FPGA Üzerinde Ring Osilatörü Tabanlı PUF Gerçeklemesi
A Ring Oscillator Based PUF Implementation on FPGA

Giray Kömürcü[1], Ali Emre Pusane[2], Günhan Dündar[2]

[1]TÜBİTAK, Bilişim ve Bilgi Güvenliği İleri
Teknolojiler Araştırma Merkezi
giray.komurcu@tubitak.gov.tr

[2]Elektrik-Elektronik Mühendisliği Bölümü
Boğaziçi Üniversitesi
ali.pusane@boun.edu.tr, dundar@boun.edu.tr

Özet

Fiziksel kopyalanamaz fonksiyonlar (physically unclonable functions - PUFs), tümdevre üretimi sırasındaki kontrol edilemeyen süreçlere dayalı olarak her bir yongaya özgü imza üreten tümdevre bileşenleridir. Kimlik tanıma,, anahtar üretimi ve fikri mülkiyet (intellectual property - IP) koruması PUF devrelerinin üç ana kullanım alanını oluşturmaktadır. Kopyalanamamazlığın yanında eşsizlik ve sağlamlık da her PUF yapısının sağlaması gereken özellikler arasındadır. Bu bildiride PUF tipleri ve özellikleri özetlenmekte, halka osilatör (ring oscillator - RO) tabanlı bir PUF yapısının FPGA uygulaması sunulmakta ve sonuçlar PUF özellikleri bakımından tartışılmaktadır.

Abstract

Physical Unclonable Functions (PUFs) are circuit primitives that generate chip specific signatures depending on the uncontrollable components present in the manufacturing process. Authentication, key generation, and IP protection are three important usage areas of PUF circuits. Beside unclonability, uniqueness and robustness are the main properties that every PUF should provide. In this work, types and properties of PUF structures are summarized. An FPGA implementation of a ring oscillator (RO) based PUF structure is presented and results are discussed in terms of PUF properties.

1. Giriş

Tümdevreye özgü ve kopyalanamaz imza üretme kapasitesine sahip olan PUF yapıları ilk olarak 2001 yılında ortaya atılmıştır [1]. Kopyalanamamazlık özelliği, üretim sürecindeki kontrol edilemeyen eşik gerilimi, oksit kalınlığı, doping konsantrasyonu gibi bileşenlerden kaynaklanmakta ve bir tümdevredeki bu bileşenleri başka bir tümdevre için kopyalamak mümkün olmadığından üretilen imza da eşsiz ve tümdevreye özgü olmaktadır.

PUF yapılarının kullanıldığı üç temel alan bulunmaktadır. Bunlardan ilki kripto işlemlerinde kullanılan anahtarların üretimidir. Devrenin her açılışında üretilen bu anahtar ile görece pahalı olan uçucu olmayan bellek gereksinimi ortadan kalkmakta, eğer uçucu bellek kullanılıyorsa saklanan anahtarların kaybolmaması için sürekli besleme sağlayacak olan bataryaya gerek olmamaktadır. Bunlara ek olarak bir çok saldırı ihtimali doğuran özel anahtarların tümdevreye transferi ihtiyacı da ortadan kalkmakta ve özel anahtarlar tümdevreyi hiçbir şekilde terketmemektedirler. Anahtar üretiminin getirdiği bir başka avantaj da FPGA üzerinde yer alan IP'lerin şifreli olarak yüklenerek çalınmalarının önüne geçilebilmesidir. PUF yapılarının kullanılabileceği bir diğer alan ise tümdevre için kimlik üretmek ve kimlik tanımanın yapılmasıdır. Özellikle RFID uygulamalarında her tümdevrenin farklı bir kimliğinin olması gerekmekte, bu da yine flash yada eeprom gibi uçucu olmayan bellekler kullanarak sağlanmaktadır. PUF yapıları sayesinde bu pahalı yapılara gerek kalmamakta, her istendiğinde devre kimliği gerçek zamanlı üretilebilmektedir. Kendine bunlar gibi önemli alanlarda kullanım imkanı bulan PUF devrelerinin yakın gelecekte çok daha yaygın kullanılacağı öngörülmektedir.

Bu bildirinin kalanı şu şekilde organize edilmiştir. İkinci bölümde PUF'ların sahip olmaları gereken eşsizlik ve sağlamlık özellikleri açıklanmaktadır. Üçüncü bölümde RO PUF, Hakem PUF ve SRAM PUF devreleri özetlenmektedir. Dördüncü bölümde RO tabanlı bir PUF yapısının FPGA uygulaması sunulmaktadır. Beşinci bölümde uygulama sonuçları PUF gereksinimleri göz

önünde bulundurularak açıklanmakta, sonuç bölümü ile de bildiri sonlandırılmaktadır.

2. PUF Özellikleri

PUF yapılarının eşsizlik, sağlamlık, kopyalanamazlık ve tahmin edilemezlik olmak üzere 4 temel özelliği vardır. Bu özelliklerden herhangi biri bile sağlanmasa yapı PUF olarak adlandırılamaz. Bu özellikler aşağıda açıklanmıştır.

2.1. Eşsizlik

PUF'lar arası çeşitlilik olarak da bilinen eşsizlik özelliği, farklı tümdevrelerin aynı koşullarda farklı çıktılar üretmesi anlamına gelmektedir. İdealde iki PUF yapısının çıktıları ortalama olarak %50 değişik olmalıdır. Bu durum yapılar arasında ilintinin olmadığı anlamına gelmektedir. Eğer PUF'un eşsizlik özelliği zayıfsa gerekli sayıda tümdevreyi ayırd etmek için yeterli sayıda imza yada kimlik üretmek mümkün olmaz. Böyle bir durumda pratik olarak birden fazla tümdevrenin aynı kimliği yada imzayı üretme sorunu doğacaktır ve sistem başarısız olacaktır.

2.2. Sağlamlık

PUF içi çeşitlilik olarak da adlandırılan sağlamlık özelliği tek bir tümdevreden ardarda yapılan ölçümlerde gözlenen tutarlılıktır ve başarı kriteri değişen bit sayısıyla ters orantılıdır. İdeal durumda, doğru çalışan bir PUF'un ürettiği çıktılar hep aynı olmalı ve hiçbir bitin değeri farklı zamanlardaki ölçümlerde değişmemelidir. Ancak gerçekte, sıcaklık, nem, yaşlanma, besleme gerilimi gibi çevresel etkenlerdeki değişimlere bağlı olarak bazı bitler durum değiştirebilmektedir. Zaten PUF'ların çalışma prensibi de üretimdeki ufak farklara dayandığından çevresel koşullardaki değişimlerin bazı bitlerde bozulmalara yol açması kaçınılmaz olmaktadır. Bu durum gürültü olarak adlandırılmakta ve anahtar üretimi gibi hatasız veri gerektiren sistemlerde bir şekilde ortadan kaldırılması gerekmektedir. Oluşan gürültünün ortadan kaldırılması için hata düzeltme kodları gibi yaklaşımlar bulunmakla beraber bunlar sistemin maliyetini arttırdığından PUF tasarımcısının temel amacı mümkün olduğunca az hata yapan PUF devreleri tasarlamaktır.

2.3. Kopyalanamamazlık

Kopyalanamamazlık, PUF yapılarının en temel özelliklerinden biri olup birbirinin tıpatıp aynısı iki devre yapmanın pratikte mümkün olmadığı anlamına gelir. Bunun yanında PUF yapısının tam doğru bir matematiksel modelinin yapılmasının imkansızlığını da ifade eder. Bu özelliğin temelinde de üretimden kaynaklanan saçılımların kontrol edilememesi bulunmaktadır.

2.4. Tahmin Edilemezlik

PUF yapılarının çok önemli bir diğer özelliği de çıktılarının tahmin edilemez oluşudur. Bu prensibe göre devrenin şeması, serimi ve ortam koşulları dahi biliniyor olsa yine de çıktının tahmin edilemez olması gerekmektedir.

Tüm bu özelliklerin yanında PUF devresinin kullanımı kolay, entegre edilebilir, mümkün olduğunca hızlı, alan ve güç efektif olması beklenmektedir.

3. PUF Yapıları

3.1. Optik PUF

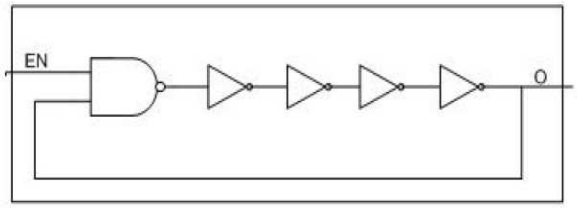
Optik PUF'lar tek yönlü fiziksel fonksiyonlar adıyla ilk olarak [1] ve [2]'de ortaya atılmıştır. Kabarcıklarla dolu transparan epoksiye tutulan lazerin yansımasıyla oluşan özgün şekil, devreye özgü bir tanımlama imkanı sağlamaktadır. Bu şekil, lazerin gücü, açısı, epoksinin kalınlığı ve özelliği gibi parametrelere bağlı olduğundan her bir devrede farklı oluşmaktadır. Bu da özgün anahtar yada kimlik oluşturulmasına olanak vermektedir.

3.2. RO PUF

RO-PUF, eş yapılar arasındaki gecikme farkına dayanmaktadır ve ilk olarak Gassend tarafından sunulmuştur [3,4]. Bu yapılarda devamlı osilasyon yapan devreler bulunmakta ve bir birine eş sayıda eleman barındıran devrelerin salınım frekansları karşılaştırılarak sonuç üretilmektedir. Frekansları karşılaştırılacak iki devreyi RO1 ve RO2 olarak adlandırırsak, RO1'in hızlı olduğu durumda '1' değeri üretiliyorsa RO2'nin hızlı olduğu durumda '0' değeri üretilir. Gerçekte PUF'un çok sayıda çıktı üretmesi gerektiğinden karşılaştırılacak RO'lar da bir kümeden çoğullayıcılar aracılığıyla seçilirler. Bu yapılarda frekansları karşılaştırma işi genel olarak sayıcılarla yapılmaktadır. Belli bir süre boyunca iki osilatör çıkışındaki darbeleri sayan sayıcıların çıkışları karşılaştırılmakta ve sonuç üretilmektedir. Örnek bir RO devresi Şekil 1'de gösterilmektedir.

RO-PUF'lar da diğer PUF yapıları gibi çevresel etkenlere çok duyarlıdır. Besleme gerilimi ve sıcaklıkta meydana gelen değişimler birbirine yakın frekanslarda salınan osilatörlerden hızlı olanın yavaş, yavaş olanınsa hızlı hale gelmesine neden olabilmekte ve hatalı bit

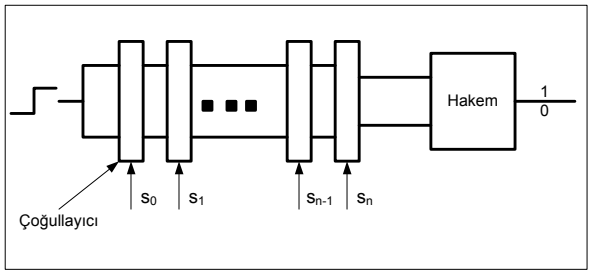
üretimi meydana gelebilmektedir. Bu problemi ortadan kaldırmak için ikiden fazla RO'yu gruplayıp frekansları birbirinden en uzakta olanları seçerek çıktı üretme kullanılan bir metottur [5]. Ancak alan açısından çok verimli olmadığı için kesin bir çözüm olarak görülmemektedir.



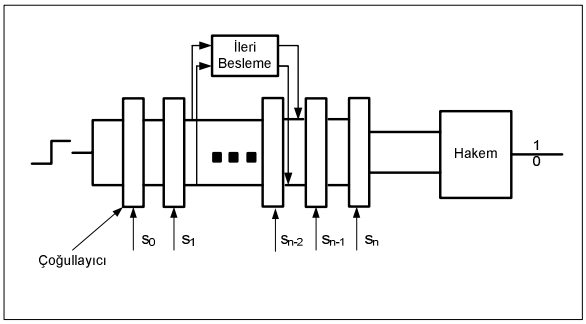
Şekil 1: Halka Osilatörü

3.3. Hakem (Arbiter) PUF

İlk hakem tipi PUF yapısı Lim tarafından sunulmuştur [6,7,8,9]. Bu yapıda belirli sayıda gecikme elemanı iki paralel ve eş hat oluşturacak şekilde peşpeşe bağlanmakta ve iki hatta aynı anda bir işaret uygulanmaktadır. Hatların sonunda yer alan bir hakem devresi hangi hattın daha hızlı olduğuna karar vererek Şekil 2'de gösterildiği gibi bir bitlik PUF çıktısı üretmektedir. Gecikme elemanı olarak *n* adet çoğullayıcı kullanıldığında uygulanacak seçme işaretine bağlı olarak 2^n farklı yol oluşturulabilmekte ve aynı devre ile çok sayıda PUF çıktısı üretilebilmektedir. Bu yapıların en zayıf tarafı, aynı devre farklı seçme işaretleri uygulanarak kullanılıyorsa modellenebilmesi ve farklı işaretler uygulandığında üretebileceği çıkışların tahmin edilebilir hale gelmesi, dolayısıyla PUF özelliğini yitirmesidir. Bu tip saldırılara karşı da Şekil 3'teki "ileri beslemeli hakem" diye adlandırılan yapı önerilmiştir [6]. İleri beslemeli hakem devresinde bazı gecikme elemanları bypass edilmektedir. Bu sayede yapılacak ölçümlerle sistemin modellenmesi zorlaştırılmakta ve PUF saldırılara karşı daha güçlü olmaktadır.



Şekil2: Hakem PUF

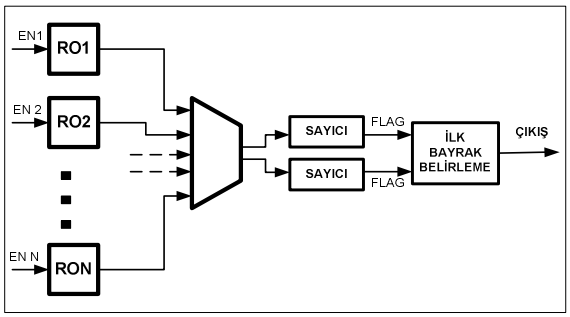


Şekil3: İleri beslemeli hakem PUF

4. RO Tabanlı PUF Gerçeklemesi

Optik PUF yapıları, silikon PUF'lara göre uygulanmaları ve kullanılmaları zor olduğundan ve FPGA'e uygun olmamaları nedeniyle tercih edilmemektedirler. Hakem PUF yapıları da ara bağlantılarının birebir aynı olmasının ancak tam özel serim tekniğiyle asic olarak tasarlanarak kullanılabilmeleri ve dolayısıyla FPGA'de uygulanmalarının mümkün olmamasından dolayı örnek olarak RO tabanlı PUF devresinin FPGA gerçeklemesi ele alınmıştır.

Bu kapsamda Gassend tarafından önerilen yapının iki farklı versiyonu [4], Xilinx 3S5000 devresi üzerinde gerçeklenmiştir. İki versiyonda da bir NAND kapısı ve dört eviriciden oluşan RO yapısı kullanılmıştır. Bu yapıda bir NAND hücresi ile osilasyon opsiyonel hale getirilmekte, böylece kullanılmayan RO devrelerinin gereksiz güç harcaması ve diğer çalışan RO'ları etkilemelerinin önüne geçilmektedir. PUF yapısının oluşturulabilmesi için bu RO yapısından çok sayıda yerleştirilmesi gerektiğinden ve bu yapıların birebir aynı olması beklendiğinden RO Hard Makro olarak tasarlanmıştır. Her iki RO-PUF versiyonunda da iki RO'nun çıkışları birer sayaca bağlı olup sayaçlardan hangisinin ilk olarak önceden belirlenen bir değere ulaştığına bakılarak bir bitlik PUF çıktısı üretilmektedir, Şekil 4. İlk versiyonda *n* bit PUF çıktısı için 2*n* adet RO kullanılmakta ve her bir RO sadece bir kez çalıştırılmaktadır. İkinci versiyonda ise *n* bit çıkış üretebilmek için *n*+1 RO kullanılmakta ve her bir RO iki yanındaki RO ile karşılaştırılmaktadır. Bu versiyonda tüm RO'lar ikişer kez kullanılmakta ve alan açısından daha verimli bir PUF yapısı ortaya çıkmaktadır.



Şekil4: RO-PUF bit üretme mekanizması

5. Ölçüm Sonuçları

128 bit PUF çıktısı üretmek üzere tasarlanan RO-PUF devrelerinden ilkinde 129 ikincisinde ise 256 adet RO kullanılmıştır. RO frekanslarının karşılaştırılabilmesi için 2 adet sayıcı ve ilk bayrak belirleme devresi de tasarımda yer almaktadır. Oluşan çıkışlar seri port aracılığıyla PC'ye gönderilmekte ve MATLAB programları ile analiz edilmektedir.

Eşsizlik testi için elimizde yeterince FPGA devresi olmadığından tasarım FPGA'in 25 farklı bölgesine yerleştirilmiş ve her birinden alınan çıktıların birbirlerinden ne derece bağımsız oldukları Hamming uzaklıkları incelenerek hesaplanmıştır.

Sağlamlık tesli için altı farklı sıcaklıkta, 0, 20, 40, 60, 80, 100 C^o 1000'er defa PUF çıktısı ölçülmüştür. Bu ölçümler iki farklı şekilde analiz edilmiştir. İlk analiz PUF'un normal şartlar altındaki (NŞA) davranışını görmek için sadece 20 C^o'de toplanan verilerle yapılmış ikinci analizde ise değişken sıcaklıklarda (DS) toplanan verilerin tamamı gözönüne alınarak hata oranları hesaplanmıştır.

Tablo 1: RO_PUF1 ve RO_PUF2 Analiz Sonuçları

Eşsizlik Analizi	**Bit Üretme Zamanı**	**Ölçüm Sayısı**	**Hamming Uzaklığı**	
RO_PUF1	82 µs	25	49,05	
RO_PUF2		25	49,55	
Sağlamlık analizi	**Bit Üretme Zamanı**		**Hata Oranı (NŞA)**	**HATA Oranı (DS)**
RO_PUF1	82 µs	1000	0,89	2,63
RO_PUF2	82 µs	1000	1,31	3,65

Her iki versiyon için de yapılan bu analiz sonuçları Tablo 1'de sunulmuştur. Eşsizlik testi için elde edilen sonuçların ideal değer olan %50'ye oldukça yakın olduğu gözlemlenmiştir. Her bir RO'nun ikişer kez kullanıldığı RO_PUF1 devresinde bu değerin biraz daha düşük olması entropinin az olmasıyla açıklanabilir. Sağlamlık testinde de beklendiği üzere bir miktar hata oluştuğu ve bu hataların sıcaklık değiştikçe arttığı gözlemlenmiştir. Elde edilen sonuçlar PUF yapılarının her ikisinin de doğru çalıştığı ve az miktarda hata yaptığını ortaya koymaktadır.

6. Sonuçlar

Fiziksel kopyalanamaz fonksiyonlar kimlik tanıma, anahtar üretimi ve IP koruması gibi alanlarda kolay çözümler sunmaktadırlar. Birkaç farklı tipi olan bu yapılardan halka osilatörü tabanlı PUF yapısı FPGA üzerinde gerçeklenmiş ve her PUF yapısının taşıması gereken eşsizlik ve sağlamlık özellikleri açısından analiz edilmiştir. Yapılan ölçümler tasarlanan devrenin PUF özellikleri taşıdığını ve gerekli görülen yerlerde kullanılabileceğini göstermiştir.

7. Kaynaklar

[1] R. S. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, 2001.

[2] R. S. Pappu, B. Recht, J. Taylor, N. Gershenfeld, "Physical one-way functions", Science, vol. 297, no. 6, pp. 2026-2030, 2002.

[3] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in ACM Conference on Computer and Communications Security CCS, pp. 148–160, 2002.

[4] B. Gassend, D. Clarke, M. Dijk, and S. Devadas, "Controlled physical random functions," in 18th Annual Computer Security Applications Conference (ACSAC), 2002.

[5] G. E. Suh, E. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation", ACM DAC, 2007.

[6] D. Lim, J.W. Lee, B. Gassend, G.E.Suh, M. Van Dijk, S. Devadas, "Extracting secret keys from integrated circuits" IEEE Transactions on VLSI Systems, 2005.

[7] B. Gassend, D. Clarke, M. Van Dijk, S. Devadas, D. Lim, "Identification and Authentication of Integrated Circuits", Concurrency and Computation: Practice & Experience. Vol. 16, no. 11, pp. 1077-1098. Sept. 2004.

[8] B. Gassend, D. Clarke, M. Van Dijk, S. Devadas, "Delay-Based Circuit Authentication and Applications", ACM symposium on Applied computing, 2003.

[9] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Dijk, S. Devadas, "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications". Symposium On VLSl Circuits Digest of Technical Papers, 2004.