AKILLIKARTLARDA GÜÇ ANALİZİNE DİRENÇLİ BELLEK YAPILARI

Engin KONUR[1] Yaman ÖZELÇİ[2] Ebru ARIKAN[3] Umut EKŞİ[4]

[1-4]TÜBİTAK-UEKAE
Gebze, 41470 KOCAELİ

[1]e-posta: engin@uekae.tubitak.gov.tr [2] e-posta: yaman@uekae.tubitak.gov.tr
[3] e-posta: ebru@uekae.tubitak.gov.tr [4] e-posta: umut-eksi@uekae.tubitak.gov.tr

Anahtar sözcükler:Akıllıkart, Bellek, SRAM, Yan Kanal Analizi, Güç Analizi

ÖZET

Akıllıkart gibi gizli bilgi güvenliğinin ön planda olduğu uygulamalarda, bilgi güvenliğini tehdit eden saldırılara karşı alınan önlemlerin çoğunluğu, işletim sistemini ve çalışan uygulamayı kapsayacak şekilde yazılım seviyesindeki yöntemleri kullanmaktadır. Ancak bu konunun donanım yönü de bulunmaktadır ve donanım seviyesinde alınacak tedbirler, yazılım seviyesindeki yöntemlerin yeterli olamadığı, yan kanal analizi saldırılarında önemli avantajlar sunmaktadır. Bu konuda, Avrupa Birliği 6. Çerçeve Programı (6.ÇP) kapsamında TÜBİTAK-UEKAE'nin de katılımcı olarak yer aldığı, Yan Kanal Analizine Dirençli Tasarım (SCARD) isimli bir proje yürütülmektedir. Bu proje kapsamında, istenen amaca yönelik yarı-özel bir tümdevre tasarım akışının geliştirilmesi ve geliştirilen yöntemler kullanılarak tasarlanmış bir tümdevrenin üretilip doğrulanması planlanmıştır. Akıllıkartlarda kullanılan şifreleme algoritmalarında sabit parametrelerin saklandığı Salt Okunabilir Bellekler ile anahtar üretme ve saklama amacıyla kullanılan Rastgele Erişilebilir Bellek yapıları bilgi güvenliği bakımından ayrı bir önem arzetmektedir. Güç Analizi, güvenli bilgi işleyen tümdevrelerde, gizli bilgileri, beslemeden çekilen akım işaretini inceleyerek elde etmeyi amaçlayan bir yan kanal analizi yöntemidir. Bu bildiride, 6.ÇP SCARD projesi kapsamında, TÜBİTAK UEKAE tarafından yapılan, güç analizine dirençli bellek yapıları konusundaki çalışmalar (devre tasarımı, benzetimi ve sonuçların analizi) ele alınmıştır.

ABSTRACT

Increase in resistance against security attacks in applications such as Smart Cards, in which information security is of primary importance, is generally achieved solely through software-level techniques that involve the operating system and/or the application(s) being executed. However, there exist certain hardware-level techniques that offer significant advantages compared to their software counterparts; they perform much better especially against Side Channel Attacks (SCA) for which software-only techniques are not sufficient alone. A project called SCARD (Side Channel Analysis Resistant Design), in which TUBITAK-UEKAE is a partner, is being conducted as a part of the European Community 6th Framework Programme. The goal of the project is to develop a semi-custom design flow and to design, produce and verify a secure chip through this flow using the techniques achieved in the course of the project. The SRAM structures, that are used to store secret keys and parameters in the crypographic algorithms, constitute an important part of information security in smart cards. This paper presents the studies on SRAM structures to improve their resistance against Power Analysis (a specific SCA technique that aims to extract secret information by analyzing the power drawn from the supply) that are conducted by TUBITAK-UEKAE in the SCARD project. It includes the circuit-level design methods, simulation and the analysis of simulation results.

1. GİRİŞ

Bilgi iletişimi sırasında, iletişime dahil olması istenenlerin dışında kalanların, iletilen bilgiye ulaşma çabası ve bu çabayı boşa çıkarma ve zorlaştırma gayreti hep var olmuştur ve göründüğü kadarıyla da var olacaktır.

İletilen ve depolanan bilgiyi gizlemek amacıyla geliştirilen kriptografik donanımlar, çalışmalarının doğal sonucu olarak hem çevrelerini etkiler hem de çevrelerinden etkilenirler. Donanımın besleme geriliminden akım çekmesi, elektromanyetik dalga yayması gibi doğal mekanizmalar, işlenen ve depolanan gizli bilginin elde edilmesiyle sonuçlanacak enformasyon kaçaklarına sebep olurlar. Bu enformasyon kaçaklarını incelemeye dayanan analizlere genel olarak yan kanal analizleri denilmektedir.

Bu analizlerden bilgi edinilmesini zorlaştırmak için hem yazılım hem donanım tarafında önleyici çalışmalar yapılabilmektedir. Bu çalışmalar, kriptografik cihazın tasarım ve üretim zamanının uzamasına ve maliyetinin artmasına sebep olmaktadır. Ayrıca yan kanal analizi tekniklerinin gelişmesi ve ucuz laboratuar aletleriyle sadece cihazın harcadığı gücü ölçerek enformasyon çalmanın mümkün olduğu güç analizi [1] gibi tekniklerin ortaya çıkması kriptografik cihazın bir bütün olarak ele alınmasını ve en alt seviyedeki kriptografik donanım olan tümdevrelerin de bu yaklaşımla tasarlanıp üretilmesini gerekli kılmaktadır.

Yan kanal analizlerine dirençli tümdevreler ile bunların kullanıldığı kriptografik donanımlar ve akıllıkartlar; hızlı ve güvenli tasarlanıp üretildiklerinde ve dolayısıyla daha ucuz olduklarında, hem bu donanımları tasarlayan ve üretenler tarafından, hem de bu donanımları örneğin akıllıkartları kişisel işlemleri için kullanan son kullanıcılar tarafından güvenilirlikleri nedeniyle tercih edileceklerdir.

Avrupa Birliği 6. Çerçeve programına sunulan ve kabul edilen SCARD (Side Channel Analysis Resistant Design Flow) isimli proje bu yaklaşımı kullanarak çözüm geliştirme amacını taşımaktadır. Avusturya, Almanya, Belçika, İtalya ve Türkiye olmak üzere 5 farklı ülkeden 9 katılımcı kuruluşun yer aldığı projede, TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE), ağırlıklı olarak Yarıiletken Teknolojisi Araştırma Laboratuvarı (YİTAL) personeliyle, yan kanal analizlerine dirençli bellek geliştirilmesi konusundan sorumlu olarak projeye katkı sağlamaktadır.

2. YAN KANAL ANALİZLERİ (YKA)

Yan kanal analizleri (atakları-saldırıları), bozucu ve bozucu olmayan saldırılar olarak gruplandırılır [2,3]. Bozucu saldırıda tümdevrenin paketi açılarak enformasyon elde edilmeye çalışılır. Bozucu olmayan saldırıda kriptografik donanıma zarar vermeden sadece dışarıdan gözlem yapılır. İşaret işleme süresinin, elektromanyetik yayınımın, harcanan gücün ölçülmesi; bozucu olmayan saldırılardır.

2.1 Bozucu Yan Kanal Analizleri

Bozucu saldırılar da aktif ve pasif olarak ikiye ayrılırlar. Tümdevrenin açılıp veri hattına ulaşılıp ölçülmesi pasif saldırıdır. Tümdevreye hata ürettirecek şekilde örneğin bağlantı yollarında açık-devre veya kısa-devre oluşturmak suretiyle müdahele etmek ise aktif saldırıdır. Bozucu saldırılar laboratuvar koşulları gerektirdiğinden pahalıdırlar.

2.2 Bozucu Olmayan Yan Kanal Analizleri

Bozucu olmayan ve gözleme dayalı saldırılardan bir tanesi, zamanlama analizi saldırısıdır. Algoritmanın bilindiği durumlarda, girişler, çıkışlar ve saat işareti ölçülerek hangi adımın ne kadar zamanda gerçeklendiği anlaşılır. Algoritmadaki adımların süresi giriş verisine bağlı ise saklı bilgiye ulaşılır.

Güç analizi saldırısında kriptografik cihazın çektiği güç ölçülür, ölçüm sonuçları depolanır ve izlenir. Basit güç analizi (Simple Power Analysis-SPA) ve farksal güç analizi (Differiential Power Analysis-DPA) bu tür yöntemlerdir. [4].

SPA, kriptografik işlemler sırasında harcanan gücün yorumlanması tekniğidir ve bir algoritmada gerçeklenen farklı adımlar (çarpma, permütasyon, üst alma, "else if" dallanmaları …) bu yöntemle tespit edilebilir. Bu algoritma adımları incelenerek şifre kırılabilir.

DPA ise harcanan güçteki farklarla ilgilenir. Çok fazla sayıda tekrarlanan ölçümlerin sonuçlarına, işaret işleme ve istatiksel hesaplama teknikleri uygulanarak, verilerdeki gürültü ayıklanır ve fark güçlendirilir. DPA, SPA'ya göre çok daha etkili ama uygulanması daha zor bir tekniktir.

3. YAN KANAL ANALİZLERİNE DİRENÇLİ TASARIM YÖNTEMLERİ

YKA dirençli tasarım için uygulanan bir yöntem, işlenen bilgiyi rastgele işaret üreteçleri kullanarak karmaşıklaştırmak, bir başka deyişle maskelemektir [5].

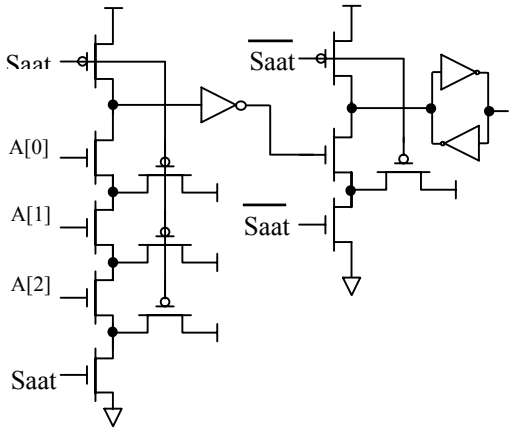
Bir diğer yöntem ise güç harcamasını her giriş verisi için eşit hale getirmektir. CMOS lojikte dört durum geçişi vardır: 0-1, 1-0, 0-0 ve 1-1. Standart CMOS lojik ile üretilen tümdevrelerde bu dört durumdan sadece 0-1 geçişinde besleme kaynağından güç çekilir. Eğer dört durum için her saat çevriminde aynı enerji harcanırsa harcanan güç (beslemeden çekilen akım)

işlenen veri ile ilgili bilgi içermez. Dinamik lojik ile farksal lojik yaklaşımlarının birleşimi olan "Algı Güçlendirici Tabanlı Lojik-AGTL" tekniği bunu sağlamaktadır [2]. Bu teknikte her saat geçişinde aynı değerde kapasitenin dolup boşalması sağlanmaktadır. Normalde güç harcanmayacak durumlarda da güç harcanacağı için devrenin toplam güç harcaması artacaktır ve standart CMOS lojik yerine daha fazla tranzistor içeren AGTL kullanıldığı için de harcanan toplam silisyum alanı artacaktır.

4.YKA DİRENÇLİ BELLEK TASARIMI

Bir bellek yapısının YKA'ne karşı dirençli olması için, belleğe erişim (okuma ya da yazma) sırasında beslemeden çekilen enerjinin, erişimle ilgili veriden (yazılan ya da okunan veri) ve adresten bağımsız olması gerekir [6]. Bu şartı sağlayabilmek için TÜBİTAK UEKAE'de, Algı Güçlendirici Tabanlı Lojik (AGTL) prensibinden yararlanılarak, belleği oluşturan temel yapı taşı olan birim hücre ile belli başlı kontrol ve veri yolu yapıları üzerinde bazı değişiklikler yapılmıştır [7].

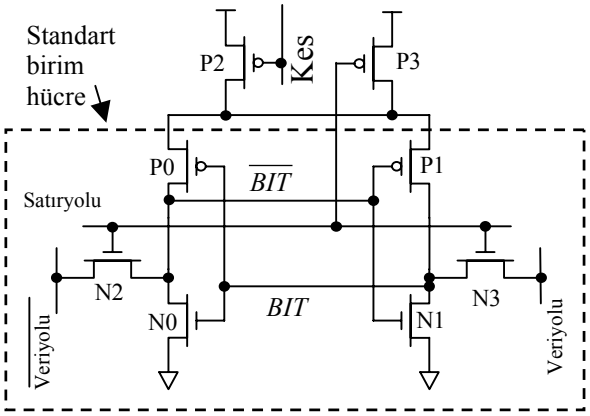
Besleme akımının adres değerine olan bağımlılığını azaltmak amacıyla, belleğin kontrol kısmında yer alan satır ve sütun çözücü bloklar AGTL yaklaşımıyla Şekil-1'deki gibi tasarlanmıştır. Aynı şekilde bellek hücresi ve sütun veriyolundaki devreler gözden geçirilmiş, AGTL işaretlerini kullanacak ve bu prensibe uygun işleyecek duruma getirilmiştir.



Şekil-1. Önerilen adres çözücü (3-bit için).

SRAM'de OKU işlemi ele alındığında, hücrenin ve sütun veriyolunun diferansiyel ve dolayısıyla simetrik olması (aynı işaretin kendisi ve evriğinin aynı anda işlem görmesi) beslemeden çekilen enerjinin okunan veriye bağımlılığını büyük ölçüde azaltmaktadır. Buna dayanarak OKU işlemi için SRAM'in çalışma düzeninde bir değişikliğe gerek görülmemiştir.

YAZ işlemi ise veriyolunun simetrik olmasına rağmen hücrede saklı bulunan değer ile yazılmak istenen veri değerine bağlı olarak enerji tüketiminde farklılık göstermektedir. Yazılmak istenen değerin hücrede o sırada saklı bulunan değerden farklı olması ya da o değerle aynı olması durumları, farklı geçiş akımlarına ve dolayısıyla farklı enerji tüketimine sebep olmaktadır. Diğer bir değişle, YAZ işlemi, herhangi bir düzenleme yapılmadığı durumda standart bir SRAM yapısında, yazılmak istenen ve saklı bulunan veri değerleri hakkında besleme hattı üzerinden dışarıya bilgi sızdıracaktır. Bu konuda AGTL prensibine dayanarak SRAM yapısının YAZ işlemi akışında birtakım düzenlemelere gidilmiştir. Beslemeden çekilen enerji miktarını SRAM hücresinde saklanmış olan değerden bağımsız hale getirebilmek için sadece ilgili hücredeki değerin, tıpkı dinamik lojikte olduğu gibi, bir önyükleme fazıyla bozularak, yazılmak istenen veriden bağımsız olarak her durumda aynı seviyeye çekilmesi (başlangıç konumlandırılması) ve bu konumdan başlayarak YAZ işleminin gerçekleştirilmesi düşünülmüştür.

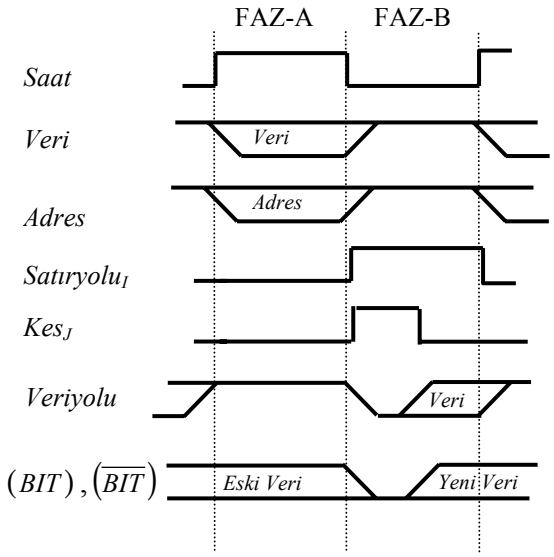


Şekil-2. Önerilen AGTL-SRAM birim hücresi

Standart CMOS SRAM bellek hücresi, TÜBİTAK UEKAE tarafından Şekil-2'de görüldüğü gibi değiştirilmiştir. Böylece gerektiği durumlarda hücrenin beslemeden izole edilebilmesi sağlanmış ve bu sayede hücre içi düğümlerin güvenli ve doğru bir biçimde uygun gerilim seviyelerine yüklenmesine olanak tanınmıştır. Şekil.2'deki yeni bellek hücresine ilave edilen PMOS tranzistora bağlı "Kes" işareti aynı sütundaki tüm hücrelerde ortaktır. Aynı sütunda bulunan ve önyükleme yapılmak istenmeyen hücrelerin de beslemeden izole edilmemesi için "satıryolu" işaretine bağlı ikinci bir PMOS tranzistoru kullanılmıştır. Böylece, sadece yazılmak istenen hücre başlangıç konumlandırmasına maruz kalmakta diğer hücrelerin içeriği değişmemektedir. Devrenin çalışması ile ilgili olarak, kullanılan işaretlerin zamanlama bilgisi Şekil-3'te verilmiştir.

Kavramların pratik bir uygulamayla ispatlanması amacıyla 256-bayt büyüklüğünde (32 satır, 64 sütun) biri standart CMOS diğeri AGTL yaklaşımıyla olmak üzere iki SRAM yapısı tasarlanmıştır. Bu yapılar,

bütün olası giriş vektör değer ve geçişlerini içeren benzetimlerden geçirilerek sonuçlar karşılaştırılmıştır.



Şekil-3. AGTL-SRAM için değiştirilmiş YAZ işlemi (I. satır ve J. sütuna).

Hücre dizisinin serimi tasarlanarak benzetimlere serimden elde edilen parazitik değerler dahil edilmiştir. Hücre dizisi dışındaki kısımlar için benzetimlerde şemalar kullanılmış ve bunlara hesaplanan tahmini parazitik değerler ilave edilmiştir.

YKA'ya karşı direnç performansının karşılaştırılması amacıyla AGTL'nin detaylı olarak ele alındığı [4]'deki makalede verilen ölçütten faydalanılmıştır. SCARD proje konsorsiyumu, bu ölçütün, normalize edilmeden kullanılmasını uygun bularak aşağıdaki gibi ifade edilmesini kararlaştırmıştır.

Enerji Dağılımı (ED),

$$ED = Maksimum(E_{DB}) - Minimum(E_{DB})$$

Burada, E_{DB} , döngü başına enerji değeridir. ED değerlerinin düşük olması, farklı veri ve adres kombinasyonlarının işlendiği farklı döngülerin, beslemeden çekilen enerji miktarları açısından birbirlerine göre az farklılık gösterdiğinin, dolayısıyla besleme hattından daha az bilgi sızdığının ve tümdevrenin yan kanal analizlerine daha dirençli olduğunun bir göstergesidir.

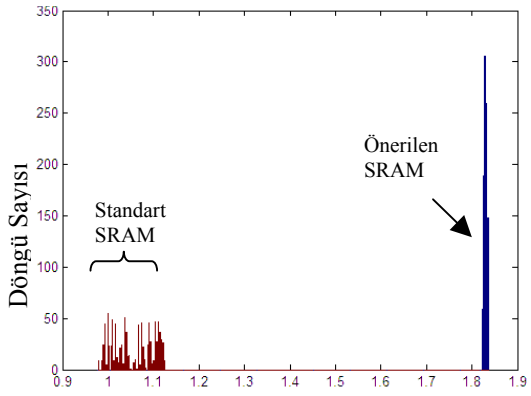
Enerji dağılımı, yapılan benzetimlerde elde edilen değerler ve aşağıdaki formül kullanılarak hesaplanmıştır.

$$ED = \frac{(I_{ort(mak)} - I_{ort(\min)})V_{DD}}{f}$$

Burada f çalışma frekansı, V_{DD} besleme gerilimi ve I_{ort} bir saat periyodu için ortalaması alınmış besleme akımı değeridir.

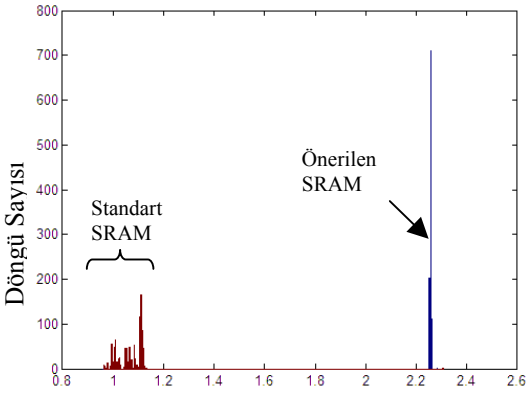
Benzetimler için analog benzetim programı yüksek doğruluk ayarlarıyla kullanılmıştır. Benzetim sonucunda elde edilen besleme akımları nümerik analiz programı kullanılarak analiz edilmiştir.

Şekil-4'de OKU, Şekil-5'de YAZ işlemi sırasında, Standart SRAM ve önerilen AGTL-SRAM'de beslemeden çekilen akımların her döngü için alınan ortalamalarının, farklı hücrelere okuma ve yazma yapılırken oluşan dağılımları histogram olarak verilmektedir.



Şekil 4: Önerilen SRAM'de OKU işleminde, döngü başına ortalama akım histogramı

Ortalama akım değerleri, standart CMOS lojik ile gerçekleştirilen SRAM'de geniş bir dağılım gösterirken, önerilen AGTL-SRAM'de her döngüde birbirine çok yakın değerler almıştır.



Şekil 5: Önerilen SRAM'de YAZ işleminde, döngü başına ortalama akım histogramı

Yapılan benzetimlerle ayrıntılı olarak elde edilen ortalama akım değerleri Tablo-1'de özetlenmiştir. Yan kanal analizlerine direnç ölçütü olarak alınan ED değerleri hesaplandığında, AGTL-SRAM için bu değerler, Standart-SRAM'den yaklaşık on kat küçük olup, AGTL-SRAM'in yan kanal analizlerine standart-SRAM'den on kat daha dirençli olduğu sonucunu vermektedir.

İşlem	Mak[µA]	Min[µA]	*ED*[pJ]
Yaz-Yaz	1128.3	955.4	2.59
Yaz-Oku	1140.4	997.3	2.15
Oku-Yaz	1189.5	1011.5	2.67
Oku-Oku	1125.2	973.2	2.28

(a) Standart CMOS Logic SRAM

İşlem	Mak[µA]	Min[µA]	*ED*[pJ]
Yaz-Yaz	2262.2	2249.9	0.18
Yaz-Oku	1913.2	1901.0	0.18
Oku-Yaz	2220.1	2209.0	0.17
Oku-Oku	1837.8	1823.7	0.21

(b) Önerilen AGTL-SRAM

Tablo 1: Farklı OKU/YAZ işlemleri sırasında, döngü başına ortalama akım değerlerinin maksimum/minimum değerleri ile karşı düşen enerji dağılım değerleri (a) Standart SRAM (b) Önerilen AGTL-SRAM (f=100MHz ve V_{DD}=1.5Volt).

Tablo-1'deki ilk sütunda işlem başlığı altında, ardarda yapılan işlemler ifade edilmektedir. Yaz-Yaz işlemi ardışıl yazmaları, Oku-Oku işlemi ardışıl okumaları göstermektedir. Yaz-Oku işlemi, yazma yapıldıktan hemen sonra yapılan okuma işlemini, Oku-Yaz işlemi de okumadan hemen sonra yapılan yazmayı anlatmaktadır. Standart SRAM'lerde ardışıl okuma işlemlerinde de yüksek ED değerlerinin elde edilmesinin nedeni, RAM dizisinin dışında kalan bölgelerin diferansiyel ve simetrik olmamasıdır. AGTL-SRAM'lerde Şekil-1'de önerilen yeni adres çözücü devre kullanılarak ve devrenin diğer bölümleri de AGTL prensibiyle tasarlanarak her türlü işlem için düşük ED değerleri elde edilmiştir.

5.SONUÇ

Avrupa Birliği 6. Çerçeve Programı kapsamında yürütülen SCARD isimli projede, TÜBİTAK UEKAE tarafından, Algı-Güçlendirici-Tabanlı-Lojik (AGTL) yaklaşımıyla tasarlanan yeni SRAM, standart CMOS lojik SRAM'lerden yaklaşık %70 daha fazla silisyum alanına gereksinim duymakta ve ortalama iki kat daha fazla güç tüketmektedir. Buna karşılık, yan kanal analizlerine direnç ölçütü olan ED değerleri dikkate alındığında AGTL-SRAM, standart-SRAM'lerden yaklaşık on kat daha düşük ED değerlerine sahiptir. Bir başka deyişle AGTL-SRAM, yan kanal analizlerine, standart-SRAM'lerden on kat daha fazla dirençlidir. Bilgi güvenliğinin, kullanılan silisyum alanı ve harcanan güçten daha önemli olduğu kriptografik donanım uygulamalarında, tarafımızdan önerilen AGTL-SRAM açık bir avantaja sahip olacaktır. Benzetimlerle elde edilen sonuçların doğrulanması amacıyla, tasarlanan AGTL-SRAM'lerin SCARD projesi kapsamında üretilmesi planlanmıştır.

KAYNAKÇA

[1.] P. Kocher, J.Jaffe, B.Jun (1999), "Differential Power Analysis", Proc. Of Advances in Cryptology, Lecture Notes in Computer Science, 1666, 388-397.

[2.] R.Anderson, M.Kuhn, "Tamper Resistance – a Cautionary Note", Proceedings of the second USENIX workshop on Electronic Commerce, Oakland, California, Nov.1996, 1-11.

[3.] F.Koeune, J.J.Quisquater, "Side Channel Attacks", Scientific Report, K2Crypt, Oct. 2002.

[4.] K.Tiri, M.Akmal, I.Werbauwhede (2002), "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards", ESSCIRC 2002, 403-406.

[5.] E.Trichina, D.De Seta, L.Germani, "Simplified Adaptive Multiplicative Masking for AES and its Secure Implementation", Proc. Cryptographic Hardware and Embedded Systems, CHES 2002, 2523 of Lecture Notes in Computer Science (2002), 277-285.

[6.] M.Neve, E.Peeters, D.Samyde, J.J.Quisquater, "Memories: A Survey of their Secure Uses in Smart Cards", Proc. of the second Intl. IEEE Security in Storage Workshop, Washington, DC, USA, October 2003, 62-72.

[7.] E.Konur, Y.Özelçi, E.Arıkan, U.Ekşi (2004), "Yan Kanal Analizlerine Dirençli Kriptografik Tümdevre Tasarım Yöntemleri Geliştirilmesi", SAVTEK-2004 Savunma Teknolojileri Kongresi, 385-393.