İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

RASPBERRY PI ÜZERİNDE GERÇEKLENMİŞ RSA ALGORİTMASINA YAN KANAL ANALİZİ

YÜKSEK LİSANS TEZİ

Ersin HATUN

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

NİSAN 2018

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

RASPBERRY PI ÜZERİNDE GERÇEKLENMİŞ RSA ALGORİTMASINA YAN KANAL ANALİZİ

YÜKSEK LİSANS TEZİ

Ersin HATUN
504121362

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Sıddıka Berna ÖRS YALÇIN

NİSAN 2018

İTÜ, Fen Bilimleri Enstitüsü'nün 504121362 numaralı Yüksek Lisans Öğrencisi Ersin HATUN, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "RASPBERRY PI ÜZERİNDE GERÇEKLENMİŞ RSA ALGORİTMASINA YAN KANAL ANALİZİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Sıddıka Berna ÖRS YALÇIN** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Dr. Öğr. Üyesi Şerif BAHTİYAR** İstanbul Teknik Üniversitesi	.....
	Doç. Dr. Burak KELLECİ Okan Üniversitesi	.....

Teslim Tarihi : 20 Mart 2018
Savunma Tarihi : 18 Nisan 2018

Saygı değer aileme,

ÖNSÖZ

Tez çalışmalarım boyunca her zaman yol gösteren ve teşvik eden danışman hocam Doç. Dr. Sıddıka Berna Örs Yalçın'a teşekkür ederim.

Ayrıca tez çalışmalarım boyunca bana sürekli yardım eden Elif Büyükkaya, Muhammet Ali Evci, Muhammet Şahinoğlu ve Gökhan Alkan başta olmak üzere eski çalışma arkadaşlarıma teşekkürü bir borç bilirim.

Son olarak bana karşı anlayış ve sabırlarından dolayı aileme teşekkür ederim.

Mart 2018

Ersin HATUN
(Elektrik Elektronik Mühendisi)

İÇİNDEKİLER

Sayfa

KISALTMALAR

SEMA	**:** Simple Electromagnetic Analysis
DEMA	**:** Differential Electromagnetic Analysis
RSA	**:** Rivest Shamir Adleman
AES	**:** Advanced Encryption Algorithm
DES	**:** Data Encryption Standard
3DES	**:** Triple Data Encryption Standard
IDEA	**:** International Data Encryption Algorithm
RC4	**:** Rivest Cipher
DSA	**:** Digital Signature Algorithm
FIB	**:** Focused Ion Beam
CRT	**:** Chinese Remainder Theorem
CMOS	**:** Complementary Metal Oxide Semiconductor
TEMPEST	**:** Transient Electromagnetic Pulse Emanation Standard
FPGA	**:** Field Programmable Gate Array
USB	**:** Universal Serial Bus
DFT	**:** Discrete Fourier Transform

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

RASPBERRY PI ÜZERİNDE GERÇEKLENMİŞ RSA ALGORİTMASINA YAN KANAL ANALİZİ

ÖZET

RSA şifreleme algoritması güvenli veri aktarımı için yaygın olarak kullanılan açık anahtarlı şifreleme sistemlerinden biridir. Bu algoritma ilk defa 1978'de Ron Rivest, Adi Shamir ve Len Adleman tarafından açıklanmıştır. Algoritmanın ismi ise bu kişilerin soyadlarının ilk harflerinden oluşmaktadır. RSA şifreleme algoritması verinin şifrelenmesi, şifrelenen verinin çözülmesi ve verinin imzalanması işlemlerinde kullanılmaktadır.

Gelişen teknolojiyle beraber bilgilerimizin büyük çoğunluğu elektronik ortama aktarılmaktadır.. Akıllı telefonlarımızı küçük birer bilgisayar gibi düşünebiliriz. Teknolojinin gelişmesi bilginin erişilebilirliğinin arttırmasının yanında bilgi güvenliğinin önemini de artırmaktadır. Bilginin güvenliğinin sağlanması için ilk tercih edilen yöntemlerden biri şifrelemedir. Şifreleme işlemi için standartlaşmış şifreleme algoritmaları kullanılmaktadır. Şifreleme algoritmalarının hepsi bir matematiksel arka plana sahiptir. Günümüzde temel olarak şifreleme algoritması gücünü klasik kriptolojide olduğu gibi algoritmanın gizliliğinden almaz, dayandığı matematiksel arka plandan alır. Örneğin; RSA, gücünü tamsayıların asal çarpanlarına ayırma probleminin zorluğundan alır. Kriptografik sistemlerin dayanıklılığının analizi kriptanalizin çalışma alanıdır. Bununla birlikte yan kanal saldırıları diye tabir edilen algoritmanın gerçeklendiği sistemden sızan ısı, işlem zamanı bilgisi, sistemden çekilen güç, elektromanyetik yayılım gibi verileri kullanan bir yöntem de mevcuttur.

Yan kanal saldırıları ilk olarak 1996'da zamanlama analizi konusunda yayınlanan makale ile tehdit olarak kabul edilmeye başlanmıştır. Bu ataklarda sistemin çalışmasına müdahale edilmez. Sistem normal çalışma modunda iken sistemin dışarıya sızdırdığı etkiler (ısı değişimi, işlem zamanı bilgisi, güç tüketimi vs.) gizli anahtar hakkında bilgi edinilmesini sağlıyorsa bu bilgilere yan kanal bilgileri denir.

Temel olarak yan kanal atakları ikiye ayrılır. Basit ataklarda tek bir ölçüm kullanılarak gizli anahtarın tamamı ya da bir parçası elde edilir. Basit ataklarda ölçüm ile yapılan işlem arasında ilişki aranır. Farksal ataklarda ise birden çok ölçüm kullanılarak sistemin sebep olduğu gürültü elimine edilip gizli anahtarla ilgili bilgi edinilir. Bu tür ataklarda ise alınan ölçümler ile işlenen veri arasındaki ilişkiye odaklanılır.

Bu tez çalışmasında Raspberry Pi üzerinde gerçeklenen RSA şifreleme algoritmasına Basit Elektromanyetik Analizi (SEMA) ve Farksal Elektromanyetik Analizi (DEMA) saldırıları gerçekleştirilmiştir. Bu atakların gerçekleştirilebilmesi için masaüstü bilgisayar, sayısal osiloskop, Raspberry Pi ve yakın alan alıcısından oluşan ölçüm düzeneği kurulmuştur. Raspberry Pi, üzerinde bir işletim sistemi koşturması ve küçük bir bilgisayar özelliğine sahip olması nedeniyle gürültü seviyesi yüksek bir

platformdur. Bu nedenle alınan ölçümlerin analiz edilmesi zorlaşmıştır. Analiz işleminin sonunda RSA algoritması herhangi bir yazılımsal önlem almadan gerçeklenir ve / veya Raspberry Pi üzerinde bir güvenlik önlemi alınmaz ise Raspberry Pi platformunun yan kanal analizi ataklarına açık olduğu görülmüştür.

SIDE CHANNEL ANALYSIS TO RSA ALGORITHM IMPLEMENTED ON RASPBERRY PI

SUMMARY

The RSA encryption algorithm is one of the public key cryptosystems commonly used for secure data transfer. This algorithm was first described by Ron Rivest, Adi Shamir and Len Adleman in 1978. The name of the algorithm consists of the first letters of the surnames of these persons. The RSA encryption algorithm is used for encrypting the data, decrypting the encrypted data and for signing the data.

In Today's world, embedded systems are an indispensable part of every device. With the development of the technology, the usage areas of embedded systems have increased. Embedded systems become interconnected on the network with Internet of Things. It is important that embedded systems are secure against attacks, such as side channel analysis, as well as being secure enough against cyber-attacks against the network. With the ever-evolving technology, the vast majority of our knowledge is electronic. We can assume that our smart phones are like a little computer. Raspberry Pi is an ideal embedded system since it is a mini computer as well as being small. The popularity of the Raspberry Pi is increasing day by day with IoT technology.

The development of technology not only increases the accessibility of information but also the importance of information security. One of the first preferred methods for security of information is encryption. Standard encryption algorithms are used for encryption. All encryption algorithms have a strong mathematical background. Basically, the encryption algorithm takes the power from the mathematical background that it does not get from the secrecy of the algorithm. For example; RSA is based on the difficulty of integrating integer multipliers.

The analysis of the resistant of cryptographic systems is the working area of cryptanalysis. However, there is also a method that uses data such as heat leaked from the system, the processing time information, power consumption of the system, electromagnetic emission. These are side channel informations leaked unintentionally from the platform that algorithm implemented. This method called side channel attacks which is a kind of cryptanalysis.

Side channel attacks were first introduced as a threat in 1996 with an article on timing analysis. This attacks will not interfere with the operation of the system. This information is called side channel information if the system is able to obtain information about the leaked effects (heat exchange, process time information, power consumption, etc.) while the system is in normal operating mode. Along with this approach, it has been revealed that besides mathematical testing of cryptographic algorithms, it should be tested against possible weaknesses based on realization.

Basically, side channel attacks are divided into two. In simple attacks, all or part of the secret key is obtained using a single measurement. In simple attacks, the

relationship between the measurement and the process is sought. In case of differential attacks, the noise caused by the system is eliminated by using multiple measurements and information about the secret key is obtained by filtering and correlation analysis. In such cases, the focus is on the relationship between the measurements taken and the data processed.

In this study, the security of the RSA algorithm implemented on Raspberry Pi against electromagnetic side channel attack has been evaluated. On the Raspberry Pi platform, fast exponential and always square and multiply algorithms are implemented for the RSA encryption algorithm.

Complementary metal oxide semiconductors (CMOS) are frequently used in the implementation of electronic circuits. The total power consumption of the circuits is divided into dynamic and static power consumption. Dynamic power consumption is more dominant in CMOS inverters. The power consumption at time when the transistor output is unchanged gives static power consumption while the power consumption at the time when the output of the transistor changes is dynamic power consumption. It is known that the change in the output value of the CMOS gate causes the instantaneous current change. In addition to the instantaneous current change, electromagnetic propagation also occurs. The electromagnetic radiation varies according to the processed data or the processing carried out. Electromagnetic radiation can be measured in terms of antennas. Electromagnetic radiation obtained by antennas is used as side channel information for electromagnetic analysis attacks.

Electromagnetic radiation analysis attacks are divided into simple electromagnetic analysis attacks and differential electromagnetic analysis attacks. In simple electromagnetic analysis attacks, the attacker tries to capture the whole or part of the secret key using a single measurement. Differential electromagnetic analysis attacks are used in cases where the measurement noise is excessive, noise is destroyed using many measurements. The relationship between processed data and power consumption are investigated using statistical methods.

A measurement system consisting of a desktop computer, a digital oscilloscope, a Raspberry Pi and a near field high precision EM probe has been set up to perform these attacks. The high-precision EM probe is ideal for receiving low-voltage electromagnetic emissions. This probe is connected to channel of the oscilloscope. One of the general-purpose input output pins of Raspberry Pi is connected to a channel of the oscilloscope. This channel triggers the oscilloscope to start measurement.When the oscilloscope detects the voltage increase at the general-purpose input / output pins, it takes the electromagnetic emission and records it in binary format. Then it is transferred to another computer for signal analysis in MATLAB. An operating system is running on the Raspberry Pi and it has small computer feature, this situation increased the noise level and it made it difficult to analyze the measurements taken. At the end of the analysis process, if the RSA algorithm is not implemented correctly and / or if any countermeasure is not applied on Raspberry Pi, it is seen that Raspberry Pi platform is vulnerable to side channel analysis attacks.

In this thesis, Simple Electromagnetic Analysis (SEMA) and Differential Electromagnetic Analysis (DEMA) attacks were performed on the RSA encryption algorithm implemented on Raspberry Pi. Using the SEMA attack, it has been shown that all key bits can be obtained by a single measurement in a countermeasure-free implementation. It is seen that the key can’t be obtained using SEMA by

implementing the algorithm resistant to SEMA attack. The DEMA attack is implemented by increasing the number of measurements and using the correlation analysis. It is seen that the bit value of the key can be obtained by DEMA attack.

This study is proof that the Raspberry Pi platform has no countermeasure against the side channel analysis attacks.

1. GİRİŞ

Günümüzde, elektronik ortamda bulunan veri miktarı hızla artmaktadır. Bununla birlikte internet kullanımı da yaygınlaşmaktadır. İnternet gibi herkesin erişimine açık olan ortamlarda kullanıcıların bilgilerine yönelik saldırılar olduğu bilinmektedir [1, 2]. Teknoloji gelişip internet yaygınlaştıkça kullanıcı alışkanlıkları değişmekte ve internet üzerinden yapılan işlemler artmaktadır. Örneğin; birçok sitede, üyelik ve kimlik doğrulama işlemleri gerçekleştiriliyor. Bu ve bunlara ek birçok durumda bilgi güvenliği gerekliliği ortaya çıkmaktadır.

Tarihi çok eskilere dayanan kriptoloji, bilgi güvenliği için en önemli bileşenlerden biridir [3]. Kriptografik sistemler kullanılarak veriler şifrelenebilir ya da gönderilen verilerin kim tarafından gönderildiğini ispatlamak için sayısal imza kullanılabilir. Kriptografik algoritmaların güvenliği genel olarak gizli anahtarın üçüncü kişilerin eline geçmemesine dayanmaktadır. Kriptoloji tarihi boyunca şifreleme anahtarını ele geçirmeye yönelik saldırılar gerçeklenmiş ve gün geçtikçe bu saldırı yöntemleri iyileştirilmiştir [4]. Bu saldırılar sayesinde daha güçlü kriptografik sistemlerin geliştirilmesi tetiklenmiştir. Saldırılar algoritmaların dayandığı matematiksel zorluğa yönelik ve gerçeklemeye yönelik olmak üzere ikiye ayrılabilir [4, 5].

Matematiksel zorluğa yönelik saldırılarda güçlü bilgisayarlar kullanılarak sistemin üstüne inşa edildiği matematiksel yapının zayıflıkları araştırılıp gizli anahtar elde edilmeye çalışılırken, gerçeklemeye özgü saldırılarda sistemin istemsiz olarak dışarıya ilettiği bilgilerden faydalanılmaktadır. İstemsiz olarak üretilen bilgileri kullanarak gizli anahtarın tamamını ya da bir bölümünü ele geçirmek mümkündür. Bu tür saldırılara yan kanal saldırıları adı verilir [6]. Kendi içinde aktif yan kanal saldırıları ve pasif yan kanal saldırıları olmak üzere ikiye ayrılır.

Aktif yan kanal saldırılarında kriptografik algoritmanın gerçeklendiği sisteme fiziksel müdahale yapılır [7]. Devrenin içyapısı sensörler yardımıyla izlenebilir [8] ya da harici bir sistemle (lazer istasyonları ile) kriptografik sisteme müdahale edilip hata yaptırılarak sonuçları izlenir [9, 10].

Pasif yan kanal saldırıları ise, sisteme fiziksel müdahale ihtiyacı doğurmadığından daha ucuza gerçeklenir ve saldırıya dair bir iz bırakmaz. Literatürde bu konuda birçok çalışma mevcuttur [4, 5, 11, 12]. En yaygın kullanılan yan kanal bilgileri sistemin tükettiği güç [5] ve elektromanyetik yayılımdır [11, 12]. Bununla birlikte sistemin şifreleme işlemi sırasında gözlemlenen zaman farklılıklarının [4], etrafa yaydığı ses dalgalarının [13] ve devrenin sıcaklık değişimlerinin yan kanal bilgisi olarak kullanıldığı çalışmalar da vardır. Son yıllarda bu tür saldırılar kolay gerçeklenmesinden ve güçlü olmasından dolayı dikkat çekmektedir.

1.1 Tezin Kapsamı

Gömülü sistemler günümüzde her cihazın vazgeçilmez bir parçasıdır [14]. Teknolojinin gelişmesiyle beraber gömülü sistemlerin kullanım alanları artmıştır. Eskiden gömülü sistemler sadece belli bir işi yapmak için kullanılmaktayken artık çoklu işlem özelliğine sahip sistemlere dönüşmüşlerdir. Raspberry Pi [15] ise küçük bir bilgisayar özelliğine sahip üstünde işletim sistemi çalışan bir gömülü sistemdir. Kredi kartı boyutunda olması ve bilgisayarda yapılan her işlemin yapılabilmesi nedeniyle çok tercih edilmektedir.

Kriptografik algoritmaların güvenliği sadece algoritmanın matematiksel altyapısına değil gerçeklendiği sistemin güvenliğine de dayanır. Raspberry Pi, içerisinde kriptografik algoritmaları barındıran birçok uygulamanın gerçeklendiği bir platform olmuştur. Dolayısıyla bu sistemin güvenliğine de dikkat çekmek gerekmektedir.

Rivest – Shamir – Adleman (RSA) algoritması 1978 yılında açıklanmıştır [16]. Günümüzde güvenli veri aktarımı için yaygın olarak kullanılan açık anahtarlı şifreleme sistemlerinden biridir. RSA şifreleme algoritması verinin şifrelenmesi, şifrelenen verinin çözülmesi ve verinin imzalanması işlemlerinde kullanılmaktadır.

Bu tez çalışmasında RSA şifreleme algoritmasının Raspberry Pi üzerinde gerçeklemesine yan kanal sızıntılarından biri olan elektromanyetik radyasyon kullanılarak yan kanal saldırısı uygulanacaktır. Genel plan aşağıdaki gibidir.

Bölüm 2'de kriptoloji ve şifreleme algoritmaları hakkında genel bilgi verilmektedir. Bölüm 3'de RSA şifreleme algoritması ve matematiksel arka planı anlatılmaktadır. Bölüm 4'de yan kanal sızıntılarından ve yan kanal saldırıları türlerinden bahsedilmektedir. Bununla beraber tez çalışmasında kullanılan elektromanyetik

analizi saldırıları anlatılmaktadır. Bölüm 5'de yan kanal analizi saldırısını gerçekleştirmek için kurulan ölçüm düzeneği ve ölçüm düzeneği parçaları açıklanmaktadır. Bölüm 6'da ölçüm düzeneği kullanılarak alınan ölçümlerin gürültüden elimine edilmesi, filtrelenmesi çalışmaları anlatılmaktadır. Daha sonra Basit Elektromanyetik Analizi (Simple Electromagnetic Analysis – SEMA) ve Farksal Elektromanyetik Analizi (Differential Electromagnetic Analysis – DEMA) saldırılarının gerçekleştirilmesi anlatılmaktadır. Bölüm 7'de tezin genel bir özeti ve sonuç bölümü yer almaktadır.

1.2 Tezin Konuya Katkısı

Literatürde RSA şifreleme algoritmasına yan kanal saldırısını konu alan çalışmalar bulunmaktadır. Üzerinde işletim sistemi koşan bir sistem için gerçekleştirilen yan kanal saldırısı çalışmaları daha azdır. Bu tip sistemlerde gürültü seviyesi daha fazla olduğundan yapılan işlemlerin tahmin edilebilirliği azalmaktadır. Bu tez çalışması Raspberry Pi üzerinde RSA şifreleme algoritmasının gerçeklenmesini ve alınan ölçümlerin analiz edilmesini içermektedir.

2. KRİPTOLOJİ

Gizlilik, veri bütünlüğü, kimlik doğrulama gibi bilgi güvenliği problemlerine matematiksel teknikler kullanarak çözüm getirme ve bu çözümleri çürütme bilimidir [17]. Kriptografi ve kripto analiz kavramlarının bir araya gelmesi kriptolojiyi oluşturur. Kriptografi, algoritma ve protokol tasarımıyla ilgilenirken kriptanaliz, bu tasarımların analiz edilmesiyle ilgilenir. Bu iki kavram, daha dayanıklı kriptografik sistemlerin ortaya çıkması için birbirini beslemektedir.

Kriptolojinin temelleri binlerce yıl öncesine dayanmaktadır [18]. İlk yıllarda şifreleme algoritması sadece haberleşmek istenilen kişilerle paylaşılırdı. Algoritmanın gizliliği güvenli haberleşme için koşulken daha sonra modern şifreleme algoritmaları geliştirildi ve anahtarın gizliliği önem kazandı.

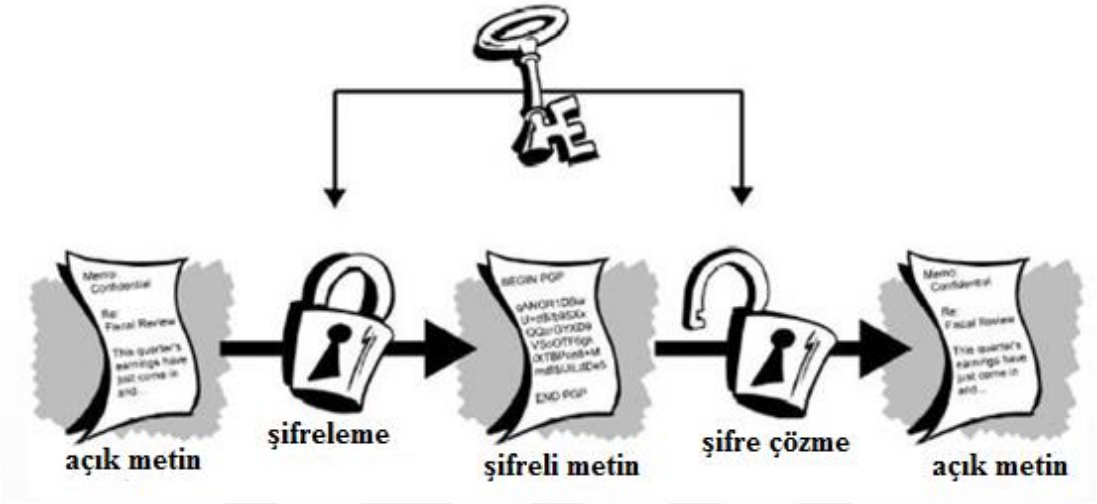
Şifreleme ve şifre çözme işlemleri taraflar arasındaki mesajların gizliliğini sağlayan temel kriptografik işlemlerdir [19]. Gönderici tarafında şifreleme işlemi uygulanarak anlamlı orijinal mesaj şifreli mesaja çevrilir. Bu sayede aradaki bir kişi mesajı ele geçirse bile anlamsız bir veriyi ele geçirmiş olur. Alıcı tarafında ise şifreleme işleminde yapılan işlemin tersi yapılır. Şifreli mesajdan orijinal mesaj geri elde edilir. Böylelikle açık bir kanalda taraflar güvenli bir şekilde haberleşmiş olurlar.

Günümüzde tek şifreleme anahtarına sahip ve iki farklı şifreleme anahtarına sahip algoritmalar vardır [20]. Tek anahtara sahip algoritmalar simetrik şifreleme algoritmaları olarak adlandırılırken, iki farklı anahtarın kullanıldığı algoritmalara asimetrik şifreleme algoritmaları ya da açık anahtarlı şifreleme algoritmaları denir. İki türünde birbirine göre avantaj ve dezavantajları vardır. Bazı uygulamalarda ise hibrit sistemler adı verilen simetrik ve asimetrik şifreleme algoritmaları bir arada kullanılmaktadır.

2.1 Simetrik Şifreleme

Veriyi şifreleme ve bu şifrelenmiş veriyi çözme işlemlerinde aynı anahtarın kullanıldığı şifreleme türüne simetrik şifreleme denir (Şekil 2.1) [21]. Kriptografik

işlemde kullanılan bu anahtar sadece veriyi gönderen ve veriyi alan tarafından bilinmelidir. Verinin gizliliği, anahtarın gizliliğini sağlamakla ve anahtarın üçüncü tarafların eline geçmemesiyle sağlanır. Anahtarın belirlenmesi ve taraflar arasında güvenli olarak paylaşılması ilk etapta problem olabilir.



Şekil 2.1 : Simetrik şifreleme [22].

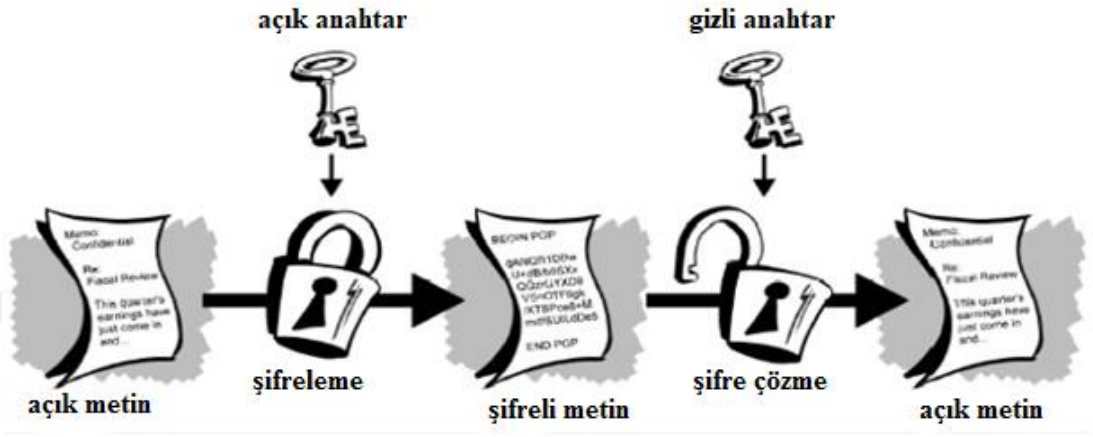
Simetrik şifreleme algoritmaları veriyi işleyiş biçimine göre blok ve dizi şifreleme olmak üzere iki kısma ayrılır [18]. Simetrik şifreleme algoritmalarına Veri Şifreleme Standardı (Data Encryption Standard – DES) [23], Gelişmiş Şifreleme Standardı (Advanced Encryption Standard – AES) [24], Blowfish [21], Üçlü Veri Şifreleme Standardı (Triple Data Encryption Standard - 3DES) [20], Uluslararası Şifreleme Algoritması (International Data Encryption Algorithm - IDEA) [21] ve Rivest Şifreleme (Rivest Cipher - RC4) [25] örnek olarak verilebilir [19].

Simetrik şifreleme algoritmalarında şifreleme ve şifre çözme işlemleri asimetrik şifreleme algoritmalarına göre çok daha hızlıdır [26]. Yazılımsal olarak gerçeklenebilecekleri gibi donanımsal olarak da gerçeklenebilirler.

2.2 Asimetrik Şifreleme

Asimetrik şifreleme algoritmaları, şifreleme işlemi için bir tane ve şifre çözme işlemi için bir tane anahtar olmak üzere toplam 2 farklı anahtara sahiptir [20]. Bu anahtar çiftinden birisi açık anahtar diğeri ise gizli anahtar olarak adlandırılır (Şekil 2.2). Bu anahtar çifti arasında matematiksel bir bağıntı vardır. Ama arkakapı (trapdoor) bilgisi bilinmeden açık anahtardan gizli anahtar, gizli anahtardan açık anahtar elde edilemez

[27]. Gizli anahtar kişiye özeldir ve kimseyle paylaşılmaz. Açık anahtarın ise üçüncü kişilerden saklanmasına gerek yoktur. Açık anahtarla şifrelenen bir veri ancak o açık anahtara karşılık gelen gizli anahtarla çözümlenebilir. Veriyi gönderen kişi, karşı tarafın açık anahtarıyla veriyi şifreler, alıcı da gizli anahtarıyla şifreyi çözümler. Bu sistemler açık anahtarlı şifreleme diye de adlandırılmaktadır.



Şekil 2.2 : Asimetrik şifreleme [22].

Asimetrik şifrelemede açık anahtara herkes ulaşabilir olduğundan anahtar paylaşmada güvenliği sağlamak gibi bir ön koşul yoktur [25]. Fakat asimetrik şifreleme simetrik şifrelemeye göre daha yavaştır. Bu yüzden simetrik ve asimetrik şifreleme algoritmalarının beraber kullanıldığı hibrit sistemler vardır [19]. Hibrit sistemlerde şifreleme işlemi için simetrik şifreleme algoritmaları, anahtar paylaşımı için asimetrik şifreleme algoritmaları kullanılmaktadır.

Çizelge 2.1 : Asimetrik ve simetrik kriptografinin karşılaştırılması [26].

Konu	Simetrik Kriptografi	Asimetrik Kriptografi
Gizlilik	Sağlar	Sağlar
Bütünlük	Sağlamaz	Sağlar
Kimlik Doğrulama	Sağlamaz	Sağlar
İnkar Edememezlik	Sağlamaz	Sağlar
Performans	Hızlı	Yavaş
Güvenlik	Anahtar uzunluğuna bağlı	Anahtar uzunluğuna bağlı

Açık anahtarlı şifreleme algoritmalarında örnek olarak RSA [16] ve Dijital İmza Algoritması (Digital Signature Algorithm - DSA) [21] verilebilir. RSA şifreleme algoritması 1978 yılında resmi olarak yayınlanmasına rağmen hala geçerliliğini korumaktadır. Bölüm 3'te daha detaylı olarak ele alınacaktır.

3. RIVEST-SHAMIR-ADLEMAN ALGORİTMASI

Rivest-Shamir-Adleman (RSA) şifreleme algoritması 1970'lerden bu yana kullanılmasına rağmen hala en çok tercih edilen açık anahtarlı şifreleme algoritmalarından biridir [28]. Daha çok dijital sertifikalar ve küçük veri paketlerinin şifrelenmesinde kullanılır. Bunun sebebi de gizli anahtarlı şifreleme algoritmalarına göre daha yavaş olmasıdır. Yine bu sebepten ötürü bazı sistemlerde sadece anahtar paylaşımının güvenli yapılması için kullanılmaktadır. Anahtar paylaşımından sonra simetrik şifreleme algoritmaları şifreleme için kullanılmaktadır.

RSA şifreleme algoritmasının arkasındaki matematiksel yapı büyük tamsayıları çarpanlarına ayırma zorluğuna dayanmaktadır. İki büyük asal sayıyı çarpmak kolay olsa da çarpım sonucu verildiğinde bu iki asal çarpanı bulmak çok zordur. Bu bölümde RSA algoritmasının matematiksel yapısından bahsedilecektir.

3.1 Anahtar Üretimi

RSA şifreleme algoritmasında kullanılan açık ve gizli anahtarların oluşturulma adımları aşağıdaki gibidir [16].

$$p \neq q \tag{3.1}$$

$$p, q \in \mathrm{P} \tag{3.2}$$

olmak üzere;

1. İki adet büyük ve birbirinden farklı asal sayı seçilir. Bunlar p ve q olarak isimlendirilir.
2. Açık ve gizli anahtar üretiminde modülüs değeri olarak kullanıcak olan n değeri denklem 3.3'deki gibi hesaplanır.

$$n = p \times q \tag{3.3}$$

3. Denklem 3.4 kullanılarak n sayısının totient değeri hesaplanır.

$$\varphi(n) = (p-1) \times (q-1) \tag{3.4}$$

$$1 < e \leq \varphi(n) - 1 \tag{3.5}$$

$$EBOB(e, \varphi(n)) = 1 \tag{3.6}$$

4. Denklem 3.5 ve denklem 3.6 kullanılarak bir e değeri seçilir. Denklemler sonucu elde edilen (n, e) değeri açık anahtardır.

$$d \equiv e^{-1} \bmod \varphi(n) \tag{3.7}$$

5. Denklem 3.7'de verilen denkliği sağlayan d değeri bulunur. Bu d değeri ise gizli anahtardır.

$p, q, \varphi(n)$ sayılarının gizli kalması gerekmektedir.

3.2 Şifreleme ve Şifre Çözme İşlemi

RSA şifreleme algoritması kullanılarak gerçekleştirilecek olan şifreli haberleşmede sadece gizli anahtar sahibinin şifreli metni çözebilmesi için gönderilecek olan mesaj herkese açık olan (n, e) değerleri kullanılarak şifrelenir [16]. Denklem 3.4'teki gibi şifrelenecek verinin e değerinci kuvvetinin mod n ' deki karşılığı şifreli metni meydana getirir.

$$c = m^e \bmod n \tag{3.8}$$

Açık anahtar kullanılarak şifrelenmiş bir verinin sadece o açık anahtarın çifti olan gizli anahtar ile şifresi çözülebilir. (n, d) gizli anahtarı şifre çözme işlemi için kullanılır. Denklem 3.5'teki gibi şifreli verinin yani c değerinin d değerinci kuvvetinin $\bmod n$'deki karşılığı açık veriyi oluşturur.

$$m = c^d \bmod n \tag{3.9}$$

3.3 Rivest-Shamir-Adleman Algoritmasındaki İşlemlerin Gerçeklenmesi

3.3.1 Hızlı üs alma

Daha önceki başlıklarda değinildiği gibi RSA şifreleme algoritması kullanılarak yapılan şifreleme ve şifre çözme işlemlerinde üs alma işlemi sıklıkla kullanılmaktadır. Sayılar büyüdükçe bu işlemi hızlı yapabilmek için bir yönteme ihtiyaç duyulmuştur [16]. Çarpma ve kare alma algoritması en çok kullanılan ve en basit hızlı üs alma algoritmasıdır. Algoritma Şekil 3.1'de verilmiştir.

$e = (e_k, e_{k-1}, e_{k-2}, e_{k-3}, ..., e_0)_2$ olmak üzere
$d = m^e \bmod n$ işlemi aşağıdaki gibi hesaplanabilir.
1: $d \leftarrow 1$
2: for $i = k : 0$ // soldan sağa doğru
3: $d \leftarrow d * d \bmod n$ // Kare alma
4: if $e_i = 1$
5: $d \leftarrow d * m \bmod n$ // Çarpma
6: end if
7: end for

Şekil 3.1 : Hızlı üs alma algoritması.

3.3.2 Açık anahtarın küçük seçilmesi

RSA işlemini hızlandırmanın bir diğer yolu ise açık anahtar olan e değerini daha az çarpma ve kare alma işlemiş yapacak şekilde seçmektir [28]. Bu amaçla, açık anahtar küçük Hamming ağırlığına sahip bir değer olarak seçilir. Aşağıdaki çizelgede en çok kullanılan e değerleri ve toplam işlem (kare alma ve çarpma) sayısı verilmiştir [29].

Çizelge 3.1 : Küçük açık anahtar değerleri.

Açık Anahtar (e)	e (ikilik sistem)	İşlem Sayısı
3	11	3
17	1 0001	5
216+1	1 0000 0000 0000 0001	17

3.3.3 Çinli kalan teoremi

Bir önceki bölümde açık anahtarın küçük değerde seçilerek şifreleme işleminin hızlandırılması anlatılmıştı. Gizli anahtar ise açık anahtarın aksine küçük seçilemez [30]. Gizli anahtar küçük seçilirse sistem kaba kuvvet (brute force) saldırısına karşı zayıf kalmış olur. Bu nedenle pratikte açık anahtar küçük seçilirken gizli anahtar olabildiğince büyük seçilir. Gizli anahtarın büyük seçilmesiyle RSA şifre çözme ve sayısal imza işlemlerini hızlandıracak bir yönteme ihtiyaç duyulmuştur. Çinli kalan

teoremi (Chinese Remainder Theorem - CRT) yöntemi sayesinde gizli anahtar kullanılarak yapılan işlemler hızlandırılmaktadır [26]. Bu yöntem için anahtar üretiminde seçilen p ve q değerleri dönüşümde kullanılır.

1. İlk olarak CRT alanına dönüşüm sağlanmalıdır.

$$y_p \equiv y \bmod p \tag{3.6}$$

$$y_q \equiv y \bmod q \tag{3.7}$$

$$d_p \equiv d \bmod (p-1) \tag{3.8}$$

$$d_q \equiv d \bmod (q-1) \tag{3.9}$$

2. Daha sonra CRT alanındaki üstel işlemler aşağıdaki gibi hesaplanır.

$$x_p = y_p^{\,d_p} \bmod p \tag{3.10}$$

$$x_q = y_q^{\,d_q} \bmod q \tag{3.11}$$

3. CRT alanından geri dönüşüm yapılır.

$$c_p \equiv q^{-1} \bmod p \tag{3.12}$$

$$c_q \equiv p^{-1} \bmod q \tag{3.13}$$

olmak üzere;

$$x \equiv (qc_p x_p + pc_q x_q) \bmod n \tag{3.14}$$

denklem 3.14 elde edilir.

3.3.4 Büyük asal sayı bulma

RSA işleminde açık anahtar ile gizli anahtar arasındaki ilişki p ve q asal sayılarının gizliliğine bağlıdır. Anahtar üretiminin ilk adımı da iki tane büyük asal sayı seçilmesidir [20]. Bu konuda genel yaklaşım rastgele sayılar üretip daha sonra asal

olup olmadığını kontrol etmektir. Asal sayının rastsallığı ve asallık kontrolü işleminin hızı dikkat edilmesi gereken iki konudur.

Çok büyük sayı aralıklarında bile asal sayıların yoğunluğu yeterince yüksektir. Rastgele bir tek sayı p olmak üzere, p sayısının asal olma oranı denklem 3.15'ten görülmektedir [29].

$$P = \frac{2}{\ln p} \tag{3.15}$$

Asallık kontrolü için birçok test mevcuttur. Bunlardan en çok tercih edilenleri Fermat testi ve Miller – Rabin testidir [31, 32]. Ayrıca, asallık kontrolü testleri hesaplama olarak da ucuzdur.

4. YAN KANAL ANALİZİ SALDIRILARI

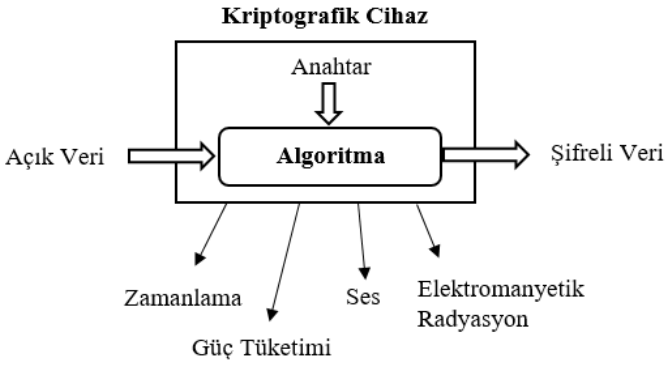
Güvenli haberleşme esasen şifreleme algoritmalarının ve gerçeklendiği platformların güvenlik önlemlerine dayanmaktadır. Kriptanaliz bilimi sayesinde şifreleme algoritmalarına çeşitli ataklar yapılagelmiştir. Daha önceleri sadece algoritmaların matematiksel olarak sağlam olması yeterli görülürken yapılan ataklarla platformların da güvenliği ana odak noktası haline gelmiştir [33]. Gerçeklenen atakların hepsinin ortak amacı gizli anahtar hakkında bilgi edinmek ve şifrelenen veriyi çözmektir. Saldırının türüne göre uzmanlık, zaman, masraf faktörleri değişmektedir.

Algoritmanın gerçeklendiği ortamdan çıkan yan kanal bilgileri kullanılarak gerçeklenen ataklara yan kanal saldırıları denir [4]. Yan kanal saldırıları aktif ve pasif olmak üzere iki şekilde incelenir.

Aktif yan kanal saldırılarında atak gerçekleştirildiğine dair iz kalmaktadır. Saldırıyı gerçekleştirmek için kriptografik cihazın iç devresine erişmek gerekir [34]. Bu tür ataklara örneklerden biri lazer istasyonları yardımıyla cihaza hata yaptırılarak gerçeklenen saldırıdır [9, 10]. Başka bir örnek verilecek olursa, Focused Ion Beam (FIB) gibi çip soyma cihazlarıyla, işlemciler soyularak anahtar tutulduğu bellekten okunabilir [8]. Pasif yan kanal saldırılarına göre uygulamaları zor ve pahalıdır.

Pasif yan kanal saldırılarında ise algoritmanın çalıştığı sisteme herhangi bir müdahalede bulunulmaz. Sadece çalışma esnasında dışarıya istemsiz sızdırılan bilgilerden faydalanılmaktadır [1]. Aktif yan kanal saldırılarının aksine bu tür ataklar için pahalı düzeneklere ve cihazlara ihtiyaç duyulmamaktadır. Pasif yan kanal saldırıları kullanılan yan kanal bilgisine göre temelde 4'e ayrılır. Bunlar ses [13], zamanlama [4], güç tüketimi [5] ve elektromanyetik radyasyon [11] olarak sıralanabilir.

Bütün pasif yan kanal saldırıları basit ve farksal olmak üzere kendi içinde ikiye ayrılır. Basit yan kanal analizinde tek ölçümle anahtar hakkında bilgi edinilirken farksal yan kanal analizinde istatistiksel yöntemlerle birden çok ölçüm kullanılarak gizli anahtar hakkında bilgi açığa çıkarılır.



Şekil 4.1 : Yan kanal bilgileri.

Zamanlama analizi atakları, kriptografik işlem yapan cihazın yaptığı işlemlerle ilgili zaman farklılıklarını dışarıya sızdırmasına dayanır [4]. Güç tüketimi analizi atakları kriptografik algoritmanın çalışma süresince kriptografik cihazın dinamik güç tüketiminin kullanılmasıyla gerçeklenir [5]. Elektromanyetik analiz atakları kriptografik cihazın kriptografik algoritma çalışırken dışarıya sızdırdığı elektromanyetik yayılımın analiz edilmesiyle gerçeklenir [12]. Ses analizi atakları ise kriptografik algoritmanın çalışma süresince kriptografik cihazın çıkardığı seslerin analiziyle yapılır [13].

Basit yan kanal analizinde alınan yan kanal bilgisiyle gerçekleştirilen işlemler arasındaki ilişki kullanılırken, farksal yan kanal analizde işlenen veriyle yan kanal bilgisi arasındaki ilişki kullanılır. Farksal yan kanal analizi istatiksel yöntemlerle gerçeklendiği için atağı gerçekleştiren kişinin yetkinliği atağın kalitesiyle doğrudan ilişkilidir.

Bu bölümde istatiksel yöntemler ve temel pasif yan kanal analizi ataklarıyla ilgili çalışmalardan bahsedilmektedir.

4.1 İstatiksel Yöntemler

Farksal yan kanal analizi ataklarında, saldırgan kriptografik cihaz için yetkinliğine göre bir model oluşturur [35]. Bu model cihazın yan kanal bilgisindeki değerleri tahmin etmek için kullanılır. Bu tahminler ile yan kanal bilgisi ölçümleri istatiksel yöntemler kullanılarak karşılaştırılır. Kullanılan birçok istatiksel yöntem olmasına karşın en çok kullanılanlar korelasyon analizi ve ortalamaya uzaklık testleridir. Bu tez çalışmasında da bu yöntemler son bölümde kullanılmaktadır.

4.1.1 Korelasyon analizi

Korelasyon iki değişken arasındaki ilişkinin derecesini gösteren istatiksel bir analiz yöntemidir [34]. Korelasyon analizi için çalışma zamanının belli noktalarındaki yan kanal bilgilerinin seviyesi oluşturulan modele göre tahmin edilir. Daha sonra bu tahminler ile gerçek yan kanal bilgilerinin korelasyonuna bakılır. Analiz işlemine giren değişkenlerin ilişkilerinin seviyesini ve yönünü korelasyon katsayısı gösterir. Farklı sistemler için farklı korelasyon katsayıları kullanılmaktadır. Bu korelasyon işlemi için 'Pearson Korelasyon Katsayısı' kullanılabilir [36].

$$C(X,Y)=\frac{E(X\cdot Y)-E(X)\cdot E(Y)}{\sqrt{Var(X)\cdot Var(Y)}} \qquad -1\le C(X,Y)\le 1 \tag{4.1}$$

Denklem 4.1 de $C(X,Y)$ korelasyon katsayısını vermektedir. $E(X)$, X değişkeninin beklenen değerini verirken $Var(X)$ X değişkeninin standart sapma değerini vermektedir.

Korelasyon katsayısı $[-1,+1]$ aralığında değer almaktadır. Korelasyon katsayısı 0 ise iki değişken arasında korelasyon yoktur denir. Değişkenlerin ikisi de aynı anda arttıkça katsayı değeri 1'e yaklaşırken, biri arttıkça diğeri azalan değişkenler için katsayı değeri -1'e yaklaşmaktadır.

4.1.2 Ortalamaya uzaklık testi

Ortalamaya uzaklık testinin ilk adımı kriptografik algoritmanın N tane rastgele oluşturulmuş giriş değeri için koşturulmasıdır [37]. Her bir giriş değeri I_i olmak üzere ayrık zamanlı yan kanal bilgisi sinyali, $S_i[j]$, kaydedilir ve O_i çıkış değeri kaydedilir. Algoritmanın belli bir parçasına saldırılır. Kaydedilen yan kanal sinyali cihazın yan kanal çıktısına göre örneklenmiş bir versiyondur. i değeri ölçüm numarasını j değeri ise alınan örneğin zaman bilgisini vermektedir. $D(.)$ fonksiyonu kullanılarak $S_i[j]$ veri seti denklem 4.2 ve denklem 4.3'teki gibi ikiye bölünür.

$$S_0=\{S_i[j]\mid D(\cdot)=0\} \tag{4.2}$$

$$S_1 = \{S_i[j] \mid D(\cdot) = 1\} \tag{4.3}$$

Bir sonraki adım ise ayrılan iki set için de ortalama yan kanal sinyali değerlerini bulmaktır:

$$A_0[j] = \frac{1}{|S_0|} \sum_{S_i[j] \in S_0} S_i[j] \tag{4.4}$$

$$A_1[j] = \frac{1}{|S_1|} \sum_{S_i[j] \in S_1} S_i[j] \tag{4.5}$$

$|S_0| + |S_1| = N$ olmak üzere. Hesaplanan iki ortalama sinyal değeri birbirinden çıkarılır ve $T[j]$ elde edilir. Bu sinyal bize şifreleme algoritmasının yaptığı işlemlerle ilgili eğilimini gösterir.

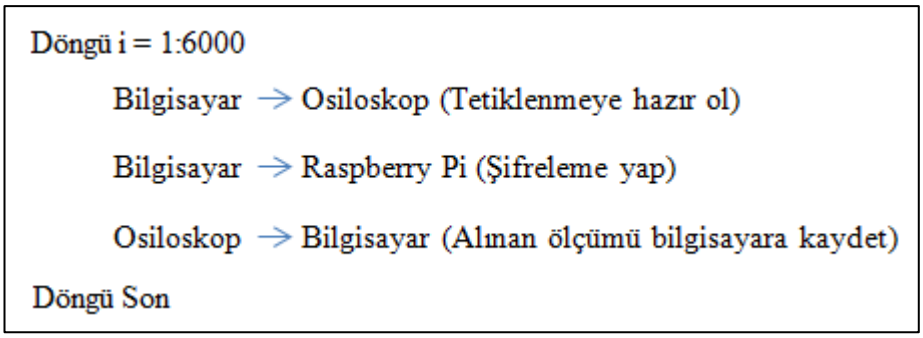
$$T[j] = A_0[j] - A_1[j] \tag{4.6}$$

Uygun bir D fonksiyonu seçilir ise $T[j]$ sinyali gizli anahtarın bir bölümünü tahmin etmek için kullanılabilir [38].

4.1.3 Pratikteki zorluklar

Yan kanal analizi atakları gerçekleştirilirken birçok değişkeni hesaba katmak gerekmektedir [35]. Alınan ölçümün kalitesi bunlardan biridir. Eğer kriptografik işlemin gerçekleştiği yere yakın bir noktadan değil de uzak bir noktadan ölçüm alınır ise gürültü oranı daha yüksek olur. Dolayısıyla kullanılan istatiksel yöntemlerin sonuçları kötü çıkar. Daha iyi sonuç alabilmek için ölçüm sayısını arttırmak gerekir. Kriptografik işlemle ilgili yan kanal bilgisi veren en iyi noktayı tespit edip o noktadan ölçüm alırsak çok daha az ölçümle bilgiye ulaşmamız mümkün olur.

Bir diğer zorluk ise ölçüm alma düzeneğinin kurulmasıdır. Ölçüm düzeneği genel olarak yan kanal bilgisi sızdıran cihaz, osiloskop, anten ve bilgisayardan oluşur. Tez çalışması kapsamında yan kanal bilgisi sızdıran cihaz Raspberry Pi platformudur. Çok sayıda ölçüm alınması için bilgisayarın hem osiloskop ile hem Raspberry Pi ile haberleşmesi gerekmektedir. Örneğin; 6000 adet ölçüm yaptırılmak istenirse Şekil 4.2'deki döngü gerçeklenmelidir [39].



Şekil 4.2 : Ölçümlerde döngü işlemleri.

Sonuç olarak başarısız olarak sonlanan bir yan kanal analizi atağında sorunun nereden kaynaklandığını tespit etmek zordur. Bilgi sızıntısı olmama durumunun yanında olası diğer ihtimalleri şöyle sıralayabiliriz.

- Ölçüm alınan noktada yeterince yan kanal bilgisi olmayabilir.
- Ölçüm düzeneğindeki cihazların birbiri ile haberleşmesinde hata olabilir.
- Ölçüm düzeneği elemanlarından biri yanlış çalışıyor olabilir.

Bu nedenle işlemler her ihtimal göz önünde bulundurularak adım adım gerçeklenmelidir. Atağı gerçekleştirmeden önce gerçekleştirilecek atağı planlamak ve simüle etmek çok önemlidir.

4.2 Zamanlama Analizi Saldırıları

Kocher, 1996 yılında yaptığı çalışmayla bu konudaki ilk pratik atağı, üzerinde RSA algoritmasının koştuğu bir akıllı kart kullanarak gerçeklemiştir [4]. Kocher bu çalışmada şu fikri öne atmıştır. Kriptografik algoritma gerçeklenir iken sabit bir zamanda gerçekleşmeyen işlemler olabilir. Eğer bu işlemler gizli parametreleri içeriyor ise bu zamansal farklılıklar kullanılarak yetkin bir kişi tarafından gizli parametrelerin tamamı elde edilebilir [40].

Güvenli olmayan sistemlerde yapılan farklı işlemler için veriye bağlı olarak zamansal farklılıklar görülmektedir. Toplama ve çarpma işlemlerinin yapılması bu duruma örnek olarak verilebilir. İki adet x ve y isimli m bit sayısına sahip değişkenimiz olduğunu varsayalım. $z = x + y$ ve $z = x \times y$ işlemleri arasındaki zamansal farkı kıyaslayalım. Toplama işlemi $t_T = m$ saat darbesi süresinde tamamlanırsa, toplama işlemini taban alan bir çarpma işlemi $t_Ç = \frac{3 \times (m-1) \times m}{2}$

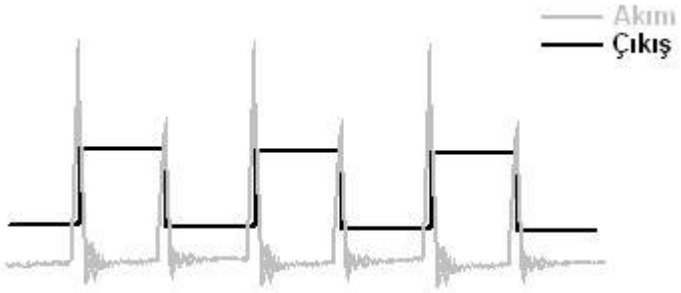
saat darbesi süresinde tamamlanır. Bu durumu kullanan bir saldırgan, yürütülen işlemin süresine bakarak hangi işlemin yapıldığını anlayabilir [38].

4.3 Güç Analizi Saldırıları

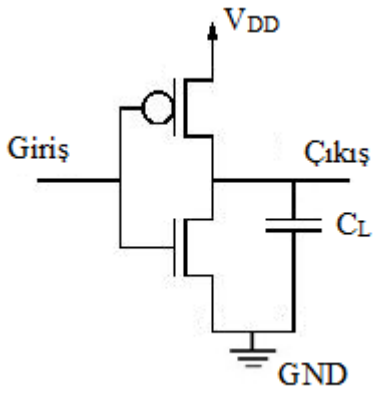
Tamamlayıcı metal oksitli yarı iletken transistörler (Complementary Metal Oxide Semiconductor - CMOS) elektronik tümdevrelerin gerçeklenmesinde çok sık kullanılmaktadır [41]. Devrelerin toplam güç tüketimi dinamik ve statik güç tüketimi olmak üzere ikiye ayrılmaktadır. CMOS eviricilerinde dinamik güç harcaması daha baskındır [34]. Transistörün çıkışının değişmediği zamandaki güç tüketimi statik güç tüketimini verir iken transistörün çıkışının değiştiği zamandaki güç tüketimi dinamik güç tüketimini vermektedir. Şekil 4.2 incelendiğinde CMOS kapısı çıkış değeri değişmediğinde akım değeri çok az olmaktadır. Çıkış değerinin 0'dan 1'e geçtiği anlardaki güç tüketimi 1'den 0'a geçtiği anlara oranla daha yüksektir.

$$P_D = C_L \times V_{DD}{}^2 \times P_{0\to1} f \tag{4.7}$$

Dinamik güç tüketimini veren denklem 4.7'de P_D dinamik güç tüketimini, C_L kapının yük kapasitesini, V_{DD} kaynak gerilimini, $P_{0\to1}$ CMOS kapısının $0\to1$ geçişlerinin olasılığını, f saat frekansını göstermektedir [41]. Bu formülle güç tüketiminin veriye bağlı olduğu görülmektedir. Saldırgan için önemli olan bu ilişkinin elde edilen bilgilerle gözlenebilir olup olmadığıdır.



Şekil 4.3 : CMOS kapısı çıkış değişimlerinde anlık akım değişimi [42]



Şekil 4.4 : CMOS evirici yapısı [42]

Güç analizi saldırılarında CMOS kapılarının çıkış değişimlerinde gösterdiği davranıştan faydanılmaktadır [34]. Kriptografik işlem yapan cihazların güç tüketimi yapılan işleme göre ya da kullanılan veriye göre değişmektedir. Yan kanal bilgisi olarak kullanılan güç tüketimi bilgisi ile yapılan işlemler ya da gizli bilgi arasında yüksek korelasyon bulunmaya çalışılmaktadır. Korelasyonu hesaplamak için ilk önce devrenin güç tüketimi hesaplanmalıdır. Güç tüketimini ölçmek için devre ile güç kaynağı arasına küçük değerli bir direnç yerleştirilmektedir. Direncin iki ucundaki gerilim farklılığından devrenin çektiği akım herhangi bir ölçüm cihazıyla (osiloskop vb.) hesaplanabilmektedir.

Güç tüketiminde yan kanal bilgisi sızıntısı ile ilgili Hamming uzaklığı ve Hamming ağırlığı olmak üzere iki tip modelleme vardır [43]. Hamming uzaklığı bütün bit değişimleri hakkında bilgi verirken Hamming ağırlığı aynı anda işlenen değeri ‘1’ olan bitlerin sayısı hakkında bilgi verir.

Güç analizi saldırıları basit ve farksal güç analizi saldırıları olmak üzere ikiye ayrılmaktadır. Basit güç analizi saldırılarında, saldırgan tek ölçüm kullanarak anahtarın tamamını ya da bir kısmını ele geçirmeye çalışmaktadır. Ölçümdeki gürültünün fazla olduğu durumlarda kullanılan farksal güç analizi saldırılarında ise, birçok ölçüm kullanılarak gürültü elimine edilmektedir. İstatistiksel yöntemlerle işlenen veri ile güç tüketimi arasında ilişki aranmaktadır.

İlk pratik güç analizi saldırısı Kocher tarafından DES üzerinde yapılmıştır [5]. Daha sonra bu konuda farklı kriptografik algoritmalar ve farklı cihazlar için pek çok çalışma yapılmıştır.

4.4 Elektromanyetik Analiz Saldırıları

CMOS kapısının çıkış değerindeki değişimin anlık akım değişimine neden olduğu bilinmektedir. Anlık akım değişiminin yanı sıra elektromanyetik yayılım da ortaya çıkmaktadır [34]. İşlenen veriye ya da gerçekleştirilen işleme göre elektromanyetik radyasyon değişmektedir. Elektromanyetik radyasyonun hesaplanmasında kullanılan Biot-Savart yasası aşağıda görüldüğü gibidir.

$$d\vec{B} = \frac{\mu I d\vec{L} \times \vec{\hat{r}}}{4\pi r^2} \tag{4.8}$$

Denklem 4.8'de μ serbest uzay geçirgenliğini, I akım değerini, $d\vec{L}$ akım taşıyan iletkenin uzunluğunu, r akım kolunun ölçüm düzeneğine dik uzaklığını ve $\vec{\hat{r}}$ birim vektörü ifade etmektedir. Bu tek denklem elektromanyetik radyasyon değerinin tamamını vermese de iki noktayı vurgulamaktadır. Bunlardan biri, akım yoğunluğuna göre elektromanyetik radyasyon yoğunluğu değişmektedir. Dolayısıyla veri ile doğrudan ilişkilidir. Diğeri ise elektromanyetik radyasyonun yönü akım yönüne bağlı olarak değişmektedir. Elektromanyetik radyasyon antenler vasıtasıyla ölçülebilmektedir. Antenlerle elde edilen elektromanyetik radyasyon elektromanyetik analiz saldırıları için yan kanal bilgisi olarak kullanılmaktadır.

Elektromanyetik radyasyonun bilgi sızıntısına neden olabileceği 1950 yıllarında fark edilmiş ve engellenmesi için TEMPEST (Transient Electromagnetic Pulse Emanation Standard) standartları getirilmiştir [44, 45]. Ancak elektromanyetik radyasyon kullanılarak yapılan ilk saldırılar 2000'li yıllarda gerçekleştirilmiştir [11, 12]. Daha sonra bu konudaki çalışmalar hızla artmıştır.

Elektromanyetik analiz saldırıları basit elektromanyetik analizi saldırıları (Simple Electromagnetic Analysis - SEMA) ve farksal elektromanyetik analizi saldırıları (Differential Electromagnetic Analysis - DEMA) olmak üzere ikiye ayrılır. Yan kanal bilgisinin farklı olması dışında ölçüm analiz işlemleri güç analizi ataklarındaki gibidir [46, 47].

Elektromanyetik analiz saldırıları ve güç analizi saldırıları arasında bazı farklar vardır. Birinin diğerine tam olarak bir üstünlük kurduğu söylenememekle beraber birbirilerine avantajları ve dezavantajları olan durumlar vardır. Güç analizinde akım

değişimi ölçümü için devre ile güç kaynağı arasına fiziksel müdahale ile bir direnç yerleştirmek gerekirken elektromanyetik analizi saldırılarında buna ihtiyaç yoktur. Devreye hiç müdahale etmeden bir anten vasıtasıyla elektromanyetik alan ölçülebilir. Güç analizinde devrenin çektiği tüm güç kullanılırken elektromanyetik analizde istenilen bölgenin elektromanyetik radyasyonu ölçülmektedir. Elektromanyetik analizde alınan ölçümlerde gerilim değeri güç analizine göre düşük olabilmektedir. Bu nedenle gürültünün çok olduğu sistemlerde ölçümün analiz edilmesi zorlaşmaktadır [48].

4.5 Ses (Akustik) Analizi Saldırıları

Yan kanal analizi saldırılarında yapılmış çalışmaların büyük çoğunluğu devreden çekilen güç tüketimi ve yayılan elektromanyetik radyasyon üzerinedir. Bilinen en eski yan kanal bilgilerinden biri olan sesi kullanarak yapılan çalışmalar diğerleriyle kıyaslandığında çok az olduğu görülmektedir [49].

2004 yılında yapılan çalışmayla işlemcinin yaptığı işlemlere ve işlemlerin süresine göre çıkardıkları seslerin değişimi arasında korelasyon olduğu görülmüştür [50].

Ses analizi saldırılarına karşı alınabilecek önlemlerin başında ses yalıtımlı bir kutu kullanılarak çıkan sesin bastırılması gelmektedir.

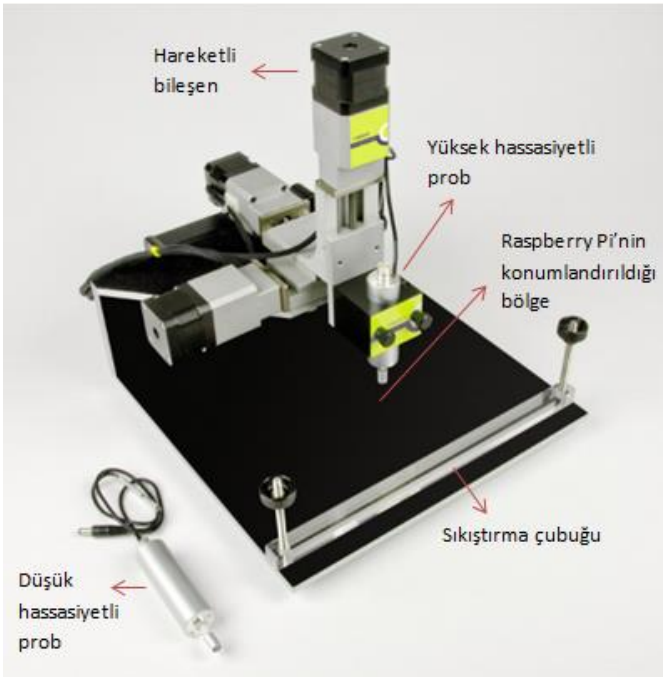
5. ÖLÇÜM DÜZENEĞİ

Bu bölümde tez çalışmasını gerçekleştirmek için kurulan ölçüm düzeneğinden ve bileşenlerinden bahsedilmiştir.

Ölçüm düzeneği şunlardan oluşur: Raspberry Pi, bilgisayar, osiloskop, elektromanyetik alan alıcısı sistemi.

5.1 Elektromanyetik Alan Alıcısı Sistemi

Raspberry Pi üzerindeki elektromanyetik radyasyonu almak için Riscure firmasının EM Probe Station ürünü kullanılmıştır [51]. Bu sistemde düşük ve yüksek hassasiyetli olmak üzere iki adet prob vardır. Düşük hassasiyetli probun genel kullanım amacı yüksek gerilimli elektromanyetik yayılımları alma iken yüksek hassasiyetli probun genel kullanım amacı düşük gerilimli elektromanyetik yayılımları almaktır. Tez çalışmasında yüksek hassasiyetli EM prob kullanılmıştır [51]. Bu prob için kullanılan farksal yükselteç 15pT/√Hz@1MHz'lik bir manyetik gürültüyle çalışır.



Şekil 5.1 : Elektromanyetik ölçüm istasyonu.

EM Prob istasyonu özellikle yan kanal analizi için üretilmiş bir güvenlik aracıdır. Üç donanım parçasından oluşmaktadır [51]. İki adet EM prob ve hareketli XYZ masasından oluşur. Bu donanımlar prob istasyonunun “Inspector” isimli yazılımıyla entegre çalışır [51]. Bu yazılım sayesinde yapılacak analize göre donanım bileşenlerinde ayarlama yapılır. Elektromanyetik radyasyondan yapılacak analizin kalitesi kullanılacak proba, probun konumuna direk bağlıdır. Hareketli XYZ donanım bileşeni sayesinde Raspberry Pi üzerinde en iyi emisyonu veren konuma EM prob yerleştirilmelidir. Raspberry Pi üzerinde Broadcom firmasının BCM2835 model işlemcisi bulunmaktadır. Şifreleme algoritması işlemci üzerinde koştuğundan EM prob işlemci üzerinde bir bölgeye konumlandırılmalıdır. EM probun ölçüm alanı Raspberry Pi platformunun üzerinde bulunan işlemcisi BCM2835’in boyutundan 16 kat daha küçüktür. Bu sebeple işlemcinin yüzeyi 16 parçaya ayrılarak her noktadan ölçümler alınmıştır. Kriptografik işlemle ilgili en iyi emisyonu veren bölgeden tez çalışmasına devam edilmiştir. Bu çalışmalarla ilgili detaylar Bölüm 6’da anlatılacaktır.

5.2 Raspberry Pi

Raspberry Pi, Raspberry Pi Vakfı tarafından 2009’da geliştirilmeye başlanmış kredi kartı boyutunda tek kartlı bir mini bilgisayardır [15]. İlk sürümü olan model B 2012 yılında piyasaya çıkmıştır (Şekil 5.2). Düşük maliyeti ve bilgisayarda yapılmak istenen her işlemin yapılabilmesi sayesinde büyük rağbet görmüştür. Secure Shell (SSH) veya putty.exe gibi uygulamalarla ağ üzerinden Raspberry Pi erişimi sağlanabilmektedir.

Şekil 5.2 : Raspberry Pi Model B [52].

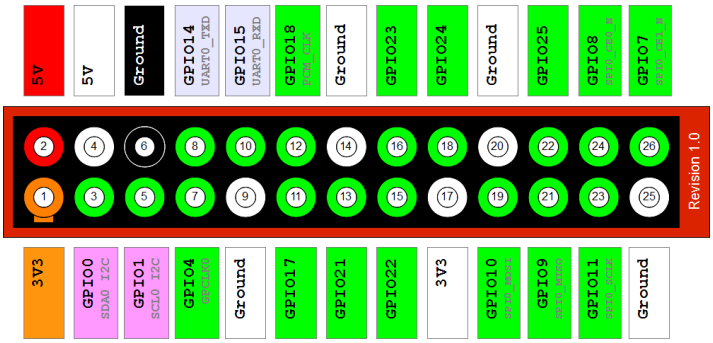
Tez çalışması boyunca Raspberry Pi Model B kullanılmıştır. İşletim sistemi güvenli dijital hafıza kartı (Secure Digital Card - SD Card) üzerinde kuruludur. Üzerinde çalışan işletim sistemi ise Debian [53] tabanlı Raspberry Pi ailesi için geliştirilmiş Raspbian [54] işletim sistemidir.

Raspberry Pi Model B'nin teknik özellikleri aşağıdaki gibidir.

- Broadcom BCM2835 işlemcisi
- 700 MHz ARM1176JZF-S tek çekirdekli CPU
- Broadcom VideoCore IV GPU
- 512 MB RAM
- 2 x USB2.0 Ports
- Video çıkışı (Compozit (PAL ve NTSC), HDMI ya da LCD (DSI) aracılığıyla)
- Ses çıkışı: 3.5mm Jack ya da HDMI üzerinden
- Depolama Alanı: SD/MMC/SDIO
- 10/100 Ethernet (RJ45)
- Düşük seviyeli çevre birimleri:
    - 8 x GPIO
    - UART
    - +3.3V
    - +5V
    - Toprak bağlantısı
- Güç gereksinimleri: 5V @ 700 mA MicroUSB veya GPIO pinleri üzerinden
- Desteklenenler: Debian GNU/Linux, Fedora, Arch Linux, RISC işletim sistemleri vb.

GPIO (General Purpose Input/Output) pinleri genel amaçlı giriş çıkış bağlantılarıdır. Bu bağlantılar tez çalışmasında büyük önem arz etmektedir. "Low" durumu 0 V,

"high" durumu 3,3V DC olarak gösterilir. Tez çalışmasında 12.pin GPIO18 çıkış portu olarak tanımlanmıştır. Osiloskop kanalına bağlı probun bir ucu bu porta bağlıyken toprak bağlantısı 25. pine bağlıdır. Bu kanal üzerinden alınan değerlerle ölçüm alma işlemi otomatize edilmiştir. Şekil 5.3'den GPIO pinleri görülebilir.



Şekil 5.3 : GPIO pin gösterimi [55].

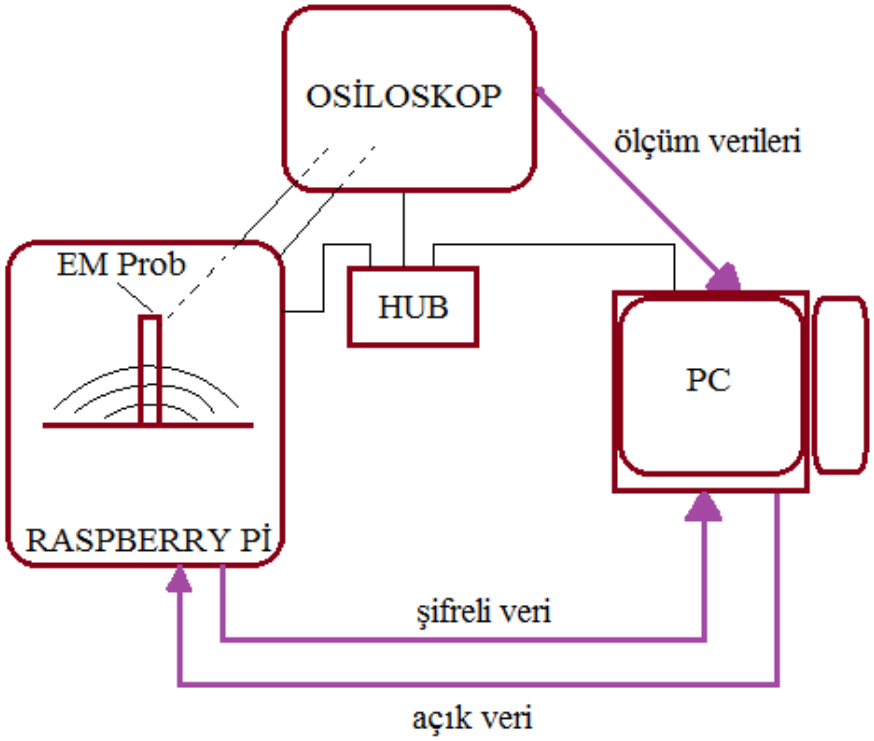
Bu tez çalışmasında yan kanal saldırısı BCM2835 işlemcisi üzerinden alınan ölçümlerle gerçekleştirilmiştir. Bu nedenle BCM2835 işlemcisiyle ilgili biraz daha detaya girilmiştir. BCM2835 işlemcisi armv11 [56] mimarisine sahip 32 bitlik bir işlemcidir [57]. Yapı olarak yüksek hızlı ve yüksek performanslıdır.

Tez çalışmasında Raspberry Pi kullanılmasının nedeni şimdiye kadar yapılan çalışmaların çoğunda gürültünün az olduğu akıllı kart ya da sadece kriptografik işlem yapan alanda programlanabilir kapı dizileri (Field Programmable Gate Array - FPGA) türevi ürünlerin kullanılmış olmasıdır. Bu gibi donanımlarda herhangi bir önlem alınmadıysa yan kanal saldırıları başarıyla gerçeklenebilmektedir. Raspberry Pi üzerinde işletim sistemi çalıştığı için kriptografik işlem gerçekleştirirken araya farklı işlemler alabilmektedir. Alınan ölçümlerde hizalama sorunları olmaktadır. Bu gibi nedenler çalışmanın motivasyon kaynağını oluşturmaktadır.

5.3 Ölçüm Düzeneğine Genel Bakış

Raspberry Pi üzerindeki Broadcom firmasının BCM2835 işlemcisi yan kanal saldırısının temel hedefi konumundadır. Raspberry Pi üzerinde 2 adet evrensel seri veriyolu (Universal Serial Bus – USB) portu bulunmaktadır. Bu portlara monitör ve klavye bağlanarak RSA algoritmasını gerçekleyecek kodların yazılması ve derlenmesi işlemleri gerçekleştirilir. Ayrıca portlar sayesinde kütüphane yükleme dosyaları ya da kodlar başka bilgisayardan Raspberry Pi içerisine kopyalanabilir.

Raspberry Pi'nin genel amaçlı kullanılan pinlerinden biri osiloskobun bir kanalına bağlıdır. Bu kanalla osiloskop ölçümü başlatmak için tetik alır. Kriptografi işlemi boyunca dışarıya sızdırılan elektromanyetik yayılım daha önce anlatılan yüksek hassasiyetli prob ile alınır. Bu prob osiloskobun başka bir kanalına bağlıdır. Osiloskop GPIO pinlerindeki gerilim artışını farkettiği an elektromanyetik radyasyonu alır ve binary formatında kaydeder. Daha sonra Matlab'ta sinyal analizi gerçekleştirilmesi için başka bilgisayara aktarılır. Şekil 5.4'te ölçüm düzeneğinin blok diyagramı görülebilir [22]. Kullanılan osiloskop cihazının markası Tektronix'dir [58]. Maksimum örnekleme oranı 40GS/saniye, bant genişliği 2.5 GHz'dir.



Şekil 5.4 : Ölçüm alma düzeneği.

5.4 Kullanılan Yazılımlar

Bu bölümde kullanılan kütüphaneler ve ölçüm düzeneğinde kullanılan yazılımlar anlatılacaktır.

Bu projede GMP (the GNU Multiple Precision Arithmetic) kütüphanesi kullanılmıştır [59]. Bu kütüphane büyük sayılarla işlem yaparken daha optimize makine kodları üretmeyi sağlar. RSA algoritmasında 1024 bitlik sayılarla işlem yapılacağından bu kütüphanenin kullanması tez çalışması için büyük avantaj

sağlamıştır. Böylelikle hem daha optimize bir kod üretildi hem de geliştirme süresi kısaltılmış oldu. Bu kütüphane kendi sitesinden indirilip kolayca yüklenebilir. Yüklendikten sonra kullanmak için kodun başına aşağıdaki gibi eklenebilir.

#include “gmp.h”

Elektromanyetik analiz için Raspberry Pi üzerinde C dilinde yazılmış RSA hızlı üs alma ile her zaman kare alma ve çarpma programları yazılmış ve derlenmiştir. Şifreleme için kullanılacak anahtar değeri bu kodların içerisine gömülmüştür. Program her çalıştırıldığında şifrelenmiş veri Raspberry Pi’nin standard çıkış akımına yazılmaktadır.

Ölçüm alma sisteminin otomatik hale getirilip birden çok ölçüm alınması farksal güç analizi için gereklidir. Bu işlemin gerçeklenmesi için tüm sistem bilgisayar kontrolünde çalışmalıdır. Bilgisayar, ölçüm alma sisteminde yapılması gereken işlemleri sırasına göre yaptırmalıdır. Bilgisayar üstünde koşan kod, osiloskop ve Raspberry Pi platformunu kontrol etmektedir. Otomatik bir ölçüm düzeneği döngü halinde sırasıyla şu işlemleri gerçekleştirir.

- Bilgisayar, osiloskob ile bağlantı kurar.
- Osiloskobun yapılandırma ayarları yapılır ve tetik bekler konuma getirilir.
- Bilgisayar, Raspberry Pi ile bağlantı kurar ve şifreleme yapmasını bildirir.
- Osiloskop ölçümü alır ve kaydedilmek üzere bilgisayara gönderir.
- Raspberry Pi’den gelen şifrelenmiş veri bilgisayarda oluşturulmuş dosyaya kaydedilir.

Bu döngü istenen ölçüm sayısına ulaşıncaya kadar devam eder.

Raspberry Pi ile bilgisayarın haberleşmesi için bir çeşit soket dinleme programı gerekmektedir. Bu program ihtiyacı C dilinde yazılmış bir kod ile giderilmiştir. Program şu işlemleri gerçekleştirmektedir.

- Sürekli 5001 numaralı port dinlenir.
- Porta gelen veri komut satırından çalıştırılır.
- Standart çıkış akımına basılan veri aynı port üzerinden geri gönderilir.
- İşlem başarılı gerçekleşmiş ise ekrana başarılı bilgisi basılır.

Böylelikle sistem otomatik olarak çalışabilecek duruma gelmiştir.

5.5 Tetik Üretme

Tetik üretme osiloskobun doğru zamanda üretilen elektromanyetik yayılımı alması için çok önemli bir faktördür [39]. Raspberry Pi üzerinde çalışan RSA kodunun kriptografik işlemlerinin olduğu bölüm çalışmadan önce osiloskop kanallarından birine bağlı pin 0V'dan 3.3V'a çekilir. Osiloskopta ise Raspberry Pi ile bağlantılı analog kanalın 2.5V ve üzerinde bir gerilim alındığında tetik alması için ayar yapılır. Osiloskop bu değişikliği farkettiği an osiloskop ekranından yapılan ayar sayesinde ölçümleri ekranında gösterir ve kaydedilmek üzere bilgisayara gönderir. Daha sonra bu ölçümler MATLAB ile analiz edilerek bilgi elde edinilmeye çalışılır.

Tetik için osiloskobun probu Raspberry Pi'nin 12. pini olan GPIO18'e bağlanır. Toprak ucu ise 25. pine bağlanır. Raspberry Pi üzerinde yazılmış olan kodda RSA işlemi başlamadan önce pin set edilir. Daha sonra pin tekrardan 0 volta çekilerek diğer işlem için beklemeye geçilir. Şekil 5.5'te ilgili kod parçası görülmektedir.

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

                        if( ! bcm2835_init() )
                return 1;

        bcm2835_gpio_clr(LED);
        bcm2835_gpio_set(LED);
...
        RSA Algoritması
...
        bcm2835_gpio_clr(LED);
```

Şekil 5.5 : GPIO 12. pinin tetik olarak ayarlanmasını sağlayan kod.

6. RSA GERÇEKLEMELERİNE ELEKTROMANYETİK ANALİZİ

Bu bölümde RSA algoritması için ölçümleri alma, filtreleme ve istenmeyen gürültülerden arındırma için yapılan işlemler anlatılmaktadır.

6.1 Kare Alma ve Çarpma Algoritması

Bu bölümde kare alma ve çarpma işlemlerinden oluşan RSA algoritmasının GMP kütüphanesiyle nasıl gerçeklendiği anlatılmaktadır. Kullanılan şifreleme anahtarı ikilik sisteme göre bitlerine ayrılmaktadır. Daha sonra en anlamlı bitten en anlamsız bite kadar (soldan sağa) tüm bitler taranır. Her turda sonucun karesi alınır. Eğer işlem yapılan anahtar bit değeri 1 ise çarpma işlemi de gerçekleştirilmektedir.

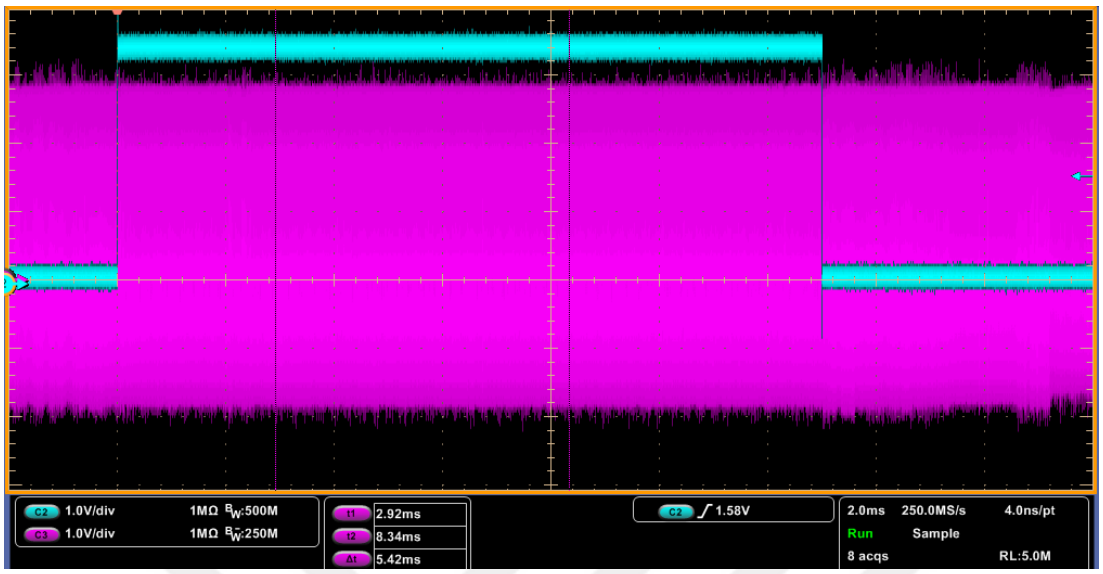
```
for(i = bits-1; i >= 0; i--) {
    mpz_mul(d, d, d); // Kare alma
    mpz_mod(d, d, n);
    if(mpz_tstbit(e, i) == 1) {
        mpz_mul(d, d, m); // Çarpma
        mpz_mod(d, d, n);
    }
}
```

Şekil 6.1 : Kare alma ve çarpma algoritması.

6.2 Ölçümleri Alma

Daha önce Bölüm 5.5'de de anlatıldığı gibi RSA işlemi gerçekleştirilmeden hemen önce genel amaçlı giriş çıkış pinleri kullanılarak sistemin tetik alması sağlanır. RSA işlemi tamamlandıktan sonra da tetik için kullanılan genel amaçlı giriş çıkış pini tekrardan sıfırlanır. Bu işlem sayesinde osiloskop RSA'in gerçekleştiği noktayı tespit eder ve doğru ölçümü kaydeder. Basit elektromanyetik analizi saldırılarında tek bir ölçüm yeterliyken farksal elektromanyetik analizde birden çok ölçüme ihtiyaç duyulur. Bu gibi durumlarda üstte bahsedilen tetik alma ve ölçümün kaydedilip bilgisayara gönderilme işlemi döngü içerisinde yapılır. Her bir işlem için ayrıca osiloskop ayarları, kullanılan açık veri, anahtar ve şifrelenmiş veri de ayrıca kaydedilir. Aşağıda örnek olarak alınan bir ölçüm bulunmaktadır. Şekil 6.2'de yeşil

renkli kanal tetik işaretidir. Mor renk ise elektromanyetik radyasyon ölçümüdür. Yatay eksen zamanı, dikey eksen ise genliği temsil etmektedir.



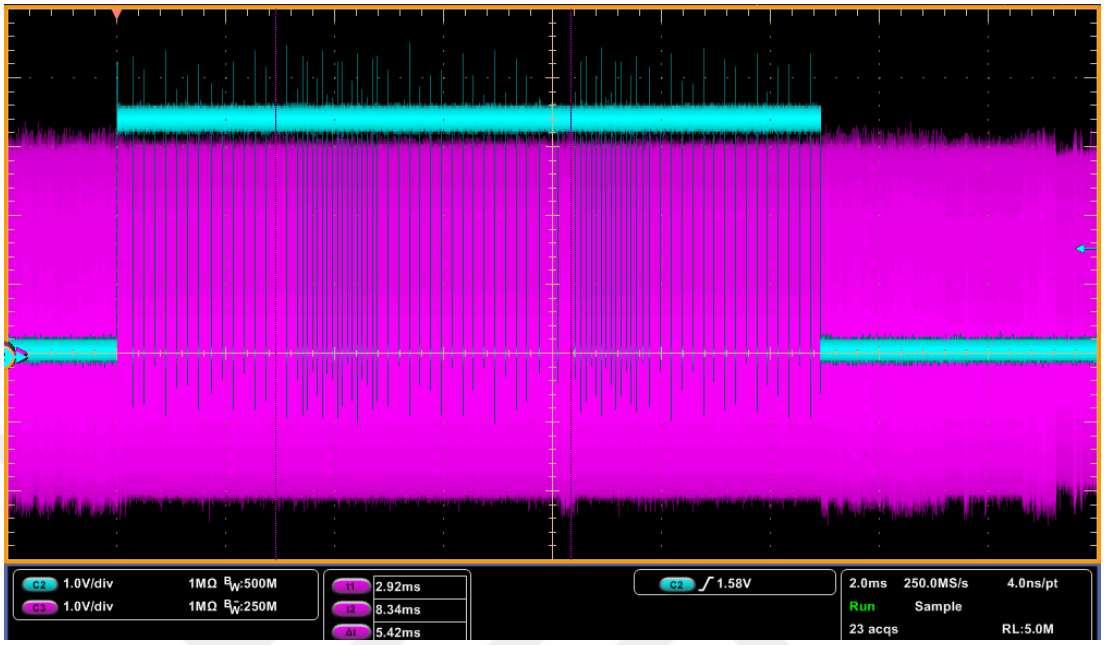
Şekil 6.2 : RSA işlemi yapılırken alınan ölçümün osiloskop ekran görüntüsü.

- RSA anahtarı: 80 bit (FFFF0000FFFF0000FFFF)
- RSA algoritması: GMP kütüphanesi kullanılarak çarpma ve kare alma
- Örnekleme frekansı: 250 MS/saniye

Örnekleme frekansı şifreleme işleminin tamamını tek bir ölçümde gösterilebilecek şekilde ayarlanmalıdır. Örneğin; 1024 bitlik RSA işlemi gerçekleştirildiğinde ölçüm tamamını ekranda gösterebilmek için örnekleme frekansı 250 MS/s olmalıdır. Bu kısıtlama osiloskop hafızasıyla ilgilidir. Şekil 6.2'de bulunan ölçümde 80 bitlik RSA işlemi yapılmasına rağmen bu değer korunmuştur. Örnekleme frekansı olarak 250 MS/saniye özelliğini sağlayan herhangi bir osiloskop ile ataklar gerçeklenebilir.

Şekil 6.2'deki ölçüm incelendiğinde tetik alma işlemi olmasaydı RSA operasyonunun gerçekleştiği yerin görülmesi mümkün olmayacaktı. Ölçümdeki gürültü seviyesi yüksek olduğundan RSA işlemi sırasında, öncesinde ve sonrasında genlik seviyesi aynı gözükmektedir. Tetik alma sayesinde işlemin nerde başladığını ve süresi sabit olmadığı için, tahmini olarak işlemin ne kadar sürdüğü görülebilmektedir. Buradan hareketle, RSA işlemini osiloskop ekranında daha da detaylı görmek ve incelemek için her bit işlemi arasında tetik almasını sağlayacak işlem gerçekleştirilmiştir. Tetik oluşturma güç tüketimini ihmal edilebilecek düzeyde değiştirmektedir. Kriptografik işlemler ile kıyaslandığında bu değer çok küçüktür.

Her bit işleminde tetik alınması sayesinde şifreleme anahtarının bit değerinin 1 ya da 0 olmasına göre yapılan işlem süresi arasındaki farklılık gözlemlenmiştir. Bunun için Şekil 6.3 incelenebilir.



Şekil 6.3 : RSA anahtarın her bit işleminde tetik alması durumu.

- RSA anahtarı: 80 bit (FFFF0000FFFF0000FFFF)
- RSA algoritması: GMP kütüphanesi kullanılarak çarpma ve kare alma
- Örnekleme frekansı: 250 MS/saniye

Analiz işlemlerinde istenilen şifre çözme ya da imzalama işlemi haricindeki gerçekleştirilen tüm işlemler gürültü kabul edilmektedir. Çevresel gürültüler (giriş çıkış portları, USB-ethernet arayüzü, monitör için HDMI çıkısı, güç bağlantısı, Raspberry Pi üzerinde çalışan işletim sistemi prosesleri ve diğer uygulamalarla örnekler çoğaltılabilir) nedeniyle RSA işleminin gerçekleştiği yerin gözle tespit edilebilmesi mümkün olmamıştır. Örnekleme frekansının 250MS/s ayarlanmasından sonra şifreleme işleminin tamamını osiloskop ekranında en geniş biçimde gösterilmesi için alınacak ölçümün zaman değeri belirlenmiştir. 2 milisaniyelik bir ölçüm alındığında şifreleme işleminin tamamı ekrana sığmaktadır. Bu işlem sonucunda Şekil 6.2'de görülen ölçümde 5000000 nokta bulunmaktadır. Yapılacak analizler sonucunda nokta sayısı yeterli gelmez ise örnekleme frekansı arttırılarak nokta sayısı arttırılmalıdır. Şekil 6.2'de resmedilen osiloskop ekranında görünen tetik sayesinde RSA işleminin 500000. nokta itibariyle başladığı görülmektedir.

Elektromanyetik radyasyon ölçümü incelendiğinde RSA işleminin gerçekleştirildiği bölge ile RSA işleminin gerçekleştirilmediği bölge arasında genlik açısından gözle görülür bir fark bulunmamaktadır. RSA işleminin nerede yapıldığının tetik olmaksızın anlaşılabilmesi için filtreleme tekniklerine ihtiyaç duyulmaktadır. Alınan ölçümde RSA işlemiyle alakası bulunmayan elektromanyetik radyasyon verisi tezin ilgi alanı dışındadır. Bu tez çalışmasında filtre kullanılmasının temel gayesi ölçümde bulunan RSA işlemiyle ilgili verileri diğer istenmeyen faktörlerden ayırmaktır. İstenmeyen faktörler sistem çalışması ve çevresel birimler kaynaklı olabilmektedir. Doğru filtre kullanılarak yapılan filtreleme sonucunda RSA işleminin gerçekleştirildiği bölge haricindeki bölgelerde ölçüm genlik seviyesinin düşmesi beklenmiştir. Bu nedenle elde edilen ölçüm farklı işlemlerden geçirilerek çarpma ve kare alma işlemleri sırasında çekilen güç farklılığı nedeniyle kaynaklanan örüntü farklılığı bulanacaktır. Örüntü farklılığı tespiti halinde RSA işleminde kullanılan anahtar için tahminde bulunmak mümkün hale gelecektir.

6.3 Filtreleme Teknikleri

Basit Elektromanyetik analizi (SEMA) atağı gerçekleştirilirken iki adet filtre kullanılmıştır. Bu bölümde bu filtrelerin mantığı detaylı şekilde ele alınacaktır. Raspberry Pi üzerinde kriptografik işlem gerçekleştirirken alınan ölçümde kriptografik işlem ile ilgisi olmayan birçok gürültü bulunmaktadır. Bu gürültüler işlemcinin üstünde koşan işletim sistemi ya da farklı sistem operasyonları nedeniyle ortaya çıkmaktadır. Kullanılacak olan ilk filtre kriptografik işlemle alakası olmayan ölçüm verilerinin ayıklanmasını sağlayacak bir bant geçiren filtre olacaktır. Kullanılacak filtrenin bandının tespiti için ölçüm frekans bölgesine geçirilir. Frekans bölgesi görüntüsü kullanılarak yüksek genliğe sahip frekans değerlerine odaklanılır.

Raspberry Pi donanımının elektromanyetik radyasyonu

$$p(t) = P_{sabit}(t) + p_{dinamik}(t) \tag{6.1}$$

olarak gösterilebilir. Bu formülde P_{sabit} anlık değişmeyen bölüm ve $p_{dinamik}$ ise dinamik bölümdür. Genellikle dinamik bölüm sabit bölümden daha zayıftır. Bilgi içeren sızıntıyı bulmak için elektromanyetik radyasyondan bu dinamik bölümü

ayırmak gerekir. Bu ayırma işlemi ne kadar iyi yapılırsa yapılan analiz işlemi de o kadar kaliteli olur [29].

Sinyalin genliğinin modülasyonu,

$$s(t) = p(t)\cos(w_r t) \tag{6.2}$$

Denklem 6.2 ile verilmektedir. Bu denklemde w_r taşıyıcı frekanstır. Genlik demodülasyonunu kullanarak $p(t)$'yi ya da zayıf dinamik parçası olan $p_{dinamik}(t)$ 'yi elde edebiliriz. Genlik demodülasyonu için 2013 yılında Intel Atom işlemci üzerinde gerçekleştirilen çalışmada kullanılan zarfla algılama (envelope detection) yöntemi kullanılmıştır [29]. Bu yöntem yaygın olarak kullanılmaktadır. Yöntem açıklaması aşağıdaki gibidir.

Orijinal sinyalin frekans bölgesi gösterimi için Ayrık Fourier Dönüşümü (Discrete Fourier Transform – DFT) kullanılabilir. $F(jw) = DFT\{p(t)\}$ şeklinde gösterilsin. Doğrultulmuş sinyalin spektrumu ise Fourier serisi kullanılarak hesaplanır [60]:

$$DFT\{|s(t)|\} = DFT\{p(t)|\cos(w_r t)|\} = DFT\left\{p(t).\frac{2}{\pi}\sum_{v=-\infty}^{\infty}\frac{(-1)^v}{1-4v^2}e^{j2vw_r t}\right\} \tag{6.3}$$

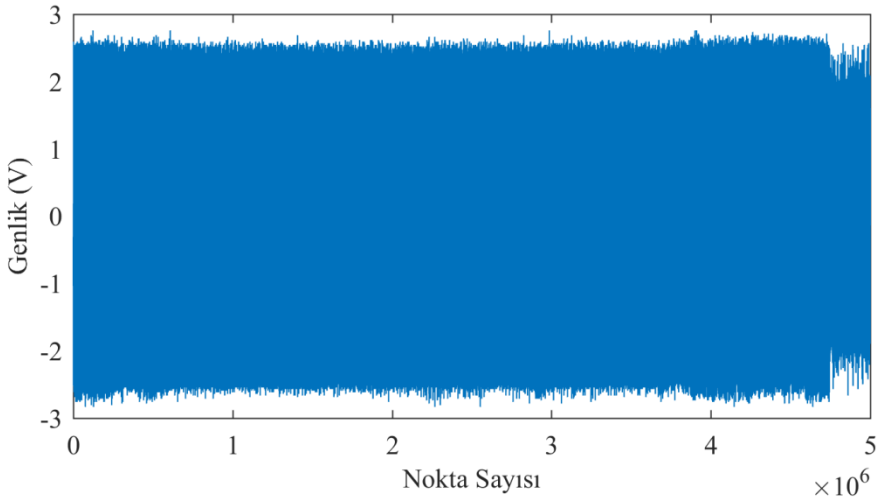
$$DFT\{|s(t)|\} = \frac{2}{\pi}\sum_{v=-\infty}^{\infty}\frac{(-1)^v}{1-4v^2}DFT\{p(t)e^{j2vw_r t}\} = \frac{2}{\pi}\sum_{v=-\infty}^{\infty}\frac{(-1)^v}{1-4v^2}F(jw - j2vw_r) \tag{6.4}$$

Doğrultulmuş sinyal, elektromanyetik radyasyon sinyalinin spektrumuna benzerdir. Fakat spektrum ölçüklendirilmiş ve taşıyıcı frekansın tüm çift katlarında tekrarlanmaktadır. Düşük frekansta çalışan uygun bir bant geçiren filtre istenen $p(t)$ sinyalini ölçümden izole etmek için kullanılabilir [29].

6.4 Ölçümleri MATLAB Kullanarak Filtreleme

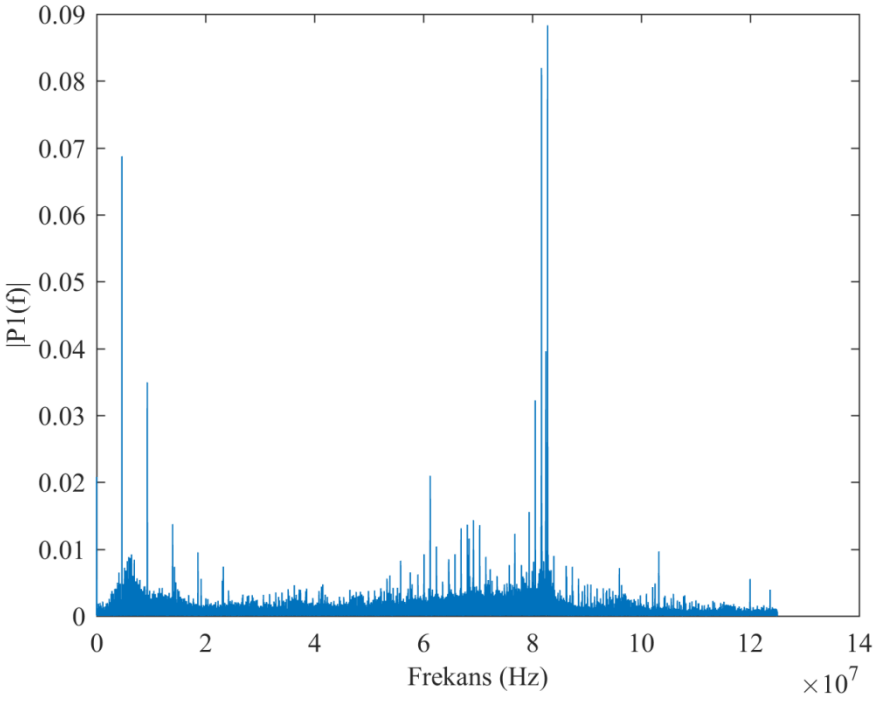
Seksen bitlik "9FFF0000FFFF0000FFFF" anahtarı kullanılarak RSA şifreleme işlemi yapılmıştır. Daha sonra osiloskoptan bilgisayara gönderilen ölçüm verisi MATLAB aracılığıyla bilgisayar ekranında oluşturulmuştur (Şekil 6.4).

Ölçümleri filtreleme yani kriptografik işlemle ilgili veriyi çevresel etkiler dolayısıyla oluşan gürültü verisinden ayırmak için öncelikle bu ölçümlerin hangi frekans aralığında olduğu bulunmalıdır [29].



Şekil 6.4 : MATLAB kullanılarak oluşturulmuş orijinal ölçüm verisi.

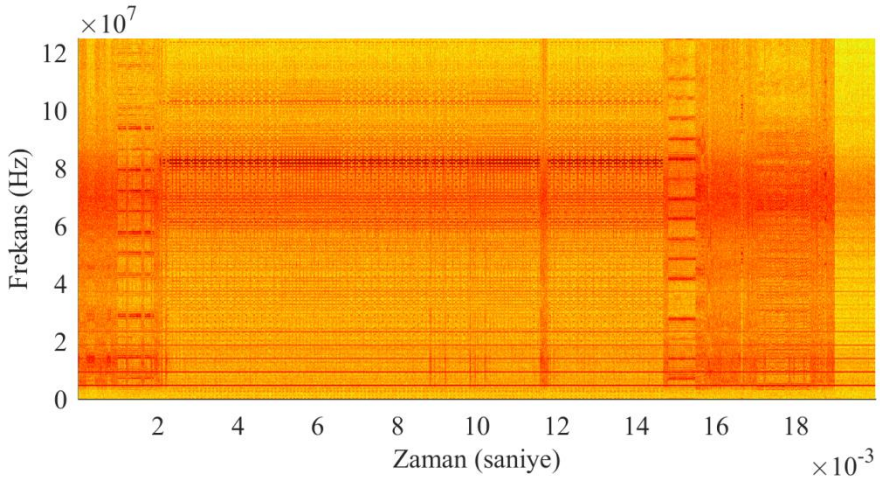
Bu işlem için ilk önce Şekil 6.4'de görünen ölçüm verisi frekans bölgesine geçirilir. Bu işlem sonucunda genliklere bakılarak hangi frekansta yoğunluk oluştuğu saptanır. Şekil 6.5'ten de görüleceği gibi en yüksek genlik 80 MHZ yakınında oluşmuştur.



Şekil 6.5 : Ölçümün frekans bölgesi görüntüsü.

Daha sonra Şekil 6.4'de gösterilen ölçümün spektrogramı MATLAB aracılığıyla çizdirilir. Spektrogram işlevi, MATLAB Sinyal İşleme Araç Kutusu'nda bulunmaktadır. Spektrogram işlevi ölçümde bulunan verilerin hangi frekanslarda yoğunlaştığını tespit etmektedir [29]. Frekansın yoğunluğuna göre ilgili yerdeki renk koyulaşmaktadır. Bu şekle bakarak hangi frekanslarda yoğunluk olduğunu tespit edilebilir.

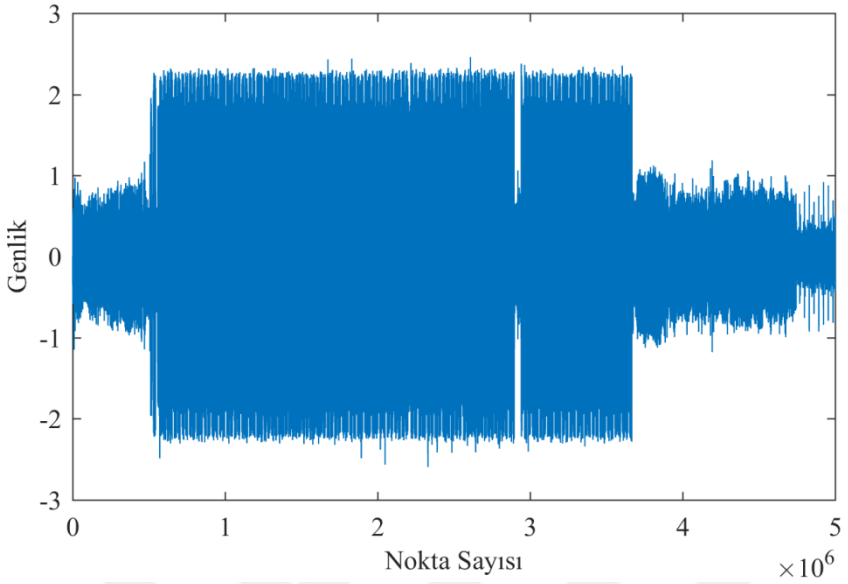
Şekil 6.6'da verilen spektrogram çizimi incelendiğinde Şekil 6.2'de verilmiş osiloskop görüntüsündeki ölçümle denk bir çizim elde edildiği görülmüştür. Şekil 6.2'deki ölçümde onda birlik bölümden sonra tetiğin aktif olduğu görülmektedir. Şekil 6.6'da da koyu kırmızı olan çizginin tetiğin olduğu yerden başladığı görülmektedir. Şekil 6.6'da kırmızı rengin yoğunlaştığı frekanslar yoğun veriyi temsil etmektedir. Kriptografik işlemin yoğun bir işlem gücü gerektirdiği bilinmektedir. Elektromanyetik yayınımın yoğun olduğu frekans aralığı incelenmek için Şekil 6.6'ya bakılabilir. Elimizdeki ölçümden çevresel gürültüleri filtreleme işlemini gerçekleştirmek için kırmızı rengin en yoğun ve koyu olduğu bölge olan 79 MHz ile 85 MHz arasını filtreleyecek bir bant geçiren filtre tasarlandı. Elde edilen ölçüm bu filtreden geçirildiğinde kriptografik işlem yapılmayan bölgelerdeki ölçüm verisinin/elektromanyetik yayınımın önemli ölçüde azalması beklenmiştir.



Şekil 6.6 : Ölçümün spektrogram çizimi.

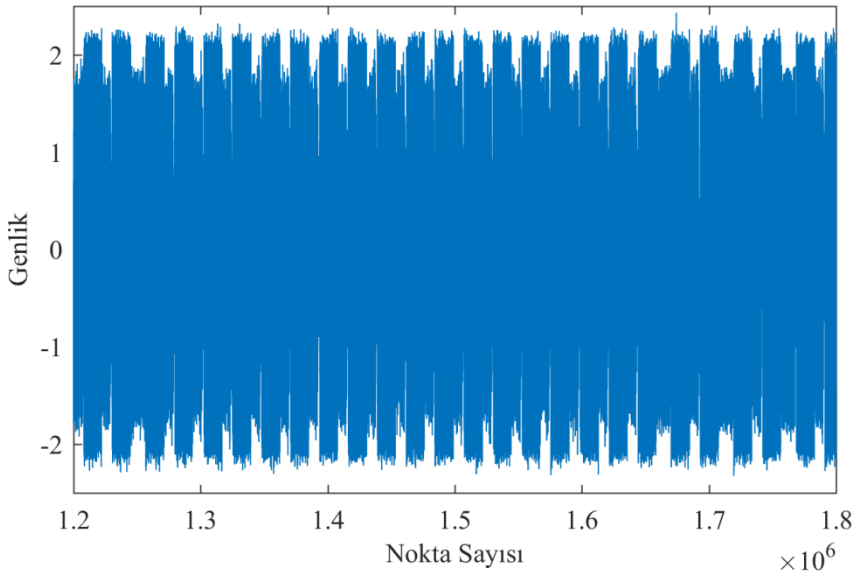
Filtreden geçirilmiş ölçüm verisi tekrardan çizdirildiğinde kriptografik işlemin yapıldığı bölüm haricindeki verilerin, yani sistem kaynaklı gürültülerin azaldığı görüldü. Şekil 6.7'de görüldüğü gibi RSA işleminin yapıldığı yer tetik ekranda olmamasına rağmen kolaylıkla fark edilebilmektedir. Çünkü RSA işleminin

gerçekleştiği bölgedeki verilerin hem genliği daha büyük hem de veriler daha düzenlidir.



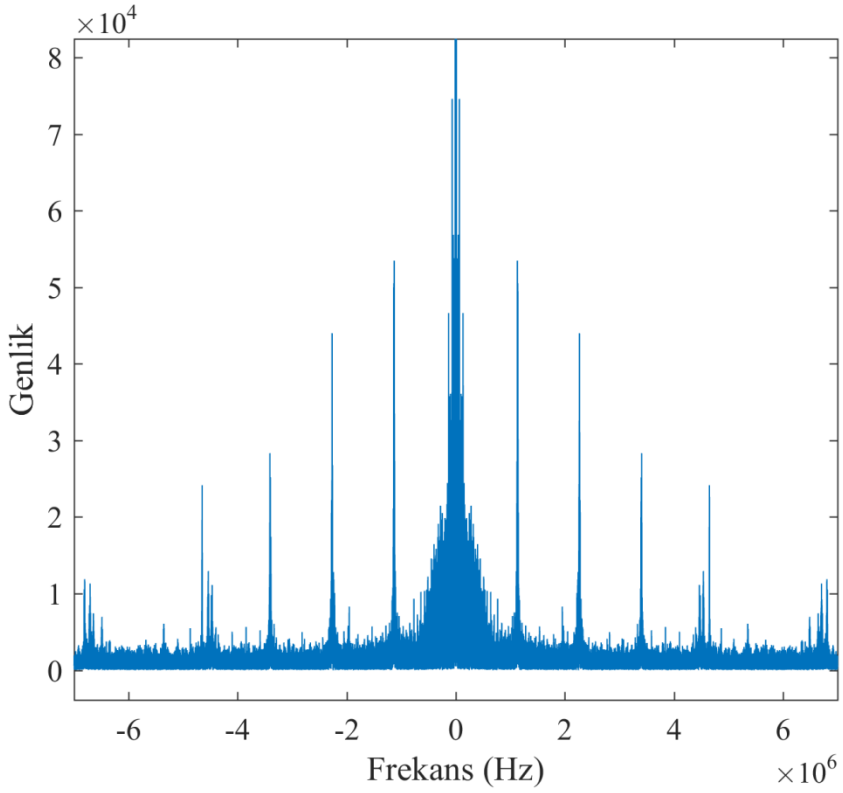
Şekil 6.7 : Bant geçiren filtreden geçirilmiş ölçüm.

Şekil 6.7 incelendiğinde RSA işleminin olduğu yer görünmesine rağmen bu filtreleme işleminde kullanılan şifreleme anahtarının değeri ile ilgili net bir fikir yürütülmesini sağlanamamaktadır. Şifrelemenin olduğu bölgeye yakınlaşıldığında anlamlı bir farklılık görülememiştir. Şekil 6.8'de RSA işleminin olduğu bölgenin yakınlaştırılmış çizimi görülmektedir.



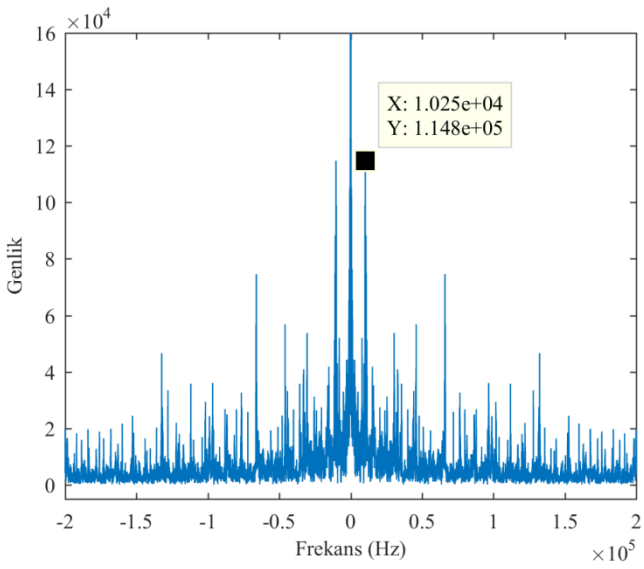
Şekil 6.8 : Bant geçiren filtre sonrası yakınlaştırılmış ölçüm.

Bölüm 6.3'de daha detaylı bahsedildiği gibi şifreleme anahtarıyla ya da işlemcinin yaptığı işlemlerle ilgili bilgi edinebilmek için elde edilen ölçüm verisinden zayıf olan dinamik bileşenin ayrılması gerekmektedir. Bu dinamik bileşen kriptografik işlemle ilgili bilgi taşımaktadır. Bunun için ilk önce taşıyıcı frekansın bulunması gerekmektedir. Taşıyıcı frekansın bulunup sinyalin dinamik parçası çıkarıldığında çarpma ve kare alma işlemleri arasında fark görülmesi amaçlanmaktadır. Bu sayede iki işlem birbirinden ayırt edilebilecektir. Taşıyıcı frekans bilinmediği için ilk önce sinyalin mutlak değeri alınmıştır. Bu işlem sinyal spektrumunun merkezini DC'ye kaydırmıştır. Daha sonra yeni spektrum çizilerek taşıyıcı frekans hakkında tahminde bulunulabilir. Şekil 6.9'da ve Şekil 6.10'da yeni spektrumun görüntüsü verilmiştir.



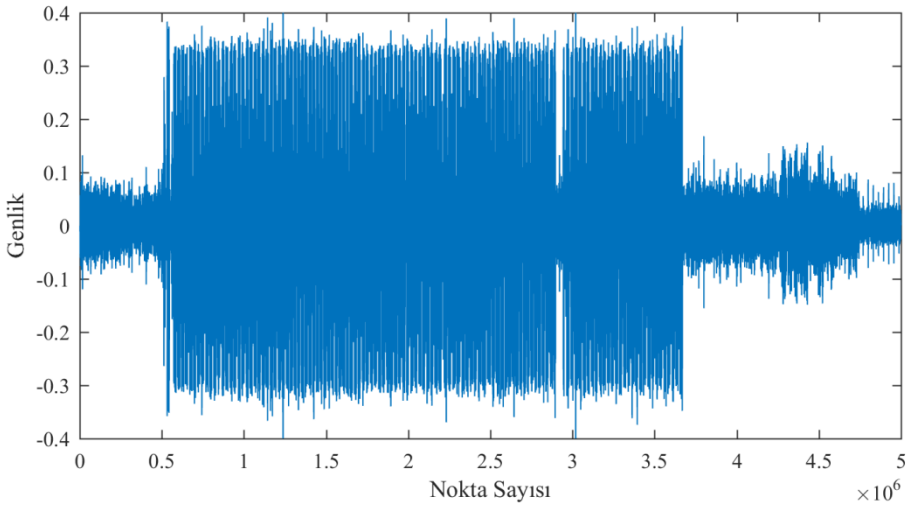
Şekil 6.9 : Doğrultulmuş sinyalin spektrumu.

Spektrum incelendiğinde DC merkezde büyük bir tepe daha sonra onun etrafında daha ufak tepelerin oluştuğu görüldü. Şekil 6.10'da spektrumun DC merkez etrafına yakınlaşılmış hali mevcuttur. DC merkez etrafına yoğunlaşıldığında kHz seviyesinde frekanslarda da tepeler oluştuğu görülmüştür.



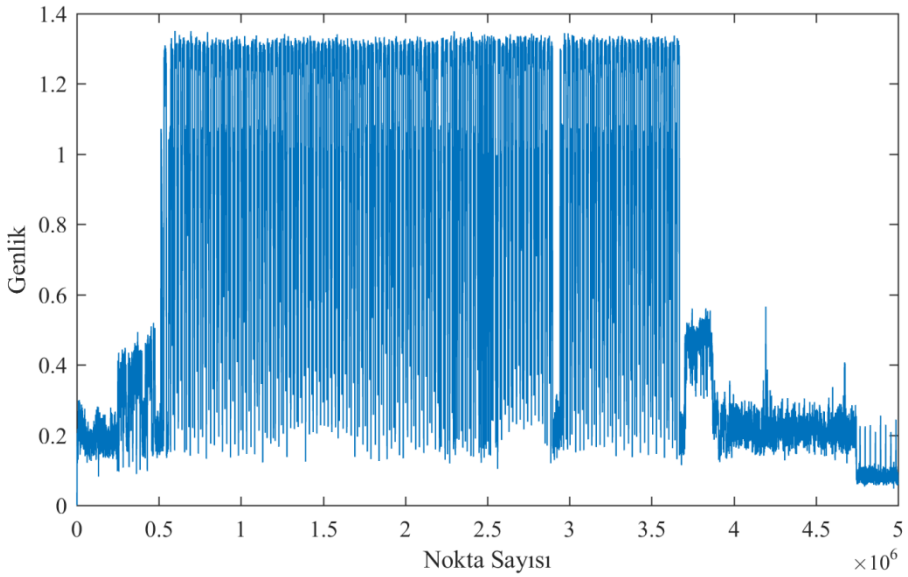
Şekil 6.10 : Doğrultulmuş sinyalin spektrumu (yakın).

Taşıyıcı frekansı bulmak için spektrum görüntüsünde tepe oluşan frekans değerleri için ayrı ayrı bant geçiren filtreler tasarlanmıştır. Daha sonra Şekil 6.9'da spektrumu bulunan ölçüm bu filtrelerden geçirilmiştir. Filtreleme işleminden sonra ölçümler incelenmiştir. İnceleme yapılırken kare alma ve çarpma işlemlerinin birbirinden kolaylıkla ayırt edilebiliyor olmasına dikkat edilmiştir. Şekil 6.9'da 1.129 MHz değerinde bir tepe gözükmektedir. Bu tepeyi filtreleyecek şekilde 1.04 MHz ve 1.21 MHz değerleri bant geçiren filtrede kullanıldığında filtreleme sonucunda elde edilen ölçüm Şekil 6.11'de gösterilmiştir. Bu ölçümden yapılan işlemler ile ilgili bilgi edinilememektedir. Ölçüm Şekil 6.7'den daha dağınık hale gelmiştir.



Şekil 6.11 : Yanlış ikinci bant geçiren filtre sonrası ölçüm.

Bant geçiren filtre MHz frekans seviyesinde bulunan tepeler için tasarlandığında Şekil 6.11'deki gibi ölçümler elde edilmiştir. Bu nedenle DC merkeze en yakın tepelere odaklanıldı. Bu tepelere bakmak için Şekil 6.10 incelenebilir. Şekil 6.10'da gösterilen DC merkeze en yakın tepe değeri 10 kHz civarındadır. Bu tepe değerindeki ölçümleri filtrelemek için bant geçiren filtre, 5 kHz ile 15 kHz değerleri kullanılarak tasarlanmıştır. Tasarlanan filtre, taşıyıcı frekans olan 5 kHz ile 15 kHz arasındaki ölçüm verilerini ölçümün tamamından ayırmaktadır. Ölçüme bu bant geçiren filtrenin uygulanmasından sonra elde edilen ölçüm verisi Şekil 6.12'de verilmiştir. Şekil 6.12 incelendiğinde ölçüm içindeki dağınıklığın azaldığı görülmüştür. Ölçüm daha detaylı incelendiğinde çarpma ve kare alma işlemlerinin birbirinden ayırt edilebildiği görülmüştür. Bu ayırt etme işlemi bir sonraki bölümde detaylandırılmıştır. 5kHz ile 15kHz arasında bulunan DC merkeze en yakın tepe aranan taşıyıcı frekans olarak tespit edilmiştir.

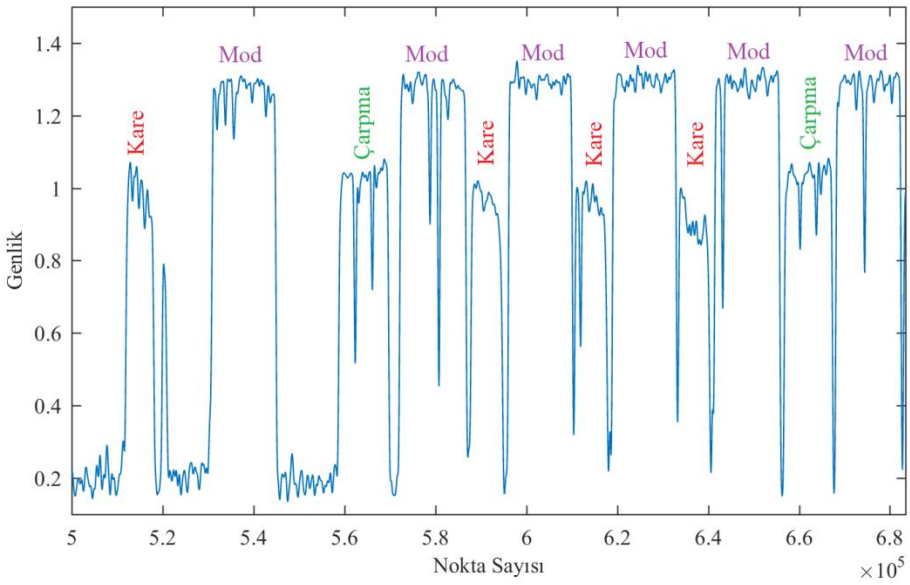


Şekil 6.12 : İdeal ikinci bant geçiren filtre sonrası ölçüm.

Filtreleme işlemleri sonrasında elde edilen ölçüm incelendiğinde RSA işleminin olduğu bölge dışındaki bölgede genlik seviyesi sıfıra yaklaşmış, birçok gürültü kaynaklı verinin ölçümden çıkarıldığı görülmüştür. Şekil 6.4'te yer alan ilk ölçüm incelendiğinde şifrelemenin nerede yapıldığı bile farkedilemezken uygulanan filtreler sonrasında daha anlamlı veri seti elde edilmiştir. Şifreleme işleminin ölçüm verisinin ortasındaki alanda yoğunlaştığı görülmüştür.

6.5 Anahtarın Bulunması

İkinci bant geçiren filtrenin ölçüme uygulanmasının ardından Şekil 6.12'de verilmiş ölçüme yakından bakıldığında her işlemin birbirinden ayırt edilebildiği tespit edilmiştir. Şekil 6.13'de de görüleceği üzere elde edilen ölçümde genliği en yüksek olan işlem mod alma işlemidir. Çarpma işleminin genliği ise kare alma işleminin genliğinden fazladır.



Şekil 6.13 : Ölçümdeki işlemlerin birbirinden ayrılması.

Ölçümdeki tüm tepeleri Şekil 6.13'deki gibi etiketledikten sonra şifreleme anahtarı hakkında tahmin yürütülebilmektedir. Bu ölçümde çarpma ve kare alma algoritması kullanılmıştır. Kare alma işleminden sonra çarpma işlemi gerçekleştiriliyor ise anahtarın ilgili bit değeri '1' olmalıdır. Eğer kare alma işlemini çarpma işlemi takip etmiyor ise ilgili bit değeri '0' olmalıdır. Bu analoji takip edildiğinde Şekil 6.13'de gösterilen anahtarın ilk 4 bitinin değeri '1001' olmaktadır. Ölçümün tamamında bu analoji uygulandığında anahtar değeri 16'lık sistemde 9FFF0000FFFF0000FFFF olmaktadır. Orijinal anahtar bilindiği için uygulanan metodun performansı bulunan anahtar ile bit bit karşılaştırılarak hesaplanabilir. Tahmin edilen anahtar ile doğru anahtarın karşılaştırılmasında XOR işlemi kullanılabilir. XOR işlemi karşılıklı bit değerleri aynı ise sıfır, farklı ise bir değerini döndürmektedir [29]. Böylelikle XOR işlemi sonucunda tüm bitler sıfır ise tüm bitler doğru tahmin edilmiş olmaktadır. Bir değerlerin sayısı toplamı, anahtarın toplam bit sayısına bölündüğünde bit hata oranı bulunmaktadır. Bu ölçümde doğru anahtar ile tahmin edilen anahtarın XOR işlemine

sokulması sonucunda tüm bit değerleri sıfır olduğundan uygulanan metodun bit hata oranı sıfırdır. Prob ile alınan elektromanyetik radyasyon kullanılarak gizli anahtarın tamamı başarılı bir şekilde elde edilmiştir.

6.6 Her Zaman Kare Alma ve Çarpma Algoritması

Daha önceki bölümlerde anlatılan çalışmalar neticesinde çarpma ve kare alma işlemleri sırasında cihazdan yayılan elektromanyetik radyasyonun birbirinden farklı olduğu kanıtlanmıştır. Hızlı üs alma RSA algoritması gerçekleme zamanı açısından eniyileme sağlasa da bit değerine göre farklı işlemlerin gerçekleştirilmesi anahtarın ele geçirilmesine neden olmaktadır. Bu durum güvenlik zafiyetine neden olmaktadır. Bu açığı kapatmak için her turda aynı işlemlerin yapılacağı bir gerçekleme tercih edilmiştir [61].

$e = (e_{k-1}, e_{k-2}, e_{k-3}, ..., e_0)_2$ kullanılan anahtar değeri olmak üzere $d = m^e \bmod n$ işlemi aşağıdaki gibi hesaplanabilir.

```
1: d ← m
2: for i = k − 1 : 0              // soldan sağa doğru
3:       d1 ← d * d mod n         // Kare alma
4:       d2 ← m * d1 mod n        // Çarpma
5:       if ei = 1
6:             d ← d2
7:       else
8:             d ← d1
9:       end if
10: end for
```

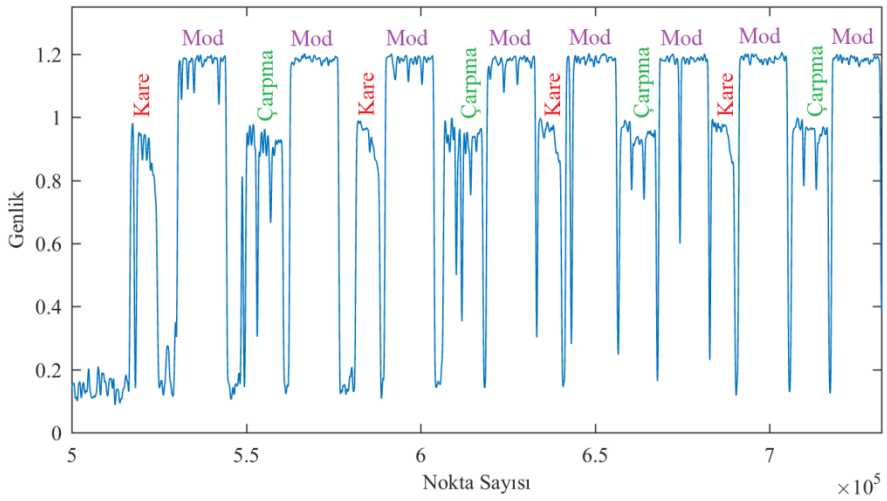
Şekil 6.14 : Her zaman kare alma ve çarpma algoritması.

Bu sayede çarpma ve kare alma işlemleri birbirinden ayırt edilse de anahtarın bit değeri tahmin edilemeyecektir. Bu algoritmada önceki gerçeklemeden farklı olarak anahtarın her turunda (1 ya da 0 olması fark etmeksizin) kare alma ve çarpma işlemleri gerçekleştirilmektedir. Eğer anahtarın biti 0 ise kare alma işleminin sonucu bir dahaki turun giriş değeri olmaktadır. Eğer anahtarın bit değeri 1 ise çarpma işleminin sonucu bir dahaki turun giriş değeri olmaktadır. Yazılımın ilgili kod parçası Şekil 6.14'de verilmiştir.

```
for(i = bits-1; i>=0; i--) {
    mpz_mul(d1, d, d); // Kare alma
    mpz_mod(d1, d1, n);
    mpz_mul(d2, d1, m); // Çarpma
    mpz_mod(d2, d2, n);
    if(mpz_tstbit(e, i) == 1)
        mpz_swap(d, d2); // d'ye d2 değişkeninin değerini ata
    else
        mpz_swap(d, d1); // d'ye d1 değişkeninin değerini ata
}
```

Şekil 6.15 : İkinci algoritmayı gerçekleyen kod parçası.

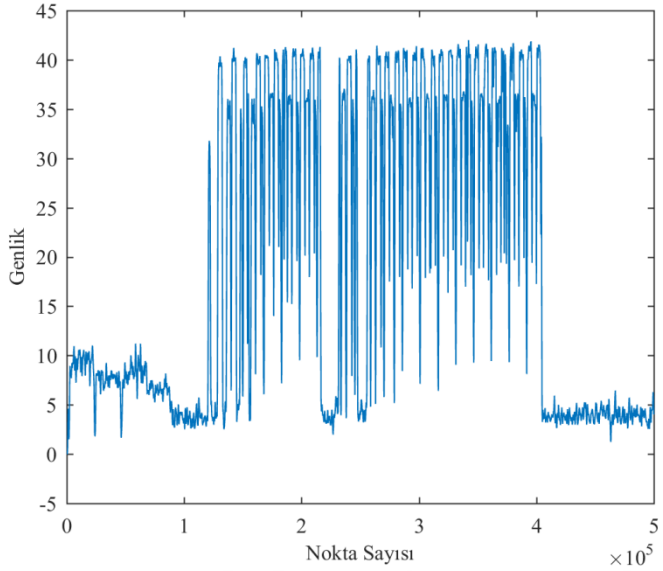
Şekil 6.15'de verilmiş olan kod parçasının ait olduğu yazılım Raspberry Pi için derlendikten sonra ölçüm tekrarlanmıştır. Tekrarlanan ölçüm daha önceki bölümlerde anlatılan işlemlerden geçirilmiştir. Bu işlemler sonrası Şekil 6.13'de incelenen bölgeye ikinci algoritmanın çalışması sonrası tekrar bakılmıştır. Şekil 6.16'da çarpma ve kare alma işleminin her turda yapıldığı gözlemlenmiştir. Tek ölçümle anahtarı tahmin etmek mümkün olmamaktadır.



Şekil 6.16 : SEMA'ya karşı dayanıklı olan RSA ölçümü.

6.7 Farksal Elektromanyetik Analizi Saldırısı

Kare alma ve çarpma algoritması kullanıldığında tek ölçümle şifreleme anahtarı elde edilebilmektedir. Bunun nedeni algoritmadaki yan kanal saldırısı zayıflığıdır. Bölüm 6.6'da anlatılan algoritma gerçeklendiğinde ise yapılan işlemler birbirinden ayırt edilse de bit değerine bağlı farklı işlemler gerçekleştirilmediğinden anahtar ile ilgili bilgi elde edilememiştir. Bu nedenle bu bölümde DEMA saldırısı uygulanarak anahtarla ilgili bilgi elde edinilmeye çalışılmıştır.



Şekil 6.17 : 16 bitlik anahtar kullanılan ölçüm.

DEMA saldırısını gerçekleştirmek için aynı anahtar değeriyle N adet veri ölçüm düzeneğinde anlatıldığı üzere işleme sokulmuştur. Şekil 6.17'de alınan ölçümlerden bir tanesinin filtre uygulanmış hali gösterilmektedir. Filtreleme işlemi için iki farklı bant geçiren filtre kullanılmıştır. Bölüm 6.4'te filtreleme işlemleri için kullanılan filtreler anlatılmıştır.

DEMA saldırılarında atak yapılacak bölgenin belirlenmesi çok önemlidir. Bu tez çalışmasında Şekil 6.14'te verilen RSA algoritmasında kullanılan anahtarın en anlamlı bitine, e_{k-1}, atak yapılacaktır. Gerçeklenen algoritmada iki adet geçici bellek bölgesi kullanılmıştır. Bunlar $d1$ ve $d2$ nesneleridir. Bu geçici bellek bölgelerinin ve d nesnesinin değeri aşağıda belirtildiği gibi değişmektedir (Şekil 6.18).

Adım 1: $d \leftarrow m$

Adım 3: $d_1 \leftarrow d^2 \bmod c = m^2 \bmod c$

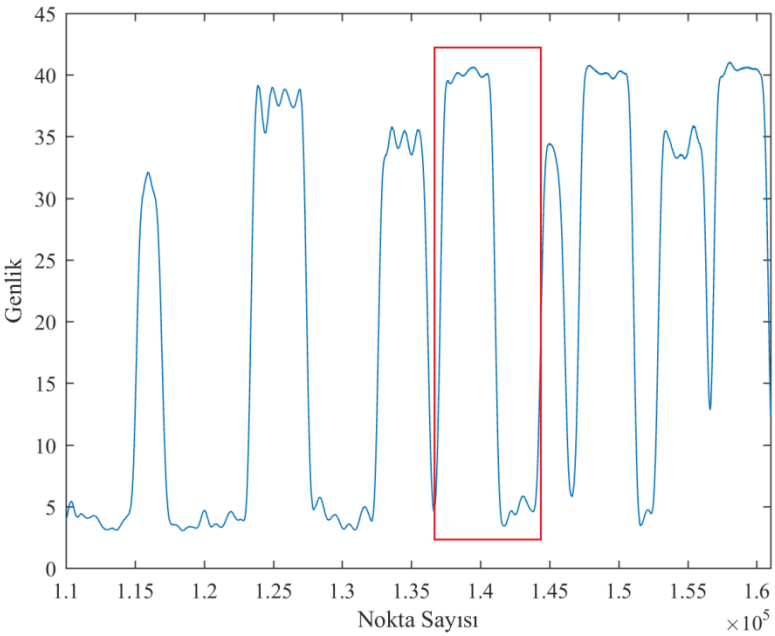
Adım 4: $d_2 \leftarrow d_1 * m \bmod c = m^3 \bmod c$

Adım 5:
$$d \leftarrow \begin{cases} d_1 = m^2 \bmod c & e_{k-1} = 0 \\ d_2 = m^3 \bmod c & e_{k-1} = 1 \end{cases}$$

Adım 5:
$$d \leftarrow \begin{cases} d_1 = m^4 \bmod c & e_{k-1} = 0 \quad e_{k-2} = 0 \\ d_2 = m^5 \bmod c & e_{k-1} = 0 \quad e_{k-2} = 1 \\ d_1 = m^6 \bmod c & e_{k-1} = 1 \quad e_{k-2} = 0 \\ d_2 = m^7 \bmod c & e_{k-1} = 1 \quad e_{k-2} = 1 \end{cases}$$

Şekil 6.18 : Bellek bölgelerinin değer değişimi

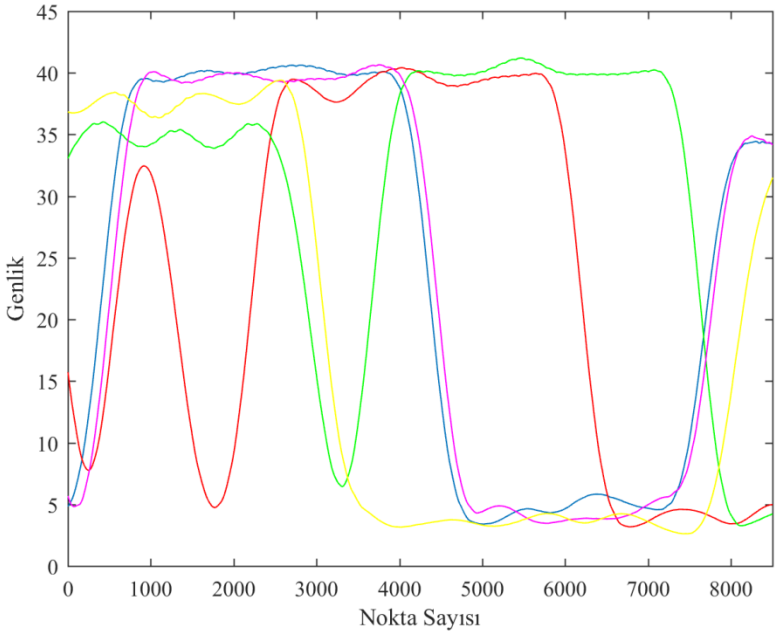
Bellek bölgelerindeki değişimlerin tahmini için ileriki bölümlerde anlatılan modellerden Hamming uzaklığı modeli tahmin matrisi oluşturmak için kullanılmıştır. Alınan elektromanyetik radyasyon ölçümlerinde değişkenin değerinin atandığı bölgeyi elde etmek gerekmektedir. Bölüm 6.6'da anlatılan algoritma uyarınca d nesnesinin değerinin atandığı bölge ilk çarpma işleminden sonra ikinci kare alma işleminden önce olmalıdır. Şekil 6.19'da ilgili bölge işaretlenmiştir.



Şekil 6.19 : Atak yapılan bölgenin belirlenmesi.

Saldırı yapılacak kısmın belirlenmesinden sonra ölçümlerden bu bölgelerin ayrılması gerekmektedir. Eğer uygulamaya özel tasarımları gerçekleyen akıllı kart gibi bir platformda çalışılsaydı kriptografik işlem harici güç tüketimine neden olan bir kaynak olmayacaktı. Sistemden sadece kriptografik işlemin yayınımı alındığında bunları ayırıp analiz etmesi de daha kolay olacaktı.

Tez çalışmasında kullanılan Raspberry Pi platformu kriptografik işlemi gerçekleştirirken araya rastgele başka işlemler de almaktadır. Araya aldığı işlemler üzerindeki işletim sistemi kaynaklıdır. Araya farklı işlemlerin alınması hem gürültüye sebep olmaktadır hem de ölçümde kaymalara yol açmaktadır. Bu nedenle analiz işlemi zorlaşmaktadır. Alınan ölçümlerin aynı noktalardaki görüntüsü çizdirildiğinde hizalı olmadığı görülmektedir (Şekil 6.20). DEMA saldırılarında alınan ölçümlerin hizalı olması gerekmektedir.

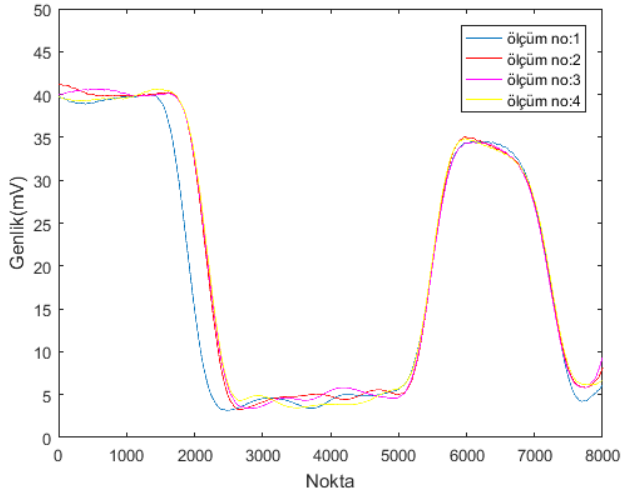


Şekil 6.20 : Ölçümlerin kayması.

Alınan ölçümlerden istenilen bölgeyi ayıklamak için bir odak noktası seçilip ölçümlerin bu odak noktasına göre hizalanması gerekmektedir. Ölçümlerden ilki referans ölçüm olarak kabul edilmiştir. Referans alınan ölçümde ikinci kare alma işlemine ait olan kısım ise kare alma işlemi sırasında yayılan elektromanyetik radyasyonun örneği olarak kabul edilmiştir. İlk ölçümde bu bölge 146000 ile 148500 nolu noktalar arasındadır. Ölçümlerin tamamı incelendiğinde ikinci kare alma işlemlerinin 140000. ile 160000. noktalar arasında, değişik bölgelerde olduğu tespit edilmiştir. Bu nedenle örnek olarak kabul edilen kısım ile bu noktalar arasındaki bölgeler kaydırılarak taranmıştır. MATLAB'ta bulunan *corrcoef* fonksiyonu kullanılarak korelasyon işlemine tabi tutulmuştur. Bu işleme dair MATLAB kodu Şekil 6.21'de verilmiştir. Referans alınan kısım ile korelasyonu en fazla olan bölge aranan bölge kabul edilmiştir. Bu bölgeler başka bir matriste kaydedilmiştir. Ölçümlerin hizalanmış hali Şekil 6.22'de gösterilmektedir.

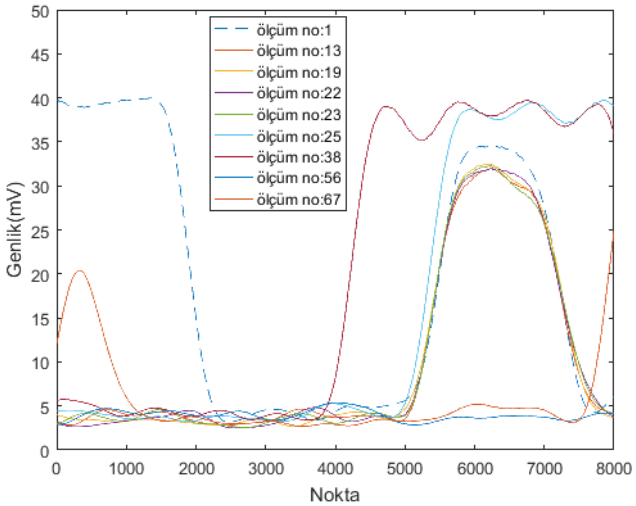
```
for i=140001:160000
      [a b] =  corrcoef([ornek_olcum(1,146001:148500)'
olcum(olcum_no,i+1:i+2500)']);
      correlation(i) = a(2) ;
      [c d] = max(correlation);
end
```

Şekil 6.21 : MATLAB'ta korelasyon işlemi ile ilgili kod parçası.



Şekil 6.22 : Hizalanmış ölçümler.

İlk başta alınan 6300 adet ölçümün çoğunun doğru hizalandığı görülmüştür. İlk 70 ölçüm tek tek ekrana çizdirilerek doğru hizalandırılıp hizalandırılmadığı kontrol edilmiştir. Bu kontroller sonucunda 8 adet yanlış hizalanan ölçüm tespit edilmiştir. Bu ölçümlerin indis numaraları 13, 19, 22, 23, 25, 38, 56 ve 67'dir. Doğru hizalanmış bir ölçüm ile beraber yanlış hizalanan ölçümler Şekil 6.23'de gösterilmektedir. Doğru hizalanmış ölçüm kesik çizgi ile gösterilmiştir.



Şekil 6.23 : Yanlış hizalanmış ölçümlerin hizalı ölçüm ile karşılaştırılması.

Analiz sonucunda 6000 ile 6400 noktaları arasındaki tepe değerinin yanlış ölçümlerde daha düşük olduğu görülmüştür. Her ölçüm için 6000 ile 6500 noktaları arası ortalama değerler elde edilmiştir. Ortalama değeri 32.8'den küçük ve 35.1'den büyük olanların yanlış hizalandığı kabul edilmiştir. Hizalama sonrası yanlış

hizalananlar çıkarıldığında 5741 adet ölçüm kalmıştır. Şekil 6.24'de bulunan güç matrisi, saldırı için hem korelasyon testinde hem de ortalamaya uzaklık testinde kullanılmıştır.

$$M_3 = \begin{bmatrix} t_{1,1} & t_{1,2} & t_{1,3} & \cdots & \cdots & \cdots & \cdots & t_{1,8000} \\ t_{2,1} & t_{2,2} & t_{2,3} & \vdots & \vdots & \vdots & \vdots & \vdots \\ t_{3,1} & t_{3,2} & t_{3,3} & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ t_{N,0} & t_{N,1} & \cdots & \cdots & \cdots & \cdots & \cdots & t_{N,8000} \end{bmatrix}_{Nx8000}$$

Şekil 6.24 : Güç matrisi.

6.7.1 Tahmin matrislerinin oluşturulması

Korelasyon analizi ve ortalamaya uzaklık testlerinin gerçekleştirilebilmesi için elektromanyetik radyasyon ölçümlerinin yanında tahmin matrisleri de gerekmektedir [38]. Tahmin matrisi oluşturulması için kullanılan iki adet yöntem vardır. Bunlardan biri Hamming Ağırlığı diğeri ise Hamming Uzaklığıdır [43].

Hamming Ağırlığı modelinde atak yapılan bellek bölgesine yazılan değişkendeki 1 değerlerinin sayısı toplanır. Her bit değeri için tek sütunu ve ölçüm sayısı kadar satırı olan tahmin matrisleri oluşturulur. İlk bite saldırı yapılacak ise bitin 1 ve 0 değerleri için iki adet tek sütunluk matris oluşturulmalıdır.

Hamming Uzaklığı modelinde ise bellek bölgesinin son değerindeki 1 değerlerinin sayısına bakılmaz. Bellek değeri güncellemesi yapılırken bit değerlerinin 0'dan 1'e ve 1'den 0'a geçişlerin sayısı hesaplanmaktadır. Bu işlem için ilk değer ile son değer xor işlemine tabi tutulur. Bu işlemin sonucu bit geçiş sayısını verir. Çizelge 6.1 'de Hamming Ağırlığı ve Hamming Uzaklığı değerlerini göstermek için 3 adet örnek verilmiştir. Hamming Ağırlığı modelinde olduğu gibi bit değerleri için tek sütun ve ölçüm sayısı kadar satırı olan tahmin matrisleri oluşturulmaktadır.

Çizelge 6.1 : Hamming ağırlığı ve uzaklığı için örnek.

İlk değer (İkilik sistem)	Son değer (İkilik sistem)	Hamming Ağırlığı	Hamming Uzaklığı
10100101	01101010	4	6
10101100	00101000	2	2
01100101	11110101	6	2

Şekil 6.14'te verilmiş her zaman kare alma ve çarpma algoritmasına göre bellek bölgeleri ayrılmış d nesnesine d_1 ya da d_2 nesnesinin değeri her bit işlemi sonucu atanmaktadır. Bu nedenle oluşturulacak tahmin matrisleri ilk turda oluşturulan d_1 ve d_2 nesnelerine bağlı olmaktadır. Tez çalışmasında Hamming Uzaklığı kullanılmıştır. Hamming Uzaklığına göre iki adet tahmin matrisi Şekil 6.25'teki gibi oluşturulmuştur. M_0 matrisi şifreleme anahtarının en anlamlı bit değerinin 0 olması durumunu göstermektedir. Bu matrisi oluşturmak için d nesnesinin değerinin a 'dan d_1'e değiştiği kabul edilmiştir. M_1 matrisi anahtarın en anlamlı bit değerinin 1 olması durumunu göstermektedir. Bu tahmin matrisi için ise d nesnesinin değerinin a'dan d_2'ye değiştiği kabul edilmiştir. Şekil 6.25'te N ölçüm adedini göstermektedir. İlk başta 6300 adet ölçüm alınmasına karşın çıkarılanlardan sonra 5741 ölçüm kalmıştır. Tahmin matrislerinin boyutu da ölçüm sayısıyla beraber düşürülmüştür.

1024 bitlik açık veriler kullanıldığı için tahmin matrislerinin her bir elemanı 0 ile 1024 arasında değişmektedir.

$$M_0 = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ \vdots \\ \vdots \\ p_N \end{bmatrix}_{NX1} \qquad M_1 = \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ \vdots \\ \vdots \\ q_N \end{bmatrix}_{NX1}$$

Şekil 6.25 : Güç tahmin matrisleri.

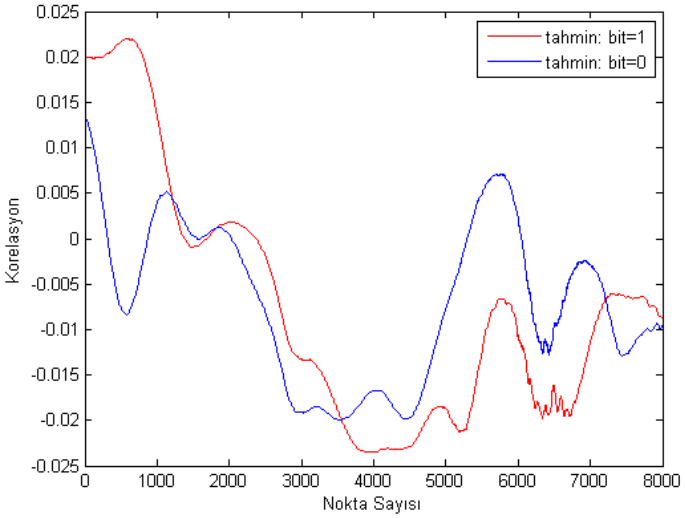
6.7.2 Korelasyon analizi

Korelasyon analizi yönteminde elektromanyetik radyasyon ölçümünün oluşturduğu güç matrisiyle, oluşturulan tahmin matrislerinin korelasyonuna bakılır [34]. Kullanılan anahtarın, b_{k-1}, doğru bit değeri için korelasyon katsayısı değerinin daha yüksek çıkması beklenir.

Hamming Uzaklığına göre güç tahmin matrisleri bir önceki bölümde anlatıldığı gibi bulunduktan sonra güç matrisi ile güç tahmin matrisleri sırasıyla korelasyon işlemine tabi tutulmuştur. İki veri seti arasında yüksek pozitif korelasyon bulunmaya

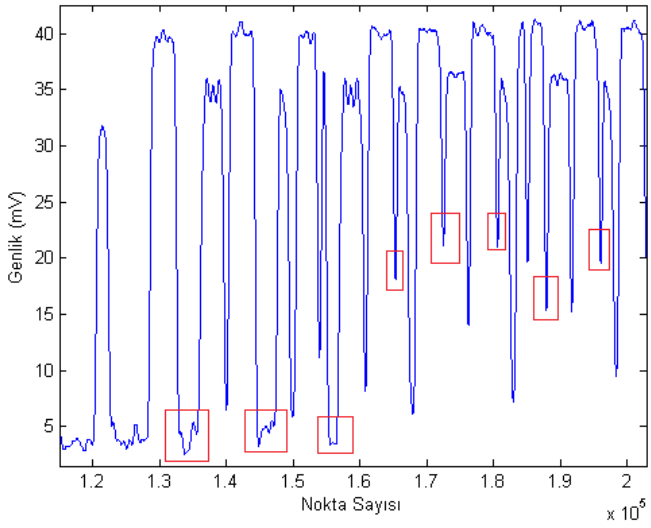
çalışılmıştır. Tez çalışmasında Hamming uzaklığı modeli kullanılarak başarıya ulaşılmıştır.

Hamming uzaklığı için oluşturulan tahmin matrisleri kullanıldığında korelasyon değerleri Şekil 6.26'da gösterildiği gibi olmaktadır. Güç matrisinin (M_3) sütunlarının M_1 matrisi ile korelasyonunu kırmızı çizgi, M_0 matrisiyle korelasyonunu mavi çizgi göstermektedir.



Şekil 6.26 : Korelasyon katsayısı grafiği.

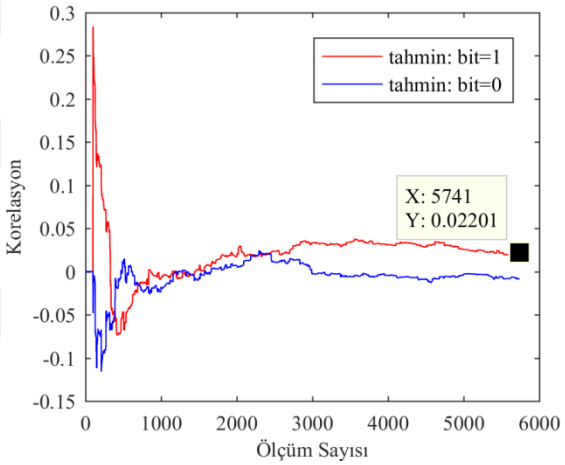
Şekil 6.26 incelendiğinde yüksek pozitif korelasyonun ilk bin noktanın bulunduğu yer olduğu görülmektedir. Bu bölge Şekil 6.22'den de görüleceği üzere mod alma olarak işaretlenen bölgedir.



Şekil 6.27 : Mod işlemleri sonrası farkların gösterimi.

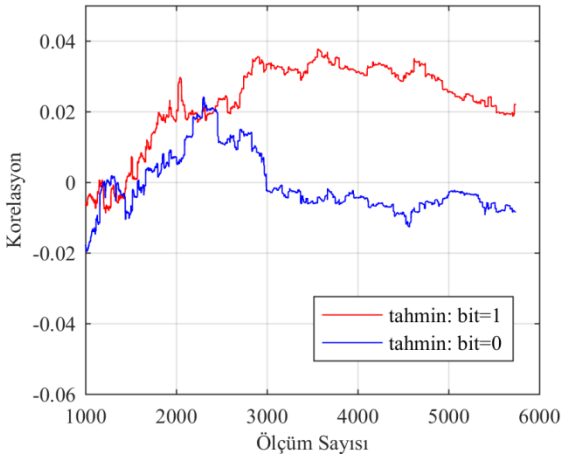
Analize başlamadan önce aranan noktanın birinci çarpma işleminden sonra ikinci kare alma işleminden önce olduğu belirtilmişti. Bu kadar geniş aralık alınmasının sebebi belleğe yazma işleminin ne zaman yapıldığının bilinmemesinden kaynaklanmaktadır. Şekil 6.27'de gösterilen mod alma işlemleri sonrası kırmızı kutucuklar ile işaretlenen boşluklara bakıldığında tur sayısı arttıkça boşlukların azaldığı gözükmektedir. Korelasyon değerinin boşluğun olduğu nokta yerine mod işlemi olarak nitelendirilen bölgede yüksek çıkması bu açıdan da önemlidir.

Şekil 6.26'da bulunan grafikte korelasyon değerinin en yüksek çıktığı nokta 576. noktadır. Bu nokta kullanılarak hesaplanan ölçüm sayısına bağlı korelasyon katsayısı değişimi grafiği Şekil 6.28'e eklenmiştir.



Şekil 6.28 : Ölçüm sayısı ile korelasyon katsayısı değişimi.

Şekil 6.29 incelendiğinde 2500. ölçümden sonra bit değerleri için oluşturulan tahmin matrisleri arasındaki korelasyon katsayısı farkı belirginleşmektedir.

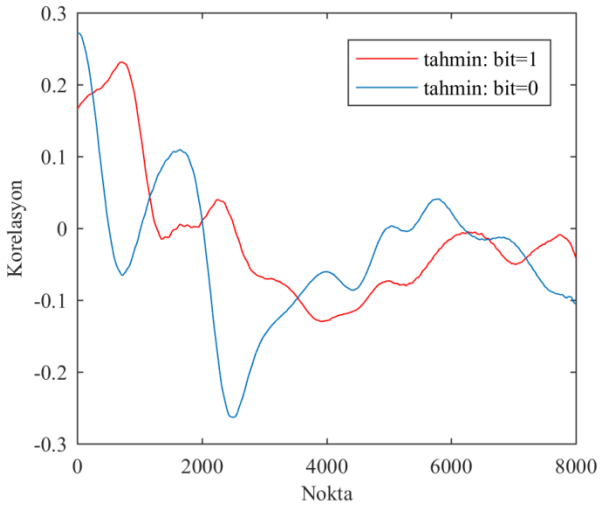


Şekil 6.29 : Ölçüm sayısı ile korelasyon katsayısı değişimi (yakın).

6.7.3 Ortalamaya uzaklık testi

Ortalamaya uzaklık testini gerçekleştirmek için Hamming uzaklığına göre oluşturulmuş tahmin matrisleri kullanılarak güç ölçümleri gruplara ayrılmıştır. Her tahmin matrisi için bir ölçüm verisi elde edilmiştir. Bu ölçüm verisini oluşturmak için izlenen yol aşağıdaki gibidir.

- M_0 tahmin matrisinin ortalama değeri bulunmuştur.
- M_0 matrisi satır değerleri bulunan ortalama değerden küçük ise az güç tüketen, büyük ise çok güç tüketen olarak kabul edilmiştir.
- Güç matrisinde bulunan ölçümlerden az güç tüketenler kendi aralarında toplanmıştır. Daha sonra az güç tüketen ölçüm sayısına bölünerek az güç tüketen ölçümler için bir matris elde edilmiştir.
- Güç matrisinde bulunan ölçümlerden çok güç tüketenler kendi aralarında toplanmıştır. Daha sonra çok güç tüketen ölçüm sayısına bölünerek çok güç tüketen ölçümler için bir matris elde edilmiştir.
- Çok güç tüketen ölçüm matrisi ile az güç tüketen ölçüm matrisi birbirinden çıkarılmıştır. M_0 tahmin matrisi için bir ölçüm elde edilmiştir.
- Bu işlemlerin tamamı M_1 matrisi için de yapılmıştır.
- Doğru bit değerine göre yapılan sınıflandırma sonucunda tepe değeri oluşması beklenmiştir (Şekil 6.30).



Şekil 6.30 : Ortalamaya uzaklık testi.

7. SONUÇ VE ÖNERİLER

Bilgi güvenliğinin önemi gün geçtikçe artmaktadır. Gömülü sistemlerde bilgi güvenliğini sağlayan temel unsurlar, gerçeklenen kriptografik algoritmanın güvenliği ve gömülü sistemin yan kanal bilgisi sızdırmamasıdır. Bu nedenle kriptografik işlemler için çoğunlukla özel olarak tasarlanmış mikroişlemciler kullanılmaktaydı.

Nesnelerin interneti ile gömülü sistem olarak hazır devrelerin kullanımı artmıştır. Raspberry Pi platformu, üzerinde işletim sistemi olmasından dolayı birçok geliştirici tarafından tercih edilmektedir. 2017 yılında yapılan gömülü sistemlerle ilgili market çalışmasında Raspberry Pi kullanan kişilerin oranı %16 iken kullanmayı planlayanların oranı %23 gözükmektedir [62]. Hazır devrelerin popülerliği hızla artmasına rağmen bu devrelerin güvenliği arkaplanda kalmaktadır.

Tez çalışması kapsamında Raspberry Pi üzerinde RSA gerçeklemesinin anahtarının ele geçirilmesi amaçlanmıştır. Bu çalışma, Raspberry Pi platformu üzerinde Raspbian işletim sistemi koşması nedeniyle literatürdeki yan kanal analizi çalışmalarının büyük çoğunluğundan ayrılmaktadır. İşletim sistemi aktivitelerinin rastsallığı ve oluşturdukları gürültü nedeniyle analiz zorlaşmıştır. Devrede atağa dair iz bırakmamak için elektromanyetik radyasyon tercih edilmiştir. Elektromanyetik radyasyonu almak için ise Riscure firmasının ölçüm istasyonu kullanılmıştır. Ölçüm düzeneği ile ilgili çalışmalar Bölüm 5'te bulunmaktadır.

Tez çalışmasında iki farklı RSA algoritması kullanılmıştır. İki gerçekleme için de alınan ölçümler filtreleme işlemlerine tabi tutulmuştur. Filtrelerin kullanılma nedeni kriptografik işlemler harici işletim sistemi vb. kaynaklı gürültülerin bastırılmasıdır. İlk RSA algoritması gerçeklemesinde basit elektromanyetik analiz saldırısıyla tek ölçümde başarılı sonuç elde edilmiştir. Daha sonra SEMA saldırısına karşı önlem olarak her zaman kare alma ve çarpma algoritması gerçeklenmiştir. Bu gerçeklemede SEMA saldırısıyla anahtarın ele geçirilemediği görülmüştür. Her zaman kare alma ve çarpma algoritmasında anahtarı ele geçirmek amacıyla DEMA saldırısı uygulanmasına karar verilmiştir. DEMA saldırısı için ilk önce ölçümler hizalanarak güç matrisi oluşturulmuştur. Daha sonra olası bit değerleri için güç tahmin matrisleri

elde edilmiştir. Analizler için iki farklı yöntem kullanılmıştır. Bunlardan biri korelasyon analizi diğeri ise ortalamaya uzaklık testi yöntemidir. Korelasyon analizi için güç matrisleri ile güç tahmin matrislerinin korelasyonu incelenmiştir. İki veri seti arasında yüksek pozitif korelasyon aranmıştır. İncelemeler sonucunda doğru bit değeri için tepe değeri oluştuğu görülmüştür. Ortalamaya uzaklık testi için ise güç tahmin matrisleri az güç tüketen ve çok güç tüketen olmak üzere ikiye ayrılmıştır. Çok güç tüketen ölçümlerin ortalaması az güç tüketen ölçümlerin ortalamasından çıkarılarak her tahmin matrisi için bir ölçüm elde edilmiştir. Ölçümler çizdirildiğinde korelasyon analizi yöntemi kullanıldığında oluşan tepenin bulunduğu bölgede doğru anahtar için tepe oluştuğu görülmüştür. Analizler ile ilgili detaylı çalışmalar Bölüm 6'da görülebilmektedir.

Literatürde bulunan RSA şifreleme algoritmasının gerçeklemelerine yapılan yan kanal saldırıları incelenmiş ve bu çalışmalar zamanlama analizi [4, 63, 64], hata analizi [9, 10, 65, 66], akustik analizi [50], şablon (template) atak [67], fotonik yan kanal analizi [68], ön belleğe dayalı (cache-based) yan kanal analizi [69, 70], taramaya dayalı (scan based) yan kanal analizi [71], seçilmiş mesaj (chosen message) atağı [72, 73], güç analizi [5, 74], elektromanyetik analizi [11, 35] başlıkları altında değerlendirilmiştir. Güç analizi ve elektromanyetik analizi başlığı dışındaki çalışmalar bu tez çalışmasıyla ilgisizdir.

Güç analizi çalışmaları ise ölçüm alınma yönünden farklılık gösterse de ölçümlerin analiz edilmesi yönünden bu tez ile benzerlik taşımaktadır. Elektromanyetik analizinde alınan ölçümler ek ön işleme tekniklerine ihtiyaç duyabilmektedir. Bu nedenle elektromanyetik radyasyon güce göre literatürde daha az yer bulmaktadır. Güç analizi ve elektromanyetik analiz çalışmaları kendi içlerinde basit ya da farksal yan kanal analizi gerçekleştirilmesine göre sınıflandırılmıştır. Bu tez çalışmasında SEMA ve DEMA atakları gerçekleştirildiğinden tez çalışması sadece basit yan kanal analizi gerçekleştirilen çalışmalardan [75-79] daha iyi ve kapsamlıdır. RSA algoritması gerçeklemesine DEMA saldırısı literatürde fazla bulunmamaktadır. Bu nedenle farksal güç analizi çalışmalarıyla da değerlendirme yapılmıştır. RSA algoritması gerçeklemelerine yapılan ilk farksal güç analizi atağı akıllı kart kullanılarak gerçekleştirilmiştir [80]. Gerçekleştirilen DPA atakları [61, 80, 81] incelendiğinde korelasyon analizi işleminden önce ölçümlerin ön işleme tabi tutulduğu görülmüştür. Ön işleme faaliyetleri olarak filtreleme, demodülasyon ve

hizalamayı gösterebiliriz. Bu tez çalışmasında bahsedilen ön işleme faaliyetlerinin tamamı uygulanmıştır. Bu sayede başarılı sonuç elde edilebilmiştir. Bu işlemlerden herhangi biri yapılmamış olsaydı başarılı sonuç elde edilemezdi.

Raspberry Pi platformu üzerinde gerçeklenen yan kanal analizleri incelenmiştir. Yan kanal analizi çalışmalarından zamanlama yan kanal analizi [82], önbellek yan kanal analizi [83, 84], hata enjeksiyonu (fault injection) yan kanal analizi [85] tez çalışmasının alanından farklı olduğu için bu çalışmanın kapsamına girmemektedir. Raspberry Pi üzerinde gerçeklenen diğer üç çalışma ise simetrik şifreleme algoritması olan gelişmiş şifreleme algoritmasına (AES) karşı yapılmıştır [22, 86, 87]. Bu tez çalışmasında ise RSA şifreleme algoritmasının gerçeklemelerine yan kanal analizi türlerinden elektromanyetik analizi saldırısı düzenlenmiştir.

Raspberry Pi platformu üzerinde gerçeklenen yan kanal analizleri içerisinden RSA algoritması gerçeklemelerine yan kanal analizi yapılan bir çalışma mevcuttur [88]. Bu çalışmada hangi yan kanal analizi türü kullanıldığı belirtilmemiştir. SASEBO devre kartıyla Raspberry Pi üzerinde aynı uygulamalar koşturularak yan kanal saldırılarına karşı güvenliği test edilmiştir. SASEBO devre kartı üzerinde kullanılan RSA algoritması gerçeklemelerine bağlı olarak açıklık görünmekteyken Raspberry Pi üzerinde açıklık fark edilememiştir [88]. Gürültüyü azaltma özelliği üzerinde durulmuştur. Raspberry Pi platformunun yan kanal analizine karşı güvenli olmadığını kanıtlaması açısından gerçekleştirilen bu tez kanıt niteliğindedir. Kullanılan filtreleme tekniği ile daha etkin, doğru ve başarılı sonuç elde edilmiştir.

Yapılan bu tez çalışması ile Raspberry Pi platformunun yan kanal analizi saldırılarına karşı önlemi olmadığı görülmektedir. Açık kaynak kodlu kripto kütüphaneleri ve ücretli kripto kütüphaneleri kullanılan gerçeklemeler için yan kanal analizi konusu ayrıca incelenmelidir.

KAYNAKLAR

[1] **Sarı, O.** (2013). *Uluslararası hukuk ve türk ceza hukuku bağlamında siber güvenlik ve bilişim sistemine yönelik suçlar.* (Yüksek lisans tezi). Harp Akademileri Stratejik Araştırmalar Enstitüsü, İstanbul.

[2] **Ercan, M.** (2015). *Kritik altyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri.* (Yüksek lisans tezi). Gebze Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli.

[3] **Türk, S.** (2017). *Yapay sinir ağları kullanılarak şifreleme yöntemlerinin performans analizlerinin gerçekleştirilmesi*. (Yüksek lisans tezi). İstanbul Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

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

[5] **Kocher, P., Jaffe, J. & Jun, B.** (1999). Differential power analysis, *Advances in Cryptography: CRYPTO'99, 1666,* 388-397.

[6] **Kayış, H.** (2006). *AES uygulamasının FPGA gerçeklemelerine karşı güç analizi saldırısı*. (Yüksek lisans tezi). İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[7] **Anderson, R. & Kuhn, M.** (1996) Tamper resistance – a cautionary note. *Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce,* (pp.1–1). Oakland, California, USA, November 18-21.

[8] **Kommerling, O. & Kuhn, M. G.** (1999). Design principles for tamper-resistant smartcard processors, *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, (pp.2-2), May 10-11, Chicago, Illinois.

[9] **Joye, M. & Lenstra, A. K.** (1999). Chinese remaindering based cryptosystem in the presence of faults, *Journal of Cryptology*, (Vol. 12, No. 4, pp.241-245).

[10] **Boneh, D., DeMillo, R. A. & Lipton, R. J.** (1997). On the importance of checking cryptographic protocols for faults (extended abstract). In W.Fumy, (Ed.), *Advances in Cryptology: EUROCRYPT'97,* (Vol. 1233, pp.37–51). Springer-Verlag.

[11] **Quisquater, J. & Samyde, D.** (2001). Electromagnetic analysis (EMA): measures and countermeasures for smart cards, *Smart Card Programming and Security, Lectuıre Notes in Computer Science,* 2140, 200-210.

[12] **Gandolfi, K., Mourtel, C. & Olivier, F.** (2001). Electromagnetic analysis: concrete results, *Proceedings of CHES. LNCS, 2162*, 251-261.

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

[14] **Akdur, D., Garausi V. ve Demirörs O**., (n.d.). *Gömülü sistem mühendisliğinde kullanılan yazılım modellemesi ve model güdümlü teknikler anketi Türkiye sonuçları*, Erişim: 5, 2017, Erişim adresi https://www.researchgate.net/profile/Vahid_Garousi2/publication/317370911_Gomulu_Sistem_Muhendisliginde_Kullanilan_Yazilim_Modellemesi_ve_Model_Gudumlu_Teknikler_Anketi_Turkiye_Sonuclari/links/593e657caca272e79e5b4f6e/Goemuelue-Sistem-Muehendisliginde-Kullanilan-Yazilim-Modellemesi-ve-Model-Gueduemlue-Teknikler-Anketi-Tuerkiye-Sonuclari.pdf

[15] **Url-1** <*https://opensource.com/resources/raspberry-pi*>, erişim tarihi 12.11.2017.

[16] **Rivest, R. L., Shamir, A. & Adleman, L.** (1978). A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM, 21* (2), 120-126.

[17] **Boyacı, U. K. ve Kara, O.** (2009). Bilgi Güvenliği Problemlerine Matematiksel Yaklaşım Getiren Bir Bilim Dalı: Kriptoloji. *Bilim ve Teknik Dergisi, 500*, 42-47.

[18] **Buluş, H. N.** (2006). *Temel şifreleme algoritmaları ve kriptanalizlerinin incelenmesi.* (Yüksek Lisans Tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

[19] **Yıldırım, K.** (2006). *Veri şifrelemesinde simetrik ve asimetrik anahtarlama algoritmalarının uygulanması (Hybrid şifreleme).* (Yüksek lisans tezi). Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli.

[20] **Çıkıkçı, Ş.** (2010). *Asimetrik şifreli sistemlerin uygulamaları.* (Yüksek lisans tezi). Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne.

[21] **Günden, Ü.** (2010). *Şifreleme algoritmalarının performans analizi.* (Yüksek lisans tezi). Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya.

[22] **Büyükkaya E.** (2017). *Raspberry Pi üzerinde AES algoritmasına yan kanal analizi ve ölçüm iyileştirme.* (Yüksek lisans tezi). İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

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

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

[25] **Özyılmaz, Ç.** (2014). *Kriptolojiye giriş*. (Yüksek lisans tezi). Karabük Üniversitesi, Fen Bilimleri Enstitüsü, Karabük.

[26] **Aksuoğlu, A.,** (2010). *RSA algoritmasının iyileştirilmesi için yeni bir yaklaşım*. (Yüksek lisans tezi). Anadolu Üniversitesi, Fen Bilimleri Enstitüsü, Eskişehir.

[27] **Url-2** <*http://anibal.gyte.edu.tr/hebe/AblDrive/59669005/w/Storage/104_20*

11_1_470_59669005/Downloads/bl470-b1-4.pdf>, erişim tarihi 05.11.2017.

[28] **Yerlikaya, T., Gençoğlu, H., Emir, M. K., Çankaya, M. ve Buluş, E.** (2013). RSA şifreleme algoritması ve aritmetik modül uygulaması. *İstanbul Aydın Üniversitesi Dergisi, 3* (9), 95-104.

[29] **Do, A., Ko, S. T. & Htet, A. T.** (2013). *Electromagnetic side-channel analysis on Intel Atom processor.* (A major qualifying project report). Worcester Polytechnic Institute, USA.

[30] **Okumuş, İ.** (2012). *RSA kriptosisteminin hızını etkileyen faktörler.* (Doktora tezi). Atatürk Üniversitesi, Fen Bilimleri Enstitüsü, Erzurum.

[31] **Url-3** *<http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/millerrabin.pdf>*, erişim tarihi 11.11.2017.

[32] **Cleinberg, B.** (2010). The miller-rabin randomized primality test, *Cornel University, Lecture Notes 5, Introduction to Algorith*ms *(CS 482).*

[33] **Cosade** (2012). Third International Workshop on Constructive Side Channel Analysis and Secure Design, May 03-04 2012, Darmstatd, Germany, Retrieved from http://cosade.cased.de/files/COSADE2012_CFP.pdf

[34] **Şahinoğlu, M.** (2009). *Gelişmiş şifreleme standardı algoritmasının donanım üzerinde gerçeklenmesine elektromanyetik alan saldırısı*. (Yüksek lisans tezi). İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[35] **Agrawal, D., Archambeault, B., Rao, J. R. & Rohatgi, P.** (2003). The EM side-channel(s). In Kaliski B.S., Koç .K., Paar C. (Ed.) *Cryptographic Hardware and Embedded Systems CHES 2002. Lecture Notes in Computer Science*, (Vol. 2523) Springer, Berlin, Heidelberg

[36] **Clarke, G. M. & Cooke, D.** (1998). *A Basic Course in Statistics*, Arnold London, 4th edition.

[37] **Kula, G. Ç.** (2009). *Gelişmiş şifreleme standardı blok şifreleme algoritmasının bir mikroişlemci üzerinde gerçeklemesine yan kanal saldırısı*. (Yüksek lisans tezi). İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[38] **Yalçın, S. B. Ö.** (2005). *Hardware design of elliptic curve cryptosystems and side-channel attacks.* (Doctoral dissertation). Katholieke Universiteit Leuven

[39] **Evci, M. A.** (2014). *Farksal güç analizi saldırılarına dayanıklı döngüsel simetrik S-kutularının tasarımı.* (Yüksek lisans tezi). Gebze Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Kocaeli.

[40] **Janke, M. & Laackmann, P.** (n.d). Power and timing analysis attacks against security controllers. Infenion Technologies AG, Technology Update, Smart Cards.

[41] **Kang, S. M. & Leblebici Y.** (2002). *CMOS Digital Integrated Circuits: Analysis and Design.* McGraw Hill.

[42] **Ordu, L.** (2006). *AES algoritmasının FPGA üzerinde gerçeklenmesi ve yan kanal analizi saldırılarına karşı güçlendirilmesi*. (Yüksek lisans tezi). İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[43] **Öztemür, M.** (2012). *AES algoritmasının bir gerçeklemesine güç analizi saldırıları*. (Yüksek lisans tezi). Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul.

[44] **Sevim, A., Altıner, H., Ünek, O. S., ve Şam, M.** (n.d). Kurumsal yapılarda bilişim güvenliği, TEMPEST problemi, erişim adresi http://ab.org.tr/ab13/bildiri/129.pdf

[45] **Altıner, H. ve Şaykol, E.** (2013). Veri güvenliğinde tempest saldırı türleri üzerine tarihsel bir inceleme. *Beykent Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 6* (2), 121-152

[46] **Chari, S., Rao, J.R. & Rotagi, P.** (2003). Advances in side-channel analysis, *RSA Laboratories Cryptobytes*, (Vol. 6, pp.20-32).

[47] **Chari, S., Rao, J.R. & Rotagi, P.** (2002). Template attacks, *Proceedings of 4th International Workshop on CHES-2002, 2523*, 13-28.

[48] **Thanh, H. L., Clediere, J., Serviere, C. & Lacoume, J. L.** (2007). Noise reduction in side channel attack using fourth-order cumulant. *IEEE Transactions on Information Forensics and Security, 2* (4), 710-720.

[49] **Thanh, H. L., Clediere, J., Serviere, C., & Lacoume, J. L.** (2005). Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing, Retrieved from https://eprint.iacr.org/2005/388.pdf

[50] **Genkin, D., Shamir, A. & Tromer, E.** (2014). RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. In Garay J.A., Gennaro R. (Ed.) *Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, 8616*, 444-461

[51] **Url-4** <*https://www.riscure.com/uploads/2017/07/datasheet_emprobestation.pdf*>, erişim tarihi 11.11.2017

[52] **Url-5** <*https://www.debian.org/index.tr.html*>, erişim tarihi 11.11.2017

[53] **Url-6** <*https://www.raspberrypi.org/documentation/raspbian/*>, erişim tarihi 11.11.2017

[54] **Url-7** <*http://www.teksun.in/wp-content/uploads/2015/04/teksun-raspberry_Pi.jpg*>, erişim tarihi 11.11.2017

[55] **Url-8** <*https://www.raspberrypi-spy.co.uk/2012/06/simple-guide-to-the-rpi-gpio-header-and-pins/*>, erişim tarihi 11.11.2017.

[56] **Url-9** <*https://developer.arm.com/products/processors/classic-processors*>, erişim tarihi 11.11.2017.

[57] **Url-10** <*https://www.raspberrypi.org/documentation/hardware/raspberrypi/bcm2835/README.md.*>, erişim tarihi 11.11.2017.

[58] **Url-11** <*https://www.tek.com/oscilloscope/dpo7000-digital-phosphor-oscilloscope*>, erişim tarihi: 11.11.2017.

[59] **Url-12** <*https://gmplib.org/*>, erişim tarihi 11.11.2017

[60] **Oswald, D. & Paar, C.** (2011). Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In Preneel B., Takagi T. (Ed.) *Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, 6917*, 207-222

[61] **Witteman, M.F., van Woudenberg, J. G. J. & Menarini, F.** (2011). Defeating RSA multiply-always and message blinding countermeasures. In Kiayias A. (Ed.) *Topics in Cryptology – CT-RSA 2011. CT-RSA 2011. Lecture Notes in Computer Science, 6558*

[62] **Url-13** <*https://m.eet.com/media/1246048/2017-embedded-market-study.pdf*>, erişim tarihi 11.11.2017

[63] **English, E. & Hamilton, S.** (1996). Network security under siege: the timing attack. *IEEE Computer, 29*, 95-97.

[64] **Shindler, W.** (2000) A timing attack against RSA with the chinese remainder theorem. In Koç Ç.K., Paar C. (Ed.) *Cryptographic Hardware and Embedded Systems – CHES 2000. CHES 2000. Lecture Notes in Computer Science, 1965*

[65] **Bell Communications research.** (1996). New threat model breaks crypto codes, *Bellcore press release*, Morristown, Sept.1996.

[66] **Shamir, A.** (1999). Method and apparatus for protecting public key schemes from timing and fault attacks, *US patent 5991415*, Nov. 1999.

[67] **Xu, S., Lu, X., Zhang, K., Li, Y., Wang, L., Wang, W., Gu, H., Guo, Z., Liu, J., Gu, D.** (2018). Similar operation template attack on RSA-CRT as a case study, *Science China Information Sciences 61: 032111*. Retrieved from https://doi.org/10.1007/s11432-017-9210-3

[68] **Elad, C., Jean-Pierre, S. & Avishai, W**. (2017). Photonic side channel attacks against RSA, *2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*

[69] **Percival, C.** (2005). Cache Missing for Fun and Profit.

[70] **Acıiçmez, O. & Schindler, W.** (2008). A vulnerability in RSA implementations due to instruction cache analysis and its demonstration on OpenSSL. In Malkin T. (Ed.) *Topics in Cryptology – CT-RSA 2008. Lecture Notes in Computer Science, 4964*

[71] **Nara, R., Satoh, K., Yanagisawa, M. & Togawa N.** (2010). Scan-based side channel attack against RSA cryptosystems using scan signatures, *IEICE Trans. Fundam. Electron., Commun. Comput. Sci., E93-A* (12), 2481-2489

[72] **Bleichenbacher, D.** (1998). Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In Krawczyk H. (Ed.) *Advances in Cryptology — CRYPTO '98. CRYPTO 1998. Lecture Notes in Computer Science, 1462*

[73] **Manger, J.** (2001). A chosen ciphertext attack on RSA optimal asymmetric encryption padding (OAEP) as standardized in PKCS #1 v2.0. In Kilian J. (Ed.) *Advances in Cryptology — CRYPTO 2001. CRYPTO 2001. Lecture Notes in Computer Science, 2139*

[74] **Thomas S. Messerges** (2000). Power analysis attack countermeasures and their weaknesses, *Security Technology Research Laboratory.*

[75] **Jia, F. & Xie, D.** (2016). A unified method based on SPA and timing attacks on the improved RSA. *In China Communications, 13* (4), 89-96.

[76] **Liangjian, S., Wei, G. & Zheng, G.** (2015). Combined attack on blinded fault resistant exponentiation algorithm and efficient countermeasure. *2015 11th International Conference on Computational Intelligence and Security* doi: 10.1109/CIS.2015.87

[77] **Yuanyuan, Z. & Shize, G.** (2011). SPA-based security evaluation of RSA implementation in internet banking USB token. *2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control* doi: 10.1109/IMCCC.2011.130

[78] **Masami, I., Kazuo, S. & Kazuo, O.** (2009). A New Approach for Implementing the MPL Method toward Higher SPA Resistance. *2009 International Conference on Availability, Reliability and Security* doi: 10.1109/ARES.2009.61

[79] **Novak, R.** (2002). SPA-based adaptive chosen-ciphertext attack on RSA implementation. In Naccache D., Paillier P. (Ed.) *Public Key Cryptography. PKC 2002. Lecture Notes in Computer Science, 2274*

[80] **Messerges, T. S., Dabbish, E. A. & Sloan R. H.** (1999). Power analysis attacks of modular exponentiation in smartcards. In Koç Ç.K., Paar C. (Ed.) *Cryptographic Hardware and Embedded Systems. CHES 1999. Lecture Notes in Computer Science, 1717.*

[81] **Mahanta, H. J., Azad, A. K. & Khan A. K.** (2015). Power analysis attack: A vulnerability card security. *Signal Processing And Communication Engineering Systems (SPACES), 2015 International Conference,* doi: 10.1109/SPACES.2015.7058206

[82] **Isa, M. A. M., Hashim, H., Adnan S. F. S., Marbukhari N. & Mohamed N. N.** (2017). An Automobile Security Protocol: Side-channel Security against Timing and Relay Attacks, *International Journal of Electronic Security and Digital Forensics.* doi: 10.1504/IJESDF.2017.10005632

[83] **Url-14** *<https://developer.arm.com/support/security-update/download-the-whitepaper>*, erişim tarihi 05.03.2018

[84] **Marco, C.** (2016). *Real time detection of cache-based side-channel attacks using hardware performance counters.* (Yüksek lisans tezi). Sabancı Üniversitesi, Bilgisayar Bilimi ve Mühendisliği, İstanbul

[85] **Colin, O.,** (2017). *A framework for embedded hardware securıty analysis,* (Doctoral dissertation). Retrieved from https://dalspace.library.dal.ca/bitstream/handle/10222/73002/OFlynn-Colin-PhD-ECED-June-2017.pdf?sequence=1&isAllowed=y

[86] **Ibraheem, F. & Barry, I.** (2017). Investigating the effects various compilers have on the electromagnetic signature of a cryptographic executable, *SAICSIT* doi: 10.1145/3129416.3129436

[87] **Ibraheem, F. & Barry, I.** (2017). Recovering AES-128 Encryption Keys from a Raspberry Pi, *Southern Africa Telecommunication Networks and Applications*

[88] **Akihiro S., Yasuyuki N. & Kengo I**. (2017). Security Analysis of Raspberry Pi Against Side-Channel Attack with RSA Cryptography, *2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*

ÖZGEÇMİŞ

Ad-Soyad **:** Ersin HATUN

Doğum Tarihi ve Yeri **:** 28.10.1990 - Üsküdar

E-posta **:** ersinhatun@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** **:** Fatih Üniversitesi, Elektrik-Elektronik Mühendisliği, 2012

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR:

- **Hatun, E., Büyükkaya, E., Yalçın, S. B. Ö.** (2018). RSA algoritmasının Raspberry Pi üzerinde gerçeklemesine elektromanyetik yayınım analizi, *26. Sinyal İşleme ve İletişim Uygulamaları (SIU) Kurultayı*, 2-5 Mayıs 2018, İzmir