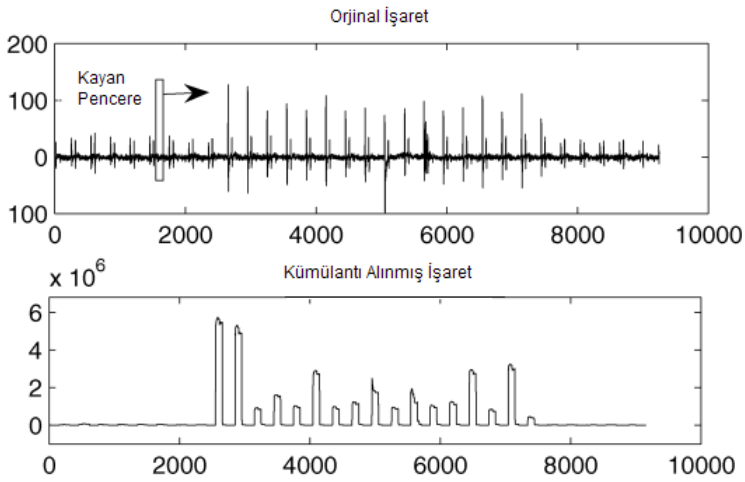
$$K_4(W_{C_l}) = K_4(S_{C_l}) + K_4(B) = K_4(S_{C_l}) \tag{2.7}$$

W_C'yi günlük hayatta kullanılan ham işaret olarak düşünürsek, bu işaretin S_C gibi ilgilenilen kısmı ve B gibi gürültüden oluşan istenilmeyen kısmı vardır. Yukarıda görüldüğü gibi 4. dereceden kümülant hesabı yapıldığında gürültü bileşeni tamamen yok olmaktadır. Elde edilen sonuç sadece istenilen işaretten gelen bileşendir.

Thanh Ha Le'nin makalesinde anlatıldığı gibi 4. dereceden kümülant alma formülü aşağıdaki gibidir [18].

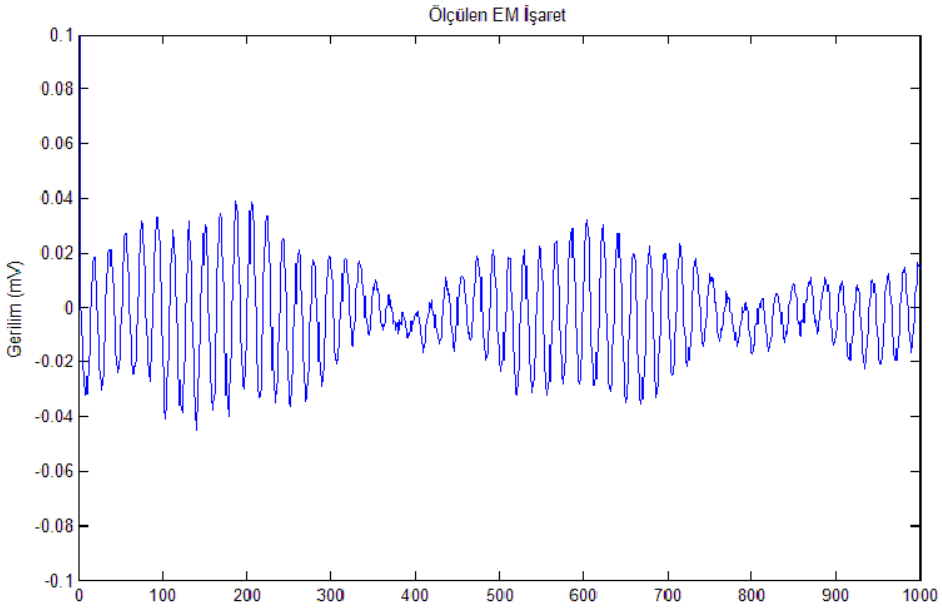
$$k_4(x) = \frac{N_C + 2}{N_C(N_C - 1)} \sum_{i=1}^{N_C} x_i^4 - \frac{3}{N_C(N_C - 1)} \sum_{i,j=1}^{N_C} x_i^2 x_j^2 \qquad (2.8)$$

Bu formülde $k_4(x)$ x işaretini 4. dereceden kümülantını, N_C x işaretinin uzun bir işaret olduğu düşünülürse pencere aralığını, x_i ve x_j işaretlerin belli kısımlarını göstermektedir. N_C parametresi işareti kaç eşit parçaya böldüğümüzü göstermekle birlikte pencereye bölme işlemi yapılıyor iken anlamlı olduğunu düşündüğümüz işaretin parçalarının aynı pencere içerisinde kaldığına dikkat etmek gerekiyor. Diğer bir parametre ise formülde geçmemekle birlikte adım aralığıdır. Uzun işaretler için işlemin çok uzun süreceği düşünülmüş ve adım adım atlayarak kümülant hesabı yapılmıştır. Adım aralığı ne kadar az olursa o kadar hassas değerler elde edilebilmektedir. Çoğu zaman küçük adımlarla tarama yapılıyor iken genel tablodan uzaklaşılabilmektedir. O yüzden bu iki parametre çok dikkatli seçilmelidir. Şekil 2.1 de orijinal işaret ve 4. dereceden kümülantı alınmış işaret gösterilmektedir.

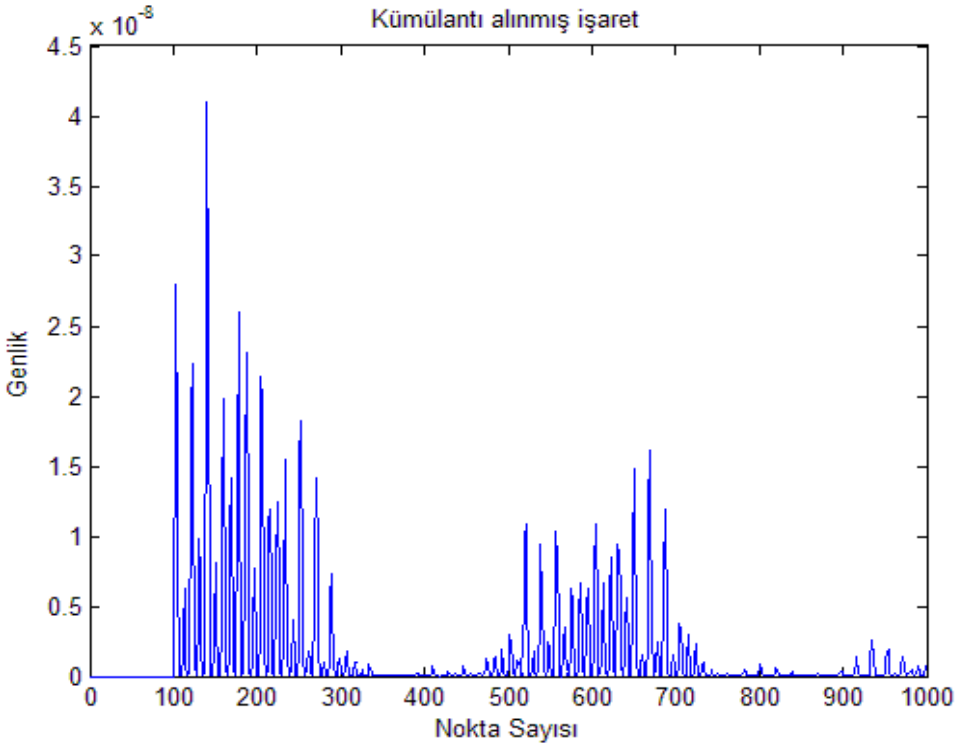


Şekil 2.1 : Orijinal ve kümülantı alınmış işaret

Şekil 2.2' de ise tez kapsamında tasarlanmış EM alıcısı ile alınmış örnek işaret ve şekil 2.3' de de aynı işaretin kümülantı alınmış resmi görünmektedir.



Şekil 2.2 : Tasarlanmış EM alıcısı ile alınmış işaret



Şekil 2.3 : Tasarlanmış EM alıcısı ile alınmış işaretin kümülantı alınmış şekli

Gürültü işaretleri için 3. dereceden kümülantı almak yeterli olacak gibi görünmektedir, yalnız simetrik olasılık yoğunluk fonksiyonlarında 3. dereceden kümülant 0'a eşit olmaktadır. Bu sebeple 4. dereceden kümülant hesaplaması yapılmıştır.

2.2.3 ANOVA analizi

İstatistik biliminde varyansların analizi olarak bilinen (analysis of variance (ANOVA)) istatiksel modellemede kullanılan ANOVA analizi işlem sonucunda gözlemlenen varyansların hangi değişkenlerden kaynaklandığını belirlemek için kullanılan istatistiksel modellerin toplamıdır. Varyansların analizi yöntemi ilk defa istatistik bilimci ve genetik bilimci R. A. Fisher tarafından 1920'li yıllarda geliştirilmiştir. Bu modelin üç kavramsal sınıfı vardır [28].

1- Belirlenmişlerin etkisi modeli

2- Rastgelelerin etkisi modeli

3- Karışıkların etkisi modeli

Anova analizinin işlem sayısına göre ve sisteme nasıl uygulandığına bağlı olmak üzere farklı çeşitleri vardır. Bunlar tek-yol ANOVA, tekrarlanan ölçümler için tek-yol ANOVA ve çoklu ANOVA' dır. Tek-yol ANOVA analizi iki ya da daha fazla bağımsız değişken grubun farklarını bulmak için kullanılır. Grubun içindeki ölçümler tekrarlı ise tekrarlanan ölçümler için tek-yol ANOVA analizi kullanılır. Çoklu ANOVA analizi ise iki ya da daha fazla bağımsız değişken üzerinde çalışılacaksa tercih edilen ANOVA analizi tipidir. Bütün bu farklı çeşitler için toplam farkın hangi kaynaktan kaynaklandığını bulmak için F-test kullanılmaktadır [28].

$$F = \frac{Grup\ Ortalamalarının\ Varyansı}{Grup\ Varyanslarının\ Ortalaması} \tag{2.9}$$

F-test için de (2.9)'daki eşitlik kullanılmaktadır. Genel bir sistem için girişlerdeki değişimin çıkışlara yansımasına göre düzenlenen bu analizde her bir değişkenin çıkıştaki etkisini görmek için kontrollü deneyler yapılmaktadır.

2.3 Elektromanyetik Alan Alıcısı Tasarım Adımları

İlk adım olarak tasarlanacak sistemin özellikleri belirlenmelidir [29]. Sistem özellikleri belirlenirken ise ilk belirlenmesi gereken anten tipidir. 6 çeşit anten tipi vardır.

Otomobillerde, binalarda, gemilerde, uçaklarda, ve uzay araçlarında görmeye alışık olduğumuz en yaygın kullanım alanı olan sınıf tel antenler sınıfı olarak adlandırılır [29]. Tel antenlerin de kendi içerisinde doğrusal tel antenleri, çevrim tel antenleri ve sarmal eğri tel antenleri olmak üzere çeşitleri vardır [29]. Diğer bir sınıf ise çoklukla uzay araçlarında ve uçaklarda kullanılan yüksek frekans özellikleri gösteren açıklığı daralıp genişleyebilen antenlerdir [29]. Çevrenin zararlı durumlarından korumak için bu antenlerin dışı genellikle yalıtkan maddelerle kaplanır. Diğer bir sınıf ticari kullanım alanı olan mikroşerit antenlerdir [29]. Mikroşerit antenler, analizi ve fabrikasyonu kolay olduğu için ve yayınım karakteristiğinin iyi olması sebebiyle yaygın olarak kullanılmaktadır. Tek bir elemanın anten olarak iyi karakteristik gösteremediği durumlarda ise dizi antenleri kullanılabilmektedir. Bunların haricinde kullanım alanı olan diğer iki sınıfı ise yansıtıcı antenler ve lens antenler oluşturur. Sistemin gereksinimlerine bakarak anten tipine karar verilir [29].

Anten tipi belirlendikten sonraki adımda ise hangi anten parametrelerinin bizim için önemli olduğu ve bu parametrelerin sistem tarafından istenen sınır değerlerinin neler olabileceği saptanmalıdır. Birbirleriyle çok bağımsız olmamakla beraber en önemli parametreler; ışınım deseni, ışınım güç yoğunluğu, ışınım yoğunluğu, yönlülük, anten ışınım verimliliği, kazanç ve band aralığı parametreleridir [29].

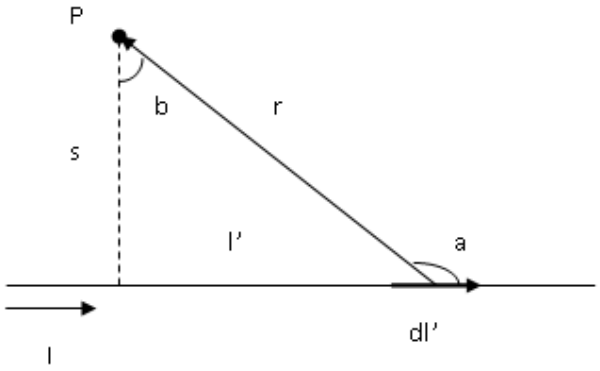
Işınım deseni, antenin ışınım özelliklerinin uzay koordinatlarında matematiksel fonksiyonları ya da grafiksel gösterimleri olarak tanımlanır [30]. Elektromanyetik dalgalar kablosuz ortamlarda ve kılavuzlanmış yapılarda bir noktadan diğer bir noktaya bilgi taşımak için kullanılırlar. Bu durumda elektromanyetik alanların güç ve enerji ile ilişkilendirilmesi doğru bir yaklaşım olacaktır. Işınım güç yoğunluğu ise elektromanyetik alan ile ilişkilendirilen bu gücün belli bir alandan birim zamanda geçen kısmı olarak tanımlanır [30]. Işınım yoğunluğu ise verilen bir doğrultuda antenin birim açı ile yaydığı güç yoğunluğu olarak adlandırılır. Matematiksel olarak ışınım güç yoğunluğunu uzaklığın karesi ile çarparak hesaplanır. Diğer en önemli parametrelerden birisi olan yönlülük ise, verilen bir doğrultuda antenin ışınım

yoğunluğunun bütün doğrultularda ortalama yayınım yoğunluğuna oranı olarak tanımlanır. Ortalama ışınım yoğunluğu, matematiksel olarak antenin yaydığı toplam gücün 4*Π ile bölünmesidir. Anten ışınım verimliliği parametresi ise, antenin giriş ucundan ve yapısından kaynaklanan kayıpları dikkate alarak hesaplanır. Kayıplar genellikle iki sebeple oluşur. İletim ortamı ve anten arasındaki uyumsuzluktan kaynaklanan yansımalar ve iletim ile yalıtım arasındaki I^2*R kayıpları bu bahsedilen iki temel kayıbı oluşturur. Antenin performansını tanımlayan diğer bir parametrede kazançtır. Kazanç yönlülükle tamamen ilgili gibi görünse de, yönsel yeteneğinin olmasının yanı sıra anten ışınım verimliliğini de göz önünde bulundurması bakımından yönlülük parametresinden ayrılır. Hatırlanacak olursa yönlülük parametresi antenin sadece yönsel özelliklerini gösteren ışınım deseni ile kontrol edilen bir nicelikti. Sonuç olarak kazanç, verilen bir doğrultuda ışınım yoğunluğunun anten tarafından alınan izotropik olarak yayılan ışınım yoğunluğuna oranı olarak tanımlanır. İzotropik yayınan güce karşılık gelen ışınım yoğunluğu anten tarafından alınan gücün 4Π ile bölümüyle elde edilir. Son olarak band aralığı ise antenin istenilen özellikleri göstererek çalıştığı frekans aralığı olarak tanımlanır. Her antenin çalıştığı belli bir band aralığı vardır. [30]

Bunların yanı sıra sistemler yakın alan alıcısı sistemleri ve uzak alan alıcısı sistemleri olarak ikiye ayrılırlar [30]. Yakın alan alıcısı sistemleri, sisteme çok yakın bölümlerinde elektromanyetik işaretin anlamlı olduğunu durumlarda kullanılır. Uzak alan alıcısı sistemi ise, sistemden uzak bölümlerde elektromanyetik işaretin anlamlı olduğu durumlarda kullanılır. Yukarıdaki adımlar uzak alan alıcısı sistemleri için çok iyi sonuçlar verebiliyor iken yakın alan alıcısı sistemleri için de yol gösterici nitelik taşımaktadır. Aşağıda yakın alan alıcısı sisteminin matematiksel ifadesi hakkında bilgi verilmektedir.

2.4 Yakın Alan Alıcısı Sisteminin Matematiksel İfadesi

Bakır ince bir telden akım geçtiğini düşünelim. Bu akımın uzaktaki bir P noktasındaki elektromanyetik davranışına bakalım.



Şekil 2.4 : Üzerinden akım geçirilen telin s uzaklığındaki manyetik davranışı

İlk olarak şekle bakarak birkaç trigonometrik denklemi yazmamız gerekmektedir.

$$l' = s * \tan b \qquad => \qquad dl' = \frac{s}{\cos^2 b} * db \quad [31] \tag{2.10}$$

$$s = r * \cos b \qquad => \qquad \frac{1}{r^2} = \frac{\cos^2 b}{s^2} \qquad [31] \tag{2.11}$$

İkinci olarak çizgi akımın manyetik alanını veren *Biot-Savart yasasının* denklemi yazılır.

$$\mathrm{B(r)} = \frac{u_0 I}{4\Pi} \int \frac{\mathrm{r*dl'}}{\mathrm{r}^2} \qquad [31] \tag{2.12}$$

u_0 = serbest uzayın geçirgenliği => $u_0 = 4 \times \Pi \times 10^{-7}$ $(\mathrm{N/A^2})$

$r \times dl$ sayfanın dışına doğru yönelmiştir ve büyüklüğü aşağıdaki gibidir.

$$dl' \times \sin a = dl' \cos b \quad [31] \tag{2.13}$$

(2.10), (2.11) ve (2.13) deki bilgiler (2.12) denkleminde kullanılacak olursa;

$$B = \frac{u_0 I}{4\Pi} \int_{b_1}^{b_2} \left(\frac{\cos^2 b}{s^2}\right)\left(\frac{s}{\cos^2 b}\right) \cos b db \;=\; \frac{u_0 I}{4\Pi s} \int_{b_1}^{b_2} \cos b db \;=\; \frac{u_0 I}{4\Pi s} (\sin b_2 - \sin b_1) \tag{2.14}$$

denklemi bulunur [30]. Yakın alan alıcısı sisteme çok yakın tutulacak olursa ölçüm yapılan telin uçlarının alıcı sistemine olan açıları $b_1 = -\Pi/2$ ve $b_2 = \Pi/2$ olarak alınabilir. Bu durumda manyetik alan için yeni formül;

$$B = \frac{u_0 I}{2\pi s} \qquad \text{olarak bulunur [31].} \tag{2.15}$$

Manyetik alan bulunduktan sonra yapılması gereken manyetik akıya geçmek ve onu formüle etmek olacaktır. Belli bir yüzeydeki manyetik akı; manyetik alanın yüzeye normal bileşeninin o yüzey ile integrasyonuyla bulunur.

$$\Phi = \int_S B_n da \quad [32] \tag{2.16}$$

Yüzey integrali olduğundan integral çift katlıdır. B_n yüzeye dik olarak gelen manyetik alanı, *da* alıcı sisteminin çevriminin boyutunu ifade eder.

Manyetik akı hesaplandıktan sonraki basamakta ise yapılması gereken *Faraday indüksiyon yasası* uyarınca manyetik akıdan alıcı sistemde akım oluşturmak ve alıcı sistemin iki ucu arasındaki gerilimi hesaplamak olacaktır.

$$V = \frac{d\Phi}{dt} \qquad (\textit{Faraday indükleme yasası}\ [32]) \tag{2.17}$$

Bu hesap akımın aniden düştüğü ya da aniden yükseldiği noktalar için yapılmıştır. Sayısal devrelerin çalışma prensibine de uyan bu sistem sayısal devrelerin manyetik yayınımını almak için kullanılabilecektir.

3. GELİŞMİŞ KODLAMA STANDARDI ALGORİTMASI (AES)

Teknolojinin gelişmesi ve çok hızlı bir şekilde gelişeceğinin bilinmesi yadsınamaz bir gerçektir [11]. Teknolojinin gelişmesi ile birlikte bilginin bir noktadan başka bir noktaya transferi için çok çeşitli yollar bulunmuştur. Yalnız transfer edilecek bilginin gizliliği önemli ise transferi sırasında korunmasına dikkat edilmesi gerekmektedir. Bu noktada bilginin gizli transferi için kriptografi bilimi gelişmiştir. Kriptografi bilimi sayesinde birtakım şifreleme, anahtarlama, çözme, sayısal imzalama algoritmaları geliştirilmiştir [11]. Bu algoritmaların teknolojinin gerektirdiği şekilde olacağı, teknolojiye ayak uyduramayanların kullanımının terk edileceği, yeni algoritmaların bulunacağı bilinen bir gerçektir.

Teknoloji ile gelişen bu algoritmalar standartlaşma ihtiyacı hissetmektedir. Bu yüzden birçok ülke kendi standartlaşma enstitüsünü kurmuştur. ABD Ulusal Standartlar ve Teknolojiler Ensititüsü (NIST)' de bunlardan birisidir. Bu bölümün devamında NIST' ın standart olarak kabul ettiği AES algoritması ayrıntılı olarak incelenecektir.

3.1 AES Algoritması için Kullanılan Aritmetik İşlemler

AES algoritması şifreleme ve çözme işlemlerini yaparken Galois sonlu uzayını kullanmaktadır [11]. Aşağıda sırası ile AES algoritması için kullanılan GF(2^8) de aritmetik işlemlerden toplama ve çarpma anlatılacaktır.

3.1.1 GF(2^8)'de toplama

2. Bölümde anlatıldığı üzere toplama işlemi toplanacak olan 2 baytın karşılıklı bitlerinin xor işleminin sonucudur [25].

{5A} değerinin polinom gösterimi $x^6 + x^4 + x^3 + x^1$ şeklindedir.

{DA}değerinin polinom gösterimi $x^7 + x^6 + x^4 + x^3 + x^1$ şeklindedir.

Bu iki değerin toplamı ise karşılıklı bitlerini xor işlemine soktuğumuz vakit X^7 olarak bulunmaktadır. Bu da yine aynı $GF(2^8)$ de olup {80} değerine eşit olmaktadır.

3.1.2 GF(2^8)'de çarpma

2. Bölümde anlatıldığı üzere 2 bayt çarpılıyor iken klasik çarpma kaydırma işlemi yapılır daha sonra alt alta yazılan bu değerler xor işlemine tabi tutulur [25]. Çarpma işlemi için indirgeme polinomu $x^8 + x^4 + x^3 + x + 1$ şeklindedir. Çıkan çarpım sonucu $GF(2^8)'$ de değil ise indirgeme polinomu yardımı ile bu alana çekilir. $GF(2^8)'$ de bütün değerlerin bu indirgeme polinomuna göre çarpmaya göre tersleri mevcuttur.

3.2 AES Algoritması

AES Algoritması genel olarak tur işlemlerinin ve tur işlemlerinin içerisinde gerçekleştirilen tur dönüşüm işlemlerinin bir bütünü olarak düşünülür [2].

3.2.1 AES algoritması tur işlemleri

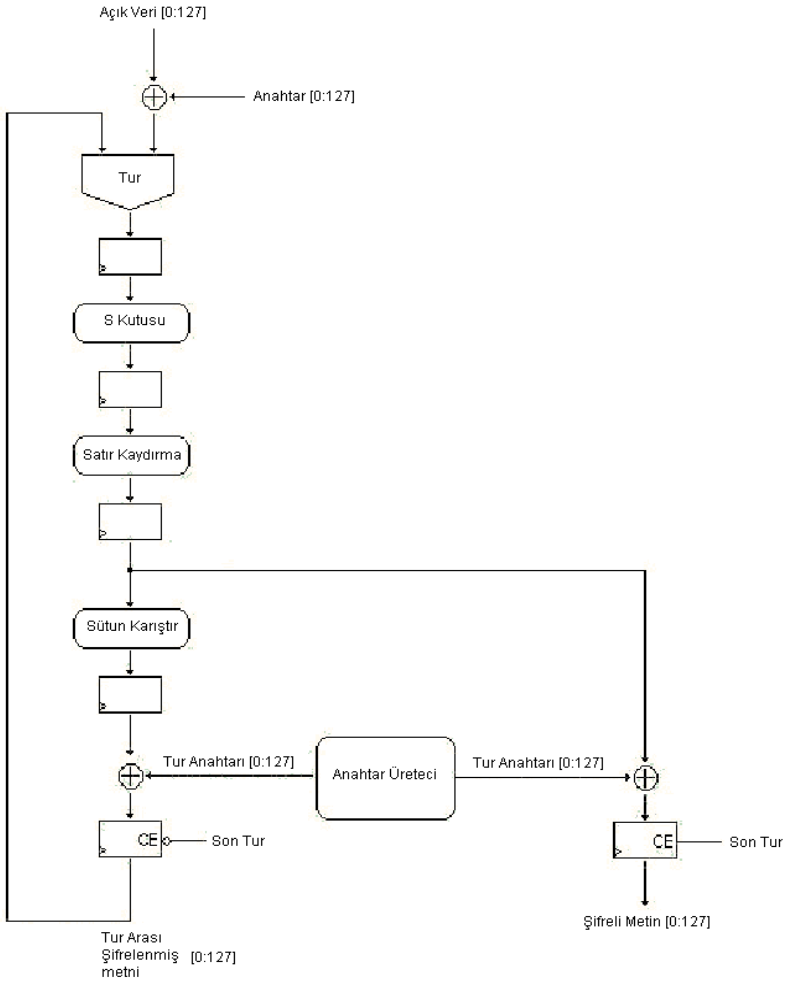
AES algoritması 128 bit veriyi şifrelemek ve çözmek için oluşturulmuş simetrik veri kodlama standardıdır. 128 bit veriyi şifrelemek/çözmek için 128 bit, 192 bit ve yahut 256 bit anahtar uzunlukları kullanılabilmektedir. Bu kullanılan anahtarın uzunluğuna göre tur sayısı değişiklik göstermektedir. Çizelge 3.1 de gösterildiği gibi 128 bit anahtar uzunluğu için 10 tur, 192 bit anahtar uzunluğu için 12 tur ve 256 bit anahtar uzunluğu için 14 tur işlem yapılmaktadır [2].

Çizelge 3.1 : Tur sayısının anahtar uzunluğuna göre belirlenmesi

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

AES algoritması 2 temel yapıdan oluşmaktadır. Bunlar şifreleme/çözme ve anahtar üreteci yapılarıdır. 128 bitlik anahtar uzunluğu için şifreleme/çözme işlemlerinde 10 tur işlem yapılıyor iken aynı zamanda her tur için farklı bir anahtar, anahtar üreteci yapısı sayesinde ana şifre kullanılarak üretilmektedir. Şekil 3.1 de AES Algoritmasının genel yapısı görülmektedir. Şifreleme/Çözme işlemi ise sırası ile ilk anahtar toplanması, tur sayısının 1 eksiği kadar tur işlemleri ve son olarak da final tur işleminden oluşmaktadır.

16 baytlık giriş verisi ilk olarak ana anahtar ile bit bit xor işlemine sokulur, devamında tur sayısının 1 eksiği kadar tur işlemleri ana anahtardan oluşturulan farklı anahtarlar kullanılarak gerçekleştirilir. Bu arada bir önceki turun çıkışı bir sonraki tur için giriş verisini oluşturmaktadır. Son olarak ise final turu gerçekleştirilir ve şifrelenmiş veri elde edilmiş olur.



Şekil 3.1 : AES algoritması blok şeması [11]

3.2.2 AES algoritması tur dönüşüm işlemleri

Bu bölümde AES algoritmasının kodlama yapılırken gerçekleştirdiği tur işlemlerinin içerisindeki yapılar anlatılacaktır. Bu yapıların her birisi birer adım olarak adlandırılır. Durum tanımlama işlemi gerçekleştikten sonra final tur hariç olmak üzere turlar aşağıdaki 4 adımı gerçekleştirirler. Final turunda ise sütunları karıştırma işlemi hariç olmak üzere diğer 3 adım gerçekleştirilir [2].

1- Bayt yer değiştirme,
2- Satırları kaydırma,
3- Sütunları karıştırma,
4- Tur anahtarının toplanması,

Bu adımlar sırası ile gerçekleştirilince 1 tur tamamlanmış olur. 1 tur tamamlandıktan sonra bu turun çıkışları bir sonraki tur için girişi oluşturur ve tur dönüşüm işlemleri aynı sıra ile devam ettirilir. Final turuna gelindiğinde ise bahsedildiği gibi sütunları karıştırma işlemi atlanarak tur anahtarı işlemi gerçekleştirilir. Bu işlem gerçekleştirildikten sonra ise kodlanmış veri elde edilmiş olur.

AES algoritması ile kodlama işleminin yapılabilmesi için öncelikle 16 baytlık kodlanacak verinin durum tanımlaması yapılır. Durum tanımlama işlemi 16 baytlık veriyi 4×4 'lük matris haline getirmektir. Bu işlem Çizelge 3.2 de gösterildiği gibi yapılmaktadır.

Çizelge 3.2 : Durum atanması işlemi

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}

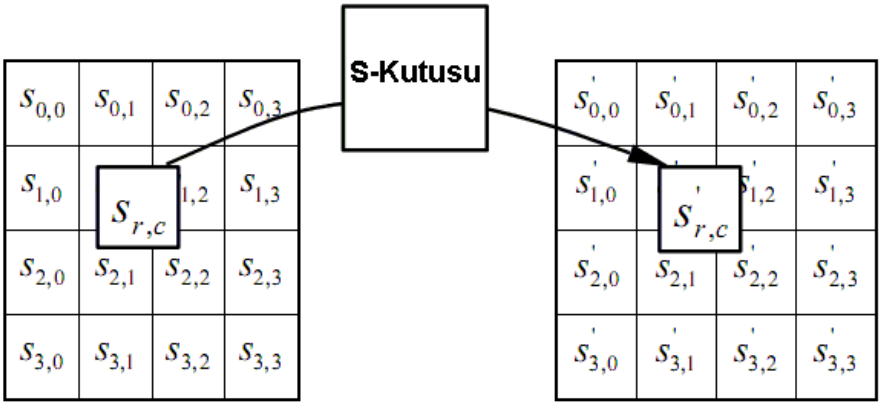
Tablodaki gibi 4×4 ' lük matris haline getirdikten sonra ise diğer tur dönüşüm işlemleri yapılacaktır.

3.2.2.1 Bayt yer değiştirme

Bayt yer değiştirme işlemi durum atanmasından sonraki tur işlemlerinin ilk adımını oluşturur. Bayt yerdeğiştirme işleminde 4x4 'lük matris içerisinde bulunan her bir baytın yeri S-kutusu tablolarına bakılarak yer değiştirilir. Bayt yer değiştirme işlemi AES algoritması içerisinde doğrusal olmayan tek işlemdir. Bayt yerdeğiştirme işleminin tersinin alınması mümkündür. Şekil 3.2 'de bayt yer değiştirme işlemi gösterilmektedir. Bayt yer değiştirme işlemi ise Çizelge 3.3 'deki S-kutusu kullanılarak yapılmaktadır [2].

Çizelge 3.3 : S-kutusu

	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



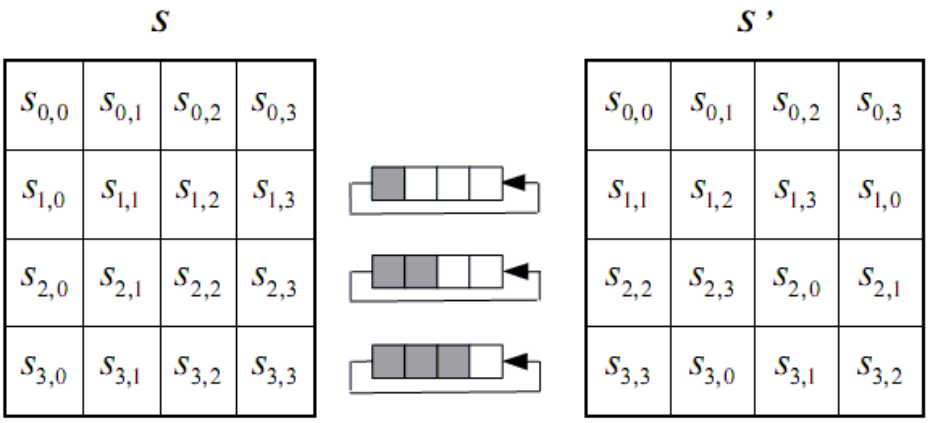
Şekil 3.2 : Bayt yer değiştirme işlemi

3.2.2.2 Satırları kaydırma

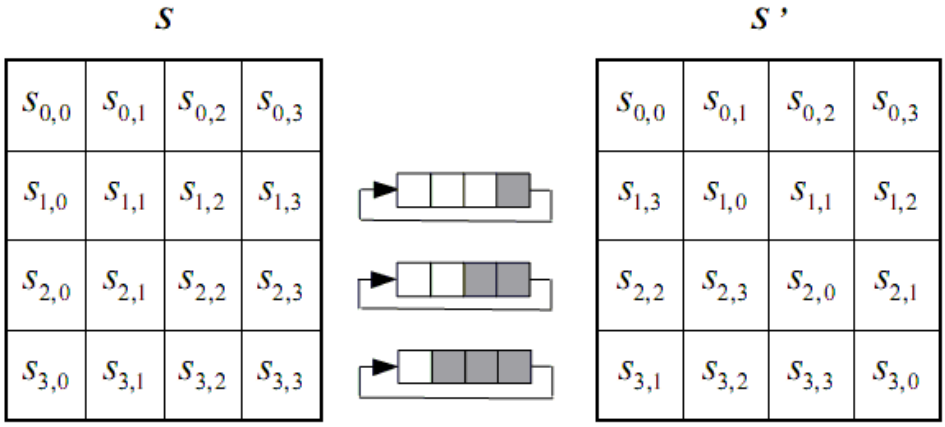
Satır kaydırma işlemi bayt yer değiştirmeden sonraki tur işlemlerinin 2. adımını oluşturmaktadır. Satır kaydırma işlemi doğrusal olan bir işlemdir. Kodlama işlemi sırasında satır kaydırma işleminin kendisi kullanılırken çözme işlemi sırasında tersi kullanılmaktadır [2].

Satır kaydırma işlemi adından da anlaşılacağı gibi satırlar üzerinde yapılan bir işlemdir. Şekil 3.3 de gösterilmiş olduğu gibi satır kaydırma işlemi sırasında ilk satıra herhangi bir işlem uygulanmaz. İkinci satır ise sağdan sola doğru 1 adım kaydırılır.Şekil 3.3 de gösterildiği gibi 2. satırın 1. sütunu 4. sütunu yerine geçmektedir. Yine benzer şekilde 3. Satır sağdan sola doğru 2 adım kaydırılır. Son olarak da 4. Satır sağdan sola doğru 3 adım kaydırılır.

Tersi işleminde ise Şekil 3.4 de gösterilmiş şekliyle işlem yapılır. 1. satır için kaydırma yapılmaz. 2. satır 1 adım soldan sağa, 3. satır 2 adım soldan sağa ve son olarak da 4. satır 3 adım soldan sağa kaydırılır. Tersi işlemi bahsedildiği gibi kodlamanın çözülmesi sırasında kullanılmaktadır.



Şekil 3.3 : Satır kaydırma işlemi



Şekil 3.4 : Satır kaydırma tersi işlemi

3.2.2.3 Sütunları karıştırma

Sütunları karıştırma işlemi satırları kaydırma işleminden sonraki tur işlemlerinin 3. adımını oluşturur. Sütun karıştırma işlemi doğrusal olan bir işlemdir. Çözme işleminde sütunları karıştırma işleminin tersi işlemi yapılmaktadır [2].

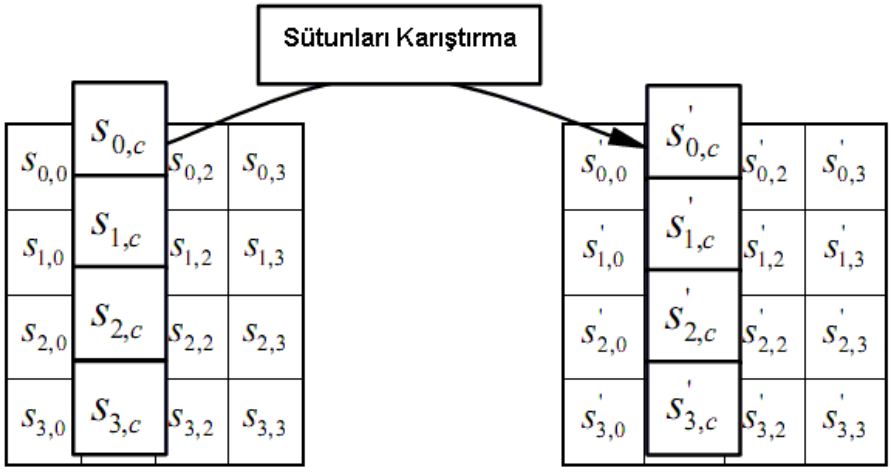
Sütunları karıştırma işleminde adından anlaşılacağı üzere sütunlar üzerinde işlem yapılmaktadır. Her bir sütun 3. dereceden polinom olarak ifade edilmektedir. İşlemler bütün AES algoritmasında olduğu gibi bu işlemde de $GF(2^8)$ de yapılmaktadır. İşleme sokulacak sütun polinom olarak ifade edildikten sonra sabit bir polinomla çarpılmakta ve x^4+1 ile modu alınmaktadır. Çarpma için kullanılan polinom aşağıdaki gibidir.

$$a(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x^1 + \{02\} \tag{3.1}$$

Sütunları karıştırma işleminden önceki sütunların oluşturduğu polinoma s(x), sütunları karıştırma işleminden sonraki sütunların oluşturduğu polinoma s'(x) denirse s'(x) polinomu aşağıdaki şekildeki gibi oluşturulmaktadır.

$$s'(x) = a(x) \times s(x) \tag{3.2}$$

Şekil 3.4 de sütunları karıştırma işlemi gösterilmektedir.



Şekil 3.5 : Sütunları karıştırma işlemi

Kodlamayı çözme işleminde ise sütunları karıştırma işleminin tersi kullanılmaktadır. Ters alma işleminde de yine her bir sütun 3. dereceden polinomlar ile ifade edilir. Kodlama kısmında olduğu gibi sabit bir polinom ile çarpılmakta ve $x^4 + 1$ ile modu alınmaktadır. Yalnız ters alma işlemindeki sabit polinom $GF(2^8)$ de kodlama işleminde kullanılan sabit polinomun çarpmaya göre tersi olarak hesaplanır. Çözme işleminin hesaplanan sabit polinomu aşağıdaki gibidir [2].

$$d(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x^1 + \{0e\} \tag{3.3}$$

3.2.2.4 Tur anahtarının toplanması

Tur anahtarının toplanması işlemi sütunları karıştırma işleminden sonraki tur işlemlerinin son adımını oluşturur. Bu adımda 128 bitlik veriyi şifrelemek için her tur için farklı olmak üzere ana şifreden 128 bit uzunluğunda tur anahtarları oluşturulur. Tur anahtarları ana şifreden anahtar üreteci algoritması ile elde edilmektedir [2].

Anahtar üreteci yapısı tur anahtarları matrislerini oluşturur. Bu matris $4\times(N_R+1)$ boyutunda bir matristir. Aşağıda anlatıldığı gibi üretilmektedir.

1-İlk N_k sütun ana şifre yazılarak Çizelge 3.4 'deki gibi oluşturulur.

Çizelge 3.4 : Anahtar üreteci ilk N_k sütunu

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}

2-Sonraki sütunlar, kendisinden bir önceki sütun ile N_k önceki sütunun karşılıklı baytlarının xor işlemi yapılarak oluşturulur. Yalnız oluşturulmakta olan sütun numarası N_k 'nın tam katı olan bir sütun numarası ise bu sütun oluşturulurken kendisinden bir önceki sütun bir dönüşüm işleminden geçirildikten sonra kendisinden N_k önceki sütun ile karşılıklı bayt bayt xor işlemine sokulur.Bu dönüşüm ise 3 adımda yapılmaktadır [2].

a- Dönüşümün ilk adımında sütunda 1 adım kaydırma işlemi yapılır. Üzerinde işlem yapılacak sütun aşağıdan yukarıya doğru olmak üzere 1 adım döngüsel olarak kaydırılır. Örnek olarak Çizelge 3.3 'deki 3. sütunu kaydıralım.

$$\{K_8, K_9, K_{10}, K_{11}\} \rightarrow \{K_9, K_{10}, K_{11}, K_8\}$$

b- Dönüşümün ikinci adımında ise bayt yer değiştirme işlemi uygulanır. Bu işlem için bölüm 3.2.2.1 ' de anlatıldığı gibi S-kutusu kullanılır.

c- Dönüşümün son adımında ise elde edilen sütun tur sabiti işlemi ile xor işlemine sokulur. Bu tur sabiti çizelge 3.5 'de gösterildiği gibi bütün turlar için değişen bir sabittir.

Çizelge 3.5.: Anahtar üreteci tur sabitleri

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

Bu şekilde anahtar üreteci ile tur anahtarı matrisleri $4\times(N_R+1)$ boyutunda olmak üzere oluşturulur. Bu matrisin yan yana gelen 4 sütunu 128 bitlik tur anahtarlarını oluşturmaktadır.

3.3 AES Algoritmasının Maskelenmesi

Bir sonraki bölümde anlatılacak olan DPA analizi ve DEMA analizi yöntemleri AES gerçeklemeleri için büyük tehditler oluşturmaktadır [7, 8, 9]. İşlenen gizli bilgi güç analizi ve elektromanyetik analizi yardımı ile elde edilebilmektedir. Bu yüzden AES algoritmasının gerçeklemelerini DPA ve DEMA analizlerine karşı kuvvetlendirme ihtiyacı hissedilmiştir. Bu saldırılara karşı AES gerçeklemelerini kuvvetlendirmeye yönelik çeşitli çalışmalar yapılmıştır [14, 15]. Bu yöntemlerden sadece maskeleme yöntemi anlatılacaktır. Bu kuvvetlendirmeye karşı maskeleme yöntemi kullanılarak gerçeklenen devrelerde anahtarı bulmak için de çeşitli çalışmalar yapılmaktadır [15]. Bizim üzerinde çalıştığımız bir yöntem aşağıda anlatılmaktadır.

3.3.1 AES maskesiz gerçeklemesi için farksal EM analizi

Farksal güç analizi (DPA) [7] ve farksal elektromanyetik analizi (DEMA) [8, 9] birçok ölçüm alınarak yapılan saldırı yöntemleridir.

1- Bu iki analiz için de analizi yapılacak olan bölge öncelikle tespit edilir.

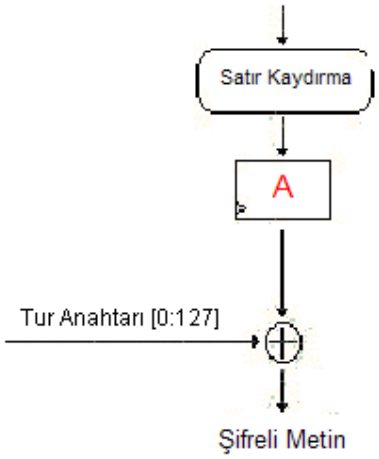
2- Gerçeklenen algoritmanın yan kanal bilgisi veren bölümü tahmin edildikten sonra ise tahmin edilen işlem (örnek: satır kaydırma işlemi) ile ilgili ölçümler alınır. İşlem ile ilgili ölçümlerden kastedilmek istenen sadece o işlem

yürütülürken ölçüm almaktır. Her ölçümde 1000 nokta olduğunu ve 10000 ayrı ölçüm alındığı düşünülürse elde edilen matris 10000 satır ve 1000 sütundan oluşmaktadır. Bu matrise M_1 matrisi adını verelim. $M_1(10000\times1000)$ ölçüm matrisidir. İşaretteki gürültünün etkisinden kurtulmak için M_1 matrisinin satır ortalaması alınmıştır ve matris $M_2(10000\times1)$ matrisine dönüştürülmüştür.

Güç kaynağının o anda tükettiği bütün dinamik güç ölçüm değerlerinin içinde yerini alacaktır. Tahmin edilen işlemin dışında yapılan diğer bütün işlemler gürültü olacaktır ve analiz için işleri zorlaştıracaktır. Yalnız gürültü probleminden de ölçüm sayısını makul derecede artırarak kurtulunabilmektedir.

3- Ölçümler alındıktan sonra ise yapılması gereken tahmin matrislerinin oluşturulmasıdır. Bu matrise M_3 adını verelim. Bunun için çeşitli modeller mevcuttur. Bunlardan birisi Hamming ağırlığı modelidir [32, 33]. Bu modele göre o tahmin edilen işlem yürütülürken kaydedicilerde bulunan bir sayısı toplanır. Bütün olası anahtar değerleri için işlem benzetim ortamında yürütülür ve bir sayıları toplam değerleri için matris oluşturulur. Ölçüm alma adımındaki gibi 10000 ayrı giriş için bütün anahtarlar kullanılarak tahmin matrisleri oluşturulacaktır. Bu girişler aynı zamanda ölçüm alma adımındaki ölçümlerin girişlerinin aynısıdır. Anahtarın bir baytına saldırı yapıldığı düşünülürse 256 farklı anahtar değeri mevcuttur. Aynı zamanda bir baytta en az sıfır tane bir ve en fazla sekiz tane bir olacağından tahminler matrisi sıfır ile sekiz arasındaki değerlerden oluşacaktır. Girişler tahmin matrisinin satırlarını anahtar değerleri ise sütunlarını oluşturmaktadır. Buna göre M_2 matrisi 10000 satır ve 256 sütundan oluşacaktır. $M_3(10000\times256)$ tahmin matrisidir. Matris oluşturulurken değerlerine bakılan kaydedici Şekil 3.6' daki A kaydedicisidir ve sadece birinci baytının değerlerine bakılmaktadır. Şekil 3.6 AES algoritmasının son tur işlemini göstermektedir.

4- Bu matris (M_3) ile ölçümlerden elde edilen güç tüketimi matrisi (M_2) sütun sütun korelasyon işlemine sokulur. Korelasyon sonucunda tahmin matrisinden (M_3) en yüksek korelasyonu veren sütun değeri anahtar olarak düşünülür.



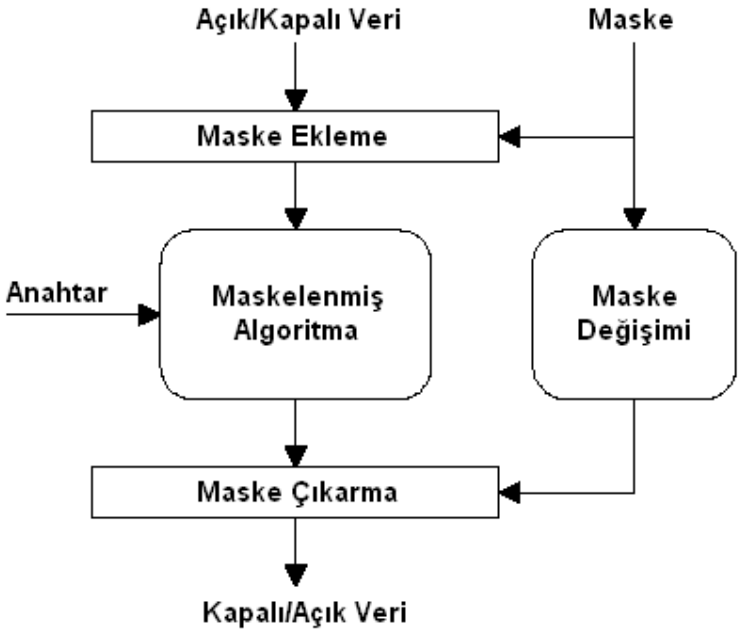
Şekil 3.6 : Tahmin matrisi için kullanılan kaydedici

Bu modele göre daha sağlıklı sonuçlar veren ancak hesaplaması zor olan diğer bir model ise Hamming uzaklığı modelidir [34]. Bu modele göre tahmin edilen o işlem sırasındaki 0→1 geçişleri sayılır ve onların toplamı tahmin matrisini oluşturur. Bu modelde kaydedici için geçiş durumunu bilmek gerektiği için bir önceki tur aynı kaydedicinin değerlerine de ihtiyaç olacaktır. Bunun için de bir önceki tur anahtarına ihtiyaç olacaktır. Yine bir önceki modelde olduğu gibi bu modelde de ölçümler alınarak korelasyon işlemi gerçekleştirilir. En yüksek korelasyonu veren tahmin elemanı anahtar olarak düşünülebilir.

3.3.2 Maskeleme yöntemi

Yukarıdaki adımlar gerçekleştirildiğinde kuvvetli olarak bilinen bir standardın (AES) bizim yaptığımız maskesiz gerçeklemesinin anahtarı elde edilebilmektedir [7, 8, 9]. Anahtar bilgisi sızıntısını engellemek için yapılması gereken ise kullanıcı tarafından değiştirilemeyen ve gözlenemeyen bir değişkenin daha kodlama gerçekleştirilirken kullanılır hale getirilmesidir. Bu değişken maske olarak adlandırılmaktadır [11]. Bu maskenin eklenmesi AES algoritmasının gerçeklemesini tamamıyla güvenilir hale getirmeyecek sadece alınması gereken ölçüm sayısını artıracaktır. Maskeleme işlemi yapılırken ilk olarak devrenin içerisinden rastgele üretilen bir değer ile kodlanacak veri toplanır. Daha sonra şifreleme bittikten sonra ise maskeyi ortadan kaldırmak için

maske kaldırma işlemi yapılır. Maske kaldırma işleminin yapılabilmesi için ise maskenin algoritma yürütülürken nasıl değişikliklere uğrayacağı ayrıca hesaplanır. Maskeleme adımları, maskenin etkisini giderici değerinin hesaplanması ve maskenin kaldırılması adımları Şekil 3.7' de gösterilmiştir.



Şekil 3.7 : AES Algoritması maskeli gerçeklemesi [11]

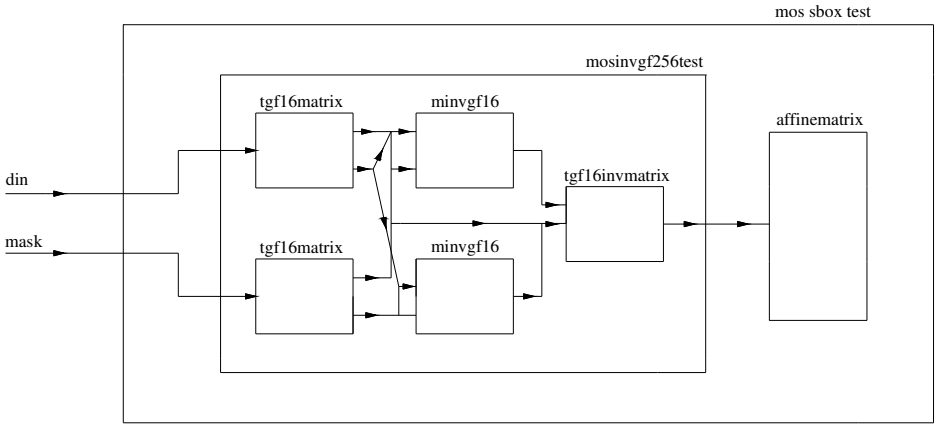
$f(x) = 2x$ iken $f(x+m) = 2x + 2m$ eşitliğini sağlayan sistemlere doğrusal sistemler denmektedir. $f(x) = x^2$ iken $f(x+m) = x^2 + 2xm + m^2$ şeklinde olan sistemlere ise doğrusal olmayan sistemler denmektedir. AES algoritması doğrusal olan işlemlerin yanı sıra doğrusal olmayan işlem de içermektedir. Bayt yer değiştirme işlemi AES algoritması içerisindeki doğrusal olmayan işlemdir. Maskeleme işlemi devrenin girişinde eklendikten ve şifreleme tamamlandıktan sonra maskenin etkisini sağlıklı bir şekilde kaldırmak için doğrusal olmayan bayt yer değiştirme işleminden sonra doğrusal olmayan sistemi doğrusal davranır hale getirmek için yeni bir işlem eklenmelidir. yukarıdaki doğrusal olmayan işlemden $2xm$ çıkarmak yeni bir işlem eklemek anlamına gelmektedir. Bu işlemden sonra sistem doğrusal davranacak şekildedir. Düzeltme işlemi ile yeni sistem $f(x+m) = x^2 + m^2$ şekline dönüşmüştür. AES algoritmasını maskeli gerçeklemesini doğrusal işlem yapar hale getirmek için ise bayt yer değiştirme işleminde bazı değişiklikler yapılmalıdır. Bayt yer değiştirme işlemi içerisindeki doğrusal olmayan işlem ters alma işlemidir. Bu işlemi doğrusal

hale getirmek maskeyi sağlıklı olarak kaldırmak için yeterli olacaktır. Bu alanda ilk çalışma Akkar [14] tarafından yapılmıştır. Bu tezde analizi yapılan ise Oswald'ın [15] maskeleme yönteminin bir gerçeklemesidir.

3.3.3 Maskenin etkisini yok etme yöntemi

Yukarıda anlatıldığı gibi rastgele bir değerin algoritmada kullanılması ölçüm sayısını artırmıştır. Bu durumda ise saldırı yapan kişinin yapması gereken bir şekilde maskenin etkisini ortadan kaldırmak ve DPA ya da DEMA işlemlerini tekrar yapmaktır [6, 7]. Bunun bir yöntemi ise S-kutusu işlemine saldırı yapıldığı düşünülürse s-kutusu içerisinde kombinezonsal devre elemanlarının geçiş sayılarını saymaktır. Aşağıda anlatılan bütün adımlar Şekil 3.9'daki gibidir.

1- Ana anahtardan 8 bit anahtar parçası elde edilmeye çalışılırsa bu durum için 256 değişik bayt yer değiştirme işlemi girişi ve aynı şekilde 256 değişik maske değeri vardır. Ölçümler alınırken kullanılan maske bunlardan 1 tanesidir. Simülasyon programı ile bütün maskelerin bütün girişleri için bayt yer değiştirme işlemi yürütülecektir. Bu sırada kombinezonsal devre elemanlarının geçiş sayıları hesaplanacaktır. 256 girişi satır olarak ve 256 maske değerini de sütun olarak düşünürsek elimizde $M_4(256\times256)$ lık bir matris olacaktır. Bu matrisin her bir elemanı herhangi bir giriş ile herhangi bir maske kullanılarak elde edilmiş kombinezonsal devre elemanlarının geçiş sayısını verecektir. Geçişleri sayılacak olan kombinezonsal devre Şekil 3.8'deki gibidir.

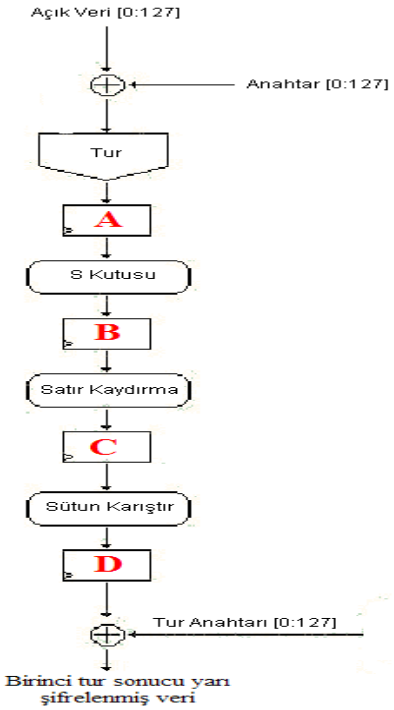


Şekil 3.8 : Tahmin değerleri için geçişleri sayılan kombinezonsal kısım

2- M_4 matrisinin bütün satırlar için ortalama aldığımızda ise maskenin etkisinin yok olacağını düşünmekteyiz. Bu durumda elimizde $M_5(256\times1)$'lık satırları bayt yer değiştirme işlemi girişi olan ve hücrelerinde kombinezonsal devre geçiş sayıları olan matris olacaktır.

3- Bu M_5 geçiş sayıları matrisi anahtar toplama işleminin çıkışıdır. M_5 matrisinin satırları anahtar toplama işleminin tersi işlemine sokularak M_6 matrisi oluşacaktır. Yalnız bu işlem için anahtarın olası bütün değerleri (256) kullanılacağından satırları şifrelenecek verinin ilk 8 biti ve sütunları anahtarın ilk 8 bitinden oluşan geçişler matrisi oluşmuş olacaktır. Nihayetinde M_4 matrisi $M_6(256\times256)$ şeklinde olacaktır.

4- Yukarıda maskesiz bir sistemde 128 bitlik anahtar uzunluğu için 10000 ölçüm alındığından bahsedilmişti. Böyle bir sistem için tahmin matrisinin $M(10000\times256)$'lık bir matris olması gerekmektedir. M_6 matrisi oluşturulurken ilk 8 bit için işlem yapıldığından M_6 matrisini $M(10000\times256)$'lük matris üzerinde dağıtmalıyız. 10000 girişin ilk 8 biti aynı olan çok sayıda elemanı vardır.



Şekil 3.9 : AES algoritması ilk tur işlemleri

5- Sonuç olarak elimizde tahmin matrisi olarak $M_7(10000\times256)$ 'luk matris oluşmaktadır. Bundan sonraki kısım maskesiz AES gerçeklemesi korelasyon analizindeki şekliyle yürütülmektedir.

4. YAN KANAL ANALİZİ

Gelişen teknoloji ile birlikte güvenli iletişim ve haberleşme çok önemli bir hal almaya başlamıştır. Kriptografi bilimi de bu şekilde gelişmeye başlamıştır. Kriptografi bilginin geri dönüşümü mümkün olacak şekilde kodlanması anlamına gelmektedir. Kriptografi biliminde verilerin kodlanması için 2. bölümde de anlatıldığı gibi simetrik ya da asimetrik algoritmalar; dizi ya da blok şifreleyici algoritmaları gibi çok çeşitli algoritmalar önerilmiştir ve kullanılmıştır. Kriptografi ile birlikte bir diğer alan da gelişmeye başlamıştır. Kriptanaliz olarak adlandırılan bu alan kriptografik algoritmalarının güvenilirliğini sorgulamaktadır. Karşılıklı olarak bu iki alan birbirini besleyerek en güvenilir sistemi oluşturmaya çalışmaktadır. Kripanaliz değerlendirmeleri yapılırken kriptografik sistem bir matematiksel model olarak düşünülür ve giriş verisine kodlama işlemini yapılıyor iken gizli anahtar elde edilmeye çalışılır. Kriptanalizin günümüzde gelişen kodlama standartlarına karşı pratikte kullanılması çok zordur.

Kripanalizin gizli anahtarı elde etmek için kullanılan bir yöntemi yan kanal analizi yöntemidir. Bu yöntem kodlama sisteminin dışarıya istemsiz olarak verdiği bilgileri kullanır [6]. Şekil 4.1 de de gösterildiği gibi bu istemsiz çıkışlar zamanlama bilgisi [6], güç tüketimi bilgisi [7], manyetik radyasyon bilgisi [8, 9], çevreye yayılan ısı bilgisi ve çevreye yayılan ses bilgisi olabilmektedir [10].

Şekil 4.1 : Yan kanal bilgisi [11]

Algoritmaların kriptografik donanıma gömüldüğü durumlarda anahtarı açığa çıkarmak için yan kanal analizi saldırıları kullanılmaktadır. Saldırı yapan kişinin yeteneklerine bağlı olarak iki farklı yan kanal analizi saldırıları yöntemi vardır. Bunlar aktif saldırı analizi [4, 5], pasif saldırı analizi yöntemleridir [6, 7, 8, 9, 10]. Kurcalama saldırıları olarak da bilinen aktif saldırı yöntemi için algoritmanın gömüldüğü kriptografik sistemin içerisindeki devrelere ulaşmak gerekir. Bu nedenle uygulamaları zordur. Gelişmiş ve pahalı düzeneklere ihtiyaç duyarlar. İki çeşit aktif saldırı yöntemi vardır; ölçüm saldırıları [4] ve hatadan çıkarsama saldırıları [5]. Ölçüm saldırılarında sensörler yardımı ile devrenin çalışması esnasında kaydedicilerdeki bilgiye ya da transfer esnasındaki bilgilere ulaşılabilir [4]. Bu bilgiler yardımı ile gizli anahtara ulaşılmaya çalışılır. Hatadan çıkarsama saldırılarında ise devrenin yanlış çalışması sağlanarak hatalı elde edilen kapalı bilgilerden anahtar elde edilmeye çalışılır [5].

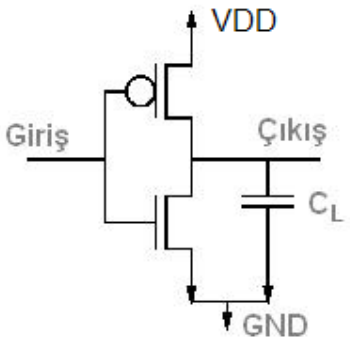
Pasif saldırı analizlerinde ise devrenin çalışmasına müdahale edilmez. Devrenin çalışması esnasında istemsiz olarak ürettiği çıkışlardan yararlanılır. Şekil 4.1 de devrenin istemsiz olarak ürettiği çıkışlar görülmektedir. Bu saldırılar aktif saldırılara göre daha basit ölçüm düzenekleriyle yapılabilmektedir. Kullandıkları yan kanal bilgisine göre beş çeşit pasif analiz saldırısı vardır. Bunlar Zamanlama analizi saldırıları [6], Güç analizi saldırıları [7], Elektromanyetik analizi saldırıları [8, 9], Akustik analizi saldırıları [10], ve sıcaklık analizi saldırılarıdır. Zamanlama analizi saldırısı, zamanlama bilgisi kullanılarak anahtarın açığa çıkarılmaya çalışıldığı saldırıdır [6]. Güç analizi saldırısında ise şifrelemenin üzerinde gerçeklendiği donanım çalışıyorken devrenin güç ünitesinden çektiği toplam dinamik güce bakılmaktadır [7]. Elektromanyetik analizi saldırılarında sayısal devrelerin konum değiştirmesi sırasında yaydığı manyetik radyasyondan yararlanılmaktadır [8, 9]. Akustik analizi saldırıları ve sıcaklık analizi saldırılarında sırası ile devrenin ürettiği ses ve sıcaklık bilgisinden faydalanılır [10]. Bu beş grubunda her biri kendi içerisinde Basit Analiz Saldırısı ve Farksal Analiz Saldırısı olmak üzere ikiye ayrılır. Basit Analiz Saldırılarında sadece bir ölçüme bakılarak anahtar hakkında bilgi edinilmeye çalışılır [6]. Farksal Analiz Saldırılarında ise gürültünün etkisini yok edebilmek için çok sayıda ölçüm kullanılarak anahtar açığa çıkarılmaya çalışılır [7, 8, 9]. Basit Analiz Saldırısı ile yürütülen işlem hakkında bilgiye sahip olunuyor iken Farksal Analiz Saldırısı ile ilerleyen veri hakkında bilgi elde edilebilmektedir. Aşağıda elektromanyetik analizi saldırısından bahsedilecektir.

4.1 Elektromanyetik Analizi Saldırısı

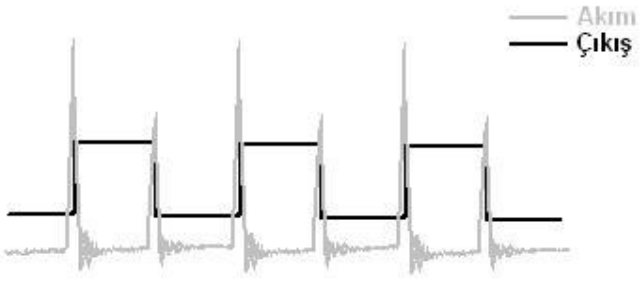
Günümüzde sayısal çalışan elektronik tümdevrelerin gerçeklenmesinde tamamlayıcı metal oksitli yarı iletken tranzistörler (CMOS) sıklıkla kullanılmaktadır [36]. Şekil 4.2 de bir CMOS evirici yapısı görülmektedir. Şekil 4.3 de ise CMOS eviricisinin çıkışına bağlı olarak güç kaynağından çekilmiş olan akım görülmektedir.CMOS kapıları için toplam güç tüketiminde baskın olan faktör dinamik güç harcamasıdır. 1 CMOS kapısının dinamik güç tüketimi aşağıdaki gibi ifade edilebilmektedir [36].

$$P_D = C_L \times V_{DD}{}^2 \times P_{0\to1} \times f \ , \quad [36] \tag{4.1}$$

Burada P_D dinamik güç tüketimini, C_L kapının yük kapasitesini, V_{DD} kaynak gerilimini, $P_{0->1}$ CMOS kapısının 0→1 geçişlerinin olasılığını, f saat frekansını göstermektedir. Bu formül CMOS ile kurulmuş tümdevrelerin güç tüketiminin veriye bağlı olduğunu gösterir. Algoritmaya saldırı yapan için önemli olan bu ilişkinin gözlenebilir olup olmayışıdır.



Şekil 4.2 : CMOS evirici yapısı



Şekil 4.3 : CMOS devresi çıkış-akım grafiği

CMOS tranzistörlerinin güç tüketimleri statik ve dinamik olmak üzere 2 farklı yapıdadır. Statik güç tüketimi tranzistörün çıkışının sabit kaldığı zamandaki güç tüketimini verirken dinamik güç tüketimi transistorun çıkışının değiştiği zamandaki güç tüketimini vermektedir [36]. Şekil 4.3 den de görüleceği üzere güç tüketiminin büyük bir kısmını dinamik güç tüketimi oluşturmaktadır.

Tranzistörlerin çıkışının konum değiştirmesi güç tüketiminin yanı sıra Elektromanyetik yayınıma da sebep olmaktadır. Transistorun çıkışının konum değiştirmesi sırasında akım ani olarak değiştiği için manyetik alan oluşmaktadır. Çizgi akımın manyetik alanını veren Biot – Savart yasası aşağıda görüldüğü gibidir.

$$B(r) = \frac{u_0 I}{4\Pi} \int \frac{r^* dl'}{r^2} \quad [31] \tag{4.2}$$

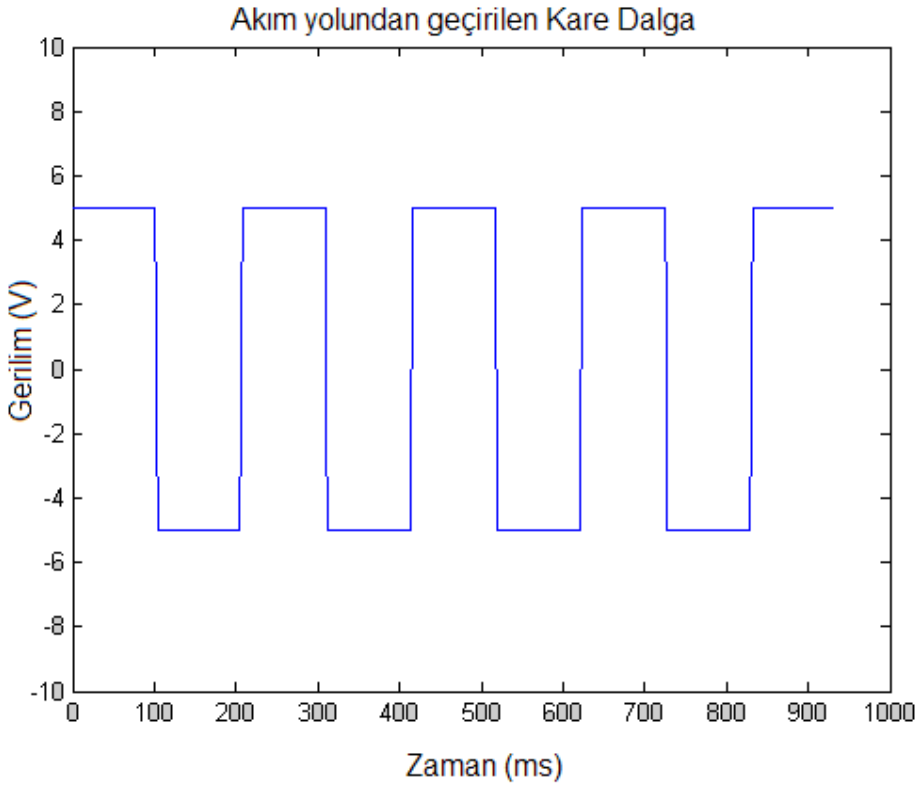
Bu formülde u_0 serbest uzayın geçirgenliğini, I yoldan geçen akımı, r akım kolunun ölçüm düzeneğine dik uzaklığını, dl ise seçilen yeterince küçük akım yolunun uzunluğunu ifade etmektedir. EM Analizi saldırısı için ölçümler yapabilmek üzere manyetik akı bilgisine ihtiyaç vardır. Manyetik akı ise manyetik alanın yüzeye normal bileşeninin o yüzey ile integrasyonu ile bulunur. Burada yüzey olarak adlandırılan ölçüm düzeninin işareti alacak olan bölümüdür. Aşağıdaki formülde Φ manyetik akıyı, B_n Manyetik alanın yüzeye dik bileşenini, da manyetik işareti alacak olan ölçüm cihazının yüzey alanını ve S integrasyonun alan integrasyonu olduğunu göstermektedir.

$$\Phi = \int_S B_n da \quad [32] \tag{4.3}$$

Manyetik akının zamanla değişimi ise alıcı bir devrede emk (voltaj) indüklenmesine sebep olmaktadır. Aşağıda Faraday indükleme yasasından görüleceği gibi devrede indüklenen emk devreden geçen manyetik akının zamanla değişimi ile doğru orantılıdır.

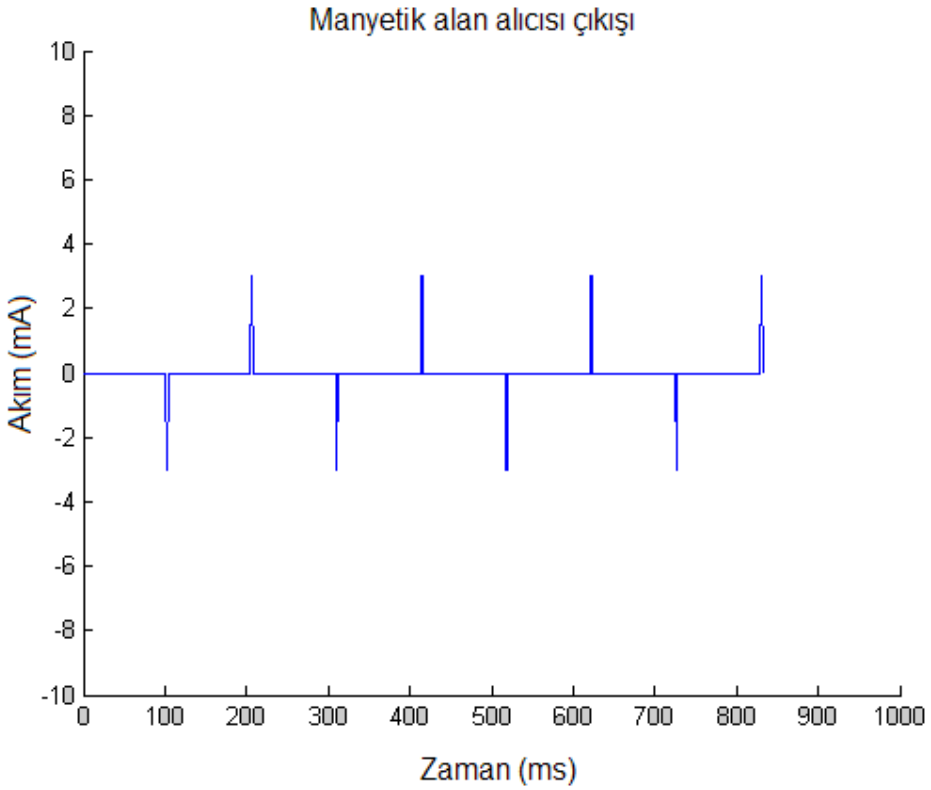
$$V = \frac{d\Phi}{dt} \text{ (Faraday indükleme yasası [32])} \tag{4.4}$$

Örnek olarak bir akım kolundan şekil 4.4 deki gibi 5V gerilim geçirilmiştir. 1kΩ luk direnç üzerinden geçirilmiştir ve manyetik alan ölçümleri yapılmıştır.



Şekil 4.4 : Akım yolundan geçirilen kare dalga

Üzerinden 5 mA kare dalga geçirilen kabloya manyetik alıcı yardımıyla yaklaşılmıştır ve şekil 4.5 deki manyetik alanın alıcı üzerinde oluşturduğu emk (voltaj) indirgenmesi görüntüsü osiloskop yardımı ile alınmıştır.



Şekil 4.5 : Manyetik alan alıcısı çıkışı

Yukarıdaki örnek ile bir devrenin yaydığı EM radyasyonun ölçülebilirliği gösterilmiştir. Devrelerden yayılan bu radyasyon ileride EM analizleri için ölçüm matrisini oluşturacaktır. EM analizleri için diğer bir matris ise Hamming uzaklıkları ya da Hamming ağırlıkları kullanılarak oluşturulacaktır. Hamming uzaklıkları ve Hamming ağırlıkları AES şifrelemesini gerçekleştirirken açık veriden şifreleme yönünde giderek ya da kapalı veriden şifrelemenin tersi yönünde giderek bulunabilir.

Manyetik Alan saldırıları da Güç analizi saldırılarındaki gibi Basit elektromanyetik analizi saldırıları (SEMA) ve farksal elektromanyetik analiz saldırıları (DEMA) olmak üzere ikiye ayrılır [8, 9]. Tamamen Güç analizindekine benzer şekilde Basit elektromanyetik analiz yapılırken bir ölçüme bakılarak yürütülen işlem hakkında bilgi edinilmeye çalışılır. Farksal elektromanyetik analiz yapılırken ise birçok ölçüm alınarak gürültünün etkisi azaltılmaya çalışılır ve işlenen veri hakkında bilgi edinilmeye çalışılır.

Manyetik alan saldırılarının Güç analizi saldırılarına göre bir takım avantajları ve dezavantajları vardır. Güç analizinde yapıldığı gibi güç kaynağı ile kriptografik cihaz

arasına direnç koyma ihtiyacı yoktur. Güç analizinde direnç üzerinden geçen akım; gerilim alıcıları vasıtasıyla alınıyordu. Elektromanyetik analizi saldırılarında ise ölçüm almak için elektromanyetik alıcılar kullanılmaktadır. Kriptografik cihaza herhangi bir müdahaleye gerek yoktur. Güç analizi için bazı sistemlerde güç kaynağından kriptografik cihaza giden güç yolunu bulmak güçtür, elektromanyetik analizinde bu tür problemlerle karşılaşılmaktadır. İkinci avantaj olarak elektromanyetik alıcılar yardımı ile istenilen bölgenin elektromanyetik radyasyonu alınabilmektedir. Güç analizinde ise böyle bir ölçüm mümkün değildir, çünkü güç kaynağından çıkan güç olduğu gibi ölçülmektedir. Dezavantajı olarak ise alınan ölçümün gerilim değerinin çok düşük olması söylenebilir. Düşük olmasının sakıncası ise işaret gürültü oranının hesaplanmasında gözlenebilmektedir. Elektromanyetik analizinde gürültü daha büyük bir problem olarak karşımıza çıkmaktadır [18].

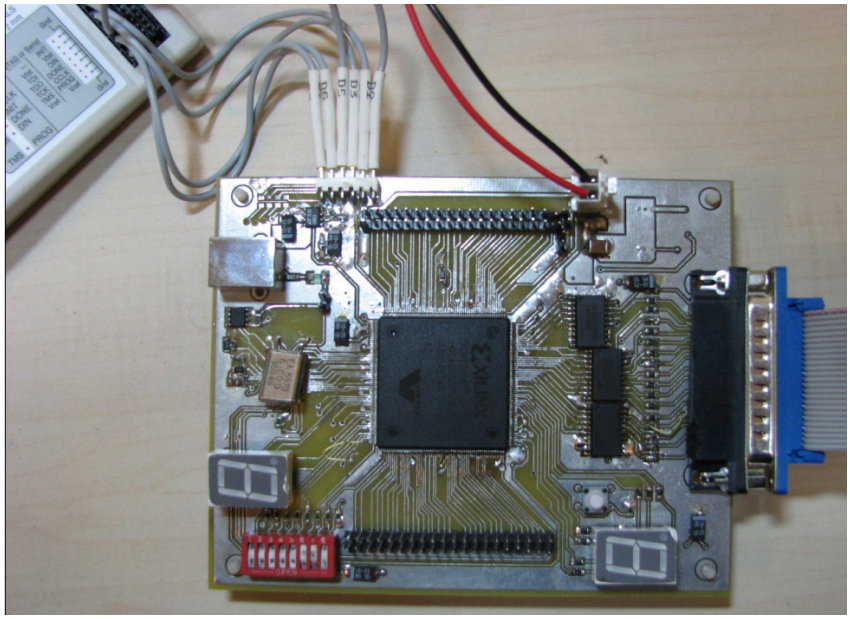
5. ÖLÇÜM DÜZENEĞİ

Bu bölümde tez çalışmaları esnasında kullanılmış olan ölçüm düzeneğinden bahsedilecektir. Bölüm 2'de EM analizini yapabilmek için FPGA'dan yayılan EM radyasyonunu alabilmek için tasarlanan EM alıcısının tasarım adımlarından bahsedilmişti. Bu bölümde EM alıcısının tasarımından bahsedilecektir. Ayrıca genel olarak ölçüm sisteminden bahsedilecektir.

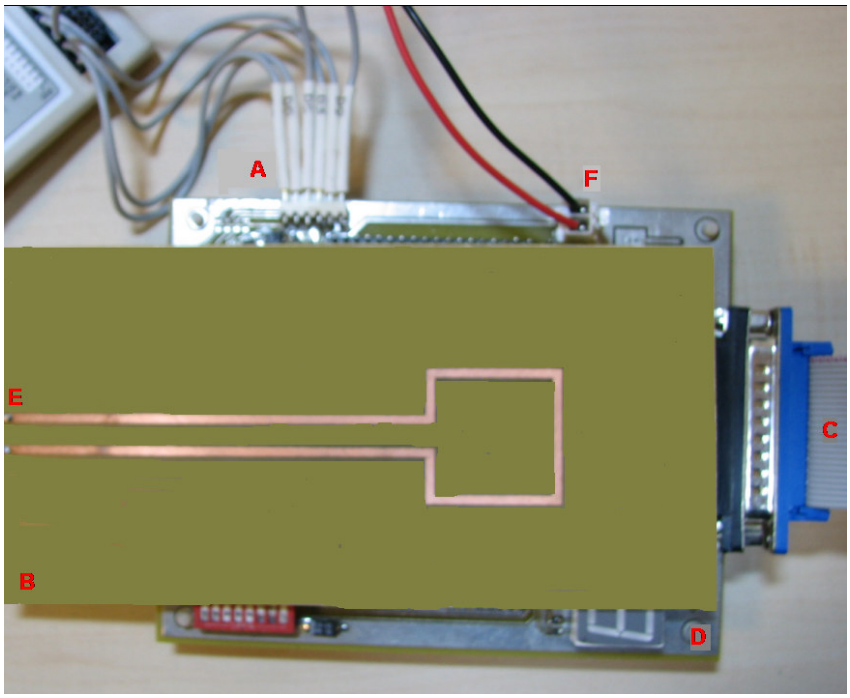
5.1 EM Analizi için Kurulan Ölçüm Düzeneği

EM analizini yapabilmek üzere düzenekte olması gerekenler; üzerinde AES algoritmasının gerçeklendiği FPGA, EM radyasyonu alıcı elemanı ve osiloskoptur.

Osiloskop hâlihazırda gömülü sistemler laboratuarında bulunan Agilent marka bir osiloskoptur. AES algoritmasının gerçeklemesi için; daha önce yüksek lisans tezini "AES Algoritmasının FPGA Üzerinde Gerçeklenmesi ve Yan Kanal Analizi Saldırılarına Karşı Güçlendirilmesi" başlığı altında tamamlamış Yük. Müh. Levent ORDU'nun hazırladığı şekliyle kullanılmıştır [11]. Bu tasarım Yük. Müh Abid Üveys DANIŞ'ın hazırlamış olduğu kartın üzerindeki FPGA'e yüklenmiştir. Kullanılan FPGA Virtex E ailesinin XCV1000E modelidir. Bu kartın ölçüm düzeneği içerisinde bilgisayar ile haberleşmesi gerekmektedir. Ayrıca osiloskop da bilgisayar ile haberleşme içerisinde olmalıdır. Osiloskop ile bilgisayarın arayüz kablosu USB/GPIB'dır. Elektronik kart ile bilgisayar ise paralel port yardımı ile haberleşmektedir. Osiloskoba bağlı olan EM radyasyon alıcısı ise FPGA kartı üzerinde belli bir mesafede durmaktadır. Yakın alan çalışması yapıldığı için bu mesafe 1mm ya da 2mm civarındadır. Bu elektronik kart üzerinde EM radyasyonu alıcısı elemanı ise tez kapsamında tasarlanmıştır. Şekil 5.1'de AES algoritmasının yüklendiği ve ölçümler için kullanılan kart görülmektedir. Şekil 5.2'de elektronik kart üzerine ölçüm almak için yerleştirilmiş EM alıcısı elemanı görülmektedir.



Şekil 5.1 : Ölçümler için kullanılan elektronik kart



Şekil 5.2 : Ölçümler için kullanılan sistem

Şekil 5.2'de A harfi ile gösterilen yer AES algoritmasının FPGA'ya yüklendiği bağlantı noktasını göstermektedir. B harfi bütün olarak EM alıcısı elemanını göstermektedir. C harfi bilgisayar ile FPGA arasındaki paralel port bağlantısını göstermektedir. Buradaki paralel port AES algoritmasının şifreleyeceği 128 bitlik şifrelenecek veriyi FPGA'ya göndermekte ve şifreleme işlemi tamamlandıktan sonra

yine 128 bitlik şifreli veriyi bilgisayara iletmektedir. Şifreli veri bilgisayara şifrenin doğru yapılıp yapılmadığını kontrol etmek amacıyla gönderilmektedir. D Şekil 5.1'de gösterilen elektronik kartı göstermektedir. E harfi EM alıcısı sistemin osiloskoba bağlanacağı uçlarını göstermektedir. EM alıcısı hakkında bilgi ilerleyen bölümlerde verilecektir. F harfi elektronik kart için güç bağlantı noktasını göstermektedir.

5.2 EM Analizi için Kullanılan Yazılımlar

Bu bölümde sahada programlanabilir kapı dizilerine (Field programmable gate array (FPGA)) yüklenen devre yazılımı ve bilgisayarda kullanılan sistemi kontrol eden yazılım anlatılacaktır.AES donanım yazılımı Bölüm 5.1 de belirtildiği gibi Yük. Müh. Levent ORDU' nun tezinden alınarak kullanılmıştır. Bölüm 3 de anlatıldığı şekli ile hem maskesiz AES gerçeklemesi hem de Oswald'ın maskesi kullanılarak oluşturulan maskeli AES gerçeklemesi FPGA'ya yüklenecek şekilde alınmıştır. Tez kapsamında kullanılan AES 128 bit veriyi şifrelemek için 128 bit anahtar kullanmaktadır [2]. 128 bit uzunluğundaki anahtar için tur sayısının 10 olacağı 3. Bölümde belirtilmişti.

1- Hatırlanacağı gibi 1 turda 4 adım gerçekleştirilmekteydi. Bir de herhangi bir turun çıkışının bir sonraki tur için girişi oluşturması adımını eklersek AES algoritmasının 1 turu 5 adımda yaptığını düşünebiliriz. Levent ORDU'nun tasarımında her adımı 1 saat darbesinde yaptığı düşünülmüş böylece 10 tur için girişin kodlanması için 50 saat darbesi süresine ihtiyaç vardır [11].

2- Bu durum maskeli AES gerçeklemesi için de geçerlidir. AES algoritmasının maskeli gerçeklemesi için değişen sadece S-kutuları ve rastgele sayının algoritmaya eklenmesidir dolayısıyla şifreleme için geçen süre değişmeyecektir.

3- Son turda sütunları karıştırma işleminin yapılmadığından bahsetmiştik. Algoritma FPGA üzerinde tasarlanırken diğer turlardan farklı olmaması için son turdan sütunları karıştırma işlemi kaldırılmamıştır yalnız işlem yapıldıktan sonra çıkışı kullanılmamaktadır.

4- Sütunları karıştırma adımından 1 önceki adım olan satırları kaydırma adımının çıkışı tur anahtarı toplanması adımının girişlerini oluşturmaktadır.

5- Diğer bazı AES algoritması tasarımlarında adımları yerleri değiştirilebilmektedir yalnız tez kapsamında kullanılan AES algoritması 3. Bölümde anlatıldığı sırası iledir.

Ölçüm düzeneğini kontrol eden yazılım ise c++ programlama dili kullanılarak oluşturulmuştur. Bu program ile hem kodlanacak veri ve kodlanmış veri trafiği takip edilmekte hem de osiloskoptaki görüntünün bilgisayara kaydedilmesi gerçekleştirilmektedir.

1- Program öncelikle 16 baytlık kodlanacak veriyi karta paralel port kullanılarak iletmektedir.

2- Paralel port ile alınan bu kodlanacak 16 bayt veri FPGA kartı üzerinde çalıştırılan AES algoritması ile şifrelenmekte ve şifrelenmiş veri yine aynı port kullanılarak bilgisayara iletilmektedir.

3- Programın ikinci kısmı ise osiloskoptan alınan görüntünün bilgisayara kaydedilmesi işleminden oluşmaktadır. Osiloskop ile alınan 1 görüntü 1000 nokta içermektedir ve bilgisayara 1000 nokta olarak kaydedilmektedir.

4- Tercihe göre bütün AES işlemleri adımları için de ölçüm alınabilir sadece 1 adım için de ölçüm alınabilir. 1 adım için alınan ölçümün örnekleme sayısının bütün AES için alınan ölçümün örnekleme sayısının 50 katı olacağı açıktır.

5- Ölçüm alınırken diğer dikkat edilmesi gereken husus ise dikeyde işaretin pencereyi tam kapsaması gerektiğidir. Bu da dikey çözünürlük için önemli bir husustur. Bütün bu önlemler şifreyi açığa çıkaracak ölçüm sayısını azaltmak için kullanılır.

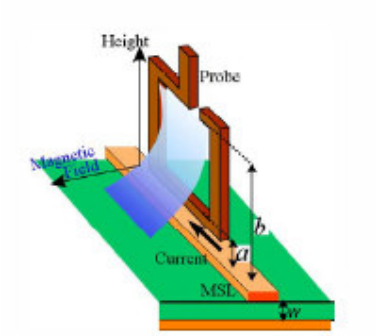
6- Tezde kullanılan ölçümler maskesiz AES kodlaması için 1 adımı içermekte, maskeli AES kodlaması için ise 2 adımı içermektedir. Maskesiz AES kodlaması için son turun satırları kaydırma işleminin çıkışına saldırılmış ve sadece bu adım için örnekler alınmıştır. Maskeli AES kodlaması için ise 1. turun bayt yer değiştirme adımına saldırılmış ve bu ve bir sonraki adımının ölçümleri alınmıştır.

7- Programın bu iki kısmının eşzamanlı çalışması için ise osiloskobun tetiklenebilirliği özelliğinin kontrol edilmesi gerekmektedir. Kart kodlanacak

veriyi aldıktan sonra kodlama işlemi başladığında osiloskoba çip kullanılabilir işaretini göndermekte ve osiloskop bu işaret ile ölçümü başlatmaktadır. Osiloskobun ayarları ile ölçümün başlangıç ve bitiş yerleri ayarlanmakta ve her şifreleme için 1000 noktalık ölçüm bilgisayara kaydedilmektedir. Tez için analizlerde kullanılmak üzere 10000 kodlama için ölçüm alınmıştır.

5.3 EM Alıcısı Sistemi

Bu bölümde ölçümleri almak için tasarlanan EM alıcısı sistemi anlatılacaktır. İlk bilinmesi gereken bu sistemin uzak alan mı yoksa yakın alan mı çalışacağıdır. İkinci Bölümde bahsedildiği üzere devre sayısal çalışan bir devredir ve saatin yükselen ve düşen kenarlarında elektromanyetik yayınımın ne olduğu merak edilmektedir. Ölçüm alınacak noktanın FPGA'dan uzaklığı dalga boyundan çok küçüktür. Bu yüzden tasarlanacak EM alıcısının yakın alan çalışıyor olması gerekmektedir. Hangi alanda çalıştığına karar verildikten sonra ise anten tipinin seçilmesi gerekmektedir. EM analizleri için ihtiyacımız olan elektromanyetik radyasyonun akım veya gerilim gibi osiloskop ile ölçülebilir şekle dönüştürülmesidir. Bunun için kullanılması gereken EM alıcısı elemanı çevrim anten yapısında olmalıdır [36].



Şekil 5.3 : Akım ve elektromanyetik alan ilişkisi [37]

Şekil 5.3'den görüleceği üzere telden akım geçtiği zaman telin etrafında sağ el kuralı uyarınca uzaklık arttıkça azalan bir elektromanyetik alan oluşacaktır. Tahmin edileceği gibi çevrimin içerisinden geçen elektromanyetik dalgalar çevrimi oluşturan iletken üzerinde akım oluşturacaktır ve osiloskoba iletilecektir [37].

Anten tipi seçildikten sonra yapılması gereken ise ölçüm için önemli parametrelerin seçilmesidir. Bu noktada proje için önemli olan ölçülecek sistemin frekansında bir anten tasarlayabilmek ve giriş çıkış empedanslarının uygunluğuna dikkat etmektir.

Giriş empedansı yayılan elektromanyetik işaretin gücünün alıcı sisteme ne kadarının iletildiğini göstermektedir. Giriş empedansı uygun sistemler gücünün %100 ünü alıcı sisteme aktarabilirler. Çıkış empedansı ise sistemden çıkan işaretin ne kadarının osiloskoba iletildiğini gösterir. Yakın alan alıcısı sistemlerin frekans band aralıkları çok geniştir. Eğer ölçümü yapılacak sistemin yaydığı elektromanyetik işaretin frekansı tam olarak biliniyor ise o frekans için tasarım yapmak gürültüden büyük oranda kurtulmak demektir. Çünkü ilgilenilmeyen diğer bütün frekanslardaki işaretler gürültü olarak asıl alınması gereken işarete eklenmektedir. Diğer taraftan istenilen işaretin ölçümünü alabilmek için antenin çevrimini olabildiğince dar tutmak gerekmektedir. Bu uygulama aynı zamanda diğer frekanslardaki işaretlerinde gücünün azalmasını sağlayacaktır.

Tasarlanacak EM alıcısı elemanının çalışma frekansı bulabilmek için çalışılan FPGA'nın yükselme ve düşme zamanlarına bakmak gerekiyor. Virtex E ailesinin XCV1000E modeli için yükselme ve düşme zamanları 5ns ile 10 ns arasındadır. Düşme ve yükselme zamanlarının çarpmaya göre tersleri EM alıcısının çalışması gereken frekansları göstermektedir. Bu yüzden 200 MHz civarı tasarlanacak EM alıcısı için çalışma frekansını oluşturmaktadır.

Frekans tespiti için yapılan diğer bir çalışma ise kaydediciler ile yapılan deneydir. Bu deney için Virtex E ailesinin XCV1000E modeli bir çip ve 30 MHz ile 1 GHz arasında çalışan Agilent marka magnetik alan alıcısı elemanı kullanılmıştır.

1- Deney için Xilinx-ISE ortamında devre oluşturulmuş ve FPGA'ya yüklenmiştir. Bu devrede 100 bitlik 6 kaydedici kullanılmıştır.

2- Başlangıç konumu olarak 6 kaydedicinin bütün bitleri '0' konumuna getirilmiştir.

3- İlk adım olarak birinci kaydedicinin 100 biti 0'dan 1'e yükseltilmiştir.

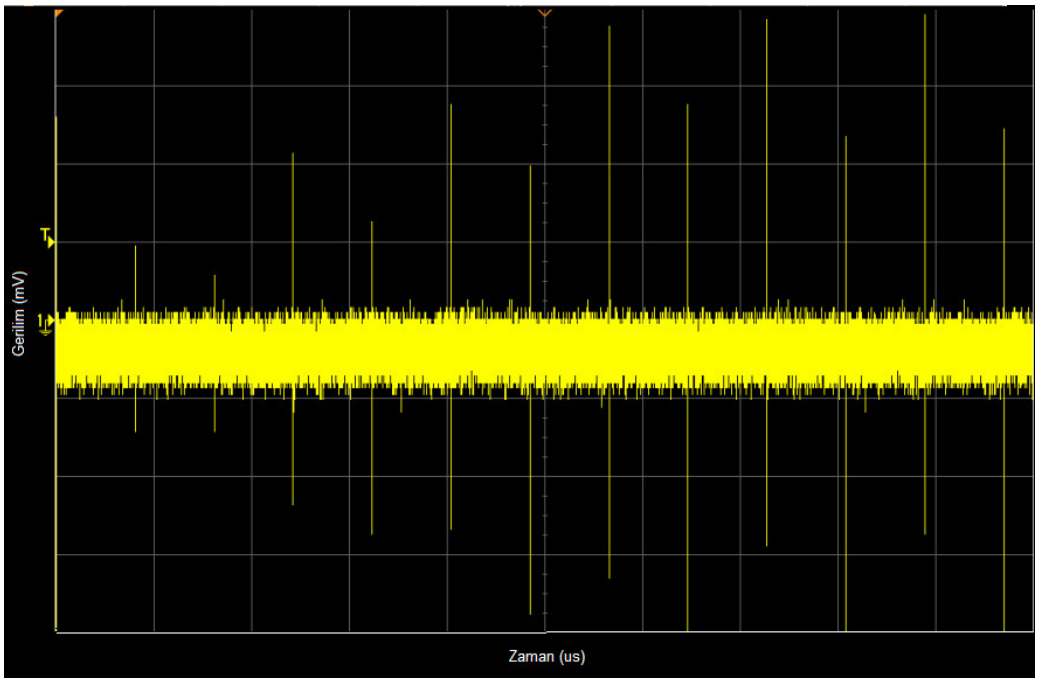
4- İkinci adımda birinci kaydedicinin 100 biti 1'den tekrar 0'a düşürülmüştür.

5- Üçüncü adımda birinci ve ikinci kaydedicilerin 100'er bitleri aynı anda 0'dan 1'e yükseltilmiştir.

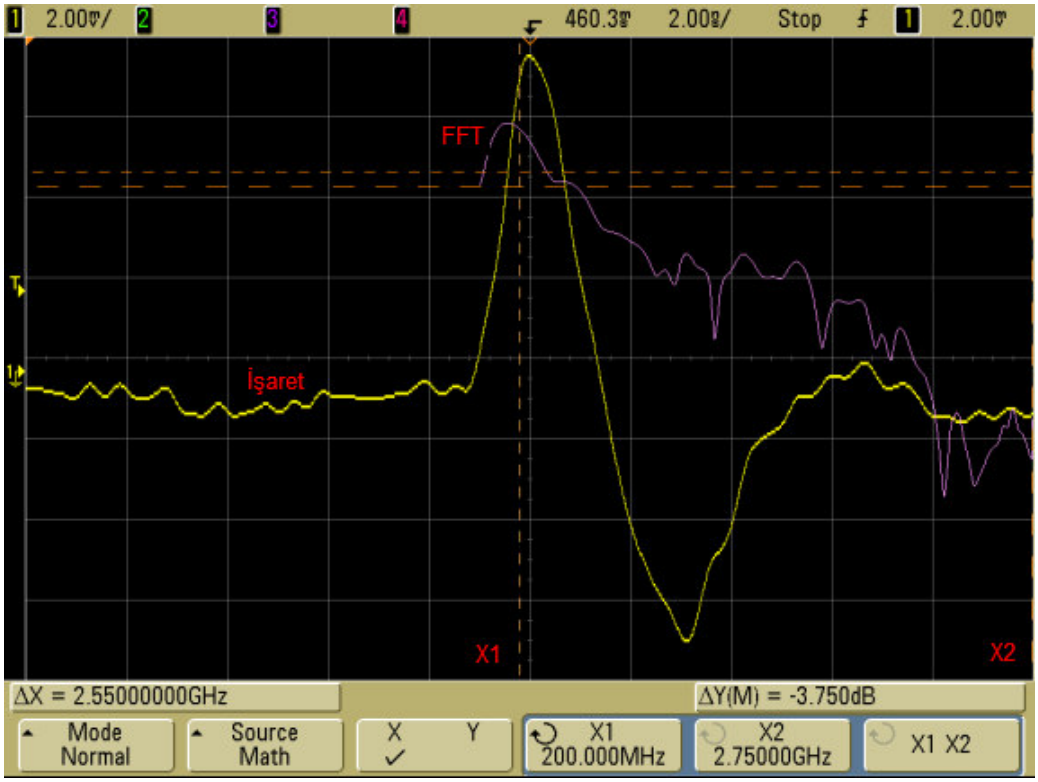
6- Dördüncü adımda birinci ve ikinci kaydedicilerin 100'er bitleri 1'den tekrar 0'a düşürülmüştür.

7- Bu şekilde devam eden döngü 6 kaydedicinin 100er bitlerinin 1'den 0'a düşürülmesi ile son bulur.

Bu arada bütün bu işlemler yapılıyor iken Agilent marka EM alıcısı elemanı ile ölçümler yapılmıştır. Deneyden beklenen artan bit sayıları ile EM radyasyonunun arttığını görmektir. Diğer görmek istediğimiz ise elimizdeki Agilent marka magnetik alıcısı elemanının frekansının yeterli olup olmayacağı idi. Eğer istediğimiz işareti görebiliyorsak FPGA'nın çalışma frekansı hakkında bilgiye sahip olacaktık. Deneyler sonucunda Şekil 5.4 elde edilmiştir. Şekil 5.4'un zaman ekseninde genişletilmesi ile Şekil 5.5 elde edilmiştir. Osiloskobun FFT alma özelliği kullanılarak elde edilen Şekil 5.5'den frekansın 200 MHz civarı olduğu gözükmektedir. Yukarıda FPGA'nın yükselme ve düşme zamanlarına göre tahmin edilen frekans bu deney ile pekiştirilmiş olmaktadır.

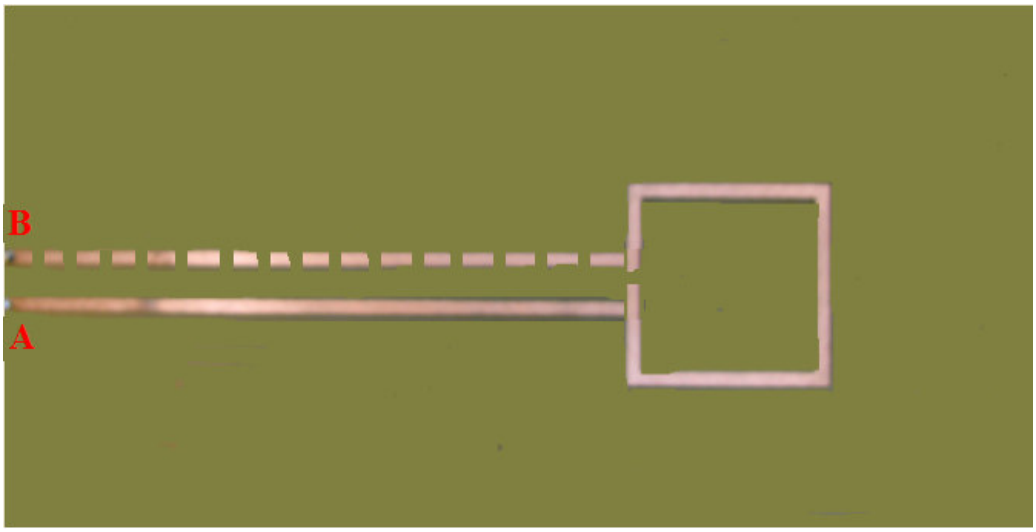


Şekil 5.4 : Kaydediciler ile yapılan deney



Şekil 5.5 : Kaydediciler ile yapılan deneyin frekansı

Frekans konusunda emin olduktan sonra yapılacak olan bu frekansı band aralığı içine alacak şekilde tasarımı gerçekleştirmektir. Bu tasarım için HFSS anten tasarım programı kullanılmıştır. Tasarım sonucunda Şekil 5.6'daki EM alıcısı elemanı oluşmuştur. Tasarım için Funuto'nun [37] tasarımı temel alınmıştır. Funuto'nun tasarımındaki frekansın bizim tasarımımızdaki frekansa çekilebilmesi için EM alıcısı elemanının boyutunun büyüyeceği açıktır. Bu tasarım 2 katlı bir yapıdadır. Arada yalıtkan malzeme olarak epoxy kullanılmıştır. Epoxy'nin hem alt yüzeyinde hem de üst yüzeyinde olmak üzere bakır yollar vardır.



Şekil 5.6 : EM alıcısı elemanı

Şekil 5.6'da sürekli çizgiler bakır yolların üst katta olduğunu kesikli çizgiler bakır yolların alt katta olduğunu göstermektedir. A bakır yolunun ucu üst kattadır ve osiloskoba giden bağlantı için canlı ucu oluşturmaktadır. B bakır yolunun ucu ise alt kattadır ve osiloskoba giden bağlantı için toprağı oluşturmaktadır. Tam tersi de uygundur. B bakır yolunun ucu canlı ucu A bakır yolunun ucu ise toprağı oluşturabilir.

Bu EM alıcısı elemanı ile alınmış olan ölçümler 6. Bölümde gösterilmiştir.

6. FPGA GERÇEKLEMELERİNE ELEKTROMANYETİK ANALİZİ

Bu bölümde tez çalışmaları esnasında yapılmış olan pratik çalışmaların sonuçlarından bahsedilecektir. Bölüm 2 de EM analizini yapabilmek için etrafa yayılan EM radyasyonu alabilmek üzere tasarlanan EM alıcısından bahsedilmişti. Yine bölüm 2 de analizlerde etkisinin çok büyük olduğu görülen gürültüyü azaltmaya yönelik Kümülant alma tekniğinden bahsedilmişti. Bölüm 3 de AES hakkında ve Oswald'ın maskesi kullanılarak maskelenmiş AES hakkında bilgiler verilmişti. Bölüm 4 de ise genel olarak yan kanal saldırıları ve biraz daha ayrıntılı olmak üzere elektromanyetik (EM) yan kanal analizinden bahsedilmişti.

Aşağıda ilk olarak EM analizi için gerekli tahmin değerleri oluşturulacak devamında da maskesiz AES algoritmasının FPGA gerçeklemesine ve maskeli AES algoritmasının FPGA gerçeklemesine düzenlenen saldırılar anlatılacaktır.

6.1 Elektromanyetik Analizi için Tahmin Değerlerini Oluşturma

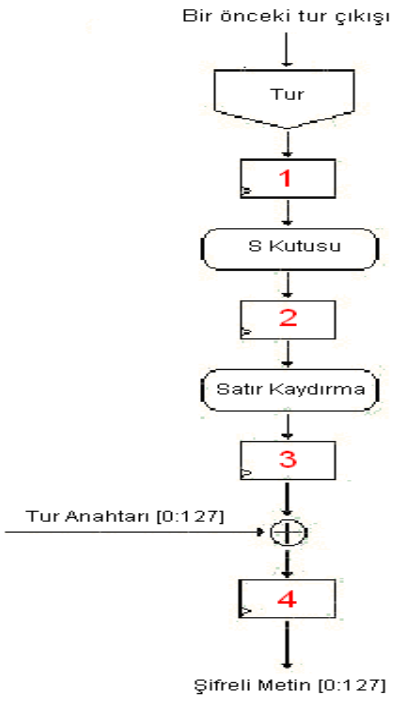
Bu bölümde EM analizinde korelasyon işlemi için kullanılacak tahmin matrislerinin oluşturulması anlatılacaktır. Maskesiz AES algoritması ve maskeli AES algoritması için tahmin matrisleri farklı şekillerde oluşturulacaktır.

6.1.1 AES algoritmasının maskesiz gerçeklemesi için tahmin değerlerini oluşturma

Maskesiz EM saldırısı için Bölüm 5.2'de son turun satırları kaydırma işlemine saldırı yapılacağı ve o adım için ölçümlerin alındığı anlatılmıştı. Korelasyon analizini yapabilmek için ise ölçümlerin yanında diğeri bir elemana ihtiyaç vardır. Bu eleman tahmin matrisidir. Tahmin matrisi Bölüm 4'de anlatıldığı gibi iki farklı şekilde oluşturulabilmektedir. Tezde kullanılan model Hamming ağırlığı modelidir [32, 33]. Bu modele göre son tur için tahmin matrisi oluşturulacağından şifrelenmiş veri kullanılır. Son tur işlemleri Şekil 6.1'de gösterilmektedir.

Şifrelenmiş veriden algoritmanın tersi yönünde hareket edilerek ölçümü alınan adım için tahmin matrisleri oluşturulur. Tez kapsamında onaltı bayt anahtarın bir baytına saldırı yapılmıştır. Anahtarın diğer baytları da aynı işlemler yapılarak

bulunabilmektedir. Tahmin değerlerini şifrelenmiş veriden geriye giderek adım adım hesaplayalım.



Şekil 6.1 : AES algoritması son tur işlemleri

Analizi yapılacak olan anahtar baytı birinci bayttır. Analizin yapılacağı işlem ise satırları kaydırma işlemidir. Hesaplanmaya çalışılan değer satırları kaydırma işleminin arkasındaki kaydedicinin değerleridir.

1- Tahmin değerleri 10000 ayrı şifreleme için yapılacaktır. Bu 10000 ayrı şifreleme aynı zamanda ölçümü EM alıcısı elemanı ile alınmış olan 10000 şifrelemedir.

2- 10000 şifreleme tamamlandıktan sonra elimizde 128 bitlik 10000 adet şifreli metin vardır.

3- Bu şifreli metinin ilk baytı analiz için kullanılacaktır, çünkü anahtarın ilk baytının analizi yapılmak istenmektedir. Dolayısıyla elimizde 10000 adet 8 bitlik veri bulunmaktadır. Bu veri Şekil 6.1'deki 4 numaralı kaydedicideki veridir.

4- Dört numaralı kaydediciden üç numaralı kaydediciye geçmek için tur anahtarını toplama işleminin tersini yapmak gerekecektir. Oluşturmaya

çalıştıklarımız tahmin değerleri olduğu için burada sekiz bitlik anahtar parçasının bütün olası değerleri hesaplanacaktır. Bir adet şifrelenmiş metin üzerinden çalıştığımızı düşünelim. 256 farklı anahtar ile tur anahtarını toplama işleminin tersinin yürütüldüğünü düşünürsek elimizde 256 farklı anahtar için 256 farklı tahmin değeri olacaktır. Şifrelenmiş veriyi oluşturulacak matrisin satırına yerleştirirsek sütunları da olası anahtar değerleri olacaktır. Matrisin elemanları ise satırdaki şifreli veri ile sütundaki anahtarın üç numaralı kaydedicideki değeri olacaktır. Oluşturulan matrise M_1 ismini verelim. $M_1(1\times256)$ 'lık bir matristir.

5- 10000 ayrı şifreleme için bu matris $M_2(10000\times256)$ olacaktır.

6- Bu durumda M_2 matrisi ile elimizde olan değerler bir baytlık satır kaydırma işleminin çıkışıdır. Bu bir baytlık veriyi 2'lik sistemde yazalım ve matrisin bütün hücrelerindeki sekiz bitlik değerin içerisindeki "1" sayılarını sayalım. Bu değerin en az 0 en fazla 8 olacağı açıktır. M_2 matrisindeki değerlerin yerine hesaplanan "1" sayılarının toplamını yazalım. Yeni oluşan M_3 matrisi korelasyon için kullanılacak tahmin matristir. $M_3(10000\times256)$ şeklindedir.

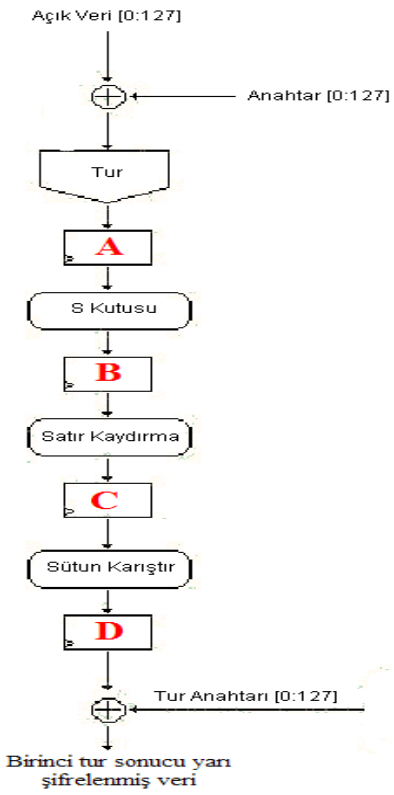
Buradaki bütün anlatılan adımlar AES algoritmasının maskeli gerçeklemesine EM saldırısı yaparken tahmin değerlerini oluşturmak için aynen kullanılmıştır.

6.1.2 AES algoritmasının maskeli gerçeklemesi kombinezonsal yöntem için tahmin değerlerini oluşturma

Maskeli EM saldırısı için Bölüm 5.2'de birinci turun bayt yer değiştirme adımına saldırı yapılacağı ve o adım için ölçümlerin alındığı anlatılmıştı [15]. AES algoritmasının maskeli gerçeklemesi için maskesiz gerçeklemesinde olduğu gibi adımların çıkışlarında kaydedicilerdeki değerlerin Hamming ağırlıklarının hesaplanması yeterli olmayacaktır. Çünkü dışarıdan giriş olarak verilmeyen içeride rastgele uygulanan bir parametre bu tahmin matrisini oluşturma yöntemine önlem olarak önerilmiş ve kullanılmıştır. Bunun için tahmin matrisini oluşturmak için önerilen yöntem ise aşağıdaki gibidir.

AES algoritmasının maskeli gerçeklemesi için saldırı birinci turun bayt yer değiştirme adımına yapılacağından bu adımla ilgili tahmin matrisleri oluşturulacaktır. Şekil 6.2 AES algoritması için birinci tur işlemlerini göstermektedir. Bayt yer

değiştirme adımının içerisindeki işlemler 1 saat darbesinde ardışıl olarak gerçekleştirilmektedir. Bayt yer değiştirmenin içerisindeki işlemlere bakılarak öncelikle maskeden bağımsız bir işlemin yapılıp yapılmadığı araştırıldı. Eğer böyle bir işlem bulunmuş olunsaydı o işlem için çıkışların kaç defa konum değiştirdiği sayısına bakarak tahmin matrisi oluşturulacaktı. Maskeye bağımsız bir işlem bulunmayışından dolayı Modelsim benzetim ortamı kullanılarak bayt yer değiştirme işlemi sırasında devrede gerçekleştirilen bütün işlemlerin çıkışlarının konum değiştirme sayısı hesaplanacaktır.



Şekil 6.2 : AES algoritması ilk tur işlemleri

1- AES algoritmasının maskesiz gerçeklemesinde olduğu gibi tahmin değerlerini bulma işlemi yine bir bayt için yapılacaktır. Diğer 15 bayt benzer yolla bulunabilmektedir. Hesaplamanın yapılacağı yer Şekil 6.2'deki A kaydedicisi ile B kaydedicisi arasındaki bayt yer değiştirme (S-kutusu) işlemidir.

2- Bayt yer değiştirme işlemi bir saat darbesinde gerçekleniyor iken içeride kombinezonsal devreler çalışmaktadır. Tahmin değerleri oluşturulurken bu kombinezonsal devrelerin konum değiştirme sayıları kullanılacaktır.

3- Konum değiştirme sayıları hesaplanırken bayt yer değiştirme işlemi bir bayt giriş varmış gibi yürütülmüştür. Daha sonra geriye adımlarla gidilerek şifrelenmemiş veriye ulaşılacaktır. Şifrelenmemiş veriye ulaşmaktaki amaç alınan ölçümler ile tahmin edilen değerlerin aynı şifrelenmemiş veriler için olmasını sağlamaktır.

4- Bayt yer değiştirme işlemi için olası bütün girişler (bir bayt için 256 tane) ve olası bütün maske değerleri (bir bayt için 256 tane) işleme sokulacaktır. Sonuçta elimizde olan satırları bayt yer değiştirme işleminin girişlerini sütunları da maske değerlerini gösteren hücrelerindeki değerler ise kombinezonsal devrelerin konum değiştirme sayılarını veren $M_1(256\times256)$ 'lık matristir. Matrisin hücrelerindeki değerler genellikle 0 ile 100 arasında değişen değerler olmaktadır.

5- Maskenin etkisini kaldırmak için ise M_1 matrisinin satır ortalaması alınacaktır. Yeni oluşan matris $M_2(256\times1)$ şeklindedir. Bu matrisin hücrelerindeki değerler ölçümü alınan bir maske ile tamamen alakasız iki yüz elli beş maskenin ortalamasından oluşmaktadır. Dolayısıyla ölçümü alınan maskenin dinamik güçteki etkisi iki yüz elli beş kat azaltılmıştır. Ölçüm sayısı artırılarak bu olumsuz etki giderilebilir. Yalnız ölçüm sayısını 255 kat artırmak çok pratik bir çözüm değildir.

6- Elimizde bulunan M_2 matrisinin satırları Şekil 6.2' de A kaydedicisinde görülen değerlerdir. Yalnız bir bayt için A kaydedicisinde yer alabilecek olan bütün değerler M_2 matrisinin satırlarında mevcuttur.

7- M_2 matrisi Şekil 6.2'de anahtarın toplanması işleminin tersi işlemine sokularak şifrelenmemiş veriye ulaşılacaktır. Bir bayt işlem yürütüldüğünden anahtarın 256 farklı değeri vardır.

8- M_2 matrisinin satırları anahtar toplanması işleminin sonucunu göstermektedir. Anahtar toplanması işleminin girişleri ise şifrelenmemiş verinin bir baytı ve anahtarın bir baytıdır. Yeni oluşacak M_3 matrisinin satırları şifrelenecek verinin bir baytını sütunları ise anahtarın bir baytını ifade etsin.

$M_3(256\times256)$ matrisi oluşturulurken satırları ile sütunları anahtar toplaması işlemini yürütsün ve çıkan sonuç M_2 matrisinin satırlarından bulunsun. Bu satıra karşı gelen değer M_3 matrisine yerleştirilsin. Böylece M_3 matrisi oluşturulacaktır.

9- M_3 matrisi satırları bir bayt için bütün değerleri içermektedir. Şifreleme işlemi için kullanılan 10000 veri rastgele seçilmişti. Bu 10000 verinin birinci baytları M_3 matrisindeki gibi sırasıyla değildir. 10000'lik verinin birinci baytına bakarak M_3 matrisi 10000 veri için dağıtılacaktır. Yeni oluşan matris $M_4(10000\times256)$ şeklindedir.

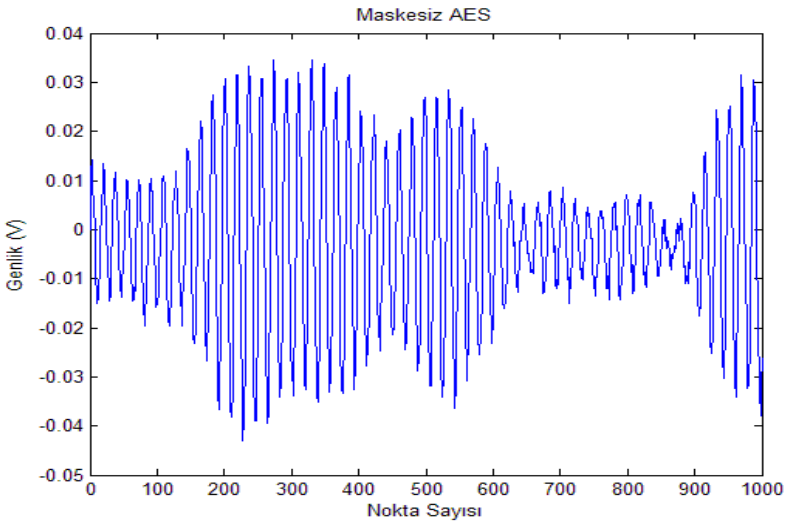
10- M_4 matrisi, ölçümlerle korelasyon analizine sokulacak tahmin matrisidir.

6.2 Elektromanyetik Analizi Sonuçları

Bu bölümde AES algoritmasının maskesiz gerçeklemesi için yapılan EM analizi sonuçları ile AES algoritmasının maskeli gerçeklemesi için yapılan EM analizi sonuçları gösterilecektir.Ayrıca iki bölüm için de kümülantlı sonuçlar belirtilecektir.

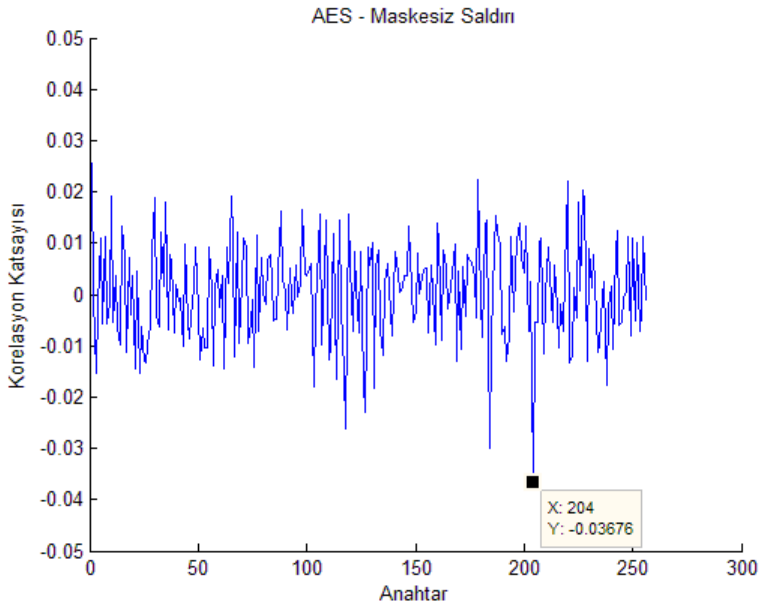
6.2.1 AES algoritmasının maskesiz gerçeklemesi için sonuçlar

Maskesiz AES algoritması yürütülürken son turdaki satırları kaydırma adımı işlemi yapılırken alınan bir ölçüm Şekil 6.3'deki gibidir.



Şekil 6.3 : AES algoritmasının maskesiz gerçeklemesi için satır kaydırma işlemi kaydedici ölçümü

Şekil 6.3'de yatay eksen nokta sayısını dikey eksen ise genliği vermektedir. 150. noktadan itibaren satır kaydırma adımı işlemi yapılmaya başlanmakta ve 600. nokta civarında da işlemin bitmiş olacağı tahmin edilmektedir. Bu yüzden korelasyon analizi yaparken bütün noktaları tek tek almak yerine sadece tahmin edilen bu noktalar arasını almak yeterli olabilir.

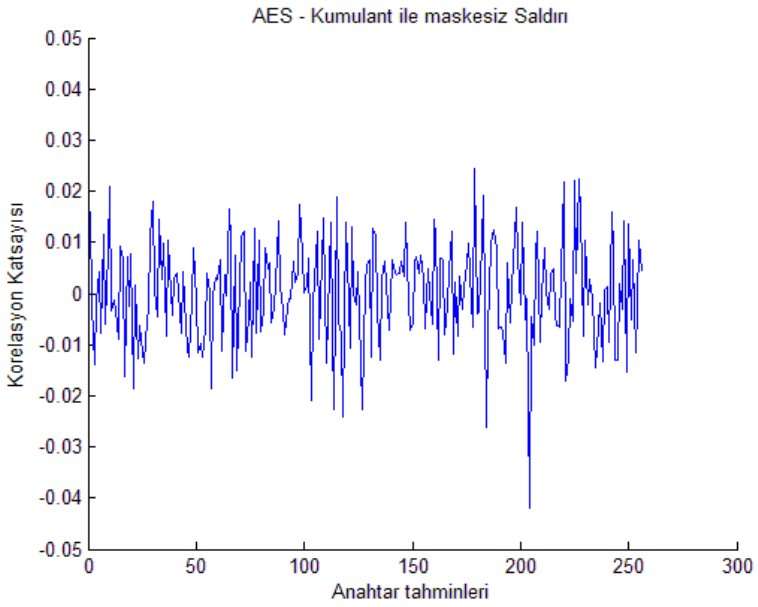


Şekil 6.4 : AES algoritmasının maskesiz gerçeklemesi için korelasyon sonucu

Alınan 10000 ölçüm için ve hesap edilen tahmin matrisleri sonucunda EM saldırısı yöntemi ile yapılan korelasyon analizi sonucu şekil 6.4 deki gibidir. Burada korelasyonu mutlak olarak fazla olan değer 204 değeridir. Bu değerden emin olabilmek için bu değerin diğerlerinden farklı bir şekilde mutlak değerinin artması gerekmektedir. Bunun için ise daha fazla ölçüm alınmalıdır. 204 değeri gerçekte bizim bulmak istediğimiz anahtar değeridir.

6.2.2 AES algoritmasının maskesiz gerçeklemesi için kümülantlı sonuçlar

Yine aynı ölçümler kullanılarak ve aynı tahmin matrisleri kullanılarak yalnız 2. bölümde anlatılan ön işleme süreci olan kümülant yöntemi uygulanarak elde edilen korelasyon sonucu ise Şekil 6.5'deki gibidir.

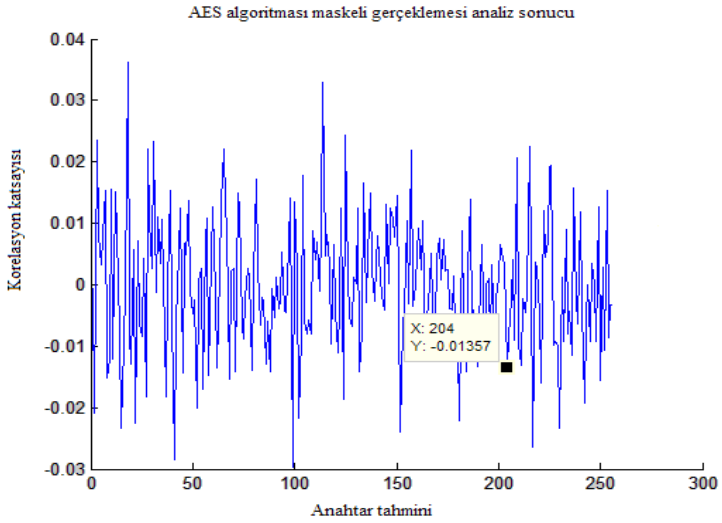


Şekil 6.5 : AES algoritmasının maskesiz gerçeklemesi için kümülant kullanılarak oluşturulan korelasyon sonucu

Şekil 6.4 ve Şekil 6.5 arasındaki farka bakılacak olursa ön işleme süreci olan kümülant analizinin bizim EM analizleri için başarılı sonuç verdiğini söyleyebiliriz. Şekil 6.4' de tahmin edilen anahtar baytı (204) korelasyon sonucu 0.036 iken Şekil 6.5'de 0.04'ün üzerindedir. Aynı sayıda ölçümle gerçekleştirildiği için ön işleme süreci başarılı olmuştur. Ön işleme süreci hakkında bilgi için ve işarete etkisini görmek için Bölüm 2'ye bakılabilir.

6.2.3 AES algoritmasının maskeli gerçeklemesi için sonuçlar

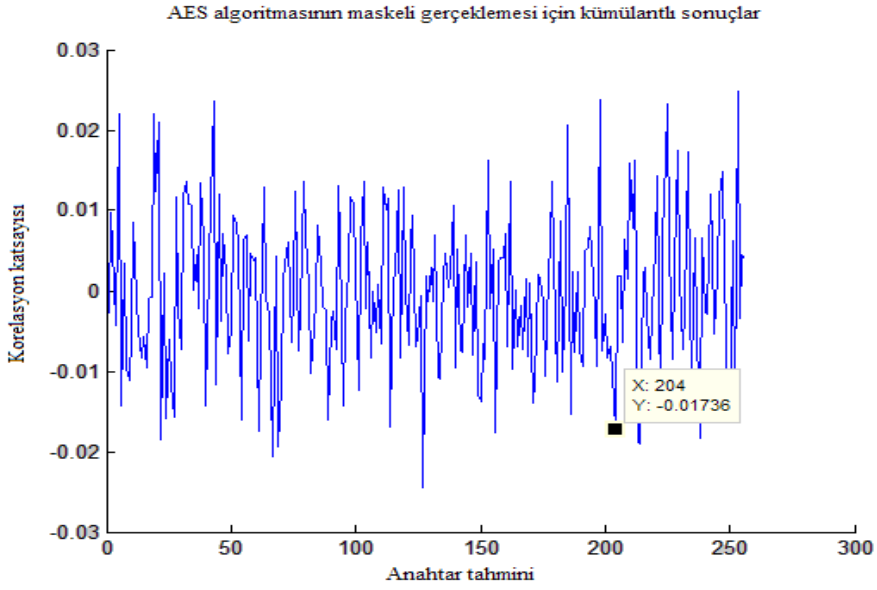
AES algoritmasının maskeli gerçeklemesi için sonuçlar Şekil 6.6'daki gibidir. Anahtarı bulamayışımızın sebebi maskenin AES algoritmasının gerçeklemesinin anahtar bilgisi sızdırmasını engellemesidir.



Şekil 6.6 : AES algoritmasının maskeli gerçeklemesi için korelasyon sonucu

6.2.4 AES algoritmasının maskeli gerçeklemesi için kümülantlı sonuçlar

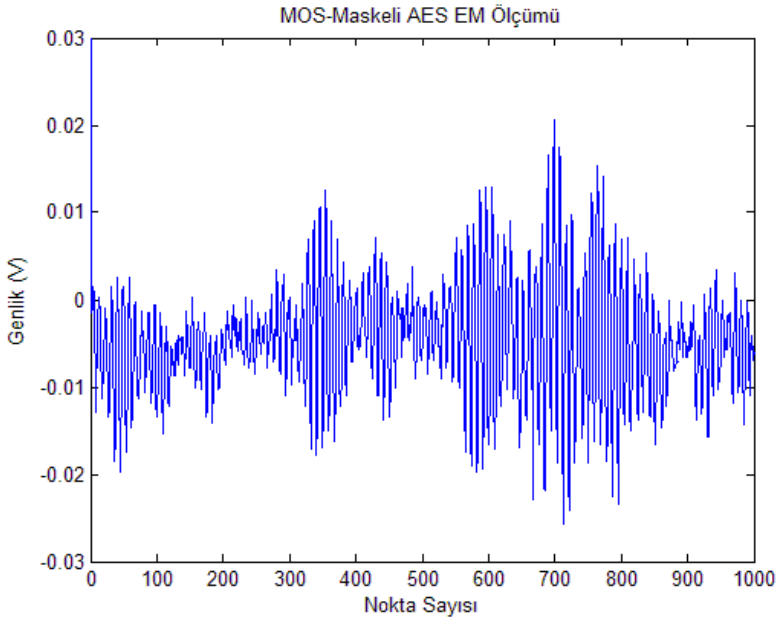
Yine aynı ölçümler kullanılarak ve aynı tahmin matrisleri kullanılarak yalnız 2. bölümde anlatılan ön işleme süreci olan kümülant yöntemi uygulanarak elde edilen korelasyon sonucu ise Şekil 6.7'deki gibidir.



Şekil 6.7 : AES algoritmasının maskeli gerçeklemesi için kümülant kullanılarak oluşturulan korelasyon sonucu

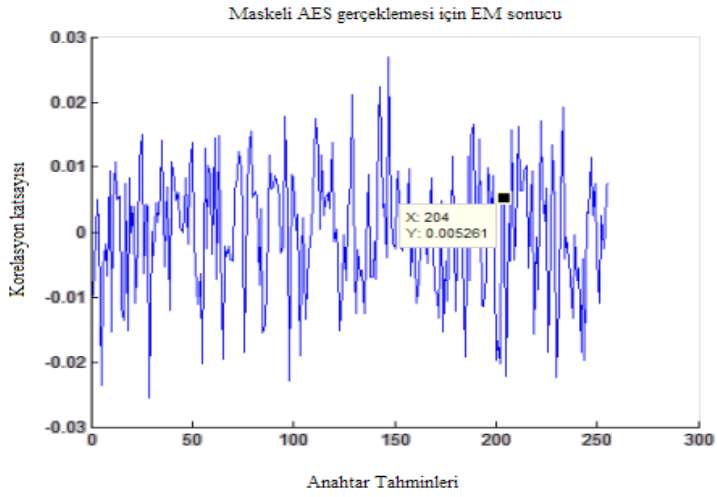
6.2.5 AES algoritmasının maskeli gerçeklemesi için kombinezonsal devre geçiş sayıları kullanılarak elde edilen sonuçlar

Maskeli AES algoritması yürütülürken birinci turun yer değiştirme adımı ve sonraki adım yürütülürken alınan bir ölçüm Şekil 6.8'daki gibidir.



Şekil 6.8 : AES algoritmasının maskeli gerçeklemesi için bayt yer değiştirme işlemi kaydedici ölçümü

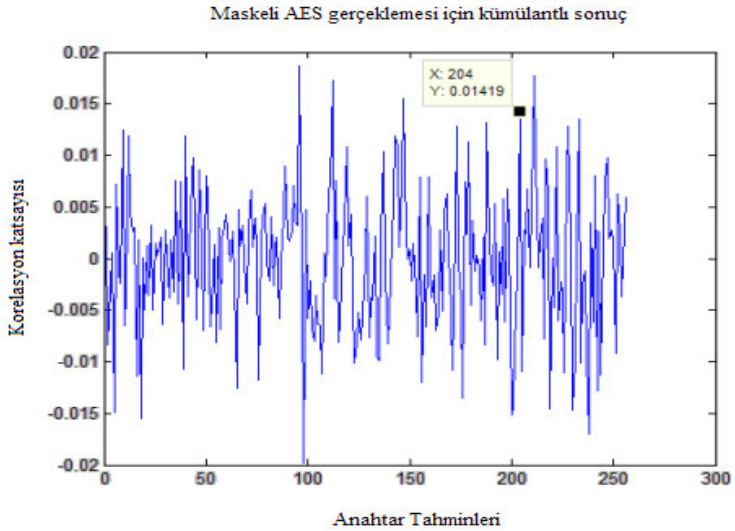
EM alıcısı elemanı ile alınan bu ölçümde iki farklı işlemin varlığı tahmin edilebilmektedir. Ölçüm alınırken osiloskop üzerinde yapılan hesaplamalara göre 200. nokta ile 600. nokta arası birinci işlem olan bayt yer değiştirme işlemini 600. nokta ile 1000. noktalar arası ise satır kaydırma işlemi ölçümlerini göstermektedir. Maskeli sistem için de korelasyon süresini kısaltmak için bütün noktalara bakmak yerine 200. nokta ile 600. nokta arasına bakmak yeterli olacaktır. Şekil 6.9 AES algoritmasının maskeli gerçeklemesi için korelasyon sonuçlarını göstermektedir. Şekil 6.9'den de görüleceği gibi AES algoritmasının maskeli gerçeklemesi için başarılı sonuçlar elde edilememiştir. Bu konu üzerinde çalışmalar devam etmektedir. Şekil 6.9'de anahtar tahmin değerinin (204) "0" a çok yakın olması anahtarı bulamadığımız göstermektedir.



Şekil 6.9 : AES algoritmasının maskeli gerçeklemesi için kombinezonsal yöntem kullanılarak elde edilen korelasyon sonucu

6.2.6 AES algoritmasının maskeli gerçeklemesi için kombinezonsal devre geçiş sayıları kullanılarak elde edilen kümülantlı sonuçlar

Maskesiz AES gerçeklemesi için yapılan kümülant analizi maskeli gerçekleme için de uygulanmıştır. Şekil 6.10 AES algoritmasının maskeli gerçeklemesi için korelasyon sonuçlarını göstermektedir.



Şekil 6.10 : AES algoritmasının maskeli gerçeklemesi için kombinezonsal yöntem ve kümülant kullanılarak oluşturulan korelasyon sonucu

6.2.7 Elektromanyetik analizleri için sonuçların karşılaştırılması

Bu bölümde AES algoritmasının maskesiz gerçeklemesi için kümülantsız ve kümülantlı analizleri için, maskeli gerçeklemesi için yine kümülantsız ve kümülantlı analizleri için ve son olarak da maskeli gerçeklemenin kombinezonsal analizi için karşılaştırmalar verilecektir. AES algoritması için maskeli analizler için başarılı sonuçların elde edilemediği söylenmişti. Çizelge 6.1 analizler için korelasyon katsayısı karşılaştırmasını vermektedir. Korelasyon katsayısı tek başına korelasyon ifadesini vermekle birlikte Şekil 6.4 ve Şekil 6.5'e bakılarak doğru anahtarın korelasyonunun diğer anahtar tahminlerinden kopuşu daha net görülmektedir.

Çizelge 6.1 : AES gerçeklemeleri için korelasyon katsayıları karşılaştırılması

Korelasyon Katsayıları	Maskesiz Gerçekleme	Maskeli Gerçekleme	Kombinezonsal Yöntem
Kümülant kullanılmayarak	0.036	0.013	0.005
Kümülant kullanılarak	0.042	0.017	0.014

7. SONUÇ

Kriptografik sistemlerin güvenliği verilerin güvenli iletilebilmesi için son derece önemli bir konudur. Bu alanda her yeni gün hem algoritma seviyesinde hem de kriptografik sistemin donanımı konusunda gelişmeler kaydedilmektedir. Açıkçası Kriptografi bilimi şu şekilde gelişmektedir; bir grup hâlihazırda kullanılan sistem daha güvenli olsun diye araştırmalar yapmakta ve sistemi gerçeklemektedir. Bir başka grup ise güvenilirliği artırılmış olan sistemi ele alıp analizler yapmaktadır. Bu grup yeni güvenlik önlemlerini aşabilmek üzere bir takım araştırmalar yapmakta ve eğer başarılı olabiliyorsa güvenlik açıklarını göstermektedir. Yeni açıklar üzerine bir takım çalışmalar ile yeni koruma yöntemleri önerilmektedir. Bu çevrim içerisinde daha güvenli bir sisteme doğru gidilmektedir.

Tezin kapsamında bizim yapmaya çalıştığımız AES gerçeklemesinin anahtarının ele geçirilmesi ve devamında AES gerçeklemesinin maskeli gerçeklemesi için anahtarı ele geçirmekti. Bu analizleri yaparken devreye müdahalede bulunmaksızın ölçüm alabileceğimiz bir sistem tasarlamak istedik. Bunun için elektromanyetik radyasyonu kullanma yolunu tercih ettik. Bu noktada elektromanyetik alıcısı elemanını satın almak yerine biz karta özel tasarlanmış bir elektromanyetik alıcısı elemanını kendimiz tasarladık. Bölüm 5'de bununla ilgili anlatımlar yer almaktadır.

Analizler için hem AES algoritmasının maskesiz gerçeklemesi için ve AES algoritmasının maskeli gerçeklemesi için tahmin matrislerini oluşturduk. Maskesiz gerçekleme için tahmin matrisleri oluşturulurken kullanılan model Hamming ağırlıkları modelidir. Maskeli gerçekleme için kullanılan model ise bizim önermeyi düşündüğümüz modeldir. Bu matrisler hakkında bilgi Bölüm 6'da bulunmaktadır.Analizler için korelasyon analizi yöntemi tercih edilmiştir. Korelasyon analizi hakkında bilgi Bölüm 2'de bulunmaktadır.

Analizler için kullanılmak üzere 10000 ayrı şifreleme ölçümü kullanılmıştır. Ölçümler alınırken kurulan sistem Bölüm 6'da anlatılmıştır. Alınan ölçümler ayrıca istatistiksel bir ön işleme sürecinden geçirilmiştir. Kümülant analizi olarak

adlandırılmış bu ön işleme süreci hakkında bilgi Bölüm 2'de bulunabilir. Kümülant analizi için alınan başarılı sonuçlar ise yine Bölüm 6'da görülebilmektedir.

Maskesiz AES gerçeklemesi için ön işleme süreci kullanılarak ve kullanılmayarak elde edilen sonuçlar başarıya ulaştırılmıştır. Diğer bir deyişle maskesiz AES gerçeklemesi için anahtarı elde edebilmekteyiz. Maskeli AES gerçeklemesi için henüz başarılı sonuçlar elde edemedik. Bölüm 6'da anahtarı bulmaya yönelik analizler anlatılmaktadır.

KAYNAKLAR

[1] **Daemen, J. ve Rijmen, V.,** 2002. The Design of Rijhndael AES-The Advanced Encryption Standart.

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

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

[4] **Kommerling, O. ve Kuhn, M.G.,** 1999. Design principles for tamper resistant smartcard processors, Proceedings of the USENIX Workshop on Smartcard Technology.

[5] **Joye, M. ve Lenstra, A.K.,** 1999. Chineese remaindering based cryptosystem in the presence of faults, Journal of Cryptology, vol. 4, no. 12, sf 241-245.

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

[7] **Kocher, P., Jaffe, J. ve Jun, B.,** 1999. Differential power analysis, Advances in Cryptography: CRYPTO'99, vol. 1666, sf 388-397.

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

[9] **Gandolfi, K., Mourtel, C. ve Olivier, F.,** 2001. Electromagnetic Analysis : Concrete Results, Proceedings of CHES. LNCS 2162, sf 251-261**.**

[10] **Chari, S., Jutla C.S., Rao, J.R. ve Rohatgi, P.,** 1999. Towards sound approaches to counteract power-analysis attacks, Advances in CRYPTO'99, vol 1666, sf 398-412.

[11] **Ordu, L.,** 2006. "AES Algoritmasının FPGA Üzerinde Gerçeklenmesi ve Yan Kanal Analizi Saldırılarına Karşı Güçlendirilmesi", İstanbul Teknik Universitesi, Fen Bilimleri Enstitüsü, Türkiye.

[12] **Anderson R., ve Kuhn M.,** Tamper resistance – a cautionary note. In D. Tygar editor, Proceedings of the 2nd USENIX Workshop on Electronic Commerce, pages 1–11, Oakland, CA, USA, November 18-21 1996.

[13] **Boneh D., DeMillo R. A., ve Lipton R. J.,** On the importance of checking cryptographic protocols for faults (extended abstract). In W. Fumy,editor, Advances in Cryptology: EUROCRYPT'97, volume 1233 of Lecture Notes in Computer Science, pages 37–51. Springer-Verlag, 1997.

[14] **Akkar, M.L. ve Giraud, C.,** 2001 .An implementation of DES and AES, secure against some attacks, CHES 2001, Third International Workshop., vol. 2162, sf 309-318.

[15] **Oswald, E., Mangard, S., Pramstaller, N., Rijmen, V.,** 2005. A side-channel analysis resistant description of the AES S-Box, FSE 2005, vol. 3557.

[16] **Goubin, L. ve Patarin, J.,** DES and Differential Power Analysis. In Proc. Workshop on Cryptographic Hardware and Embedded systems, Aug. 1999, LNCS 1717, Springer-Verlag, pp 158-172.

[17] **Kocher P., Jaffe J., ve Jun B.,** Differential Power Analysis:Leaking Secrets. In Proc. Crypto '99**,** , LNCS 1666, Springer-Verlag, pp 388-397.

[18] **Thanh H. L., Clediere J., Serviere C., ve Lacoume J. L.,** Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant. IEEE Transactions on Information Forensics and SEcurity, vol.2, No.4, December 2007.

[19] **Agrawal D., Archambeault B., Rao J. R., ve Rohatgi P.,** The EM Side channel(s). In: Kaliski Jr., B. S., Koç Ç. K., Paar C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 29-45. Springer, Heidelberg (2003).

[20] **Fuchs, László** Infinite abelian groups, Vol. *I*. Pure and Applied Mathematics, Vol. 36. New York-London: Academic Press. xi+290 pp.

[21] **Griffith, Phillip A.** Infinite Abelian group theory. 1970. Chicago Lectures in Mathematics. University of Chicago Press. ISBN 0-226-30870-7.

[22] **MacLane, S. ve Birkhoff, G.**, Algebra (2nd ed.), 1999. AMS Chelsea, ISBN 978-0-8218-1646-2.

[23] **Axler, S**. Linear Algebra Done Right, 2e, Springer. 1997. Abstract algebra theory. Covers commutativity in that context. Uses property throughout book.

[24] **Allenby R.B.J.T.** Rings, Fields and Groups. (1991). Butterworth-Heinemann.

[25] **Lidl, R., ve Niederreiter, H.**, Finite Fields, 1997, 2nd ed., Cambridge University Press.

[26] **Clarke G. M. ve Cooke D.,** A Basic Course in Statistics. Arnold London, 4th edition, 1998.

[27] **Kendall, M.G., Stuart, A.** The Advanced Theory of Statistics, Volume 1 (3rd Edition). Griffin, London. Section 3.12, 1969.

[28] **Ferguson, G. A., Takane, Y.** Statistical Analysis in Psychology and Education, (2005) Sixth Edition. Montréal, Quebec: McGraw-Hill Ryerson Limited.

[29] **Balanis C. A.,** Antenna Theory (Analysis and Design). A.John Wiley and Sons, Inc., Publication.3. Baskı. 2005.

[30] **Cheng D. K.**, Çev: Armağan N., Can N., Çıncı E., İşçi C., Önengül G., ve Sözüer S. Dalga ve Alan Elektromanyetizması. Akademi Yayıncılık.1. Baskı. 2003.

[31] **Griffiths D. J.,** Çev: Unal B., Elektromanyetik Teori. Gazi Kitabevi. Ekim 2003.

[32] **Jordan E. C. ve Balmain K. G..** Electromagnetic Waves & Radiating Systems. 2. Baskı.Şubat 1967.

[33] **Sommer M. R.,** Smartly analysing the simplicity and the power of simple power analysis on smartcards, in Proc. CHES,Worcester,MA, 2000, pp. 78–92.

[34] **Coron J., Kocher P., ve Naccache D.,** Statistics and secret leakage, in Proc. Financial Cryptography, Anguilla, British West Indies, 2001, pp. 157–173.

[35] **Brier E., Clavier C., ve Olivier F.,** Correlation power analysis with a leakage model, in Proc. CHES, Cambridge, MA, 2004.

[36] **Kang S. M. ve Leblebici Y.,** CMOS Digital Integrated Circuits: Analysis and Design. McGraw Hill, 2002.

[37] **Funato H., ve Suga T.,** Magnetic Near-field Probe for GHz Band and Spatial Resolution Improvemetn Technique. 17th International Zurich Symposium on Electromagnetic Compatibility, T2 – MEAS – 1 – 2 . 2006

ÖZGEÇMİŞ

Ad Soyad: Muhammet ŞAHİNOĞLU

Doğum Yeri ve Tarihi: Senirkent/ISPARTA, 1983

Adres: İstinye Mah. İ. Galip Arcan Sok. Demircioğlu Apt. No:9 Daire:9
Sarıyer/İSTANBUL

Lisans Üniversite: İstanbul Teknik Üniversitesi, Elektronik Mühendisliği, 2006