Sahada Programlanabilir Analog Diziler Üzerinde Gerçeklenen Lojistik Denklemiyle Rastsal Sayı Üretimi

Random Number Generation Using Field Programmable Analog Array Implementation of Logistic Map

İhsan Çiçek[1,2], Ali Emre Pusane[2], Günhan Dündar[2]
[1]TÜBİTAK BİLGEM UEKAE, Kocaeli
[2]Elektrik ve Elektronik Mühendisliği Bölümü,
Boğaziçi Üniversitesi, İstanbul
Email: ihsan.cicek@uekae.tubitak.gov.tr, ali.pusane@boun.edu.tr, dundar@boun.edu.tr

***Özetçe* —Rastsal sayı üreteçleri bağımsız ve eş dağılımlı, tahmin edilemez sayılar üreten kriptografik bileşenlerdir. Bu çalışmada tek boyutlu kaotik lojistik fonksiyonunun rastsal sayı üreteci olarak kullanımı gerçekleştirilmiştir. Lojistik denkleminin doğrusal olmayan dinamiği, istatistiksel ve spektral özellikleri sayısal benzetimler yardımıyla incelenmiştir. Ayrık zamanlı çalışan sahada programlanabilir analog dizi tümdevresi üzerinde gerçeklenen lojistik fonksiyonundan rastsal sayılar üretilmiş ve NIST800.22 istatistiksel testleri uygulanarak lojistik fonksiyonunun rastsal sayı üretim performansı değerlendirilmiştir.**

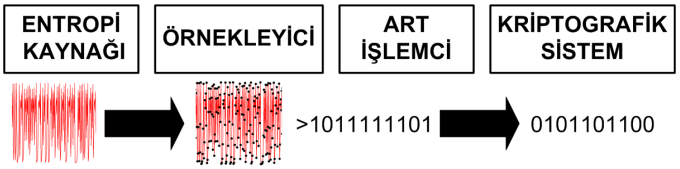
Anahtar Kelimeler*—*Lojistik fonksiyon, Sahada programlanabilir analog diziler, Ayrık zamanlı kaos.

***Abstract*—Random number generators are cryptographic components that generate unpredictable, independent and identically distributed bits. We studied 1D chaotic logistic map in the context of random number generation. Nonlinear dynamics of the logistic map, its statistical and spectral features are studied using numerical simulations. Logistic map based random number generator is implemented on a discrete time operating field programmable analog array chip. We evaluated the random number generation performance of our design using NIST 800.22 statistical tests.**

Keywords*—*Logistic function, Field programmable analog arrays, Discrete time chaos.

I. GİRİŞ

Kriptografik sistemlerde hiçbir belirlenimci blok çıkışında girişindekinden daha fazla entropi üretemez[1]. Bu nedenle sistemin tahmin edilemezliği rastsal sayı üreteceninkiyle (RSÜ) sınırlıdır. Güvenlik için yüksek entropiye sahip sayılar üretebilen bir RSÜ bileşenine ihtiyaç vardır. Bir rastsal sayı üreteci Şekil 1'de gösterildiği gibi üç bileşenden oluşur: Entropi kaynağı, örnekleyici ve art işlemci.



Şekil 1. Genel rastsal sayi üreteç bileşenleri.

Entropi kaynağı tahmin edilmesi olanaksız, ısıl gürültü, çığ gürültüsü, osilatör seğirtimi gibi fiziksel olaylara dayanır ve rastsal sayıların kaynağını oluşturur. Örnekleyici entropi kaynağından periyodik ya da aperiyodik edinilen ayrık örnekleri sayısallaştıran bileşendir. Örnekleyici bileşeni, entropi kaynağının istatistiksel özellikleri gözönüne alınarak tasarlanır. Uygulamada üretim hataları nedeniyle entropi kaynakları ideal olmayan istatistiksel özelliklere sahip olmaktadırlar. Bu durum, genelde üretilen bitlerde sıfır/bir oranının ideal değeri olan 0.5'ten sapma olarak kendini gösterir. Art işlemci bileşeni uygulamada üretim hataları ya da toleransları nedeniyle karşılaşılan istatistiksel sapmaları gidermek amacıyla kullanılırlar. Sayısal olarak gerçeklenen art işlemcilerin en yaygın kullanılanları XOR fonksiyonu ve Von Neumann algoritmasıdır. Art işlemci sıfır/bir oranındaki istatistiksel sapmaları gidererek bu oranı ideal orana yaklaştırır ancak bunu yaparken veri kaybı kaçınılmaz olduğu için bit üretim hızı örnekleme hızından daha düşük olur. Örneğin XOR fonksiyonunun art işlemci olarak kullanıldığı bir durumda işlenen her iki bir için bir bitlik çıkış oluşturulduğundan bit üretim hızı yarıya düşmektedir.

Kaos, dinamik sistemlerin kontrol parametrelerinin almış olduğu değerlere göre sergilediği düzensiz ve karmaşık bir davranış şeklidir. Kaos, başlangıç koşullarına hassas bağımlılık

Bu çalışmayı destekleyen TÜBİTAK BİLGEM'e teşekkür ederiz.

978-1-4673-5563-6/13/$31.00

ve aperiyodik salınım üretebilme özelliği nedeniyle RSÜ uygulamalarında entropi kaynağı olarak kullanılabilmektedir[2], [3]. Kaosun göstergesi de sayılan ve dinamik sistemi karakterize eden pozitif Lyapunov üsteli nedeniyle başlangıç koşullarındaki en küçük bir hata, zamanda evrilen sistemde büyük sapmalara neden olmaktadır. Bu ıraksak karakter, kaotik sistemlerin uzun vadeli kestirimlerini olanaksızlaştırır. Teoride belirlenimci yapısı nedeniyle tahmin edilebilir olan kaotik RSÜ'lerin uygulamada tahmin edilemezliği, başlangıç koşullarının ısıl gürültü nedeniyle sürekli değişmesine ve bunları sonsuz bir kesinlikle ölçmenin mümkün olmamasına dayanmaktadır. Kaotik sistemleri çalışma şekillerine göre sürekli zaman ve ayrık zaman olarak ikiye ayırmak mümkündür. Sürekli zaman kaotik sistemlerde sistemin evrimi durum değişkenlerinin birim zamandaki değişim oranına bağlıdır. Ayrık zamanlı kaotik sistemlerde ise durum değişkenlerininin değerlerine bağlıdır. Kaotik sistemler başlangıç koşullarına hassas bağlılık gösterseler de uzun vadeli istatistiksel özellikleri başlangıç koşullarından bağımsız olmaktadır [4].

Tek boyutlu kaotik lojistik fonksiyonunun entropi kaynağı olarak kullanıldığı bu çalışmada, lojistik fonksiyonunun istatistiksel ve spektral özellikleri gerçekleştirilen sayısal benzetimlerle karakterize edilmiştir. Entropi kaynağı lojistik fonksiyonu olan bir rastsal sayı üreteci sahada programlanabilir analog dizi (SPAD) tümdevresi üzerinde gerçeklenmiştir. Gerçeklenen sistemden edinilen sayısal veriye NIST800.22 istatistiksel testleri uygulanarak lojistik fonksiyonunun rastsal sayı üretim performansı değerlendirilmiştir.

II. LOJİSTİK FONKSİYONUNUN KAOTİK, İSTATİSTİKSEL VE SPEKTRAL ÖZELLİKLERİ

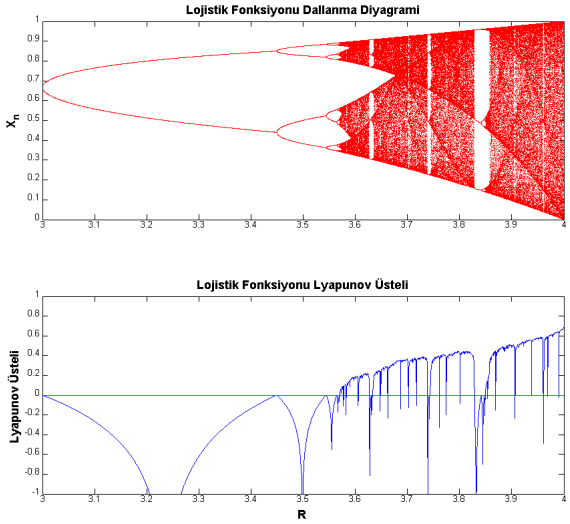
Lojistik fonksiyonu, biyolojik popülasyonların nüfus dinamiğini modellemek amacıyla literatüre ilk olarak 1838'de P. F. Verhulst tarafından sunulmuştur[5]. Lojistik denkleminin çok karmaşık davranışlar sergileyebildiği ise 1976 yılında keşfedilmiştir[6]. Matematiksel sadeliği ve zengin dinamik içeriği nedeniyle kaos teorisinin üzerinde en çok çalışılan popüler denklemlerinden biri olan ayrık zamanlı lojistik fonksiyonu,

$$x(n+1) = Rx(n)(1-x(n)) \tag{1}$$

şeklinde ifade edilebilir. R lojistik denkleminin kontrol parametresidir. Lojistik denklemi zamanda bir $x(0)$ ilk değerinden başlayıp zamanda evrilerek matematiksel olarak

$$Y_n = \{x(0), x(x(0)), ..., x^n(x(0))\} \tag{2}$$

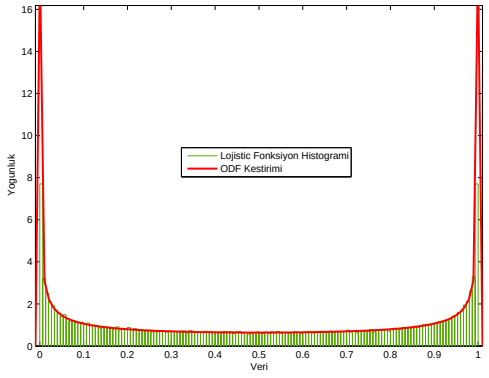
şeklinde tanımlanabilecek bir yörünge üretir. Denklem, R parametresinin değerine göre Şekil 2'de gösterildiği gibi degişik dinamik davranışlar sergileyebilmektedir. Lojistik fonksiyonunun R parametresine göre dinamik davranışı Şekil 2'deki dallanma diyagramında gösterilmiştir. $R = 3.57$ değerinden sonra kaotik rejime geçildiği gözlenebilir. Denklemin kaosta olduğu bölgelerde $Lyapunov$ üstelinin pozitif değer aldığı, dallanma grafiğiyle eş eksenli olarak çizdirilen grafikte görülmektedir. Pozitif $Lyapunov$ üsteli, dinamik sistemin kaotik rejimde çalıştığının belirtecidir ve lojistik denklemi için en yüksek değerini $(\lambda = 0.6931)$ $R = 4$'te almaktadır. Kaotik sistemin üreteceği entropi $Lyapunov$ üsteliyle orantılıdır[7]. Bu nedenle denklemin üretebileceği entropi en büyük değerini sistemin en kaotik davranacağı $R = 4$'te almaktadır.



Şekil 2. Lojistik denkleminin dallanma ve $Lyapunov$ üsteli grafiği.

Rastsal sayı üretiminde kullanılacak entropi kaynağının istatistiksel özelliklerine göre örnekleme yöntemi tasarlanacağı için lojistik denkleminden üretilen zaman serisinin istatistiksel özellikleri incelenerek olasılık dağılım fonksiyonu, numerik benzetim ve en büyük olabilirlik kestirim yöntemiyle belirlenmiştir. Kaotik sistemlerin uzun vadeli istatistiksel özelliklerinin başlangıç koşullarından bağımsız olduğu bilinmektedir [4].

Lojistik denkleminin olasılık dağılım fonksiyonunu belirlemek amacıyla rastsal bir ilk koşuldan başlayarak 10^5 örneklik numerik benzetim yapılmıştır. Denklemin ürettiği zaman serisine ait verinin normalize histogramı kullanılarak olasılık dağılımı Şekil 3'teki gibi elde edilmiştir.



Şekil 3. $R = 4$ için histogram ve olasılık yoğunluk fonksiyonu.

Deneysel dağılımın beta dağılımına olan benzerliği nedeniyle en büyük olabilirlik kestirim yöntemi kullanılarak beta dağılımına ait şekil parametreleri $\alpha = 0.5, \beta = 0.5$, olarak elde edilmiştir. Şekil ve değer kümesi parametreleri $p = 0, q = 1$,

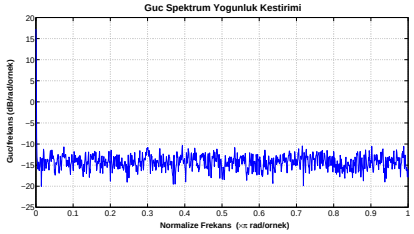
$$f_x(x) = \frac{(x-p)^{\alpha-1}(q-x)^{\beta-1}}{(q-p)^{\alpha+\beta-1}\int_0^1 t^{\alpha-1}(1-t)^{\beta-1}dt}, \quad x \in [p,q], \quad \alpha,\beta > 0 \tag{3}$$

şeklinde verilen genel beta olasılık dağılım fonksiyonunda yerine konarak lojistik denkleminin analitik olasılık dağılım fonksiyonu,

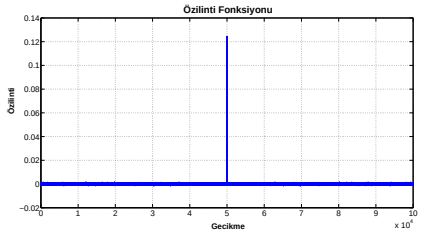
$$f_x(x) = \frac{1}{\pi\sqrt{x(1-x)}} \tag{4}$$

olarak elde edilmiştir.

Lojistik denkleminden üretilen zaman serilerinin aperyodik olduğunu gösterebilmek için denklemin ürettiği zaman serisinin spektral özellikleri incelenmiştir. Denklemin $R = 4$ ve 10^5 örnekli zaman serisine Welch yöntemi uygulanarak Şekil 4'te gösterilen spektral güç yoğunluk kestirimi elde edilmiştir. Lojistik denkleminin zaman serisi içinde periyodik bir bileşen bulunmadığı spektrumun düzlüğünden anlaşılabilmektedir. Birim frekansa düşen işaret enerjisinin eş dağılımlı olduğu gözlenmektedir.



Şekil 4. $R = 4$ için 10^5 örnekli zaman serisinden hesaplanan güç spektrum yoğunluğu.



Şekil 5. $R = 4$ için hesaplanan özilinti fonksiyonu.

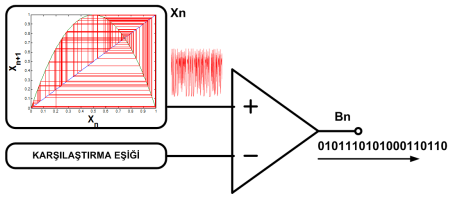
Üretilen zaman serisine ait özilinti fonksiyonu Şekil 5'te gösterildiği gibi denklemin zaman serisi içinde periyodik bir işaret bulunmadığını doğrulamaktadır. Gerçekleştirilen numerik benzetim sonuçlarına göre, lojistik denkleminin $R = 4$ için ürettiği zaman serisinin spektral olarak beyaz gürültüyle benzer özellikler sergilediği gözlenebilir.

III. LOJİSTİK DENKLEMİ TABANLI RASTSAL SAYI ÜRETECİ

Lojistik denkleminin entropi kaynağı olarak kullanıldığı rastsal sayı üreteci modeli Şekil 6'da gösterilmiştir. Rastsal sayı üretmek için faz portresi birbiriyle örtüşmeyen parçalara bölünüp, kaotik sistemin zamanda evrilirken takip ettiği yörüngenin faz portresindeki konumu kullanılmıştır. Faz portresinin $G_0 = [0, T_h)$ ve $G_1 = [T_h, 1]$ gibi iki üreteç bölgesinden oluştuğu varsayılırsa, kaotik yörüngenin faz portresindeki konumu T_h eşik parametresine göre $S(.)$ fonksiyonu ile ikilik kodlanarak,

$$S(x(n)) = \begin{cases} 0 & x(n) \in [0, T_h) \\ 1 & x(n) \in [T_h, 1] \end{cases} \tag{5}$$

rastsal sayılar üretilebilir. Denklem 1 ve 5 'in serbest değişkenleri olan kaos kontrol parametresinin $R = 4$ ve karşılaştırma eşiğinin $T_h = 0.5$ değerlerinde sistemden bağımsız ve eş olasılıklı bitler üretilebileceği teorik olarak gösterilmiştir[8]. [8]'deki matematiksel analizde eşik değeri sabit alınmıştır. Ancak uygulamada, eş dağılımlı bitler üretebilmek için üretilen zaman serisinin değişen ortalama değerinin eşik olarak kullanılması tercih edilmiştir. Böylece bitler kaotik işaret ve bu işaretin zamanla değişen ortalama değerine göre dinamik olarak üretilebilmektedir.

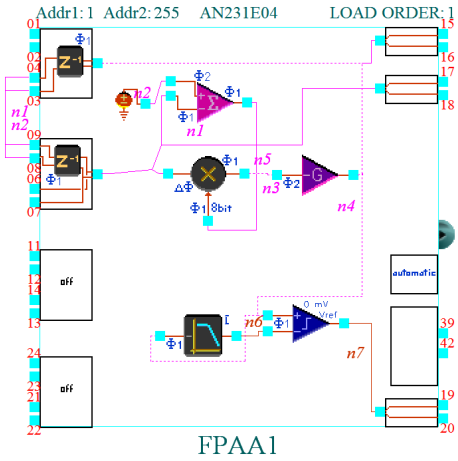


Şekil 6. Lojistik fonksiyonuna dayalı RSÜ modeli.

Lojistik denklemini entropi kaynağı olarak kullanabilmek için transfer fonksiyonu lojistik denklemi olan ve, zamanda gecikme yaratan iki devre gereklidir. Rastsal sayı üretimi için bunlara ek olarak bir karşılaştırıcı ile işaretin ortalama değerini hesaplayan bir alçak geçiren filtre de gerekmektedir. Anadigm AN231E04 tümdevresi anahtarlamalı kapasitör tabanlı bir SPAD devresidir [9] ve lojistik denkleminin RSÜ gerçeklemesi için gereken programlanabilir analog bileşenlere sahiptir. Lojistik denklemine dayalı RSÜ'nün gerçeklenmesi için AN231E04'ün tasarım programı kullanılarak Şekil 7'de gösterilen devre tasarlanmıştır.

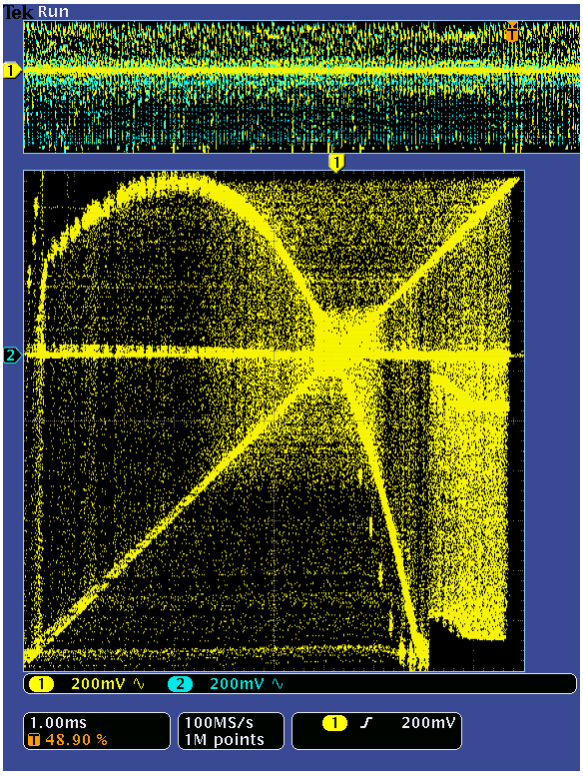
IV. SONUÇLAR VE TARTIŞMA

Tek boyutlu endomorfik lojistik fonksiyonunun kaotik, istatistiksel ve spektral özellikleri numerik analizler yardımıyla incelenerek kaotik rejimde öz ilintisiz, beyaz gürültü benzeri düz bir güç spektrumuna sahip olduğu gözlenmiştir. Kaotik sistemlerin entropi kaynağı olarak kullanılabilmelerinden yola çıkarak lojistik fonksiyonunu entropi kaynağı olarak kullanan bir rastsal sayı üreteci tasarlanmıştır. Kaotik fonksiyonun ürettiği yörünge ikilik bir alfabe ile kodlanarak rastsal sayılar üretilmiştir. Ayrık zamanlı çalışan anahtarlamalı kapasitör tabanlı bir SPAD tümdevresi üzerinde tek boyutlu kaotik lojistik denklemine dayalı bir rastsal sayı üreteci gerçeklenmiştir. Şekil



Şekil 7. Lojistik denklemine dayalı RSÜ'nün SPAD gerçeklemesi.

8'de sunulan faz portresi ölçümü, lojistik devresinin kaotik rejimde çalıştığını göstermektedir. Üretilen bitler ikili tabanda dosyaya aktarılarak 100 Milyon bitlik işlenmemiş RSÜ verisine NIST 800.22 istatistiksel testleri uygulanmıştır.



Şekil 8. Lojistik denkleminin SPAD gerçeklemesinden alınan faz portresi ölçümü.

Testlerin uygulandığı ham verilerin sıfır/bir oranını test eden frekans testinden ve ilişkili diğer istatistiksel testlerden geçemediği gözlenmiştir. Bu nedenle toplanan verinin ardışıl bitlerine çevrimdışı XOR art işlemi uygulanarak sıfır/bir oranındaki istatistiksel dengesizlik giderilmiştir. İşlenmiş olan ham verinin NIST test sonuçları Tablo I'de sunulmuştur. Tablo I'de P-değeri kolonundaki sayılar test edilen verinin ideal bir gerçek rastsal sayı üretecinden üretilmiş olma olasılığını göstermektedir. Orantı kolonu ise ham veri 1 Mbitlik bloklara ayrılarak test edildiğinde blokların testlerden geçme oranını vermektedir. NIST 800.22 tanım dökümanına göre P-değeri $>$ 0.01 ise test sonucu başarılı sayılmaktadır. [10].

Tablo I. NIST ISTATISTIKSEL TEST SONUÇLARI

Test	P-değeri	Orantı
Frekans	0.474986	1.0000
Blok Frekans	0.075719	0.9800
Birikimli Toplamlar	0.719747	1.0000
Koşular	0.115387	0.9800
Uzun-Koşu	0.249284	0.9800
Rütbe	0.61630	0.9800
FFT	0.514124	0.99
Evrensel	0.037566	0.97
Yaklaşık Entropi	0.678686	0.99
Seri	0.334538	0.98
Doğrusal-Karmaşıklık	0.153763	0.99

Anahtarlamalı devrelerdeki anahtarlama gürültüsü ve programlanabilir analog devre bileşenlerinin offset ve toleransları nedeniye ham verinin sıfır/bir dengesinde sorun olduğu düşünülmektedir. SPAD devresindeki analog bloklar 4MHz'e kadar çalışabilmelerine rağmen bit üretim hızını sınırlayan temel bileşen 250 kHz'de çalışan çarpma bloğudur. Yapılan çalışma, basit bir art işlemci fonksiyonu yardımıyla SPAD tümdevreleri üzerinde gerçeklenen tek boyutlu kaotik lojistik fonksiyonunun rastsal sayı üreteci olarak kullanılabileceğini göstermiştir.

KAYNAKÇA

[1] H. Bock, M. Bucci and R. Luzzi, "An Offset-Compensated Oscillator-Based Random Bit Source for Security Applications," *Cryptographic Hardware and Embedded Systems - CHES 2004*, cilt. 3156, ss. 27–83, 2004.

[2] T. Stojanovski, J. Pihl and L. Kocarev,"Chaos-based random number generators. Part II: practical realization," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, cilt. 48, no. 3, ss. 382–385, 2001.

[3] F. Pareschi, G. Setti and R. Rovatti,"A fast chaos-based true random number generator for cryptographic applications," *Proceedings of the 32nd European Solid-State Circuits Conference, ESSCIRC 2006*, ss. 130–133, 2006.

[4] J. P. Eckmann ve D. Ruelle, "Ergodic theory of chaos and strange attractors", *Reviews of Modern Physics*, cilt 57, no. 3, ss. 617–656, 1985.

[5] P. F. Verhulst, "Recherches sur la loi d'mathematics accroissement de la population.", *L'Académie Royale de Bruxelles et de l'Université Louvain*, cilt 18, ss. 1–42, 1845.

[6] R. M. May, "Simple mathematical models with very complicated dynamics," *N*ature, cilt 261, no. 5560., ss. 459–467, 1976

[7] A. N. Kolmogorov, "A new metric invariant of transitive dynamical systems and automorphisms in Lebesgue space," *Dokl. Acad. Nauk. SSSR* 119, 1958.

[8] İ. Çicek, A. E. Pusane ve G. Dündar, *"Tek boyutlu bir kaotik fonksiyonun gerçek rastsal sayı üretimine uygunluğunun incelenmesi,"* Sinyal İşleme ve İletişim Uygulmaları Kurultayı (SIU), ss. 1-4, 18-20 Nisan 2012

[9] Anadigm, *"The AN231E04 dpASP Dynamically Reconfigurable Analog Signal Processor," AN231E04 Datasheet*, Rev. 1.1

[10] A. Rukhin *et al.*, "NIST special publication 800.22 Rev.1a: A statistical test suite for random and pseudorandom number generators for cryptographic applications," http://csrc.nist.gov/publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf, *NIST*, ss. 1–153, 2010.