T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

GÖMÜLÜ SİSTEMLERDE ŞİFRELEME ALGORİTMALARININ GERÇEKLENMESİ VE YAN KANAL ATAKLARINA KARŞI GÜÇLENDİRİLMESİ

Mehmet Şahin AÇIKKAPI

Doktora Tezi

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

MAYIS 2020

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Tezi

GÖMÜLÜ SİSTEMLERDE ŞİFRELEME ALGORİTMALARININ GERÇEKLENMESİ VE YAN KANAL ATAKLARINA KARŞI GÜÇLENDİRİLMESİ

Tez Yazarı
Mehmet Şahin AÇIKKAPI

Danışman
Prof. Dr. Ahmet Bedri ÖZER

MAYIS 2020
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Tezi

Başlığı: Gömülü Sistemlerde Şifreleme Algoritmalarının Gerçeklenmesi ve Yan Kanal Ataklarına Karşı Güçlendirilmesi

Yazarı: Mehmet Şahin AÇIKKAPI

İlk Teslim Tarihi: 31.03.2020

Savunma Tarihi: 06.05.2020

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

İmza

Danışman: Prof. Dr. Ahmet Bedri ÖZER — Onayladım
Fırat Üniversitesi, Mühendislik Fakültesi

Başkan: Doç. Dr. Eser SERT — Onayladım
Turgut Özal Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi

Üye: Doç. Dr. Taner TUNCER — Onayladım
Fırat Üniversitesi, Mühendislik Fakültesi

Üye: Doç. Dr. Fatih ÖZKAYNAK — Onayladım
Fırat Üniversitesi, Teknoloji Fakültesi

Üye: Dr. Öğr. Üyesi Selman YAKUT — Onayladım
Turgut Özal Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Soner ÖZGEN
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Gömülü Sistemlerde Şifreleme Algoritmalarının Gerçeklenmesi ve Yan Kanal Ataklarına Karşı Güçlendirilmesi" Başlıklı Doktora Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

06.05.2020

Mehmet Şahin AÇIKKAPI

ÖNSÖZ

Başdöndürücü bir hızla gelişen teknoloji dünyası hayatımızı kolaylaştırdığı kadar veri güvenliğimizi de bir o kadar tehlikeye atmaktadır. Süregelen teknolojik gelişmeler içerisinde gömülü sistemler birçok açıdan hayatımızı kolaylaştırmaktadır. Ancak gömülü sistemler yaygınlaştıkça bu sistemlere fiziksel saldırılarda da artışlar meydana gelmiştir. Veri güvenliğini sağlamak açısından bu sistemlerin güvenliği büyük bir sorun oluşturmaya başlamıştır. Bu fiziksel saldırılara karşı koyma konusu klasik kriptoanaliz saldırılarını engellemekten daha zor bir durum haline gelmiştir. Bu durum bizi bu konuda çalışmaya teşvik eden sebeplerin başında gelmiştir. Bu tez kapsamında bu güvenlik sorunları farklı bir bakış açısı ile ele alınmış ve kaotik sistemlerden elde edilen veriler ile bu fiziksel saldırılara karşı güvenliği artırmak amaçlanmıştır.

Tez konusunun belirlenmesinden sonuçlanmasına kadar her aşamada desteğini esirgemeyen Prof. Dr. A. Bedri ÖZER hocama ve kaotik sistemlerin fiziksel saldırılara karşı kullanılmasında önerileri ile eksikliklerimi gidermeme yardımcı olan Doç. Dr. Fatih ÖZKAYNAK hocama teşekkürlerimi sunmayı bir borç bilirim.

Bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **MF.16.66** protokol numaralı proje ile desteklenmiştir.

Mehmet Şahin AÇIKKAPI
ELAZIĞ, 2020

İÇİNDEKİLER

Sayfa

ÖZET

Gömülü Sistemlerde Şifreleme Algoritmalarının Gerçeklenmesi ve Yan Kanal Ataklarına Karşı Güçlendirilmesi

Mehmet Şahin AÇIKKAPI

Doktora Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Mayıs 2020, Sayfa: 75

Hızla gelişen teknoloji, insan hayatını birçok yönden etkilemektedir. Özellikle bilgi teknolojileri alanındaki gelişmeler hızına yetişilemeyecek ölçüye ulaşmış bulunmaktadır. Teknoloji alanında sürekli gelişmeler meydana gelirken bilgi güvenliği kavramı her zamandan daha fazla olacak şekilde önem kazanmış bulunmaktadır. Son yıllara kadar bilgi güvenliği konusunda daha çok şifreleme algoritmalarının matematiksel olarak güçlülüğü ve bilgisayar sistemlerinin yazılımsal olarak güvenliği ön planda tutulmaktaydı. Ancak son yıllarda gömülü sistemler hayatımızın her alanında yer almaya başlamış ve bu sistemlere karşı yapılabilecek yan kanal saldırıları gibi fiziksel saldırılar büyük tehlikeler arz etmeye başlamıştır. Bu tez kapsamında getirilen önerilerle gömülü sistemlerin yan kanal saldırılarına karşı güvenliklerinin maximum seviyeye çıkarılması hedeflenmiştir.

Anahtar Kelimeler: Gömülü sistemler, Yan kanal saldırıları, Farksal Güç Analizi, Kaotik s-box

ABSTRACT

Implementation of Encryption Algorithms in Embedded Systems and Strengthening Against Side Channel Attacks

Mehmet Şahin ACIKKAPI

PhD Dissertation

FIRAT UNIVERSITY
Institute of Natural Sciences

Department of Computer Engineering

May 2020, Pages: 75

Rapidly developing technology affects human life in many ways. In particular, the developments in the field of information technologies have reached a level that cannot be reached. While continuous developments are occurring in the field of technology, the concept of information security has become more important than ever. Until recent years, mathematical strength of encryption algorithms and software security of computer systems were prioritized in terms of information safety. However, embedded systems have started to take place in every area of our lives in recent years and physical attacks such as side channel attacks against these systems have started to pose great dangers. With the suggestions brought within the scope of this dissertation, it is aimed to maximize the security of embedded systems against side channel attacks.

Keywords: Embedded systems, Side channel attacks, Differential power analysis, Chaotic s-box

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

EKLER LİSTESİ

Sayfa

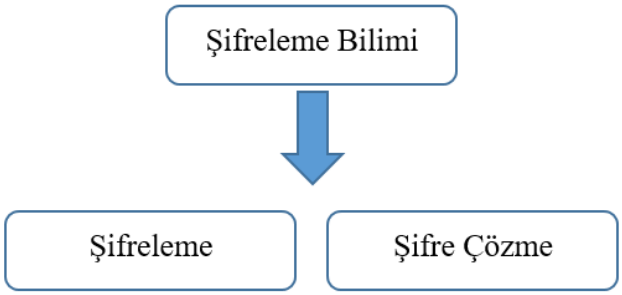
SİMGELER VE KISALTMALAR

Kısaltmalar

AES : Advanced Encryption Standard
BIC : Bit Independence Criterion
DPA : Differential Power Analysis
HD : Hamming Distance
HW : Hamming Wight
SAC : Strict Avalance Criteria
S-BOX : Substitution Box
SPA : Simple Power Analysis

1. GİRİŞ

Bilgi çağı olarak isimlendirilen çağımızda bilgi ve iletişim teknolojilerinin hayatımızın her alanında kullanılması kaçınılmaz olmuştur. Ülkeler gerçek ordularının yanında siber ordular kurma gayretine girişmekte hatta ileri kriptografik tekniklerle oluşturulan dijital para birimleri para piyasalarında yer almaya başlamaktadır. Tüm bu gelişmeler içerisinde bilgi ve iletişim teknolojileri kullanılırken veri güvenliği konusu çok önemli bir etken olarak karşımıza çıkmaktadır. Diğer yandan teknolojinin gelişmesiyle günlük hayatımıza dahil olan elektronik cihazlarda veri güvenliğini sağlamakda büyük önem kazanmıştır. Veri güvenliğini sağlamak için en önemli faktör verilerin şifrelenmesidir. Bu nedenle şifreleme biliminin önemi çok büyük bir hızla artmaya devam etmektedir. Kavram olarak şifreleme bilimi; Veri alış verişinde bulunan iki veya daha fazla tarafın veri alışverişlerini güvenli bir şekilde yapmalarını sağlayan ve bunu sağlamak içinde çözülmesi çok zor matematiksel işlemler ve problemler kullanan bilim dalıdır. Günümüzde ise şifreleme bilimi; matematik, elektronik, optik, bilgisayar bilimleri gibi birçok disiplinden faydalanan özelleşmiş bir bilim dalı olarak bilim dünyasında yerini almıştır. Şekil 1.1' de görüldüğü gibi şifreleme bilimi şifreleme ve şifre çözme olmak üzere iki alt dala sahiptir [1].



Şekil 1.1. Şifreleme biliminin alt dalları

Veri güvenliğini sağlamada şifreleme ne kadar öneme sahipse şifre çözmede en az o kadar öneme sahiptir. Güçlü şifreleme sistemleri oluşturabilmek için şifreleme algoritmalarının şifre çözme yöntemlerine karşı oldukça dayanıklı olmaları gerekmektedir. Buna ek olarak, algoritmaların şifre çözme yöntemlerine karşı mukavemetleri yapılacak şifre çözme testleri ile denenmelidir. Aksi takdirde çok güçlü oldukları düşünülen şifreleme algoritmaları kripto analizciler tarafından dakikalar içerisinde kırılma tehlikesi içerisinde olabilirler.

Bir kriptografik algoritma şemasına iki bakış açısından bakılabilir. Birincisi; Şemaya soyut bir matematiksel obje veya gizli anahtar ve giriş bilgisini alarak çıkış bilgisi üreten bir kara kutu gibi bakmaktır. İkinci bakış açısı ise bilinen bir işlemci üzerinde gerçeklenmiş bir program olarak

bakmaktır. Birinci bakış açısı klasik kripto analizin konusudur. İkinci bakış açısı ise genellikle gömülü sistemler üzerinde icra edilen ***fiziksel atakları*** konu alır [2].

Klasik kriptoanalizde algoritmaların zayıflıkları araştırılır, algoritmaların matematiksel olarak dezavantajları sömürülmeye çalışılır veya yüksek performanslı bilgisayar sistemleri kullanılarak kaba kuvvet atakları ile algoritmaya ait olabilecek tüm gizli anahtar bilgileri deneme yanılma yöntemi ile denenerek algoritmanın gerçek anahtar bilgisi tespit edilmeye çalışılır.

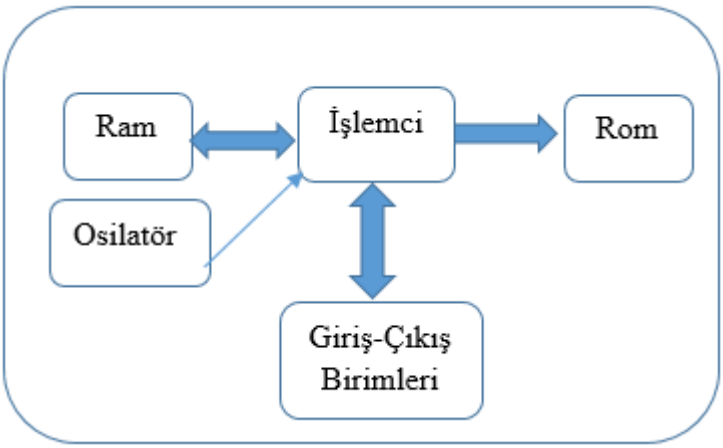
Fiziksel ataklarda ise bir gömülü sistem üzerinde çalışan kriptografik algoritmanın çalışması esnasında aygıtın dışarıya sızdırdığı veriler üzerinden şifre çözme işlemleri gerçekleştirilmeye çalışılır.

2. FİZİKSEL ATAKLAR

Teknolojik gelişmelerin bir getirisi olarak dijitalleştirilmiş gömülü sistemlerin önemi hayatımızda giderek artarken buna paralel olarak bu gömülü sistemlere karşı birtakım yeni atak türleri geliştirilmiştir. Bu atakların en tehlikelisi fiziksel ataklardır. Fiziksel ataklar incelenmeden önce fiziksel atakların icra merkezi olan gömülü sistemlerin incelenmesi önemlidir. Zira günümüzde son derece yoğun kullanılan elektronik devreler için genellikle gömülü sistemler kullanılmaktadır. Buna bağlı olarak bu cihazların güvenliklerinin sağlanması çok kritik öneme sahiptir.

2.1. Gömülü Sistemler

Bir gömülü sistem bir veya bir dizi işlevi yerine getirmek üzere ve genelde bir kişisel bilgisayar gibi son kullanıcının programlaması için olmayacak şekilde yazılım ve donanımın kombinasyonu olarak tasarlanan sistemdir [3]. Çamaşır makinesi, bulaşık makinesi, buzdolabı, akıllı kimlik kartı, garaj kumandası, araç uzaktan kumandası ve benzeri günlük kullandığımız birçok teknolojik alet gömülü sistemlere örnek olarak verilebilir.



Şekil 2.1. Mikrodenetleyici genel yapısı

Bir kişisel bilgisayarda mikroişlemci, bellek, giriş çıkış birimleri, osilatör gibi birimler ayrı ayrı olarak bulunur. Ancak bir gömülü sistemde Şekil 2.1' de görüldüğü gibi tüm bu birimler mikrodenetleyici içerisinde bütünleşik olarak bulunur. Bu sayede gömülü sistemden istenen işlevler çok daha uygun maliyetlerle en uygun performansı gösterecek şekilde yerine getirilebilmektedir. Aksi halde gömülü sistem için mikroişlemci kullanılması durumunda Ram-Rom bellek, osilatör, analog dijital çevirici gibi tüm birimler ayrı ayrı temin edilip bu birimler ve mikroişlemci arasında

veri yolu, adres yolu bağlantılarının oluşturulması gerekecektir [4]. Tahmin edileceği gibi bu durum sistem tasarım sürecini maliyet ve zaman açısından olumsuz olarak etkileyecektir. Bu sebeplerden dolayı birçok sektörde gömülü sistemlerin kullanımı hızla artmış ve artmaya devam etmektedir.

2.2. Gömülü Sistemlere Karşı Fiziksel Ataklar

Fiziksel ataklar literatürde iki dikey eksende sınıflandırılabilir. Birinci eksendeki ataklar Invasive-istilacı ve Non Invasive-istilacı olmayan ataklardır. Invasive ataklarda aygıtın iç yapısına ulaşılabiliyordur. Örneğin bir kablo bağlantısı ile data yolundaki veriler elde edilebilir. Non-Invasive ataklarda ise aygıtın dışarıya sızdırdığı veriler sömürülmeye çalışılır [2].

Fiziksel atakların sınıflandırılmasında ikinci eksende ise ***aktif*** ve ***pasif*** ataklar yer alır. Aktif ataklarda aygıt dışarıdan karıştırılmaya çalışılır, yani aygıta dış müdahale söz konusudur. Örneğin aygıta hata enjekte edilerek açığa çıkan sonuçlar üzerinden şifre çözme işlemleri için ipuçları elde edilmeye çalışılabilir. Bu hata enjektesi, aygıta uygulanacak voltaj değişiklikleri, osiloskop frekans değişiklikleri gibi istila adımları olabilir. Bu hata enjekte durumlarında aygıtın farklı davranma durumlarında aygıttan dışarıya sızacak veriler sömürülmeye çalışılır. Pasif ataklarda ise aygıta dışarıdan müdahale olmamakla birlikte aygıtın şifreleme esnasındaki işlem süreci incelenir ve aygıtın dışarıya sızdırdığı bilgiler sömürülerek şifre çözmeye çalışılır [5]. Bu tezin konusu olan ataklar aygıtın iç yapısına müdahale etmeyecek olan Non-Invasive ve Pasif olan yan kanal ataklarıdır.

2.3. Yan Kanal Atakları

Şifreleme algoritmaları genellikle algoritma yapısı itibarıyla güçlü olmaları ve anahtar uzayının büyük olması ile kaba kuvvet ataklarına karşı güçlerini korumaktadırlar. Ancak son yıllarda önemi hızla artan yan kanal ataklarında algoritmalar matematiksel temelleri çok sağlam ve anahtar uzayları çok geniş olsa dahi bu fiziksel atak yöntemi karşısında yetersiz kalabilmektedirler [6]. Bu saldırılar özellikle kriptografik gömülü cihazlarda (Smart Kart, Asic, Mikrodenetleyici, FPGA, RFIDs vb.) çok etkili olabilmektedir. Kriptografik cihazların çalışmaları esnasında yaydıkları elektromanyetik alan [7], ses, ısı seviyelerinden, harcadıkları güç tüketiminden [8], algoritmaların çalışma sürelerinden [9] yola çıkılarak yapılacak yorumlamalarla şifreleme sistemi kırılabilmektedir [10].

Yan kanal atağı fiziksel atakların en popüler olanıdır [11]. Yan kanal atağı ile yapılan analizin amacı kriptografik operasyonlardaki gizli parametreleri öğrenmektir. Normal operasyonların fiziksel ve/veya elektriksel etkileri analiz için kullanılır. Eğer bu etkiler istemsiz olarak gizli anahtar hakkında bilgi veriyorsa bu sundukları bilgiye ***yan kanal bilgisi*** ve etkilere de

yan kanal denir. Yan kanal analizi kullandığı etkiye göre zamanlama, güç, elektromanyetik radyasyon analizleri ve akustik analiz olmak üzere dört gruba ayrılır. Zamanlama analizinde kriptografi işleminin tamamlanma zamanı kullanılır [12]. Aygıtın kriptografi işlemi sırasındaki dinamik güç tüketimi güç tüketim analizinde kullanılır [13]. Elektromanyetik radyasyon analizi aygıtın operasyon sırasında ürettiği elektromanyetik radyasyonu kullanır [14]. Akustik analiz aygıtın operasyon sırasında ürettiği sesi kullanır [15].

Yan Kanal atakları ilk olarak 1956 yılında İngiliz iç istihbarat servisi tarafından Mısır büyükelçiliklerinde kullanılan şifreleme makinalarının çıkardığı ses dinlenerek kullanılmıştır [16]. Yan kanal ataklarından bahseden ilk akademik yayın ise 1996 yılında Paul KOCHER tarafından yayınlanmıştır [17]. Yan kanal analizi ataklarına karşı alınacak önlemler yazılımsal ve donanımsal önlemler olmak üzere iki grup olarak değerlendirilebilir [18,19].

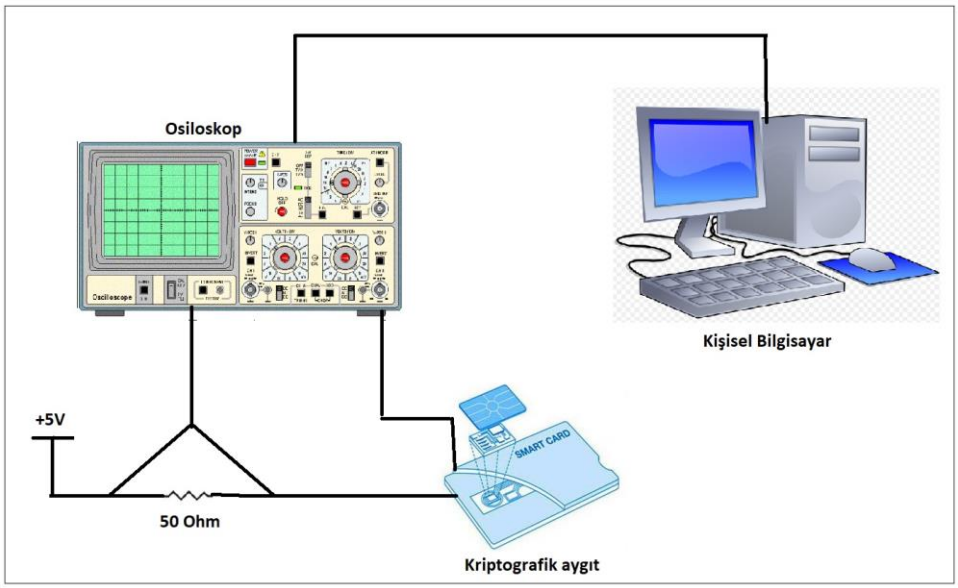
Yan kanal atakları klasik kriptoanaliz ataklarından daha güçlüdürler. Son zamanlarda geliştirilen bazı donanım sistemleri ile yan kanal analizleri düşük maliyetli bir şekilde gerçekleştirilebilmektedir [20,21]. Gömülü sistem üreticileri açısından özellikle bir yan kanal analizi atağı türü olan ***güç analizi atakları*** çok tehlikeli boyutlara varmıştır [2]. Bu nedenle kriptografik aygıt üreticileri çok ciddi bir şekilde ürettikleri aygıtların güç analizi ataklarına karşı dayanıklılığını göz önünde bulundurmaktadırlar [22].

3. GÜÇ ANALİZİ ATAKLARI

Fiziksel ataklardan olan yan kanal ataklarında en fazla kullanılan yöntem aygıtın güç tüketiminden faydalanılarak analiz yapılan yöntemlerdir. Güç tüketiminden yola çıkılarak Basit Güç Analizi Atağı ve Diferansiyel Güç Analizi Atağı olmak üzere iki önemli atak türü yapılmaktadır [23,24]. Basit güç analizinde aygıtların anlık güç tüketimleri ölçülerek yorumlanır ve anahtarla ilgili bilgilere ulaşılmaya çalışılır. Algoritmalarda yürütülen işlemlerin, üzerinde işlem yapılan veri ile bağlantılı olarak değiştiği bölümler bulunuyorsa basit güç analizi sonuç verebilir [13]. Diferansiyel güç analizi ataklarında ölçülen güç tüketimi değerleri ile gizli bilgiler arasında ilişki kurulmaya çalışılır. Bunun için çok fazla sayıda güç tüketimi ölçümü yapılır ve bu değerler istatistiki değerlendirmelere tabi tutulur [25].

Smart kartlar gibi kriptografik aygıtların güç tüketimleri aygıtın işlediği dataya ve yürüttüğü komutlara bağlıdır. Bu güç tüketimleri aygıtın güç kaynağına bağlı pini veya toprak pinine bir direnç eklenerek osiloskop vasıtasıyla ölçülebilir. Bu şekilde elde edilen ölçüme ***güç izi*** ismi verilir [26].

Bir kriptografik aygıta yapılacak güç saldırılarında Şekil 3.1' de görüldüğü gibi cihazın güç tüketim değerleri bir osiloskop vasıtasıyla ölçülür. Çok sayıda şifreleme işlemi yürütülürken ölçülen güç tüketim değerleri istatistiksel olarak değerlendirmeye tabi tutulmak üzere kişisel bilgisayara kaydedilir.



Şekil 3.1. Güç analizi atağı için atak ortamı

3.1. Basit Güç Analizi

Kısaca SPA (Simple Power Analysis) olarak adlandırılan basit güç analizi kriptografik işlem sırasında elde edilen güç tüketim izinin görsel olarak yorumlanmasını içeren bir tekniktir [13]. Diğer bir deyişle saldırgan doğrudan elde edilmiş bir güç izinden anahtar hakkında bilgi edinmeye çalışır. Buna bağlı olarak, saldırgan elde ettiği tek güç izini daha önceden farklı anahtarlar kullanılarak oluşturulan elinde bulundurduğu güç izi örnekleri ile karşılaştırarak uygun bir eşleşme bulmaya çalışır. Bu SPA ataklarını pratikte oldukça etkili kılar. SPA atakları çoğu zaman saldırı altındaki aygıt tarafından yürütülen kriptografik algoritmanın implementasyonu hakkında detaylı bilgi gerektirirler. Bununla birlikte sadece bir tane güç izi varsa anahtar hakkında bilgi edinmek için genellikle kompleks istatistiksel metotlar kullanılmak zorundadır. Pratikte SPA atakları; verilmiş bir giriş seti için sadece çok az güç izi mevcutsa kullanılır. Bir müşterinin alışveriş yaptığı herhangi bir işyerinde smart kart sisteminin kullanıldığı bir ödeme aracı ile ödeme yaptığı varsayılsın. Müşteri benzer miktarlarda bir alışveriş yapıyorsa ödemeler esnasında kötü niyetli bir kart okuyucu ödeme kartının güç tüketimlerini kaydedebilir. Bu durumda saldırgan benzer açık metinler için birkaç güç izi toplayabilir. Kötü niyetli kişi bu izlerden yola çıkarak basit güç analizi atağında bulunabilir.

SPA ataklarının hedefi az sayıdaki açık metin için az sayıda güç izi bulunduğu durumlarda anahtarı açığa çıkarmaktır. SPA atakları bir güç izi içerisindeki anahtara bağlı farklılıkları sömürür bundan dolayı saldırılan aygıtta; anahtar değeri güç tüketimi üzerinde doğrudan veya dolaylı olarak önemli bir etkiye sahip olmalıdır. Aksi halde atak sonuç vermeyecektir [2].

SPA icra edilen komutların sırasınıda açığa vurabildiği için işlem sırası işlediği dataya bağlı olan kriptografik imlementasyonu kırmada DPA atakları için ön hazırlık niteliğindede kullanılabilmektedir [27].

3.2. Diferansiyel Güç Analizi

Kısaca DPA (Differential Power Analysis) olarak isimlendirilen diferansiyel güç analizi atakları en popüler güç analizi ataklarıdırlar. Bunun sebebi atak yapılacak aygıt hakkında detaylı bilgi gerektirmemeleridir. Ayrıca kaydedilen güç izleri aşırı şekilde gürültülü olsa dahi DPA, aygıtın güvenli anahtarını açığa çıkarabilir [5,28].

SPA ataklarının aksine DPA atakları çok sayıda güç izi gerektirirler [29]. Bu nedenle bir aygıtın üzerinde DPA atağı gerçekleştirebilmek için aygıta üzerinde şifreleme işlemleri yapılıp sonuçları alınabilecek şekilde fiziksel erişim gereklidir [10]. Bir örnek olarak elektronik cüzdan verilebilir. Saldırgan güvenli anahtarı açığa çıkarmak için cüzdana veya cüzdandan küçük miktarlarda birçok defa transfer gerçekleştirerek bu transferler esnasında güç izlerini kaydedebilir. Saldırgan bu güç izlerini kullanarak cüzdanın kriptografik anahtarını açığa çıkarabilir [30].

3.2.1. Dpa Ataklarının Genel Tanımı

DPA ataklarının genel amacı atakda bulunulacak kriptografik aygıt şifreleme veya şifre çözme işlemini gerçekleştirirken kaydedilmiş olan çok sayıdaki güç izine dayalı olarak aygıtın gizli anahtarını açığa çıkarmaktır. DPA atakları SPA atakları ile karşılaştırıldığı zaman en büyük avantajı aygıt hakkında detaylı bilgi gerektirmemesidir [30]. Hatta genellikle aygıt tarafından gerçekleştirilen algoritmanın bilinmesi yeterlidir.

İki atak türü arasındaki diğer önemli ayrım kaydedilen güç izlerinin farklı bir şekilde analiz edilmesidir [19]. SPA ataklarında aygıtın güç tüketimi başlıca olarak zaman ekseninde analiz edilir. Saldırgan tek bir iz içerisinde örnek bulmayı veya uygun bir şablona eşleşmeyi dener. DPA atağı durumunda ise izlerin zaman ekseni boyunca biçimleri çok önemli değildir. DPA atakları güç izlerinin zamanın sabit anlarında işlenen dataya (açıkmetin veya şifreli metin) nasıl bağlı olduğunu analiz eder. Bu nedenle DPA atakları yoğunlukla güç izlerinin veri bağımlılığına odaklanır. Kısacası DPA atakları kriptografik aygıtların güç tüketiminin veri bağımlılığını sömürür [18,31]. Bu ataklar işlenen verinin bir fonksiyonu olarak zamanın sabit anlarında aygıtın güç tüketimini analiz etmek için çok sayıda güç izi kullanır [25].

3.3. Dpa Ataklarının Adımları

Detaylı bir şekilde DPA analizinin kriptografik aygıtın gizli anahtarını nasıl açığa çıkardığına bakıldığında SPA ataklarının aksine DPA atakları 5 adımdan oluşacak şekilde genel bir strateji kullanırlar [2,11-15].

3.3.1. Algoritmanın Bir Ara Sonucunu Seçmek

DPA atağının 1.adımı atak yapılacak aygıt tarafından gerçekleştirilen algoritmanın bir ara sonucunu yani algoritmanın atak yapılacak olan alt bölümlerinden birinde elde edilen sonucu seçmektir. Örneğin bu ara sonuç AES için herhangi bir adımın çıkış değeri olabilir [32].

d → Bilinen sabit olmayan data değeri(açık metin veya şifreli metin olabilir)

k → Anahtarın küçük bir bölümü (tamamı değil) olmak üzere;

Bu ara sonuç bir ***f(d,k)*** fonksiyonu olarak düşünülebilir. Bu ara sonuçlar k‘ yı açığa çıkarmak için kullanılabilir. Atak senaryosunda d, şifreli metin veya açık metinden herhangi biri olabilir. Saldırı açık metinler üzerinden yapılacaksa **d** açık metini, şifreli metinler üzerinden yapılacaksa **d** şifreli metini temsil eder.

3.3.2. Güç Tüketimini Ölçmek

Şifreleme esnasında işleme tabi tutulacak açık metin sayısı D ile gösterilsin, DPA atağının 2.adımı kriptografik aygıt D tane random veri bloğunu şifrelerken veya şifresini çözerken aygıtın güç tüketimini ölçmektir [33]. Bu şifreleme/şifre çözme adımlarının herbiri için saldırgan karşılık gelen d değerini bilmektedir.

d → Bölüm 3.3.1' de seçilen ara sonucun hesaplanmasında kullanılan d değeri olmak üzere bilinen bu data değerleri bir d' vektörü olarak;

d' = (d_1, d_2, ….., d_D) şeklinde yazılabilir.

Burada $\mathbf{d_i}$: i. Şifreleme adımındaki data değerine karşılık gelir. D tane(örneğin 1000) şifreleme adımı boyunca saldırgan güç izlerini kaydeder.

$\mathbf{d_i}$ (i.adımdaki data değeri) ile şifreleme yapılırken ölçülen güç izi; $\mathbf{t_i' = (t_1, t_2, \ldots, t_T)}$ vektörü olarak gösterilir. Burada T güç izinin uzunluğunu temsil eder. Örneğin 5 Mhz de örneklenmiş 1 milisaniyelik bir işlem ölçülüyorsa güç izi 5000 nokta içerecek uzunlukta olacaktır. Saldırgan D tane data bloğunun herbirinin şifrelenmesi esnasında güç izlerini ölçer. Ölçülen bu izler **D x T** boyutundaki bir **T matrisi** olarak yazılabilir.

$$
\begin{bmatrix}
t_{11} & t_{12} & t_{13} & \ldots\ldots t_{1T} \\
t_{21} & t_{22} & t_{23} & \ldots\ldots t_{2T} \\
. & & & \\
. & & & \\
t_{D1} & t_{D2} & t_{D3} & \ldots\ldots t_{DT}
\end{bmatrix}
$$

Şekil 3.2. T ölçülen güç izleri matrisi

Şekil 3.2' de görülen T matrisinde;

- t_{11} : 1 nolu data değerine karşılık gelen güç izinin 1.bölümü
- t_{1T} : 1 nolu data değerine karşılık gelen güç izinin T.bölümü
- t_{D1} : D. data değerine karşılık gelen güç izinin 1.bölümü
- t_{DT} : D. data değerine karşılık gelen güç izinin T.bölümü

şeklindedir.

Algoritma önceden bilinen random giriş değerleri ile aygıtta çalıştırılırken ölçülen her güç izi T uzunluğunda bir vektördür. Bu vektörlerden D tane vardır. D toplam açıkmetin sayısıdır. T matrisinin her satırı; bu satıra karşılık gelen random data değeri için ölçülen güç izlerini ifade eder.

DPA atakları için ölçülen güç izlerinin doğru bir şekilde hizalanmış olması çok önemlidir. Bu şu anlama gelir; T matrisinin her t_j sütunundaki güç tüketim değeri farklı açık metinlerle şifreleme yapıldığı esnada algoritmanın aynı operasyonları tarafından oluşturulan güç tüketim

değerleri olmalıdır. Hizalanmış güç izleri elde etmek için osiloskop için tetikleme sinyali öylebir şekilde oluşturulmalıdır ki; osiloskop güç izlerini, her şifreleme adımı boyunca tam olarak aynı operasyon sırasında kaydetmelidir. Böyle bir tetikleme sinyali mevcut değilse güç izleri "güç izleri hizalama teknikleri" kullanılarak hizalanmalıdır [2,20,34].

3.3.3. Ara Değerleri Hesaplamak

Bölüm 3.3.2' de kriptografik aygıt bilinen çok sayıda random açık metin değeri (D tane) için çalıştırılarak güç tüketim değerleri kaydedilmiştir. DPA atağının 3. adımı ise Bölüm 3.3.2' de kullanılan D tane açık metin değeri ile muhtemel her k gizli anahtar değerini kullanarak Bölüm 3.3.1' de seçilmiş olan algoritmanın alt bölümünü yazılım ortamında çalıştırmak ve oluşan ara sonuç değerlerini hesaplayarak saklamaktır. Ancak algoritmada kullanılan gizli anahtarın tümü için atak düzenlenmez. Çünkü bu durumda anahtar uzayı çok büyük olacağı için yapılacak atak, kaba kuvvet saldırılarına benzeyecek ve zaman-maliyet açısından verimli bir atak olmayacaktır. Örneğin 128 bitlik AES anahtarının 8 bitlik kısmı için atak düzenleniyor olabilir. Bu durumda k nın 2^8 yani 256 muhtemel değeri olacaktır.

K : muhtemel k değerlerinin toplam sayısı olmak üzere;

Muhtemel k değerleri bir **k' = (k_1, k_2, …, k_K)** vektörü olarak ifade edilir. DPA atakları bağlamında genellikle bu **k'** vektörü **key hypotheses** (anahtar hipotezleri-muhtemel anahtar değerleri) olarak adlandırılır. Verilmiş bir data vektörü **d** ve **k** anahtar hipotez vektörü için, D şifrelenecek açık metin sayısı olmak üzere saldırgan kolaylıkla tüm **D** şifreleme adımları ve tüm **K** anahtar hipotezleri için ara değerler olan **f(d,k)** yı hesaplayabilir. 1000 tane açık metin değeri ve anahtarın 8 bitlik kısmı ile atak yapılacaksa algoritma yazılım ortamında çalıştırılarak $1000*2^8=1000*256=256.000$ tane ara değer elde edilir. Bu hesaplama Şekil 3.3' te görülen D x K boyutunda ara sonuç değerlerinden oluşan bir V matrisi ile sonuçlanır.

d_1k_1 d_1k_2 …….. d_1k_K
d_2k_1 d_2k_2 …….. d_2k_K
.
.
d_Dk_1 d_Dk_2 ……d_Dk_K

Şekil 3.3. V matrisi

i = 1, …, D ve j = 1, …., K olmak üzere V matrisinin elemanları şu şekilde hesaplanır;

V matrisinin her $\mathbf{V_{i,j}}$ elemanı ; Algoritmanın i (muhtemel 1000 açık metinden biri) ve j (256 muhtemel anahtardan biri) değerlerini girdi olarak alması durumunda üreteceği arasonucu gösterir.

V matrisinin j.sütunu d_i. açık metin ve k_j. anahtar hipotezi ile hesaplanan ara sonucu içerir. Bu şekilde V matrisinin bir sütunu aynı anahtar değeri ile hesaplanan D tane şifreleme adımı boyunca hesaplanan ara değerleri içermiş olur. k' vektörü muhtemel tüm k değerlerini içerir. Bu nedenle aygıtta kullanılan değer (gerçek anahtarın 8 bitlik ilgili kısmı) k' vektörünün bir üyesidir. Bu üyenin (gerçek anahtarın) indexi ck olarak adlandırılsın. Şayet bu ck değeri bulunabilirse buradan k_{ck} aygıtın anahtarını gösterecektir ve DPA atağı hedefine ulaşmış olacaktır. İşte DPA ataklarının amacı: D tane şifreleme adımı boyunca V matrisinin hangi sütununun işlendiğini bulmaktır. DPA atakları ile kısa sürede atak yapılan aygıtta V matrisinin hangi sütununun işlendiği belirlenebilir. Böylelikle hızlı bir şekilde k_{ck} yani aygıtın gerçek anahtar değeride bilinmiş olur.

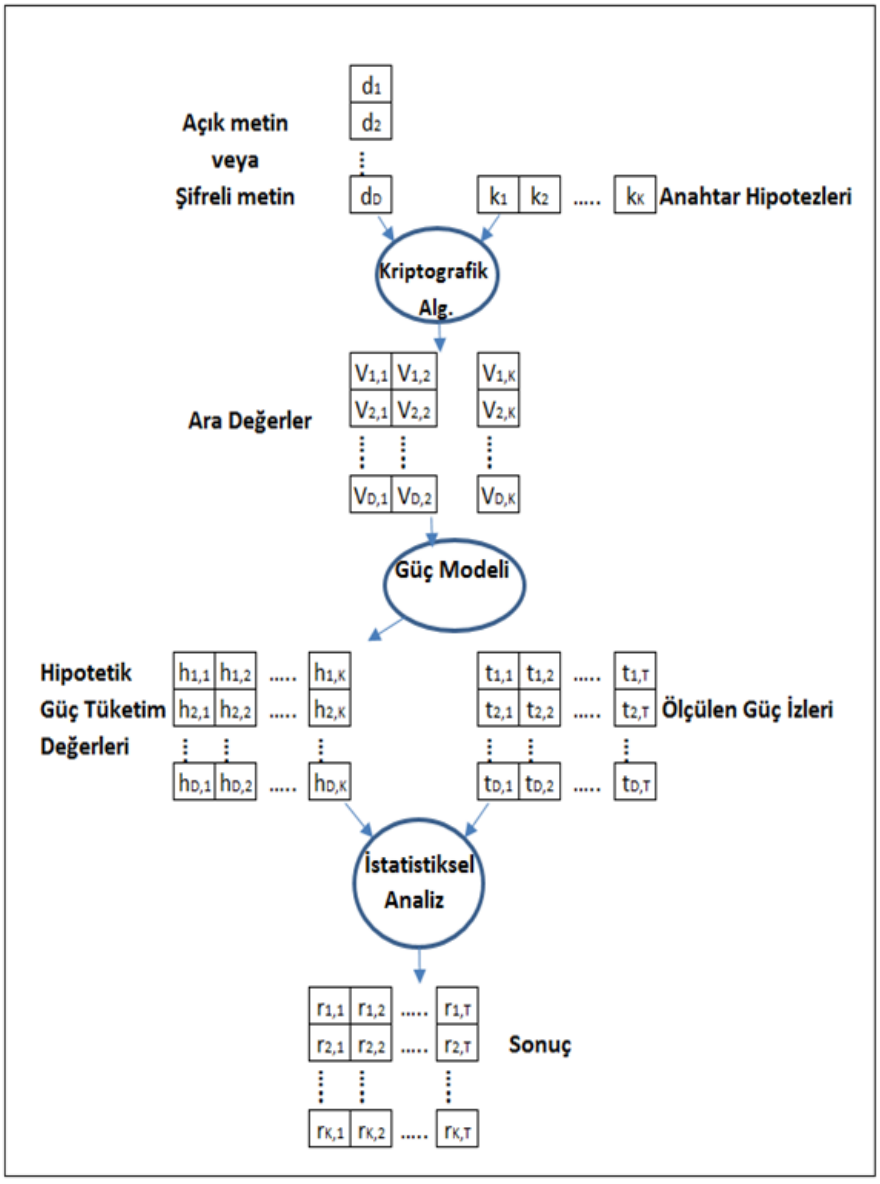
3.3.4. Ara Değerlerin Tüketeceği Güç Tüketim Değerlerini Belirlemek

Bir DPA atağının 4.adımı: Bölüm 3.3.3' de nasıl oluşturulduğu gösterilen V matrisindeki $V_{i,j}$ ara değerlerinin tüketeceği varsayımsal güç tüketim değerlerini bularak H matrisini oluşturmaktır. H matrisindeki $H_{i,j}$ hipotetik-varsayımsal güç tüketim değerleri Vi,j aradeğerlerinin tüketeceği güç değerinin modellenmesidir. V aradeğerler matrisini, H hipotez güç tüketim izleri matrisine haritalamak amacı ile saldırgan Bölüm 3.4' te değinilen güç modelleme tekniklerini kullanır. Bu tekniklerden birini kullanırken her ara değer $v_{i,j}$ için bir hipotez güç tüketim değeri $h_{i,j}$ elde etmek için aygıtın güç tüketimi simule edilir. Simulasyon kalitesi, saldırganın aygıt hakkındaki bilgisine güçlü bir şekilde bağlıdır. Saldırganın en iyi simülasyonu aygıtın gerçek güç tüketimi karakteristiğine en yakınıdır. V matrisini H matrisine haritalamak için kullanılan en yaygın güç modeli Hamming Weight güç simulasyon modelidir [35,36]. Data değerlerini güç tüketim değerlerine haritalamak için Bölüm 3.4' teki diğer modelleme yöntemleride kullanılabilir.

3.3.5. Hipotez Güç Tüketim Değerleri İle Gerçek Güç İzlerini Karşılaştırmak

V matrisi H matrisine haritalandıktan sonra DPA atağının son adımı icra edilir. Bu adımda hipotez güç tüketim değerlerinden oluşan H matrisinin her bir sütunu gerçek güç tüketim değerlerinden oluşan T matrisinin her bir sütunu ile istatistiksel analize tabi tutulur. Bu şu anlama gelir; saldırgan her hipotez anahtar değerinin hipotez güç tüketim değerleri ile aygıtın gerçek güç tüketimi esnasında kaydedilen güç izlerini karşılaştırır. Bu karşılaştırmanın sonucu R matrisidir. K muhtemel anahtar değerleri sayısı ve T ise ölçülen güç izleri sayısı olmak üzere R matrisi K x T uzunluğundadır. R matrisinin her $R_{i,j}$. üyesi; Bölüm 3.3.4' de oluşturulan H matrisinin h_i. Sütunu ile Bölüm 3.3.2' de oluşturulan T matrisinin t_j. sütunları arasındaki karşılaştırmanın sonucunu içerir. h_i ve t_j sütunları en iyi korelasyona sahip olduğunda r_{ij} değeri en yüksek korelasyon değerine sahiptir. R matrisindeki en yüksek değer; işlenen seçilmiş ara sonuç ve aygıt tarafından kullanılan gerçek anahtar pozisyonlarını açığa çıkarır. Buradan aygıtın anahtarı elde edilebilir.

Şuda önemli bir noktadır ki; bazı durumlarda R deki bütün değerler yaklaşık olarak aynı olabilir. Bu durumda genellikle saldırgan H ve T sütunları arasındaki ilişkiyi tahmin etmek için yeterince güç izlerini ölçmemiştir. Saldırganın ölçtüğü daha fazla iz, H ve T matrislerinin sütunları arasındaki daha fazla eleman anlamına gelir ve saldırgan H ve T nin sütunları arasındaki ilişkiyi daha kesin olarak saptayabilir. Buradan şu sonucada ulaşılır; sütunlar arasındaki en küçük ilişkileri tespit edebilmek için ölçülen güç izi sayısı fazla olmalıdır [13]. Şekil 3.4 DPA ataklarının adımlarını göstermektedir.



Şekil 3.4. DPA ataklarının adımları [2]

Hipotetik (varsayımsal olarak muhtemel tüm k anahtar değerleri ve random giriş verileri için hesaplanan) güç tüketim değerlerini içeren H matrisi ile gerçek güç tüketim değerlerinden oluşan T matrisi arasındaki ilişki 0 ve 1 arasında sonuç veren ***Correlation coefficient***-korelasyon katsayısı hesaplanarak bulunmaya çalışılır. Korelasyon katsayısı datalar arasındaki liner ilişkileri belirlemek için en yaygın yoldur. Bu nedenle bu yöntem DPA atakları icra etmek için mükemmel bir seçimdir.

DPA analizinin son adımı olan ***Hipotez Güç Tüketim Değerleri İle Gerçek Güç İzlerini Karşılaştırma*** işleminde i=1,…,K ve j=1,….,T olmak üzere h_i ve t_j sütunları arasındaki liner ilişkileri tanımlamak için korelasyon katsayısı formül 3.1 ile bulunabilir;

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i) \cdot (t_{d,j} - \bar{t}_j)}{\sqrt{\sum_{d=1}^{D}(h_{d,i} - \bar{h}_i)^2 \cdot \sum_{d=1}^{D}(t_{d,j} - \bar{t}_j)^2}} \quad (3.1)$$

Her $r_{i,j}$ değeri h_i ve t_j sütunlarının D elemanı üzerine hesaplanır. $\bar{h}_i$ and $\bar{t}_j$ h_i ve t_j sütunlarının ortalamasını ifade eder. Her zaman için r değeri -1 ile +1 arasında bir değere sahiptir. Değerin +1 olması durumu karşılaştırılan iki değerin en yüksek korelasyona sahip olduğu anlamına gelmektedir. Değerin -1 durumu ise iki değer arasındaki en uzak korelasyon değerini gösterir.

3.4. Yan Kanal Atakları İçin Güç Modelleri

Gömülü sistemlerin güç tüketim değerleri işledikleri datalar ile doğrudan veya dolaylı olarak ilişkilidir [37]. Diferansiyel Güç Analizi atakları gerçekleştirilirken öncelikle aygıt birçok şifreleme işlemi yaparken birçok güç izi ölçümü yapılarak kaydedilir. Diğer taraftan hipotez anahtar değerleri (anahtar havuzundaki muhtemel anahtarlar) ve çok sayıda açık metin/şifreli metin değerleri için algoritma çalıştırılarak ara sonuçlar elde edilir. Bu ara sonuçların üreteceği güç tüketim değerleri ile gerçek güç tüketim değerleri karşılaştırılarak aygıtın anahtarı ortaya çıkarılabilir. Ancak bu ara sonuç değerlerinin gerçekleştirilmesi durumunda hangi güç tüketim değerlerine karşılık geleceği bilinmek/tahmin edilmek durumundadır. İşte güç modelleri işlenen herhangi bir datanın hangi güç tüketim değerlerini oluşturacağının hesaplanmasını sağlar. En yoğun şekilde kullanılan güç modelleri **HW (**Hamming Weight) ve **HD (**Hamming Distance) güç modelleridir [38].

3.4.1. Hamming Weight Güç Modeli

En temel güç modeli HW güç modelidir. Bu güç modelinde saldırganın aygıtın netlisti hakkında bilgi sahibi olması gerekmez. Elektronik tasarımda "netlist" bir elektronik devrenin bağlantılarının tanımlanmasıdır. Netlist tasarımdaki tüm fiziksel bağlantıları tanımlar [39]. Hamming weight güç modelinde saldırgan; güç tüketim değerinin işlenen datadaki "1" bit değerleri ile orantılı olduğunu varsayar [30].

HW çoğunlukla bir data bus veya address bus kullanarak bir devrenin güç tüketimine yaklaşmak için kullanılabilir. HW şu temel öncüle dayanır; bir bus; bus içerisinde anahtarlanan bitlerin sayısına orantılı olacak miktarda güç tüketir. Şayet bitler anahtarlanmıyorsa bus bütün bitlerin '0' a anahtarlanmasına göre çok düşük güç tüketir [38]. Şekil 3.5' te 2 baytlık data için HW modeli gösterilmektedir.

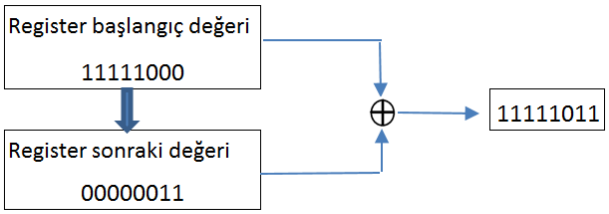
Şekil 3.5. Hamming weight güç modelinin gösterimi

Sadece işlenen data hakkında bilgi varsa bile Hamming weight güç modeli aygıtın güç tüketim değerlerinin yaklaşık olarak tahmin edilebilmesine yardımcı olacaktır. Bu model; üzerinde atak icra edilecek aygıt hakkında çok az bilgi sahibi olunan durumlarda kullanılır. Hamming Distance modeline göre bir avantajıda şifreleme işlemleri süresince bustaki data değişimleri hakkında herhangi bir bilgi gerektirmemesidir. Fakat HW modeli HD ile karşılaştırıldığı zaman HD modeli aygıtın güç tüketimini daha iyi modeller. Bu nedenlerle saldırgan aygıt hakkında fazla bilgi sahibi değilse HW modeli, güç tüketim değerlerini hesaplamak için gayet uygun bir modeldir [38].

3.4.2. Hamming Distance Güç Modeli

Hamming Distance modeli Hamming weight modelinin genişletilmiş bir modelidir denilebilir. Hamming Distance modeli güç tüketimini tanımlamak için belli bir zaman aralığında lojik değerlerdeki değişimleri kullanır. Değişim; bir data bus, adres bus, register, memory gibi bir çok farklı bileşende meydana gelebilir. Bu modeli kullanarak bir devrenin güç tüketimi devrede yapılan 0→1 ve 1→0 geçişlerine orantılı olarak modellenebilir. Bit geçişlerinin sayısı basit bir şekilde iki değerin ayrıcalıklı veya (exor) değerinin hamming ağırlığıdır. Örneğin R1 ve R2 register değerleri için; $HD(R1,R2) = HW(R1 \oplus R2)$ olarak hesaplanabilir.

Bu güç modeli kullanıldığı zaman birkaç basit varsayım yapılır. 0→0 ve 1→1 geçişlerinin güç tüketimine katkıda bulunmadığı farzedilir. Ayrıca 0→1 ve 1→0 geçişlerinin aynı miktarda güç tüketeceği varsayılır. Çoğu devrede bu durum olmayabilir. Şayet aygıtın spesifik güç tüketimi hakkında biraz bilgi varsa geçişler farklı şekilde ağırlıklandırılarak modelde küçük geliştirmeler yapılabilir. Şekil 3.6' da bir registerin bir clock edge de değerini nasıl güncellediği görülmektedir.



Şekil 3.6. Hamming distance modelinin örnek bir gösterimi

Register bir durumdan diğerine güncellenirken belirli miktarda güç tüketir. Şekil 3.6' da görülen registerin 5 tane değeri 1→0 şeklinde 2 tane değeri 0→1 şeklinde güncellenmiştir. Hamming distance register güncellemesi 7 ye orantılı olduğu zamanki güç tüketimini gösterir. Zayıflıklar yani güç modeli oluşturulurken ihmal edilen durumlar dikkate alınmazsa Hamming distance modeli belli bir zaman süresi boyunca bir devrenin beklenen güç tüketimi değerini hesaplama konusunda çok uygun bir metoddur. Datalarda bir değişiklik gözlemlenebildiği durumlarda Hamming weight modeli yerine hamming distance modeli kullanılması daha uygun olacaktır [30].

3.4.3. Diğer Güç Modelleri

HW ve HD modelleri bir kriptografik aygıtın bir bölümünün güç tüketimini simüle etmek için saldırganlar tarafından kullanılan en yaygın güç modelleridir. Bu iki güç modeli çok basit ve genel oldukları için çok yaygın bir şekilde kullanılmaktadırlar. Diğer güç modelleri genellikle belirli bir aygıt türü için kullanırlar. Böyle özel aygıtlar için genişletilmiş HD güç modeli kullanılabilir.

HD güç modeli datanın tüm bitlerinin güç tüketimine eşit bir şekilde katkıda bulunduğunu varsayar. Şayet saldırgan bir devrenin bazı hücrelerinin diğerlerinden daha fazla güç tüketimini etkilediğini biliyorsa elbette bu durum işlenen data değerinin farklı bitleri için farklı ağırlıklar tanıtılarak göz önünde bulundurulur. HD modeli farklı yaklaşımlarla farklı şekillerdede uygulanabilir. Örnek olarak 0→1 geçişi ile 1→0 geçişleri aynı ağırlıkta değilde biri diğerinin iki katı güç tüketiyor ise güç modeli buna uygun şekilde oluşturulabilir [40].

3.5. Yan Kanal Ataklarına Karşı Önlemler

Temel amacı kriptografik aygıtın güç tüketimini şifreleme algoritmasının içyapısından bağımsız hale getirmek olan yan kanal ataklarını engellemek için geliştirilen önlemlerin çoğu patent altındadır. Karşı önlemler genelde iki sınıf altında incelenmektedir. Bunlar Gizleme ve Maskeleme yöntemleridir [2,41]. **Gizleme** yönteminde; kriptografik aygıtın güç tüketimi random hale getirilir veya aygıtın güç tüketimi algoritmanın her clock saykılında eşit olacak şekilde tasarlanarak aygıtın güç tüketim değeri saldırganlardan gizlenmeye çalışılır. **Maskeleme** yönteminde ise aygıtın güç tüketim karakteristikleri yerine algoritmada işlenen iç değerler maskelenmeye çalışılır. Saldırgan güç tüketim izleri üzerinden korelasyon ile bazı bilgilere ulaşıp anahtar değerini elde etse dahi elde ettiği değerler maskelenmiş değerlerdir. Son zamanlarda ortaya konan bir diğer karşı önlemde bazı açılardan maskeleme yöntemine benzeyen Ruben Lumbiarres ve arkadaşlarının çalışmasıdır [42]. Bu yöntemde klasik yaklaşımlardaki "işlenen data ile güç tüketimi arasındaki korelasyonu engelleme" yaklaşımı yerine şifreleme donanım/yazılımına ek olarak ikinci bir dizayn şifrelemeye eşlik ederek yan kanal sızıntısında yanlış anahtar açığa vurulması hedeflenmektedir. Ancak bu tür yöntemlerde maliyet ve/veya performans açısından dezavantajlar ortaya çıkmaktadır.

4. KRİPTOLOJİDE KAOS

Kaotik sistemler bilim ve mühendislik çalışmalarında özel bir yere sahiptir [43]. Çünkü birçok araştırmacının amacı gerçek dünya olaylarını anlayabilmek ve bu olayları kontrol edebilmek için matematiksel modellerini elde edebilmektir. Kaotik sistemlerde bu gerçek dünya olgularındaki rasgele benzeri süreçlerin aslında bir matematiği olduğunu açıklamaya çalışmaktadır. En genel ifade ile kaos gerekirci bir sistemin rasgeleliği olarak tanımlanmaktadır [43-45].

Kaotik davranışlar, doğrusal olmayan sistemlerde gözlenen dinamiklerdir. Tabiattaki veya insan yapımı birçok sistem, doğrusal olmayan yapıdadır. Dolayısıyla, kaotik davranışlar ve sistemlerle karşılaşma olasılığı çok yüksektir. Son yıllarda, kaos teorisi ve doğrusal olmayan sistemlerde gözlenen ve tuhaf çekiciler olarak adlandırılan kaotik dinamikler, araştırmacılar tarafından yoğun bir şekilde çalışılmaya başlanmıştır. Kaos kabaca; başlangıç şartlarına hassas bağlı davranış gösteren doğrusal olmayan deterministik bir sistemde, düzensiz davranışlar olarak tanımlanabilir. Deterministik sistemler; sistem davranışlarının, sistem parametreleri ve başlangıç şartları tarafından belirlendiği sistemlerdir. Kaotik sistemin deterministik olması, gürültü ile kaos arasındaki en önemli farklılıktır.

Bir sistemde, garip çekiciler olarak tanımlanan karmaşık dinamiklerin gözlenebilmesi için gerekli koşullar şunlardır:

- Sistemin doğrusal olmayan eleman bulundurması gerekir.
- Başlangıç şartına hassas bağlılık gereklidir.

Bu koşullar bir sistemde kaos varlığı için gerekli koşullardır. Ancak yeterli değildir. Eğer sistem sürekli zamanlı bir sistem ise sistem derecesinin en az üç olması gerekir. Çünkü sistem derecesi üçten küçük olan doğrusal olmayan sistemlerde kaos gözlenmez. Ayrık zamanlı sistemler için böyle bir koşula gerek yoktur. Birinci dereceden bir sistemde bile kaos gözlemlenebilir. Bu yüzden kaosun birçok pratik uygulamasında ayrık zamanlı kaotik sistemler tercih edilmiştir. Bu tip bir tercihin en önemli nedeni ayrık zamanlı kaotik sistemlerin sürekli zamanlı sistemlere göre daha basit bir yapıya sahip olmasıdır. Buna karşın, gerek mevcut kaotik sistemlerin kesir dereceli modellerinde ve gerek yeni tanımlanan kesir dereceli sistemlerde, sistem derecesi üçten küçük olmasına rağmen sistemde kaotik davranışlar gözlenmiştir [43-45].

4.1. Kaos ve s-box

Kaos ve kriptoloji bilimleri arasında benzerlikler kullanılarak birçok uygulama alanında yeni tasarımlar gerçekleştirilmiştir [46, 47]. Bu tasarımların en yaygın örneklerinden biri kriptolojik s-box yapıları olmuştur. Bir kriptolojik birleşen olan s-box yapıları birçok şifreleme algoritmasında

doğrusal olmama özelliğini sağlayan tek bileşen olduğu için popüler bir konudur. Bu yüzden literatürde neredeyse tüm kaotik sistem sınıfları için kaos tabanlı s-box tasarımları önerilmiştir.

Kaotik davranış az rastlanan bir olgu değildir. Matematikten biyolojiye, ekonomiden elektronik devrelere, mühendislikten sosyal bilimlere, insan vücudunun davranışından vahşi nüfusun dağılımına kadar çok geniş bir alanda bu davranışa rastlanmaktadır. Kaotik sistemlerin bilgisayar bilimlerindeki en yaygın kullanım alanlarından biri ise kaotik sistemlerin sahip olduğu dinamikleri kullanarak çeşitli kriptolojik protokollerin tasarlanmasıdır [46, 47]. Bu ilişkinin en başarılı örneklerinden biri kaos tabanlı s-box yapıları olmuştur.

S-box yapılarının tasarımı için literatürde birçok yöntem önerilmiştir. Bu yöntemler üç ana kategoride toplanmaktadır: cebirsel tabanlı yöntemler, sözde rasgele tabanlı yöntemler ve sezgisel yöntemler. Modern blok şifreleme algoritmalarında genellikle güçlü cebirsel ilişkilere dayanan s-box tasarım teknikleri kullanılmaktadır. Bunlardan en yaygın şekilde bilinenleri Nyberg tarafından önerilmiş olan sonlu cisimde ters alma yöntemidir. Bu yöntem gelişkin şifreleme algoritması olarak bilinen AES [48, 49] (Advanced Encryption Standard) blok şifreleme algoritmasının s-box tasarımında da kullanılmıştır. Ancak, hem yan kanal analizleri gibi uygulamaya yönelik saldırılar hem de cebirsel saldırılarının ortaya koyulması ile mevcut s-box tasarım tekniklerine alternatif olabilecek yeni yöntemler araştırılmaya başlanmıştır [50-52]. Kaotik sistemlerin temel alındığı yeni tasarım teknikleri de bu amaca yönelik çalışmalar arasındadır.

Kaos tabanlı s-box tasarım çalışmaları ilk olarak 2000'li yılların başlangıçlarında görülmeye başlanmıştır [53]. Bu tasarımlarda daha basit matematiksel modellere sahip olan ayrık zamanlı kaotik haritalar kullanılarak s-box yapıları üretilmiştir. Bu grup tasarımlarda genel yaklaşım farklı kaotik haritalar kullanarak s-box performans kriterlerinin iyileştirilmesi hedeflenmiştir [54-84]. İkinci grup çalışmalar 2010 yılında ortaya çıkmıştır [85]. Bu grup çalışmaların tasarım mantığındaki ortak nokta kaotik sistem karmaşıklığını artırarak s-box performans ölçütlerini iyileştirmektir. Dolayısıyla bu grup tasarımlarda daha karmaşık matematiksel modele sahip sürekli zamanlı kaotik sistemler kullanılmıştır [86-95]. Üçüncü grup kaos tabanlı s-box tasarımlarında ise kaotik sistemin karmaşıklığını daha fazla artırabilmek için hiper kaotik veya zaman gecikmeli kaotik sistemler kullanılmıştır [96-117]. Ancak son yapılan bir çalışmada kaos tabanlı s-box yapılarının performansının kaotik sistemden bağımsız olduğunu göstermiştir. Yine aynı çalışmada kaos tabanlı s-box tasarımları için ulaşılabilecek en iyi performans ölçütlerinin doğrusal olmama için 106.75 olduğunu göstermiştir [118].

5. AES ALGORİTMASI

AES şifreleme algoritması 128, 192, 256 bit şifreleme anahtarı kullanarak şifreleme yapabilen bir simetrik şifreleme algoritmasıdır. 128, 192, 256 bit anahtar boyutlarına bağlı olarak şifreleme işlemleri sırasıyla 10, 12, 14 turda gerçekleştirilir. AES şifreleme algoritmasında tüm açık metin öncelikle 2' lik sistemde ifade edilir ardından açık metin verileri 128 bitlik bloklar halinde şifreleme işlemine tabi tutulur. Şifrelenecek 128 bit açık metin verileri 4x4 boyutunda 16 elemandan oluşan bir durum matrisine alınır. Bu matris elemanlarının herbiri 1 byte yani 8 bitlik bir açıkmetin verisidir. Bu bir byte lık veriler 16 lık sistemde ifade edilirler. İkilik sistemdeki değeri onaltılık sistemde göstermek için bir bayt iki adet dörtlüye bölünür ve her iki dört bitlik değer karşılık gelen onaltılık değer ile gösterilir. Örneğin ikilik sistemdeki 10110011 değeri 1011 ve 0011 olmak üzere iki dörtlük olarak değerlendirilir ve 1011 değerine karşılık 16 lık sistemdeki karşılığı olan **B**, 0011 değerine karşılık 16 lık sistemdeki karşılığı olan **3** değeri şifreleme işlemlerinde kullanılacaktır, yani bu 1 byte lık verinin durum matrisindeki değeri **B3** olacaktır.

"**3243F6A8885A308D313198A2E0370734"** şeklinde olan 16 byte yani 128 bitlik bir açık metin verisi Şekil 5.1' de görüldüğü gibi durum matrisinde yerini alır.

Durum Matrisi			
32	88	31	E0
43	5A	31	37
F6	30	98	07
A8	8D	A2	34

Şekil 5.1. AES durum matrisi

128 bit AES algoritması açık metine bir takım işlemlerin uygulanacağı 10 adımdan oluşur. Ancak öncelikle bu 10 adımda kullanılmak üzere 10 tane alt anahtarın oluşturulması gerekmektedir.

5.1. AES Alt Anahtarlarının Üretilmesi

AES algoritması her adım için bir tane olmak üzere 10 adet farklı şifreleme anahtarı kullanır. Bu anahtarların hepsi başlangıçta seçilen şifreleme anahtarından oluşturulurlar.

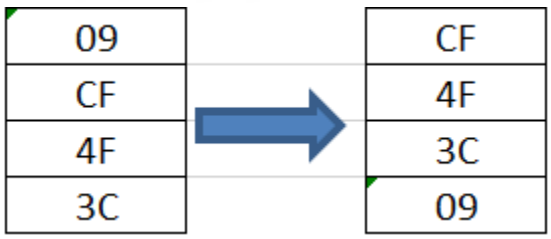
Şifreleme anahtarı "**2B7E151628AED2A6ABF7158809CF4F3C"** olsun. Bu ana anahtar Şekil 5.2' de görüldüğü gibi anahtar matrisinde yerini alır. Bu başlangıç anahtarından AES' in 10 adımında kullanmak üzere 10 adet adım anahtarı oluşturulacaktır.

Anahtar Matrisi			
2B	28	AB	09
7E	AE	F7	CF
15	D2	15	4F
16	A6	88	3C

Şekil 5.2. Ana anahtar matrisi

Bu başlangıç ana anahtarından 10 tane Adım anahtarı şu şekilde elde edilir; Herbir adım anahtarının 1. sütunu bir önceki anahtarın (1.adım anahtarı için ana anahtarın) son yani 4. sütununun bazı işlemlerden geçirilmesiyle oluşturulur. Adım anahtarının diğer sütunları ise (2.,3.,4. sütunlar) bir önceki anahtarın aynı sütunu ile oluşturulmakta olan bu anahtarın bir önceki sütununun XOR işlemine tabi tutulması ile oluşturulur.

Adım anahtarlarının ilk sütunları oluşturulurken yapılacak işlemler **rotword**, **subbyte**, **rcon(adım sabiti)** işlemleridir. **Rotword** işleminde bir önceki adım anahtarının son sütunu (1.adım anahtarı oluşturuluyorsa ana anahtarın son sütunu) aşağıdan yukarıya olmak üzere bir adet dairesel olarak kaydırılır. Rotword Şekil 5.2.' de görülen ana anahtarın 4. Sütunu için yapılıyorsa sütunun son hali Şekil 5.3' te görüldüğü gibi olacaktır.



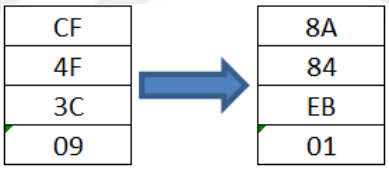
Şekil 5.3. Rotword işlemi

Subbyte işleminde ise Şekil 5.3' te Rotword işlemi sonucunda elde edilen sütundaki herbir veri Tablo 5.1' de görülen görülen s-box' tan geçirilerek s-box çıkışında alınan değer bu verinin yerine yazılır.

Tablo 5.1. AES s-box tablosu

	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	1	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	4	C7	23	C3	18	96	5	9A	7	12	80	E2	EB	27	B2	75
4	9	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	0	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	2	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	6	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	8
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	3	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Şekil 5.3’ te görülen CF verisi yerini s-box tablosunda C ile F’ nin kesiştiği hücrede bulunan 8A değerine bırakır. Aynı şekilde 4F verisi yerini 84 değerine, 3C verisi yerini EB değerine, 09 verisi yerini 01 değerine bırakır. Oluşan yeni sütun Şekil 5.4’ te görülmektedir.



Şekil 5.4. S-box değişiminden sonra

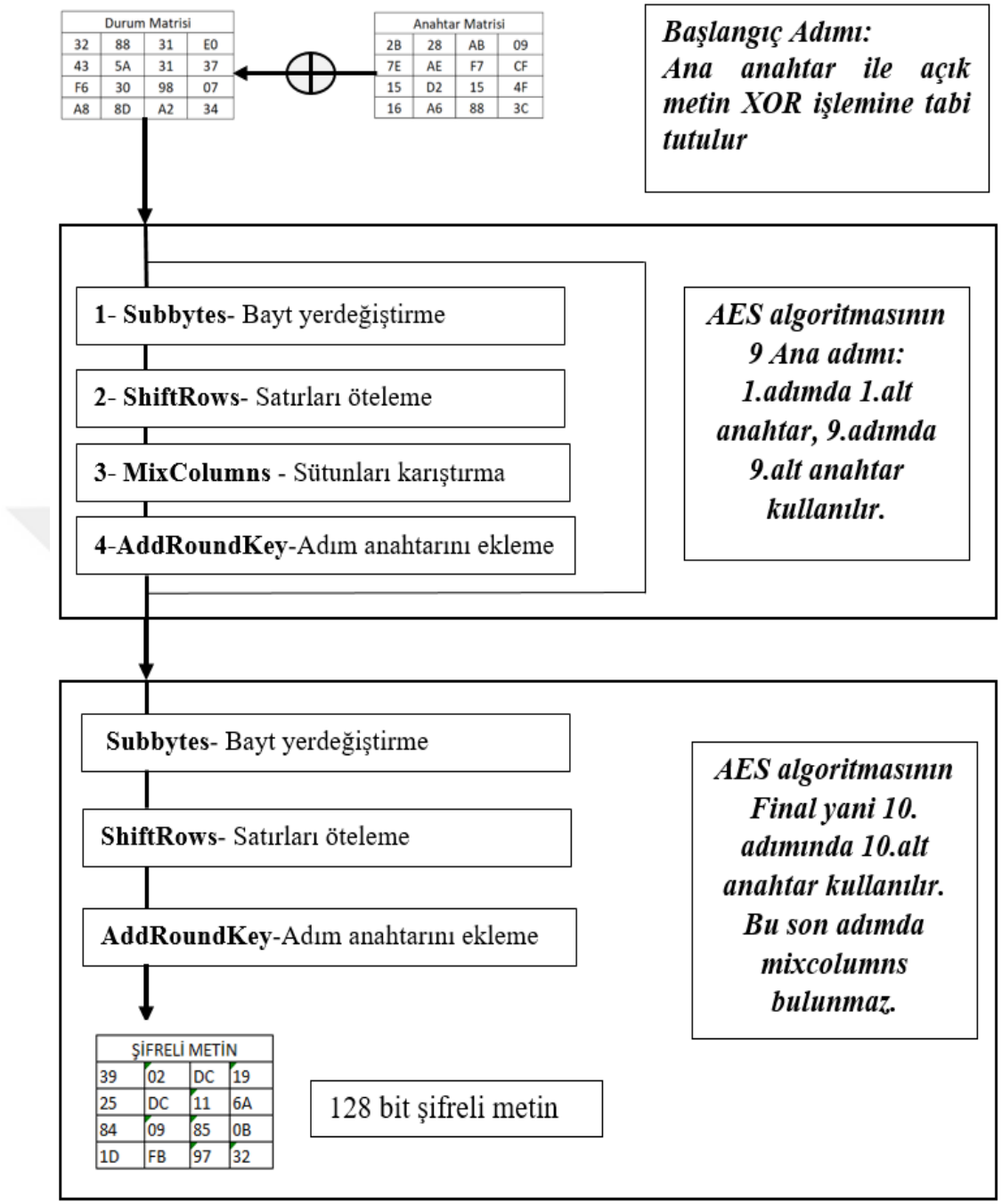
Rcon işleminde ise oluşturulacak olan adım anahtarından önceki anahtarın ilk sütunu, Subbyte işleminden elde edilen sütun ve adım sabiti XOR işlemine tabi tutulur. Oluşan değer oluşturulmakta olan adım anahtarının ilk sütununu oluşturur. Her bir adım için kullanılacak olan adım sabitleri Tablo 5.2’ de görülmektedir.

Tablo 5.2. Rcon tablosu

Adım No	Adım Sabiti
1	01 00 00 00
2	02 00 00 00
3	04 00 00 00
4	08 00 00 00
5	10 00 00 00
6	20 00 00 00
7	40 00 00 00
8	80 00 00 00
9	1B 00 00 00
10	36 00 00 00

5.2. AES Algoritma Akışı

AES algoritmasının genel akış şeması Şekil 5.5' te görüldüğü şekildedir. Başlangıç aşamasında durum matrisine yerleştirilmiş olan açık metin ile şifreleme anahtarı xor işlemine tabi tutulur. Bu işlemin sonucu AES algoritmasının 10 adımı için giriş değeri olacaktır. AES algoritmasının ilk 9 adımında sırası ile **subbytes**, **shiftrows**, **mixcolumns**, **addroundkey** işlemleri yerine getirilir. Bu 9 adımın herbirinin çıkışı bir sonraki adımın girişi olacak şekilde döngü 9 defa tekrar eder. 9. adımın çıkışını alan 10. adımda ise diğer adımlardan farklı olarak **mixcolumns** işlemi yer almaz. Bu 10 adımın herbirinde Bölüm 5.1' de oluşturulan alt anahtarlar kullanılır [119].



Şekil 5.5. AES genel akış şeması

Subbytes (byte yer değiştirme) işleminde durum matrisindeki herbir değer Tablo 1' deki s-box' tan geçirilir. Durum matrisi bu yeni verilerle güncellenir.

Shiftrows (satırları öteleme) işleminde Durum matrisinin 2.satırı 1 defa, 3.satırı 2 defa, 4. Satırı ise 3 defa soldan sağa doğru ötelenir. 1. Satır için öteleme işlemi uygulanmaz.

Mixcolumns (sütunları karıştırma) işleminde durum matrisinde herbiri 1x4 boyutunda olan sütunlar ile Şekil 5.6' da görülen 4x4 lük sabit matris değeri ile çarpılarak elde edilen sonuçlarla durum matrisi güncellenir.

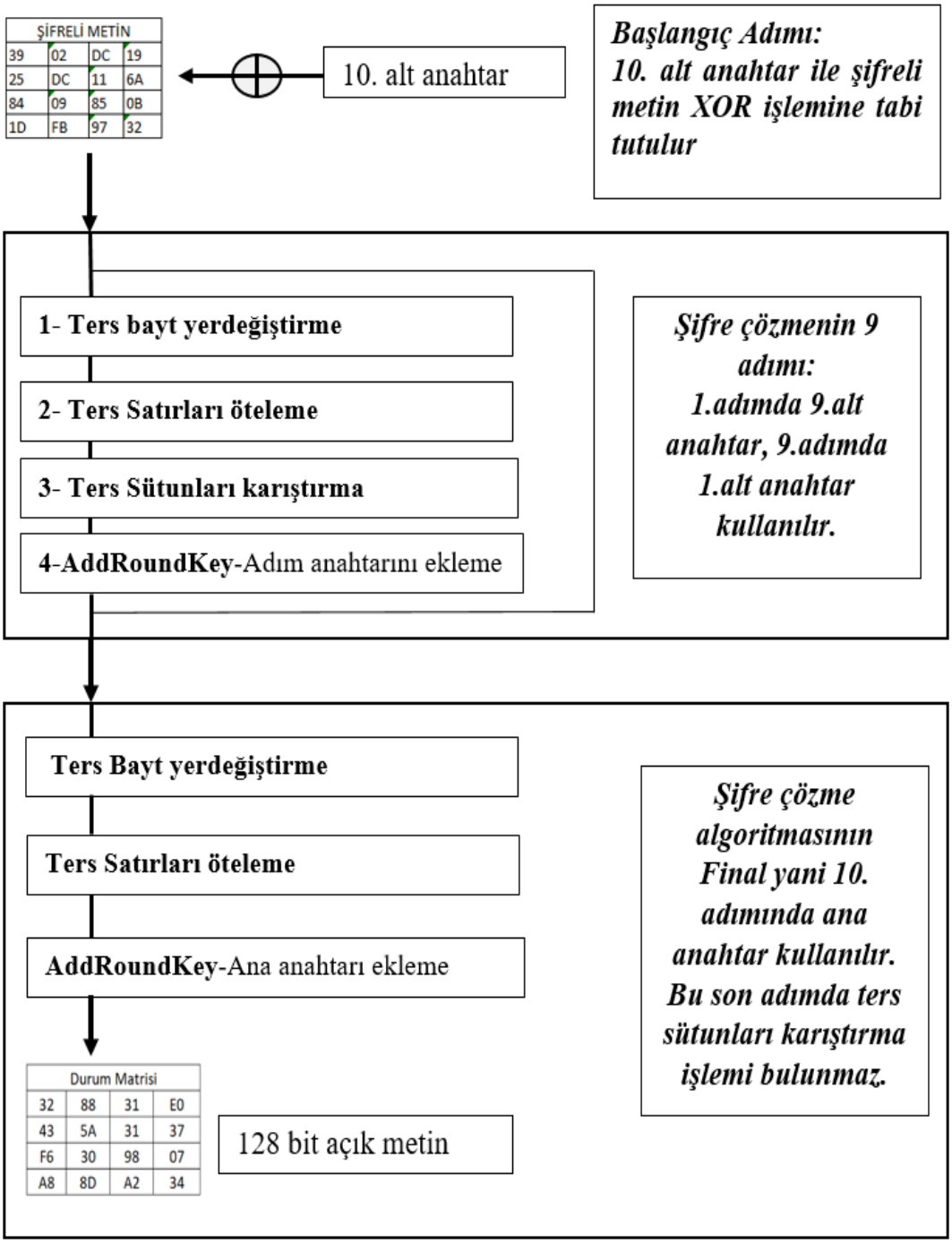
02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Şekil 5.6. Sütun karıştırma çarpım matrisi

Addroundkey(adım anahtarı ekleme) işleminde ise durum matrisi ile ilgili adıma ait olan anahtar xor işlemine tabi tutulur [120,121].

5.3. AES Şifre Çözme

AES şifre çözme işlemi şifreleme işlemine benzer 10 adımdan oluşmaktadır. Şifreleme işleminden farklı olarak adım anahtarları ters sırada kullanılır. Yani şifre çözme algoritması başlamadan önce şifreli metin 10. Alt anahtar ile xor işlemine tabi tutulur. Ardından 9 adımdan oluşan şifre çözme işlemleri yerine getirilir. Bu adımlarda şifreleme işlemindekine benzer işlemler yerine getirilir. Şifreleme işleminden farklı olarak byte yerdeğiştirme adımına karşılık ters byte yerdeğiştirme, satır kaydırma işlemine karşılık ters satır kaydırma, sütun karıştırma işlemi yerine ters sütun karıştırma işlemleri uygulanır. 9 adımlık şifre çözme döngüsünde 1. adımda 9. alt anahtar, 9. adımda 1. alt anahtar kullanılır. Final adımında ise addroundkey kısmında xor işlemi için şifrelemenin ana anahtarı kullanılır. Şifre çözme algoritmasının genel akış şeması Şekil 5.7' de görüldüğü şekildedir.



Şekil 5.7. AES şifre çözme algoritması akış şeması

Ters byte yerdeğiştirme işleminde Tablo 5.3' te görülen Ters s-box tablosu kullanılır.

Tablo 5.3. Ters s-box tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
3	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
6	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
7	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
A	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
B	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
C	1f	dd	a8	33	88	7	c7	31	b1	12	10	59	27	80	ec	5f
D	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
E	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
F	17	2b	4	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

Ters satır kaydırma işleminde satır kaydırma işleminde yapılan işlemler sağa kaydırılarak yapılır. Ters sütun kaydırma işleminde şifrelemedekinin aksine Şekil 5.8’ de görülen ters sütun karıştırma çarpım matrisi kullanılır.

0x0e	0x0b	0x0d	0x09
0x09	0x0e	0x0b	0x0d
0x0d	0x09	0x0e	0x0b
0x0b	0x0d	0x09	0x0e

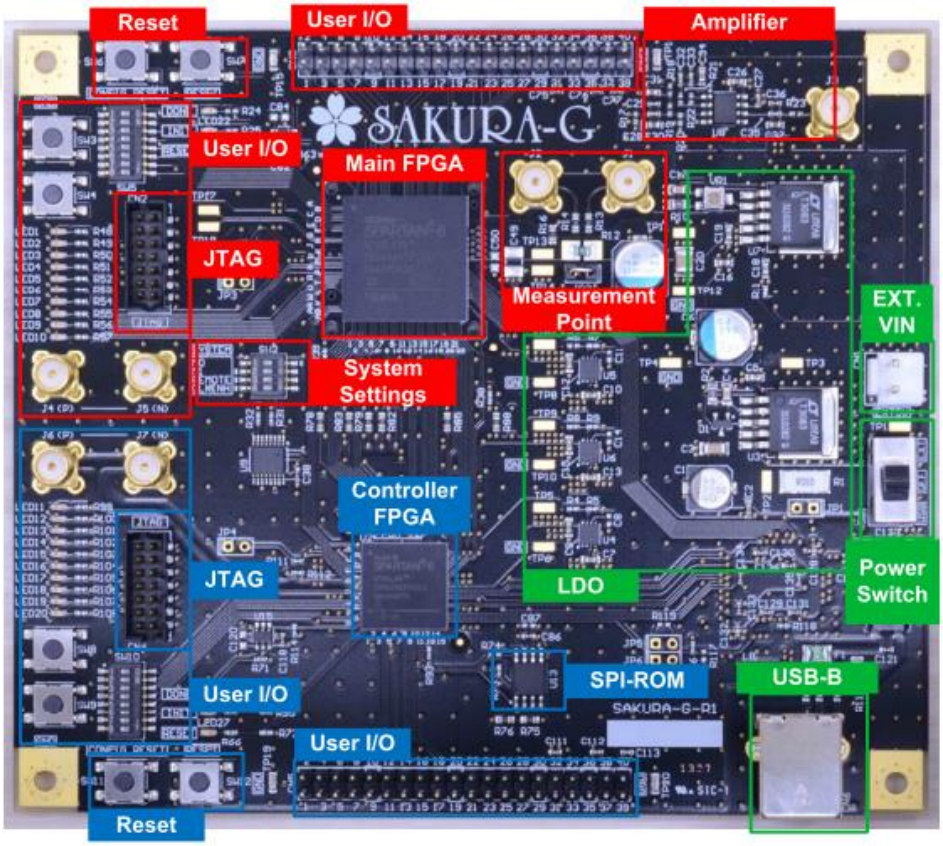
Şekil 5.8. Ters sütun karıştırma çarpım matrisi

6. MATERYAL VE METOT

Gömülü sistemler üzerinde yan kanal analizi yapabilmek için gömülü sistemin güç tüketimi bir osiloskop vasıtası ile ölçülerek elde edilen izler kaydedilir. Bu izler daha sonra bilgisayar programları aracılığıyla istatistiksel yöntemlerle değerlendirmelere tabi tutularak kriptografik aygıtın gizli anahtarı elde edilmeye çalışılır. Ancak bu deney ekipmanının uygun bir şekilde kurulması ve tam doğru bir şekilde çalışması yeterince uzmanlık bilgisi gerektirmektedir. Son zamanlarda geliştirilen 3.parti yan kanal analiz cihazları sayesinde gömülü sistemlere yapılacak yan kanal analiz saldırıları daha pratik bir şekilde ve daha düşük maliyetlerle yapılabilmektedir.

6.1. Sakura-G

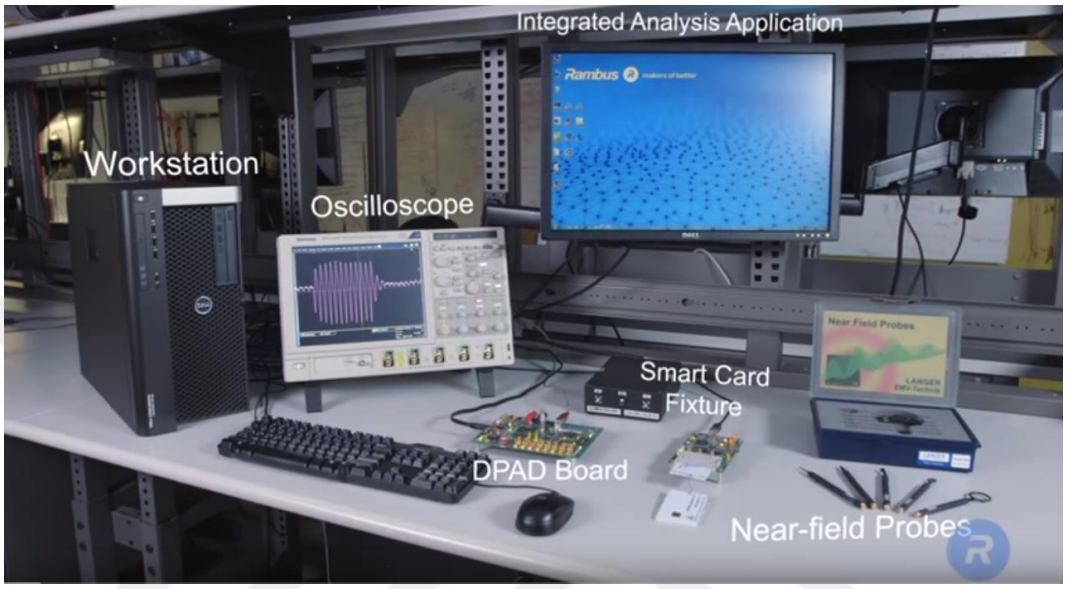
Şekil 6.1'de görülen Sakura-G cihazı TROCHE Co.Ltd. firması tarafından geliştirilmiş olup yaklaşık 1440$ fiyatıyla satışa sunulmaktadır. Üzerinde bulunan Xilinx® Spartan™-6 FPGA üzerinde şifreleme işlemleri yapılabileceği gibi yine devre üzerindeki Spartan-6 (XC6SLX9) FPGA kontrol ünitesi ile şifreleme algoritmasının yan kanal analizi gerçekleştirilebilmektedir [122].



Şekil 6.1. Sakura-G yan kanal analiz cihazı [122]

6.2. DPA Workstation Analysis Platform

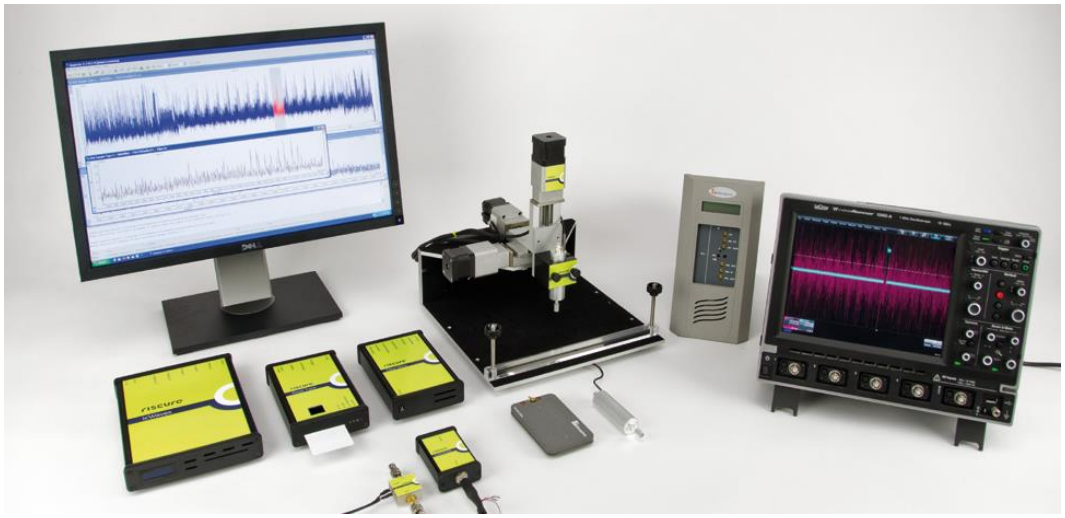
Şekil 6.2’ de görülen diferansiyel güç analizi iş istasyonu DPA nın mucidi sayılan Paul Kocher tarafından kurulan Rambus firmasına aittir. Bu iş istasyonu çok kapsamlı bir şekilde gömülü sistemlere DPA atakları gerçekleştirebilmektedir [123].



Şekil 6.2. DPA workstation analysis platform [123]

6.3. Inspector Side Channel Analysis

Şekil 6.3’ de görülen ve Riscure firmasına ait olan yan kanal analiz cihazı Bölüm 6.2’ de görülen DPA Workstation Analysis Platformu gibi çok detaylı yan kanal analizleri yapılabilecek sistemlerden biridir [124].

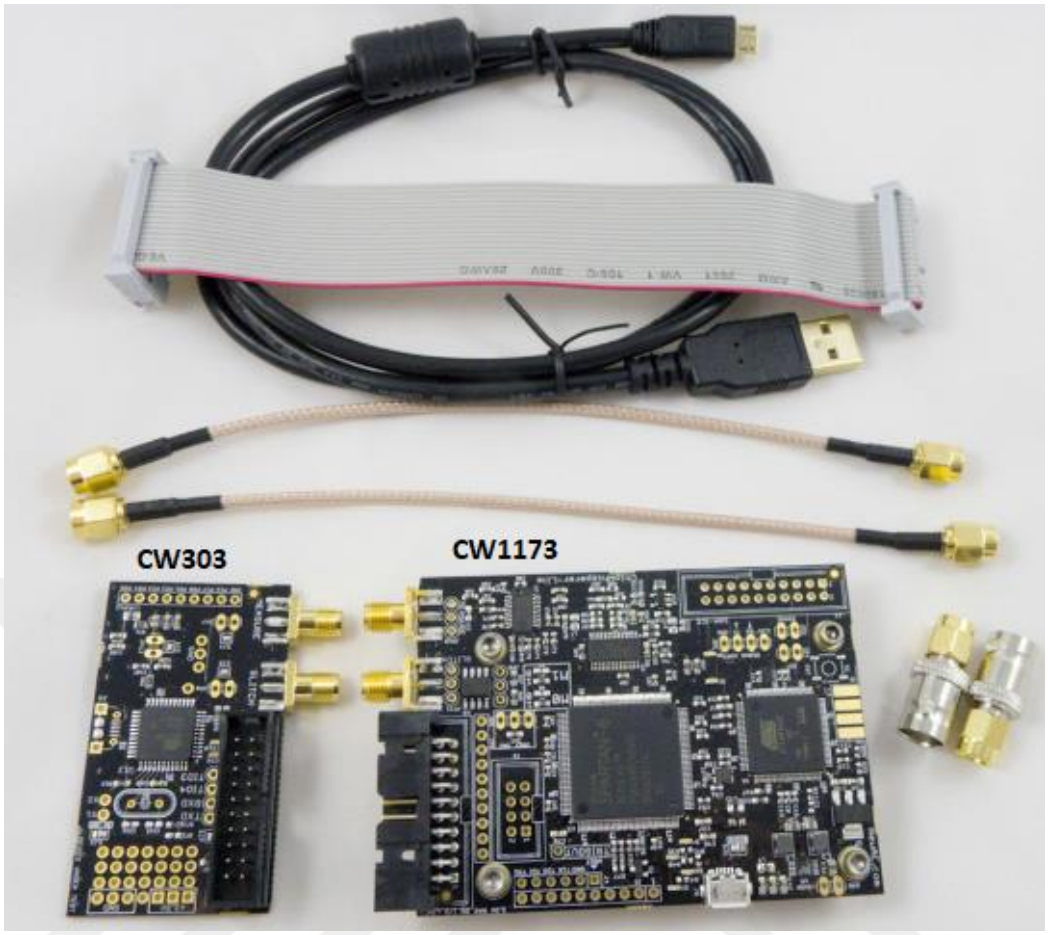


Şekil 6.3. Inspector yan kanal analiz cihazı [124]

6.4. Chipwhisperer

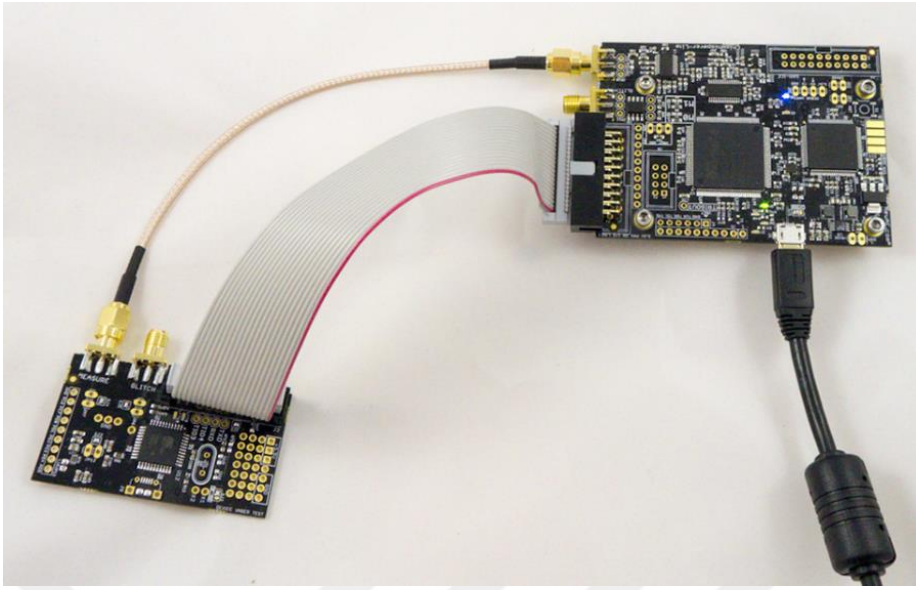
Bu tez kapsamında yapılan çalışmalarda Şekil 6.4' te görülen Newae firmasına ait Chipwhisperer-Lite CW1173 yan kanal atak test cihazı kullanılmıştır. Bu cihaz üzerinde Spartan-6 FPGA bulundurmaktadır. Üzerinde dahili osiloskop bulunmaktadır ve CW1173 cihazı hem düşük maliyetlere sahip hemde cihaz ile yapılacak atakları yönetmek üzere açık kaynak bir yazılım paketi ile sunulmaktadır. Bu sayede yan kanal analizi üzerine yapılabilecek çalışmalar için çok uygun bir ortam sunmaktadır [125]. Yan kanal analizleri hakkında birçok makale ve kitapda bu cihazdan faydalanılmıştır [125-130]. Ek-1 de chipwhisperer cihazının datasheet' i görülmektedir.

Cihazı kullanmak için açık kaynak kodlu Chipwhisperer Capture ve Chipwhisperer Analyzer programları üretici firma web sitelerinden ücretsiz olarak indirilebilir [131].



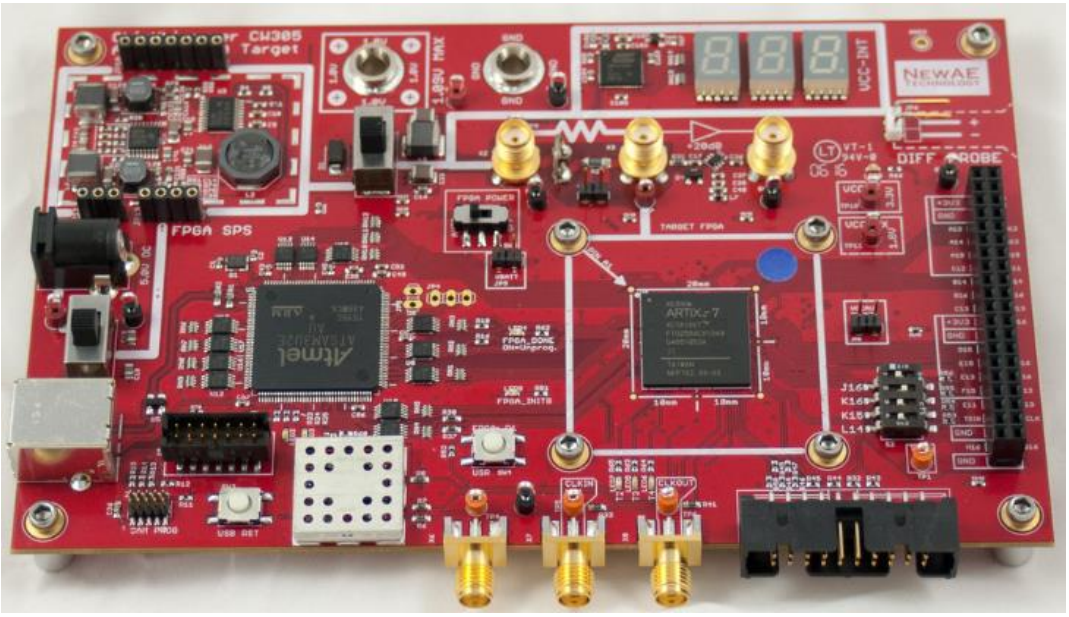
Şekil 6.4. Chipwhisperer-Lite CW1173

Şekil 6.4’ de görülen cihazlardan CW303 cihazı xmega işlemcisine sahip olup atakda bulunulacak olan hedef cihazdır. CW303 üzerinde bulunan xmega işlemcisi çeşitli şifreleme algoritmalarını çalıştıracak şekilde programlanabilmektedir. Ayrıca bu gömülü sistem üzerinde şifreleme işlemleri yapılırken Chipwhispere-Lite ile hedef cihaz olan CW303’ ün güç tüketim değerleri Şekil 6.5’ de görüldüğü gibi ölçülebilmekte ve chipwhisper açık kaynak yazılım sitemi ile ölçülen güç izleri üzerinden DPA atağı yapılarak sisteme yan kanal atakları gerçekleştirilebilmektedir.



Şekil 6.5. Chipwhisperer-lite atak gerçekleştirilirken

Şekil 6.6' da görülen CW305 Artix FPGA Target Board'u üzerinde Artix-7 FPGA bulunmaktadır. Bu cihaz üzerindeki FPGA, şifreleme işlemlerini gerçekleştirecek şekilde programlanabilmekte ve chipwhispere-lite yan kanal analizi cihazı ile Artix hedef aygıtındaki FPGA üzerinde çalışan şifreleme algoritmalarına ataklar düzenlenebilmektedir.



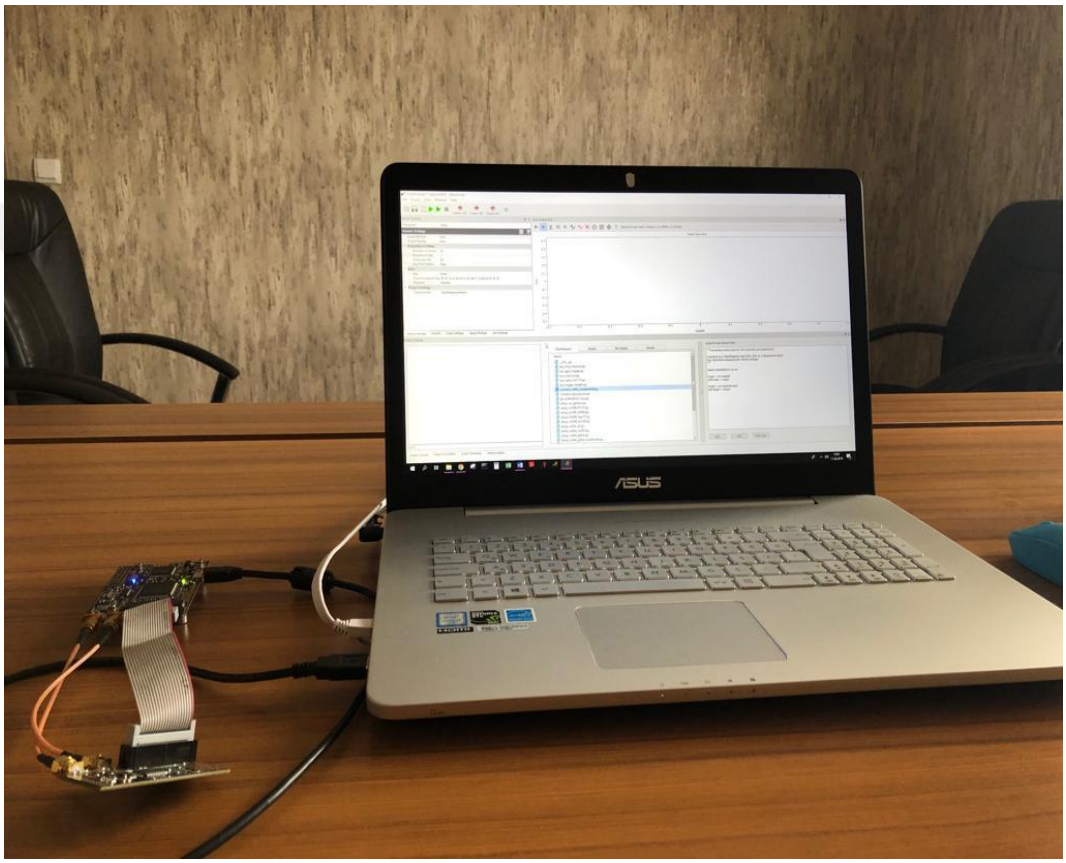
Şekil 6.6. CW305 Artix FPGA target board [131]

Chipwhisper ile bir kriptografik aygıta yan kanal analizi iki adımda yerine getirilir. Birinci adımda Chipwhisperer lite aygıtı ile Chipwhisperer Capture yazılımını kullanılarak hedef aygıtın

güç tüketim değerleri ölçülerek kaydedilir. İkinci adımda ise Chipwhisperer Analyzer programı ile kaydedilen bu güç izleri analiz edilerek hedef aygıtın gizli anahtar değerlerine ulaşmaya çalışılır.

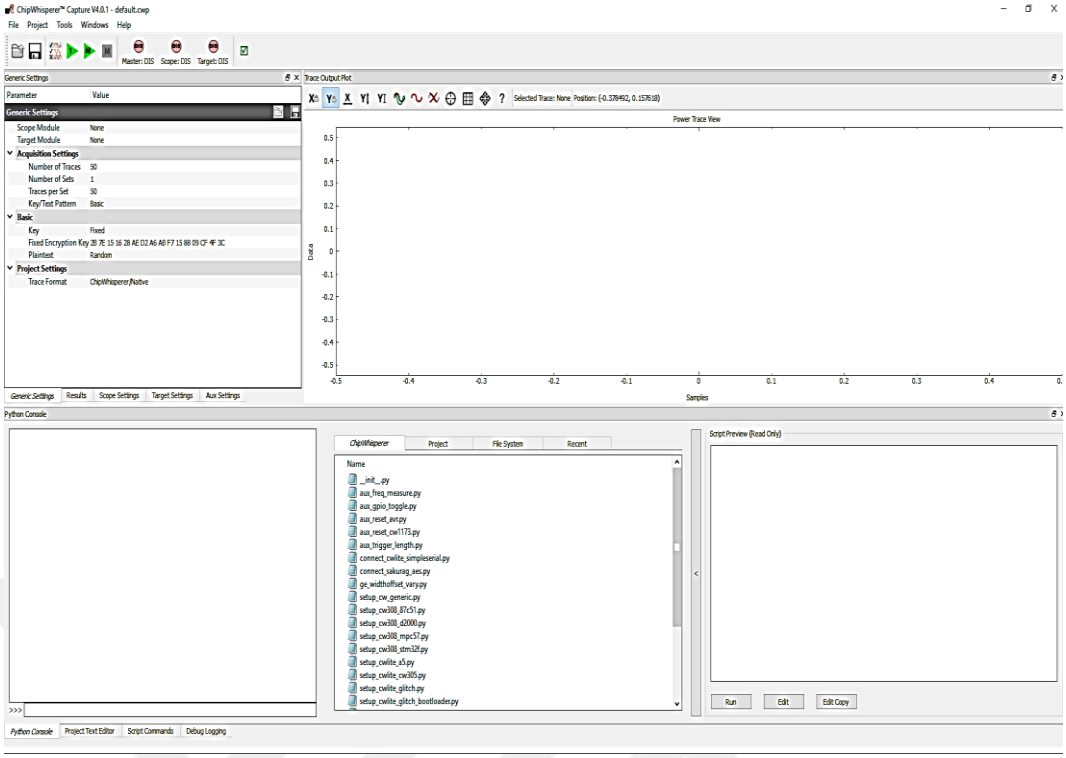
6.4.1. Chipwhisperer İle Hedef Aygıtın Güç Tüketimini Ölçmek

Hedef aygıtın güç tüketim değerlerini ölçmek için Şekil 6.7' de görüldüğü gibi öncelikle Chipwhisper Lite kişisel bilgisayara usb portundan bağlanır.



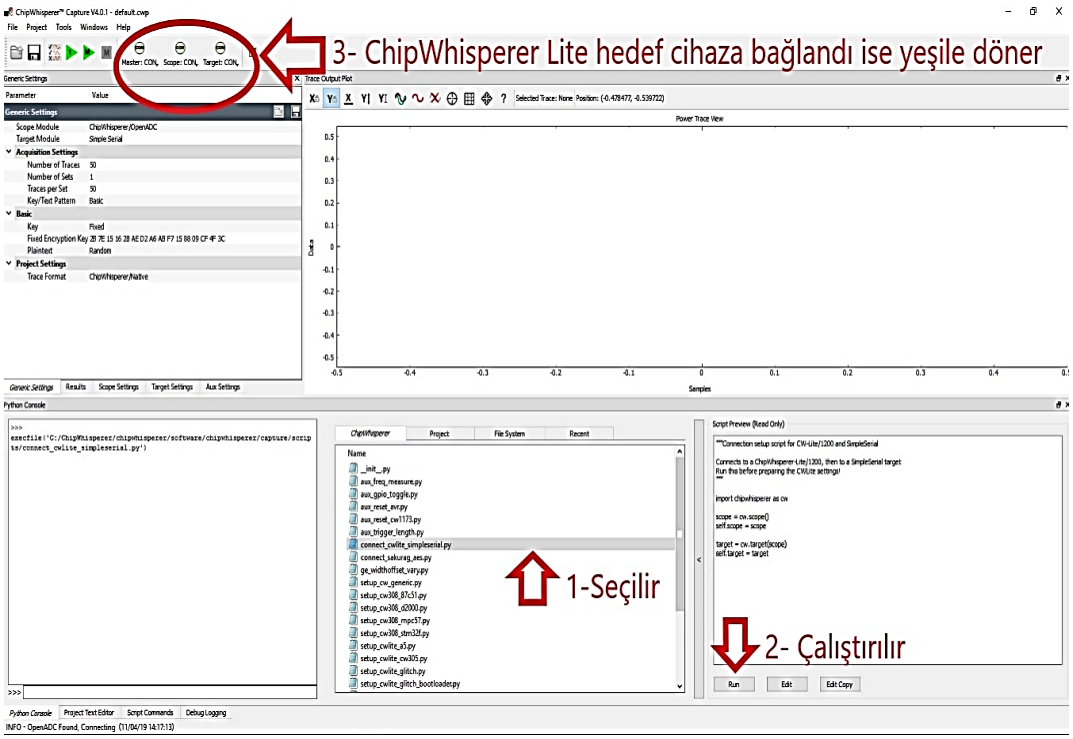
Şekil 6.7. Analiz cihazının kişisel bilgisayara bağlanması

Bilgisayara fiziksel bağlantı sağlandıktan sonra Şekil 6.8' de görülen Chipwhisperer Capture yazılımı açılır.



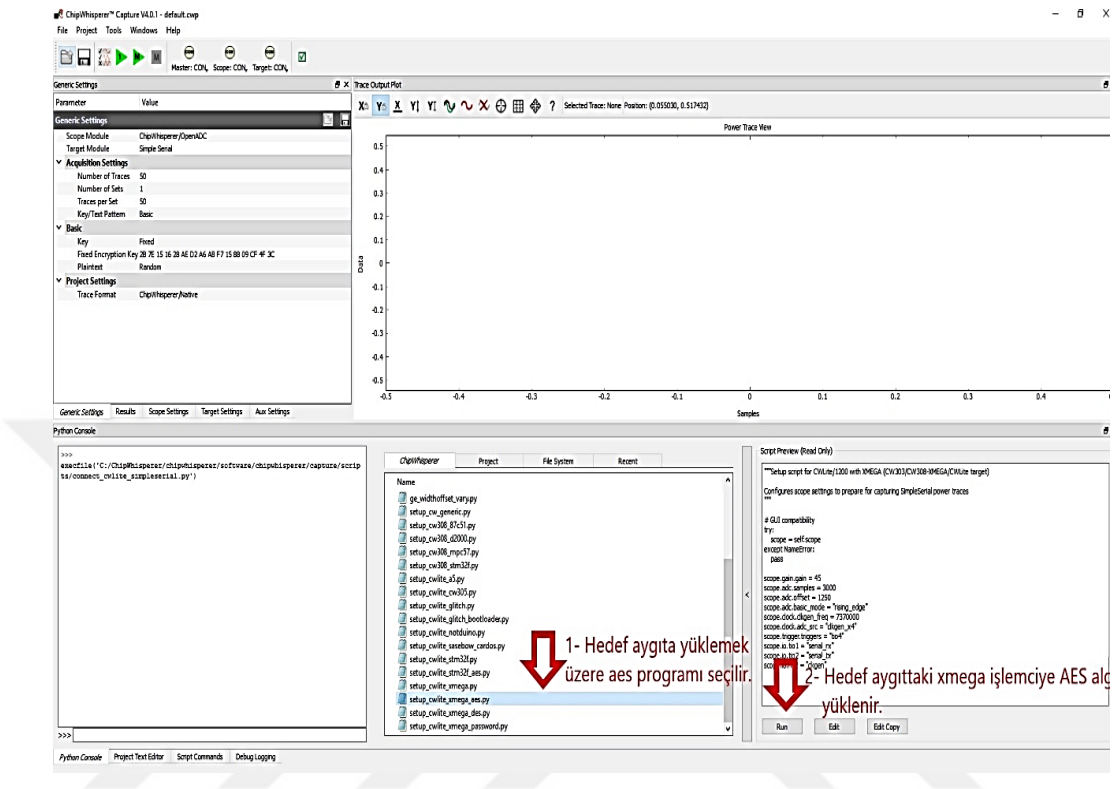
Şekil 6.8. Chipwhisperer capture programı

Program açıldıktan sonra bilgisayara bağlanmış olan Chipwhisperer Lite cihazının Hedef aygıta (cw303) bağlanması için Şekil 6.9’ da görülen adımlar takip edilir.



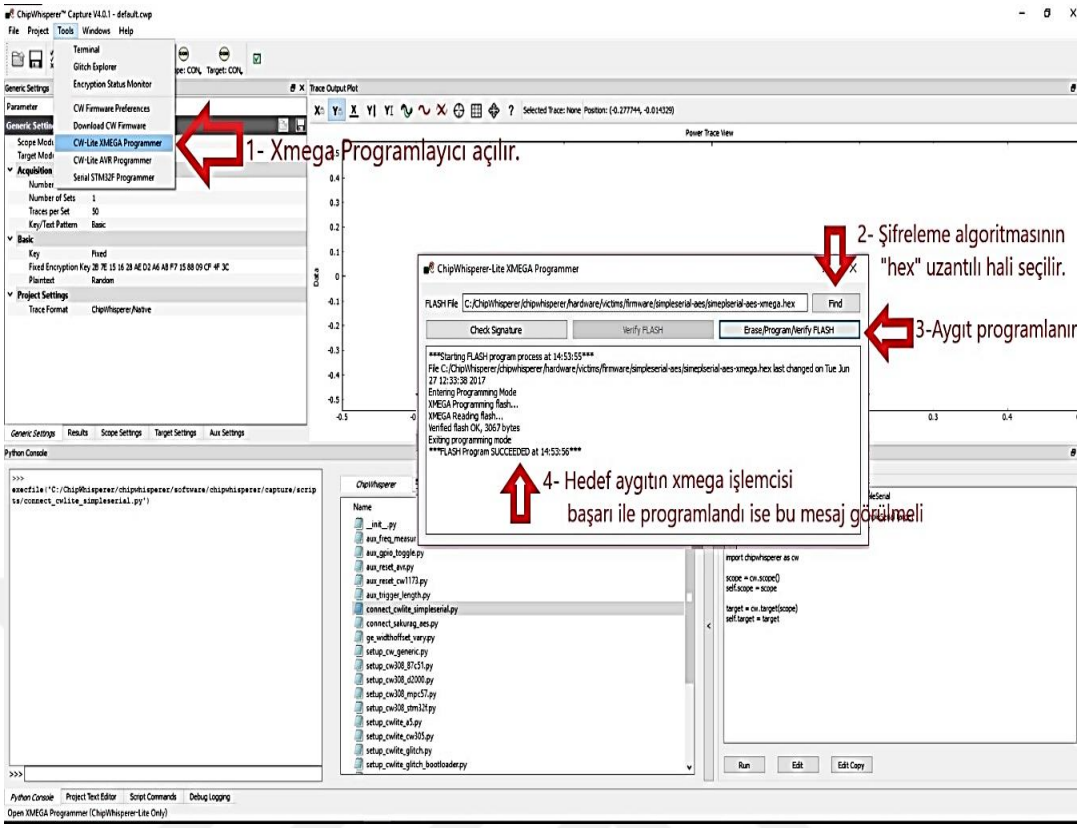
Şekil 6.9. Chipwhisperer lite cihazının hedef aygıta bağlanması

Sonraki adımda atakda bulunulacak hedef cihazda çalıştırılacak şifreleme algoritması Şekil 6.10’ da görüldüğü gibi seçilir. Burada xmega işlemciye AES algoritması yüklenecektir.



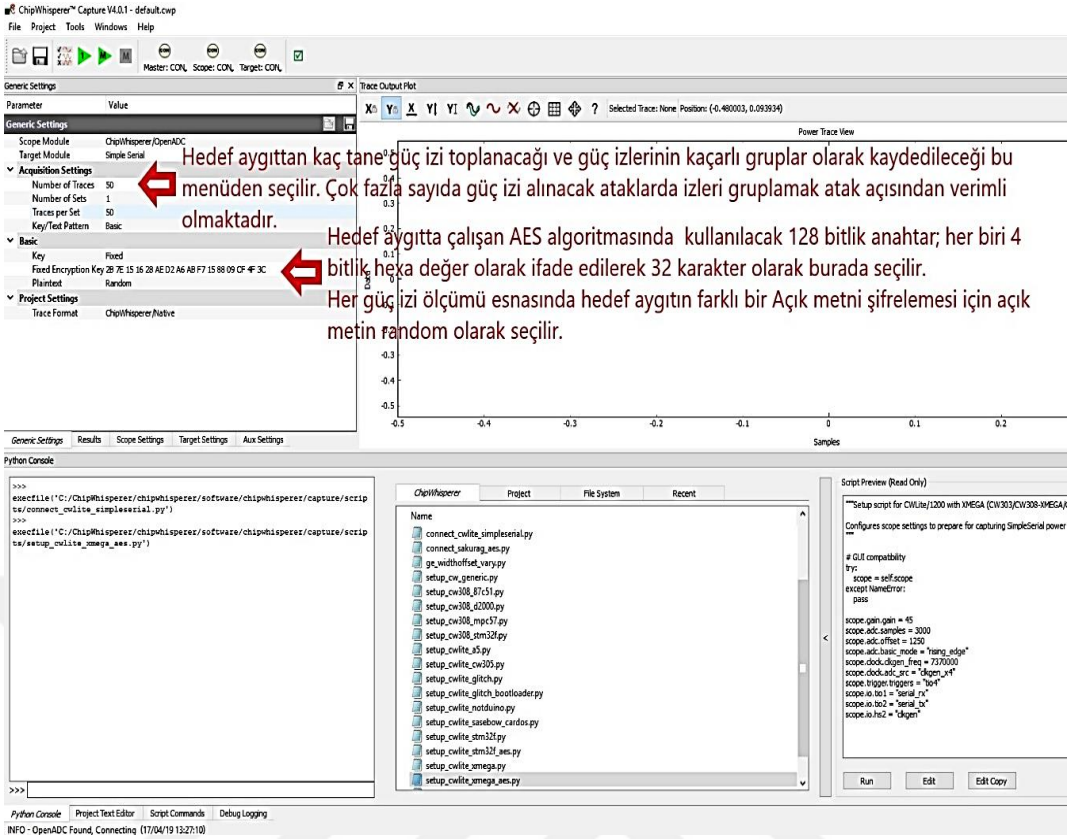
Şekil 6.10. Hedef aygıta AES algoritmasının yüklenmesi

Standart AES algoritması üzerinde değişiklikler yapıldı ise derlenen programın “hex” uzantılı program kodları Xmega işlemcisine Şekil 6.11’ deki gibi manuel yüklenmelidir.



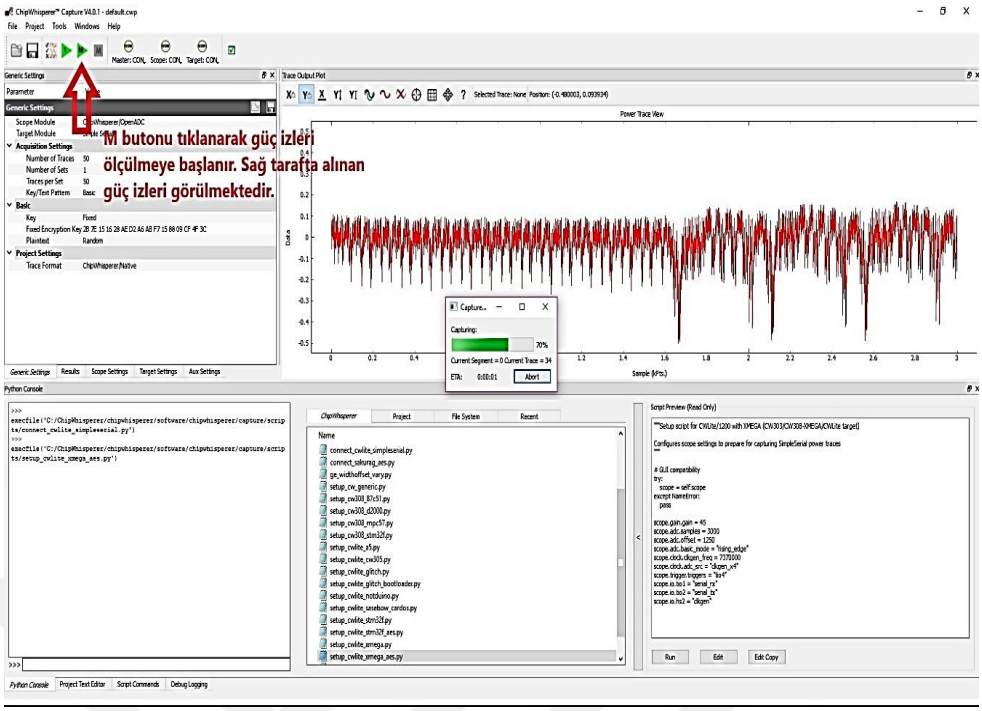
Şekil 6.11. Derlenmiş AES algoritmasının hex kodlarının hedef aygıta yüklenmesi

Hedef aygıtta çalışacak AES algoritmasının anahtar değeri ve kaç tane güç izi toplanacağı Şekil 6.12' de görülen menülerden seçilir.



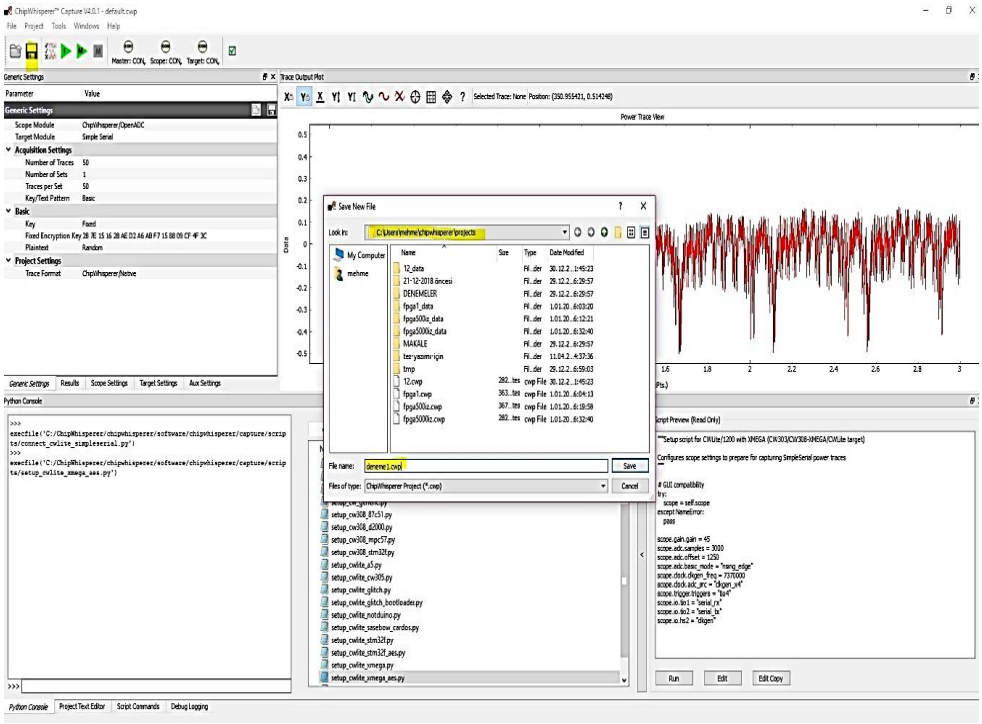
Şekil 6.12. Hedef aygıtta çalışacak anahtar ve aygıttan alınacak güç izi sayılarının seçimi

Bu aşamadan sonra hedef aygıt çalışırken güç izleri ölçmek üzere Şekil 6.13' de görüldüğü gibi ölçüm işlemi gerçekleştirilir.



Şekil 6.13. Seçilen sayıda güç izinin ölçümü

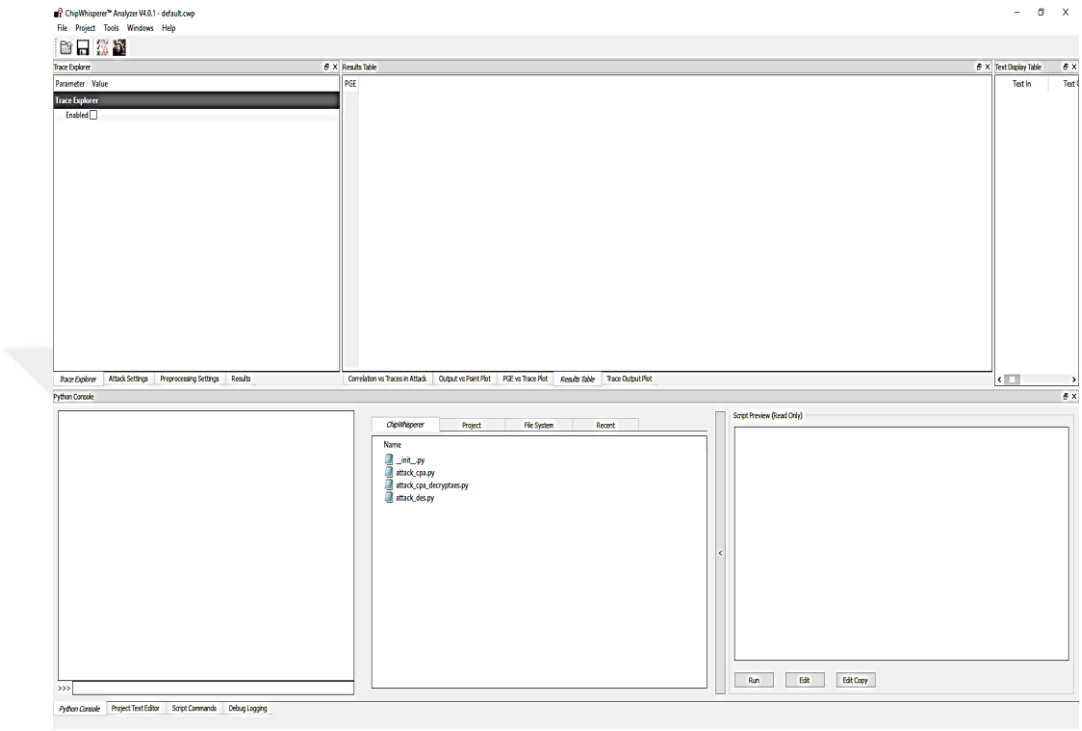
Güç izleri ölçüldükten sonra Şekil 6.14' de görüldüğü gibi daha sonra analiz edilmek üzere kaydedilmelidir.



Şekil 6.14. Hedef aygıt çalışırken alınan güç izlerinin kaydedilmesi

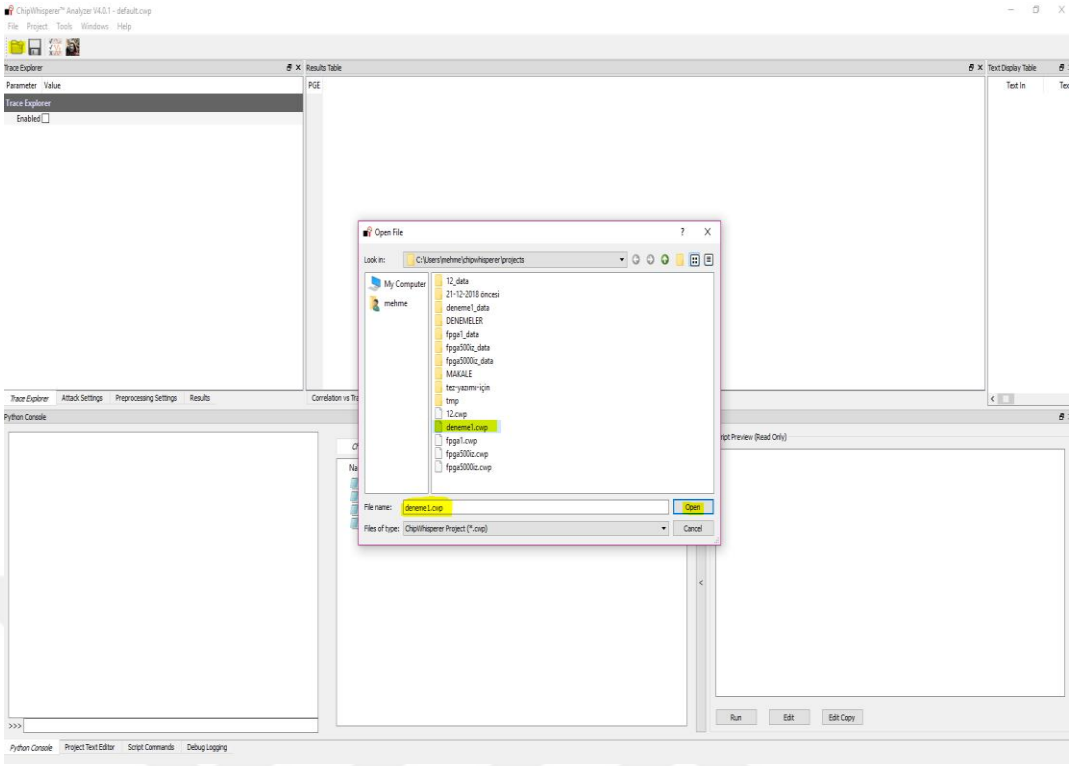
6.4.2. Kaydedilen güç izlerini chipwhisperer analyzer ile analiz etmek

Güç izleri kaydedildikten sonra Chipwhisperer Capture programı kapatılarak Şekil 6.15’ de görülen Chipwhisperer Analyzer programı çalıştırılır.



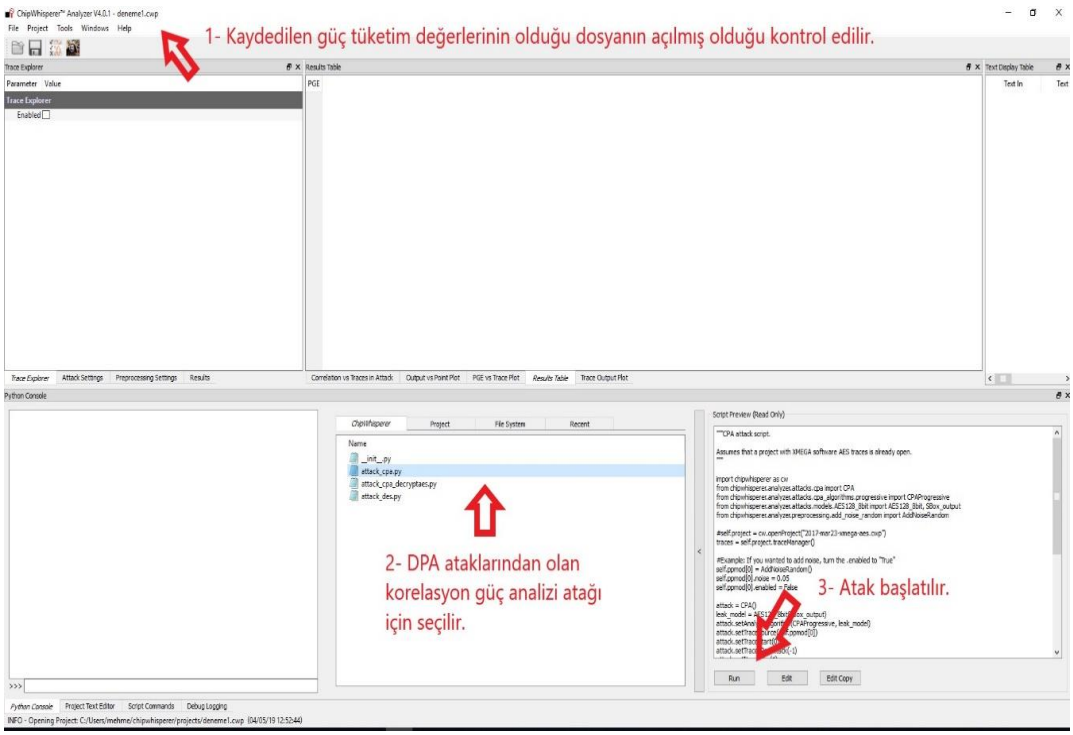
Şekil 6.15. Chipwhisperer analyzer programı

Chipwhisper analyzer programında daha önce Capture programı ile kaydedilen güç izleri analiz edilmektedir. Öncelikle Şekil 6.16’ da görüldüğü gibi daha önce kaydedilen güç izi kayıt dosyası açılır.



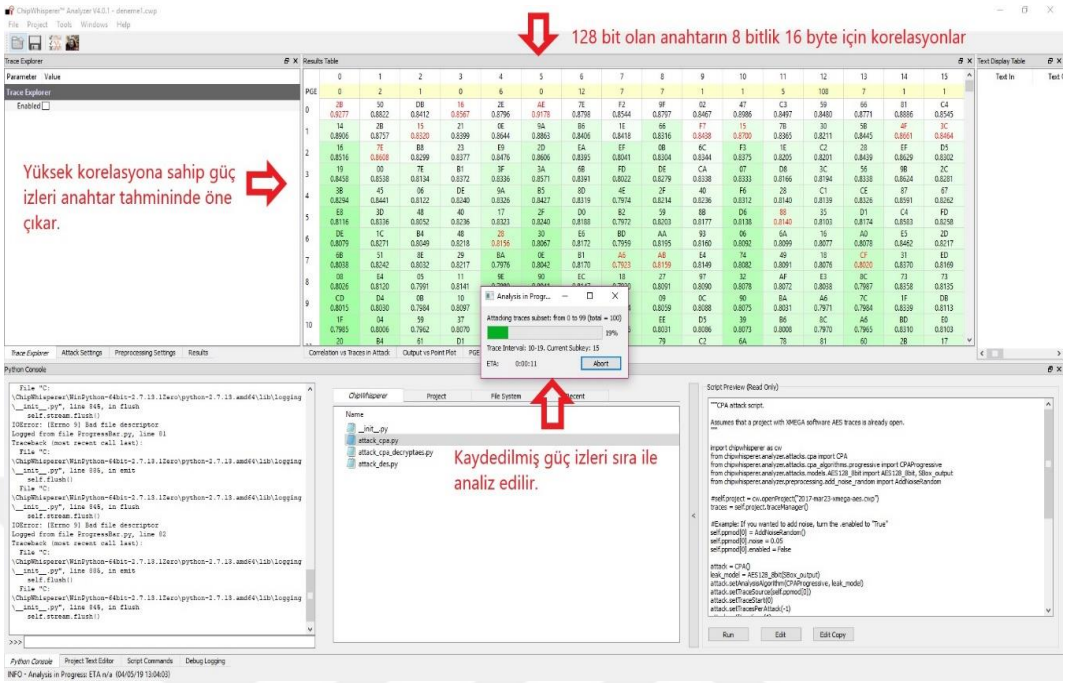
Şekil 6.16. Capture programı ile kaydedilen güç izi dosyasının açılması

Kaydedilen güç izi dosyası açıldıktan sonra Şekil 6.17’ de görülen adımlar izlenir.



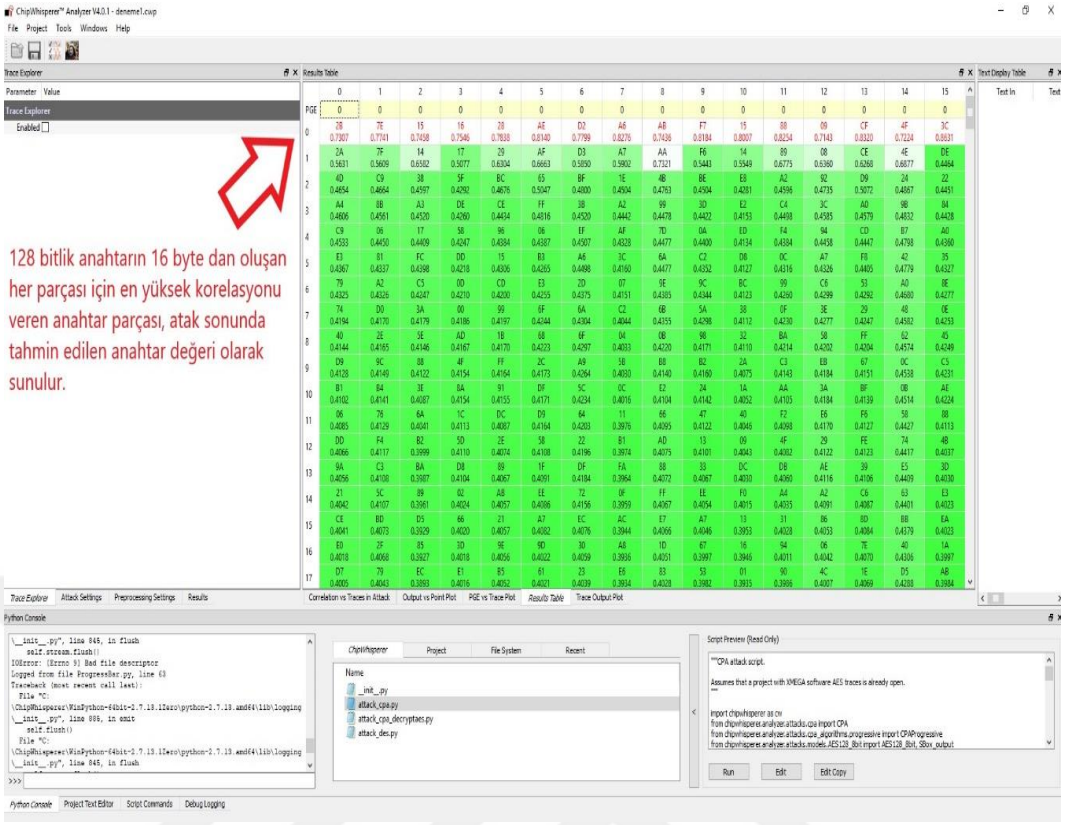
Şekil 6.17. Kaydedilmiş güç izleri üzerinde atak başlatılması

Atak Şekil 6.18 de görüldüğü gibi devam eder.



Şekil 6.18. Atak devam ederken

Atak sona erdiğinde Şekil 6.19' da görüldüğü gibi en yüksek korelasyona sahip anahtar tahminleri aygıtın gerçek anahtarının tahmini olarak öne sürülür.



Şekil 6.19. Atak sonucu olarak aygıtın gerçek anahtarının bulunması

7. BULGULAR VE TARTIŞMA

Kaos ve kriptoloji arasında teorik olarak güçlü bir ilişki vardır. Pratikte bu ilişkinin en başarılı uygulamalarından birisi kaos bazlı yer değiştirme yapılarıdır (substitution box, s-box). Bununla beraber, kaos bazlı s-box dizaynlarının performans ölçüleri AES gibi modern şifreleme algoritmalarında kullanılan, cebirsel tekniklere dayalı s-box yapılarına kıyasla daha kötüdür. Daha kötü kriptolojik özelliklere sahip olmasına rağmen kaos bazlı s-box yapılarının kullanılmasının nedeni bazı araştırmacıların kaos bazlı s-box yapılarının başta yan kanal saldırıları olmak üzere uygulama saldırılarına karşı alternatif bir savunma olabileceğini iddia etmeleridir. Fakat şimdiye kadar bu iddiayı destekleyen ya da çürüten bir çalışma olmamıştır. Bu tez kapsamında yapılan çalışmada iki farklı kaos bazlı s-box yapısında yan kanal analizleri gerçekleştirilmiştir. Bu iki s-box yapısı literatürde geçmişte önerilmiş kaotik s-box yapıları içinde en iyi ve en kötü kriptolojik özelliklere sahip olmaları nedeniyle seçilmiştir. Sonuçlar AES orijinal s-box yapısı ile kıyaslanmıştır. Sonuçların analizi kaos bazlı s-box yapılarının yan kanal saldırılarına karşı daha dirençli olduğunu göstermiştir. Bu yüzden kaos bazlı dizaynlar iddia edildiği gibi uygulama saldırılarına karşı bir alternatif savunma olabilir [46]. Fakat eğer saldırganın yan kanal analizinde 30' dan daha fazla şifresiz metni varsa hem cebirsel hem de kaos bazlı s-box dizaynlarının güvenli olmadığı gözlemlenmiştir.

Bir blok şifreleme algoritması konfüzyon ve difüzyon adı verilen iki temel özelliği sağlıyor olmalıdır. Birçok blok şifreleme algoritmasında konfüzyon özelliği yer değiştirme kutu (s-box) yapıları olarak bilenen kriptolojik bileşenler aracılığı ile sağlanmaktadır. Bu yüzden blok şifreleme algoritmaları gücünü s-box yapılarından almaktadır. Literatürde s-box yapılarının dizaynı üzerine cebirsel, sözde rastgele ve sezgisel yöntemlerin de arasında olduğu birçok yöntem önerilmiştir [132]. Modern blok şifreleme algoritmaları sıklıkla güçlü cebirsel ilişkilere dayalı s-box dizayn teknikleri kullanır. Bunların en iyi bilineni Nyberg tarafından önerilmiştir [133]. Bu yöntem ayrıca AES (Advanced Encryption Standard - Yüksek Seviye Şifreleme Standardı) blok şifreleme algoritmasında da kullanılmaktadır [134].

Son on yılda kaos bazlı s-box dizayn teknikleri cebirsel s-box dizayn algoritmalarına bir alternatif olarak önerilmiştir. Kaotik sistemleri s-box dizayn sürecinde kullanma fikri kaos ve kriptografi arasındaki benzerliklere dayanmaktadır [135]. Bu iki dizayn da kaotik sistemleri rastgelelik kaynağı olarak kullanmaktadır. S-box yapıları kaotik sistemin tahmin edilemez çıktıları aracılığıyla yaratılır. Kaos bazlı s-box yapılarının performans kriterleri incelendiğinde, kaos bazlı s-box yapılarının AES s-box yapılarına göre daha kötü kriptolojik özellikleri olduğu görülmüştür. Örneğin, AES s-box açısından nonlineerite değeri 112'dir. AES s-box bilinen en iyi kriptolojik özellikler kullanılarak dizayn edildiği için bu değer ulaşılabilecek azami limittir. Kaos bazlı s-box dizaynlarında ise nonlineerite değerinin azami limitinin 106,75 olduğu gösterilmiştir. Bir diğer

önemli performans ölçütü olan Girdi/Çıktı XOR (diferansiyel analiz) tablosundaki azami değer de diferansiyel saldırılara direnci ölçmek için kullanılmıştır ve AES s-box yapısı için bu değer 4' tür. Bu değer olabildiğince küçük olmalıdır ve 4 erişilebilecek asgari limittir. Kaos bazlı dizaynlarda asgari limitin 10 olduğu gösterilmiştir [136].

Bu noktada akla bir soru gelmektedir. Ortada AES s-box gibi üstün kriptolojik özellikleri olan kriptolojik bileşenler varken kaos bazlı s-box yapılarını kullanmak mantıklı mıdır? Literatürde kaos bazlı s-box yapılarının [137-169] AES s-box yapılarına kıyasla en önemli avantajının yan kanal saldırılarına karşı direnci olduğu iddia edilmiştir. Fakat bu iddia teorik veya deneysel bir çalışmayla kanıtlanmamıştır. Bu tez çalışmasında kaos bazlı s-box yapılarının yan kanal saldırılarına karşı direnci analiz edilmiştir. Bu çalışma literatürde bu amacı gerçekleyen ilk çalışmadır. Elde edilen sonuçlar düşünüldüğünde bunun kaos bazlı kriptoloji literatürüne yeni bir bakış açısı getireceği düşünülmektedir.

Bölüm 3' te yan kanal saldırıları adım adım açıklanmıştır. Bölüm 6' da yan kanal saldırıları için kullanılan deney kümesi detaylı olarak anlatılmıştır. Bu bölümde ise AES algoritma mimarisindeki Nyberg s-box ve iki farklı kaos bazlı s-box yapısı için yan kanal analizleri raporlanmıştır. Kaos bazlı yapıların ilki literatürdeki en iyi kriptolojik özelliklere sahip s-box yapısının analizlerinde kullanılmıştır. Diğer kaos bazlı s-box yapısı ise en kötü kriptolojik özelliklere sahip s-box yapısının analizlerinde kullanılmıştır. Bu yolla kaos bazlı s-box yapılarının etkisi en iyi ve en kötü koşullarda incelenmiş ve geniş bir değerlendirme sunulmuştur.

Üç farklı s-box ile gerçekleştirilen üç farklı yan kanal analizi standart AES blok şifreleme algoritması için gerçekleştirilmiştir. Analizin amacı yan kanal bilgisini kullanarak standart AES algoritmasının 128 bit uzunluğundaki anahtar değerini elde etmektir. Analizde değiştirilen tek faktör s-box yapısıdır. Birinci analizde orijinal AES s-box [133] kullanılmıştır. İkinci ve üçüncü analizlerde kaos bazlı s-box yapıları [136,170] kullanılmıştır. Bu s-box yapılarının performans özellikleri Tablo 7.1' de verilmiştir.

Tablo 7.1. Analizde kullanılan s-box yapılarının pereformanslarının kıyaslanması

S-Box	SAC			Azami G/Ç XOR	Nonlineerite			BIC-Nonlineerite	BIC-SAC
	Asgari	Ortalama	Azami		Asgari	Ortalama	Azami		
AES s-box	0.5	0.5	0.5	4	112	112	112	0.5	0.5
Kaotik s-box 1	0.3909	0.4941	0.6094	10	106	106.75	108	103.5	0.4957
Kaotik s-box 2	0.3906	0.5178	0.6719	54	96	102.5	106	102.5	0.4026

Bu s-box' ların kalitesini değerlendirmek için literatürde beş temel gereksinim kullanılmıştır. Bunlar birebir ve örtenlik (bijectivite), nonlineerite, mutlak çığ kriteri (SAC), bit bağımsızlık kriteri (BIC) ve girdi/çıktı XOR dağılımıdır [132, 136].

Birebir ve örtenlik kriteri s-box' taki her elemanın eşsiz olup olmadığını denetler. Nonlineerite s-box'un en önemli özelliklerinden biridir. Bu özelliğin testi için ilk olarak s-box lineer denklemler şeklinde ifade edilir. Denklemlerin olabildiğince lineer olmaması istenilen bir durumdur. Walsh spektrumu bunu ölçmek için kullanılmıştır ve bu ölçüm için ulaşılabilecek azami değer 112'dir.

S-box' lar için bir diğer önemli test kriteri Fesitel tarafından önerilen SAC' dır [132]. Bu test kriteri girdideki değişimin çıktıya yansıma boyutunu ölçmektedir. İdeal koşulda girdideki bir bitlik değişimin çıktıda yarım bitlik değişime neden olması istenir. SAC kriteri için en iyi değer 0,5 tir.

S-box yapısının saptanması için hibrit bir ölçüt olan BIC çıktı bitleri üzerinde önceki iki test kriterinin etkilerini analiz eder.

Son ölçü girdi/çıktı XOR dağılımıdır. Bu kriter diferansiyel kriptanaliz ile ilişkilidir. S-box' taki en yüksek değer olabildiğince küçük olmalıdır. Bu ölçüt için var olan en küçük değer 4' tür.

Tablo 7.1' deki analiz sonuçları incelendiğinde Nyberg tarafından önerilen AES s-box yapısının cebirsel yöntemlere dayalı olması dolayısıyla ideal karakteristiklere sahip olduğu açıktır.

Kaotik s-box 1 [136] kaotik sistemlere dayalı en iyi kriptolojik özelliklere sahip s-box yapısıdır. Bu değerler kaos bazlı dizaynlar için var olan en iyi değerlerdir. Nonlineerite 106,75'tir ve azami G/Ç XOR 10 dur. Bu değerler teorik [169] ve deneysel [136] olarak elde edilebilecek en yüksek değerlerdir.

Kaotik s-box 2 yapısı literatürde yayınlanmış en kötü kriptolojik özelliklere sahip kaos bazlı s-box'tur [170].

7.1. Orjinal S-box İle AES Algoritmasının Yan Kanal Analizi

Yan kanal analizinin etkilerini daha iyi anlamak için üç farklı vaka çalışması yapılmıştır. İlk vaka çalışmasında 10 adet şifresiz metnin her biri için saldırı noktasındaki değerler öngörülmüştür. Başarı oranı ve tahmin entropisi yan kanal saldırılarını değerlendirilmek amacıyla geniş çapta kullanılır. Bu çalışmada yan kanal saldırısının başarısını değerlendirmek için başarı oranı kriteri kullanılmıştır. Anahtar kısmıyla eşleşen değerler kestirilen değerlerde italik olarak gösterilmiştir. 128-bitlik AES algoritmasının gizli anahtarı 16 kısma ayrılmıştır. Örneğin, Tablo 7.2' de görülebileceği gibi ilk saldırı denemesinde sadece anahtarın "***D2***" değeri elde edilmiştir. Diğer bir deyişle, 10 adet şifresiz metin verisi kullanılarak gerçekleştirilen ilk saldırı denemesinin başarı oranı 1/16'dır. Bu saldırı denemeleri güvenilir bir değerlendirme elde edebilmek amacıyla 10 kere tekrarlanmıştır. Tablo 7.2' nin son hücresi 10 adet şifresiz metin kullanılarak gerçekleştirilen saldırı denemelerinin ortalama başarı oranını göstermektedir.

Tablo 7.2. Orijinal s-box ile 10 Adet şifresiz metin için saldırı sonuçları

Kısım	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Toplam
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	55	1E	ED	FF	21	6F	***D2***	8D	22	C1	36	B2	E7	D6	8C	BD	**1**
Saldırı 2	4F	E9	A7	18	1D	F2	3B	11	D7	09	11	AC	68	2C	E5	8B	**0**
Saldırı 3	44	E4	4F	3C	6C	6D	D7	B2	E4	DA	CC	F3	8D	17	BD	68	**0**
Saldırı 4	C8	***7E***	9C	DD	23	D2	70	62	28	50	ED	A5	88	A8	9E	40	**1**
Saldırı 5	2C	26	AE	7B	5B	2A	2D	3C	9A	11	14	57	30	44	E6	41	**0**
Saldırı 6	74	66	80	FC	***28***	***AE***	45	98	4E	00	C5	***88***	2F	41	C8	***3C***	**4**
Saldırı 7	5D	C4	1D	33	96	13	9A	5B	1F	3E	95	7A	CD	95	A3	***3C***	**1**
Saldırı 8	25	54	07	9E	27	EB	54	1E	56	09	BA	29	9D	8D	EF	D2	**0**
Saldırı 9	40	B8	C3	27	A8	17	2D	C3	23	C8	B0	22	C8	65	47	9B	**0**
Saldırı 10	FD	59	8E	65	20	9C	66	EE	76	77	C3	80	3D	7F	CD	E6	**0**
Toplam	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**2**	**7/160**

İkinci vaka çalışmasında 20 adet şifresiz metnin her biri için saldırı noktasındaki değerler öngörülmüştür. Tablo 7.3' ten görülebileceği gibi daha fazla yan kanal bilgisi kullanıldığından daha fazla anahtar kısmı elde edilmiştir. Toplamda 10 farklı saldırı denemesi gerçekleştirilmiştir ve 20 adet şifresiz metin kullanılarak gerçekleştirilen saldırı denemelerinin ortalama başarı oranı 89/160'dır.

Tablo 7.3. Orijinal s box ile 20 Adet şifresiz metin için saldırı sonuçları

Kısım	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Toplam
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	C2	7D	72	***16***	31	DA	97	A1	BA	***F7***	***15***	***88***	***09***	***CF***	F6	98	**6**
Saldırı 2	B6	***7E***	***15***	***16***	***28***	***AE***	AE	7B	***AB***	***F7***	5B	A4	95	***CF***	***4F***	***3C***	**10**
Saldırı 3	71	***7E***	***15***	***16***	84	***AE***	***D2***	6B	8D	89	***15***	B9	***09***	54	***4F***	***3C***	**9**
Saldırı 4	BC	***7E***	3E	09	***28***	B8	***D2***	87	***AB***	***F7***	***15***	***88***	E0	C0	***4F***	***3C***	**9**
Saldırı 5	7B	***7E***	***15***	***16***	58	7A	93	6D	AA	87	***15***	***88***	EB	***CF***	06	***3C***	**7**
Saldırı 6	CB	***7E***	***15***	06	B9	***AE***	4E	BE	***AB***	***F7***	***15***	***88***	80	27	5F	***3C***	**8**
Saldırı 7	07	***7E***	***15***	CE	B8	***AE***	***D2***	***A6***	AE	EA	FD	51	2F	***CF***	***4F***	***3C***	**8**
Saldırı 8	***2B***	***7E***	***15***	***16***	CA	16	***D2***	***A6***	EF	29	37	***88***	6B	9D	***4F***	***3C***	**9**
Saldırı 9	5C	***7E***	***15***	***16***	***28***	***AE***	99	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**14**
Saldırı 10	***2B***	***7E***	8B	***16***	78	***AE***	***D2***	A5	A4	***F7***	FC	***88***	32	***CF***	F7	***3C***	**9**
Toplam	**2**	**9**	**7**	**7**	**3**	**6**	**5**	**3**	**4**	**6**	**6**	**7**	**3**	**6**	**6**	**9**	**89/160**

Üçüncü vaka çalışmasında 30 adet şifresiz metnin her biri için saldırı noktalarındaki değerler kestirilmiştir. Sonuçlar Tablo 7.4' te gösterilmiştir. Bu senaryoda ortalama başarı oranı 144/160'tır. Bu vaka çalışmasında 4 ve 6 numaralı saldırı denemelerinde tüm anahtar elde edilmiştir. Bazı anahtar kısımları anahtarın tamamını öngörmek için kullanılabilir. Her saldırı denemesinde anahtar kısımlarının %75' inden fazlası elde edildiği için daha fazla şifresiz metin iziyle analize devam edilmemiştir. Diğer bir deyişle, eğer saldırganın yan kanal saldırı senaryosunda 30 veya daha fazla şifresiz metni varsa kaos bazlı s-box yapıları güvenli olmaktan çıkmaktadır.

Tablo 7.4. Orijinal s-box ile 30 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	***2B***	***7E***	***15***	***16***	9A	9D	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**14**
Saldırı 2	***2B***	***7E***	***15***	***16***	59	***AE***	***D2***	***A6***	8F	***F7***	***15***	***88***	4B	***CF***	***4F***	***3C***	**13**
Saldırı 3	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	03	4E	DB	**13**
Saldırı 4	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**16**
Saldırı 5	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	2D	***88***	***09***	***CF***	***4F***	***3C***	**15**
Saldırı 6	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**16**
Saldırı 7	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	E6	***CF***	***4F***	***3C***	**15**
Saldırı 8	D9	***7E***	***15***	***16***	***28***	***AE***	D3	***A6***	***AB***	***F7***	***15***	***88***	***09***	C9	4E	***3C***	**12**
Saldırı 9	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	D1	***CF***	***4F***	***3C***	**15**
Saldırı 10	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	F7	***09***	***CF***	***4F***	***3C***	**15**
Toplam	**9**	**10**	**10**	**10**	**8**	**9**	**9**	**10**	**9**	**10**	**9**	**9**	**7**	**8**	**8**	**9**	**144/160**

7.2. En İyi Kaotik S-box Kullanan AES Algoritmasının Yan Kanal Analizi

Bölüm 7.1 ve Bölüm 7.2 deki analiz çalışmalarının farkı s-box yapısıdır. Bu bölümdeki analizde sadece standart AES blok şifreleme mimarisindeki s-box yapısı Tablo 7.5' de görülen s-box yapısı ile değiştirilmiştir.

Tablo 7.5. Kaos bazlı en iyi kriptolojik özelliklere sahip s-box 2A

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

Tablo 7.5' deki s-box yapısı kaos bazlı s-box yapıları için literatürdeki en iyi kriptolojik özellik kriterlerini sergilemiştir [136]. İlk vaka çalışmasında 10 adet şifresiz metnin her biri için saldırı noktalarındaki değerler öngörülmüştür. Sonuçlar Tablo 7.6' da görüldüğü gibi 160 anahtar kısmından sadece birinin elde edildiğini göstermiştir. Buna göre 10 adet şifresiz metin biliniyor olsa da bu en iyi kriptolojik özelliklere sahip kaos bazlı s-box yapısı [136] kullanıldığında orijinal s-box kullanılan Bölüm 7.1' deki analizin aksine sadece 1 adet yan kanal bilgisi elde edilmektedir.

Tablo 7.6. Kaotik s-box 2A ile 10 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	42	F0	32	B2	A0	EC	97	02	77	A1	EC	48	B8	AC	5E	80	**0**
Saldırı 2	A2	D4	83	B2	7C	72	2F	71	67	37	99	85	B0	06	E7	F1	**0**
Saldırı 3	83	96	EA	6A	8D	88	CE	7A	4F	3E	52	FA	9D	79	BA	9C	**0**
Saldırı 4	A1	03	B2	5F	CF	97	03	BE	32	55	24	13	62	78	AC	5E	**0**
Saldırı 5	33	F1	6B	7B	48	77	9F	6A	A6	80	AD	49	5C	7B	80	26	**0**
Saldırı 6	66	AA	A9	E4	BC	77	E7	68	1B	58	18	20	D7	A7	23	93	**0**
Saldırı 7	FD	59	5F	82	1A	D9	A1	74	4D	FF	44	6D	B8	B3	E5	3D	**0**
Saldırı 8	F9	7F	AF	0E	C8	19	47	A2	3C	11	***15***	82	67	B8	D1	73	**1**
Saldırı 9	F4	D5	1C	E0	C4	53	F4	E0	D3	46	94	B5	12	1B	88	6D	**0**
Saldırı 10	3C	83	F5	33	99	B0	AD	7B	75	4A	7F	4B	8E	34	77	D9	**0**
Toplam	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1/160**

İkinci vaka çalışmasında 20 adet şifresiz metnin her biri için saldırı noktalarındaki değerler kestirilmiştir. Tablo 7.7 160 anahtar unsurundan 63' ünün elde edilebildiğini göstermektedir. 20 adet şifresiz metin kullanılarak gerçekleştirilen saldırının ortalama başarı oranı 63/160'tır. Yine AES s-box yapısı ile karşılaştırıldığında kaos bazlı s-box yapısı yan kanal analizi için orijinal AES s-box'a göre daha güvenlidir.

Tablo 7.7. Kaotik s-box 2A ile 20 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	37	***7E***	***15***	***16***	***28***	D9	B8	***A6***	***AB***	***F7***	C4	39	ED	***CF***	79	39	**8**
Saldırı 2	0E	***7E***	A5	***16***	78	D3	***D2***	***A6***	***AB***	DD	***15***	F5	06	A6	4B	***3C***	**7**
Saldırı 3	B5	A8	B8	A8	AC	07	17	EB	B9	8F	***15***	***88***	9B	59	19	85	**2**
Saldırı 4	17	9D	***15***	3E	8B	***AE***	***D2***	***A6***	C5	F6	C0	84	***09***	***CF***	***4F***	***3C***	**8**
Saldırı 5	B1	D8	***15***	***16***	B9	58	31	***A6***	2F	8C	***15***	CD	***09***	***CF***	B9	6E	**6**
Saldırı 6	B0	***7E***	AE	***16***	***28***	***AE***	2B	***A6***	7F	***F7***	4D	86	EE	79	***4F***	37	**7**
Saldırı 7	0A	52	***15***	***16***	***28***	19	EE	***A6***	9D	E9	***15***	***88***	28	***CF***	59	96	**7**
Saldırı 8	D4	45	***15***	8A	71	AF	F7	9B	***AB***	B2	***15***	66	***09***	***CF***	***4F***	***3C***	**7**
Saldırı 9	D7	F8	7C	08	4B	08	36	4A	***AB***	9F	E1	***88***	08	82	***4F***	D7	**3**
Saldırı 10	AD	***7E***	***15***	62	07	C9	5A	9A	7B	***F7***	***15***	6D	***09***	***CF***	***4F***	***3C***	**8**
Toplam	**0**	**4**	**6**	**5**	**3**	**2**	**2**	**6**	**4**	**3**	**6**	**3**	**4**	**6**	**5**	**4**	**63/160**

Üçüncü vaka çalışmasında 30 adet şifresiz metnin her biri için saldırı noktasındaki değerler öngörülmüştür. Sonuçlar Tablo 7.8.' de raporlanmıştır. Bu senaryoda 10 farklı saldırı denemesi için 160 anahtar unsurundan 139' u elde edilmiştir. Bu senaryoda 7 ve 9 no'lu saldırı denemelerinde anahtarın tümü elde edilmiştir. Bu yüzden daha fazla izle analize devam edilmemiştir.

Tablo 7.8. Kaotik s-box 2A ile 30 Adet şifresiz metin için saldırı sonuçları

Kısım	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Toplam
Anahtar	*2B*	*7E*	*15*	*16*	*28*	*AE*	*D2*	*A6*	*AB*	*F7*	*15*	*88*	*09*	*CF*	*4F*	*3C*	
Saldırı 1	83	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	69	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	14
Saldırı 2	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	*AB*	***F7***	***15***	***88***	96	***CF***	***4F***	***3C***	15
Saldırı 3	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	0B	***F7***	***15***	***88***	2C	***CF***	***4F***	***3C***	14
Saldırı 4	***2B***	FA	***15***	***16***	D2	***AE***	***D2***	***A6***	AA	***F7***	***15***	***88***	83	07	***4F***	***3C***	11
Saldırı 5	2A	***7E***	***15***	***16***	***28***	***AE***	D3	***A6***	B7	***F7***	***15***	***88***	08	***CF***	***4F***	***3C***	12
Saldırı 6	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	4A	***F7***	***15***	***88***	F3	***CF***	***4F***	***3C***	14
Saldırı 7	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	16
Saldırı 8	1B	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	15
Saldırı 9	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	16
Saldırı 10	99	***7E***	93	***16***	***28***	***AE***	D3	***A6***	***AB***	***F7***	***15***	***88***	6C	***CF***	***4F***	***3C***	12
Toplam	6	9	9	10	9	10	8	10	5	10	10	10	4	9	10	10	139/160

7.3. En kötü Kaotik S-box Kullanan AES Algoritmasının Yan Kanal Analizi

Bu analizde Tablo 7.9' da görülen kaos bazlı s-box yapısı [170] kullanılmıştır. Bu s-box yapısı literatürdeki kaos bazlı s-box yapıları içinde en kötü kriptolojik özelliklere sahiptir [136].

Tablo 7.9. Kaos bazlı en kötü kriptolojik özelliklere sahip s-box 12 yapısı

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

İlk vaka çalışmasında 10 adet şifresiz metnin her biri için saldırı noktasındaki değerler öngörülmüştür. Tablo 7.10 bu saldırıda 160 anahtar unsurundan beşinin elde edildiğini göstermektedir. 10 adet şifresiz metin kullanarak yapılan saldırının ortalama başarı oranı 6/160 tır.

Tablo 7.10. Kaotik s-box 12 ile 10 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	B2	78	8F	40	63	A0	5E	3F	54	32	28	06	32	88	4D	7B	**0**
Saldırı 2	AE	DA	F8	A4	DC	E9	92	0B	B4	***F7***	F3	EC	46	30	CA	49	**1**
Saldırı 3	5C	AD	17	78	84	E2	1B	***A6***	F8	09	72	59	63	B0	AB	8C	**1**
Saldırı 4	EC	CD	***15***	77	75	72	B4	C3	CA	B1	EE	90	1C	29	3B	50	**1**
Saldırı 5	17	A5	D3	4B	59	83	B6	13	FA	91	81	2E	89	0C	CB	***3C***	**1**
Saldırı 6	EB	42	E5	2F	1C	44	F9	08	56	FF	D7	65	E9	E5	C3	81	**0**
Saldırı 7	37	9C	E8	EB	24	6B	8D	30	73	A0	03	44	71	6A	BB	40	**0**
Saldırı 8	24	3B	8B	***16***	29	62	63	12	BA	A6	83	D2	02	E1	***4F***	07	**2**
Saldırı 9	AC	87	16	41	00	3D	33	50	60	8F	1D	83	90	9B	70	54	**0**
Saldırı 10	FE	37	88	BB	EA	33	9F	A9	A2	1B	01	BE	F6	8D	30	74	**0**
Toplam	**0**	**0**	**1**	**1**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**1**	**1**	**6/160**

İkinci vaka çalışmasında 20 adet şifresiz metnin her biri için saldırı noktasındaki değerler kestirilmiştir. Toplamda 10 deneme gerçekleştirilmiştir. Tablo 7.11' de gösterildiği gibi 160

anahtar unsurundan 85’ i elde edilmiştir. 20 adet şifresiz metin kullanılarak yapılan saldırının ortalama başarı oranı 85/160’tır.

Tablo 7.11. Kaotik s-box 12 ile 20 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	FC	***7E***	14	***16***	A9	***AE***	CD	82	49	***F7***	***15***	***88***	D9	***CF***	7E	***3C***	**8**
Saldırı 2	E0	***7E***	***15***	***16***	35	***AE***	***D2***	***A6***	13	***F7***	F9	***88***	63	***CF***	***4F***	***3C***	**11**
Saldırı 3	6C	5E	D3	***16***	BD	***AE***	***D2***	***A6***	4A	***F7***	***15***	FD	3D	CE	4D	***3C***	**7**
Saldırı 4	***2B***	6D	3B	***16***	56	08	84	***A6***	DD	E9	***15***	52	8D	***CF***	***4F***	***3C***	**7**
Saldırı 5	07	***7E***	E2	***16***	EC	***AE***	***D2***	***A6***	***AB***	FE	***15***	***88***	AF	***CF***	BE	***3C***	**10**
Saldırı 6	5B	***7E***	CE	***16***	6D	F4	***D2***	***A6***	***AB***	A7	6B	***88***	***09***	C4	86	***3C***	**8**
Saldırı 7	***2B***	***7E***	E3	***16***	76	61	***D2***	***A6***	C7	***F7***	***15***	23	6C	B0	***4F***	***3C***	**9**
Saldırı 8	F9	***7E***	AC	***16***	C8	***AE***	B9	***A6***	DC	***F7***	F2	***88***	05	DF	***4F***	F6	**7**
Saldırı 9	***2B***	***7E***	***15***	9F	A2	***AE***	D0	***A6***	B1	***F7***	2C	***88***	6F	3B	***4F***	***3C***	**9**
Saldırı 10	8D	69	***15***	***16***	89	FA	***D2***	***A6***	24	***F7***	8A	***88***	***09***	8F	***4F***	***3C***	**9**
Toplam	**3**	**7**	**3**	**9**	**0**	**6**	**6**	**9**	**2**	**7**	**5**	**7**	**2**	**4**	**6**	**9**	**85/160**

Üçüncü vaka çalışmasında 30 adet şifresiz metnin her biri için saldırı noktasındaki değerler kestirilmiştir. Sonuçlar Tablo 7.12’ de gösterilmektedir. Bu senaryoda 10 farklı deneme için 160 anahtar kısmından 147’ si elde edilmiştir. Bu senaryoda 1, 3 ve 7 numaralı saldırı denemelerinde anahtarın tamamı elde edilmiştir. Bu yüzden daha fazla iz kullanarak analize devam edilmemiştir. 30 adet şifresiz metin kullanılarak yapılan saldırının ortalama başarı oranı 147/160 tır.

Tablo 7.12. Kaotik s-box 12 ile 30 Adet şifresiz metin için saldırı sonuçları

Kısım	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**Toplam**
Anahtar	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	
Saldırı 1	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**16**
Saldırı 2	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	AA	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**15**
Saldırı 3	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**16**
Saldırı 4	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	C7	08	***CF***	***4F***	***3C***	**14**
Saldırı 5	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	C8	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**15**
Saldırı 6	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	4E	***CF***	***4F***	***3C***	**15**
Saldırı 7	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	***A6***	***AB***	***F7***	***15***	***88***	08	***CF***	***4F***	***3C***	**15**
Saldırı 8	***2B***	***7E***	***15***	***16***	***28***	***AE***	***D2***	A7	AA	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**14**
Saldırı 9	***2B***	***7E***	***15***	***16***	***28***	***AE***	AD	***A6***	***AB***	***F7***	***15***	***88***	ED	***CF***	4E	***3C***	**13**
Saldırı 10	***2B***	***7E***	***15***	***16***	29	***AE***	***D2***	***A6***	AA	***F7***	***15***	***88***	***09***	***CF***	***4F***	***3C***	**14**
Toplam	**10**	**10**	**10**	**10**	**9**	**10**	**9**	**9**	**6**	**10**	**10**	**9**	**6**	**10**	**9**	**10**	**147/160**

8. SONUÇLAR

Kaos ve kriptoloji bilimleri arasındaki benzerliklerin en başarılı örneklerinden biri rastgele seçime dayalı s-box yapısı dizaynıdır. Bu dizaynlarda kaotik sistemler rastgelelik kaynağı olarak kullanılmış ve literatürde birçok s-box yapısı önerilmiştir. Önerilen kaotik s-box yapıları AES s-box yapısına göre daha kötü kriptolojik performans ölçümlerine sahip olsa da araştırmacılar bu dizaynların yan kanal analizi gibi uygulama saldırılarına daha dirençli olabileceğini iddia etmiştir. Fakat bugüne kadar bu hipotezi doğrulayan hiçbir çalışma raporlanmamıştır. ***Bu tez çalışması kaos bazlı s-box yapılarının yan kanal analizi ile ilgili ilk çalışmadır.*** Bu çalışmada literatürdeki en iyi ve en kötü performans karakteristiklerine sahip önerilmiş kaos bazlı s-box yapıları arasında yan kanal analizleri gerçekleştirilmiştir. Bu analizler standart AES algoritmasına dayalı, Nyberg tarafından geliştirilen s-box yapısı ve kaos bazlı s-box yapılarını kıyaslamak için kullanılmıştır.

Bölüm 7' de verilen detaylı analizler Tablo 8.1' de özetlenmiştir. Tüm saldırı senaryoları bir ortalama değer elde etmek adına 10 kere tekrarlanmıştır. Standart AES algoritmasındaki anahtar uzunluğu 128 bittir. Bu analizlerde anahtar 16 kısma ayrılmış ve saldırı noktaları oluşturulmuştur.

Toplamda 10 deneme için anahtar kısım sayısı $16 \times 10 = 160$ tır. Tablo 8.1' de sunulan sonuçlar yan kanal saldırısının başarı oranını göstermektedir. Düşük değerler yan kanal saldırılarına karşı daha iyi dirence işaret etmektedir. Bu yüzden kaos bazlı s-box yapısının AES s-box yapısına göre yan kanal saldırılarına daha dirençli olduğu söylenebilir.

Bunlara ek olarak, yan kanal saldırı senaryosunda saldıranın elinde 30 veya daha fazla şifresiz metin verisi bulunuyorsa kaos bazlı s-box yapıları güvenli olmaktan çıkmaktadır. Bu sonuçlar kaos bazlı kriptoloji literatüründe uygulama analizi çalışmalarının gerekliliğini göstermektedir.

Tablo 8.1. Yan kanal analizinin ortalama başarı oranına genel bakış

	Nyberg s-box	**En Kötü Kaotik s-box-12**	**En İyi Kaotik s-box-2A**
10 şifresiz metin	7/160	6/160	1/160
20 şifresiz metin	89/160	85/160	63/160
30 şifresiz metin	144/160	147/160	139/160

Sonuçlara göre aşağıdaki çıkarımlar yapılabilir:

- İddia edildiği gibi kaos bazlı dizaynlar yan kanal analizi gibi uygulama saldırılarına karşı bir alternatif olabilir.
- Fakat bu özellik tek başına kullanılamaz çünkü en iyi kriptolojik özelliklere sahip kaos bazlı s-box yapısı bile hâlâ AES s-box yapısından kötüdür. Ayrıca 30 şifresiz metin ve üstü bilindiği zaman yan kanal saldırısıyla tüm anahtarın elde edilebileceği gösterilmiştir.

- Gelecekte literatürdeki diğer kaos bazlı dizaynların yan kanal analizi dirençlerini değerlendirmek bir zarurettir.
- Gelecek çalışmalarda kaotik sistemler yan kanal saldırılarını önlemek için bir karşı tedbir olarak kullanılabilir.

KAYNAKLAR

[1] Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.

[2] Mangard, S., Oswald, E., & Popp, T. (2008). *Power analysis attacks: Revealing the secrets of smart cards* (Vol. 31). Springer Science & Business Media.

[3] Heath, S. (2002). *Embedded systems design*. Elsevier.

[4] https://www.elektrikport.com/makale-detay/mikrodenetleyiciler-nasil-calisir-1-bolum/14785#ad-image-0, Erişim: 10 Aralık 2019.

[5] Standaert, F. X. (2010). Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems* (pp. 27-42). Springer, Boston, MA.

[6] Kizhvatov, I. (2011). *Physical Security of Cryptographic Algorithm Implementations*, PhD Thesis, University of Luxembourg.

[7] Agrawal, D., Archambeault, B., Rao, J. R., & Rohatgi, P. (2002, August). The EM side—channel (s). In *International workshop on cryptographic hardware and embedded systems* (pp. 29-45). Springer, Berlin, Heidelberg.

[8] FIPS, P. (1977). 46-\Data Encryption Standard"-Federal Information Processing Standards Publication 46. *US Department of Commerce/National Bureau of Standards, National Technical Information Service*.

[9] Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference* (pp. 104-113). Springer, Berlin, Heidelberg.

[10] Ordu, L., Yalçın, S. B. Ö. (2006). Yan-Kanal Analizi Saldırılarına Genel Bakış, *Ulusal Elektronik İmza Sempozyumu*, Ankara.

[11] S. B. Ors, B. Preneel, I. Verbauwhede, "Side-Channel Analysis Attacks on Hardware Implementations of Cryptographic Algorithms", Chapter in *Wireless Security and Cryptography: Specifications and Implementations*, Boca Raton, FL, USA: CRC Press, 2007.

[12] Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference* (pp. 104-113). Springer, Berlin, Heidelberg.

[13] Kocher, P., Jaffe, J., & Jun, B. (1999, August). Differential power analysis. In *Annual International Cryptology Conference* (pp. 388-397). Springer, Berlin, Heidelberg.

[14] Quisquater, J. J., & Samyde, D. (2001, September). Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In *International Conference on Research in Smart Cards* (pp. 200-210). Springer, Berlin, Heidelberg.

[15] Shamir, A., & Tromer, E. (2004). Acoustic cryptanalysis, preliminary proof of concept presentation.

[16] Kahn, D. (1996). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.

[17] Kocher, P. C. (1996, August). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Annual International Cryptology Conference* (pp. 104-113). Springer, Berlin, Heidelberg.

[18] Messerges, T.S. (2002). *Power Analysis Attacks and Countermeasures on Cryptographic Algorithms*, PhD thesis, University of Illinois

[19] Borst, J. (2001). *Block Ciphers: Design, Analysis and Side-Channel Analysis*, PhD Thesis, K.U.Leuven.

[20] Guntur, H., Ishii, J., & Satoh, A. (2014, October). Side-channel attack user reference architecture board SAKURA-G. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 271-274). IEEE.

[21] O'Flynn, C., & Chen, Z. D. (2014, April). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.

[22] Standaert, F. X. (2010). Introduction to side-channel attacks. In *Secure Integrated Circuits and Systems* (pp. 27-42). Springer, Boston, MA.

[23] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (1999). Investigations of Power Analysis Attacks on Smartcards. *Smartcard*, *99*, 151-161.

[24] Bos, J. W., Hubain, C., Michiels, W., & Teuwen, P. (2016, August). Differential computation analysis: Hiding your white-box designs is not enough. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 215-236). Springer, Berlin, Heidelberg.

[25] Yalçın, S. O. (2005). *Hardware design of elliptic curve cryptosystems and side-channel attacks* , PhD Thesis, Katholieke Universiteit Leuven

[26] Joye, M. (2009). Basics of side-channel analysis. In *Cryptographic Engineering* (pp. 365-380). Springer, Boston, MA.

[27] https://www.cryptrec.go.jp/exreport/cryptrec-ex-1047-2002.pdf, Erişim: 25 Ocak 2020.

[28] Coron, J. S. (1999, August). Resistance against differential power analysis for elliptic curve cryptosystems. In *International workshop on cryptographic hardware and embedded systems* (pp. 292-302). Springer, Berlin, Heidelberg.

[29] Skorobogatov, S. P. (2005). *Semi-invasive attacks: a new approach to hardware security analysis*, PhD Thesis, University of Cambridge

[30] Mangard, S., Oswald, E., & Popp, T. (2008). *Power analysis attacks: Revealing the secrets of smart cards* (Vol. 31). Springer Science & Business Media.

[31] Chen, C., Eisenbarth, T., Von Maurich, I., & Steinwandt, R. (2015, June). Differential power analysis of a McEliece cryptosystem. In *International Conference on Applied Cryptography and Network Security* (pp. 538-556). Springer, Cham.

[32] Oswald, E., Mangard, S., Pramstaller, N., & Rijmen, V. (2005, February). A side-channel analysis resistant description of the AES S-box. In *International Workshop on Fast Software Encryption* (pp. 413-423). Springer, Berlin, Heidelberg.

[33] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (1999). Investigations of Power Analysis Attacks on Smartcards. *Smartcard*, *99*, 151-161.

[34] Bar-El, H., Choukri, H., Naccache, D., Tunstall, M., & Whelan, C. (2006). The sorcerer's apprentice guide to fault attacks. *Proceedings of the IEEE*, *94*(2), 370-382.

[35] Brier, E., Clavier, C., & Olivier, F. (2004, August). Correlation power analysis with a leakage model. In *International workshop on cryptographic hardware and embedded systems* (pp. 16-29). Springer, Berlin, Heidelberg.

[36] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE transactions on computers*, *51*(5), 541-552.

[37] Kleidermacher, D., & Kleidermacher, M. (2012). *Embedded systems security: practical methods for safe and secure software and systems development*. Elsevier.

[38] Hnath, W., Pettengill, J. (2010). Differential power analysis side-channel attacks in cryptography. *Major Qualifying Project*, Worcester Polytechnic Institute.

[39] www.quora.com/What-is-a-netlist-in-PCB, Erişim: 5 Aralık 2017.

[40] Kocher, P., Jaffe, J., Jun, B., & Rohatgi, P. (2011). Introduction to differential power analysis. *Journal of Cryptographic Engineering*, *1*(1), 5-27.

[41] Mangard, S., Oswald, E., & Popp, T. (2008). *Power analysis attacks: Revealing the secrets of smart cards* (Vol. 31). Springer Science & Business Media.

[42] Lumbiarres-Lopez, R., Lopez-Garcia, M., & Canto-Navarro, E. (2016). A new countermeasure against side-channel attacks based on hardware-software co-design. *Microprocessors and Microsystems*, *45*, 324-338.

[43] Sprott, J. C. (2010). *Elegant chaos: algebraically simple chaotic flows*. World Scientific.

[44] Strogatz, S. (2018). *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry and Engineering*, CRC Press, Florida

[45] Kocarev, L., & Lian, S. (Eds.). (2011). *Chaos-based cryptography: Theory, algorithms and applications* (Vol. 354). Springer Science & Business Media.

[46] Açikkapi, M. Ş., Özkaynak, F., & Özer, A. B. (2019). Side-channel analysis of chaos-based substitution box structures. *IEEE Access*, *7*, 79030-79043.

[47] Li, C., Zhang, Y., & Xie, E. Y. (2019). When an attacker meets a cipher-image in 2018: A year in review. *Journal of Information Security and Applications*, *48*, 102361.

[48] Nyberg, K. (1993, May). Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 55-64). Springer, Berlin, Heidelberg.

[49] Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael.

[50] Wu, C. K., & Feng, D. (2016). *Boolean functions and their applications in cryptography*. Springer Berlin Heidelberg.

[51] Cusick, T. W., & Stanica, P. (2017). *Cryptographic Boolean functions and applications*. Academic Press.

[52] Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, *31*(8), 3317-3326, https://doi.org/10.1007/s00521-017- 3287-y

[53] Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers based on chaotic maps. *Ieee transactions on circuits and systems i: fundamental theory and applications*, *48*(2), 163-169.

[54] Tang, G., Liao, X., & Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons & Fractals*, *23*(2), 413-419.

[55] Tang, G., & Liao, X. (2005). A method for designing dynamical S-boxes based on discretized chaotic map. *Chaos, solitons & fractals*, *23*(5), 1901-1909.

[56] Chen, G., Chen, Y., & Liao, X. (2007). An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. *Chaos, solitons & fractals*, *31*(3), 571-579.

[57] Chen, G. (2008). A novel heuristic method for obtaining S-boxes. *Chaos, Solitons & Fractals*, *36*(4), 1028-1036.

[58] Wang, Y., Wong, K. W., Li, C., & Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A*, *376*(6-7), 827-833.

[59] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2013). A projective general linear group based algorithm for the construction of substitution box for block ciphers. *Neural Computing and Applications*, *22*(6), 1085-1093.

[60] Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., & Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. *Neural Computing and Applications*, *23*(1), 97-104.

[61] Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2013). An efficient approach for the construction of LFT S-boxes using chaotic logistic map. *Nonlinear Dynamics*, *71*(1-2), 133-140.

[62] Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2013). Efficient method for designing chaotic S-boxes based on generalized Baker's map and TDERC chaotic sequence. *Nonlinear Dynamics*, *74*(1-2), 271-275.

[63] Ahmad, M., Chugh, H., Goel, A., & Singla, P. (2013, August). A chaos based method for efficient cryptographic S-box design. In *International Symposium on Security in Computing and Communication* (pp. 130-137). Springer, Berlin, Heidelberg.

[64] Hussain, I., Shah, T., Gondal, M. A., & Mahmood, H. (2013). A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence. *Nonlinear Dynamics*, *73*(1-2), 633-637.

[65] Khan, M., & Shah, T. (2014). A construction of novel chaos base nonlinear component of block cipher. *Nonlinear Dynamics*, *76*(1), 377-382.

[66] Lambić, D. (2014). A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, *58*, 16-21.

[67] Liu, H., Kadir, A., & Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. *AEU-international Journal of Electronics and Communications*, *68*(7), 676-686.

[68] Khan, M., & Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S 8 symmetric group. *Neural Computing and Applications*, *25*(7-8), 1717-1722.

[69] Khan, M. (2015). A novel image encryption scheme based on multiple chaotic S-boxes. *Nonlinear Dynamics*, *82*(1-2), 527-533.

[70] Khan, M., Shah, T., & Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. *Neural Computing and Applications*, *27*(3), 677-685.

[71] Khan, M., Shah, T., & Batool, S. I. (2016). A new implementation of chaotic S-boxes in CAPTCHA. *Signal, Image and Video Processing*, *10*(2), 293-300.

[72] Lambić, D. (2017). A novel method of S-box design based on discrete chaotic map. *Nonlinear Dynamics*, *87*(4), 2407-2413.

[73] Farah, T., Rhouma, R., & Belghith, S. (2017). A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization. *Nonlinear Dynamics*, *88*(2), 1059-1074.

[74] Belazi, A., & El-Latif, A. A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, *130*, 1438-1444.

[75] Belazi, A., Khan, M., El-Latif, A. A. A., & Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics*, *87*(1), 337-361.

[76] Ahmed, H. A., Zolkipli, M. F., & Ahmad, M. (2019). A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Computing and Applications*, *31*(11), 7201-7210, doi: 10.1007/s00521-018- 3557-3.

[77] Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication*, *2*(2), 181-191.

[78] Ahmad, M., & Ahmad, Z. (2018). Random search based efficient chaotic substitution box design for image encryption. *International Journal of Rough Sets and Data Analysis (IJRSDA)*, *5*(2), 131-147, doi: 10.4018/IJRSDA.2018040107.

[79] Khan, M., & Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Computing and Applications*, *29*(4), 993-999, doi: 10.1007/s00521-016-2511-5.

[80] Ahmed, H. A., Zolkipli, M. F., & Ahmad, M. (2019). A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Computing and Applications*, *31*(11), 7201-7210.

[81] Alzaidi, A. A., Ahmad, M., Doja, M. N., Al Solami, E., & Beg, M. S. (2018). A New 1D Chaotic Map and beta-Hill Climbing for Generating Substitution-Boxes. *IEEE Access*, *6*, 55405-55418.

[82] Ali, K. M., & Khan, M. (2019). Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. *International Journal of Theoretical Physics*, *58*(9), 3091-3117, doi: 10.1007/s10773-019-04188-3.

[83] Zahid, A. H., & Arshad, M. J. (2019). An innovative design of substitution-boxes using cubic polynomial mapping. *Symmetry*, *11*(3), 437, doi: 10.3390/sym11030437.

[84] Khan, M. F., Ahmed, A., Saleem, K., & Shah, T. (2019). A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system. *IEEE Access*, *7*, 84980-84991, doi: 10.1109/ACCESS.2019.2925081.

[85] Özkaynak, F., & Özer, A. B. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. *Physics Letters A*, *374*(36), 3733-3738.

[86] Khan, M., Shah, T., Mahmood, H., Gondal, M. A., & Hussain, I. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. *Nonlinear Dynamics*, *70*(3), 2303-2311.

[87] Hussain, I., Shah, T., Mahmood, H., & Gondal, M. A. (2012). Construction of S8 Liu J S-boxes and their applications. *Computers & Mathematics with Applications*, *64*(8), 2450-2458.

[88] Hussain, I., Shah, T., & Gondal, M. A. (2012). A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. *Nonlinear Dynamics*, *70*(3), 1791-1794.

[89] Khan, M., Shah, T., Mahmood, H., & Gondal, M. A. (2013). An efficient method for the construction of block cipher with multi-chaotic systems. *Nonlinear Dynamics*, *71*(3), 489-492.

[90] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics*, *87*(2), 1081-1094.

[91] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynamics*, *92*(4), 1745-1759, doi: 10.1007/s11071-018- 4159-4.

[92] Wang, X., Akgul, A., Cavusoglu, U., Pham, V. T., Vo Hoang, D., & Nguyen, X. Q. (2018). A chaotic system with infinite equilibria and its S-box constructing application. *Applied Sciences*, *8*(11), 2132, doi: 10.3390/app8112132.

[93] Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *Applied Sciences*, *8*(12), 2650, doi: 10.3390/app8122650.

[94] Özkaynak, F. (2020). An analysis and generation toolbox for chaotic substitution boxes: a case study based on chaotic labyrinth rene thomas system. *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *44*(1), 89-98, doi: 10.1007/s40998-019-00230-6.

[95] Khan, M. F., Ahmed, A., & Saleem, K. (2019). A novel cryptographic substitution box design using Gaussian distribution. *IEEE Access*, *7*, 15999-16007, doi: 10.1109/ACCESS.2019.2893176.

[96] ul Islam, F., & Liu, G. (2017). Designing S-box based on 4D-4wing hyperchaotic system. *3D Research*, *8*(1), 9.

[97] Al Solami, E., Ahmad, M., Volos, C., Doja, M. N., & Beg, M. M. S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes. *Entropy*, *20*(7), 525, doi: 10.3390/e20070525.

[98] Özkaynak, F. (2019). Chaos based substitution boxes as a cryptographic primitives: Challenges and opportunities. *Chaotic Model. Simul.*, *1*, 49-57.

[99] Naseer, Y., Shah, T., Shah, D., & Hussain, S. (2019). A novel algorithm of constructing highly nonlinear sp-boxes. *Cryptography*, *3*(1), 6, doi: 10.3390/cryptography3010006.

[100] Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics*, *74*(3), 551-557.

[101] Khan, M., Shah, T., & Gondal, M. A. (2013). An efficient technique for the construction of substitution box with chaotic partial differential equation. *Nonlinear Dynamics*, *73*(3), 1795-1801.

[102] Özkaynak, F. (2017, September). From biometric data to cryptographic primitives: A new method for generation of substitution boxes. In *Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics* (pp. 27-33), doi: 10.1145/3143344.3143355.

[103] Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., & Liu, J. (2019). A novel block encryption algorithm based on chaotic S-box for wireless sensor network. *IEEE Access*, *7*, 53079-53090, doi: 10.1109/ACCESS.2019.2911395.

[104] Zhang, X., Zhao, Z., & Wang, J. (2014). Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Processing: Image Communication*, *29*(8), 902-913.

[105] Ahmad, M., Khan, P. M., & Ansari, M. Z. (2014, March). A simple and efficient key-dependent S-box design using fisher-yates shuffle technique. In *International Conference on Security in Computer Networks and Distributed Systems* (pp. 540-550). Springer, Berlin, Heidelberg.

[106] Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dynamics*, *82*(4), 1867-1877.

[107] Ahmad, M., Bhatia, D., & Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science*, *57*(2015), 572-580.

[108] Khan, M., & Shah, T. (2015). An efficient construction of substitution box with fractional chaotic system. *Signal, Image and Video Processing*, *9*(6), 1335-1338.

[109] Ahmad, M., & Malik, M. (2016, March). Design of chaotic neural network based method for cryptographic substitution box. In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)* (pp. 864-868). IEEE.

[110] Ahmad, M., Bhatia, D., & Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science*, *57*(2015), 572-580.

[111] Ahmad, M., Doja, M. N., & Beg, M. S. (2018). ABC optimization based construction of strong substitution-boxes. *Wireless Personal Communications*, *101*(3), 1715-1729.

[112] Lambić, D., Janković, A., & Ahmad, M. (2018). Security analysis of the efficient chaos pseudo-random number generator applied to video encryption. *Journal of Electronic Testing*, *34*(6), 709-715.

[113] Alzaidi, A. A., Ahmad, M., Ahmed, H. S., & Solami, E. A. (2018). Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. *Complexity*, *2018*.

[114] Özkaynak, F., Çelik, V., & Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. *Signal, Image and Video Processing*, *11*(4), 659-664.

[115] Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, *88*, 37-50.

[116] Ye, T., & Zhimao, L. (2018). Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dynamics*, *94*(3), 2115-2126, doi: 10.1007/s11071-018- 4478-5.

[117] Zahid, A. H., Arshad, M. J., & Ahmad, M. (2019). A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy*, *21*(3), 245.

[118] Tanyildizi, E., & Özkaynak, F. (2019). A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps. *IEEE Access*, *7*, 117829-117838, doi: 10.1109/ACCESS.2019.2936447

[119] https://www.nist.gov/publications/advanced-encryption-standard-aes, Erişim: 8 Ekim 2018.

[120] Kayış, H. (2006). *AES Uygulaması'nın FPGA Gerçeklerine Karşı Güç Analizi Saldırısı*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü

[121] Öztemür, M. (2012). *AES algoritmasının bir gerçeklemesine güç analizi saldırıları,* Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü

[122] http://satoh.cs.uec.ac.jp/SAKURA/hardware/SAKURA-G.html, Erişim: 10 Ocak 2020.

[123] http://www.rambus.com, Erişim: 21 Şubat 2020.
[124] http://www.riscure.com, Erişim: 15 Mart 2020.
[125] O'Flynn, C., & Chen, Z. D. (2014, April). Chipwhisperer: An open-source platform for hardware embedded security research. In *International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 243-260). Springer, Cham.
[126] https://wiki.newae.com/Press, Erişim: 14 Kasım 2019.
[127] Maghrebi, H., Portigliatti, T., & Prouff, E. (2016, December). Breaking cryptographic implementations using deep learning techniques. In *International Conference on Security, Privacy, and Applied Cryptography Engineering* (pp. 3-26). Springer, Cham.
[128] Bos, J. W., Hubain, C., Michiels, W., & Teuwen, P. (2016, August). Differential computation analysis: Hiding your white-box designs is not enough. In *International Conference on Cryptographic Hardware and Embedded Systems* (pp. 215-236). Springer, Berlin, Heidelberg.
[129] Belaïd, S., Coron, J. S., Fouque, P. A., Gérard, B., Kammerer, J. G., & Prouff, E. (2015, September). Improved side-channel analysis of finite-field multiplication. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 395-415). Springer, Berlin, Heidelberg.
[130] Pahlevanzadeh, H., Dofe, J., & Yu, Q. (2016, January). Assessing CPA resistance of AES with different fault tolerance mechanisms. In *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)* (pp. 661-666). IEEE.
[131] https://wiki.newae.com/Main_Page, Erişim: 3 Ocak 2020.
[132] Cusick, T. W., & Stanica, P. (2017). *Cryptographic Boolean functions and applications*. Academic Press.
[133] Nyberg, K. (1993, May). Differentially uniform mappings for cryptography. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 55-64). Springer, Berlin, Heidelberg.
[134] J. Daemen and V. Rijmen, ''AES proposal: Rijndael,'' in Proc. 1st Adv.Encryption Conf., CA, USA, 1998, pp. 1–45.
[135] Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, *92*(2), 305-313, 2018. doi: 10.1007/s11071-018-4056-x.
[136] Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, *31*(8), 3317-3326.
[137] Ma, S., Zhang, Y., Yang, Z., Hu, J., & Lei, X. (2019). A new plaintext-related image encryption scheme based on chaotic sequence. *IEEE Access*, *7*, 30344-30360.
[138] Özkaynak, F. (2019). Chaos based substitution boxes as a cryptographic primitives: Challenges and opportunities. *Chaotic Model. Simul.*, *1*, 49-57.
[139] Zhu, C., & Sun, K. (2018). Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps. *IEEE Access*, *6*, 18759-18770.
[140] Zhang, T., Chen, C. P., Chen, L., Xu, X., & Hu, B. (2018). Design of highly nonlinear substitution boxes based on I-Ching operators. *IEEE Transactions on Cybernetics*, *48*(12), 3349-3358.
[141] Ahmed, H. A., Zolkipli, M. F., & Ahmad, M. (2019). A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. *Neural Computing and Applications*, *31*(11), 7201-7210, doi: 10.1007/s00521-018-3557-3.
[142] Ye, T., & Zhimao, L. (2018). Chaotic S-box: six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. *Nonlinear Dynamics*, *94*(3), 2115-2126, doi: 10.1007/s11071-018-4478-5.
[143] Çavuşoğlu, Ü., Kaçar, S., Zengin, A., & Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. *Nonlinear Dynamics*, *92*(4), 1745-1759, doi: 10.1007/s11071-018-4159-4.

[144] Wang, X., Hou, Y., Wang, S., & Li, R. (2018). A new image encryption algorithm based on CML and DNA sequence. *Ieee Access*, *6*, 62272-62285.

[145] Guo, J. M., Riyono, D., & Prasetyo, H. (2018). Improved beta chaotic image encryption for multiple secret sharing. *IEEE Access*, *6*, 46297-46321.

[146] Wang, X., Zhu, X., & Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*, *6*, 23733-23746.

[147] Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access*, *6*, 67581-67593.

[148] Zhu, S., Zhu, C., & Wang, W. (2018). A novel image compression-encryption scheme based on chaos and compression sensing. *IEEE Access*, *6*, 67095-67107.

[149] Khan, M. A., Ali, A., Jeoti, V., & Manzoor, S. (2018). A chaos-based substitution box (S-Box) design with improved differential approximation probability (DP). *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, *42*(2), 219-238, doi: 10.1007/s40998-018-0061-9.

[150] Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication*, *2*(2), 181-191.

[151] Altaf, M., Ahmad, A., Khan, F. A., Uddin, Z., & Yang, X. (2018). Computationally efficient selective video encryption with chaos based block cipher. *Multimedia Tools and Applications*, *77*(21), 27981-27995, doi: 10.1007/s11042-018-6022-5.

[152] Wang, X., Akgul, A., Cavusoglu, U., Pham, V. T., Vo Hoang, D., & Nguyen, X. Q. (2018). A chaotic system with infinite equilibria and its S-box constructing application. *Applied Sciences*, *8*(11), 2132, doi: 10.3390/app8112132.

[153] Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *Applied Sciences*, *8*(12), 2650, doi: 10.3390/app8122650.

[154] Al Solami, E., Ahmad, M., Volos, C., Doja, M. N., & Beg, M. M. S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes. *Entropy*, *20*(7), 525, doi: 10.3390/e20070525.

[155] Diab, H. (2018). An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. *IEEE Access*, *6*, 42227-42244.

[156] Belazi, A., & El-Latif, A. A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, *130*, 1438-1444.

[157] Belazi, A., El-Latif, A. A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, *88*, 37-50.

[158] Belazi, A., Khan, M., El-Latif, A. A. A., & Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. *Nonlinear Dynamics*, *87*(1), 337-361.

[159] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics*, *87*(2), 1081-1094.

[160] ul Islam, F., & Liu, G. (2017). Designing S-box based on 4D-4wing hyperchaotic system. *3D Research*, *8*(1), 9.

[161] Özkaynak, F. (2017, September). From biometric data to cryptographic primitives: A new method for generation of substitution boxes. In *Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics* (pp. 27-33), doi: 10.1145/3143344.3143355.

[162] Ye, G., & Huang, X. (2015). An image encryption algorithm based on autoblocking and electrocardiography. *IEEE MultiMedia*, *23*(2), 64-71.

[163] Wang, Q., Yu, S., Li, C., Lü, J., Fang, X., Guyeux, C., & Bahi, J. M. (2016). Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *63*(3), 401-412.

[164] Ahmad, J., & Hwang, S. O. (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms. *Nonlinear Dynamics*, *82*(4), 1839-1850, doi: 10.1007/s11071-015-2281-0.

[165] Seyedzadeh, S. M., Norouzi, B., Mosavi, M. R., & Mirzakuchaki, S. (2015). A novel color image encryption algorithm based on spatial permutation and quantum chaotic map. *Nonlinear Dynamics*, *81*(1-2), 511-529, doi: 10.1007/s11071-015-2008-2.

[166] Zaibi, G., Peyrard, F., Kachouri, A., Fournier-Prunaret, D., & Samet, M. (2014). Efficient and secure chaotic S-Box for wireless sensor network. *Security and Communication Networks*, *7*(2), 279-292.

[167] Zhang, X., Zhao, Z., & Wang, J. (2014). Chaotic image encryption based on circular substitution box and key stream buffer. *Signal Processing: Image Communication*, *29*(8), 902-913.

[168] Özkaynak, F., & Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. *Nonlinear Dynamics*, *74*(3), 551-557, doi: 10.1007/s11071-013-0987-4.

[169] L. Dragan and ö. Miodrag, ‘‘Comparison of random S-box generation methods,’’ *Publications l’Inst. Math.*, vol. 93, no. 107, pp. 109–115, 2013. doi: 10.2298/PIM1307109L.

[170] Khan, M., & Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Computing and Applications*, *29*(4), 993-999, doi: 10.1007/s00521-016-2511-5.

EKLER

EK- 1: Chipwhispere CW1173 Datasheet CD-ROM

ÖZGEÇMİŞ

Mehmet Şahin AÇIKKAPI

KİŞİSEL BİLGİLER

Doğum Yeri : Elazığ
Doğum Yılı : 1982
Uyruğu : TC
Adres : Munzur Üniversitesi Tunceli M.Y.O Merkez/Tunceli
E-posta : mehmetacikkapi@gmail.com
Yabancı Diller : İngilizce ÜDS: 66.25

EĞİTİM BİLGİLERİ

Yüksek Lisans :"Mobil aygıtlar için tek kullanımlık şifre üretilmesi ve güvenliğinin sınanması" Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yazılım Anabilim Dalı, 2011
Danışman: Prof.Dr. A. Bedri ÖZER

Lisans : Fırat Üniversitesi, Müh. Fakültesi, Bilgisayar Mühendisliği Bölümü, 2005

Lise : Elazığ M.Akif ERSOY Lisesi, Elazığ, 1999

ARAŞTIRMA DENEYİMİ

- ✓ Altera DE-2-115 FPGA Development and Education Board, Chipwhisperer-Lite CW1173
- ✓ C-C++, C#, Coldfusion, Html, Php

İŞ DENEYİMİ

2009 – ... : Munzur Üniversitesi Tunceli M.Y.O

AKADEMİK FAALİYETLER

Makaleler:

1. Açikkapi, M. Ş., Özkaynak, F., & Özer, A. B. (2019). Side-channel analysis of chaos-based substitution box structures. *IEEE Access*, *7*, 79030-79043.

Bildiriler:

1. Turgut, Y. E., Aslan, A., Göksu, İ., & Açıkkapı, M. Ş. (2017). Meslek Yüksekokulu Öğrencilerinin İnternet Bağımlılığı Düzeyleri. 11th International Computer and Instructional Technology Symposium, Malatya, 24-26 May.
2. Turgut, Y. E., Göksu, İ., Aslan, A., & Açıkkapı, M. Ş. (2017). Ön Lisans Öğrencilerinin BT Yönelik Tutumları ve Yeterlilik Düzeyleri. 11th International Computer and Instructional Technology Symposium, Malatya, 24-26 May.
3. Açikkapi, M. Ş., & Özer, A. B. (2018). Strentening the Encoding Algoritmhs in Embedded Systems to Side Channel Attacks. 3rd Internetional Conference on Computational Mathemativs and Engineering Sciences, Girne-Cyprus, 4-6 May.

Projeler:

1. MF.16.66 nolu BAP Projesi, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi