T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK ve FEN BİLİMLERİ ENSTİTÜSÜ

FARKSAL GÜÇ ANALİZİ SALDIRILARINA DAYANIKLI DÖNGÜSEL SİMETRİK S-KUTULARININ TASARIMI

MUHAMMET ALİ EVCİ
YÜKSEK LİSANS TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2014

T.C.
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ
MÜHENDİSLİK ve FEN BİLİMLERİ ENSTİTÜSÜ

FARKSAL GÜÇ ANALİZİ SALDIRILARINA DAYANIKLI DÖNGÜSEL SİMETRİK S-KUTULARININ TASARIMI

MUHAMMET ALİ EVCİ
YÜKSEK LİSANS TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
DR. SELÇUK KAVUT

GEBZE
2014

GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ	YÜKSEK LİSANS JÜRİ ONAY FORMU

GYTE Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 09/06/2014 tarih ve 2014/35 sayılı kararıyla oluşturulan jüri tarafından 11/06/2014 tarihinde tez savunma sınavı yapılan Muhammet Ali EVCİ'nin tez çalışması Elektronik Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : Öğr. Gör. Dr. Selçuk KAVUT

ÜYE : Yrd. Doç. Dr. Hasari ÇELEBİ

ÜYE : Yrd. Doç. Dr. Serdar Süer ERDEM

ONAY

GYTE Mühendislik ve Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..... tarih ve ...../..... sayılı kararı.

İMZA/MÜHÜR

ÖZET

Yan kanal analizi (YKA), kriptografik algoritmaların gerçeklendiği FPGA gibi donanımsal yapılarda, sıcaklık, zamanlama işlemleri, güç tüketimi ve elektromanyetik radyasyon gibi sızıntılara dayanmaktadır. Bazı yan kanal metotları, kriptografik algoritmaların fiziksel gerçeklenmesine saldırma olanağı sağlar. Saldırgan, şifreleme ve çözme işlemleri esnasında kriptografik algoritmanın fiziksel gerçeklemesinden sızan bilgiyi kullanır. Bu türden yan kanal saldırıları, algoritmaları güvensiz hale getirmektedir. Yan kanal saldırıların en güçlü biçimlerinden bir tanesi de Farksal Güç Analizidir (FGA). FGA atağı, kriptosistemin güç tüketiminden kazanılan bilgiye dayalı olarak gerçekleştirilir.

Tez kapsamında, en dik iniş prensibine dayalı arama algoritması ile 8x8 Döngüsel Simetrik S-kutuları (DSSK) sınıfında aramalar gerçekleştirilmiş ve doğrusal olmama değeri 104, farksal birbiçimliliği 6 ve saydamlık derecesi ile FGA sinyal gürültü oranı AES S-kutusundan oldukça iyi S-kutuları elde edilmiştir.

AES gerçeklemesi için SASEBO-GII kartı kullanılmış ve osiloskop vasıtasıyla alınan güç ölçümleriyle FGA uygulanmıştır. FGA saldırısında güç tüketimi ile AES'in son turundaki giriş ve çıkış baytları arasındaki Hamming mesafesinin korelasyonu kullanılmıştır. Elde edilen sonuçlar, tahmin entropisi ve başarı oranı gibi metriklerle ifade edilmiştir. Arama algoritması ile elde edilen en iyi kriptografik özelliklere sahip DSSK'lardan 4 tanesi, AES S-kutusu ve lineer bir S-kutusu SASEBO-GII kartı üzerinde gerçeklenerek, FGA saldırısı karşısındaki dayanıklılıkları tahmin entropisi ve başarı oranı gibi YKA güvenlik metrikleri kullanılarak karşılaştırılmıştır.

Deneysel olarak FGA atağının yapılmasının yanında her bir S-kutusu için simülasyonla güç ölçümleri üretilerek FGA saldırısı gerçekleştirilmiştir. Simülasyon sonuçları, deneysel verilerle karşılaştırılmıştır.

Anahtar Kelimeler: Döngüsel Simetrik S-kutusu (DSSK), Saydamlık Derecesi, Farksal Birbiçimlilik, Doğrusal Olmama, Farksal Güç Analizi (FGA), SASEBO-GII, Başarı Oranı, Tahmin Entropisi, FPGA.

SUMMARY

A cryptographic algorithm implemented on FPGAs leaks data sensitive information through side channels such as time taken for computations, temperature, power consumption etc. Some side-channel methods enable to attack the physical implementation of cryptographic algorithms. An attacker uses the information leaked from the physical implementation of cryptographic algorithm during encryption or decryption. One of the most powerful forms of the side channel attacks (SCAs) is Differential Power Analysis (DPA). DPA attack is based on the information gained from the power consumption of cryptosystem.

In this thesis, we perform a steepest-descent-like iterative search algorithm in the class of 8×8 Rotation Symmetric S-Boxes (RSSB) and attain S-boxes which, while achieving transparency orders and DPA signal-to-noise ratios (SNR) noticeably better than those of AES S-box, have nonlinearity 104 and differential uniform 4.

We use SASEBO-GII board for the implementation of AES and carry out DPA exploiting the power traces acquired by means of an oscilloscope. In our DPA attack, we use the correlation of the power consumption with Hamming distance between the input and output bytes of the last round of AES. Implementing the four RSSBs with the best attained cryptographic properties, found by search algorithm, the AES S-box, and a linear S-box (used for comparison purpose) on SASEBO-GII, their resistivity against DPA attacks are compared using SCA security metrics such as success rate and guessing entropy.

In addition to DPA attack performed experimentally, we simulate DPA attack by generating power traces. Then, the simulation results are compared with the experimental results.

Key Words: Rotation Symmetric S-Box (RSSB), Transparency Order, Differential Uniformity, Nonlinearity, Differential Power Analysis (DPA), SASEBO-GII, Success Rate, Guessing Entropy, FPGA.

TEŞEKKÜR

Tez çalışmamda benden yardımlarını esirgemeyen ve sürekli yol gösteren saygıdeğer hocam Öğr. Gör. Dr. Selçuk Kavut'a,

Tez çalışmam sırasındaki yardımlarından dolayı TUBİTAK BİLGEM OKTEM laboratuvarı araştırmacı arkadaşlarıma,

Ölçüm alma altyapısı oluşturulmasındaki desteklerinden dolayı Melik Yücel'e,

Anlayış ve sabırlarından dolayı aileme ve dualarını her zaman yanımda hissettiğim anneme ve babama şükranlarımı sunarım.

İÇİNDEKİLER

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Kısaltmalar		**Açıklamalar**
AES	:	Advanced Encryption Standard
ANF	:	Algebraic Normal Form
CMOS	:	Complementary-Metal-Oxide-Semiconductor
CPA	:	Correlation Power Analysis
DES	:	Data Encryption Standart
DPA	:	Differential Power Analysis
DSSK	:	Döngüsel Simetrik S-kutusu
EEPROM	:	Electrically Erasable Programmable Read Only Memory
FPGA	:	Field Programmable Gate Array
GAC	:	Global Avalanche Characteristic
GE	:	Guessing Entropy
HW	:	Hamming Weight
NIST	:	National Institute of Standards and Technology
PROM	:	Programmable Read Only Memory
PTT	:	Polarity Truth Table
SASEBO	:	Side Channel Attacks Standart Evaluation Board
SPA	:	Simple Power Analysis
SR	:	Success Rate
TO	:	Transparency Order
TT	:	Truth Table
USB	:	Universal Serial Bus

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

1. GİRİŞ

Çoğu blok şifreleme kriptosistemlerinde, tek doğrusal olmayan bileşenler S-kutuları olmaktadır ve bu kriptosistemlerin gücü ağırlıklı olarak S-kutularının kriptografik özelliklerine dayanmaktadır. S-kutularının doğrusal olmama, farksal birbiçimlilik ve cebirsel derece gibi geleneksel özellikleri, kriptografik kriptosistemin donanımsal tasarımından bağımsız olmakla birlikte sırasıyla lineer [1], farksal [2] ve yüksek mertebeden farksal [3] kriptanalizine karşı direncini gösterir.

Diğer taraftan, yan kanal analizi (YKA); zamanlama işlemleri [18], güç tüketimi [4] ve elektromanyetik radyasyon [5] gibi donanımsal sızıntılara dayanmaktadır ve kullanılan kriptografik bileşenler YKA'ya karşı da dayanıklı olmalıdırlar. Bu kapsamda, bir S-kutusunun YKA'ya karşı dayanıklılığı [6]'da ele alınmış ve *saydamlık derecesi* ile ilişkilendirilmiştir. Yüksek saydamlık derecesine sahip S-kutularının FGA saldırılarına karşı daha zayıf oldukları [6]'da gösterilmiştir. Claude Carlet [7]'de AES'deki S-kutusu gibi bazı S-kutuların çok kötü saydamlık derecesine sahip olduğunu göstermiştir. Bununla birlikte, henüz düşük saydamlık derecesine sahip olup aynı zamanda da yüksek doğrusal olmama, düşük farksal birbiçimlilik ve yüksek cebirsel dereceye sahip S-kutularını elde eden teorik bir inşa yöntemi yoktur. Yakın zamanda sınırlı rastgele arama yapılarak AES S-kutusundan daha düşük saydamlık derecesine sahip 8x8'lik S-kutuları bulunmuştur [8]. Bunun ardından, Döngüsel Simetrik S-kutuları (DSSK) sınıfında aramalar yapılarak, [8]'de bulunan saydamlık dereceleri ve doğrusal olmama sonuçları geliştirilmiştir [9]. Ardından, [10]'da genetik algoritmalar kullanılarak [8] ve [9]'da bulunanlardan daha iyi saydamlık derecesine sahip S-kutuları elde edilmiştir. Bu tez kapsamında da saydamlık derecesiyle beraber doğrusal olmama, farksal birbiçimlilik ve mutlak gösterge gibi geleneksel kriptografik özellikleri daha iyi olan S-kutuları aranmış ve elde edilen sonuçlar literatürdekiler ile karşılaştırılmıştır.

En dik iniş prensibine dayalı bir algoritma [11] ile 8×8 DSSK sınıfında aramalar gerçekleştirilerek, geleneksel kriptografik özellikleriyle beraber saydamlık derecesi bakımından literatürde bulunanlardan [8, 9, 10] üstün olan S-kutuları bulunmuştur.

Verilog ile yazılan AES algoritması, SASEBO-GII (Standart Yan Kanal Saldırısı Değerlendirme Kartı) kullanılarak gerçeklenmiş ve FGA atağı

gerçekleştirilmiştir [4]. Bununla birlikte, bulunan DSSK'lardan en iyi kriptografik özelliklere sahip olan dört tanesi ve karşılaştırma amaçlı kullandığımız lineer bir S-kutusu da AES S-kutusu ile değiştirilerek SASEBO-GII'de gerçeklenmiş ve FGA saldırısı gerçekleştirilmiştir.

Tezin diğer bölümleri şu şekilde organize edilmiştir. Bölüm 2'de S-kutularının saydamlık derecesi, FGA sinyal gürültü oranı ve geleneksel kriptografik özelliklerinin tanımlarına yer verilmiştir. 8x8'lik S-kutularının aranması Bölüm 3'de yer alırken, yan kanal analizi saldırılarından ve tahmin entropisi (GE), başarı oranı (SR) gibi farksal güç analizi güvenlik metriklerinden Bölüm 4'de bahsedilmiştir. Bölüm 5'de AES işleminden bahsedildikten sonra, Bölüm 6'da ölçüm alma düzeneğinden ve FPGA konfigürasyonundan bahsedilmiştir. DSSK'ların ve lineer S-kutusunun AES S-kutusu olarak gerçeklenmesi, bu gerçeklemelerin korelasyon güç analizi Bölüm 6'da, yapılan simülasyon sonuçlarıyla karşılaştırılması ise Bölüm 7'de yer almaktadır.

2. S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİ

2.1. (Kutupsal) Doğruluk Tablosu

Bir Boole fonksiyonu f , F_2^n den F_2 ye bir gönderim olarak tanımlanır. *n*-bit girişli ve *m*-bit çıkışlı S-kutusu $F: F_2^n \to F_2^m$ gönderimi olarak tanımlanır. Bu gönderim $m = 1$ için *n*-değişkenli Boole fonksiyonu olarak isimlendirilir. S-kutusu $F, x \in F_2^n$ olmak üzere *n*-değişkenli Boole fonksiyonlarının bir kombinasyonu $F(x) = (f_0(x), \dots, f_{m-1}(x))$ olarak düşünülebilir. *F*'nin f_i fonksiyonları koordinat fonksiyonları, bu fonksiyonların sıfırdan farklı lineer kombinasyonları ise komponent fonksiyonları olarak isimlendirilir. Bu bölümde tanımladığımız kriptografik özellikler, bir bit çıkışlı Boole fonksiyonları için tanımlanan kriptografik özelliklerin *n*-bit çıkışlı S-kutularına genişletilmesi olarak düşünülebilir.

Bir bit çıkışlı Boole fonksiyonu $f(x)$ aşağıdaki gibi doğruluk tablosu ile gösterilebilir.

$$f(x) = (f(00..00), f(00..01)....., f(11..11)) \tag{2.1}$$

Diğer bir ifadeyle, *n*-değişkenli Boole fonksiyonu *f*'nin doğruluk tablosu 2^n-bitten oluşan bir vektördür.

Kutupsal doğruluk tablosu ise $g(x) = (-1)^{f(x)} = 1 - 2f(x)$ fonksiyonu ile tanımlanır ve $g = ((-1)^{f(00..01)}, \dots, (-1)^{f(11..11)})$ olarak verilir.

2.2. Cebirsel Normal Biçim (CNB)

Bir $f: F_2^n \to F_2$ Boole fonksiyonunu temsil etmenin diğer bir yolu da polinomsal bir gösterim yöntemi olan cebirsel normal biçimidir ve (2.2) ifadesindeki gibi gösterilebilir.

$$
\begin{aligned}
f(x) = f(x_1, x_2, \ldots, x_n) &= \sum_{u \in F_2^n} a_u \left(\prod_{i=1}^{n} x^{u_i} \right) \\
&= \sum_{u \in F_2^n} a_u x^u \qquad a_u \in F_2 \\
&= a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \oplus a_{12} x_1 x_2 \\
&\quad \oplus \ldots \oplus a_{(n-1)n} x_{(n-1)} x_n \oplus a_{123} x_1 x_2 x_3 \\
&\quad \oplus \ldots \oplus a_{123\ldots n} x_1 x_2 x_3 \ldots x_n
\end{aligned}
\tag{2.2}
$$

2.3. Cebirsel Derece

Bir $f: F_2^n \to F_2$ Boole fonksiyonunun cebirsel derecesi $\deg(f)$ ya da kısaca d ile gösterilir. f Boole fonksiyonunun cebirsel derecesi CNB gösterimindeki terimlerin sahip olduğu en yüksek değişken sayısıdır. Bir S-kutusu $F: F_2^n \to F_2^m$ için ise cebirsel derece, koordinat fonksiyonlarının cebirsel derecelerinin en büyüğü olarak tanımlanır.

Kriptografik fonksiyonların, iyi karıştırma özelliğine sahip olabilmesi için yüksek cebirsel dereceye sahip olmaları gerekir. Derecesi en fazla 1 olan Boole fonksiyonları afin fonksiyonları olarak adlandırılır. Sabit terimi sıfıra eşit olan afin fonksiyonlara ise lineer fonksiyonlar denir.

2.4. Doğrusal Olmama

n-değişkenli bir f Boole fonksiyonunun Walsh-Hadamard dönüşümü $W_f: \{0,1\}^n \to [-2^n, 2^n]$, aşağıdaki eşitlikle tanımlanır.

$$
W_f(w) = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{w \cdot x} \tag{2.3}
$$

Burada $w \cdot x = x_0 w_0 \oplus x_1 w_1 \oplus \ldots \oplus x_{n-1} w_{n-1}$, $x = (x_0, \ldots, x_{n-1})$ ve $w = (w_0, \ldots, w_{n-1})$ vektörlerinin iç çarpımıdır.

n-değişkenli bir f fonksiyonunun doğrusal olmama değeri, *n*-değişkenli afin fonksiyonlara olan Hamming mesafelerinin minimumudur. Walsh spektrumu kullanılarak doğrusal olmama ölçütü şu şekilde ifade edilebilir.

$$NL_f = \frac{1}{2}\left(2^n - \max_{w \in \{0,1\}^n} |W_f(w)| \right) \tag{2.4}$$

S-kutuları için doğrusal olmama değeri, komponent fonksiyonlarının doğrusal olmama değerlerinin en küçüğü olarak tanımlanır. Bir S-kutusunun lineer kriptanaliz [1] karşısında dayanıklı olması için doğrusal olmama değerinin yüksek olması beklenir.

2.5. Mutlak Gösterge

Bir S-kutusu $F(x) = (f_1(x), \dots, f_n(x))$ için koordinat fonksiyonu $f_i(x)$'in oto-korelasyon fonksiyonu, girişine $\alpha \in F_2^n$ farkı uygulandığında elde edilen versiyonu ile kendisi arasındaki korelasyon olarak tanımlanır ve aşağıdaki eşitlikte verilir.

$$\Delta_{f_i}(\alpha) = \sum_{x \in F_2^n} (-1)^{f_i(x) \oplus f_i(x \oplus \alpha)}. \tag{2.5}$$

S-kutusu $F: F_2^n \to F_2^m$ için ise, $v \in F_2^m$ olmak üzere, oto-korelasyon fonksiyonu aşağıdaki gibi tüm komponent fonksiyonları için genelleştirilebilir.

$$r_F(a, v) = \sum_{x \in F_2^n} (-1)^{v \cdot (F(x) \oplus F(x \oplus a))}. \tag{2.6}$$

Oto-korelasyon spektrumuyla ilgili olarak global çığ etkisi karakteristiği [25] olarak adlandırılan iki önemli kriptografik ölçüt vardır. Oto-korelasyon spektrumunun $(a, v) = ((0, 0, \dots, 0), (0, \dots, 0))$ hariç alacağı maksimum mutlak değer, mutlak gösterge olarak adlandırılır ve şu şekilde ifade edilir:

$$\Delta_F = \max_{\substack{a \in F_2^{n^*} \\ v \in F_2^{n^*}}} |r_F(a, v)|. \tag{2.7}$$

Diğer ölçüt ise kareler toplamı göstergesi olarak bilinir ve aşağıdaki gibi ifade edilir:

$$\sigma_F = \sum_{\alpha \in F_2^m} \sum_{v \in F_2^n} r_F^2(a, v). \tag{2.8}$$

Kriptografik fonksiyonların iyi yayılma özelliklerini sağlayabilmesi için bu iki ölçütün düşük değerler alması önemlidir.

2.6. Farksal Birbiçimlilik

Bir $n \times m$ S-kutusu F'nin farksal birbiçimliliği δ, $\gamma \neq (0,0,\ldots,0)$ olmak üzere $F(x) \oplus F(x \oplus \gamma) = \beta$ eşitliğini sağlayan çözümlerin maksimum sayısı olarak tanımlanmıştır [12].

Bir S-kutusunun farksal kriptanaliz karşısında dayanıklı olabilmesi için, farksal birbiçimlilik değerinin düşük olması gerekir.

2.7. Saydamlık Derecesi

Saydamlık derecesi, [6]'da FGA'ya karşı S-kutularının dayanıklılığını gösteren bir metrik olarak tanımlanmıştır. Bir S-kutusu $F: F_2^n \rightarrow F_2^m$ için $HW(.)$ Hamming ağırlığını göstermek üzere ve $R = |m - 2HW(\beta)|$ olmak üzere saydamlık derecesi aşağıdaki eşitlikle ifade edilir:

$$\tau_F = \max_{\beta \in F_2^m} \left(R - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n^*}} \left| \sum_{\substack{v \in F_2^m \\ HW(v)=1}} (-1)^{v \cdot \beta} r_F(a,v) \right| \right) \tag{2.9}$$

[6]'da belirtildiği gibi, bir S-kutusunun FGA karşısında dayanıklı olabilmesi için saydamlık derecesi değerinin düşük olması gerekir. Bununla birlikte, aynı çalışmada lineer S-kutuları için saydamlık derecesinin düşük iken, en yüksek doğrusal olmama değerine sahip S-kutuları için ise saydamlık derecesinin yüksek olduğu gösterilmiştir.

[13]'de ise saydamlık derecesinin $\beta = (0,\ldots,0)$ veya $\beta = (1,\ldots,1)$ iken her zaman en yüksek değeri verdiği ve bu yüzden tanımdaki β parametresinin bir fazlalık olduğu gösterilmiştir. Ayrıca, saydamlık derecesinin [6]'daki tanımında, koordinat fonksiyonları arasındaki bazı çapraz korelasyon terimlerinin sıfır kabul edildiği ve bunun genelde doğru olmadığı iddia edilmiştir. Buradan yola çıkılarak, çapraz

korelasyon terimlerini de kapsayacak şekilde saydamlık derecesi aşağıdaki gibi yeniden tanımlanmıştır.

$$\underline{\tau}_F = \max_{\beta \in F_2^m} \left(m - \frac{1}{2^{2n} - 2^n} \sum_{a \in F_2^{n^*}} \sum_{j=1}^{m} \left| \Delta_{f_j}(a) + J \right| \right) \tag{2.10}$$

Bu tanımdaki $J = \sum_{\substack{i=1 \\ j \neq i}}^{m} (-1)^{\beta_i \oplus \beta_j} C_{f_i, f_j}(a)$ ve $C_{f_i, f_j}(u)$, koordinat fonksiyonları $f_i(x)$ ile $f_j(x)$ arasındaki çapraz korelasyondur ve aşağıdaki eşitlikle verilir:

$$C_{f_i, f_j}(a) = \sum_{x \in F_2^n} (-1)^{f_i(x) \oplus f_j\left(x \oplus \alpha\right)} \tag{2.11}$$

2.8. Sinyal Gürültü Oranı

Bir S-kutusunun tek bitli FGA saldırıları karşısındaki dayanıklılığını ölçen diğer bir parametre de FGA sinyal gürültü oranı (SNR)'dır. Kriptografik cihazdan elde edilen güç ölçümleri gürültü olmasa bile, yanlış anahtarlar için dahi oluşan ikincil tepeler doğru tepenin belirlenememesine yol açabilmektedir. İkincil tepelerin gürültü olarak modellenerek S-kutusu $F: F_2^n \rightarrow F_2^m$ için FGA SNR'ı aşağıdaki eşitlikle ifade edilir [14]:

$$SNR(FGA) = m\, 2^{2n} \left(\sum_{w \in 2^n} \left(\sum_{i=1}^{m} W_{f_i}(w) \right)^4 \right)^{-1/2} \tag{2.12}$$

3. 8×8 DÖNGÜSEL SİMETRİK S-KUTULARININ ARANMASI

3.1. Döngüsel Simetrik S-kutusu

$$\rho^k(x_0, x_1, \dots, x_{n-1}) = (x_{0+k\ (mod\ n)}, x_{1+k\ (mod\ n)}, \dots, x_{n-1+k\ (mod\ n)})$$

k-döngüsel kaydırma operatörü olsun. Eğer bir S-kutusu F, $\rho^k\big(F(x)\big) = F(\rho^k(x))$ eşitliği $\forall x = (x_0, x_1, \dots, x_{n-1}) \in F_2^n$ ve $k \in \{1, .., n\}$ için sağlanıyorsa S-kutusu F'ye Döngüsel Simetrik S-kutusu (DSSK) denir. F, sonlu cisim F_{2^n} için bir normal baz kullanılarak $s: F_{2^n} \to F_{2^n}$ 'den elde edilmiş olsun. [15]'de gösterildiği gibi, $\forall \alpha \in F_{2^n}$ için $\big(s(\alpha)\big)^2 = s(\alpha^2)$ koşulunu sağlayan S-kutuları döngüsel-simetrik S-kutularına karşılık gelmektedir.

$x \in F_2^n$'in yörüngesi, döngüsel permütasyon altında $G(x) = \{\rho^k(x) \mid 1 \leq k \leq n\}$ seti olarak tanımlanır. g_n toplam yörüngelerin sayısı olsun. Burnside lemması kullanılarak ve $\varphi(t)$, Euler *phi*-fonksiyonu olmak üzere $g_n = \frac{1}{n}\sum_{t|n} \varphi(t) 2^{\frac{n}{t}} (\approx \frac{2^n}{n})$ olduğu gösterilebilir [16]. Sözlüksel olarak, $1 \leq i \leq g_n$ olmak üzere $i.$ yörüngenin ilk elemanına yörünge temsilcisi denir ve $\wedge_i$ ile gösterilir.

3.2. DSSK'ların Aranması

8x8 DSSK'lar, [11]'te sunulmuş olan en dik iniş prensibine dayalı arama algoritması ile aranmıştır. Arama algoritması her yinelemede aşağıdaki maliyet fonksiyonunu minimize etmeye çalışmaktadır:

$$Maliyet(S) = \frac{A}{(g_n - 1)(2^{4n} - 2^{3n})} \sum_{i=1}^{g_n - 1} \sum_{\omega \in F_2^n} (W_S^2(\omega, \wedge_i) - 2^n)^2 + \frac{1}{n}\tau_S \tag{3.1}$$

Burada $\wedge_i \in F_2^n$, sıfırdan farklı yörünge temsilcisidir. $W_S(\omega, \wedge_i)$ ise $\wedge_i S(x)$ komponent fonksiyonunun Walsh-Hadamard dönüşümüdür. Maliyet fonksiyonundaki A değişkeni, ayarlama parametresi olarak kullanılmaktadır. Bu parametre doğrusal olmama ve saydamlık derecesi arasında dengeyi sağlamak için

kullanılır. Yürüttüğümüz aramalarda A parametresi 40 ile 120 arasında değerler almıştır. Eşitliğin sağ tarafındaki iç toplam, hataların karelerinin toplamı olarak isimlendirilmektedir [17] ve doğrusal olmama değeri en yüksek olan fonksiyonun Walsh transformuna olan uzaklığının bir ölçüsüdür. $\sum_{a\neq(0,\ldots,0)} {r_s}^2(\alpha, \wedge_i) = 2^{-n}\sum_w (W_s^2(w, \wedge_i) - 2^n)^2$ olduğu [17]'da gösterilmiştir. Buradan görülmektedir ki, eğer Boole fonksiyonu f afin bir fonksiyon ise hataların karelerinin toplamı en çok $2^{4n} - 2^{3n}$ değerini alabilmektedir. [24]'de de belirtildiği gibi herhangi bir $1 \leq k < n$ değer için $\wedge_i S(x)$ komponent fonksiyonu lineer olarak $\rho^k(\wedge_i)S(x)$ fonksiyonuna eşdeğerdir. Dolayısıyla hataların karelerinin toplamı, $\wedge_i$'nin döngüsel permütasyonu altında değişmemektedir. Bundan dolayı, $i = 1,2,\ldots, g_n \; için \wedge_i \in F_2^n$ olmak üzere sadece sıfırdan farklı yörünge temsilcilerine karşılık gelen $\wedge_i S(x)$ komponent fonksiyonları hesaba katılmıştır.

En dik iniş prensibine dayalı arama algoritması ile 8x8 DSSK'lar sınıfında bulduğumuz en iyi doğrusal olmama değeri 104 olmuştur. Bundan dolayı genellikle doğrusal olmama değeri 104 olan DSSK'lar ile çalışılmıştır.

Şekil 3.1'de literatürde bilinen S-kutuları ve AES S-kutusu ile bu çalışmada bulduğumuz en iyi kriptografik özelliklere sahip DSSK'lar karşılaştırılmıştır. Bulunan DSSK'lar, DSSK #1, DSSK #2, DSSK #3, DSSK #4 olarak adlandırılmıştır. Elde edilen sonuçlar, doğrusal olmama değeri 104 ve saydamlık derecesi ≥ 7.31 olarak [12, 13, 15]'den daha iyi kriptografik özelliklere sahip olduğu görülmektedir.

DSSK #1'in farksal birbiçimliliğinin AES S-kutusuna en yakın olduğu ve DSSK #4'ün saydamlık derecesinin AES S-kutusundan çok daha iyi olduğu gözükmektedir.

	Doğrusal Olmama	Farksal Birbiçimlilik	Mutlak Gösterge	Cebirsel Derece	Saydamlık Derecesi τ_F	Saydamlık Derecesi $\tau_{\underline{F}}$	SNR
AES S-Kutusu	112	4	32	7	7.86	6.92	9.56
[12]'deki S-Kutusu	98	-	≥88	7	≥7.78	-	≥8.54
[15]'deki S-Kutusu	98 100	12 12	104 104	7 7	7.358 7.53	-	5.825 5.44
[13]'deki S-Kutusu	102	8, 10, 12	80, 88, 96	7	≥ 7.76	-	-
DSSK#1	104	6	80	7	7.627	6.87	4.67
DSSK#2	104	8	88	7	7.555	6.93	7.04
DSSK#3	104	8	72	7	7.476	6.66	9.15
DSSK#4	102	8	88	7	7.31	6.53	11.78
Lineer S-Kutusu	0	256	256	1	5.83	0	2.83

Şekil 3.1: Literatürdeki S-kutuları ile bulduğumuz DSSK'ların karşılaştırması.

Tablo 3.1, Tablo 3.2, Tablo 3.3 ve Tablo 3.4'de sırasıyla bulduğumuz DSSK #1, DSSK #2, DSSK #3, DSSK #4 S-kutularının değerleri yer almaktadır. Ayrıca karşılaştırma amaçlı olarak kullandığımız lineer bir S-kutusu da verilmektedir.

Tablo 3.1: DSSK #1'in heksadesimal değerleri.

DSSK #1	00C081B2031565E506132AE8CA2CCB5D 0C77269D5472D14195CF581B975ABADB 1862EEF94C0F3B19A878E480A3A9829E 2BD99F22B05B366E2FC8B42E75E3B71A 3045C40BDD9CF39698C31E6A76D632F8 5127F0B5C9AA01254704537D05943D38 561DB3633F1044C5614DB6AF6CF5DC12 5E1491E669525C66EAF4C7906FE034BF 60598AF2897416AEBBCE39A0E78D2DED 31FC878C3C40D44FEC11AD376417F10D A2854E4BE1356B7C93DA559202BE4A1C 8EB108E2A6D7FA090A7329337A4870DF AC793A576750C6F67E4620A7889B8B86 C2A59A3E6D495F0ED871EB84B99924EF BCAB287B23D3CD43D21FA407B842CCF7 D5BDE9A18F8321FBDED0C1FD68FE7FFF]

Tablo 3.2: DSSK #2 ve DSSK #3'ün heksadesimal değerleri.

DSSK #2	0072E495C9482BFC93F0905A564FF954 2766E11F21B1B4C8AC579E76F303A8AF 4E1ECCEAC3013E074208639B69979114 59F1AE883DB6EC5CE73806A6514A5F61 9C123CD3996CD5C0874002E57CAD0E92 841B106BC6AA37EFD2DC2F1A23BF28D1 B24BE3CE5D7311D47ABC6D43D968B86F CF8C70C50CFE4D77A2A0947BBE47C24C 39CA247E782DA72A338FD864AB3B81D7 0F75808304CDCB0AF8445B2E1C5325B0 09E9366020F2D6498DB555F76E0DDFE8 A567B96A5EA134B746E27FBB50BDA326 653F9615C7329DEBBAC1E6052217A958 F43079A4DAFB8674B335D0DB71DDDE13 9F8A19F5E0828B2C1852FD3A9AEDEE89 45FA4116291DF6C47D0B8E62853198FF
DSSK #3	00E2C54C8BED988D17FADB48313F1B9B 2E66F559B72D9091629E7E6A36BA37DF 5C5FCCD3EBE3B2876F1F5A1D21B02393 C4953DDDFCB6D4416C3C75106E2FBF03 B87BBECF994BA7AED7F8C72C65AD0FCB DED23E6BB4553A1C42E8616846702776 89092B4D7AA3BB02F9856D0DA9A18292 D8197814EAC12022DC9C5E947FD906A2 7126F6C67D249FCD33AC96C84F355DEF AFE9F1C38F8E58C9CAEE5BA01E089781 BDE7A5577C16D6E569B5AA0E7434383B 84A6D101C286D0498C0AE0114E4AEC51 136312E656649AF7F4E147E4775004C0 F3AB0BF2DA071A9D538043A4058825A8 B17332FBF0722860D57983CE40524454 B9FD3930BC67292AFE18B3150C8A45FF

Tablo 3.3: DSSK #4 ve AES S-kutusunun heksadesimal değerleri.

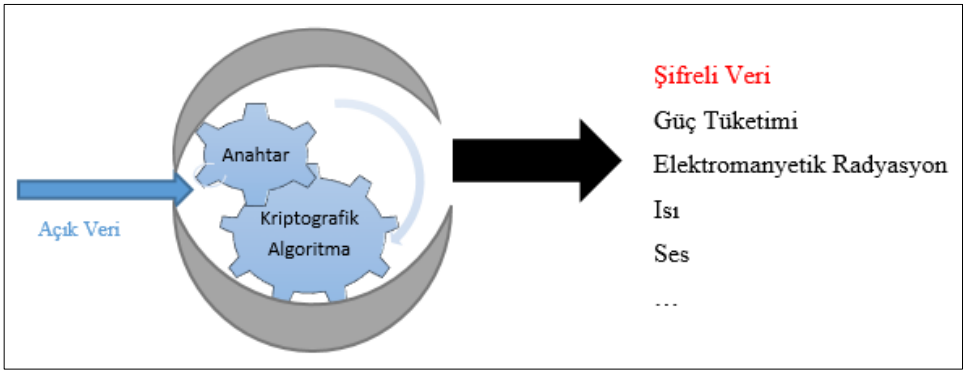
DSSK #4	002C58E0B049C146619392A9833D8C12 C299279825CF537F07E37A1D19602428 8572337C4E8A31974A549F6BA6A1FEB1 0E89C722F4A53AD932BCC00248F6500F 0B52E44F66F3F8189CA2156862692FBD 94FCA85A3F55D6AF4D5B436EFDBE63D5 1C3513A38F6D4440E90D4BCD74B9B3B2 64F7799D81FA04BB908DED95A0571E5C 1670A423C9D49E09CC4CE7BFF18E3014 393E45CB2AB5D0D8C411D2EC5E017B87 29A7F90C5134B4DE7E2DAAD7AD375FEA 9AD1B62086E6DC59FBCE7DDDC6CAAB2E 38916A8426DF470A1FE5DA6C887680C3 D3061A6F96EB9B75E81073AC67EE6517 C842EF05F2363BE103B7F5BA0856778B 21821BF0DB5D2BC54178AEE23C71B8FF
AES S-kutusu	637C777BF26B6FC53001672BFED7AB76 CA82C97DFA5947F0ADD4A2AF9CA472C0 B7FD9326363FF7CC34A5E5F171D83115 04C723C31896059A071280E2EB27B275 09832C1A1B6E5AA0523BD6B329E32F84 53D100ED20FCB15B6ACBBE394A4C58CF D0EFAAFB434D338545F9027F503C9FA8 51A3408F929D38F5BCB6DA2110FFF3D2 CD0C13EC5F974417C4A77E3D645D1973 60814FDC222A908846EEB814DE5E0BDB E0323A0A4906245CC2D3AC629195E479 E7C8376D8DD54EA96C56F4EA657AAE08 BA78252E1CA6B4C6E8DD741F4BBD8B8A 703EB5664803F60E613557B986C11D9E E1F8981169D98E949B1E87E9CE5528DF 8CA1890DBFE6426841992D0FB054BB16

Tablo 3.4: Lineer S-kutusunun heksadesimal değerleri.

Lineer S-kutusu	C63725D401F0E21349B8AA5B8E7F6D9C D9283ACB1EEFFD0C56A7B54491607283 F8091BEA3FCEDC2D77869465B04153A2 E71604F520D1C33268998B7AAF5E4CBD BA4B59A87D8C9E6F35C4D627F20311E0 A55446B7629381702ADBC938ED1C0EFF 8475679643B2A0510BFAE819CC3D2FDE 9B6A78895CADBF4E14E5F706D32230C1 3ECFDD2CF9081AEBB14052A376879564 21D0C233E61705F4AE5F4DBC69988A7B 00F1E312C73624D58F7E6C9D48B9AB5A 1FEEFC0DD8293BCA9061738257A6B445 42B3A15085746697CD3C2EDF0AFBE918 5DACBE4F9A6B7988D22331C015E4F607 7C8D9F6EBB4A58A9F30210E134C5D726 63928071A45547B6EC1D0FFE2BDAC839

4. YAN KANAL ANALİZİ SALDIRILARI

Kriptografik algoritmaları gerçekleyen cihazlar, açık veri ve kapalı veri dışında tabii yapısından dolayı istemsiz bazı çıkışlar üretmekte ve bu bilgiler ölçülebilir olabilmektedir. Bir işlemin yapılmasının ne kadar zaman aldığı [18], işlem adımlarının ne kadar güç çektiği [4], ne kadar elekromanyetik yayınım yaptığı veya ne kadar ısı yaydığı örnek olarak verilebilir[5]. Eğer bu çıkışların gizli bilgi olan anahtar ile bir şekilde ilişkisi var ise bu bilgiler yan kanal bilgisi olarak adlandırılırlar. Yan kanal analizi saldırıları, kriptografik cihazın ürettiği yan kanal bilgilerini (Şekil 4.1) kullanarak gizli bilgiye ulaşmaya çalışır. Aynı algoritmanın farklı gerçeklemeleri değişik miktar ve biçimlerde yan kanal bilgisi sızdırabilir. Bundan dolayı, çoğunlukla, yan kanal analizi saldırıları genelleştirilemezler. Bununla birlikte bu saldırılar genellikle pratikte uygulanabilmektedir.



Şekil 4.1: Yan kanal bilgileri.

Yan kanal analizi saldırıları, aktif ve pasif olarak iki gruba ayrılmaktadır. Aktif saldırılar [5], kriptografik cihazın içindeki devrelere ulaşılmasını gerektirir. Bu nedenle uygulanmaları daha zordur ve oldukça gelişmiş ve pahalı düzeneğe ihtiyaç duyulur. Ölçüm saldırıları [19] ve hata oluşturma saldırıları [20] adında iki tür aktif saldırı vardır. Saldırgan, ölçüm saldırılarında, cihaz içindeki devrelere erişip ya da iletim hatlarını gözleyerek doğrudan gizli bilgiye erişmeye çalışır. Belirli noktalara dışarıdan müdahale edip, işlemlerde hataya yol açarak gizli bilgiler elde edilmeye çalışılması ise hata oluşturma saldırısıdır.

Pasif saldırılarda ise cihazın çalışmasına müdahale edilmez. Cihazın normal çalışması sırasında ürettiği yan kanal bilgileri kullanılır. Bu saldırı pasif saldırıya girer ve cihazın çalışmasına müdahale söz konusu değildir. Bu saldırılar, aktif

saldırılarda kullanılan ölçüm düzeneklerine nispeten daha basit ve maliyeti düşük ölçüm düzenekleriyle yapılabilmektedir.

Pasif saldırıların her biri kendi içerisinde, basit analiz ve farksal analiz olarak iki gruba ayrılır. Basit analizde, sadece tek bir ölçüme ihtiyaç duyulur ve bu tek bir ölçümden elde edilen yan kanal bilgisi doğrudan gizli bilginin belirlenmesi için kullanılır. Yürütülen işlemlerle yan kanal bilgisi arasındaki ilişkiden yararlanılır. Farksal analizde ise çok sayıda ölçüm kullanılır ve bu sayede gürültünün etkisi yok edilmeye çalışılır. İşlenen veriler ile yan kanal bilgisi arasındaki ilişki incelenir.

Tez kapsamında, yan kanal analizi saldırısı sadece pasif olarak güç analizi saldırılarını kapsayacak şekilde yapılmıştır.

4.1. Güç Analizi Saldırıları

Güç analizi saldırıları ilk kez Kocher tarafından DES üzerinde uygulanmıştır [19]. Bu uygulamanın başarısının ardından, güç analizi üzerine pek çok çalışma yapılmıştır.

Elektronik tümdevrelerin gerçeklenmesinde tamamlayıcı metal oksitli yarı-iletken (CMOS) tranzistörler çok yaygın olarak kullanılmaktadır [21]. Dinamik güç tüketimi (konum değiştirme anlarındaki güç tüketimi), bir CMOS tranzistörün güç tüketimindeki en büyük payı oluşturur. Dinamik güç tüketimi, tranzistörün sürdüğü yük kapasitesinin üzerindeki gerilim değişiminin hızlanmasıyla artar. Bununla birlikte çıkışın sabit kaldığı anlardaki güç tüketimi, diğerine nispeten çok düşük kalmaktadır.

Lojik kapıların güç tüketimi, giriş değerleri ile doğrudan ilişkilendirilebilir. Buradan yola çıkılarak CMOS kapıların güç tüketimi, gizli bir bilgi işleniyorsa, yan kanal bilgisi olarak kullanılabilir. Algoritma koşarken farklı işlemlerin birbirinden farklı güç tüketim karakteristiğine sahip olması, saldırıların başarısını artırmaktadır.

Güç tüketimi söz konusu olduğunda, Hamming mesafesi ve Hamming ağırlığı sızıntısı olmak üzere iki tür yan kanal bilgisi sızıntısı vardır. Hamming ağırlığı sızıntısı aynı anda işlenmekte olan ‘1’ bitlerinin sayısı hakkında bilgi verirken Hamming mesafesi sızıntısı ne kadar bit değiştiği hakkında bilgi verir.

Güç analizi saldırılarında, kriptografik cihazın güç tüketimi ile gizli bilgi ya da yapılan işlemler arasında bir korelasyon kurularak gizli bilgiye erişilmeye çalışılır. Bu amaçla, devreyi besleyen hat üzerine küçük değerli bir direnç yerleştirilir ve bu

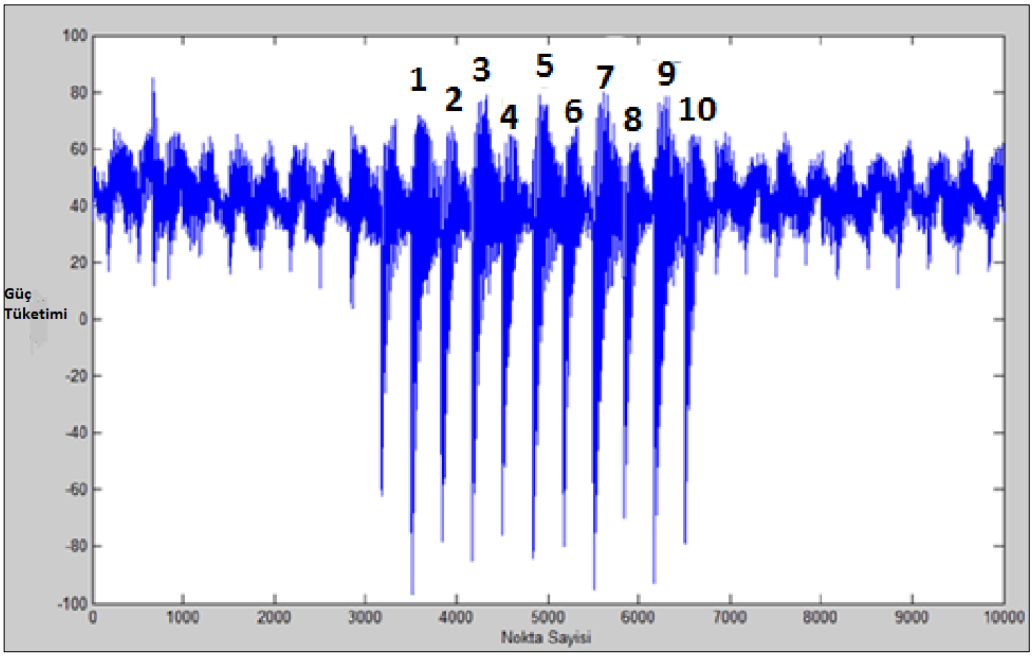
direncin her iki ucundaki gerilim değerlerinin farkından yararlanılarak çekilen akım bilgisi elde edilir.

Güç analizi saldırıları basit güç analizi saldırıları ve farksal güç analizi saldırıları olmak üzere ikiye ayrılır.

4.2. Basit Güç Analizi (BGA) Saldırıları

Basit güç analizi saldırılarında, saldırgan güç tüketimini görsel olarak inceleyip yorumlayarak, saldırılan gerçekleme ve/veya algoritma hakkında bilgi ve nedenleri araştırır. Saldırgan, çalıştırılan algoritma işlemlerini belirler ve nihayetinde kriptografik anahtara ulaşmaya çalışır.

Şekil 4.2'deki ölçüm, bir AES gerçeklemesine aittir.



Şekil 4.2: Örnek bir AES ölçümü.

Her şekil, aynı anahtarla farklı giriş verisinin şifreleme anındaki güç ölçümlerini göstermektedir. Gözüktüğü gibi, her güç ölçümünde 11 adet tepe vardır ve burada AES'in 10 turu ve ilk anahtar eklemesine ait kısım gözükmektedir. 10 tur, AES gerçeklemesinin 128-bit anahtar uzunluğunda söz konusudur ve saldırgan bu bilgiyi kolayca elde edebilmektedir. Ancak, basit güç analizi sadece çok az veya hiç gürültü olmayan ölçümlerde etkili olabilmektedir.

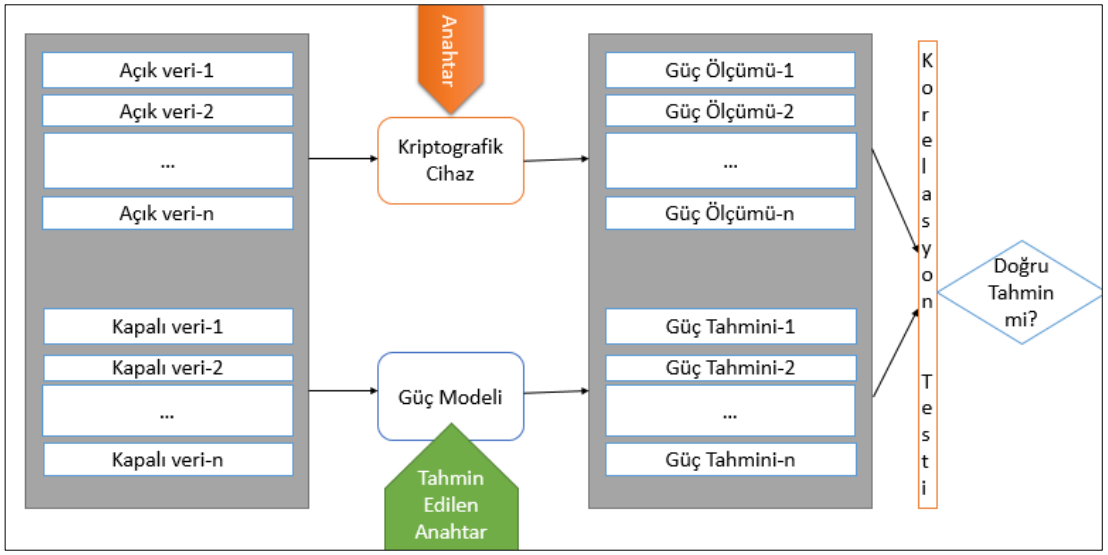
4.3. Farksal Güç Analizi (FGA) Saldırıları

Yürütülen komutlara veya yapılan işlemlere bağlı olarak oluşan büyük ölçekli güç tüketimi değişimlerine ilaveten, işlenen veriye bağlı olarak da güç tüketiminde değişimler oluşmaktadır. Bu değişimlerin çok düşük boyutta olmaları, ölçüm hataları ya da gürültü nedeniyle gözlemlenmelerini engeller. Ancak yine de, hedeflenen algoritmaya yönelik bazı istatistiksel teknikler ve hata düzeltme yöntemleri kullanılarak yan kanal bilgisi elde edilebilir ve gizli bilgiye ulaşılabilir [18][4].

FGA saldırılarında işlenen veri ile güç tüketimi arasında ilişki kurulmaya çalışılır. BGA'dakinin aksine, gürültüyü filtreleyebilmek amacıyla çok sayıda ölçüm yapılır ve güç modeli ile güç tüketimi arasındaki istatiksel ilişki kullanılır. Özel olarak, Brier tarafından ortaya atılan Korelasyon Güç Analizi (CPA) [22], saldırılan cihaz tarafından işlenilen veri ile güç tüketimi arasında lineer bir ilişki olduğunu varsaymaktadır. Sadece doğru anahtar güç modeli ile güç tüketimi arasında en yüksek ilişkiye sahip olacaktır. FGA saldırısı aşağıdaki adımlardan oluşur:

- Atağın yapılacağı yer belirlenir ve algoritmanın ilgili yazmacına yazılacak olan ara değeri hesaplanır.
- Algoritma koşturulurken, saldırılacak noktaya odaklanılarak güç tüketimi ölçümleri alınır.
- Hedeflenen şifreleyicinin işlemleri temel alınarak kuramsal güç modeli tasarlanır.
- Bu güç modeli, anahtarı elde etmek için güç ölçümüyle ilişkilendirilir.

FGA atak akışı Şekil 4.3'de gösterilmektedir.



Şekil 4.3: FGA atak akışı.

4.4. Pearson Korelasyonu

Pearson korelasyonu en yaygın kullanılan korelasyon ölçümüdür ve iki değişken arasındaki lineer ilişkinin derecesini verir. Korelasyon +1 ve -1 arasında değişmekle birlikte +1 için değişkenler arasında mükemmel pozitif lineer ilişki olduğunu, -1 için değişkenler arasında mükemmel negatif lineer ilişki olduğunu gösterir. Korelasyonun 0 olması iki değişkenin birbirleriyle hiç lineer ilişkisi olmadığını gösterir.

Cihazın güç tüketimi (P) ve kuramsal güç modeli (H) arasındaki Korelasyon katsayısı (r) Şekil 4.4'de verildiği gibidir.

$$r(P,H)=\frac{n\sum_{i}^{n}PiHi-n\sum_{i}^{n}Pi\sum_{i}^{n}Hi}{\sqrt{n\sum_{i}^{n}P_i^2-(\sum_{i}^{n}P_i)^2}\sqrt{n\sum_{i}^{n}H_i^2-(\sum_{i}^{n}H_i)^2}}$$

Şekil 4.4: Korelasyon eşitliği.

Bu tezde, Hamming mesafesiyle birlikte Pearson korelasyonu kullanılmış ve CPA analizi gerçekleştirilmiştir.

4.5. Farksal Güç Analizi için Güvenlik Metrikleri

Yan Kanal Analizi (YKA) ataklarının literatüre girmesinden [4] itibaren, bunlara karşı [2, 7, 8]'deki gibi çok sayıda önlemler ve farklı ataklar ortaya çıktı. Farklı atakların karşılaştırılabilmesi amacıyla "tahmin entropisi" [23], "başarı oranı" [23], "sinyal gürültü oranı" gibi çeşitli YKA güvenlik metrikleri literatürde tanıtıldı. Bir metrik saldırının gerçekleştiği koşullardan ve saldırı tipinden ne kadar bağımsız olursa o kadar anlamlı olmaktadır. Bundan dolayı bir YKA atağını değerlendirmede birden çok metrik kullanılmaktadır.

Bu tezde, yapılan atakların performansını değerlendirebilmek için tahmin entropisi ve başarı oranı kullanılmıştır. Birinci-mertebeden başarı oranı, N tane ölçüm ile atak sonucunda tahmin edilen anahtarın, doğru anahtar olma olasılığıdır. İkinci-mertebeden başarı oranı, N tane ölçüm ile atak sonucunda doğru anahtarın, tahmin edilen ilk iki anahtar arasında olma olasılığı, Üçüncü-mertebeden başarı oranı da aynı şekilde tahmin edilen anahtarın ilk üç anahtar arasında olma olasılığıdır. m bitlik bir anahtar için 2^m'inci mertebeden başarı oranının 1 olduğu gözükmektedir.

Örneğin, birinci-mertebeden başarı oranı Şekil 4.5'de verilen algoritma ile hesaplanabilir. 10000 tane güç ölçümü kullanılarak saldırı sonuçlarını değerlendirmek için ölçümler 10 tane alt sete ayrılır: v_i $(i = 1, \ldots, 10)$ olmak üzere her sette 1000 ölçüm bulunur ve aşağıdaki algoritma çalıştırılır.

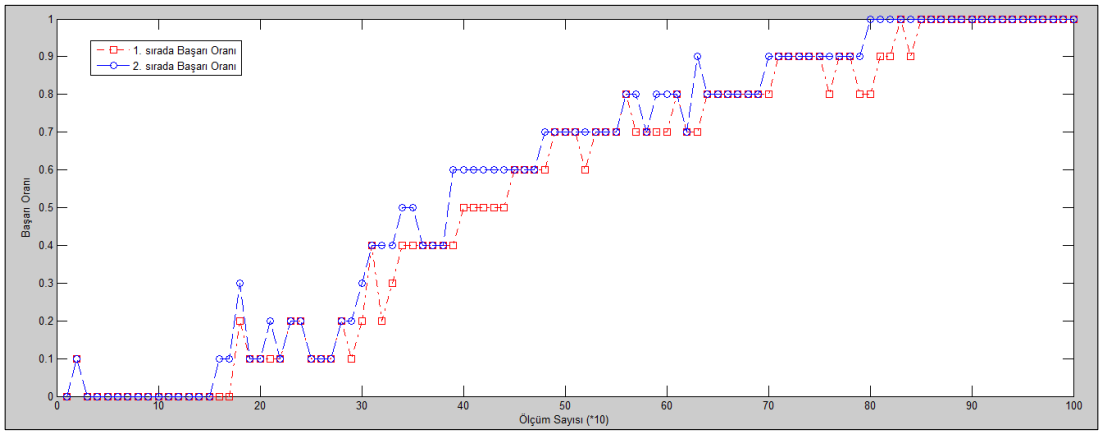
```
1. Döngü n := 100:100:1000
sayaç ← 0
        2. Döngü i = 1:10
        1 − ilk n tane ölçümü v_i'den al
        2 − FGA Atağı gerçekleştir.
        3 − Eğer anahtar doğru tahmin edildiyse sayaçı 1 artır
        2. Döngü sonu
N adet ölçüm için başarı oranı hesapla = sayaç/10
1. Döngü sonu
```

Şekil 4.5: Birinci-mertebeden başarı oranı hesaplama algoritması.

Benzer şekilde doğru anahtarın tahmin edilen ilk k-anahtar arasında olma olasılığı kullanılarak k'nıncı mertebeden başarı oranı elde edilebilir. Ayrıca set sayısı

ve ölçüm sayısı artırılarak elde edilen başarı oranının doğruluğunu iyileştirmek mümkündür.

Şekil 4.6'da örnek bir başarı oranı grafiği yer almaktadır. Burada toplam 10000 adet ölçüm 1000'lik setlere ayrılmış ve yukarıdaki algoritma ile başarı oranı hesaplanmıştır. Görüldüğü gibi yaklaşık 800 ölçümde doğru anahtar, anahtar tahmininde ilk 2 sırada yer alırken, 850 ölçümde artık ilk sıradaki anahtar tahmini doğru anahtar olmaktadır.

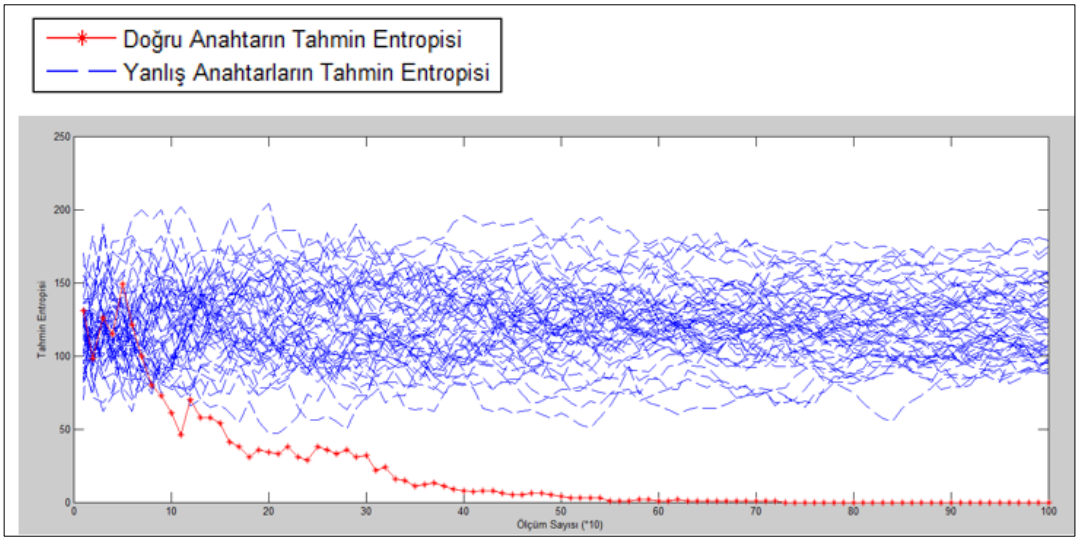


Şekil 4.6: 1000lik 10 set ile hesaplanan başarı oranı.

Bu tezde hesaplanan diğer bir metrik ise tahmin entropisi'dir. Tahmin entropisi, doğru anahtar değerini bulmadan önce test edilen ortalama anahtar sayısıdır. Tahmin entropisi, başarı oranının bütün mertebeleri ile alakalıdır. Aslında, doğru anahtar (d) tahmini ancak ve ancak ilk "o" aday arasında olursa, anahtar tahmin sıralamasında o'uncu sıra için değer alır. Sonuç olarak, doğru anahtarın o'uncu sırada olma olasılığı $P[sıralama(d) = o] = Başarı\ Oranı(o) - Başarı\ Oranı(o-1)$'e eşittir. Burada $Başarı\ Oranı(0)$ doğal olarak sıfır değerini alır. Bu durum aşağıdaki ilişkiyi getirir:

$$TE = \sum_{o=1}^{|K|} o\ P[sıralama(d) = o]$$
$$= |K| - \sum_{o=1}^{|K|-1} Başarı\ Oranı(o) \quad (4.2)$$

Şekil 4.7'de örnek bir tahmin entropisi verilmektedir.



Şekil 4.7: Örnek bir tahmin entropisi.

Görüldüğü gibi 7300 ölçümden sonra tahmin edilen anahtar doğru anahtar olmaktadır. Beklenildiği üzere yanlış anahtarların tahmin Entropisi hiçbir zaman sıfıra düşmemektedir.

5. İLERİ ŞİFRELEME STANDARDI (AES)

AES algoritması, veri güvenliği sağlamak amacıyla, akıllı kartlardan haberleşme sistemlerine kadar çok değişik alanlarda kullanılmaktadır. Bu nedenle gerek yazılımsal, gerekse donanımsal olarak farklı şekillerde gerçeklenmektedir.

AES algoritması, tur dönüşümünün belirli sayıda tekrar edilmesiyle gerçeklenmektedir. Tekrar sayısı anahtar uzunluğuna göre değişmektedir. Anahtar uzunluğu 128 bit ise 10 tur, 192 bit ise 12 tur, 256 bit ise 14 tur işlem yapmaktadır. Algoritmanın bu tekrar eden yapısı, donanımsal gerçeklemede değişik yollarla algoritmanın gerçeklenmesine olanak sağlar. Tur dönüşümlerini gerçekleyen bloklar artarda bağlanabilir ya da tur dönüşümü bir blok olarak gerçeklenip tekrar tekrar kullanılabilir.

Şekil 5.1'de AES şifreleme algoritması yer almaktadır. Algoritma girdisi olan w[] sözcük dizisi tur anahtarlarını içermektedir. Nb ise durum matrisindeki sütun sayısıdır ve AES-128 için 4 değerini alır.

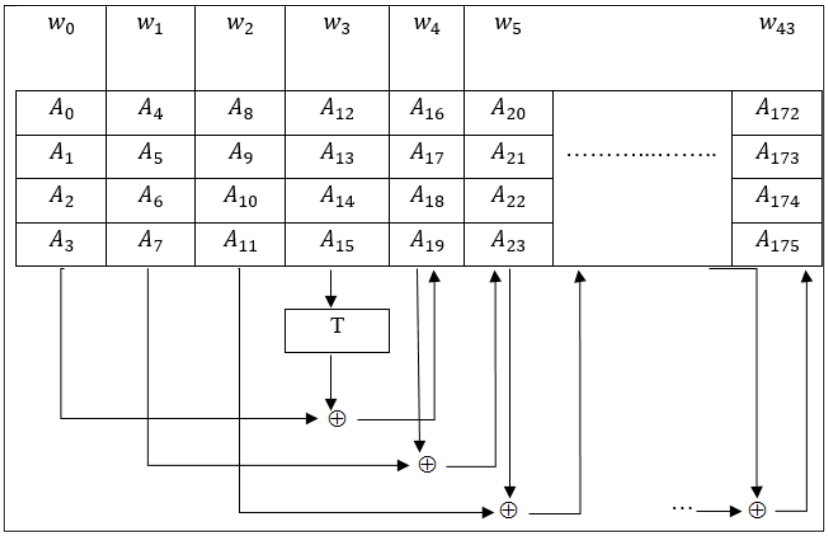
```
Şifreleme (bayt Giriş[4*Nb], bayt çıkış[4*Nb], sözcük w[Nb*(Tur Sayısı+1)])
başla bayt Durum[4,Nb]
        Durum = Giriş
        Tur Anahtarı Ekleme(Durum, w[0, Nb-1])
        Döngü tur= 1:Tur Sayısı–1 için
                Yer Değiştirme(Durum)
                Satırları Karıştırma(Durum)
                Sütunları Karıştırma(Durum)
                Tur Anahtarı Ekleme (Durum, w[tur*Nb, (tur+1)*Nb-1])
        Döngü Sonu
        Yer Değiştirme(Durum)
        Satırları Karıştırma(Durum)
        Tur Anahtarı Ekleme(Durum, w[Nr*Nb, (Nr+1)*Nb-1])
        Çıkış = Durum
son
```

Şekil 5.1: AES şifreleme algoritması.

Verilog dili kullanılarak yapılan gerçeklemede, tur dönüşümünü gerçekleyen sadece bir blok oluşturulmuştur. Bloğun ürettiği çıkış, bir sonraki girişi olarak kullanılmaktadır. Bu şekilde aynı blok, tur sayısı kadar çalıştırılarak şifreleme/çözme işlemi gerçekleştirilmektedir.

5.1. Anahtar Üretme İşleminin Gerçeklenmesi

AES, farklı uzunluktaki anahtarlar ile çalışabilmektedir. Bu tezde 128 bitlik anahtar ile çalışan AES kullanılmıştır. Her tur işlemlerinin son kısmı olan tur anahtarı ekleme işleminde, w[ ] dizisinde bulunan128-bitlik anahtarlar kullanılır. w[ ] dizisi, anahtar üretim fonksiyonu ile üretilir. Bu fonksiyon, anahtar olarak girilen 128-bitlik veriyi alarak baytlar ($A_0, \ldots, A_{15}$) halinde 4x4'lük matris oluşturur ve her bir tur için ürettiği 128-bitlik anahtar bloklarını bu matrisin yanına koyar. Böylece AES-128 için 4x44 büyüklüğünde matris oluşur. Şekil 5.2'de bunun için örnek bir matris gösterilmektedir.



Şekil 5.2: Tüm tur anahtarlarının matrisi.

Oluşturulacak olan sütun, yeni 4x4 matrisin ilk sütunu ise kendinden bir önceki sütun, dönüştürme işlemine uğrar (Şekil 5.22'deki T bloğu). Dönüşüm işleminin ilk adımında 4 baytlık veriden oluşan sütun üzerinde kaydırma işlemi gerçeklenir. İkinci adımda herbir bayt, Yer Değiştirme işlemine tabii tutulur. Son adımda ise bir tur sabiti ile EXOR işlemine tabii tutulur.. Tur vektörünün ilk baytı kaçıncı turda olunduğuna göre değişirken diğer baytları sıfırdır.

5.2. Yer Değiştirme İşleminin Gerçeklenmesi

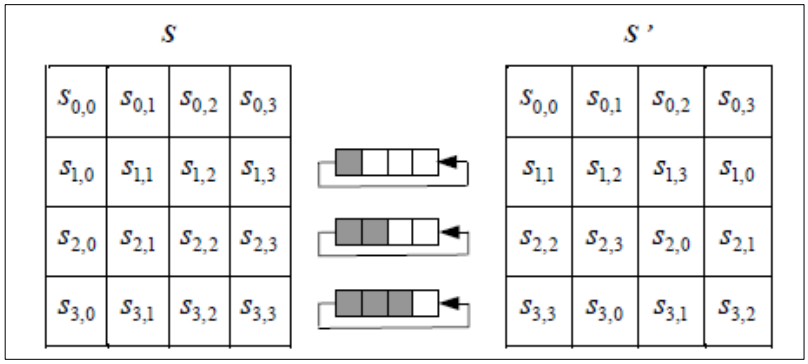
AES algoritmasında, yer değiştirme işlemlerinde kriptografik özellikleri [12]'de verilen ve F_{2^8} sonlu cisminde ters alma fonksiyonu olarak tanımlanan S-kutusu belirlenen bir afin transformasyondan geçirilmiş olarak kullanılmaktadır. S-kutuları güvenlik açısından incelenmek istendiğinde, birçok kriptografik kriter söz konusu olmaktadır. Bu kriterlerin başlıcaları ise Bölüm 2'de tanımları verilen doğrusal olmama, farksal birbiçimlilik, cebirsel derece, mutlak gösterge ve saydamlık katsayısı olarak verilebilir.

Yer değiştirme dönüşümünde, her bir bayt S-kutusundan geçirilir. Bu nedenle, yer değiştirme dönüşümü, AES-128 için 16 adet S-kutusu içeren bir blokla gerçeklenir.

Bu tezde, S-kutusunun olası her girişi için (2^8 = 256 farklı giriş vardır) çıkışı hesaplanmış ve elde edilen çıkış değerleriyle bir tablo oluşturulmuştur. Oluşturulan tüm tablolar Bölüm 3'de verilmektedir.

5.3. Bayt Kaydırma İşleminin Gerçeklenmesi

Bayt kaydırma işlemi, Şekil 5.3'de gösterildiği gibi sadece durum baytlarının yerlerini değiştirmektedir. Bu dönüşümün gerçeklemesi herhangi bir kombinezonsal devre gerektirmemektedir. Çünkü bu dönüşüm sadece tur yazmacının girişindeki baytların yeri kaydırılarak çıkışa verilmesi ile gerçeklenir.



Şekil 5.3: Bayt kaydırma dönüşümü.

5.4. Sütun Karıştırma İşleminin Gerçeklenmesi

Sütun karıştırma işleminde, durum matrisinin sütunları, elemanları {03, 02, 01} baytları olan bir matrisle çarpılmaktadır.

a_0, a_1, a_2, a_3 bu durum matrisinin sütunları olsun. Sütun değiştirme işlemi Şekil 5.4'de gösterildiği şekilde gerçeklenebilir:

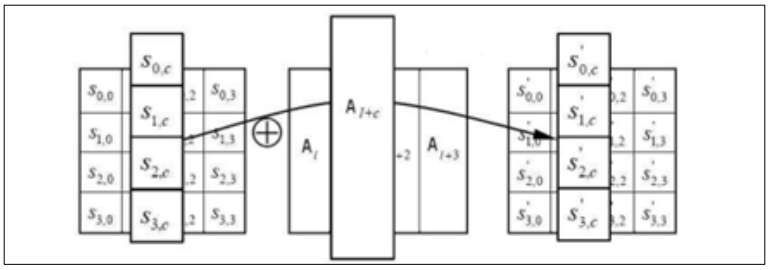
$$
\begin{aligned}
b_0 &= (\{02\} \times a_0) \oplus (\{03\} \times a_1) \oplus a_2 \oplus a_3 \\
b_1 &= a_0 \oplus (\{02\} \times a_1) \oplus (\{03\} \times a_2) \oplus a_3 \\
b_2 &= a_0 \oplus a_1 \oplus (\{02\} \times a_2) \oplus (\{03\} \times a_3) \\
b_3 &= (\{03\} \times a_0) \oplus a_1 \oplus a_2 \oplus (\{02\} \times a_3)
\end{aligned}
$$

Şekil 5.4: Sütun karıştırma denklemleri.

Bu eşitlikteki işlemler, baytların F_2 üzerindeki polinom gösterimleri kullanılarak ve $m(x) = x^8 + x^4 + x^3 + x + 1$ indirgenemez polinom alınarak gerçekleştirilir.

5.5. Anahtar Ekleme İşleminin Gerçeklenmesi

Her bir tur için 128-bitlik tur anahtarı, anahtar üretme fonksiyonu ile üretilir ve Şekil 5.5'de gösterildiği gibi durum matrisi ile EXOR işlemi yapılır. Şekil 5.5'de $l, Tur \times N_b$ değerini almaktadır.



Şekil 5.5 Anahtar Ekleme İşlemi

6. ÖLÇÜM DÜZENEĞİ ve FPGA KONFİGÜRASYONU

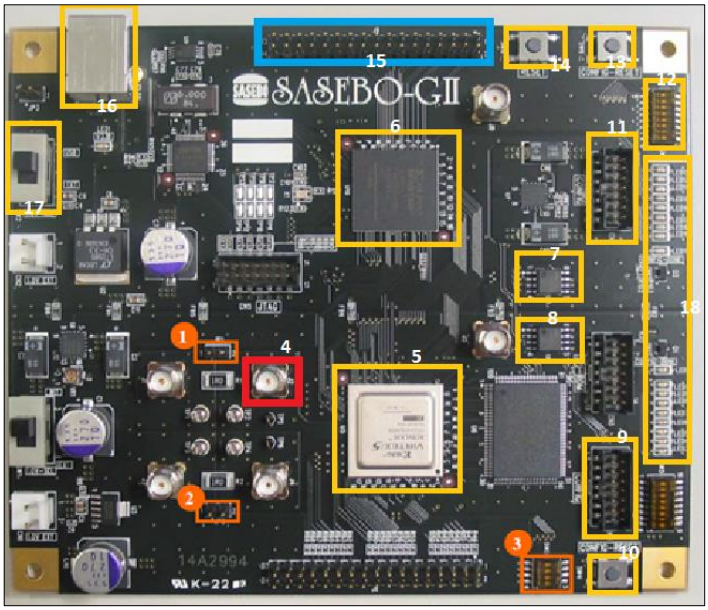
Yan kanal saldırılarına karşı güvenlik değerlendirmesi için uluslararası bir standart oluşturma çabasına destek vermek amaçlı AIST'ın (National Institute of Advanced Industrial Science and Technology) araştırma merkezi (Research Center for Information Security) ve Tokyo Üniversitesi, yan kanal atağı standart değerlendirme kartlarını geliştirmişlerdir. SASEBO kartları, güç analiz ataklarını gerçekleştirmeye odaklanmış olup günümüzde 6 farklı çeşit SASEBO kartı vardır. Bu tezde SASEBO-GII üzerinde çalışmalar gerçekleştirilmiştir.

AES algoritması SASEBO-GII, yan kanal analizi değerlendirme kartında Verilog dili kullanılarak gerçeklenmiştir. SASEBO-GII kartı üzerinde Xilinx Spartan-3A ve Xilinx Virtext-5 LX30/50 olmak üzere iki adet FPGA vardır.

Şekil 6.2'da SASEBO-GII kartı gözükmektedir. Şekildeki kart üzerinde kullanılan bazı kısımlar numaralandırılmıştır ve şu şekildedir:

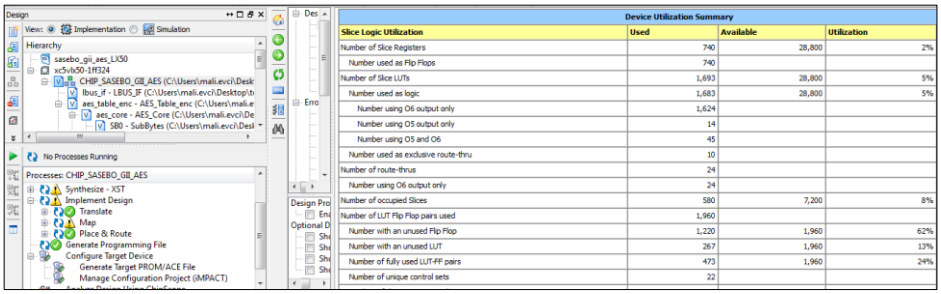
1- JP1: açık olmalı
2- JP2: kısa devre olmalı
3- J6: Ölçüme tetiklenmek için ilk pini kullanılıyor
4- Güç ölçümü alınan direnç için arayüz
5- Kriptografik FPGA: XC5VLX50 - 1FFG324 (Virtex-5 series)
6- Kontrol FPGA: XC3S400A - 4FTG256 (Spartan-3A series)
7- Flash ROM (Kontrol FPGA için)
8- Flash ROM (Kriptografik FPGA için)
9- JTAG arayüzü (Kriptografik FPGA'i programlamak için)
10- Config-Reset butonu
11- JTAG arayüzü (Kontrol FPGA'i programlamak için)
12- Anahtar-7 (frekans ayarlama)
13- Config-Reset butonu
14- Reset butonu
15- Anahtar-3
16- USB host arayüzü
17- Açma kapama anahtarı
18- LED'ler (D1-D11)

Şekil 6.1: SASEBO-GII kartı üzerindeki noktalar.



Şekil 6.2 SASEBO-GII kartı.

Xilinx ISE 14.4 programı ile hazırlanmış olan Verilog kodu derlenerek uzantısı bit olan dosya oluşturulur. Şekil 6.3'de bit dosyası oluşturma sonrasına ait ekran görüntüsü yer almaktadır. Bu ekran görüntüsünde FPGA üzerinde kullanılan kaynaklar hakkında bilgi de verilmektedir.



Şekil 6.3: Xilinx ISE bit dosyası oluşturma ekranı.

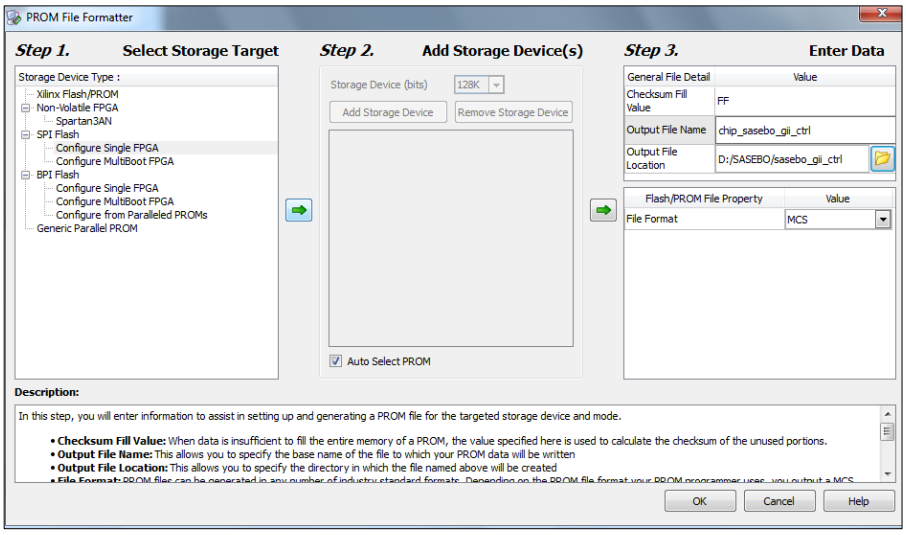
SASEBO-GII ile PC arasındaki bağlantı USB kablo ile sağlanmaktadır. Kart üzerinde öncelikli olarak JP1'in açık ve JP2'nin ise kapalı (kısa devre) olması gerekmektedir.

FPGA'leri programlamak için bit dosyalarına ve mcs dosyalarına ihtiyaç vardır. Bit dosyası, mcs dosyasını üretmek için gerekmektedir. Mcs dosyaları ise Flash ROM'ları programlamak için gerekmektedir.

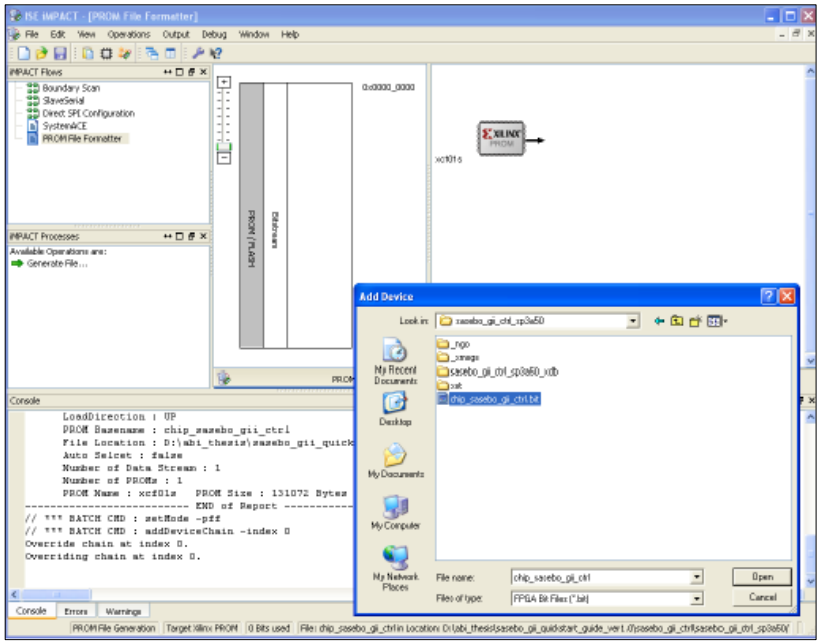
Config-Reset anahtarları ise FPGA'leri programlamak için kullanılır. Bu bölümde adım adım SASEBO-GII FPGA konfigürasyonları anlatılmıştır.

Proje, Xilinx ISE'de sentezlenip gerçeklendikten sonra programlanabilir olan bit dosyası üretilebilmektedir. Bit dosyası üretilmesi sonrası, FPGA'ler Xilinx Impact programı kullanılarak konfigüre edilebilir. Kontrol FPGA (Spartan-3A)'in Flash ROM'unu (ST45DB16D, U11) yeniden programlamak için konfigürasyon kablosu CN7'ye bağlanması gerekir. Kriptografik FPGA (Virtex-5 LX30)'in Flash ROM'unu (ST45DB16D, U4) yeniden programlamak için ise konfigürasyon kablosunun CN4'e bağlanması gerekir.

Xilinx Impact programında bit dosyasından mcs dosyasını oluşturmak için "Generate Target PROM/ACE file" seçeneği çalıştırılır. Bit dosyası FPGA'da çalışan dosya, msc dosyası ise Flash ROM'a kaydedilen dosyadır. Açılan sayfada "Creat PROM file" seçilir ve Şekil 6.4'deki ekranda ise SPI Flash altındaki "configure single FPGA" seçilerek diğer adıma geçilir. Bir sonraki adımda aşağıdaki "Auto select PROM" seçilir. Daha sonra "output file" ismi ve kaydedilecek yeri seçilir.



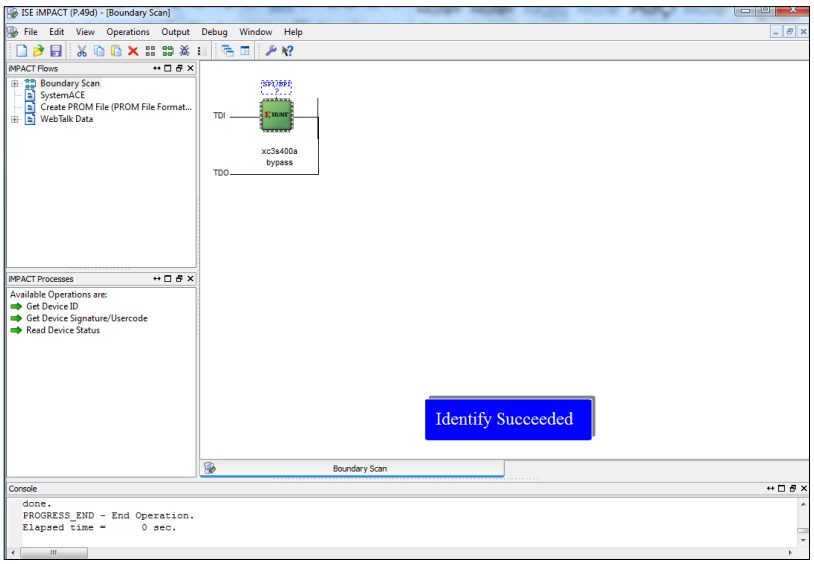
Şekil 6.4: Msc dosyası oluşturma-1.



Şekil 6.5: Mcs dosyası oluşturma-2.

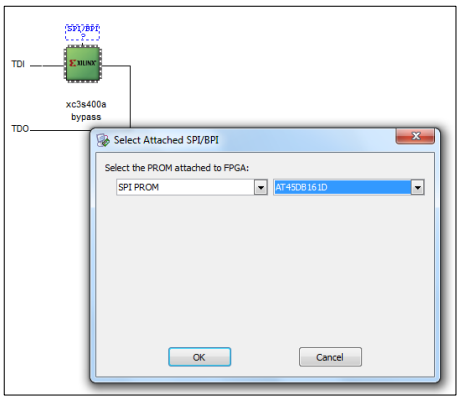
Yeni gelen sayfada “Generate file” seçilerek Flash ROM için gösterilen dizin altında msc dosyası oluşturulmuş olur.

Kontrol kodunun Flash ROM’a yüklenmesi için JTAG kablosu CN7 konnektörüne bağlanır. Öncelikle kart üzerinde “Config-Reset” butonuna basılır. ISE IMPACT programı çalıştırılır ve “Boundary scan” seçilerek, “initialize chain” işlemi gerçekleştirilir.



Şekil 6.6: Boundary scan.

Kesikli mavi çizgi ile belirtilmiş SPI/BPI seçeneklerinden msc dosyası Şekil 6.7'deki bilgiler kullanılarak eklenir ve "flash" seçilerek programlanır.



Şekil 6.7: SPI/BPI tipinin seçimi.

Kriptografik FPGA kodunun Flash ROM'a yüklenmesi JTAG kablosunun CN4 konnektörüne bağlanmasının dışında bütün adımlar kontrol kodunun Flash ROM'a yüklenmesi ile aynıdır.

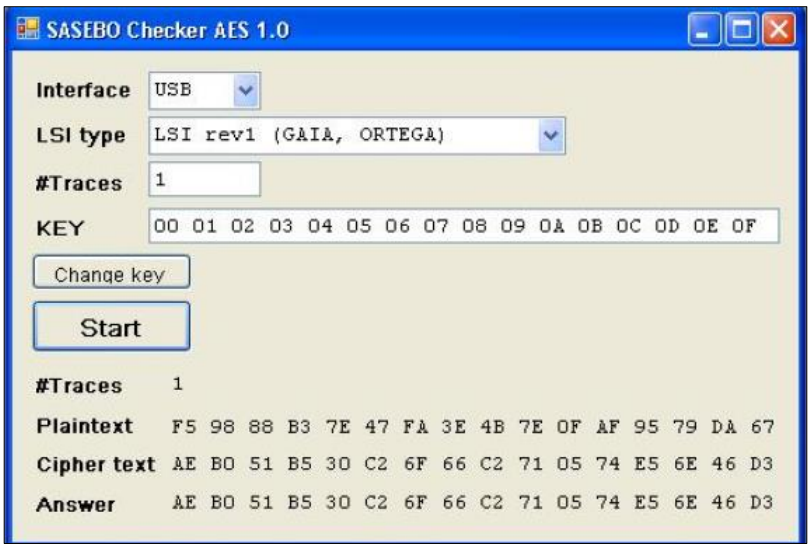
FPGA'ler programlandıktan sonra SASEBO kart yeniden çalıştırılır. Başarılı yükleme sonrası D1, D2 ve D11 ledlerinin yanması beklenmektedir. Eğer D1 yanmıyorsa, arızanın güç beslemesinden, D2 ve D11 ledleri yanmıyorsa da SASEBO ayar problemi veya Flash ROM'un programlanmasında hata oluştuğu anlamına gelir.

FGA atağı için öncelikle güç ölçümlerinin toplanması gerekmektedir. Bu işlem için Osiloskop ile PC ve SASEBO-GII ile PC arasında iletişimin sağlanması gerekmektedir.

SASEBO-GII ile PC arasında iletişim kurulabilmesi için açık kaynak kodlu C# ile yazılmış SASEBO Checker programı [26]'daki web adresinden temin edilmiştir. Şekil 6.8'de bu programın arayüzü gösterilmektedir. Burada kriptografik FPGA'ya yaptırılan AES işlemi programın rastgele oluşturacağı açık veri ve işlemin sonucu gösterilmektedir. "Cipher text" karşısındaki sonuç, kriptografik FPGA'den işlem sonucu alınan değer olmakla birlikte, "Answer" karşısındaki sonuç ise yazılımsal olarak kriptografik işlemin sonucu olmaktadır. Böylece kriptografik FPGA'in gerçekten doğru işlemi yapıp yapmadığı da test edilebilmektedir. Ayrıca kaç ölçümün alınacağı ve anahtarın ne olacağı da dışarıdan ayarlanabilmektedir.

"Sasebo Checker" programı bu haliyle tez kapsamında kullanılamamaktadır. Farksal Güç Analizinde açık veriye (Plaintext) ve buna karşılık işlem sonucunda

oluşan şifreli veriye (Cipher text) ihtiyaç duyulmaktadır. Bu amaçla kod içinde daha önceden açık verilerin olduğu bir dosya gösterilmiş ve programın açık verileri bu dosyadan okuması sağlanmıştır. Aynı zamanda şifrelenen veriler, gösterilen bir dizindeki dosyaya yazdırılmıştır.



Şekil 6.8: SASEBO checker programı.

Aşağıda belirtilen yazılım ve ekipmanlar, SASEBO-GII ile PC arasında iletişim sağlanabilmesi için gerekli olan yazılım ve donanımlardır.

- Karta güç kaynağı sağlamak ve PC ile kart arasında ara yüz görevini sağlamak için USB kablosu
- FPGA'lere bağlı olan Flash ROM'ları programlayabilmek için Xilinx Paltorm Cable USB veya Platform Cable USB II adaptörü
- Microsoft .Net Framework 3.5
- USB üzerinden haberleşebilmek için FTDI tarafından sağlanan D2XX sürücü yazılımı [27]
- National Instruments NI-VISA 4.6.2 yazılımı
- AES modülünü test etmek için: SASEBO AES Checker [28]
- Xilinx ISE WebPACK yazılımı [29]

Tezde gerçekleştirilen FGA atağında kullanılacak olan ölçümler, Tektronix DPO7254 marka osiloskop kullanılarak alınmıştır. Tektronix bu osiloskop ürününde C/C++ için API'ler sağlamaktadır. Osiloskop ile bu API'leri kullanan bir C++ kodu

gerçeklenmiş ve osiloskop ile iletişim kurma, tetiklemeye hazırlama ve kriptografik işleme tetiklendikten sonra alınan ölçümü PC'ye kaydetme işlemleri hazırlanan bu kodla sağlanmıştır. Bütün bu işlemler Ethernet ara yüzü ile yapılmaktadır. FGA gerçekleştirme üzere çok sayıda ölçüm alınması için PC'nin hem osiloskop ile hem SASEBO-GII ile koordineli bir şekilde haberleşmesi gerekmektedir.

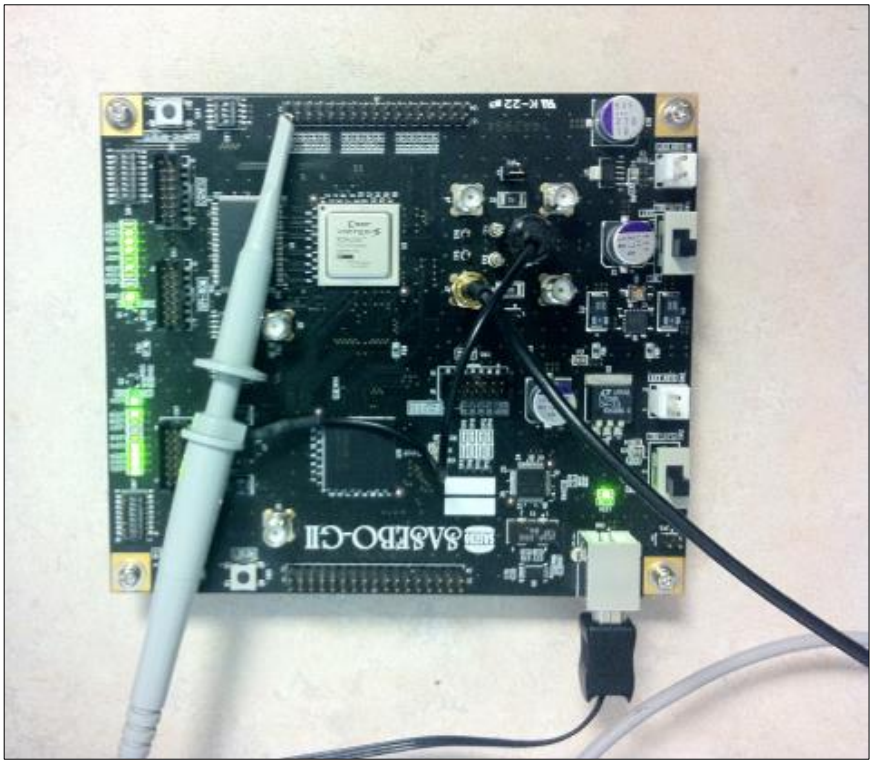
Örneğin, 300000 adet ölçüm yaptırılmak istendiğinde Şekil 6.9'daki döngü söz konusu olmaktadır.

```
Döngü i=1 : 300000
        PC → Osiloskop (Tetiklenmeye Hazır Ol)
        PC → Sasebo-GII (Gösterilen Dizindeki Açık veri ile şifreleme yap)
        PC ← Osiloskop (Alınan Ölçümü PC'ye Kaydet)
Döngü Son
```

Şekil 6.9: Ölçüm işlemleri.

Çok fazla sayıda ölçüm alınması gerektiğinden bu işlemlerin otomasyonuna ihtiyaç duyulmuştur. Bu amaçla PC'nin SASEBO-GII ile haberleştiği C# kodu içerisinden, PC'nin osiloskopla ihtiyaç duyulan işlemlerin yapıldığı kod parçaları çağrılmıştır. Böylece yukarıda tanımlanmış döngü dakikada 80 ölçüm gibi bir hızla yapılabilmiştir.

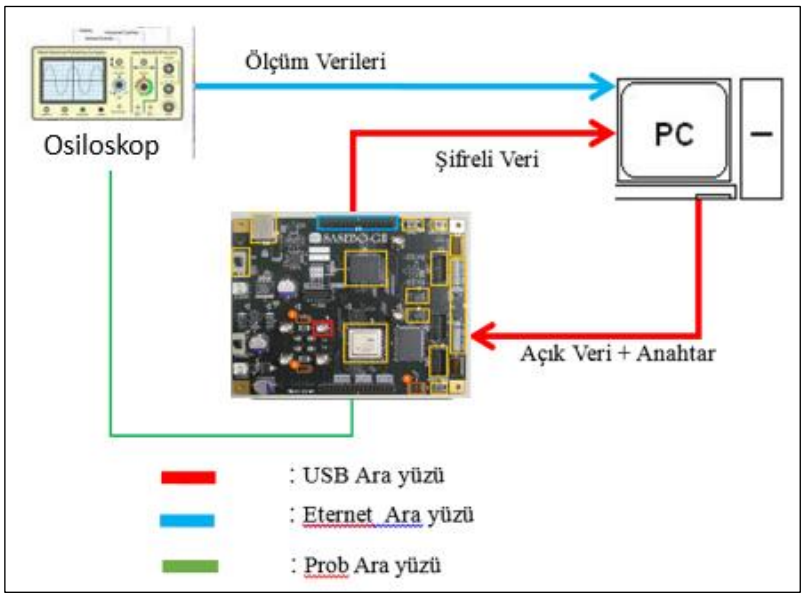
Yukarıda listelenen donanım ve yazılım parçalarının birleşiminden oluşan ölçüm alma düzeneği Şekil 6.10 ve Şekil 6.11'de verilmiştir.



Şekil 6.10: Ölçüm alma düzeneği-1.

Aşağıdaki adımlar ölçümleri ve ilgili veriyi yakalamak için gereklidir. SMA-BNC kablo ve bir adet prob kullanılarak; osiloskopun 1. Kanalı ile J2 üzerinden SMA-BNC kablo kullanılarak güç ölçümleri alınır. 2. Kanaldan ise J6'nın ilk pini kullanılarak osiloskopun tetiklenmesi sağlanır. 1. kanal için, dikey ölçekleme 10mV/div olarak ayarlanmıştır. Tetiklenme sinyali, 2. kanala bağlı prob ile J6'nın ilk pininden alınır. Probun toprak ucu ise kart üzerindeki TP3'e bağlanır. 2. kanal için dikey ölçekleme 1.0 V/div olarak ayarlanmıştır ve tetiklenme modu negatif kenardır. Şekil 4.2'de örnek bir ölçüm gözükmektedir. Ölçüm üzerindeki noktalar AES işleminin hangi turu olduğunu göstermektedir. Örnek ölçümde gözüktüğü gibi herbir ölçüm için 10000 nokta alınmıştır. Hazırlanan AES kodu, frekansı 3 Mhz olacak şekilde sentez edilmiştir.

Düzeneğin kurulmasından sonra ölçüm alma işlemine geçilmiştir. Her bir S-kutusunun analizi için 30000 ölçüm ile çalışılmıştır. Fakat olabildiğince gürültüyü azaltmak için her açık veriden 10 adet ölçüm alınmış ve bunların ortalaması analizde kullanılmıştır. Bu nedenle 30000 bin adet 128 bit rastgele veri içeren bir veri paketi hazırlanmıştır.



Şekil 6.11 Ölçüm alma düzeneği-2.

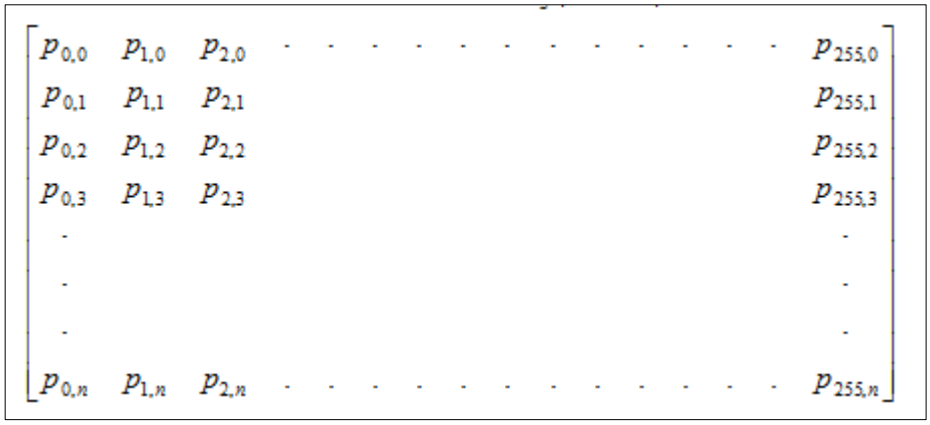
Bu veriler için, belirlenen bir anahtar ile şifreleme işlemleri yaptırılarak 1 GS/s ile 300000 güç ölçümü alınmıştır. Her bir veri için yapılan şifreleme işlemi esnasında alınan güç ölçümü 10000 örneklem ile kaydedilmiştir. Ölçüm alma işlemi sonunda, 30000 açık veri için oluşturulan 30000 güç ölçüm verisi analiz işleminde kullanılmıştır.

7. FARKSAL GÜÇ ANALİZİNİN GERÇEKLENMESİ

Bu çalışmada AES algoritmasındaki S-kutularının çıkışları, DPA saldırısı için hedef seçilmiştir. Bulunan saydamlık derecesi güçlü DSSK'lar ve karşılaştırma amaçlı kullandığımız bir lineer S-kutusu AES algoritmasındaki S-kutuları yerine yerleştirilerek Verilog kodları oluşturulmuştur. Verilog kodları SASEBO-GII'deki kriptografik FPGA'de gerçeklenmiş, Şekil 6.11'de gösterilen düzenekle ölçümler alınmıştır.

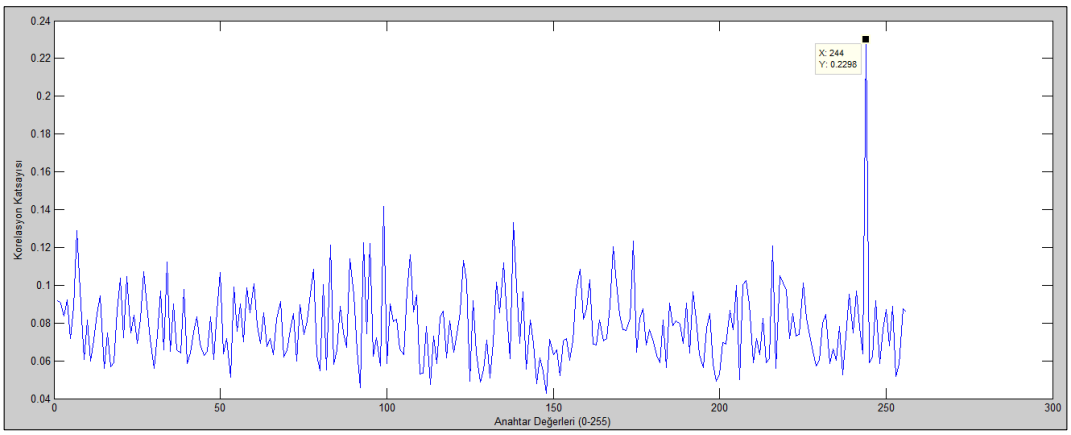
Aşağıdaki işlemler vasıtasıyla FGA atağı gerçeklenmiş ve test edilen her bir S-kutusuna uygulanmıştır:

- Algoritma, aynı gizli anahtar kullanılarak, *n* farklı açık veri için *n*x10 defa koşturulur.
- Her giriş için S-kutusunun çıkışının değiştiği saat darbesini hedef alan, k adet örnekten oluşan, güç ölçümleri hazırlanır. Her bir açık veri için elde edilmiş olan 10 ölçümün ortalaması alınır. Böylelikle, $n \times k$ boyutunda bir ölçüm matrisi (M_1) elde edilir. Matrisin *i*'inci satırı, *i*'inci girişe karşı düşen ölçüm değerlerini içermektedir.
- Bu matrisin her sütununun ortalama değeri alınarak $n \times 1$ boyutunda bir ölçüm sütun matrisi oluşturulur ve her bir sütundan çıkartılarak (M_2) matrisi elde edilir.
- Son turda saldırılan S-kutusunun, olası tüm anahtar baytları ($2^8 = 256$ adet) üzerinden *n* farklı kapalı veriye karşılık gelen girişleri hesaplanır.
- Elde edilen değerlerden yola çıkılarak, S-kutularının güç harcaması Hamming mesafesine göre modellenir. Saldırılan S-kutusuna karşılık gelen tur çıkışları ile bir önceki adımda hesaplanan giriş değerleri arasındaki Hamming mesafesi bulunur. Bu değerlerle $n \times 256$ boyutunda bir tahmin matrisi (M_3) oluşturulur. M_3 matrisinin her sütunu, *n* kapalı veriden elde edilen ve son turun saldırılan S-kutusuna karşılık gelen giriş ve çıkış baytları arasındaki Hamming mesafelerini göstermektedir.



Şekil 7.1: Tahmin matrisi $M_3(n\text{x}256)$.

- Son adımda ise, eşitlik (4.1) kullanılarak M_3 matrisinin her bir sütununun, M_2 matrisinin tüm sütunları ile korelasyonları hesaplanır. Başarılı bir FGA saldırısında, Şekil 7.22'de görüldüğü gibi, doğru anahtar tahminine karşı düşen M_3 sütununun, M_2 matrisi ile korelasyonu yüksek çıkarken, M_3'ün diğer sütunları için oldukça düşük korelasyon verir.



Şekil 7.2: Anahtar tahminlerinin ölçümlerle korelasyonu.

7.1. FGA Sonuçları

Test edilen her bir S-kutusu, AES için hazırlanan Verilog kodu içine yerleştirilip, SASEBO-GII'de gerçeklendikten sonra Bölüm 4.3'de anlatıldığı gibi FGA atağı gerçekleştirilmiştir. Bölüm 4.5'de bahsedilen güvenlik metrikleri kullanılarak atağın başarısı değerlendirilmiştir. Son tur anahtarının bir baytı için gerçekleştirilmiş atağın başarı oranları, tahmin entropisi ve her bir anahtar tahmini

için elde edilen korelasyon katsayıları verilmiştir. Diğer baytlar için gerçekleştirilen FGA atağının sonuçları da benzer sonuçlar vermiştir.

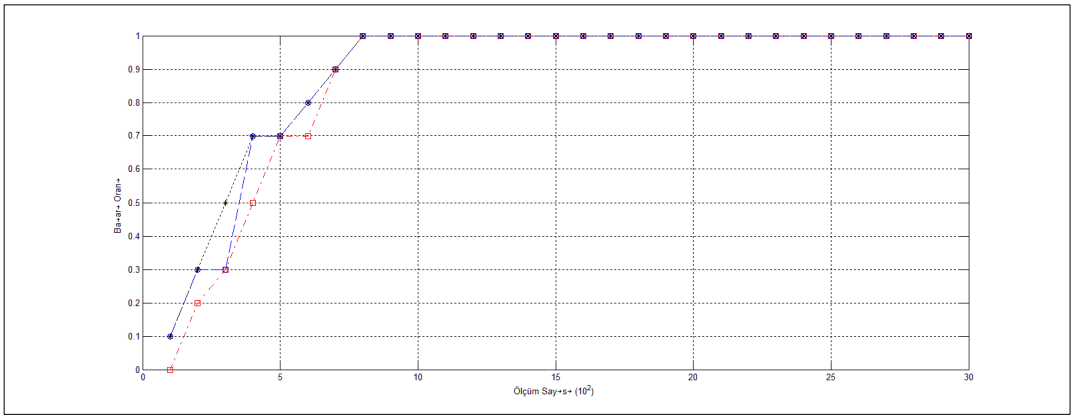
7.1.1. AES S-kutusu İçin FGA Sonuçları

Tablo 7.1'de AES S-kutusunun kriptografik özellikleri verilmiştir. Diğer DSSK'lar ile karşılaştırıldığında saydamlık derecesi daha kötü olmasına rağmen geleneksel kriptografik özelliklerinin daha iyi olduğu görülmektedir.

Tablo 7.1: AES S-kutusu kriptografik özellikleri.

	Doğrusal Olmama	**Farksal Birbiçimlilik**	**Mutlak Gösterge**	**Cebirsel Derece**	**Saydamlık Derecesi**		**SNR**
					τ_F	$\tau_{\underline{F}}$	
AES S-kutusu	112	4	32	7	7.86	6.92	9.56

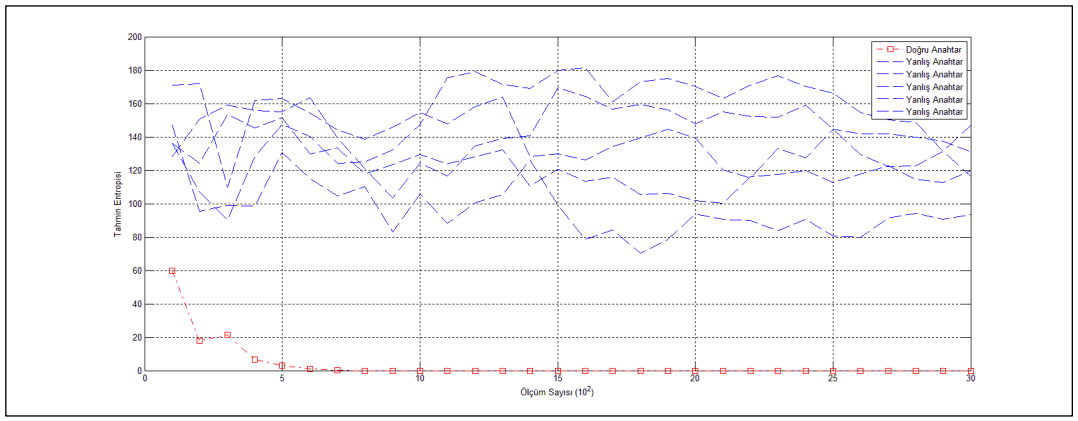
Başarı oranı grafiğinden, 800 ölçümden itibaren tahmin edilen anahtar, doğru anahtarla aynı çıkmaktadır.



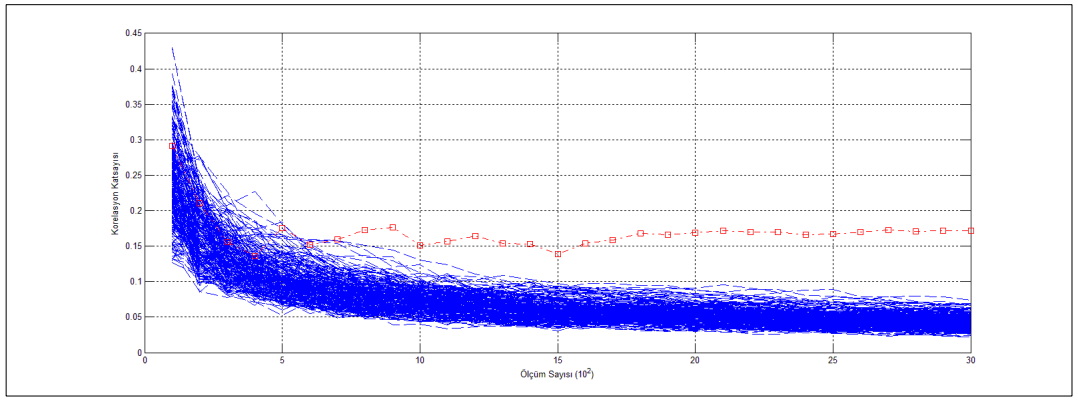
Şekil 7.3: AES S-kutusu için başarı oranı.

Bu çalışmada, başarı oranı ve tahmin entropisi 10 tane ölçüm seti (her birinde 3000 ölçüm bulunmakta) üzerinden elde edilirken korelasyon katsayıları bir adet ölçüm seti kullanılarak elde edilmiştir. Bununla birlikte, Şekil 7.4'deki tahmin

entropisi grafiği ve Şekil 7.5'deki korelasyon katsayısı grafiği kullanılan ölçüm setleri için 800 ölçümden itibaren doğru anahtarı tahmin edildiğini göstermektedir.



Şekil 7.4: AES S-kutusu için tahmin entropisi.



Şekil 7.5: AES S-kutusu için korelasyon katsayıları.

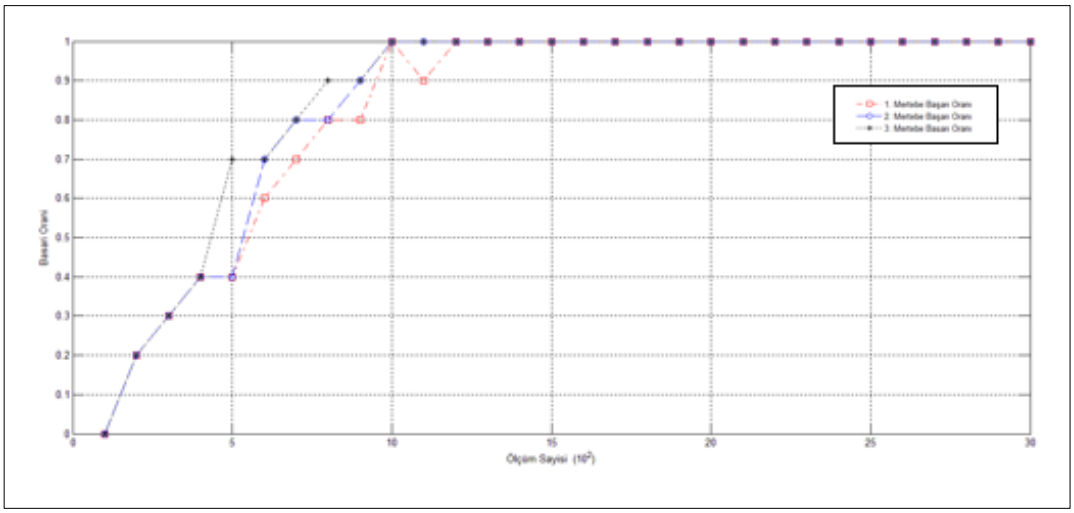
7.1.2. DSSK #1 için FGA Sonuçları

Tablo 7.2 incelendiğinde DSSK #1'in elde edilen diğer DSSK'lar arasında farksal birbiçimliliği AES S-kutusununkine en yakın olan DSSK olduğu gözükmektedir.

Tablo 7.2: DSSK #1 S-kutusu kriptografik özellikleri.

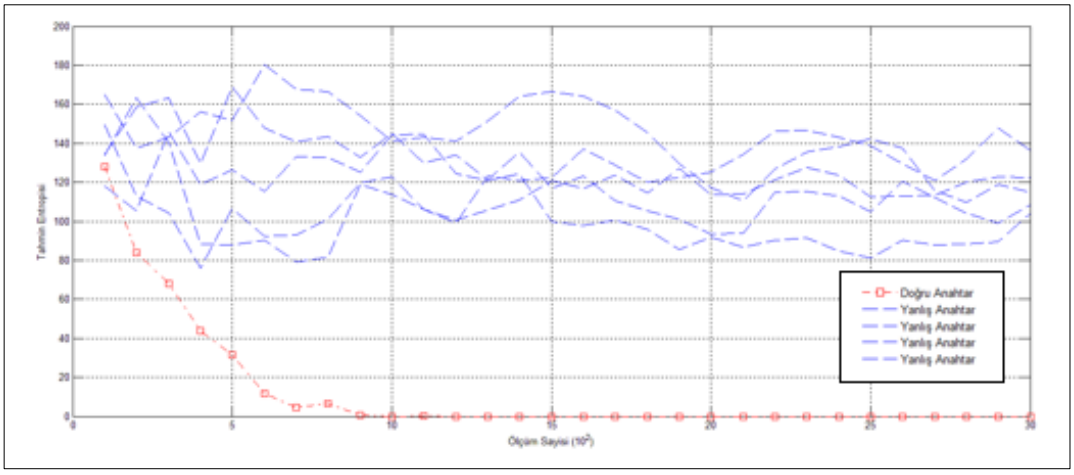
	Doğrusal Olmama	Farksal Birbiçimlilik	Mutlak Gösterge	Cebirsel Derece	Saydamlık Derecesi		SNR
					τ_F	$\tau_{\underline{F}}$	
DSSK #1	104	6	80	7	7.627	6.87	4.67

Şekil 7.6'da verilen başarı oranı grafiğinden, 1200 ölçümden itibaren doğru anahtarın tahmin edildiği anlaşılmaktadır. AES S-kutusunun başarı grafiği ile karşılaştırıldığında, doğru anahtar tahmini için yaklaşık %50 oranında daha fazla ölçüm alınması gerektiği görülmektedir.

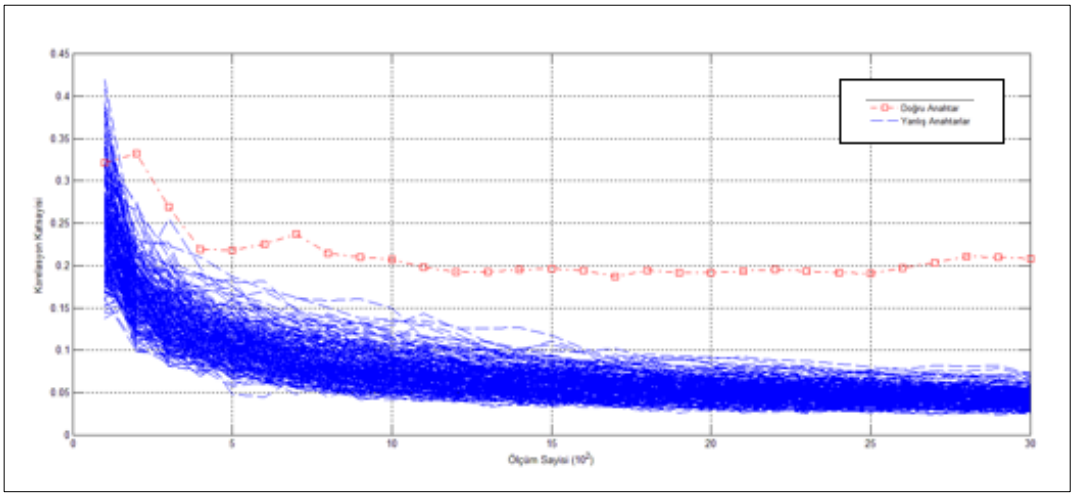


Şekil 7.6: DSSK #1 için başarı oranı.

Şekil 7.7'deki tahmin entropisi ve Şekil 7.8'deki korelasyon katsayıları grafiği kullanılan setler için sırasıyla 1200 ve 200 ölçümden itibaren doğru anahtarın tahmin edildiğini göstermektedir.



Şekil 7.7: DSSK #1 için tahmin entropisi.



Şekil 7.8: DSSK #1 için korelasyon katsayıları.

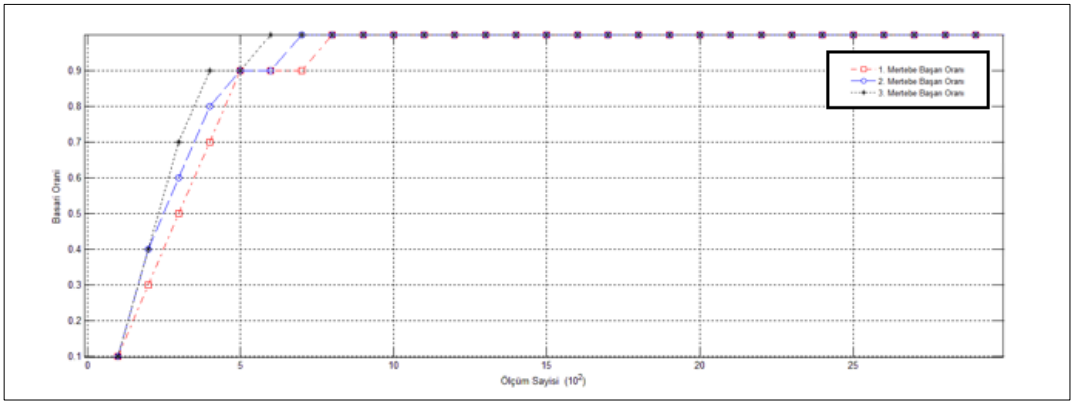
7.1.3. DSSK #2 için FGA Sonuçları

Tablo 7.3'den, DSSK #2'nin saydamlık derecesinin DSSK #1 ve AES S-kutusunun saydamlık derecelerinden daha iyi olduğu görülmektedir.

Tablo 7.3: DSSK #2 S-kutusu kriptografik özellikleri.

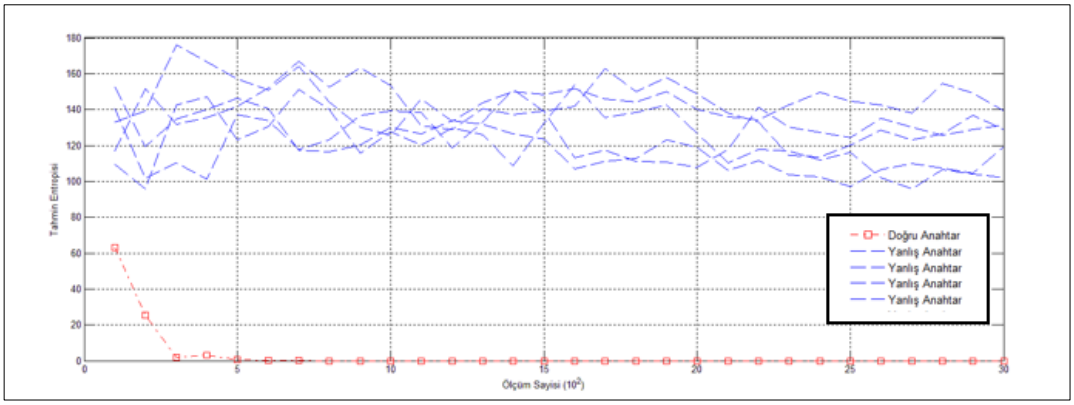
	Doğrusal Olmama	Farksal Birbiçimlilik	Mutlak Gösterge	Cebirsel Derece	Saydamlık Derecesi		SNR
					τ_F	$\tau_{\underline{F}}$	
DSSK #2	104	8	88	7	7.555	6.93	7.04

Fakat, DSSK #2 için elde edilen başarı oranı grafiği, doğru anahtar tahmini için gerekli olan ölçüm sayısının (800 ölçüm), DSSK #1'de doğru anahtar tahmini için gerekli olan ölçüm sayısından daha az ve AES S-kutusu ile aynı olduğunu göstermektedir.



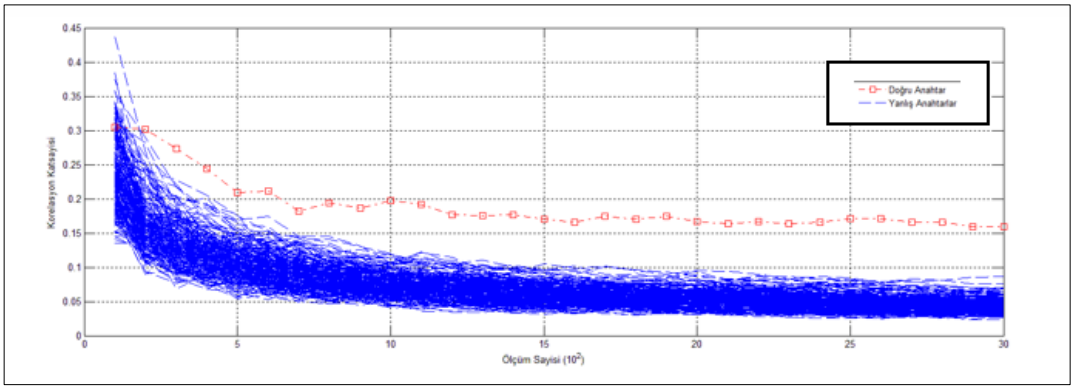
Şekil 7.9: DSSK #2 için başarı oranı.

Bundan dolayı, düşük saydamlık derecesinin her zaman doğru anahtar tahmini için gerekli olan ölçüm sayısını artırmayabileceği sonucuna varılmıştır.



Şekil 7.10: DSSK #2 için tahmin entropisi.

Şekil 7.10'daki tahmin entropisi ve Şekil 7.11'deki korelasyon katsayıları grafiği kullanılan setler için sırasıyla 800 ve 200 ölçümden itibaren doğru anahtarın tahmin edildiğini göstermektedir.



Şekil 7.11: DSSK #2 için korelasyon katsayıları.

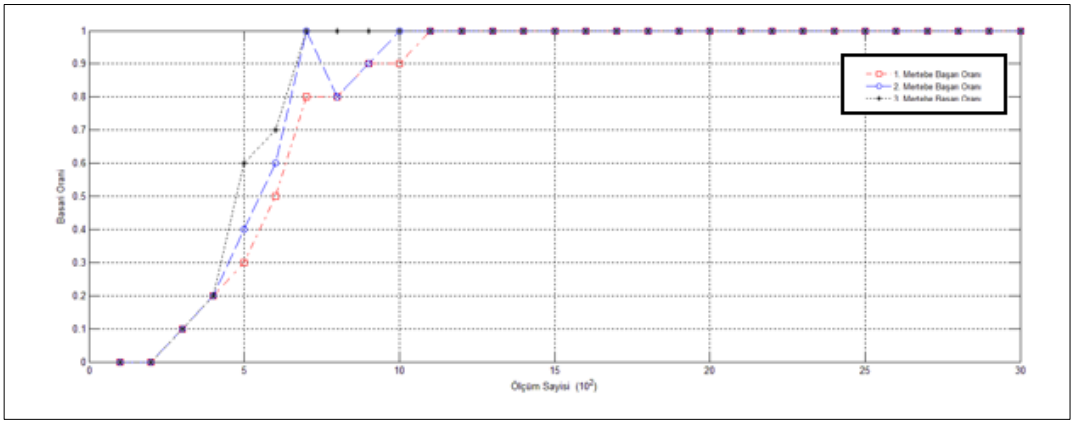
7.1.4. DSSK #3 FGA Sonuçları

Tablo 7.4'den, DSSK #3'ün saydamlık derecesinin AES S-kutusunun ve DSSK #1 ve DSSK #2'nin saydamlık derecelerinden daha düşük olduğu görülmektedir. Bununla birlikte Şekil 7.12'deki başarı oranı grafiğinden, DSSK #3 için saydamlık derecesindeki düşüşe paralel olarak FGA karşısındaki direncin arttığı görülmektedir.

Tablo 7.4: DSSK #3 S-kutusu kriptografik özellikleri.

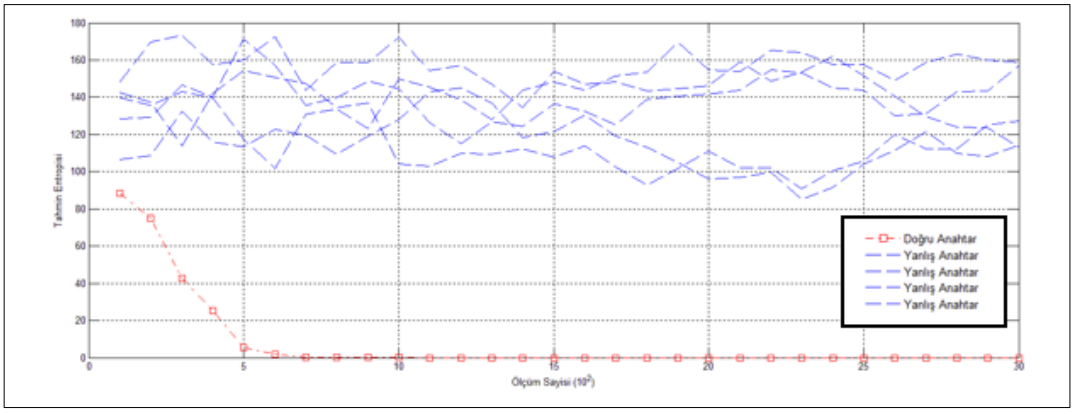
	Doğrusal Olmama	Farksal Birbiçiml	Mutlak Gösterge	Cebirsel Derece	Saydamlık Derecesi	SNR

					τ_F	$\tau_{\underline{F}}$	
DSSK #3	104	8	72	7	7.476	6.66	9.15

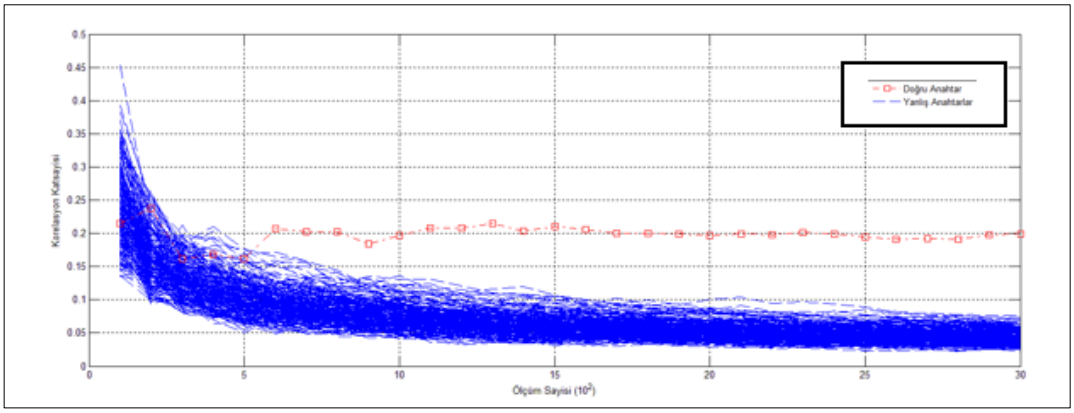


Şekil 7.12: DSSK #3 için başarı oranı.

Şekil 7.13'deki tahmin entropisi ve Şekil 7.14'deki korelasyon katsayıları grafiği kullanılan setler için sırasıyla 1200 ve 600 ölçümden itibaren doğru anahtarın tahmin edildiğini göstermektedir.



Şekil 7.13: DSSK #3 için tahmin entropisi.



Şekil 7.14: DSSK #3 için korelasyon katsayıları.

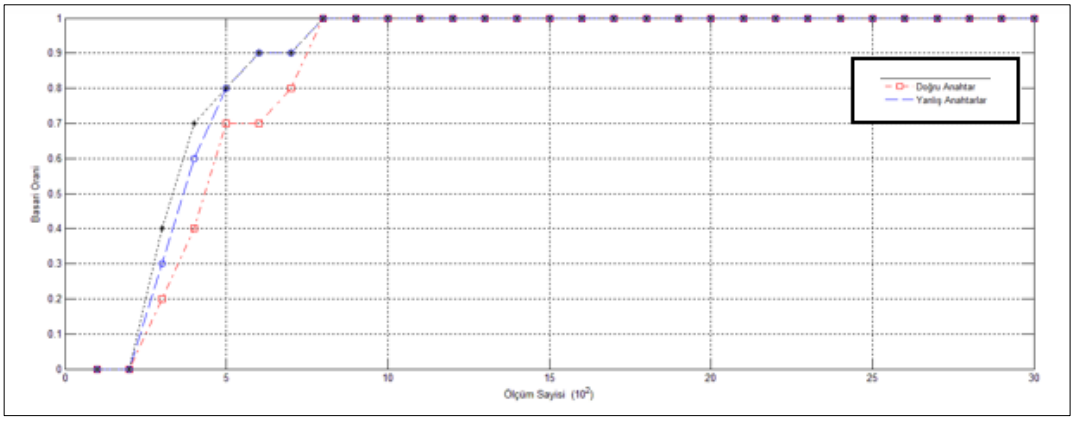
7.1.5. DSSK #4 için FGA Sonuçları

Elde edilen DSSK'lar içinde saydamlık derecesi en düşük olanın DSSK #4 olduğu, Tablo 7.5'de gözükmektedir.

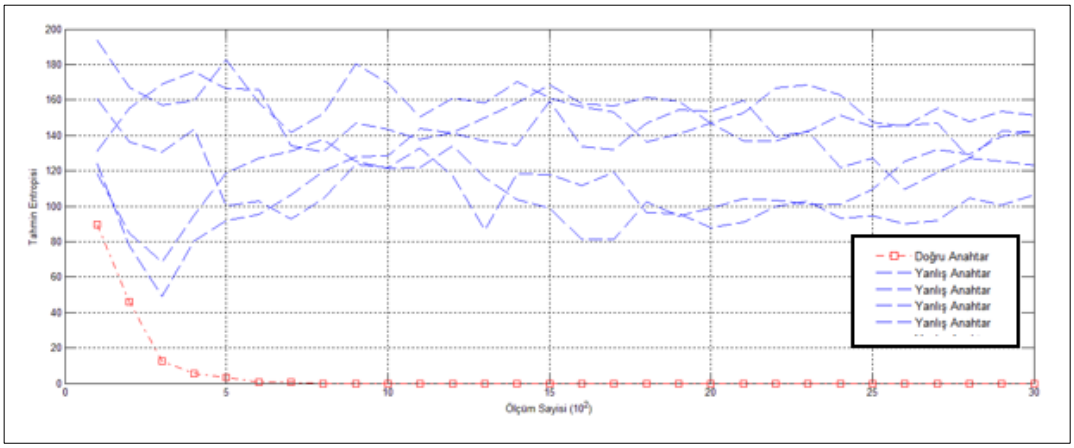
Tablo 7.5: DSSK #4 S-kutusu kriptografik özellikleri.

	Doğrusal Olmama	Farksal Birbiçimlilik	Mutlak Gösterge	Cebirsel Derece	Saydamlık Derecesi		SNR
					τ_F	$\tau_{\underline{F}}$	
DSSK #4	102	8	88	7	7.31	6.53	11.78

Fakat, Şekil 7.15'de verilen başarı oranı grafiğinden, doğru anahtarı tahmin etmek için AES S-kutusu ve DSSK #2 ile aynı sayıda ölçüm sayısı gerektirdiği anlaşılmaktadır.

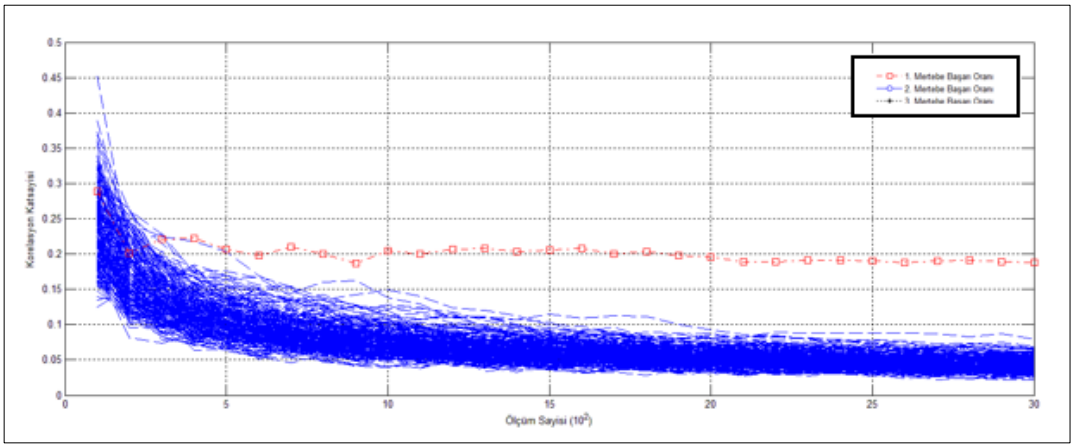


Şekil 7.15: DSSK #4 için başarı oranı.



Şekil 7.16: DSSK #4 için tahmin entropisi.

Şekil 7.16'deki tahmin entropisi ve Şekil 7.17'deki korelasyon katsayıları grafiği kullanılan setler için sırasıyla 800 ve 400 ölçümden itibaren doğru anahtarın tahmin edildiğini göstermektedir.



Şekil 7.17: DSSK #4 için korelasyon katsayıları.

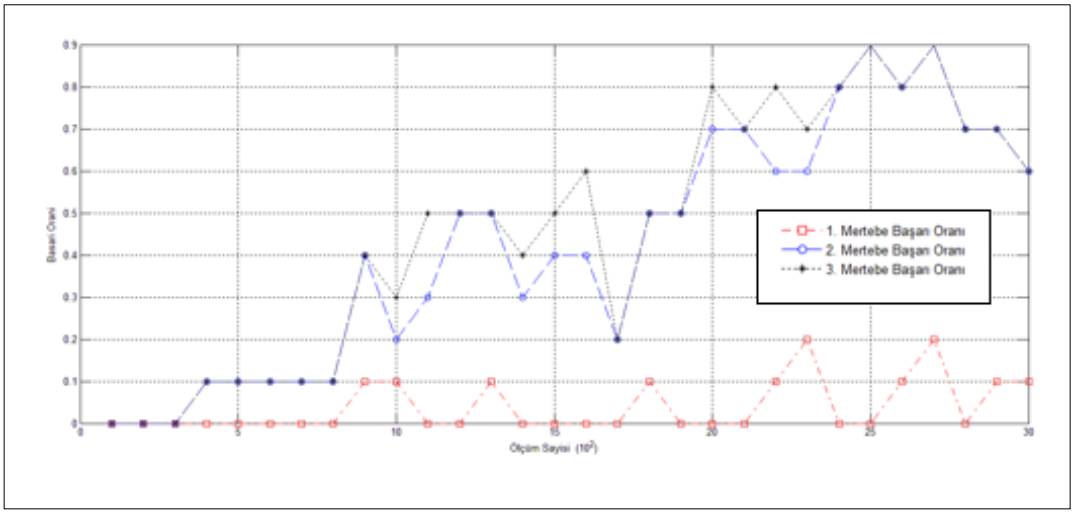
7.1.6. Lineer S-kutusu FGA Sonuçları

Karşılaştırma amaçlı olarak, saydamlık derecesi oldukça düşük olan lineer bir S-kutusu için FGA atağı gerçekleştirilmiştir.

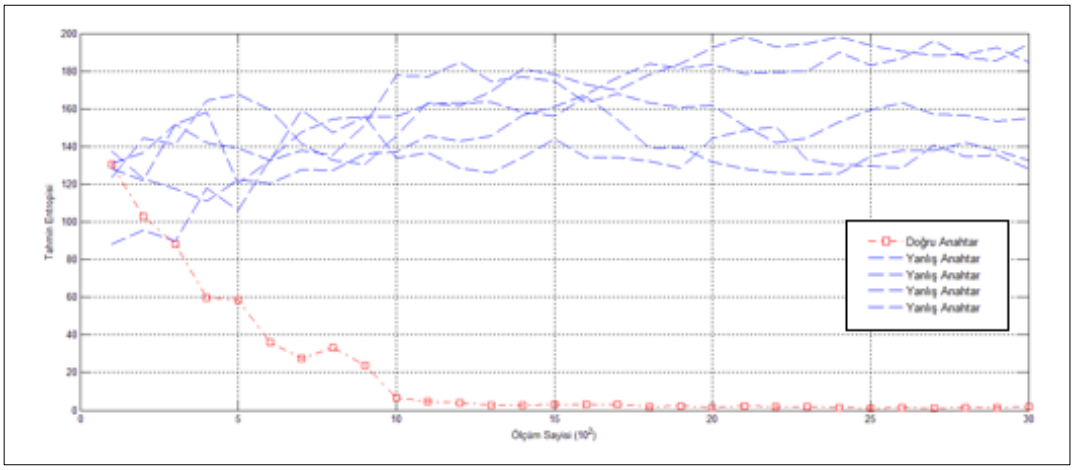
Tablo 7.6: Lineer S-kutusu kriptografik özellikleri.

	Doğrusal Olmama	**Farksal Birbiçimlilik**	**Mutlak Gösterge**	**Cebirsel Derece**	**Saydamlık Derecesi**		**SNR**
					τ_F	$\underline{\tau_F}$	
Lineer S-kutusu	0	256	256	1	5.83	0	2.83

Şekil 7.18'de verilen başarı oranı grafiğinden, 3000 ölçüm içerisinde doğru anahtarın tahmin olasılığının en fazla %20 olabildiği, bunun da kararlı olmadığı görülmektedir. Bunun yanısıra, doğru anahtarın tahmin edilen ilk iki anahtar arasında olma olasılığı, 2000 ölçümden itibaren %70 olmaktadır.

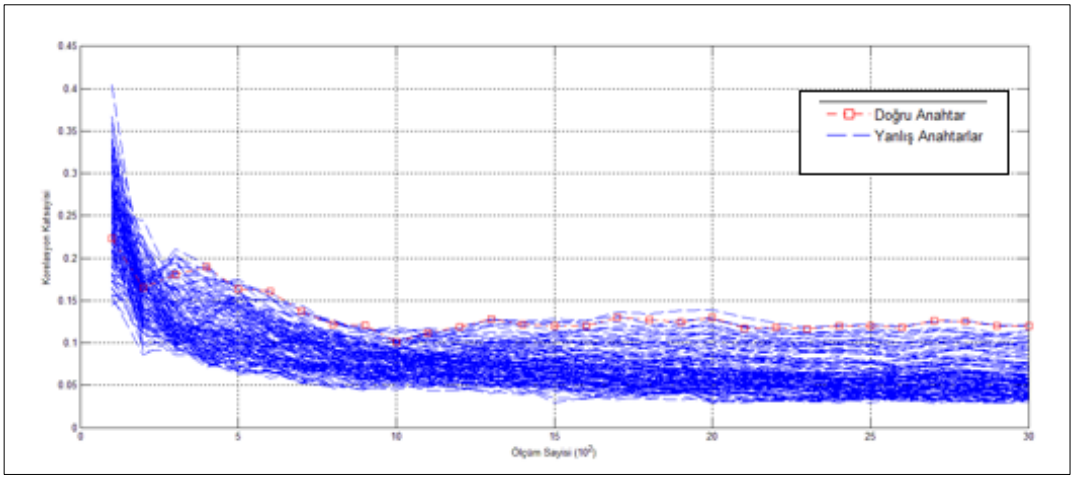


Şekil 7.18: Lineer S-kutusu için başarı oranı.



Şekil 7.19: Lineer S-kutusu için tahmin entropisi.

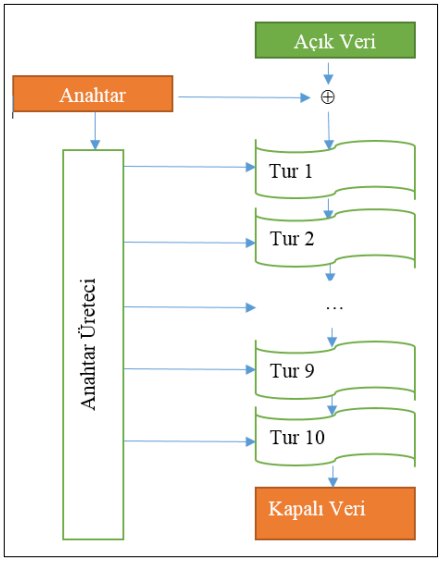
Şekil 7.19'deki tahmin entropisi ve Şekil 7.20'deki korelasyon katsayıları grafikleri, Şekil 7.18'deki başarı oranı grafiğinden vardığımız sonuçları doğrular niteliktedir.



Şekil 7.20: Lineer S-kutusu için korelasyon katsayıları.

7.2. Simülasyon ve Sonuçları

Simülasyon, Şekil 7.21'de gösterildiği gibi Matlab programında bir betik yazılarak gerçekleştirilmiştir.

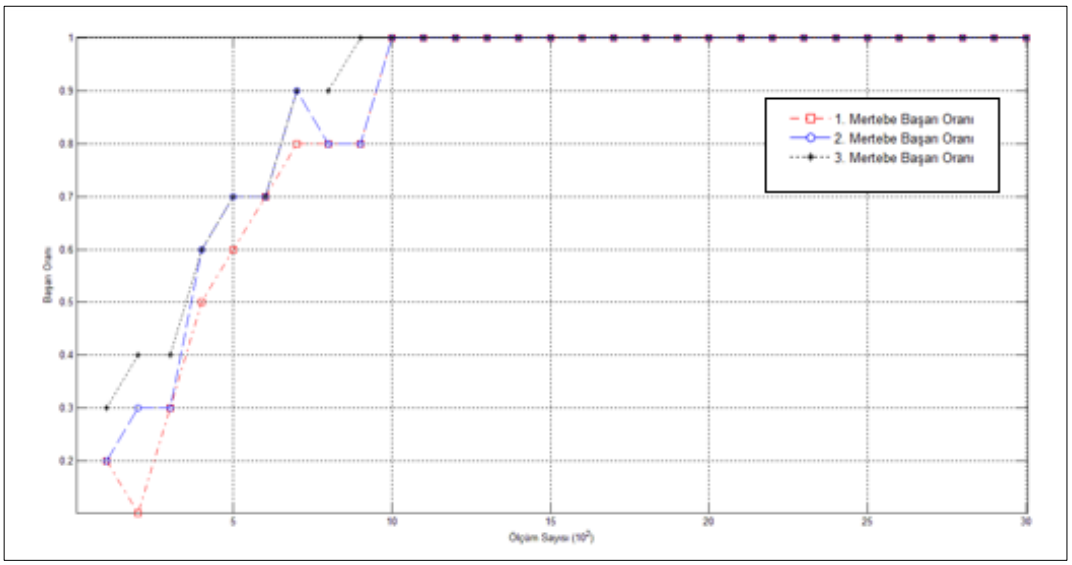


Şekil 7.21: Matlab'de yazılan AES simülasyon akışı.

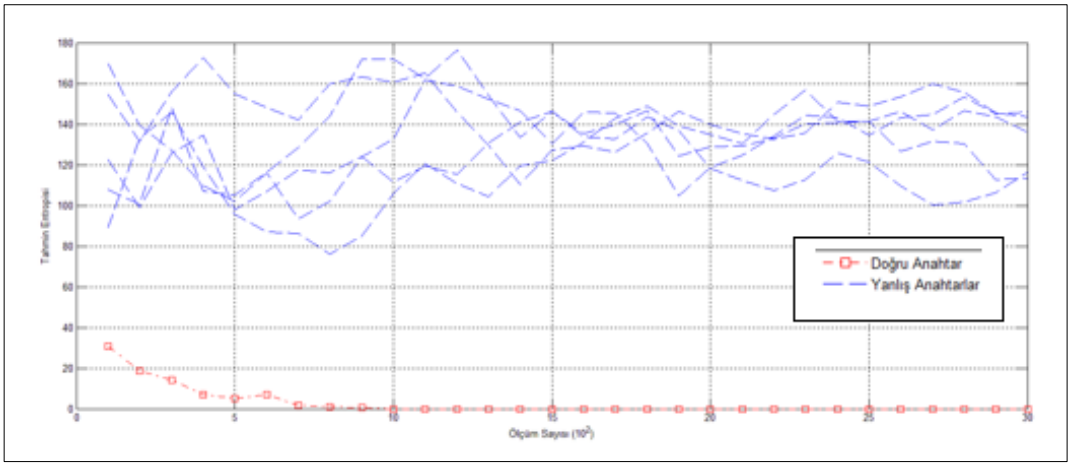
Bu betik sırasıyla şu işlemleri gerçekleştirmektedir:

- 30000 tane 128 bitlik farklı açık veriler AES ile şifrelenmiştir.
- Tüm tur çıkışları $TÇ^{(1)}, TÇ^{(2)}, \ldots, TÇ^{(10)}$ olarak gösterilsin. Bu modelde, simüle edilen güç ölçümleri üzerinde Hamming mesafesi kullanılarak korelasyon güç analizi (CPA) gerçekleştirilmiştir. Simülasyon için güç ölçümleri son tur çıkışı $TÇ^{(10)}$ (kapalı veri) ile son tur girişi ($TÇ^{9}$) arasındaki Hamming mesafesine göre üretilmiştir: $HW(TÇ^{10}, TÇ^{9}) + r$. Burada r, ortalaması sıfır, standart sapması σ olan Gauss gürültüsüdür. Gerçekleştirdiğimiz simülasyonda $\sigma = 12$ olarak alınmıştır. i 'inci açık veriye karşılık gelen güç ölçümü vektörü $g_{i,1}, g_{i,2}, \ldots, g_{i,T}$ olmak üzere; T, güç ölçümünün uzunluğunu göstermektedir. Simülasyonda T değeri 12 olarak alınmıştır.
- Bölüm 6.4'de anlatılan Farksal Güç Analizi, üretilen ölçümler üzerine uygulanmıştır.

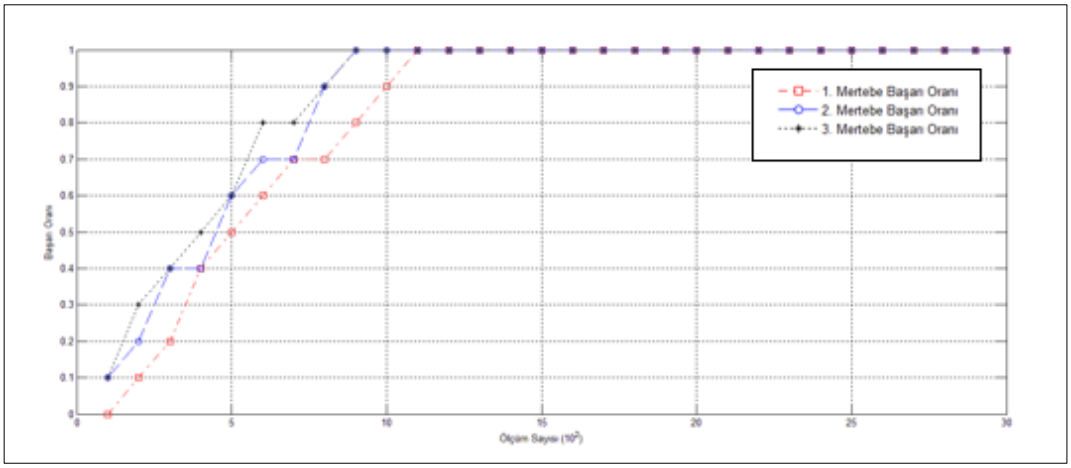
Aşağıdaki grafikler her bir S-kutusu için 3000 ölçümden oluşan 10 set ve toplamda 30000 ölçüm ile gerçekleşen sonuçlardır.



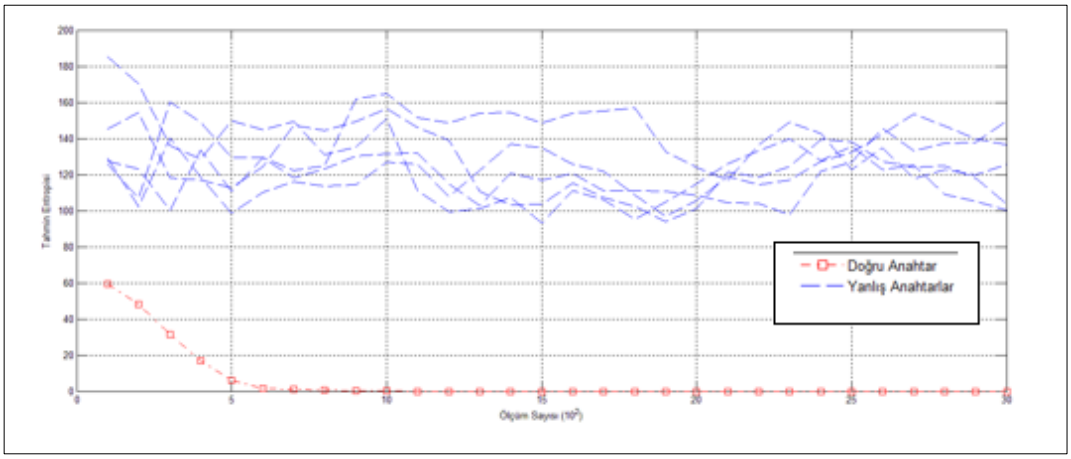
Şekil 7.22: AES S-kutusu başarı oranı simülasyonu.



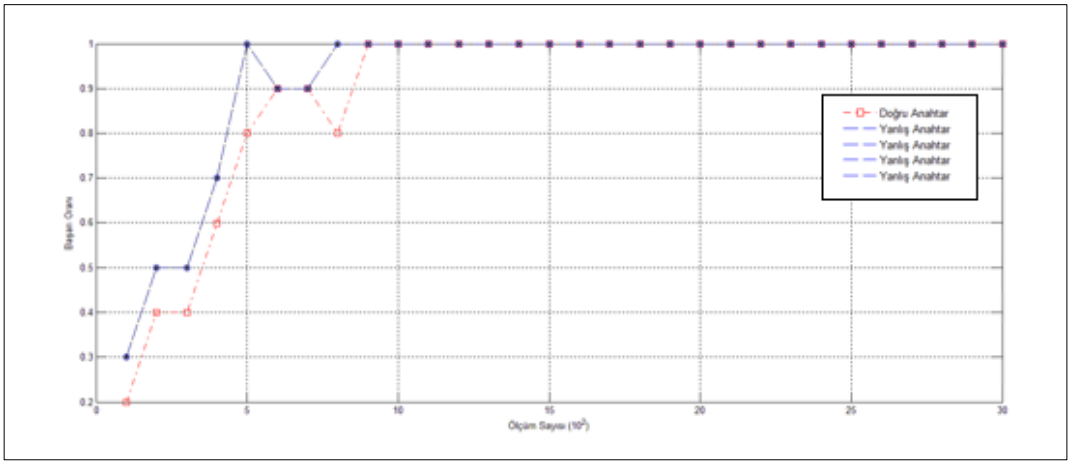
Şekil 7.23: AES S-kutusu tahmin entropisi simülasyonu.



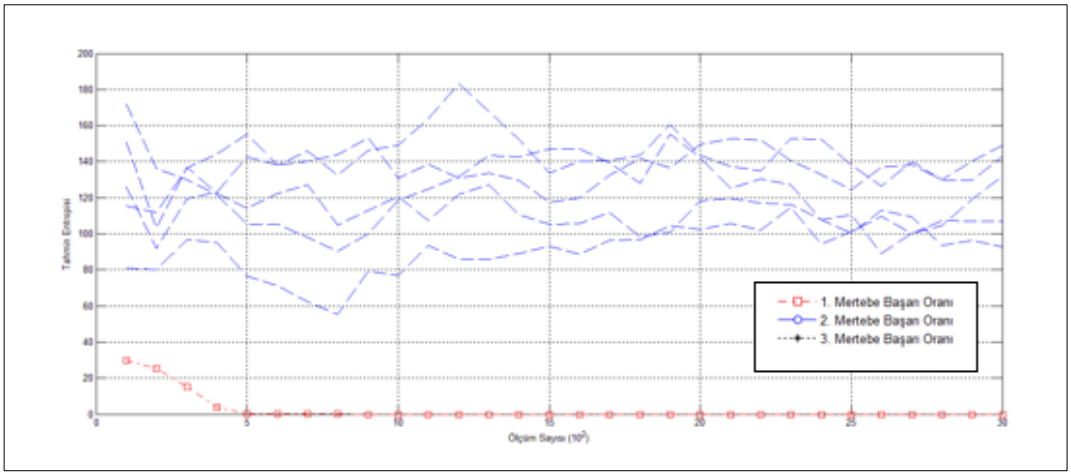
Şekil 7.24: DSSK #1 için başarı oranı simülasyonı.



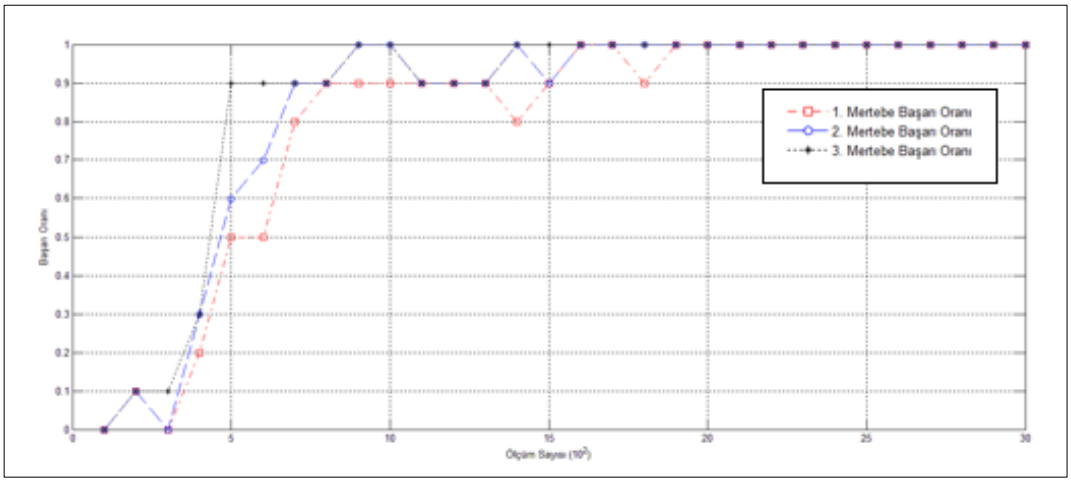
Şekil 7.25: DSSK #1için tahmin entropisi simülasyonu.



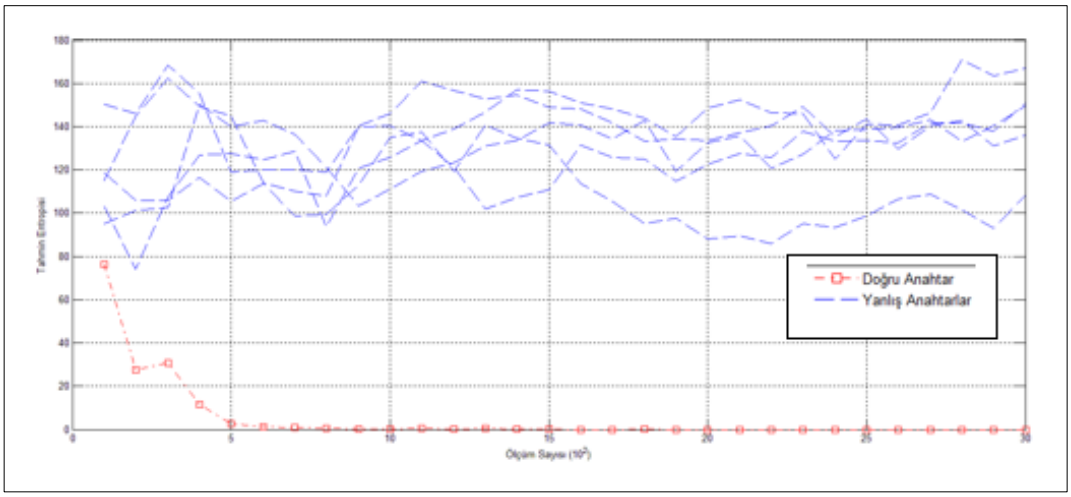
Şekil 7.26: DSSK #2 için başarı oranı simülasyonu.



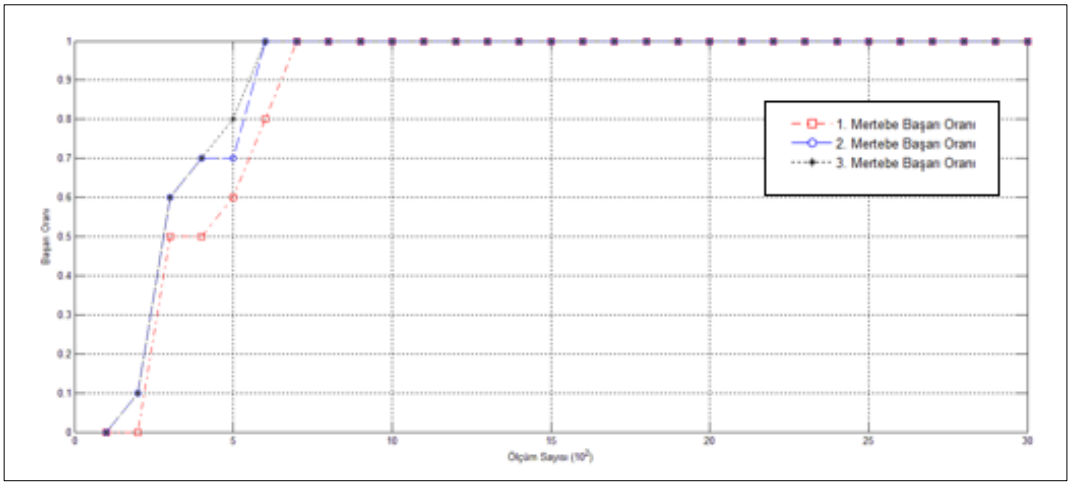
Şekil 7.27: DSSK #2 için tahmin entropisi simülasyonu.



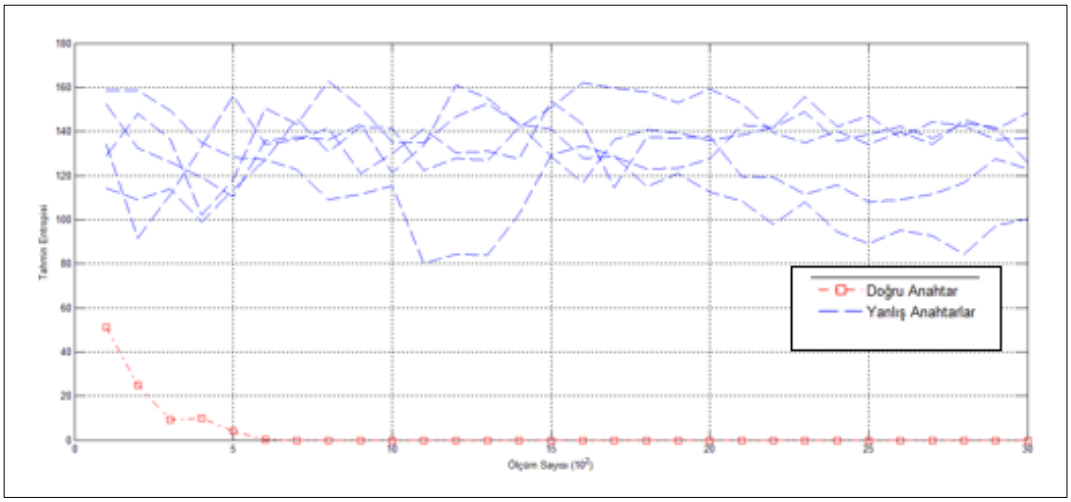
Şekil 7.28: DSSK #3 için başarı oranı simülasyonı.



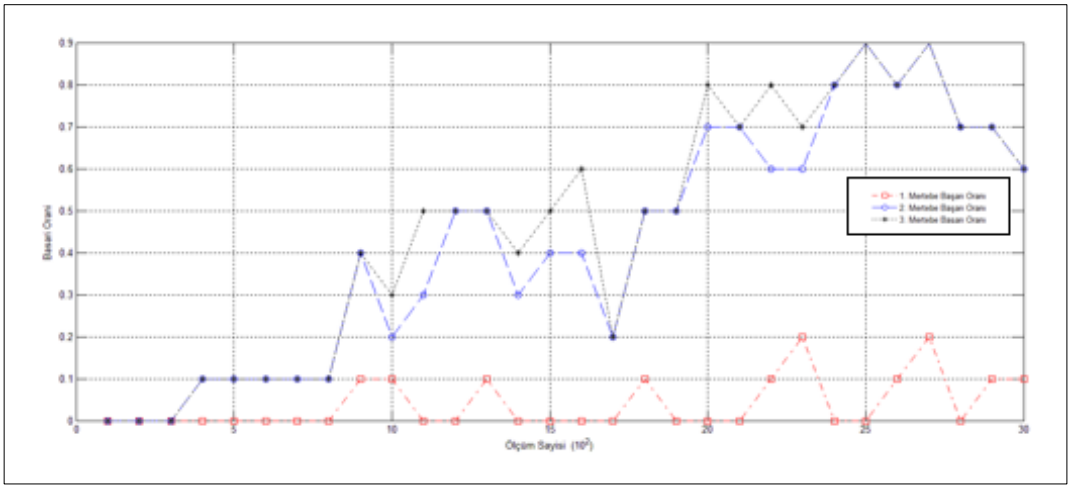
Şekil 7.29: DSSK #3 için tahmin entropisi simülasyonu.



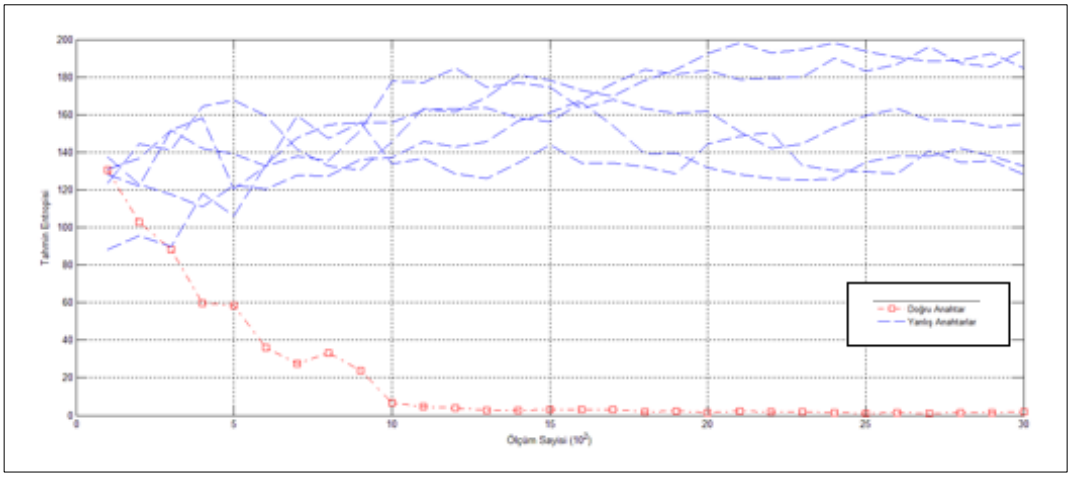
Şekil 7.30: DSSK #4 için başarı oranı simülasyonı.



Şekil 7.31: DSSK #4 için tahmin entropisi simülasyonu.



Şekil 7.32: Lineer S-kutusu başarı oranı simülasyonu.



Şekil 7.33: Lineer S-kutusu tahmin entropisi simülasyonu.

Simülasyon sonuçları da SASEBO-GII kartındaki gerçekleme sonuçlarımıza paralel olarak, saydamlık derecesindeki düşmenin her zaman doğru anahtar tahmini için gerekli olan ölçüm sayısını azaltmadığını, bununla birlikte lineer S-kutusunda olduğu gibi saydamlık derecesindeki büyük bir düşüşün FGA karşısındaki dayanıklılığı önemli ölçüde artırabileceği görülmektedir. Fakat lineer bir S-kutusu kriptografik açıdan bir önem taşımamaktadır.

8. SONUÇLAR

Tez kapsamında, 8x8 DSSK'lar, [11]'te sunulmuş olan en dik iniş prensibine dayalı arama algoritması ile aranmıştır. Bulunan DSSK'lar, doğrusal olmama değeri 102 ve 104, cebirsel dereceleri 7, mutlak göstergeleri 88'den daha düşük ve en önemlisi saydamlık dereceleri ≥7.31 ve FGA SNR'ı ≥4.67 olarak bulunmuştur.

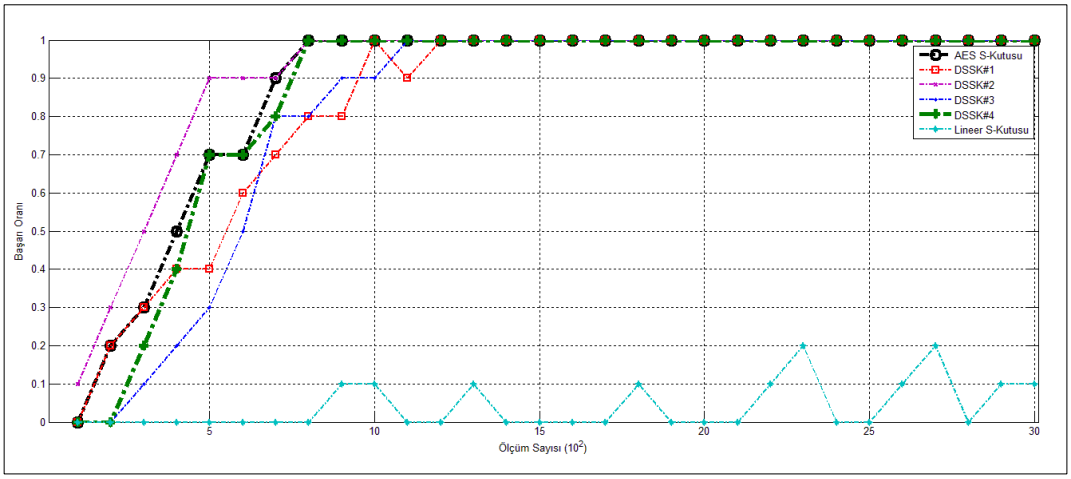
Elde edilen DSSK'lar, geleneksel kriptografik özellikleri ile birlikte saydamlık derecesi ve FGA SNR'ı bakımından literatürde [12-13,15] bulunan S-kutularından daha iyi kriptografik özelliklere sahiptir.

AES algoritmasındaki S-kutusu ile bulunan DSSK'lar yer değiştirilerek FGA atağı gerçekleştirilip, tahmin entropisi ve başarı oranı gibi YKA güvenlik metrikleriyle değerlendirilmiştir. Bu metrikler, gerçekleştirdiğimiz Hamming mesafesine dayalı korelasyon güç analizi ile, AES'in son tur anahtarının elde edilebilmesi için gerekli olan ortalama ölçüm sayısı hakkında bilgi vermektedir. Bu analizde belirli bir bayt için metrikler hazırlanmıştır.

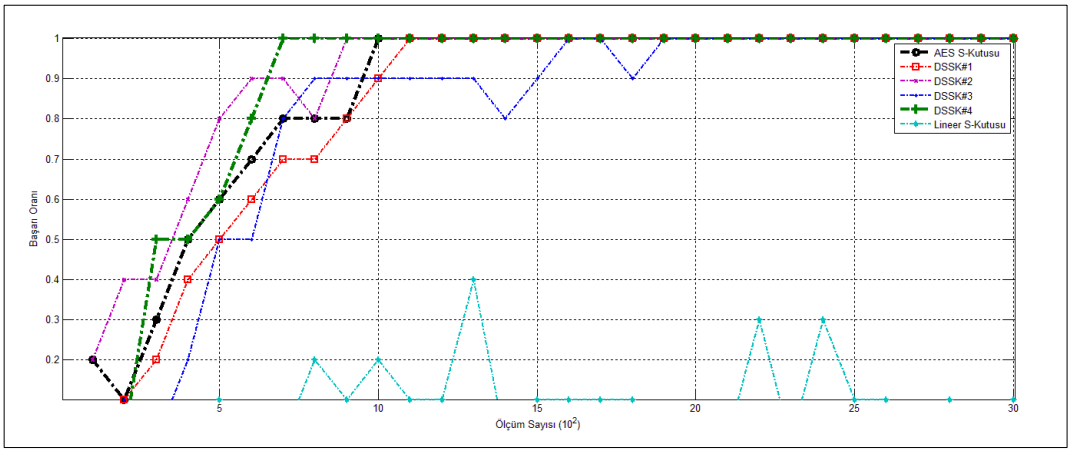
Şekil 8.1 incelendiğinde, en düşük saydamlık derecesine sahip ($\tau_F = 5.83$) lineer S-kutusunun beklendiği gibi başarı oranı, 3000 ölçümde diğer S-kutularına göre net bir şekilde düşük çıkmıştır.

Lineer S-kutusundan sonra en düşük saydamlık derecesine sahip olan DSSK #4'ün ve AES S-kutusuna göre saydamlık derecesi düşük olan DSSK #2'nin başarı oranları, beklenmedik bir şekilde AES S-kutusu ile aynı sayıda ölçüm için %100'e çıkmıştır.

DSSK #1 ve DSSK #3 ise AES S-kutusuna göre daha düşük saydamlık derecesine sahip olduklarından dolayı beklendiği üzere başarı oranları ancak sırasıyla 1000 ve 1100 ölçümde %100 olabilmiştir.



Şekil 8.1: DSSK'ların birinci mertebe başarı oranlarının karşılaştırılması.



Şekil 8.2: DSSK'ların birinci mertebe başarı oranlarının simülasyon karşılaştırması.

Deneysel elde edilen sonuçların yanında Bölüm 6.2'de anlatılan yöntemle simülasyon gerçekleştirilmiş ve farksal güç analizi uygulanmıştır. Bu simülasyonun sonuçları Şekil 8.2'de yer almaktadır. Lineer S-kutusunun başarı oranı, beklendiği gibi genellikle tahmin edilen anahtarın doğru anahtar olmadığını göstermektedir. Fakat, saydamlık derecesi en düşük olan DSSK #4 ile AES S-kutusuna göre saydamlık derecesi düşük olan DSSK #2'nin başarı oranları, AES S-kutusunun başarı oranından daha yüksek çıkmaktadır.

DSSK #1 ve DSSK #3'ün hem gerçeklemede hem de simülasyonda AES S-kutusuna göre daha güçlü olduğu gözükmektedir. Buraya kadar, yukarıdaki başarı oranı grafikleri [6]'daki saydamlık derecesi tanımına göre yorumlanmıştır. Bununla birlikte, [13]'de tekrar tanımlanan saydamlık derecesi ve FGA SNR'ı [14] ele

alındığında da elde edilen DSSK'ların tümü için tutarlı bir parametre olmadıkları görülmektedir.

Sonuç olarak, hem deneysel hem de simülasyon sonuçlarına bakarak, AES'in son tur anahtarının belirli bir baytını ele aldığımızda saydamlık derecesinin her zaman için FGA atağına karşı olan direnci artırmadığı anlaşılmaktadır. Daha kapsamlı analiz için tüm anahtar baytlarının ele alınması ve SNR gibi başka metriklerin de göz önünde bulundurulması gerekmektedir.

KAYNAKLAR

[1] Matsui M., (1994), "Linear cryptanalysis method for DES cipher", Proceedings of EUROCRYPT'93, Lecture Notes in Computer Science, 765, 386-397.

[2] Biham E., Shamir A., (1991), "Differential cryptanalysis of DES-like cryptosystems", Journal of Cryptology, 4 (1), 3-72.

[3] Lai X., (1994), "Higher order derivatives and differential cryptanalysis", The Springer International Series in Engineering and Computer Science, 276, 227-233.

[4] Kocher P. C., Jaffe J., Jun B., (1999) "Differential Power Analysis", Lecture Notes in Computer Science, 1666, 388-397.

[5] Kommerling O. ve Kuhn, M.G., (1999). "Design principles for tamper resistant smartcard processors", Proceedings of the USENIX Workshop on Smartcard Technology, 9-20, Chicago/Illinois/USA, 10-11 Mayıs 1999.

[6] Prouff E., (2005), "DPA Attack and S-boxes", FSE 2005, Lecture Notes in Computer Science, 3557, 424-441.

[7] Carlet C., (2005), "On highly nonlinear S-Boxes and their inability to thwart DPA attacks", Lecture Notes in Computer Science, 3797, 507-522.

[8] Mazumdar B., Mukhopadhyay D., Sengupta I., (2013), "Constrained Search for a Class of Good Bijective S-boxes with Improved DPA Resistivity", IEEE Transactions on Information and Forensics, 12(8), 2154-2163.

[9] Mazumdar B., Mukhopadhyay D., Sengupta I., (2013), "Design and Implementation of Rotation Symmetric S-boxes with High Nonlinearity and High DPA Resiliency", In IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 87-92, Austin/Texas, 2-3 Haziran 2013

[10] Picek S., Ege B., Batina L., Jakobovic D., Chmielewski L., Golub M., (2014), "On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box", In Proceedings of the First Workshop on Cryptography and Security in Computing Systems", 13-18, Viyana/Avusturya, 20 Ocak 2014.

[11] Kavut S., Yucel M. D., (2005), "A New Algorithm for The Design of Strong oolean Functions", First National Cryptology Symposium, 95-105, Ankara/Turkiye, 15-17 Aralık 2006.

[12] Nyberg K., (1994), "Differentially uniform mappings for cryptography", Lecture Notes in Computer Science, 765, 55-64.

[13] Web 1, (2014), http://eprint.iacr.org/2014/367.pdf, (Erişim Tarihi: 14/05/2014).

[14] Guilley S., Hoogvorst P., Pacalet R., (2004), "Differential power analysis model and some results", Smart Card Research and Advanced Applications VI, 153, 127-142.

[15] Rijmen V., Barreto P. S. L. M., Filho D. L. G., (2008), "Rotation Symmetry in Algebraically Generated Cryptographic Substitution Tables", Information Processing Letters, 106(6), 246-250.

[16] Stanica P., Maitra S., (2008), "Rotation Symmetric Boolean Functions−Count and Cryptographic Properties", Electroinc Notes in Discrete Mathematics", 15, 139-145.

[17] Yucel M. D., (2001), "Alternative Nonlinearity Criteria for Boolean Functions", 2001-1, Electrical and Electronics Engineering Department, Middle East Technical University, Turkey.

[18] Kocher P. C., (1996), "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", Lecture Notes in Computer Science, 1109, 104-113.

[19] Kocher P. C., Jaffe J., Jun B., (1999) "Differential Power Analysis", Lecture Notes in Computer Science, 1666, 388-397.

[20] Boneh, D., DeMillo, R.A., Lipton R.J., (1997), "On the importance of checking cryptographic protocols for faults", Lecture Notes in Computer Science, 1233, 37-51.

[21] Kang S. M. ve Leblebici Y., (2002). "CMOS Digital Integrated Circuits: Analysis and Design", 0072460539, McGraw-Hill Science Engineering Math.

[22] Brier E., Clavier C., and Olivier F., (2004), "Correlation power analysis with a leakage model", Cryptographic Hardware and Embedded Systems (CHES), 135-152, Berlin/Heidelberg/Germany, Aug 2004.

[23] Francois-Xavier S., Tal G. M., Moti Y., (2009), "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks", Lecture Notes in Computer Science, 5479, 443-461.

[24] Kavut S., (2012), "Results on Rotation-Symmetric S-boxes", Information Sciences, 201, 93-113.

[25] Zahng M., Zheng Y., (1995), "GAC-the Criterian for Global Avalanche Characteristics of Cryptographic functions", Journal of Universal Computer Science, 1(5), 320-337.

[26] Web 2, (2014), http://www.rcis.aist.go.jp/special/SASEBO/index-en.html,

(Erişim Tarihi: 14/01/2014).

[27] Web 3, (2014), http://www.ftdichip.com/Drivers/D2XX.htm, (Erişim Tarihi: 14/01/2014).

[28] Web 4, (2014), http://www.rcis.aist.go.jp/special/SASEBO/index-en.html, (Erişim Tarihi: 14/01/2014).

[29] Web 5, (2014), http://www.xilinx.com/ise/logic_design_prod/webpack.htm, (Erişim Tarihi: 14/01/2014).

ÖZGEÇMİŞ

1987 yılında Karaman'da doğan Muhammet Ali EVCİ, 2010 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliğinden mezun olmuştur. 2011 yılından beri TÜBİTAK BİLGEM Ortak Kriterler Test Merkezi Laboratuvarında (OKTEM) Common Criteria Uzman Değerlendirici olarak çalışmaktadır.

Evli ve bir kızı vardır.

EKLER

Ek A: Tez Çalışması Kapsamında Kabul Edilen Yayınlar

Evci M. A., Kavut S., (2014), "DPA Resilience of Rotation-Symmetric S-Boxes", The 9th International Workshop on Security-IWSEC2014, Hirosaki, Aomori, Japan, 27-29 Ağustos 2014.