Konvensiyonel ve Sıralama Tabanlı RO-PUF'ların Uygulanması ve Karşılaştırılması

Giray Kömürcü
Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
TÜBİTAK, 41470, Kocaeli, Türkiye
Email: giray.komurcu@tubitak.gov.tr

Ali Emre Pusane, Günhan Dündar
Boğaziçi Üniversitesi, Elektrik, Elektronik Müh.
34342 Bebek, İstanbul, Türkiye
Email: {ali.pusane, dundar}@boun.edu.tr

***Özet* - Fiziksel Klonlanamaz Fonksiyonlar (PUF) üretim sırasındaki kontrol edilemeyen süreçlere dayalı olarak tümdevreye özgü imza üreten yonga bileşenleridir. Asıllama, kimlik üretimi, anahtar üretimi ve IP koruması, PUF devrelerinin üç ana kullanım alanını oluşturmaktadır. Klonlanamamanın yanında, eşsizlik ve sağlamlık her PUF yapısının sağlaması gereken özellikler arasındadır. Bu bildiride ilk olarak hata düzeltme kodları (ECC) bloğu ile birlikte konvensiyonel Ring Osilatörü (RO) PUF gerçeklemesi anlatılmaktadır. Devamında, sıralama tabanlı bir RO-PUF uygulaması sunulmaktadır. Son olarak, iki sistem performansları açısından karşılaştırılmakta ve avantajları ile dezavantajları tartışılmaktadır.**

***Anahtar Kelimeler*-PUF, Fiziksel Klonlanamaz Fonksiyonlar, Eşsizlik, Sağlamlık, Ring Osilatörü, FPGA, Anahtar Üretimi.**

***Abstract* - Physical Unclonable Functions (PUFs) are security primitives that have the capability of chip specific signatures on the fly depending on small mismatches present in the manufacturing process. Key generation, IP protection, authentication, and ID generation are the main usage areas of PUF circuits. Beside unclonability, uniqueness and robustness are two other key features that each PUF circuit should provide. In this work, conventional PUF circuits with Error Correction Codes (ECC) are summarized. Then, Ordering-Based RO-PUFs are presented. Finally, two system is compared in terms of performances and their advantages and disadvantages are discussed.**

***Keywords*-PUF, Physical Unclonable Functions, Uniqueness, Robustness, Ring Oscillator, FPGA, Key Generation.**

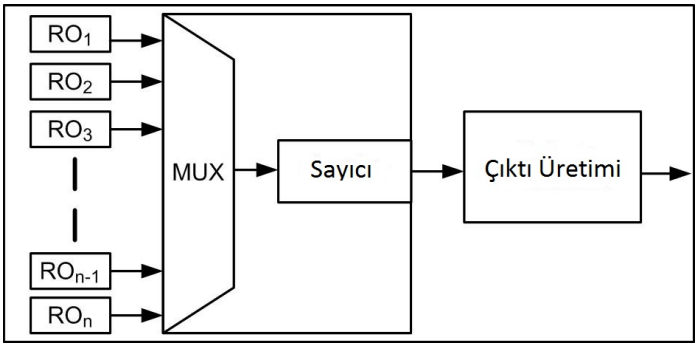
I. GİRİŞ

Tümdevreye özgü ve klonlanamaz imza üretme kapasitesine sahip olan Fiziksel Klonlanamaz Fonksiyon (PUF) yapıları ilk olarak 2001 yılında ortaya atılmıştır [1], [2]. Klonlanamama özellikleri üretim sürecindeki kontrol edilemeyen eşik gerilimi, oksit kalınlığı, doping konsantrasyonu gibi bileşenlerden kaynaklanmaktadır ve bir tümdevredeki bu bileşenleri başka bir tümdevre için kopyalamak mümkün olmadığından üretilen imza eşsiz ve tümdevreye özgüdür [3].

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 ihtiyacı ortadan kalkmakta yada uçucu bellekte saklanan anahtarların kaybolmaması için sürekli besleme sağlayacak olan bataryaya olan gereksinim ortadan kalkmaktadır [4]. Bunlara ek olarak bir çok saldırı ihtimali doğuran özel anahtarların tümdevvreye 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 alansa tümdevre için kimlik üretmek ve otantikasyon sağlamaktır. 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 anında üretilebilmektedir. Kendine bunlar gibi önemli alanlarda kullanım imkanı bulan PUF devrelerinin yakın gelecekte çok daha yaygın kullanılacağı öngörülmektedir.

Bugüne kadar geliştirilen PUF yapılarının başında Arbiter PUF, SRAM PUF, Ring Oscillator (RO) PUF, Butterfly PUF ve Glitch PUF gelmekte olup, silikon üzerine uygulanabilir olmaları nedeniyle kullanışlı ve ekonomiktirler [5]–[9]. Genel olarak gürültüye duyarlı olan PUF yapılarının oluşturduğu bit dizileri %100 doğru sonuç isteyen anahtar üretimi gibi uygulamalarda kullanılmadan önce Hata Düzeltme Kodları (ECC) ile hatasız hale getirilmektedir. Buna karşın sıralama tabanlı RO-PUF yapıları %100 doğru bit dizileri üretme kapasitesine sahiptir.

Gerek FPGA uyumlulukları, gerekse değişken koşullar altında güvenilir çalışmaları itibariyle RO-PUF'lar anahtar üretimine en uygun PUF çeşitlerindendir [10], [11]. Konvensiyonel RO-PUF'lar iki adet eş RO'nun frekanslarını karşılaştırarak 1 bit veri üretirler. Uygulamalar belli uzunlukta bit dizisi üretimi gerektirdiğinden aynı anda belli sayıda RO sistemde kullanılır ve ikişer ikişer frekansları karşılaştırılarak ihtiyaç duyulan dizi üretilir. Sıralama tabanlı RO-PUF'ların çalışma prensibi ikiden fazla sayıda RO'nun gruplanarak frekanslarının karşılaştırılması ve çıktı üretilmesine dayanır. Burada önemli olan gruplama adımında frekans olarak birbirinden uzak RO'ların seçilip dış etkenlere bağlı olarak frekans sıralamalarının değişimi ve dolayısı ile bit dizisinin hatalı üretilmesinden kaçınılmasıdır. Bu gruplama doğru şekilde yapılabildiği takdirde %100 doğru bit dizilerinin ECC bloklarına ihtiyaç duyulmadan üretilmesi mümkün olmaktadır. Bu avantajının yanında, sıralama tabanlı RO-PUF'lar yüksek



Şekil 1. Konvensiyonel RO-PUF'ların Blok Yapısı.

entropi üretim yetenekleri ile kullanılacak RO sayısının da azaltılması, dolayısı ile alan, zaman ve güç açısından da avantajlı PUF devrelerinin üretilmesini sağlamaktadırlar [12], [13].

Bu çalışmada bizim temel amacımız, konvensiyonel ve sıralama tabanlı RO-PUF'ların uygulama örneklerini sunmak ve performanslarını karşılaştırmaktır. Bu amaçla, ilk olarak II. bölümde bir adet konvensiyonel RO-PUF yapısı ECC bloğu ile birlikte sunulmaktadır. III. bölümde sıralama tabanlı RO-PUF uygulaması anlatılmaktadır. IV. bölümde iki farklı RO-PUF yapısı performansları itibariyle karşılaştırılmakta, avantajları ve dezavantajları tartışılmaktadır. V. bölüm ile bildiri sonlandırılmaktadır.

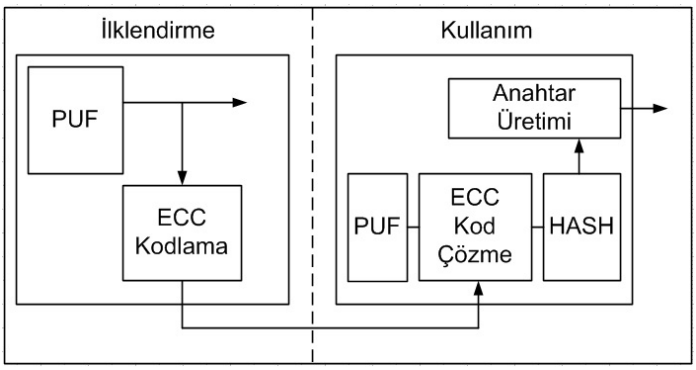
II. Konvensiyonel RO-PUF'ların ve Hata Düzeltme Kodlarının Uygulanması

Konvensiyonel RO-PUF'ların blok yapısı Şekil 1'de sunulmaktadır. Şekilden de görülebileceği gibi ilk olarak uygulanan RO'ların frekansları belirlenmekte ve bu frekanslar kullanılarak bit çıktıları oluşturulmaktadır. Frekans belirleme işlemi hem konvensiyonel hem de sıralama tabanlı PUF'larda kullanılmakta olup, genelde sayıcı ve çoğullayıcı ile gerçekleştirilmektedir. Bu adımda, belli bir zaman dilimi boyunca tüm RO'ların salınım sayıları belirlenmektedir. Önerilen sistemde, bir çoğullayıcı ve sayıcı kullanılarak RO'lar teker teker seçilir ve frekansları belirlenir. Bu kapsamda 96, 128, 160, 192, 222 ve 256 RO'dan oluşan altı adet örnek sistem uygulaması yapılmıştır. Bu sistemlerin alan karşılaştırmaları Xilinx Virtex5 FPGA'ler için yapılmış ve Tablo I'de sunulmuştur. Tablodan da görülebileceği üzere önerilen frekens belirleme devresinin maksimum çalışma frekansı 430 MHz olmaktadır. Bu frekans da 5 katmanlı RO'ların salınım frekansından önemli ölçüde yüksek olduğu için çalışma sorunsuz olarak sağlanabilmektedir. Frekans belirleme adımından sonra gelen çıktı üretme adımı da bir karşılaştırıcıdan oluşmakta olup Virtex5 cihazlarda 5 slice kullanılarak gerçeklenebilmektedir.

Konvensiyonel RO-PUF'lar ile %100 güvenilir çıktı üretmek için gerekli son blok ECC'dir. ECC'nin PUF uygulamalarındaki kullanımcı Şekil 2'de gösterilmektedir. Şekilden de görülebileceği üzere, ilklendirme fazında PUF çıktısı ECC kodlayıcıya aktarılmakta ve yardımcı veri üretilerek

Tablo I
Frekans Belirleme Devresinin Virtex5 Cihazlarda Alan Kullanımı.

FPGA Tipi	96 RO	128 RO	160 RO	192 RO	224 RO	256 RO
Virtex5	31	44	44	57	62	68



Şekil 2. Konvensiyonel RO-PUF'lar ile Anahtar Üretim Şeması.

veri tabanına kaydedilmektedir. Kullanım fazında ise ECC kod çözücü o anda kendisine gelen gürültülü PUF çıktısını yardımcı veriyi kullanarak düzeltmektedir. Bose, Chaudhuri, and Hocquenghem (BCH) kodları çok sayıda hatalı biti bulunan verileri düzeltme garantisi ile PUF devrelerinde kullanıma uygun bir ECC algoritmasıdır [14]. Bu çalışmada BCH kodları uygulanmış, alan ve zaman performansları analiz edilmiştir.

Birden fazla hata düzeltme yeteneğine sahip ECC algoritmalarının kapasiteleri üç bileşenli bir notasyon ile gösterilmektedir, (a, b, c). Bu formatta a düzeltilecek veri ve yardımcı veri bitlerinin sayısını, b veri bitlerinin sayısını, c de ECC algoritmasının gürültülü bir veride düzeltebileceği maksimum hatalı bit sayısını simgelemektedir. Düzeltilecek maksimum hatalı bit sayısı arttıkça, ECC bloğunun hem kodlayıcı hem de kod çözücü birimlerin karmaşıklığı, dolayısı ile de alan, zaman ve güç tüketimi artmaktadır.

ECC gerçeklemesinin PUF sistemi üzerine getireceği alan artışının belirlenebilmesi için farklı hata düzeltme kapasitelerine sahip BCH kodlayıcı ve kod çözücüler gerçeklenmiş ve alan kullanımları analiz edilmiştir. İncelenen tüm sistemlerde a bileşeni 255 bit olarak seçilmiştir. Sonuçlar Tablo II'de sunulmaktadır. Sonuçlar incelendiğinde, beklendiği gibi hata düzeltme kapasitesi arttıkça alan kullanımının da arttığı görülmektedir. Örneğin, Virtex5 cihazlarda 3 bit düzeltme kapasiteli BCH kod çözücü 148 slice yer kaplarken 18 bit hata düzeltme kapasiteli kod çözücü 427 slice yer kaplamaktadır. Gerçeklenen RO-PUF devresinin 18 bite kadar hata yapabileceği bilindiğinden $(255, 131, 18)$ BCH kodlayıcı ve kod çözücünün kullanılması ideal çözüm olarak görülmektedir [15].

Tablo II
VIRTEX5 CIHAZLARDA GERÇEKLENEN HATA DÜZELTME KODLARININ ALAN KULLANIMI.

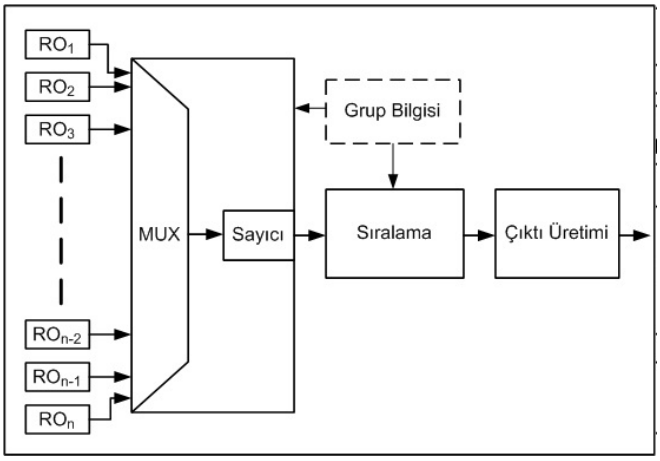
Hata Düz. Kap.	**(255, 231,3)**	**(255, 207,6)**	**(255, 187,9)**	**(255, 163,12)**	**(255, 139,15)**	**(255, 131,18)**
Enc. Vir.	17	19	21	25	33	33
Dec. Vir.	148	178	272	288	363	427

III. SIRALAMA TABANLI RO-PUF'LARIN GERÇEKLENMESI

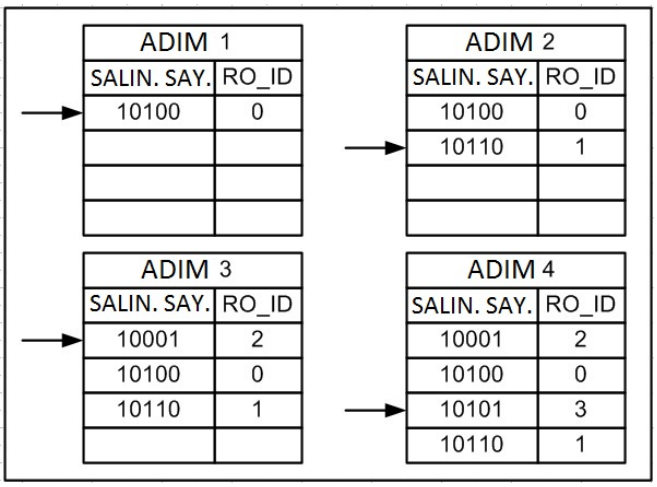
Daha önceden de belirtildiği gibi sıralama tabanlı RO-PUF'ların temel avantajı %100 güvenilir veri üretimini yüksek entropi kullanımı ile sağlamasıdır. Her ne kadar belirli bir uzunluktaki PUF çıktısının üretimi için gerekli RO sayısı sıralama tabanlı RO-PUF'larda konvensiyonel yapılara göre önemli ölçüde azalsa da, daha doğru bir analizin yapılabilmesi için çıktı üretim bloklarının da gerçeklenmesi ve alan ve zaman bakımından performans analizlerinin yapılması faydalı olacaktır. Bu amaçla, sıralama ve çıktı üretme yapıları geliştirilmiş ve farklı sayıda RO ve grup büyüklükleri için gerçeklenmiştir.

Sıralama tabanlı RO-PUF'lar için geliştirilen çıktı üretim mekanizması Şekil 3'te gösterilmektedir. Bu yapıya göre, gruplama adımının ilklendirme fazında PC tarafından yapılıp tümdevre üzerinde yada dışarıdaki bir hafızada tutulacağı yada tümdevre üzerindeki bir mikroişlemci tarafından gerçekleştirileceği öngörülmektedir. Bir grup içindeki RO'lara ait frekansların sıralanması ve bu sıralamaya göre çıktı üretilmesi sıralama tabanlı RO-PUF'ların zorunlu adımları olup, sistemin performansı ve maliyeti açısından kritik öneme sahiptir. Bu adımda gerekli fonksiyonlar varolan bir mikroişlemci yada bu işler için özel olarak tasarlanıp tümdevre üzerinde gerçeklemiş donanımlar tarafından yapılabilir. Sistemde bir mikroişlemcinin bulunmadığı varsayımıyla bu fonksiyonlara özel donanımlar tasarlanmış ve gerçeklenmiştir. Bu tasarıma göre RO'lara ait salınım sayılarının belirlenmesi ardışıl olarak yapılmaktadır. Herbir RO numarası ve RO'ya ailt salınım sayıları, bu sayılar küçükten büyüğe bir sıra oluşturacak şekilde kütüklerde tutulmaktadır. 4 RO'ya ait sıralama işlemi Şekil 4'te gösterilmiştir. Bu işlem için harcanan zaman m adet RO içeren bir grup için $m^2/2$ ile sınırlıdır. Ancak sıralama işlemi frekans belirleme işlemi ile aynı anda gerçekleştirilebildiği için sadece son grubun sıralama işlemi sistemin hızını düşürmektedir.

Sıralama tabanlı RO-PUF'ların çıktı üretme işlemi her bir sıralamanın farklı bir bit dizisiyle eşleştirilerek, ardışıl devreler ile gerçeklenmiştir. Bu adımda RO numarası ve sıralama bilgisi beraber kullanılır. Çıktı üretme işleminin pseudo kodu Algoritma 1'de sunulmuştur. 4 RO içeren bir grup için bu işlem Şekil 5'te gösterilmektedir. Sıralama devresinin çalışma zamanı m RO için m ile sınırlıdır. Sıralama işlemine benzer şekilde, sadece son grubun çıktı üretme zamanı sistemin hızını düşürmektedir.



Şekil 3. Sıralama Tabanlı RO-PUF'ların Blok Yapısı.



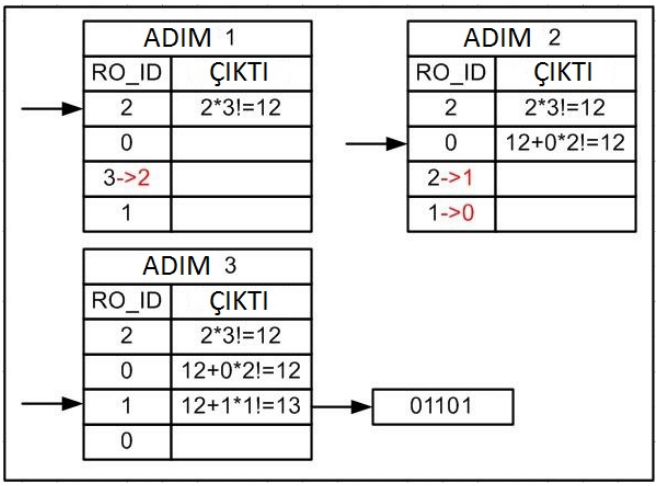
Şekil 4. Sıralama Devresi Örnek Çalışması.

IV. UYGULAMA SONUÇLARI VE ANALIZI

Her bir RO'nun tek tek ölçülmesi birbirlerine kilitlenmelerinin önüne geçtiği için doğru bir tasarım uygulaması olduğundan, bir adet sıralama belirleme ve çıktı üretme bloğu sıralama tabanlı RO-PUF'lar için yeterlidir. Ancak bu blokların sistemde ortaya çıkabilecek en büyük RO grubuna göre gerçeklenmesi gerekir.

Bu mettota, grup büyüklükleri için bir üst sınır belirlenir ve gruplama adımında bu üst sınır dikkate alınarak gruplar oluşturulur. Bu çalışmada, önerilen sıralama ve çıktı üretme devreleri 3'ten 10'a kadar sayıda RO içeren grup büyüklükleri için gerçeklenmiş ve Virtex5 cihazlardaki alan kullanımları Tablo III'te sunulmuştur. Tablodan görülebileceği üzere, gruplar büyüdükçe devreler için gereken kaynaklar da önemli ölçüde artmaktadır.

Konvensiyonel ve sıralama tabanlı RO-PUF'lar kullanılarak 128 bit çıktı üretmek için gerekli alan, farklı maksimum grup uzunluklarına göre belirlenmiş ve Tablo III ile Şekil 6'da gösterilmiştir. Bu sonuçlara göre, izin verilen maksimum grup büyüklüğü arttıkça entropi kullanımı da arttığından gereken



Şekil 5. Çıktı Üretimi Örnek Çalışması.

Data:
Bir gruptaki RO numaralarının frekanslarına göre sıralanmış listesi, $RO[m]$.
Result: çıktı.
for $i \leftarrow 1$ **to** $m-1$ **do**
  çıktı = çıktı + RO[i]*(m-i)!
  for $j \leftarrow i$ **to** $m-1$ **do**
    if *RO[i] < RO[j]* **then**
      Azalt RO[i]
    end
  end
end

Algorithm 1: Çıktı Üretimi Pseudo Kodu.

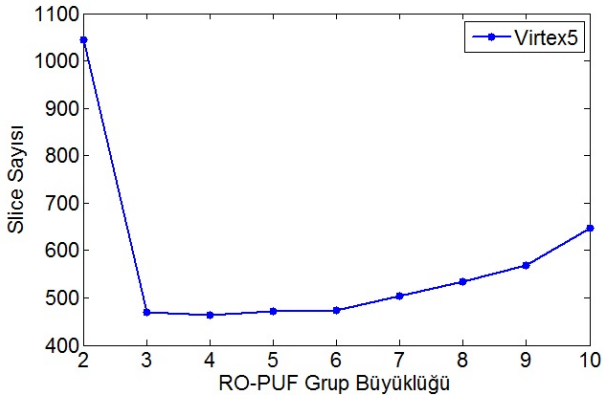
RO sayısı düşmektedir. Sunulan sonuçlar Matlab analiziyle belirlenmiş olup güvenli olarak sunulabilmeleri için yukarı doğru yuvarlanmışlardır. Gerçekleme sonuçlarına göre maksimum 4 RO'lu grupların kullanıldığı sıralama tabanlı RO-PUF kullanımının ideal çözüm olduğu ortaya çıkmaktadır. Grupları daha fazla büyütmenin, sıralama ve çıktı üretme devrelerinin alan kullanımı arttığından sistem performansına faydası olmamaktadır. Bunların yanında, konvensiyonel RO-PUF gerçeklemesinin alan kullanımının ECC bloğu nedeniyle ciddi miktarda fazla olduğu da gözden kaçırılmamalıdır. Ancak bu adım %100 doğru sonuç gerektirmeyen uygulamalarda elimine edilebilir.

V. SONUÇ

Sıralama tabanlı RO-PUF'lar %100 doğru çıktı üretim yetenekleri, yüksek entropi kullanımları ve FPGA ortamına uyumlulukları ile gelecek vaat eden yapılardır. Ancak bu çalışmaya kadar tüm bileşenleriyle tam bir gerçeklemeleri yapılmamıştır. Bu nedenle de konvensiyonel RO-PUF'larla adil bir karşılaştırma yapılması mümkün değildi. Bu çalışmada konvensiyonel ve sıralama tabanlı RO-PUF'ların alan kullanımları araştırılmıştır. Analiz sonuçlarına göre sıralama tabanlı RO-PUF'ların küçük RO grupları kullanılarak %100 doğru çıktı üretimi için optimum çözümü sundukları belirlenmiştir. Bu yapılar sayesinde hem ECC bloklarına olan gereksinim ortadan kalkmakta hem de devrenin alan, zaman ve güç bakımından performansı iyileşmektedir.

Tablo III
RO-PUF'LARIN VIRTEX5 CIHAZLARDAKI ALAN KULLANIMI.

PUF Tipi	RO Say	RO Slice	Fr. Bel. Slice	Sır. Slice	Çıktı Ü. Slice	ECC Slice	Toplam Slice
Conv.	256	512	68	0	5	460	1045
OB(3)	195	390	62	10	7	0	469
OB(4)	185	370	57	26	10	0	463
OB(5)	175	350	57	49	15	0	471
OB(6)	170	340	57	54	23	0	474
OB(7)	165	330	57	71	45	0	503
OB(8)	160	320	44	114	56	0	534
OB(9)	155	310	44	117	98	0	569
OB(10)	150	300	44	181	123	0	648



Şekil 6. RO-PUF'ların Alan Kullanımı.

KAYNAKLAR

[1] R. S. Pappu, "Physical one-way functions." Ph.D. dissertation, Massachusetts Institute of Technology, Massachusetts, 2001.
[2] R. S. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 6, pp. 2026–2030, 2002.
[3] A. Maiti, L. McDougall, and P. Schaumont, "The impact of aging on an FPGA-based physical unclonable function," in *International Conference on Field Programmable Logic and Applications (FPL)*, 2011, pp. 151–156.
[4] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Design Automation Conference (DAC)*, 2007, pp. 9–14.
[5] D. Lim, J. Lee, B. Gasend, G.E.Suh, M. V. Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Transactions on VLSI Systems*, vol. 13, no. 10, pp. 1200–1205, 2005.
[6] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas, "Delay-based circuit authentication and applications," in *ACM Symposium on Applied Computing*, 2003, pp. 294–301.
[7] B. Gassend, "Physical random functions," M.S. Thesis, Massachusetts Institute of Technology, Massachusetts, 2003.
[8] J. Guajardo, S. Kumar, G. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *18th Annual Computer Security Applications Conference (CHES)*, vol. 4727, 2007, pp. 63–80.
[9] D. Suzuki and K. Shimizu, "The glitch PUF: A new delay-PUF architecture exploiting glitch shapes," in *Cryptographic Hardware and Embedded Systems (CHES)*, 2010, pp. 366–382.
[10] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *Journal of Cryptology*, vol. 24, no. 2, pp. 375–397, 2011.

[11] C. Yin and G. Qu, "Temperature aware cooperative ring oscillator PUF," in *IEEE International Workshop on Hardware Oriented Security and Trust (HOST)*, 2009, pp. 36–42.

[12] C. Yin and G. Qu, "LISA: Maximizing RO-PUF's secret extraction," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2010, pp. 100–105.

[13] G. Komurcu, A. E. Pusane, and G. Dundar, "Dynamic programming based grouping method for RO-PUFs," in *9th Conference on Ph. D. Research in Microelectronics and Electronics (PRIME)*, 2013, pp. 329–332.

[14] W. W. Peterson, "Encoding and error-correction procedures for the bose-chaudhuri codes." *IRE Transactions on Information Theory*, vol. 6, no. 4, pp. 459–470, 1960.

[15] G. Komurcu and G. Dundar, "Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs," in *IEEE 10th International New Circuits and Systems Conference, (NEWCAS)*, 2012, pp. 73–76.