RSA Algoritmasının Raspberry Pi Üzerinde Gerçeklemesine Elektromanyetik Yayınım Analizi
Electromagnetic Radiation Analysis of Implementation of RSA Algorithm on a Raspberry Pi

Ersin Hatun
Elektronik Mühendisliği
İstanbul Teknik Üniversitesi
İstanbul, Türkiye
hatun@itu.edu.tr

Elif Büyükkaya
Bilgi Güvenliği Mühendisliği
İstanbul Şehir Üniversitesi
İstanbul, Türkiye
elifbuyukkaya@std.sehir.edu.tr

Sıddıka Berna Örs Yalçın
Elektronik Mühendisliği
İstanbul Teknik Üniversitesi
İstanbul, Türkiye
siddika.ors@itu.edu.tr

***Özetçe*—Bu bildiride RSA algoritmasının Raspberry Pi platformu üzerinde gerçeklemesinin elektromanyetik yayınım analizine karşı güvenliği değerlendirilmiştir. Raspberry Pi üzerinde iki farklı RSA algoritması gerçeklenmiştir. Bu algoritmalar üzerinde Basit Elektromanyetik Analizi ve Farksal Elektromanyetik Analizi saldırıları gerçekleştirilmiştir. Basit Elektromanyetik Analizi saldırısıyla önlem alınmamış bir gerçeklemede anahtarın tüm bitleri tek ölçüm ile elde edilmiştir. Ayrıca Basit Elektromanyetik Analize karşı dayanıklı bir gerçeklemeye Farksal Elektromanyetik Analizi saldırısı gerçeklenerek korelasyon analiziyle 2500 ölçüm ile anahtarın bir bit değeri elde edilmiştir.**

Anahtar Kelimeler — Raspberry Pi; RSA; Basit Elektromanyetik Analizi; Farksal Elektromanyetik Analizi.

***Abstract*—In this paper, security analysis of RSA implementation on a Raspberry Pi against electromagnetic radiation analysis is evaluated. Two different RSA algorithm is implemented on Raspberry Pi. Simple Electromagnetic Analysis and Differential Electromagnetic Analysis attacks are performed. Using Simple Electromagnetic Analysis attack on an unprotected implementation, all key bits are found with one measurement. Also, Differential Electromagnetic Analysis attack is performed against an improved implemantation that has countermeasure against Simple Electromagnetic Analysis attack. One key bit is found using 2500 measurements with a correlation analysis in Differential Electromagnetic Analysis attack.**

Keywords — Raspberry Pi; RSA; Simple Electromagnetic Analysis; Differential Electromagnetic Analysis.

I. GİRİŞ

Gömülü sistemler günümüzde her cihazın vazgeçilmez bir parçasıdır [1]. Teknolojinin gelişmesiyle beraber gömülü sistemlerin kullanım alanları artmıştır. Nesnelerin interneti ile birlikte gömülü sistemler ağ üzerinde birbiriyle bağlı hale gelmektedir. Ağ üzerinden gerçekleştirilen siber saldırılara karşı cihazların yeterince güvenli olmasının yanında, yan kanal analizi gibi ataklara karşı da gömülü sistemlerin güvenli olması önemlidir [2]. Yan kanal analizi atakları sistemin istemeden dışarıya yaydığı bilgileri kullanarak gizli anahtar hakkında bilgi etme yöntemidir. İlk pratik atak Kocher tarafından gerçeklenmiştir [3]. 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 [4]. Bu yaklaşımla beraber kriptografik algoritmaların matematiksel olarak sınanmasının yanında gerçeklemeye dayalı olası zayıflıklara karşı da sınanması gerektiği ortaya çıkmıştır. En çok kullanılan yan kanal bilgileri güç tüketimi, zamanlama ve elektromanyetik radyasyondur [5]. Raspberry Pi [6] küçük olmasının yanında mini bir bilgisayar özelliğine sahip olduğundan ideal bir gömülü sistemdir. Nesnelerin interneti ile birlikte popülerliği günden güne artmaktadır.

Bu bildiride, RSA algoritmasının Raspberry Pi platformu üzerinde gerçeklemesinin yan kanal analizi saldırılarından biri olan Elektromanyetik yayınım yan kanal analizine karşı güvenliği değerlendirilmiştir. Raspberry Pi platformu üstünde RSA şifreleme algoritması için kullanılan hızlı üs alma ve her zaman kare alma ve çarpma algoritmaları gerçeklenmiştir.

II. MATEMATİKSEL ARKA PLAN

A. *RSA şifreleme algoritması*

RSA şifreleme algoritması 1978 yılında açıklanmıştır [7]. En çok tercih edilen açık anahtarlı şifreleme algoritmalarından biridir. RSA algoritmasında açık veri m ve şifrelenmiş veri c olmak üzere şifreleme: $c = m^e \bmod n$, şifre çözme işlemi: $m = c^d \bmod n$ şeklinde tanımlanmıştır.

B. *Hızlı Üs Alma Algoritması*

RSA şifreleme algoritması kullanılarak yapılan şifreleme ve şifre çözme işlemlerinde modüler üs alma işlemi kullanılmaktadır. Sayılar büyüdükçe bu işlemi hızlı yapabilmek için bir yönteme ihtiyaç duyulmuştur [7]. Çarpma ve kare alma algoritması en çok kullanılan ve en basit hızlı modüler üs alma algoritmasıdır (Şekil 1). Anahtar e olmak üzere, anahtarın bit değerleri bulunduğunda algoritma kırılmış olur.

C. *Elektromanyetik Yayınım Analiz Saldırısı*

Tamamlayıcı metal oksitli yarı iletken transistörler (Complementary Metal Oxide Semiconductor - CMOS) elektronik tümdevrelerin gerçeklenmesinde çok sık kullanılmaktadır [8]. Devrelerin toplam güç tüketimi dinamik ve statik güç tüketimi olmak üzere ikiye ayrılmaktadır.

978-1-5386-1501-0/18/$31.00 © 2018 IEEE

$e = (e_k, e_{k-1}, e_{k-2}, e_{k-3}, ..., e_0)_2$

$c = m^e \bmod n$

1: $c \leftarrow 1$

2: for $i = k : 0$ // soldan sağa doğru

3: $c \leftarrow c * c \bmod n$ // Kare alma

4: if $e_i = 1$

5: $c \leftarrow c * m \bmod n$ // Çarpma

Şekil. 1.Hızlı üs alma algoritması

CMOS eviricilerinde dinamik güç harcaması daha baskındır. Tranzistörün çıkışının değişmediği zamandaki güç tüketimi statik güç tüketimini verir iken tranzistörün çıkışının değiştiği zamandaki güç tüketimi dinamik güç tüketimini vermektedir. CMOS kapısının çıkış değerindeki değişimin, anlık akım değişimine neden olduğu bilinmektedir. Anlık akım değişiminin yanı sıra elektromanyetik yayılım da ortaya çıkmaktadır. İşlenen veriye ya da gerçekleştirilen işleme göre elektromanyetik radyasyon değişmektedir. Antenlerle elde edilen elektromanyetik radyasyon elektromanyetik analiz saldırıları için yan kanal bilgisi olarak kullanılmaktadır.

Elektromanyetik yayınım analiz saldırıları basit elektromanyetik analizi saldırıları (Simple Electromagnetic Analysis - SEMA) ve farksal elektromanyetik analizi saldırıları (Differential Electromagnetic Analysis - DEMA) olmak üzere ikiye ayrılır [10]. Basit elektromanyetik analizi saldırılarında, saldırgan tek ölçüm kullanarak anahtarın tamamını ya da bir kısmını ele geçirmeye çalışmaktadır. Ölçümdeki gürültünün fazla olduğu durumlarda kullanılan farksal elektromanyetik analizi saldırılarında ise, birçok ölçüm kullanılarak gürültü yok edilmektedir.

D. Korelasyon Analizi

Korelasyon iki değişken arasındaki ilişkinin derecesini gösteren istatistiksel bir analiz yöntemidir. 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 [11].

$$C(X,Y) = \frac{E(X,Y) - E(X)E(Y)}{\sqrt{Var(X)Var(Y)}} \quad (1)$$

Denklem (1)'de $C(X,Y)$ korelasyon katsayısını vermektedir. $E(X)$, X değişkeninin beklenen değerini verirken $Var(X)$ ise 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.

III. ÖLÇÜM DÜZENEĞİ

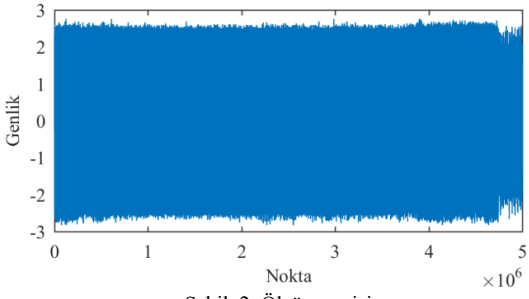
Ölçüm düzeneği Raspberry Pi, bilgisayar, osiloskop ve elektromanyetik alan alıcısı sisteminden oluşmaktadır. Raspberry Pi üzerindeki Broadcom firmasının BCM2835 işlemcisi yan kanal saldırısının temel hedefi konumundadır. Raspberry Pi üzerinde 2 adet evrensel seri veri yolu (Universal Serial Bus – USB) 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 yüksek hassasiyetli prob ile alınır. Yüksek hassasiyetli EM prob düşük gerilimli elektromanyetik yayınımları almak için idealdir. Bu prob osiloskobun başka bir kanalına bağlıdır. Osiloskop genel amaçlı giriş çıkış pinlerindeki gerilim artışını fark ettiği an elektromanyetik yayınımı alır ve ikili formatta kaydeder. Daha sonra Matlab'ta sinyal analizi gerçekleştirilmesi için başka bilgisayara aktarılır. Kullanılan yüksek hassasiyetli probun yüzey alanı çipin yüzey alanının 16'da biri kadardır. Bu nedenle çip üzerindeki 16 ayrı bölge taranmıştır ve en iyi noktadan ölçüm alınmıştır.

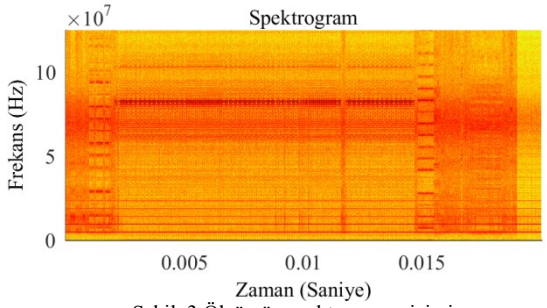
80 bitlik RSA anahtarı (9FFF0000FFFF0000FFFF) kullanılarak hızlı üs alma algoritması gerçeklenmiştir. Algoritmada anahtarın işlem yapılan bit değeri 1 ise çarpma işlemi yapılmakta, 1 değil ise yapılmamaktadır. Bu bilgi kullanılarak çarpma ve kare alma işlemleri birbirinden ayırt edilirse anahtarın bit değerleri tahmin edilebilir olacaktır. Osiloskoptan bilgisayara aktarılan ölçüm Matlab aracılığıyla tekrar oluşturulmuştur (Şekil 2).Ölçüm incelendiğinde, ön işleme tabi tutulmadan ham veriden bilgi elde etmek mümkün görünmemektedir.

IV. FİLTRELEME

Basit Elektromanyetik analizi atağı gerçekleştirilirken iki adet filtre kullanılmıştır. 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 ölçümün spektrogramı çizdirilmiştir. Spektrogram, ölçümdeki sinyalin zamana bağlı frekans değişimini görsel olarak ifade etmektedir. Kriptografik işlemin yoğun işlem gücü gerektirdiği bilinmektedir. Şekil 3'te elektromanyetik yayınımın yoğun olduğu frekans aralığı kırmızı rengin en yoğun ve koyu olduğu bölge olan 75 MHz ile 90 MHz arasıdır. Bu aralığı filtreleyen tasarım metodu FIR olan bant geçiren filtre tasarlanmıştır. Bu filtre uygulandıktan sonra RSA algoritmasının çalışması ile alakalı olmayan sinyallerin bir kısmı ortadan kalkmış olacaktır.



Şekil. 2. Ölçüm verisi



Şekil. 3.Ölçümün spektrogram çizimi

Raspberry Pi donanımının elektromanyetik radyasyonu dinamik ve sabit bileşen olmak üzere iki bileşenden oluşur.

$$p(t) = P_{sabit}(t) + p_{dinamik}(t) \quad (2)$$

(2)'de P_{sabit} anlık değişmeyen bölümdür, $p_{dinamik}$ ise dinamik bileşendir. Genellikle dinamik bölüm sabit bölümden daha zayıftır [12]. Bilgi içeren sızıntıyı bulmak için elektromanyetik radyasyondan bu dinamik bölümü ayırmak gerekir. Kasıtsız oluşturulan EM sızıntısı kendini taşıyıcı frekansa modüle olmuş halde göstermektedir.

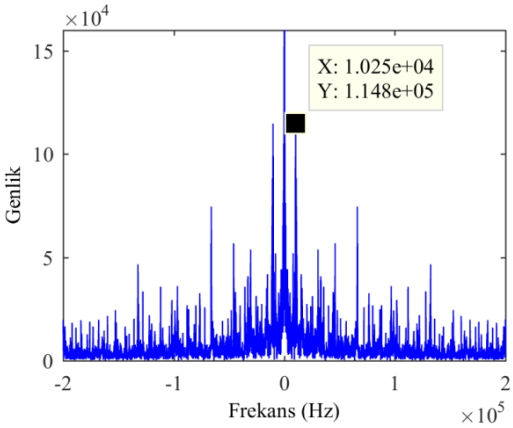
$$s(t) = p(t)\cos(w_r t) \quad (3)$$

Denklem (3) sinyalin genliğinin modülasyonunu vermektedir. Bu denklemde w_r taşıyıcı frekanstır. Genlik demodülasyonu kullanılarak $p(t)$ ve bileşenleri elde edilebilir. Genlik demodülasyonu için yaygın olarak kullanılan zarfla algılama yöntemi kullanılmıştır [12]. 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 [13].

Doğrultulmuş sinyal, elektromanyetik radyasyon sinyalinin spektrumuna benzerdir. Fakat spektrum ölçeklendirilmiş ve taşıyıcı frekansın çift katlarında tekrarlanmaktadır.

Bilgi içeren sızıntıyı elde etmek için taşıyıcı frekansın bulunması ve ona uygun filtre ile ölçümün filtrelenmesi gerekmektedir. Taşıyıcı frekansı bulmak için birinci filtreden geçirilmiş olan ölçümün mutlak değeri alınmıştır. Elde edilen ölçüm frekans bölgesine geçirilerek filtre uygulanacak bant belirlenmiştir. Şekil 4'te spektrum verilmiştir.



Şekil. 4.Doğrultulmuş sinyalin spektrumu

Oluşan tepeler için ayrı bant geçiren filtreler kullanılarak bilgi içerip içermediği kontrol edilmiştir. Genliği en yüksek olan tepe 10 kHz civarındadır. Düşük frekansta çalışan uygun bir bant geçiren filtre istenen sinyal bileşenini ölçümden izole etmek için kullanılabilir. İkinci filtre olarak 5 kHz ile 15 kHz arasını geçiren FIR bant geçiren filtre kullanıldığında bilgi elde edilmiştir.

V. Basit Elektromanyetik Analizi Saldırısı

Bir önceki bölümde anlatılan iki adet filtrenin ölçüme uygulanmasının ardından ölçüm tekrar çizdirilmiş ve RSA işleminin başladığı bölgeye yoğunlaşılmıştır. Şekil 5'te yer alan ölçümde de görüleceği üzere elde edilen ölçümde genliği en yüksek olan işlem mod alma işlemidir. Çarpma işleminin genliği ise kare alma işleminin genliğinden fazladır.

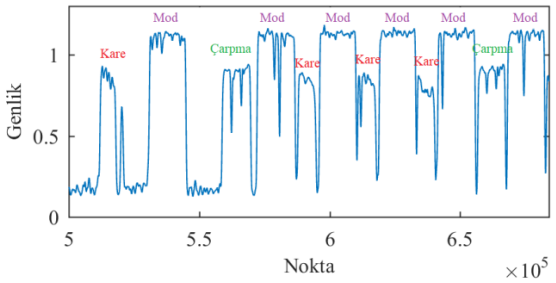
Hızlı üs alma algoritmasına göre kare alma işleminden sonra çarpma işlemi gerçekleştiriliyor ise anahtarın ilgili bit değeri '1' olmalıdır. Eğer kare alma işlemini çarpma işlemi takip etmiyor ise ilgili bit değeri '0' olmalıdır. Bu analoji takip edildiğinde Şekil 5'te gösterilen anahtarın ilk 4 bitinin değeri '1001' olmaktadır. Ölçümün tamamında bu analoji uygulandığında anahtar değeri 16'lık sistemde 9FFF0000FFFF0000FFFF olmaktadır.

Hızlı üs alma RSA algoritması gerçekleme zamanı açısından eniyileme sağlasa da bit değerine göre farklı işlemlerin gerçekleştirilmesi anahtarın ele geçirilmesine neden olmaktadır. Bu atağa karşı önlem olarak her turda aynı işlemlerin yapılacağı bir gerçekleme tercih edilmiştir [14]. Hızlı üs alma algoritması yerine her zaman kare alma ve çarpma algoritması kullanıldığında tek ölçüm ile anahtarı tahmin etmek mümkün olmamıştır. Şekil 6'de algoritma verilmiştir. Şekil 7'de ise her turda kare alma ve çarpma işlemlerinin yapıldığını gösteren ölçüm verisi verilmiştir.

VI. Farksal Elektromanyetik Analizi Saldırısı

DEMA saldırılarında atak yapılacak bölgenin belirlenmesi çok önemlidir. Gerçekleştirilen DEMA saldırısında RSA her zaman kare alma ve çarpma algoritmasında kullanılan anahtarın en anlamlı bitine atak yapılmıştır. En anlamlı bitin değeri 0 ise kare alma işlemi sonucu d nesnesine atanacakken, değeri 1 ise kare alma işlemini takip eden çarpma işleminin sonucu d nesnesine atanacaktır.

Aynı anahtar değeriyle N adet veri işleme sokulmuştur. Bu işlem sonucunda N adet ölçüm elde edilmiştir. Bu ölçümler SEMA saldırısında uygulanan filtrelerden geçirilmiştir. Daha sonra ilk bit sonucunda d nesnesinin değerinin güncelleneceği bölgeye göre ölçümler hizalanmıştır. Bu bölge ölçümdeki ilk çarpma işlemi ile ikinci kare alma işlemi arasında kalan bölgedir. Güç matrisi bu bölgedeki verilerden oluşmaktadır.



Şekil. 5.Ölçümdeki işlemlerin birbirinden ayrılması

$e=(e_{k-1},e_{k-2},e_{k-3},...,e_0)_2$, $d=m^e \bmod n$

1: $d \leftarrow m$

2: for $i=k-1:0$ // soldan sağa doğru

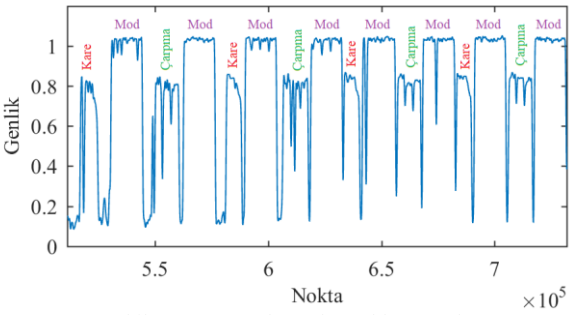
3: $d_1 \leftarrow d*d \bmod n$ // Kare alma

4: $d_2 \leftarrow m*d_1 \bmod n$ // Çarpma

5: if $e_i=1$ $d \leftarrow d_2$

7: else $d \leftarrow d_1$

Şekil. 6.Her zaman kare alma ve çarpma algoritması



Şekil. 7.SEMA'ya karşı dayanıklı RSA ölçümü

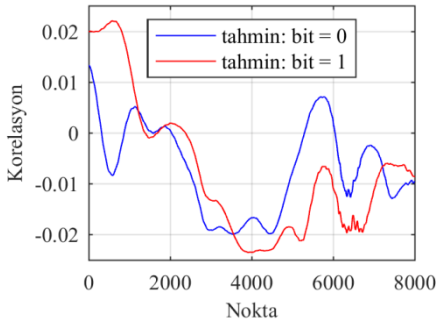
Korelasyon analizi gerçekleştirebilmek için elektromanyetik radyasyon ölçümlerinin yanında tahmin matrisleri de gerekmektedir [15]. Tahmin matrislerinin oluşturulması için Hamming Uzaklığı yöntemi kullanılmıştır. Anahtarın ilk bit değerinin 1 ya da 0 olmasına göre iki adet tahmin matrisi oluşturulmuştur. En anlamlı bit değeri 0 ise d nesnesinin değeri m değerinden d1 değerine, 1 ise m değerinden d2 değerine değişmiştir. Tahmin matrisleri bu değişim sonucunda 0'dan 1'e ya da 1'den 0'a değişen bit sayısını tutmaktadır. 1024 bitlik veriler kullanıldığından tahmin matrislerinin her bir elemanı 0 ile 1024 arasında değişmektedir.

Hamming Uzaklığına göre güç tahmin matrisleri bulunduktan sonra, güç matrisi ile güç tahmin matrisleri sırasıyla korelasyon işlemine tabi tutulmuştur. İki veri seti arasında yüksek pozitif korelasyon aranmıştır (Şekil 8).

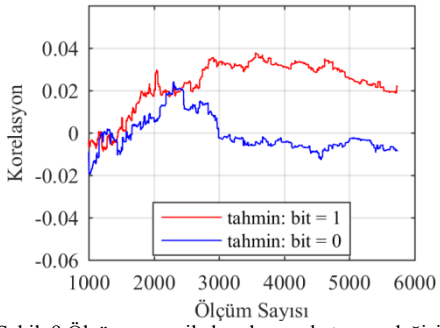
Korelasyon değerinin en yüksek çıktığı nokta (576. nokta) baz alınarak ölçüm sayısına bağlı korelasyon katsayısı değişimini gösteren grafik Şekil 9'da yer almaktadır. 2500. ölçümden sonra bit değerinin 1 olmasına bağlı olarak hazırlanan tahmin matrisinin korelasyonu artarken, diğeri 0 civarına düşmüştür.

VII. SONUÇ VE ÖNERİLER

Bu çalışmada, Raspberry Pi üzerinde gerçeklenmiş RSA algoritmalarına SEMA ve DEMA saldırıları yapılmıştır. SEMA saldırısı sonucunda karşı önlem içermeyen bir gerçeklemede bütün anahtar bitlerinin tek bir ölçüm ile elde edilebileceği gösterilmiştir. SEMA saldırısına dayanıklı algoritma gerçeklenerek anahtarın SEMA ile elde edilemediği görülmüştür. Ölçüm sayısının arttırılması ve korelasyon analizinin kullanılmasıyla DEMA saldırısı gerçeklenmiştir. DEMA saldırısıyla anahtarın bit değerinin elde edilebileceği görülmüştür. 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.



Şekil. 8.Korelasyon katsayısı grafiği



Şekil. 9.Ölçüm sayısı ile korelasyon katsayısı değişimi

KAYNAKLAR

[1] Akdur D., Demirörs O. ve Garousi V., "Gömülü Sistem Mühendisliğinde Kullanılan Yazılım Modellemesi ve Model Güdümlü Teknikler Anketi: Türkiye Sonuçları Teknik Raporu, " Orta Doğu Teknik Üniversitesi, Enformatik Enstitüsü ODTÜ/II-TR-2015-54, 2015.

[2] Sanada A., Nogami Y., Iokibe K. and Khandaker M. A. A., "Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography," *2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW)*, Taipei, 2017, pp. 287-288.

[3] Kocher P., "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems" in *Advances in Cryptology: Proceedings of CRYPTO'96*, vol. 1109 of LNCS, pp. 104-113, 1996, Springer-Verlag.

[4] Janke M. and Laackmann P., "Power and timing analysis attacks against security controllers", Infenion Technologies AG, Technology Update, Smart Cards.

[5] De Mulder E., Buysschaert P., Ors S.B., Delmotte P., Preneel B., Vandenbosch G. and Verbauwhede I., "Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem", *EUROCON 2005 - The International Conference on "Computer as a Tool"*, Belgrade, 2005, pp. 1879-1882.

[6] Raspberry Pi https://raspberrypi.org Erişim Tarihi : 11.02.2018

[7] Rivest R. L., Shamir A., Adleman L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Communications of the ACM*, Vol. 21, Issue 2, pp. 120-126, February 1978.

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

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

[10] Chari S., Rao J.R. and Rotagi P., "Advances in Side-Channel Analysis", *RSA Laboratories Cryptobytes*, vol. 6, sf 20-32, 2003.

[11] Clarke G. M. and Cooke D., *A basic course in statistics*, Arnold London, 4th edition, 1998.

[12] Do A., Ko S. T. and Htet A. T., "Electromagnetic Side-Channel Analysis On Intel Atom Processor", *A Major Qualifying Project Report*. Worcester Polytechnic Institute, 2013.

[13] Oswald D., Paar C., "Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World" In: Preneel B., Takagi T. (eds) Cryptographic Hardware and Embedded Systems – CHES 2011. CHES 2011. Lecture Notes in Computer Science, vol 6917. Springer, Berlin, Heidelberg

[14] Witteman M.F., van Woudenberg J.G.J., Menarini F., "Defeating RSA Multiply-Always and Message Blinding Countermeasures", In: Kiayias A. (eds) Topics in Cryptology – CT-RSA 2011. CT-RSA 2011. Lecture Notes in Computer Science, vol 6558. Springer, Berlin, Heidelberg

[15] Yalçın S. B. Ö., Hardware design of elliptic curve cryptosystems and side-channel attacks. *Doktora tezi*. Katholieke Universiteit Leuven, 2005