Journal of the Faculty of Engineering and Architecture of Gazi University 39:2 (2024) 693-707

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

# Performance analysis of pseudo-random number generations of two-dimensional linear uniform cellular automata that considers initial state densities

Hürevren Kılıç[1,2]*

[1]Department of Computer Engineering, Engineering Faculty, Atılım University, Kızılcaşar Mah.,06830, İncek, Gölbaşı, Ankara, Türkiye
[2]Metal Forming Center of Excellence, Atılım University, Kızılcaşar Mah.,06830, İncek, Gölbaşı, Ankara, Türkiye

**Highlights:**

- Pseudo-random number generation using two-dimensional linear uniform cellular automata
- The necessity of considering initial state densities of automata' in the mentioned generations
- Successful random number generation when the initial density ratios of 7 automata are 25% - 70%

**Keywords:**

- Modelling & Simulation
- Pseudo-random number generation
- Cellular Automata
- Two-dimensional linear uniform cellular automata
- Initial configuration state densities

**Article Info:**

Research Article
Received: 31.08.2021
Accepted: 12.04.2023

**DOI:**

10.17341/gazimmfd.989265

**Acknowledgement:**

I would like to thank to Atılım Univ. Metal Forming Center of Excellence; Dr. H. Bayındır – Chief Expert & Researcher of TÜBİTAK ULAKBİM High Performance & Grid Computing Center; Atılım Univ. faculty member Dr. Beytullah Yıldız; O.C. Acar, B.Y. Şahinoğlu, İ. Tarakçı and Ö.D. Kılıç for their support and useful comments & discussions.

**Correspondence:**

Author: Hurevren Kılıç
e-mail: hurevren.kilic@atilim.edu.tr
phone: +90 533 469 5492

**Graphical/Tabular Abstract**

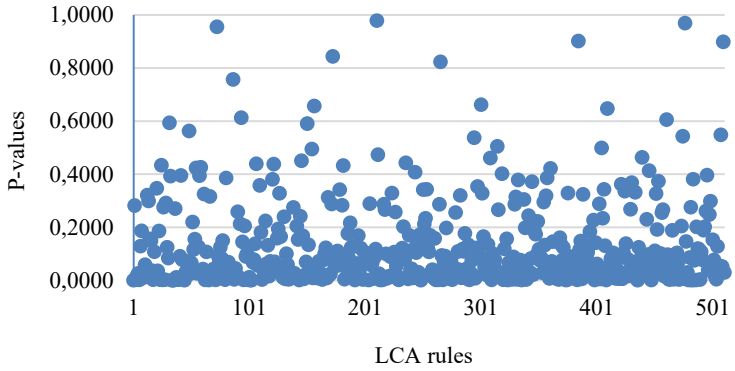



**Figure A.** P-values obtained as a result of applying the Shapiro-Wilk normal distribution test for the sum of passed tests values of 511 LCA rules

**Purpose:** To investigate possible impact of initial state densities 2D Linear Cellular Automata in pseudo-random number generation process.

**Theory and Methods:** The effect of initial state densities of two-dimensional linear uniform cellular automata on pseudo-random number generation is investigated, experimentally. The developed approach is original since it takes into account initial state densities in high quality pseudo-random number generation of cellular automata. In the experiments, 512 two-dimensional linear cellular automata (LCA) are examined for 19 different initial state densities (ρ) (total of 512*19 = 9728), varying between 0.05 and 0.95. In the first stage of the experiments, the LCAs are subjected to the National Institute of Standards & Technology (NIST) statistical test suite tests together with the random number generators known in the literature. Then, in the second stage, tests in the AIS31 and TestU01 test suites are applied to the 7 successful cellular automata and generators known in the literature.

**Results:** As a result of the comparative study, it is observed that the 2D linear cellular automata generators, which are successful in random number generation, are not suitable for their use in cryptographic applications, especially as a result of the application of TestU01 tests being one of the stringent tests in the literature. This result supports the results known in the literature. On the other hand, according to the results obtained by the NIST tests applied to 9728 automata, it is shown that the initial state density ratios of the automata affect their pseudo-random number generation and this situation, which was not taken into account in the literature, should be taken into account in the automata-based pseudo-random number generation research. The P-values obtained as a result of applying the Shapiro-Wilk normal distribution test for the sum of passed tests values of 511 LCA rules are given in Figure A. Specifically, when we consider all the different initial state densities of the 7 most successful automata that passed the NIST test, successful random number generation was observed when the initial density ratio was between 25% and 70% regardless of the automata.

**Conclusion:** (1) Linear cellular automata are known to be qualified random number generators, but they are not suitable for direct cryptographic applications due to their short cycle length. This result, known in the literature, has been experimentally confirmed in the context of two dimensional linear cellular automata (2) As shown experimentally in the context of two-dimensional linear cellular automata, initial state density is an important point in random number generation and should not be ignored.

Journal of the Faculty of Engineering and Architecture of Gazi University 39:2 (2024) 693-707

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

# İki boyutlu doğrusal tek tip hücresel özdevinirlerin başlangıç durum yoğunluklarını dikkate alan sözde rastgele sayı üretimlerinin başarım analizi

Hürevren Kılıç[1,2]*

[1]Atılım Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Kızılcaşar Mah.,06830, İncek, Gölbaşı, Ankara, Türkiye
[2]Atılım Üniversitesi, Metal Şekillendirme Mükemmeliyet Merkezi, Kızılcaşar Mah., 06830, İncek, Gölbaşı, Ankara, Türkiye

## ÖNEÇIKANLAR

- İki-boyutlu doğrusal tek tip hücresel özdevinirler kullanarak sözde-rastgele sayı üretimi
- Söz konusu üretimlerde özdevinirlerin ilk durum yoğunluklarının dikkate alınmasının gerekliliği
- 7 adet özdevinirin başlangıç yoğunluk oranları %25 - %70 olduğunda başarılı rastgele sayı üretmeleri

**Makale Bilgileri**

Araştırma Makalesi
Geliş: 31.08.2021
Kabul: 12.04.2023

**DOI:**

10.17341/gazimmfd.989265

**Anahtar Kelimeler:**

Modelleme ve benzetim, sözde-rastgele sayı üretimi, hücresel özdevinirler, iki boyutlu doğrusal tek tip hücresel özdevinirler, başlangıç konfigürasyonu durum yoğunlukları

ÖZ

Bu çalışmada, iki boyutlu doğrusal tek tip hücresel özdevinirlerin başlangıç durum yoğunluklarının sözde-rastgele sayı üretimlerine olan etkisi deneysel olarak incelenmiştir. Geliştirilen yaklaşım, hücresel özdevinirlerin kaliteli sözde-rastgele sayı üretimlerinde başlangıç durum yoğunluklarının dikkate alması açısından özgündür. Deneylerde 512 adet iki boyutlu doğrusal hücresel özdevinir (DHÖ) değerleri 0,05 ile 0,95 arasında değişen 19 adet farklı başlangıç durum yoğunlukları (ρ) için (toplam 512*19 = 9728 adet) incelenmiştir. Sayı dizisi üretimlerini takiben deneylerin ilk aşamasında söz konusu DHÖ'ler literatürde bilinen rastgele sayı üreteçleriyle birlikte National Institute of Standards and Technology (NIST) istatistiksel test süiti testlerine tabi tutulmuştur. İkinci aşamada ise, ilk aşamadaki NIST testlerinden başarılı olarak geçen 7 adet farklı yoğunluktaki hücresel özdevinire ve literatürde bilinen üreteçlere AIS31 ve TestU01 test süitlerinde yer alan testler uygulanmıştır. Yapılan karşılaştırmalı çalışma neticesinde, rastgele sayı üretimlerinde başarılı olan 2D doğrusal hücresel özdevinir üreteçlerin doğrudan kriptografik amaçlı uygulamalar için kullanımlarının uygun olmadığı, özellikle literatürde yer alan zorlu (stringent) testlerden olan TestU01 testlerinin uygulanması neticesinde görülmüştür. Bu netice literatürde bilinen sonuçları desteklemektedir. Öte yandan 9728 adet özdevinire uygulanan NIST testleri neticesinde alınan sonuçlara göre özdevinirlerin başlangıç durum yoğunluk oranlarının sözde rastgele sayı üretimlerini etkilemektedir ve literatürde dikkate alınmayan bu durum özdevinir tabanlı sözde rastgele sayı üretimi araştırmalarında dikkate alınmalıdır.

# Performance analysis of pseudo-random number generations of two-dimensional linear uniform cellular automata that considers initial state densities

## HIGHLIGHTS

- Pseudo-random number generation using two-dimensional linear uniform cellular automata
- The necessity of considering initial state densities of automata' in the mentioned generations
- Successful random number generation when the initial density ratios of 7 automata are 25% - 70%

**Article Info**

Research Article
Received: 31.08.2021
Accepted: 12.04.2023

**DOI:**

10.17341/gazimmfd.989265

**Keywords:**

Modelling and simulation, pseudo-random number generation, cellular automata, two-dimensional linear uniform cellular automata, initial configuration state densities

ABSTRACT

In this study, the effect of initial state densities of two-dimensional linear uniform cellular automata on pseudo-random number generation is investigated, experimentally. The developed approach is original since it takes into account initial state densities in high quality pseudo-random number generation of cellular automata. In the experiments, 512 two-dimensional linear cellular automata (LCA) are examined for 19 different initial state densities (ρ) (total of 512*19 = 9728), varying between 0.05 and 0.95. In the first stage of the experiments, following the number sequence generation, the LCAs are subjected to the National Institute of Standards & Technology (NIST) statistical test suite tests together with the random number generators known in the literature. Following this step, in the second stage, tests in the AIS31 and TestU01 test suites are applied to the 7 successful cellular automata and generators known in the literature. As a result of the comparative study, it is observed that the 2D linear cellular automata generators, which are successful in random number generation, are not suitable for their use in cryptographic applications, especially as a result of the application of TestU01 tests being one of the stringent tests in the literature. This result supports the results known in the literature. On the other hand, according to the results obtained by the NIST tests applied to 9728 automata, it is shown that the initial state density ratios of the automata affect their pseudo-random number generation and this situation, which was not taken into account in the literature, should be taken into account in the automata-based pseudo-random number generation research.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *hurevren.kilic@atilim.edu.tr / Tel: +90 533 469 5492

## 1. Giriş (Introduction)

Kaliteli rastgele sayı üretimine, modelleme ve benzetim (simulation) tabanlı tüm temel mühendislik uygulamaları, kriptografi, türlü gündelik yazılım sistemleri uygulamaları, bilgisayar oyunları, istatistik araştırmaları, tıkış fonksiyonları (hash functions), sayısal analiz, sürü zekası ve rastgeleleştirilmiş algoritmalar gibi birçok alanda ihtiyaç duyulmaktadır. Termal gürültü, mikrofon sesi, hava burgacı (turbulence) gibi doğal fiziksel süreçlerden gerekirci olmayan (nondeterministic) yöntemlerle gerçek rastgele sayı üretimi (true random number generation) mümkündür [1]. Alanda Programlanabilen Kapı Dizisi – APKD (Field Programmable Gate Array – FPGA) - tabanlı sayısal kaotik sistem yaklaşımıyla gerçek rastgele sayı üretiminin önemi ve potansiyeli Tuna ve Fidan [2] tarafından incelenmiştir. Tuncer vd. [3] ise periodik olmayan örnekleme yaklaşımıyla kriptografik uygulamalarda kullanım amaçlı halka osilatör tabanlı, nitelikli gerçek sayı üreteci geliştirmiş ve APKD ortamında gerçekleştirmiştir. Kaos tabanlı bir rastgele sayı üretimi çözümü olan ve Ozkaynak [4] tarafından önerilmiş olan yaklaşımda, kesikli mertebe kaotik sistemlerin ayrık zaman tabanlı kaotik sistem çözümlerine alternatif olabileceği kesirli mertebe kaotik Chua sistemi bağlamında gösterilmiştir. Yine kaos tabanlı ve pratik uygulamalı çalışmalarında Akkaya vd. [5], banka şifrematik cihazı tasarlamış ve donanımsal olarak gerçekleştirmiştir. Öte yandan, Arnold'un kedi görüntüsü örneği üzerinden tanımlanan dönüşüm yöntemi tabanlı sözde rastgele sayı üretimi (Pseudo-Random Number Generation) çözümünün, kriptografi dahil birçok farklı alanda kullanılabileceği Avaroğlu [6] tarafından gösterilmiştir. Gerçek rastgele sayı üretimine alternatif bir yaklaşım olan ve verilen sabit uzunluktaki bir başlangıç değerine (seed), algoritma(lar) vasıtasıyla ardışık dönüşümler uygulamak ve bu dönüşümler neticesinde olabildiğince uzun ve rastgele sayı dizilerinin elde edilmesi şeklinde tanımlanabilecek sözde rastgele sayı üretimi (Pseudo-Random Number Generation) problemine ilişkin, günümüzden 40 yıl öncesine kadar dayanan birçok araştırma yapılagelmiştir. Bu yaklaşım kapsamında yer alan hücresel özdevinirler matematiksel modelinin sözde rastgele sayı dizisi üretiminde kullanımına örnek teşkil eden erken dönem çalışmaları için Knuth'ın [7] Programlama Sanatı eserine, Wolfram'ın [8] hücresel özdevinirler modelini baz alan temel çalışmasına ve Park ve Miller'ın [9] minimal uygulama standardını tanımlayan ve problemin önemini vurgulayan çalışmalarına başvurulabilir.

Sözde rastgele sayı üretimi problemine ilişkin literatürde geçmişten günümüze yer alan Alanda Programlanabilen Kapı Dizisi – APDK (Field Programmable Gate Array – FPGA) gerçekleştirimlerini inceleyen bir tarama (survey) makalesi olarak Bakiri vd.'nin [10] çalışmasının yanısıra, sözde rastgele sayı üreteçlerini doğrusal eşleşik (linear congruential), doğrusal geri besleme öteleme yazmacı (linear feedback shift register) ve hücresel özdevinirler olmak üzere üç ana başlığa ayırıp bunların göreli performanslarını detaylı bir şekilde inceleyen Bhattacharjee vd.'nin [11] makalesi hem tarama hem de kapsamlı bir karşılaştırmalı çalışma niteliğindedir. Sözde rastgele sayı üretiminde hücresel özdevinirlerin tercih edilmelerinin temel bir sebebi, donanım olarak gerçekleştirimlerinin diğer yaklaşımlara göre çok daha maliyet etkin olmalarıdır. Ayrıca, çok büyük ölçekli bütünleşik devrelerin (Very Large Scale Integration – VLSI circuits) testi gibi donanım uygulamaları için, bir sözde rastgele sayı üretecinin alan verimliliği ve taşınabilirliği, gösterdiği karmaşık rastgele sayı üretim kalitesinin öneminin önüne geçmektedir. Doğrusal geri besleme öteleme yazmaçları ile hücresel özdevinirlerin rastgele sayı üretimi donanım uygulamalarını karşılaştırdığımızda ise, hücre bazında yerel bağlantılar yoluyla geri besleme sağlayan hücresel özdevinirler daha düşük bağlantı maliyetleri sebebiyle doğrusal geri besleme öteleme yazmaçlarına göre tercih edildikleri bilinmektedir.

Hücresel özdevinirler tabanlı sözde rastgele sayı üretimi literatüründeki yaklaşımların sınırlarını ve çeşitliliğini belirleyen, tek boyut (1B), iki boyut (2B), tek tip (uniform), tek tip olmayan (non-uniform), melez (hybrid), doğrusal (linear), doğrusal olmayan (non-linear), asimetrik komşuluk (asymmetric neighborhood), ikili durum (two-state), üçlü-durum (three-state), onluk (decimal) durum gibi birçok farklı model alt sınıflamaları bulunmaktadır. Bu sınıflamaların tanımladığı sınırlandırmalara karşın hala devasa büyüklükte olan hücresel özdevinir üreteci arama uzayı göz önüne alındığında, analitik tasarıma alternatif olan ve akıllı arama algoritmaları vasıtalarıyla özdevinir bulma yaklaşımını benimseyen Sipper'in [12] hücresel programlama; Faraoun'un [13] genetik strateji tabanlı hücresel özdevinir blok şifreleme; Guan vd.'nin çok-amaçlı genetik algoritma (multi-objective genetic algorithm) [14] ve Hanin vd.'nin [15] parçacık sürü optimizasyonu (Particle Swarm Optimization) tabanlı yaklaşımları mevcuttur.

Genel olarak hücresel özdevinirleri ve özel olarak bu makalenin ele aldığı bir alt model olan doğrusal tek tip hücresel özdevinir üreteçlerin bir sonraki rastgele değerin tahmin edilemezliğini zedeleyen: "döngü boyunun (cycle length) kısalığı" problemi literatürde bilinmektedir [16]. Soruna alternatif çözümler olarak, Shin vd.'nin [16] doğrusal olmayan; Temiz vd.'nin [17] doğrusal melez; Hosseini vd.'nin [18] tek tip olmayan hücresel özdevinirler (HÖ) ile bir ayrık dinamik sistem (Discrete Dynamical System) olan Langton'un karıncası (Langton's ant) modellerini birleştirdiği HÖ ile Langton'un karıncası; Szaban'ın [19] 1B bütünsel (totalistic) hücresel özdevinirleri 1, 2, 3 ve 4 komşuluk yarıçapları için inceleyen ve Nayyeri ve Dastghaibyfard'ın [20] rastgele sayı üretimini bilgi teorisi temelli analiz eden yaklaşımları bulunmaktadır. Alternatif model olarak, Bhattacharjee vd. [21] hücrelerin klasik ikili-durumları yerine üçlü-durumlarını dikkate aldıkları modelleri ile 1B hücresel özdevinirler bağlamında yetkin sonuçlar almıştır. Bhattacharjee ve Das'ın [22] önerdiği onluk sistem durum değerli hücresel özdevinir yaklaşımında ise kural uzayı diğerlerine göre çok daha devasa olduğu için obur (greedy) stratejileri temel alan sezgisel çözümler önerilmiş ve elde edilen üreteçlerin en azından literatürde yer alan çözümler kadar iyi oldukları gözlemlenmiştir. Hücresel özdevinir tabanlı sözde rastgele üreteçlerinin donanım düzeyinde tasarım ve gerçekleştirimlerine bakıldığında ise Guan ve Tan'ın [23] kendi kendine programlanabilen ve doğrusal olmayan hücresel özdevinirleri; Roy vd.'nin [24] melez şifreleme amaçlı programlanabilen hücresel özdevinirleri ve Petrica'nın [25] Alanda Programlanabilen Kapı Dizisi - APKD (Field Programmable Gate Array – FPGA) ile optimize edilmiş hücresel özdevinir yaklaşımları bulunmaktadır.

Tüm bu yaklaşımlarda kendi içlerinde ve göreli olarak iyi sonuçlar elde edilmesine rağmen, söz konusu yaklaşımların hiçbirinde hücresel özdevinirlerin elde edilmek istenen uzun döngü boylarınca gösterdikleri rastgele/kaotik davranışlarını doğrudan etkileyen önemli bir unsur olan "başlangıç durum yoğunlukları" dikkate alınmamıştır. Buna karşın, Baetens ve Gravner [26] kimi iki-durumlu (two-state) 1B ve 2B hücresel özdevinirlerin uzun vadedeki davranışlarının başlangıç durumlarına olan hassasiyeti ve başlangıç durumlarına uygulanan küçük uyartıların (perturbation) sistem kararlılığına ve davranışına olan etkilerini araştırmışlardır. Aynı çalışmada, başlangıç örüntülerinin 0/1 durum yoğunluğu ile uygulanan uyartıların birikimsel bozum (damage) etkisini tanımlayan en büyük Lyapunov üssü (maximal Lyapunov exponent) arasındaki ilişki farklı özdevinir kuralları için hem 1B hem de 2B hücresel özdevinirler bağlamlarında detaylı olarak incelenmiştir. Çalışmanın sonuç kısmında, hücresel özdevirlerin başlangıç durum yoğunluklarına bağlı olarak hangi özelliklerinin sınırlı (marginal) ve geniş (expansive) ölçek dinamikleri arasında faz geçişine sebep olduğunun incelenmesi ve varsa ilgili kritik yoğunluk değerinin ($\rho$) ne olduğu cevaplanmayı bekleyen açık

bir problem olarak sorulmuştur. Bu bağlamda 1B üreteçlere göre daha az çalışılmış olan 2B doğrusal hücresel özdevinirlerin başlangıç durum yoğunluklarına bağlı olarak sözde rastgele sayı üretimindeki olası iyi/kötü performanslarının ortaya çıkarılması, bu çalışma için temel motivasyon kaynağı olmuştur. Bu amaçla, Moore komşuluğu (neighborhood) ile tanımlı, toplamda 512 adet farklı 2B doğrusal hücresel özdevinirin her biri, değerleri %5 ile %95 arasında değişen 19 farklı başlangıç durum yoğunluğu için çalıştırılmıştır. Sonuçların başarı ölçümü amacıyla NIST [27], AIS31 [28] ve TestU01 [29] test süiti testleri uygulanmıştır. Yapılan kademeli uygulamada, ilk etapta söz konusu 512x19=9182 adet özdevinire NIST test süiti uygulanmış sonrasında ilk etapta başarılı olan özdevinirlerin tümüne hem AIS31 hem de TestU01 testleri ara elemeye tabi tutmadan uygulanmıştır. Makale Bölüm 2'de doğrusal hücresel özdevinirlere ilişkin teorik model tanımlaması, davranış tabanlı hücresel özdevinir sınıflandırmaları ve sözde rastgele sayı üretim yöntemi sunulmuştur. Uygulanan deneysel metot Bölüm 3'te, elde edilen deneysel sonuçlar ve bunlara dayalı tartışmalar ise Bölüm 4'te bulunmaktadır. Son kısımda ise varılan sonuçlar yer almaktadır.

## 2. Teorik Model (Theoretical Model)

Hücresel özdevinirler, birbirleriyle etkileşen çok sayıda basit bileşenden oluşan ve bu etkileşim neticesinde karmaşık davranış örüntüleri oluşturan sistemlerin matematiksel modellemesi için kullanılırlar. Ayrık dinamik sistem modeli olan hücresel özdevinirler, hücrelerden oluşan düzenli kafes (regular lattice) yapısına sahiptir. Hücresel özdevinirler, 1 Boyutlu (1B) olabildiği gibi çok boyutlu da (2B, 3B, … gibi) olabilirler. Sistem bileşenlerini temsil eden hücreler, bileşenin herhangi bir $t$ anındaki durumunu gösteren sonlu $k$ sayıda farklı durum değerinden birine sahiptir. Sistem dinamikleri ise her bir hücrenin eşzamanlı (senkron) veya asenkron olarak ayrık zaman adımlarında global sistem davranışını yerel (local) durum değişiklikleri cinsinden tanımlayan $\varphi$ hücre durum değişikliği fonksiyonu ile tanımlanır. Her bir hücrenin bir sonraki $(t+1)$ zamanındaki yeni durumu, düzenli kafes üzerinde kendisi ve komşularının $t$ anındaki durumlarına göre belirlenir. Örneğin, 1B bir hücresel özdevinirin $i$'inci hücresinin $t+1$ anındaki değeri $x_i^{t+1}$, Eş. 1'deki gibi güncellenir.

$$x_i^{t+1} = \varphi(x_{i-1}^t, x_i^t, x_{i+1}^t) \tag{1}$$

Bu çalışmada 2B hücresel özdevinirler dikkate alınmıştır. 2B hücresel özdevinirler için birçok farklı kafes ve komşuluk yapısı mevcuttur. Çalışmamızda kare kafes (square lattice) üzerinde Moore komşuluğunu temel alan (Şekil 1a), Eş. 2'deki durum geçiş fonksiyonuyla tanımlı 2B hücresel özdevinir modeli benimsenmiştir [30].

$$x_{i,j}^{t+1} = \varphi(x_{i-1,j-1}^t, x_{i,j-1}^t, x_{i+1,j-1}^t, x_{i-1,j}^t, x_{i,j}^t, x_{i+1,j}^t, x_{i-1,j+1}^t, x_{i,j+1}^t, x_{i+1,j+1}^t) \tag{2}$$

Şekil 1a'nın merkezinde yer alan siyah renkli hücrenin durum değeri, kendisinin ve komşuları olan beyaz renkli hücrelerin durum değerleri kullanılarak güncellenir. Diğer komşuluk tanımlamalarından olan beş-komşu, üçgensel ve altıgensel komşuluk yapılarının tümü, dokuz-komşu hücre yapısı cinsinden ifade edilebilen özel komşuluk durumlarından ibarettir. Bu açıdan dokuz-komşu yapısı genel bir tanımlamayı ifade eder. Dokuz-komşu hücre yapısı ve her bir hücrenin bulunabildiği $k$ farklı durum sayısı dikkate alındığında, toplam $k^{k^9}$ farklı $\varphi$ fonksiyonu tanımlanabilir. Devasa sayıda olan farklı $\varphi$ fonksiyonlarının yarı bütünsel (semi totalistic) olanlarının bir alt kümesi olan $k=2$ değeriyle sabit Doğrusal Hücresel Özdevinirlerde merkez hücre değeri güncellemesi, merkez hücre ve bu hücrenin Moore komşuluğunda yer alan hücrelerin değerleri ve katsayılar dikkate alınarak Eş. 3'teki gibi hesaplanır.

$$x_{i,j}^{t+1} = c_0 x_{i,j}^t + c_1 x_{i,j+1}^t + c_2 x_{i+1,j+1}^t + c_3 x_{i+1,j}^t + c_4 x_{i+1,j-1}^t + c_5 x_{i,j-1}^t + c_6 x_{i-1,j-1}^t + c_7 x_{i-1,j}^t + c_8 x_{i-1,j+1}^t \ (mod)\ 2 \tag{3}$$

$c_i \in \{0,1\}, 0 \le i \le 8$ katsayılarını ve dolayısıyla kural kodlamalarını göstermektedir (Şekil 1b). Verilen katsayılar için kural kodlaması onluk sistemde: $\sum_{i=0}^{8} c_i 2^i$ şeklinde ifade edilir. Örneğin, $c_0=1, c_1=1, c_2=0, c_3=1, c_4=0, c_5=1, c_6=0, c_7=1, c_8=0$ katsayı değerleri, Kural 171'i tanımlamaktadır. Buna göre, toplam 9 farklı katsayı değeri için $2^9=512$ farklı doğrusal kural kodlaması yapmak mümkündür.

İki boyutlu doğrusal tek tip hücresel özdevinirlerin ürettikleri global örüntüler, döngü boyu (cycle length) uzunlukları ve davranışları (belirli bir global örüntüye yakınsama, döngüye girme, kaotik örüntüler üretme gibi) açısından farklılıklar gösterebilmektedir [30]. Rastgele sayı üretimi için davranışı tahmin edilemeyen kaotik nitelikli örüntü üretebilen özdevinirler daha güçlü çözüm adaylarıdır zira mevcut konfigürasyondan takip eden konfigürasyonları tahmin etmek güçtür. Kaotik davranış gösteren hücresel özdevinirler hangileridir sorusuna ilişkin Packard ve Wolfram [30] niteliğe dayalı (qualitative) bir sınıflandırma yapmıştır. Bu sınıflandırmaya göre, hücresel özdevinirler uzun vadeli davranışlarına bakılarak dört ayrı başlıkta incelenir:

- *Sınıf I* : Stabil duruma erişenler (sabit/limit noktası – fixed/limit point)
- *Sınıf II* : Periyodik salınım davranışı gösterenler (limit döngü – limit cycle)
- *Sınıf III* : Türbulant sıvı davranışı gibi kaotik davranış sergileyenler (garip çekiciler – strange attractors)
- *Sınıf IV* : Basit salınımdan daha karmaşık ancak kaosa durumuna göre daha düzenli davranış sergileyenler. Bu sınıfın özdevinirleri, Sınıf II ile Sınıf III arasında davranış göstermeleriyle beraber hücreleri arasında bilgi yayılımına (yani iletişim) olanak tanımaları


**Şekil 1.** a) 2B Moore komşuluk yapısı b) Moore komşuluk yapısı için doğrusal hücresel özdevinir hücre katsayı ve konumları
(a) 2D Moore neighborhood structure b) Linear cellular automata cell coefficients and locations for the Moore neighborhood structure)

ve birçok yarı-stabil durumda olabilen hücrelerden oluşmaları (yani yazılıp silinebilir hafıza) sebebiyle hesaplama yapılabilir ortam niteliğindedirler.

Bu sınıflandırmaya göre, rastgele sayı üreteci olarak kullanılmaya aday olanların uzun vadeli davranışlarının tahmin edilebilirliklerinin zorluğu sebebiyle Sınıf III'e dahil, kaotik davranış gösteren hücresel özdevinirlerden olması gerektiği düşünülebilir. Öte yandan, kimi hücresel özdevinirlerin farklı başlangıç durumları için çalıştırımlarında bir süre bir sınıfının davranışını gösterirken zaman içinde başka bir sınıfın davranışını gösterebildikleri bilinmektedir [31]. Kaotik davranışın temel bir özelliği başlangıç durumlarındaki küçük değişikliklere olan hassasiyettir. Bu bağlamda Zenil [32] faz değişikliklerini belirleyen ve başlangıç durumlarına olan hassasiyeti ölçen sıkıştırma tabanlı bir yöntem önermiştir. Hücresel özdevinirlerin kaotik davranışlarına ilişkin varılan sonuçların ancak sonsuz kafesler (infinite lattice) için geçerli olduğu ve pratikte kaçınılmaz olarak ancak sonlu kafesler üzerinde tanımlayabileceğimiz hücresel özdevinirlerin benzer kaotik davranışlar göstermeleri yine ancak belirli bir düzeye kadar beklenebilir [22]. Hücresel özdevinirlerin davranışsal sınıflandırması problemi ele alındığında, Culik ve Yu [33] tarafından kanıtlandığı üzere, verilen bir hücresel özdevinirin hangi sınıfa ait olduğunun belirlenmesi karar verilemeyen (undecidable) bir problemdir. Sonuç olarak, iki boyutlu doğrusal hücresel özdevinirlerin sözde rastgele sayı üretiminde kullanımına yönelik yapılan bu çalışmada tüm aday özdevinirler (512 adet) literatürdeki sınıflandırmalarına bakılmaksızın dikkate alınmıştır.

## 3. Deneysel Metot (Experimental Method)

Yapılan deneylerde, $2B\ ZxZ$ kare kafes formundaki üreteçler için $Z = 20$ olduğu kabul edilmiştir. Sınır komşulukları periyodik sınır durumu (periodic boundary conditions) olarak tanımlı bir yumrudur (torus). Üreteçlerin başlangıç durumunu tanımlayan 0/1 durum atamaları rastgele yapılmıştır. Başlangıç durumuna göre, üreteçler çalıştırımları sırasında $2^{Z^2}$ farklı durumdan birinde olabilir. Bir 2B hücresel özdevinirin ürettiği global örüntü silsilesinden rastgele sayı dizisi üretimi farklı yöntemlerle yapılabilir. Üretilen ikili (binary) değerlerin tümünün değil ancak belirli bir pencere büyüklüğünde tanımlı kısmının kullanılarak oluşturulduğu, döngü boyunu verimli kullanmayı hedefleyen ancak sayı üretim aralığını kısıtlayan yaklaşım [21] yerine bu çalışmada hücresel özdevinirler tarafından üretilen tüm ikili değerlerin filtreleme yapmadan doğrudan kullanıldığı bir rastgele sayı üretim şekli benimsenmiştir.

Pratikte, örüntü silsilesi üretiminde her hücre için, zaman içinde oluşan 0/1 bit dizileri, belirli bir zaman adım derinliği (d) kadar dikkate alınmış ve ardı sıra eklenmiştir. Literatür ile tutarlılık açısından deneylerde d=4 ve d=64 zaman adım derinlikleri uygulanmıştır [34]. Ekleme işlemi soldan sağa ve yukarıdan aşağıya tüm 2 boyutlu örüntü alanını kapsayacak şekilde yapılmıştır. Uç uca ekleme işlemi istatistiksel testlerin sağlıklı olarak yapılabilmesi için ihtiyaç duyulan uzunlukta rastgele diziler elde edilene kadar sürdürülmüştür. Bu yöntemle d = 4 zaman adımı derinliği için oluşan örnek dizi Eş. 4'te tanımlanmıştır.

$$x_{1,1}^{1}x_{1,1}^{2}x_{1,1}^{3}x_{1,1}^{4}\cdots x_{N,N}^{1}x_{N,N}^{2}x_{N,N}^{3}x_{N,N}^{4}x_{1,1}^{5}x_{1,1}^{6}x_{1,1}^{7}x_{1,1}^{8}\cdots \\ x_{i,j}^{t+1}x_{i,j}^{t+2}x_{i,j}^{t+3}x_{i,j}^{t+4}\cdots x_{N,N}^{19997}x_{N,N}^{19998}x_{N,N}^{19999}x_{N,N}^{20000} \quad (4)$$

Yapılan deneylerde, t = 300000 global örüntü adımı ve Z = 20 kabul edildiğinden, her bir özdevinirin farklı yoğunlukları için $t * Z^2$ (= 120 milyon) bitlik ($\sim 120MB$) rastgele sayı dizisi üretilmiştir. Üretimi başlatan başlangıç durum örüntüleri (seed), başlangıç yoğunluk değeri dikkate alınacak şekilde, C programlama dili rand() fonksiyonu kullanılarak üretilmiştir. Deneylerde, Moore komşuluğu ile tanımlı 512 adet farklı doğrusal hücresel özdevinirin her biri, değerleri %5 ile %95 arasında değişen 19 farklı başlangıç durum yoğunluğu için çalıştırılmıştır. Sonuç olarak, her bir farklı hücresel özdevinir üretecin farklı başlangıç durum yoğunlukları dikkate alındığında toplam 512*19 = 9728 adet aday üreteç dikkate alınmıştır.

Ne kadar test yapılırsa yapılsın verilen bir sayı dizisinin gerçekten rastgele olduğunu kanıtlamak mümkün değildir. Ancak rastgeleliğinin yetersiz olduğu gösterilebilir. İstatistiksel testler, verilen bir sayı dizisinin sözde rastgeleliğini değerlendirmek için geçerli ve pratik yöntemlerdir. Bu sebeple, bu çalışmada literatürde son yıllarda sıklıkla kullanılan ve farklı ölçüm perspektiflerini yansıtmaları sebebiyle olabildiğince kapsamlı istatistiksel testlerden oluşan NIST İstatistiksel Test Süiti [27], AIS31 Test Süiti [28] ve TestU01 Test Süiti [29] testleri kademeli olarak uygulanmıştır. Dikkat edilmesi gereken önemli bir husus, istatistiksel test süitlerinde yer alan testlerin yaptıkları rastgele olmama (non-randomness) ölçümlerinin kendi içlerinde ne derece bağımsız olduklarıdır. Bu bağlamda, örneğin NIST test süitinde yer alan testler arasından boyları 38.912 bit'ten kısa olan dizilere uygulanabilenler, Sulak vd. [35] tarafından çalışılmış ve süitte yer alan yaklaşık entropi testi (approximate entropy test), seri-1 ve seri-2 testlerinin kendi aralarında; frekans testi (frequency test) ve blok frekans testlerinin (frequency test within a block) de kendi aralarında kayda değer oranda karşılıklı bağımlı oldukları gözlemlenmiştir. Bu çalışma kapsamında yaptığımız deneylerde test süitlerinde yer alan tüm testler kendi içlerinde ve karşılıklı bağımlılıkları dikkate alınmadan uygulanmıştır.

### *3.1. NIST Test Süiti Rastgelelik Testleri*
### *(NIST Test Suit Randomness Tests)*

Aday doğrusal hücresel özdevinirlerden türetilen diziler, NIST STS yazılım paketinde yer alan 15 temel tip testin tamamına tabi tutulmuştur. Bu testlerden, Rastgele Gezintiler (Random Excursions) ve Rastgele Gezintiler Değiştirilmiş (Random Excursions Variant) testleri için yetersiz sayıda döngü (cycle) içeren veri üretimini engellemek amacıyla, zaman içinde oluşan sayı dizilerini uç uca ekleme işlemi diğer testlerden farklı olarak, d = 4 zaman derinliği boyunca değil d = 64 zaman derinliği boyunca uygulanmıştır. Dikkat edilecek olursa, NIST test süitindeki testlerden frekans testi dışındaki tüm testler için sayı sıralamaları test sonucunu doğrudan etkiler niteliktedir. Bu sebeple farklı bit sıralamalarıyla neticelenebilen zaman derinliği değeri seçimi sonuçlar açısından önem arz etmektedir.

Her bir üretece uygulanan 15 adet testten Birikimsel Toplamlar (Cumulative Sums) ve Seri (Serial) testlerinin her biri ikişer farklı P-değeri verdikleri için ayrı testler olarak kabul edilmiştir. Buna göre toplam 17 farklı test tipi uygulanmıştır. Öte yandan, Çakışmayan Şablonlar (Nonoverlapping Templates) testi, Rastgele Gezintiler (Random Excursions) testi ve Rastgele Gezintiler Değiştirilmiş (Random Excursions Variant) testi resmi tanımları gereği her bir üreteç için sırasıyla 148, 8 ve 18'er kere uygulanmıştır. Uygulanan toplam kalan (17-3) + 148 + 8 + 18 = 188 adet testte gösterilen başarıyı ölçümü için 2 farklı temel ölçüt dikkate alınmıştır. İlk ölçüt adayın i'inci testten bağımsız denemeler neticesinde hangi oranda geçtiğini yansıtan $0 \leq B_i \leq 1$ başarı skorları toplamı $BST = \sum_{i=1}^{188} B_i$ ölçütü, diğer ölçüt ise adayın i'inci testten bağımsız denemeler neticesinde NIST STS tarafından belirtilen eşik değerini geçen $G_i = \{0, 1\}$ test toplamı $GTT = \sum_{i=1}^{188} G_i$. NIST test süiti uygulama sonuçlarını toplam 188 üzerinden detaylı olarak dikkate alan bu metrikler Hosseini vd. [18] tarafından geliştirilmiştir ve NIST tabanlı deneysel çalışmalarımızda karşılaştırmalı çalışma olabilmesi amacıyla doğrudan kullanılmışlardır. Ayrıca, aday üreteç başarısını tek bir kombine ölçüte indirgemek amacıyla, bu makalenin yazarı tarafından

iki ölçütü birlikte dikkate alan kombine skor ölçütü $KS = \sqrt{BST * GTT}$ önerilmiş ve uygulanmıştır. Buna göre, herhangi bir üretecin 17 farklı tipte NIST STS testinin uygulanması neticesinde alabileceği en fazla kombine skor 188'dir.

Uygulanan NIST STS testlerine ilişkin girdi tanımlamaları, sağlanan koşullar ve uygulama parametre değerlerine ilişkin bilgiler Tablo 1'de görülmektedir. Teste tabi tutulan her bir dizinin uzunlukları, uzun dizi boyu gerektiren testler olan Rastgele Gezintiler (Random Excursions), Rastgele Gezintiler Değiştirilmiş (Random Excursions Variant), Çakışan Şablon (Overlapping Template), Maurer'in Evrensel (Maurer's Universal Test) ve Doğrusal Karmaşıklık (Linear Complexity) testleri için n ≥ 1.000.000 bit; Derece (Rank) testi için n = 100.000 olarak alınmıştır. Uzun dizi boyu gerektirmeyen kalan tüm testler için n = 25.000 bit ve örneklem sayısı 100 adet alınmıştır.

Dizi değerlendirmeleri sıfır hipotezi: "Verilen ikili (binary) dizi rastgeledir" şeklindedir. P ∈ [0,1] ve anlamlılık düzeyi α = 0,01 olarak alınmıştır. Başarı kriteri P ≥ α olmasıdır. Aksi halde dizinin yeterince rastgele olduğu söylenemez. Uygulanan testlerde 512 adet doğrusal hücresel özdevinir rastgele sayı üreteci dikkate alınmıştır. Her bir üreteç için 0,05 ve 0,95 arasında 0,05 adım büyüklüğü ile 19 adet farklı başlangıç yoğunluk/doluluk (0-boş, 1-dolu olmak üzere) oranları (ρ) dikkate alınmıştır. Rastgele Gezintiler (Random Excursions) ve Rastgele Gezintiler Değiştirilmiş (Random Excursions Variant) testleri, tanımları gereği üretilen ve her biri 1.000.000 bit

**Tablo 1.** NIST STS testleri parametre açıklamaları ve deneylerde uygulanan değerler
(Explanations about NIST STS test parameters and the values applied in the experiments)

| Test Adı | Koşul ve Büyüklükler | Açıklama | Deney Değeri |
|---|---|---|---|
| Frekans (Frequency) | $n \geq 100$ | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Blok Frekans (Block Frequency) | $n \geq N * M$ | $M$ : Blok uzunluğu | $M$ = 128 |
| | | $N$ : Çakışmayan blok sayısı | $N$ = 195 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Birikimsel Toplamlar - 1 (Cumulative Sums - 1) | $n \geq 100$ | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Birikimsel Toplamlar - 2 (Cumulative Sums - 2) | $n \geq 100$ | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Çalıştırımlar (Runs) | $n \geq 100$ | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| En Uzun Çalıştırım (Longest Run) | $n \geq 6272$ eğer $M = 128$ ise | $M$ : Blok uzunluğu | $M$ = 128 |
| | | $N$ : Blok sayısı | $N$ = 195 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Derece (Rank) | $n \geq N * M * Q$ | $M$ : Matris satır sayısı | $M$ = 32 |
| | | $Q$ : Matris sütun sayısı | $Q$ = 32 |
| | | $N$ : Matris sayısı | $N$ = 97 |
| | | $n$ : Girdi uzunluğu | $n$ = $10^5$ |
| Ayrık Fourier Dönüşümü (Discrete Fourier Transform) | $n \geq 1000$ | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Çakışmayan Şablon (Nonoverlapping Template) | $N \leq 100$ | $N$ : Bağımsız blok sayısı | $N$ = 8 |
| | $M > 0.01 * n$ | $m$ : Her bir şablon boyu | $m$ = 9 |
| | $N = \lfloor \frac{n}{M} \rfloor$ | $M$ : Alt dizi boyu | $M$ = 3.125 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Çakışan Şablon (Overlapping Template) | $\lambda = (M - m + 1)/2^m \approx 2$ | $N$ : Alt dizilerin sayısı | $N$ = 968 |
| | | $m$ : 1'lerin blok boyu | $m$ = 16 |
| | $m \approx log_2^M$ | $M$ : Alt dizi boyu | $M$ = 1032 |
| | $N = \lfloor \frac{n}{M} \rfloor$ | $n$ : Girdi uzunluğu | $\lambda$ = 0,015 |
| | | | $n$ = $10^6$ |
| Maurer'in Evrensel Testi (Maurer's Universal Test) | $K = \lceil \frac{n}{L} \rceil - Q$ | $L$ : Her bir blok uzunluğu | $L$ = 7 |
| | $Q = 10 * 2^L$ | $Q$ : Başlangıç dizi blok sayısı | $Q$ = 1280 |
| | $n \geq (Q + K) * L$ | $K$ : Çakışmayan blok sayısı | $K$ = 141.577 |
| | | $n$ : Girdi uzunluğu | $n$ = $10^6$ |
| Yaklaşık Entropi (Approximate Entropy) | $m < \lfloor log_2^n \rfloor - 5$ | $m$ : Blok uzunluğu | $m$ = 6 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Rastgele Gezintiler (Random Excursions) | $n \geq 10^6$ | $n$ : Girdi uzunluğu | $n$ = $10^6$ |
| Rastgele Gezintiler Varyantı (Random Excursions Variant) | $n \geq 10^6$ | $n$ : Girdi uzunluğu | $n$ = $10^6$ |
| Seri-1 (Serial-1) | $m < \lfloor log_2^n \rfloor - 2$ | $m$ : Blok uzunluğu | $m$ = 4 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Seri-2 (Serial-2) | $m < \lfloor log_2^n \rfloor - 2$ | $m$ : Blok uzunluğu | $m$ = 4 |
| | | $n$ : Girdi uzunluğu | $n$ = 25.000 |
| Doğrusal Karmaşıklık (Linear Complexity) | $500 \leq M \leq 5000$ | $M$ : Blok uzunluğu | $M$ = 950 |
| | $N \geq 200$ | $N$ : Alt dizilerin sayısı | $N \cong$ 1150 |
| | $n \geq N * M$ | $n$ : Girdi uzunluğu | $n \cong 1{,}1 *$ $10^6$ |
| | $n \geq 10^6$ | | |

boyunda 100'er adet örneklemin tümü için değişebilen örneklem oranlarında uygulanmıştır. Bu testler için NIST STS tarafından belirlenmiş eşik değerleri başarı kriteri olarak alınmıştır. Örneğin, 100 adet adaydan testin tanımı gereği 70 adet örneklemin uygulanabilmesi durumda eşik değeri yaklaşık 66 değer olmuştur. Bu iki testin dışındaki tüm testler için, uygulanan 100 adet örneklem testinden 96 ve üzeri başarı kriteri olarak kabul edilmiştir. Test süiti tarafından dinamik olarak hesaplanan söz konusu %96 kabul edilebilir başarı eşiği, $\hat{p} \pm k\sqrt{\frac{\hat{p}(1-\hat{p})}{n}}$ şeklinde tanımlı güven aralığı tanımına dayanmaktadır. Formülasyonda, güven düzeyi $\hat{p} = 1 - \alpha = 1 - 0{,}01 = 0{,}99$, standart sapmaların sayısı $k = 3$ ve örneklem sayısı $n = 100$ olduğu düşünülürse, kabul edilebilir başarı eşiği $0{,}99 \pm 3\sqrt{\frac{0{,}99(1-0{,}99)}{100}} = 0{,}96015 \approx 0{,}96$'dır. NIST STS paketi eşik değeri hesaplama detayları için [27].

### *3.2. AIS31 Test Süiti Rastgelelik Testleri*
*(AIS31 Test Suit Randomness Tests)*

AIS31 test süiti gerçek rastgele sayı üreteçlerinin testi amacıyla Killmann ve Schindler [28] tarafından geliştirilmiş bir test süitidir. Bu sebeple, literatürdeki sözde rastgele sayı üreteçlerine ilişkin karşılaştırmalı çalışmalarda tercih edilmemektedir [36]. Buna rağmen çalışmamızda AIS31 rastgelelik testleri uygulanmıştır. Süit, Ayrıklık Testi (Disjointness Test-T0); Monobit Testi (Monobit Test-T1); Poker Testi (Poker Test-T2); Çalıştırım Testi (Run Test-T3); Uzun Çalıştırım Testi (Long Run Test-T4); Otokorelasyon Testi (Autocorrelation Test-T5); Tektip Dağılım Testi (Uniform Distribution Test-T6a ve T6b); Karşılaştırmalı Çok Terimli Test (Comparative Multinomial Test-T7a ve T7b) ve Entropi Testi (Entropy Test-T8) bileşenlerinden oluşmaktadır. Prosedür A olarak adlandırılan ve T0 ve T1'den T5'e kadar olan testlerden oluşan kısım ve Prosedür B olarak adlandırılan ve T6a, T6b, T7a, T7b ve T8 testlerinden oluşan kısım, AIS31 test süitini oluşturan 2 temel prosedürü tanımlamaktadır. T0 testi için gereken en azından 3.145.728 bit boyunda dosyalar oluşturulması, T1'den T5'e kadar olan testler için en azından 5.140.000 bit boyunda dosyalar oluşturulması ve T6a'dan T8'e kadar olan Prosedür B testleri için en azında 7.200.000 bit boyunda dosyalar oluşturulması şartları 120.000.000 bit boyunda olan üretim dosyaları oluşturulmasıyla sağlanmıştır.

Prosedür A'nın tanımı gereği, bir kere uygulanan T0 testinin yanısıra T1'den T5'e kadar olan testler her bir diziye 257'şer kere uygulanmıştır. Sonuç olarak Prosedür A kapsamında 1+5x257=1286 test uygulanmıştır. Prosedür B ise tanımı gereği, T6a, T6b ve T8 testleri için birer kere, T7a testi için 2 kere, T7b testi için ise her bir diziye 4'er kere uygulanmıştır. Sonuç olarak Prosedür B kapsamında dizi başına 1+1+2+4+1=9 test uygulanmıştır. Testlerde kullanılan doğrusal özdevinirler çıktı dosyaları örneklem zaman derinliği değeri d=64 olacak şekilde oluşturulmuştur. Dosyalara yazılan değerler 1 bayt = 8 bit formatında oluşturulmuştur. Kısım 3.1'de bahsi geçen ve Hosseini vd. [18] tarafından geliştirilen üretece ilgili çalışmada AIS31 testi uygulanmadığı için yapılan AIS31 tabanlı karşılaştırmalı çalışmada bu üreteç dikkate alınmamıştır.

### *3.3. TestU01 Test Süiti Rastgelelik Testleri*
*(TestU01 Test Suit Randomness Tests)*

TestU01 istatistiksel test süiti, üretilmiş herhangi bir sayı dizisinin rastgeleliğini sıkı bir şekilde incelemek için kullanılan çeşitli istatistiksel testleri içeren bir C programlama dili kütüphanesidir [29]. Kütüphanenin kullanım şekli ilgili kütüphane fonksiyonlarını yazılan kod içerisinden doğrudan çağırma yoluyla olabildiği gibi 32-bitlik ikili (binary) formatta üretilmiş rastgele sayı dizisi dosyalarının verilen bir örneklem boyu için baştan itibaren işlenmesi şeklinde de olabilmektedir. Sayı dizinin içeriği adının da ima ettiği gibi (0, 1) aralığında tanımlı tek biçimli (uniform) rastgele dağılımlı veya bit dizisi olabilmektedir. Üretilen 32-bit'lik ikili formattaki sayılar bağlamında sayı üretim değer aralığı [0, $2^{32}$ -1]'dir.

Bir endüstri normu haline gelmiş olan TestU01 süiti çeşitli bataryalardan oluşmaktadır. Bu makalede uygulanan Rabbit test bataryası özellikle ikili diziler için tasarlanmıştır ve 38 adet istatistikten oluşmaktadır. Bu istatistikler: Çok Terimli Bitler (MultinomialBitsOver); Yakın İkililer Bit Eşlemesi (ClosePairsBitMatch) 2 ve 4 boyutta; Görünüm Boşlukları (AppearanceSpacings); Doğrusal Karmaşıklık (LinearComplexity) 2 adet; LempelZiv; Fourier1 ve Fourier3 Spektral; En Uzun Ardışık 1'ler (LongestHeadRun); Dizilerdeki Peryotlar (PeriodsInStrings); 32-bit blok boyutlu Hamming Ağırlığı (HammingWeights); 32, 64 ve 128 bitlik Hamming Korelasyon (HammingCorr); 16, 32 ve 64 bitlik Hamming Serbestlik (HammingIndep); 1 ve 2 Gecikmeli Otokorelasyon (AutoCor); Bit Koşturum (RunOfBits) 2 adet; 32x32 matris boyutu için Matris Derece (MatrixRank) ve 128, 1024 ve 10016 yürüyüş boylarında H, M, J, R, C Rastgele Yürüyüş 1 (RandomWalk1) testlerine temel teşkil ederler. Testlerden geçme kriteri, p-değerinin 0.001 ve 0.999 arasında olmasıdır. Test edilen her bir bit dizisinin boyu $10^6$ bit olmuştur. Üretilen rastgele sayılar 32-bit ikili (binary) sayılardır. Kısım 3.1'de bahsi geçen ve Hosseini vd. [15] tarafından geliştirilen üretece ilgili çalışmada TestU01 testi uygulanmadığı için yapılan TestU01 tabanlı karşılaştırmalı çalışmada bu üreteç dikkate alınmamıştır.

## 4. Deneysel Sonuçlar ve Tartışmalar
**(Experimental Results and Discussions)**

### *4.1. NIST Sonuçları ve Tartışmaları (NIST Results and Discussions)*

Bölüm 2'de tanımlanan teorik model ve Bölüm 3'te tanımı verilen deneysel kurulumlara dayanılarak yapılan deneyler sonucunda, $\rho$ belirtilen başlangıç yoğunluk oranı olmak üzere ilk adım olarak uygulanan NIST testlerinde başarılı olan 7 adet doğrusal hücresel özdeviniri tanımlayan örüntüler Şekil 2'de görülmektedir. Örüntülerin altında yer alan (XXX:0,YY) formatındaki gösterimde, XXX özdevinir numarasını, 0,YY ise başlangıç durum yoğunluğu oranını göstermektedir. Örüntüler, ilgili kuralın katsayılar ($c_0$-$c_8$) tabanlı gösterimleri olup başlangıç durum yoğunluklarıyla ilgisi yoktur.


**Şekil 2.** Saptanan başarılı hücresel özdevinirlerin örüntü tabanlı tanımlamaları ve başlangıç durum yoğunlukları
(The pattern-based descriptions of the identified successful cellular automata and their initial state densities)

Saptanan 7 adet başarılı özdevinirden biri olan DHÖ Kural 95:0,25 tarafından üretilmiş ve örneklem derinliği d = 64 olan her biri 32-bit boyunda 10 adet örnek sayı dizisi Tablo 2'de görülmektedir. Rastgele üretilen 1.000.000 sayıdan farklı olanların sayısı 6380 adettir. Şekil 3'te tekrar eden farklı sayılara ilişkin tekrar istatistiği verilmiştir. Buna göre üretilen 380 adet sayı 1 kere (380x1=380); 2.380 adet sayı 166 kere (2.380x166=395.080) ve 3.620 adet sayı 167 kere (3.620x167=604.540) tekrar etmiştir.

DHÖ Kural 95:0,25 tarafından üretilmiş örnek 1.000.000 adet 32-bitlik sayıya ait durum uzayı ise Şekil 4'te görülmektedir. Çizgedeki her bir düğüm rastgele üretilmiş bir sayıyı, yönlendirilmiş oklar ise sayıların ardışık dizilişlerini göstermektedir. Bu örnekte ilk üretilen sayı $(2025632517)_{10}$ olmuştur. Takip eden ve kırmızı oklar ile tanımlı ilk döngünün boyu ise 6.399 sayıdır. Sonrasında mavi oklar ile tanımlı ve boyu 5.601 sayı olan döngüye girilmektedir. Mavi döngü sonrasında boyu 6.399 olan siyah oklarla tanımlı döngüye girilir. Bu adımdan sonra tekrar mavi, tekrar siyah, tekrar mavi vs. sırasıyla her bir mavi-siyah ikili döngüsü boyunca 12.000 sayı üretilir. Mavi-siyah ikili döngüsü 82 kere tekrar etmektedir. 83'üncü Mavi-Siyah ikili döngüsünde mavi yörünge boyunca üretilen 5.601 rastgele sayıyı takiben siyah yörünge boyunca üretilen 3.999 sayı neticesinde (1 + 6.399 + 82*(5.601+6.399) + 5.601 + 3.999) = 1.000.000 sayı üretilmiş olur. Üretilen son sayı $(3530663397)_{10}$'dir. Dikkate edilecek olursa, asimetrik olan mavi ve siyah yörüngeler boyunca üretilen $(951890693)_{10}$ sayısını takiben mavi yörüngede $(279662659)_{10}$ sayısı üretilir ve mavi yörünge başa dönmüş olur. Siyah yörüngede ise $(951890693)_{10}$ sayısını takiben döngü, ilk yörünge olan kırmızı yörüngeye girer ve $(279662659)_{10}$ sayısının üretilmesiyle siyah yörünge döngüsü kapanmıştır.

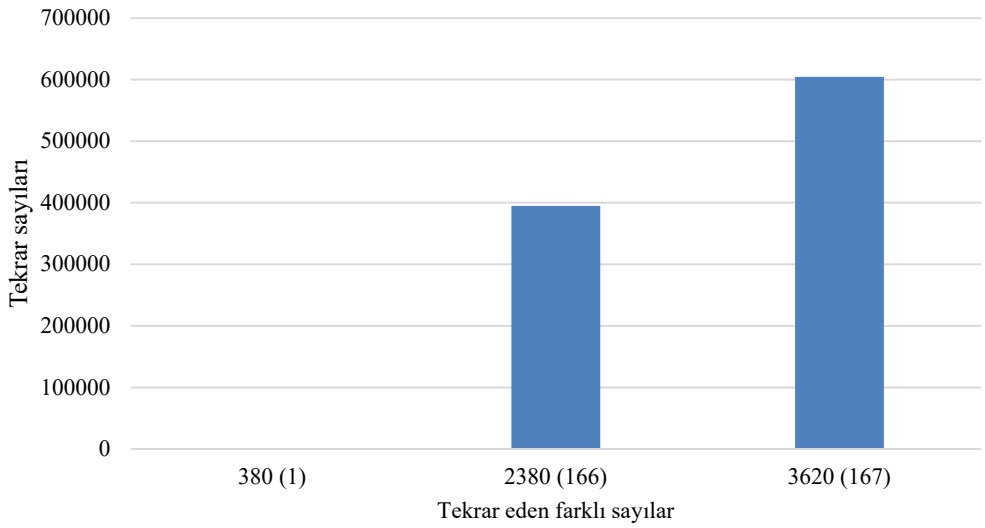
Başarı düzeyi en düşük olan özdevinirlerden biri olan DHÖ Kural 0:0,50 tarafından üretilmiş ve örneklem derinliği d = 64 olan her biri 32-bit boyunda 10 adet örnek sayı dizisi Tablo 3'de görülmektedir. DHÖ Kural 0:0.50 sadece 2 farklı 32-bit'lik sayı üretilebilmiştir. Bu sayılar: $(10000000000000000000000000000000)_2$ ve $(00000000000000000000000000000000)_2$'dir. Bu sayıların onluk sistem karşılıkları: $(4294967296)_{10}$ ve $(0)_{10}$.'dır.

Bu iki sayının üretilen 1.000.000 sayı için frekans dağılımı Şekil 5'te yer almaktadır. DHÖ Kural 0:0.50'nin t=0 ilk adımdan sonraki tüm hücre değerlerini doğrudan 0 değerine sabitlemesi dikkate alındığında, t=0 adımındaki 20x20=400 değerin kuralın yarı yoğunluğu oluşturan 400/2=200 adedinin başlangıç değeri olarak 1 değerine sahip olacağı 32-bit'i oluşturan kalan 31-bit'lik kısmından 0'lardan oluşacağı açıktır. Ayrıca, zaman derinliği olarak d=64 alınmasına karşın sayı üretiminde 32-bit'lik sayılar üretilmesi sebebiyle kalan 999.800 adet sayının tümü 0 olmuştur.

DHÖ Kural 0:0,50 tarafından üretilmiş örnek 1.000.000 adet 32-bitlik sayıya ait durum uzayı Şekil 6'da görülmektedir. Bu örnekte ilk üretilen sayı $(4294967296)_{10}$, son üretilen sayı $(0)_{10}$'dır. Takip eden

**Tablo 2.** Örneklem derinliği d = 64 olan, doğrusal hücresel özdevinir Kural 95:0.25 tarafından üretilmiş 32-bit boyunda ilk 10 adet örnek rastgele sayı dizisi ve onluk sistem karşılıkları (First 10 example 32-bit random number sequences generated and their equivalent decimal values by linear cellular automaton Rule 95:0.25 having sampling depth d = 64)

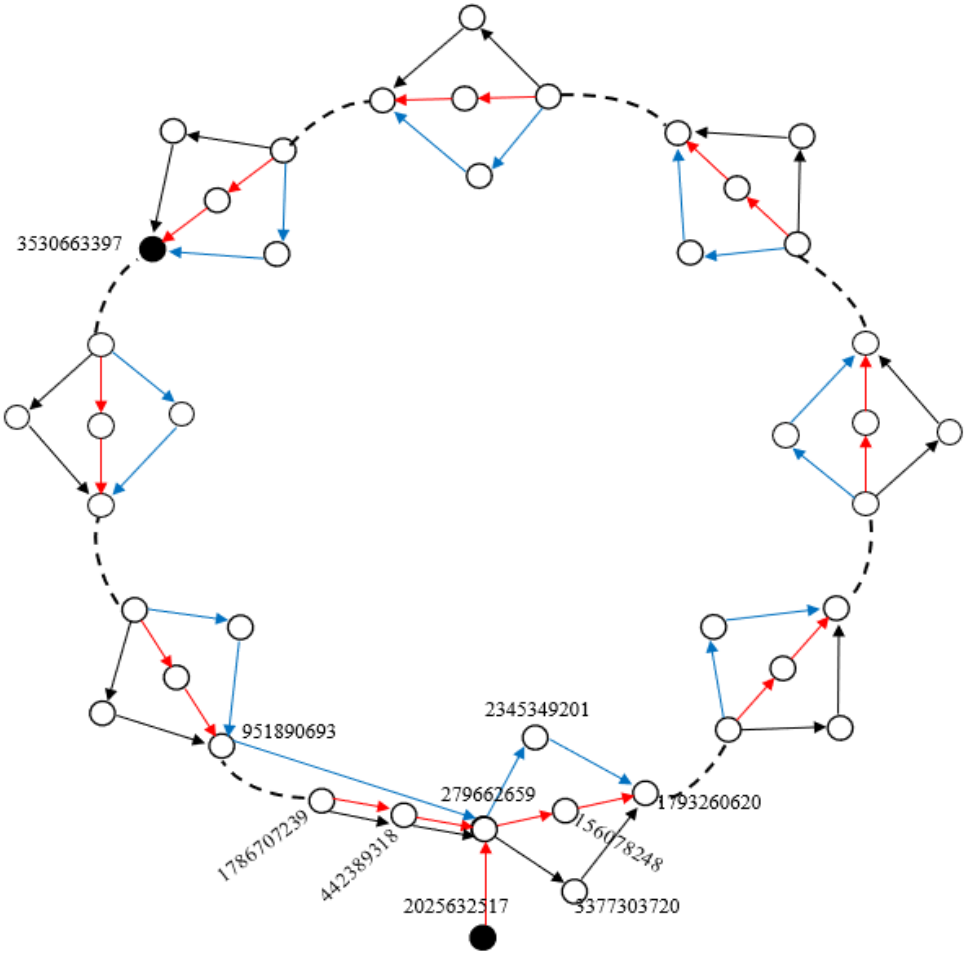
| 32-bit'lik İkili Değer | Onluk Sistem Karşılığı |
|---|---|
| $(01111000101111001011001100000101)_2$ | $(2025632517)_{10}$ |
| $(00010000101010110101000001000011)_2$ | $(279662659)_{10}$ |
| $(00001001010011011001000010101000)_2$ | $(156078248)_{10}$ |
| $(01101010111000101111110001001100)_2$ | $(1793260620)_{10}$ |
| $(00101001001010110010110001001101)_2$ | $(690695245)_{10}$ |
| $(11011001011101010010010011101001)_2$ | $(3648333033)_{10}$ |
| $(10011000000111001100111100100111)_2$ | $(2552024871)_{10}$ |
| $(01011101100001000011110001001100)_2$ | $(1568947276)_{10}$ |
| $(10101011110000011100001100000110)_2$ | $(2881602310)_{10}$ |
| $(01000010010110111100001101001100)_2$ | $(1113310028)_{10}$ |




**Şekil 3.** DHÖ Kural 95:0,25 tarafından üretilen örnek 1.000.000 sayı için tekrar eden 6380 farklı sayıya ait tekrar istatistiği (Repetition statistics of 6380 different numbers repeated in 1,000,000 example numbers produced by LCA Rule 95:0.25)

ve kırmızı oklar ile tanımlı yörüngenin boyu ise 800 sayıdır. Kırmızı yörünge boyunca üretilen sayıların 200 adedi $(4294967296)_{10}$ kalanlar ise $(0)_{10}$'dır. 801'inci sayıdan itibaren mavi yörünge boyunca üretilen kalan 999200 sayı yine $(0)_{10}$'dır. 200 + 600 + 999.200 = 1.000.000.

Toplam 9728 adet aday üreteç arasından saptanan 7 başarılı üreteç için seçim kriteri $BST > 186{,}5$ ve $GTT > 184$ olmuştur. Karşılaştırmalı çalışma amacıyla, NIST test süiti içerisinde yer alan ve literatürde bilinen toplam 11 adet rastgele sayı üretecinin başarı skorları ayrıca dikkate alınmıştır. Şekil 2'de yer alan 7 üretecin NIST test süitinde yer alan üreteçlerin çoğundan daha başarılı skorlar elde ettikleri gözlemlenmiştir. Bu üreteçlerden en başarılı olan 2 adedinin (DHÖ Kural 471:0,70 ve DHÖ Kural 95:0,25), NIST test süitinde yer alan 9 adet üreteçten, literatürde yer alan Mersenne Twister üretecinden [37] ve yine literatürde yer alan Hosseini vd. [18] tarafından önerilmiş üreteçten daha iyi başarı skor toplamı ve kombine skor elde ettiği Tablo 4'te görülmektedir. Eşik değeri tabanlı olan geçilen test toplamı (GTT) ölçütüne göre ise, 188 adet testin tümünden geçebilen Hosseini vd. [18] üreteci ve test süitinde yer alan Doğrusal Eşleşik (Linear Cong.) üretecinin yanısıra, kombine skor performansları iyi olan Mersenne Twister ve Blum-Blum-Shub üreteçleri ve süitte yer alan XOR üreteci dışındaki 6 adet başarılı üretecin kaliteli sözde rastgele sayı üretimi amacıyla dikkate alınabileceği uygulanan NIST testleri sonucunda gözlemlenmiştir. Üretilen verilerin detaylı tam dökümü,




**Şekil 4**. DHÖ Kural 95:0,25 tarafından üretilmiş 1.000.000 adet 32-bitlik örnek sayıya ait durum uzayı
(State space of 1,000,000 32-bit sample numbers generated by LCA Rule 95:0.25).

**Tablo 3.** Örneklem derinliği d = 64 olan, doğrusal hücresel özdevinir Kural 0:0.50 tarafından üretilmiş 32-bit boyunda ilk 10 adet örnek rastgele sayı dizisi ve onluk sistem karşılıkları (First 10 example 32-bit random number sequences generated and their equivalent decimal values by linear cellular automaton Rule 0:0.50 having sampling depth d = 64)

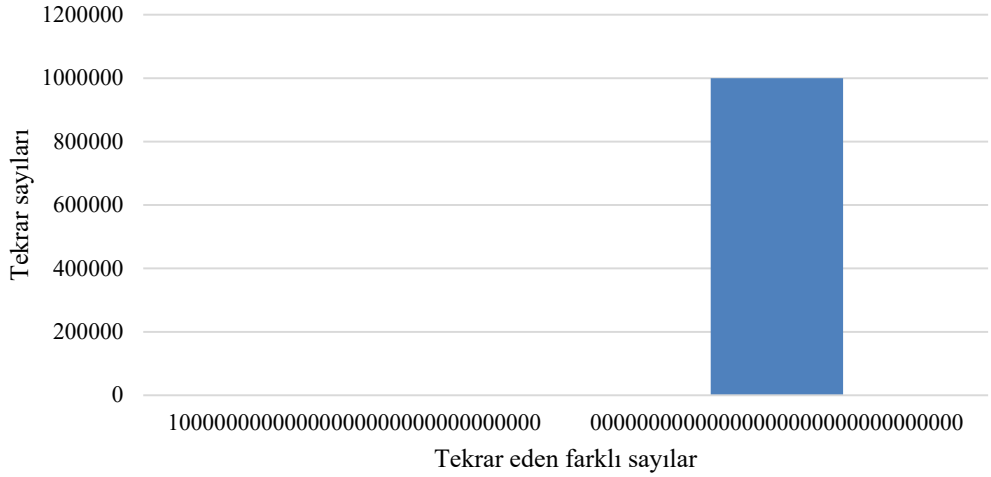
| 32-bit'lik İkili Değer | Onluk Sistem Karşılığı |
|---|---|
| $(10000000000000000000000000000000)_2$ | $(4294967296)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(10000000000000000000000000000000)_2$ | $(4294967296)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |
| $(00000000000000000000000000000000)_2$ | $(0)_{10}$ |

okuyucu tarafından talep edilmesi durumunda yazar tarafından sağlanabilir.


**Şekil 6**. DHÖ Kural 0:0,50 tarafından üretilmiş 1.000.000 adet 32-bitlik örnek sayıya ait durum uzayı (State space of 1,000,000 32-bit sample numbers generated by LCA Rule 0:0.50).

### *4.2. AIS31 Sonuçları ve Tartışmaları*
*(AIS31 Results and Discussions)*

Tablo 4'de yer alan 18 üretecin, yazarları tarafından AIS31 testi uygulanmamış olan Hosseini vd. [18] üreteci dışında kalan 17'sine ikinci kademe testi olarak hücresel özdevinirler tabanlı sözde rastgele sayı üretimi literatüründe genellikle uygulanmayan AIS31 testi uygulanmıştır. AIS31 testi bileşenlerinden olan Prosedür A uygulaması neticesinde elde edilen sonuçlar Tablo 5'de, Prosedür B uygulaması neticesinde elde edilen sonuçlar ise Tablo 6'da görülmektedir. Prosedür A sonuçlarına göre NIST testi aşamasında başarılı olan 7 adet doğrusal hücresel özdevinirin hiçbirinin AIS31 Ayrıklık testinden (Test-0) geçemediği, benzer şekilde DHÖ Kural 95:0,25 dışındaki 6 özdevinirin hiçbirinin AIS31 Otokorelasyon testinden (Test-5) tam başarıyla geçemediği görülmüştür (Tablo 5). Benzer şekilde söz konusu 7 testin hiçbiri, AIS31 Karşılaştırmalı Çok




**Şekil 5.** DHÖ Kural 0:0.50 üreteci tarafından üretilen 1.000.000 sayıyı oluşturan 2 sayının frekans istatistiği
(Frequency statistics of 2 numbers that constitute 1,000,000 numbers generated by LCA Rule 0:0.50)

**Tablo 4.** Literatürde yer alan 11 rastgele sayı üretecinin ve başarılı 7 doğrusal hücresel özdevinir üretecin NIST STS tabanlı başarı skorları
(NIST STS based success scores of 11 random number generators in literature vs. successful 7 linear cellular automata generators)

| Üreteç | Başarı Skor Toplamı (BST) $\sum_{i=1}^{188} B_i$ | Geçilen Test Toplamı (GTT) $\sum_{i=1}^{188} G_i$ | Kombine Skor (KS) $\sqrt{BST * GTT}$ |
|---|---|---|---|
| DHÖ Kural 471:0,70 | 187,72 | 187 | 187,36 |
| DHÖ Kural 95:0,25 | 187,56 | 187 | 187,28 |
| Hosseini vd. | 186,14 | 188 | 187,07 |
| Doğrusal Eşleşik | 185,90 | 188 | 186,95 |
| Mersenne Twister | 186,28 | 187 | 186,64 |
| DHÖ Kural 29:0,50 | 186,91 | 186 | 186,45 |
| DHÖ Kural 382:0,30 | 187,05 | 185 | 186,02 |
| DHÖ Kural 351:0,45 | 186,78 | 185 | 185,89 |
| Blum-Blum-Shub | 185,68 | 186 | 185,84 |
| DHÖ Kural 475:0,60 | 186,64 | 185 | 185,82 |
| DHÖ Kural 350:0,55 | 186,55 | 185 | 185,77 |
| Micali-Schnorr | 185,69 | 185 | 185,34 |
| Modüler Üs Alma | 185,54 | 185 | 185,27 |
| Kübik Eşleşik | 185,34 | 185 | 185,17 |
| İkinci Dereceden Eşleşik-2 | 185,19 | 184 | 184,59 |
| İkinci Dereceden Eşleşik-1 | 185,43 | 183 | 184,21 |
| SHA-1 Kullanan G | 184,94 | 183 | 183,97 |
| XOR | 114,28 | 26 | 54,51 |

Terimli Testlerinden biri olan Test 7b'den geçememiş ancak DHÖ Kural 95:0,25, DHÖ Kural 29:0,50 ve DHÖ Kural 351:0,45 Test 7a'dan ve diğer tüm Prosedür B testlerinden geçebilmişlerdir (Tablo 6). Diğer taraftan NIST test süitinde yer alan ancak bu süit bağlamında sınırlı başarı gösteren Micali-Schnorr, Modüler Üs Alma ve İkinci Dereceden Eşleşik-2 üreteçleri AIS31 testlerinin tümünden tam başarıyla geçmiştir. Bu üçlüye ek olarak, sözde rastgele sayı üretimi literatüründe başarılı olduğu bilinen Mersenne Twister üreteci de AIS31 testlerinin tümünden tam başarıyla geçmiştir (Tablo 5 ve Tablo 6). 7 adet doğrusal özdevinirin genel olarak NIST test süitinde yer almayan ancak AIS31 süitinde yer alan Ayrıklık testi, Otokorelasyon testi ve Karşılaştırmalı Çok Terimli Testlerinde başarısız olduğu dikkat çekmektedir. 7 doğrusal hücresel özdevinirin, özellikle Ayrıklık testi, Otokorelasyon testi ve Karşılaştırmalı Çok Terimli testlerin genişlik değeri 4 olanından geçememesi, bu üreteçlerin rastgele sayı oluşturma şekillerinin zaman içindeki örneklem derinliği (d) seçimine hassas olması ve gerekirci (deterministic) olmayabilen gerçek rastgele sayı üreteçlerinin niteliklerini de sınamayı hedefleyen AIS31 testinin uygulama açısından hücresel özdevinirler tabanlı üreteçlerin testine uygun olmaması olarak açıklanabilir.

### *4.3. TestU01 Sonuçları ve Tartışmaları*
### *(TestU01 Test Results and Discussions)*

Tablo 4'de yer alan 18 üretecin, yazarları tarafından TestU01 testi uygulanmamış olan Hosseini vd. [18] üreteci dışında kalan 17'sine diğer bir ikinci kademe testi olarak TestU01 uygulanmıştır. Hücresel özdevinirler tabanlı sözde rastgele sayı üretimi literatüründe 1B hücresel özdevinirler tipi üreteçlere TestU01 süiti nadiren uygulanmıştır. Bunlardan biri olan Zarezadeh'nin çalışmasında [38] uygulanan Crush bataryası ikili (binary) diziler için özel olarak geliştirilmemiştir. Süitte yer alan ve bu makalede uyguladığımız ve ikili (binary) diziler için özel olarak geliştirilmiş Rabbit bataryasının öncelikle uygulanması daha doğru bir seçimdir. Ayrıca Zarezadeh'nin çalışması 1B tek tip olmayan (non-uniform) bir hücresel özdevinir uygulaması olması açısından çalışmamızla doğrudan karşılaştırılabilir nitelikte değildir. TestU01 süitinin hücresel özdevinirlere uygulanmasına bir örnek olan ve 30 adet aday sözde rastgele sayı üretecini 7 adet doğrusal eşleşik (linear congruential), 16 adet doğrusal geri besleme öteleme yazmacı (linear feedback shift register) ve 7 adet 1B hücresel özdevinirler olmak üzere üç ana başlıkta

**Tablo 5.** Literatürde yer alan 10 rastgele sayı üreticinin ve 7 doğrusal hücresel özdevinir üretecin AIS31 Prosedür A uygulama başarı skorları (AIS31 Procedure A application success scores of 10 random number generators in literature vs. the 7 linear cellular automata generators)

| Üreteç | Test-0 | Test-1 | Test-2 | Test-3 | Test-4 | Test-5 |
|---|---|---|---|---|---|---|
| DHÖ Kural 471:0,70 | *Başarısız* | 257/257 | 257/257 | 257/257 | 257/257 | *245/257* |
| DHÖ Kural 95:0,25 | *Başarısız* | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| Doğrusal Eşleşik | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| Mersenne Twister | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| DHÖ Kural 29:0,50 | *Başarısız* | 257/257 | 257/257 | 257/257 | 257/257 | *256/257* |
| DHÖ Kural 382:0,30 | *Başarısız* | *229/257* | *246/257* | 257/257 | 257/257 | *248/257* |
| DHÖ Kural 351:0,45 | *Başarısız* | 257/257 | 257/257 | *256/257* | 257/257 | *255/257* |
| Blum-Blum-Shub | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| DHÖ Kural 475:0,60 | *Başarısız* | 257/257 | 257/257 | 257/257 | 257/257 | *254/257* |
| DHÖ Kural 350:0,55 | *Başarısız* | 257/257 | 257/257 | 257/257 | 257/257 | *241/257* |
| Micali-Schnorr | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| Modüler Üs Alma | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| Kübik Eşleşik | Başarılı | *255/257* | *256/257* | 257/257 | 257/257 | 257/257 |
| İkinci Dereceden Eşleşik-2 | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| İkinci Dereceden Eşleşik-1 | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| SHA-1 Kullanan G | Başarılı | 257/257 | 257/257 | 257/257 | 257/257 | 257/257 |
| XOR | *Başarısız* | *216/257* | *150/257* | *119/257* | *245/257* | *88/257* |

**Tablo 6.** Literatürde yer alan 10 rastgele sayı üreticinin ve 7 doğrusal hücresel özdevinir üretecin AIS31 Prosedür B uygulama başarı skorları (AIS31 Procedure B application success scores of 10 random number generators in literature vs. the 7 linear cellular automata generators)

| Üreteç | Test-6a | Test-6b | Test-7a | Test-7b | Test-8 |
|---|---|---|---|---|---|
| DHÖ Kural 471:0,70 | Başarılı | Başarılı | *Başarısız* | *Başarısız* | Başarılı |
| DHÖ Kural 95:0,25 | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| Doğrusal Eşleşik | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| Mersenne Twister | Başarılı | Başarılı | Başarılı | Başarılı | Başarılı |
| DHÖ Kural 29:0,50 | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| DHÖ Kural 382:0,30 | Başarılı | Başarılı | *Başarısız* | *Başarısız* | Başarılı |
| DHÖ Kural 351:0,45 | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| Blum-Blum-Shub | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| DHÖ Kural 475:0,60 | Başarılı | Başarılı | *Başarısız* | *Başarısız* | Başarılı |
| DHÖ Kural 350:0,55 | Başarılı | Başarılı | *Başarısız* | *Başarısız* | Başarılı |
| Micali-Schnorr | Başarılı | Başarılı | Başarılı | Başarılı | Başarılı |
| Modüler Üs Alma | Başarılı | Başarılı | Başarılı | Başarılı | Başarılı |
| Kübik Eşleşik | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| İkinci Dereceden Eşleşik-2 | Başarılı | Başarılı | Başarılı | Başarılı | Başarılı |
| İkinci Dereceden Eşleşik-1 | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| SHA-1 Kullanan G | Başarılı | Başarılı | Başarılı | *Başarısız* | Başarılı |
| XOR | *Başarısız* | Başarılı | *Başarısız* | *Başarısız* | *Başarısız* |

**Tablo 7.** Literatürde yer alan 10 rastgele sayı üreticinin ve 7 doğrusal hücresel özdevinir üretecin TestU01 Rabbit bataryası uygulama sonuçları (TestU01 Rabbit battery application results for 10 random number generators in literature vs. the 7 linear cellular automata generators)

| Üreteç | Başarıyla Geçilen Test Sayısı (38 üzerinden) | Başarı Durumu |
|---|---|---|
| DHÖ Kural 471:0,70 | 14 | *Başarısız* |
| DHÖ Kural 95:0,25 | 12 | *Başarısız* |
| Doğrusal Eşleşik | 38 | Başarılı |
| Mersenne Twister | 38 | Başarılı |
| DHÖ Kural 29:0,50 | 12 | *Başarısız* |
| DHÖ Kural 382:0,30 | 9 | *Başarısız* |
| DHÖ Kural 351:0,45 | 10 | *Başarısız* |
| Blum-Blum-Shub | 38 | Başarılı |
| DHÖ Kural 475:0,60 | 13 | *Başarısız* |
| DHÖ Kural 350:0,55 | 11 | *Başarısız* |
| Micali-Schnorr | 38 | Başarılı |
| Modüler Üs Alma | 38 | Başarılı |
| Kübik Eşleşik | 18 | *Başarısız* |
| İkinci Dereceden Eşleşik-2 | 28 | *Başarısız* |
| İkinci Dereceden Eşleşik-1 | 38 | Başarılı |
| SHA-1 Kullanan G | 38 | Başarılı |
| XOR | 1 | *Başarısız* |

gruplayıp bunların göreli performanslarını detaylı bir şekilde inceleyen Bhattacharjee vd.'nin [11] makalesi sonuçlarına göre, uygulanan 26 adet Rabbit bataryası testlerinin tümünden geçebilen herhangi bir üreteç olmamıştır. Yapılan derecelendirmede ise dikkate alınan 7 adet 1B hücresel özdevinirin arasında yer alan ve hücrelerin onlu (decimal) durum değeri alabildiği hücresel özdevinir en iyi performansı gösteren derece 1 (Rank 1) grubunda yer almıştır. Kural 30 kodlu 1B temel hücresel özdevinir (1D Elementary Cellular Automata) ise derece 3 (Rank 3) düzeyinde bir başarı gösterebilmiştir. Kalan 5 adet hücresel özdevinir tabanlı üreteç ise kayda değer başarı gösterememiştir. Bu çalışmadaki başarısız 5 adet 1B hücresel özdevinirin başarısızlık sebeplerinden biri olarak, rastgele sayı üretimi sırasında mevcut hücresel özdevinir konfigürasyonlarının topyekun veya blok olarak dikkate alınması gösterilmiştir [11]. TestU01 uygulanmış diğer bir 1B hücresel özdevinir olan ancak hücrelerin üçlü durum (tri-state) değeri alabildiği Bhattacharjee vd.'nin [21] çalışmasında yazarlar kendi belirledikleri ve kısmen de TestU01 süitinden aldıkları testlerden oluşan uygulamalarının neticesinde, önerdikleri 1B üçlü durum hücresel özdevinir üretecinin literatürdeki en iyi üreteçlerden bir olduğu bilinen 1B Kural 30 hücresel özdevinirinden daha iyi sonuç verdiğini duyurmuştur. Öte yandan, aynı yazarların 1B üçlü durum hücresel özdevinirlerden oluşan ve listesini verdikleri potansiyel rastgele sayı üreteçlerini bildiren detaylı çalışmalarında, TestU01 süitinde yer alan ve ikili (binary) diziler için özel olarak tasarlanmış Rabbit bataryasında yer alan 25 adet test uygulanmış ve aday üreteçlerin, uygulanan testlerden ancak 12-15 arasında sayıdaki testte başarılı olabildikleri belirtilmiştir [39].

Yukarıdaki sonuçlar bağlamında 2B hücresel özdevinirler için uygulamasına literatürde rastlamadığımız TestU01 için elde edilen sonuçlar Tablo 7'de görülmektedir. Rabbit bataryasında yer alan 38 adet testin tümünü önceden belirlediğimiz başarılı 7 adet DHÖ'ye uyguladığımız bu çalışmada, başarıyla geçilebilen test sayısı ancak 9-14 arasında olmuştur. Buna karşın, Doğrusal Eşleşik, Mersenne Twister, Blum-Blum-Shub, Micali-Schnorr, Modüler Üs Alma, İkinci Dereceden Eşleşik-1 ve SHA-1 Kullanan G üreteçlerinin tümü 38 testin tümünden başarıyla geçebilmişlerdir.

Bhattacharjee ve Das'ın detaylı literatür çalışmalarında [11] dikkat çekildiği üzere: "Genel olarak, kriptografik olmayan basit sözde rastgele sayı üreteçleri NIST test süiti testlerinden geçememektedirler. Bununla birlikte, TestU01 ve Diehard testlerinin tümünü veya çoğunu geçen iyi bir sözde rastgele sayı üreteci, NIST testlerinde de iyi performans gösterir. Bu nedenle, kriptografik olarak güvenli olmayan iyi bir sözde rastgele sayı üreteci, bazı başlangıç durumları için (seed) tüm NIST testlerini geçebilir" [11]. Bu yorum Tablo 7'de alınan sonuçları kısmen açıklamakla birlikte, denenen çok sayıda farklı başlangıç durum yoğunluklarını dikkate alan detaylı çalışmamızda alınan başarılı NIST ancak başarısız TestU01 test neticelerinin sebebini tam olarak açıklamamaktadır. TestU01 sonuçlarının dikkate alınan 2B doğrusal DHÖ'ler açısından başarısızlığının potansiyel bir sebebi, rastgele sayı üretimi sırasında kullanılan zaman derinliğidir (d=64 değeri) denilebilir. Amaca yönelik olarak farklı derinlik değerlerinin denenmesinin yanısıra, sayı oluşturumunun zaman boyutunda değil zaman noktasındaki uzaysal konum dikkate alınarak yapılması da alternatif bir yaklaşım olabilir. Diğer taraftan, temel bir sebep, çalışmada dikkate aldığımız hücresel özdevinirlerin doğrusal hücresel özdevinirler olmalarıdır. Bataryada yer alan kimi testlerde aranan nitelikli sözde rastgele sayı üretiminin doğrusal olmayan üreteçler tarafından üretilmesi gereksinimi, elde edilen sonuçları yetersizliğini açıklamaktadır.

### *4.4. Başlangıç Durum Yoğunluklarına İlişkin Sonuçlar ve Tartışmalar (Results and Discussions On Initial State Densities)*

NIST testinden geçen en başarılı 7 adet özdevinire ait tüm farklı başlangıç durum yoğunlukları dikkate alındığında özdevinir ne olursa olsun başlangıç yoğunluk oranı %25'den az veya %70'den fazla

olması durumunda başarılı rastgele sayı üreteci gözlemlenmemiştir. Bu durum, alınan NIST tabanlı sonuçların saptanan üreteçlerin tüm başlangıç yoğunluk değerleri için genellemenin doğru olmayacağını kabaca ortaya koymaktadır. Tablo 8'de yer alan, en başarılı 7 özdevinire ait 0,5 ile 0,95 arasında değişen 19 adet farklı başlangıç durum yoğunlukları için elde edilen BST, GTT ve KS performans ortalama ve standart sapma değerlerinden görüldüğü üzere sonuçların tümü 171'in altında kalan düşük ortalama skor değerine ve en az 14,81 olan standart sapma değerine sahiptir. Bu üreteçlerin farklı başlangıç durum yoğunlukları için performans skorlarına bakıldığında ise başlangıç yoğunluğuna göre değişiklik göstermeyen tek düze dağılımdan (uniform distribution) ziyade normal dağılım (normal distribution) gösterdiği düşünülmektedir.

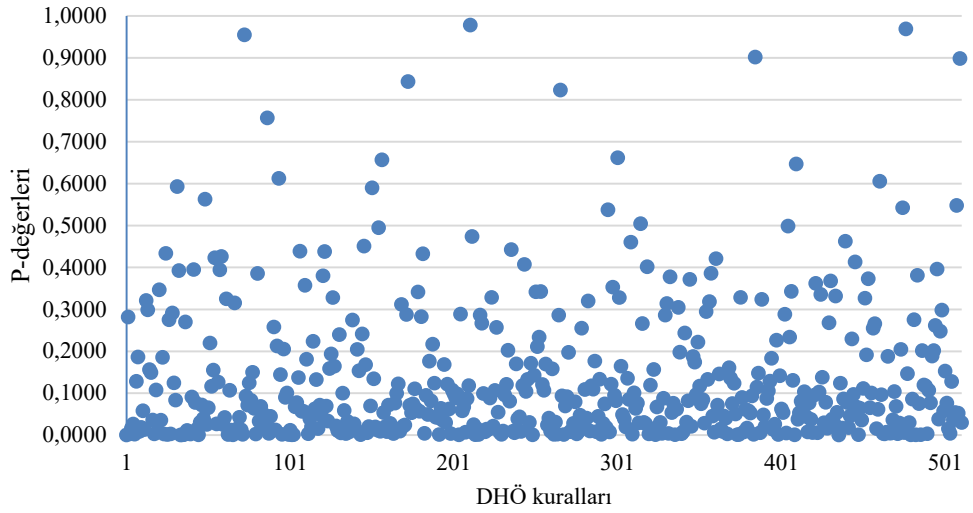
Bir genelleme yapabilmek adına sadece başarılı skor sonuçlarıyla yetinilmeyip tüm özdevinir skorlarına bakılması gerektiği açıktır ve bu amaçla, dikkate alınan 512 hücresel özdevinirin her birine 19 adet farklı başlangıç doluluk oranı için GTT ve BST sonuçları ayrı ayrı dikkate alınarak normal dağılım kontrolü amaçlı Shapiro-Wilk [40] testi uygulanmıştır. Test için sıfır hipotezi: "Hücresel özdevinir için ölçüm sonucu normal dağılım gösterir" şeklindedir. Uygulanan testlerde anlamlılık düzeyi α=0,01 kabul edilmiş olup aykırı (outlier) değerler hesaplamaya dahil edilmiştir. Öte yandan, hem BST hem de GTT sonuç değerleri tüm başlangıç doluluk oranları için 1 olan DHÖ Kural 0'a Shapiro-Wilk testi uygulanabilir nitelikte değildir ve bu özdevinire test uygulanmamıştır. GTT ve BST sonuçları dikkate alınarak kalan 511 özdevinir için hesaplanan P-değerleri sırasıyla Şekil 7 ve Şekil 8'de sunulmuştur. Toplam 511 özdevinirden GTT için 412'sinin BST için ise 326'sının normal dağılım gösteriyor olması dağılımın tek düze olduğu kabullenmesinin yanıltıcı olacağını göstermektedir.

## 5. Simgeler (Symbols)

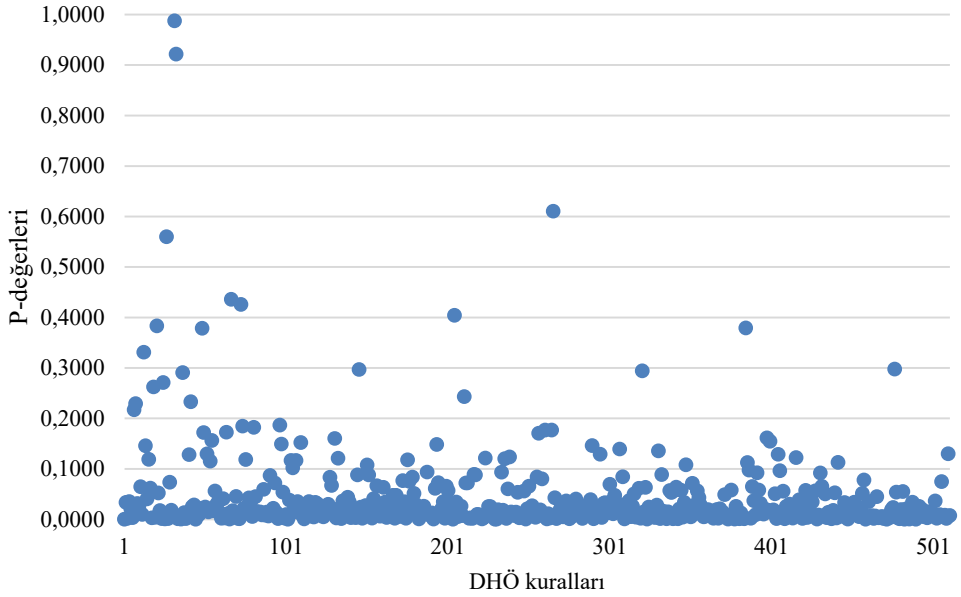
$1B, 2B, 3B$ : 1 boyut, 2 boyut, 3 boyut
$c_i$ : Doğrusal hücresel özdevinir $i$'inci hücre katsayısı
$d$ : Sayı oluşturum zaman adımı derinliği
$k$ : Tek bir hücrenin bulunabildiği farklı durum sayısı
$n$ : Girdi uzunluğu
$x_i^t$ : 1B bir hücresel özdevinirin $i$'inci hücresinin $t$ anındaki durum değeri
$x_{i,j}^t$ : 2B bir hücresel özdevinirin $(i,j)$'inci hücresinin $t$ anındaki durum değeri
$Z$ : Kare kafes hücresel özdevinirin bir boyutunun büyüklüğü
$\rho$ : Özdevinir başlangıç durum yoğunluğu
$\varphi$ : Hücre durum değişikliği fonksiyonu

**Tablo 8.** Başarılı 7 doğrusal hücresel özdevinir üretecin 19 farklı ilk yoğunluk değeri için BST, GTT ve KS ortalama ve standart sapma skor değerleri
(The mean and standard deviation values for 19 different initial densities of the 7 successful linear cellular automata generators)

| Üreteç (DHÖ Kural) | BST Ortalama | BST Std. Sap. | GTT Ortalama | GTT Std. Sap. | KS Ortalama | KS Std. Sap. |
|---|---|---|---|---|---|---|
| 29 | 158,66 | 17,42 | 151,26 | 20,22 | 154,89 | 18,82 |
| 95 | 166,25 | 16,44 | 158,16 | 18,06 | 162,14 | 17,23 |
| 350 | 164,09 | 14,81 | 155,89 | 16,39 | 159,93 | 15,57 |
| 351 | 165,77 | 15,58 | 158,32 | 16,24 | 161,99 | 15,85 |
| 382 | 162,81 | 15,87 | 156,05 | 17,01 | 159,39 | 16,41 |
| 471 | 170,97 | 16,31 | 162,37 | 17,70 | 166,60 | 16,93 |
| 475 | 163,50 | 16,87 | 153,84 | 18,85 | 158,58 | 17,82 |




**Şekil 7**. 511 adet DHÖ kuralına ait GTT değerleri için Shapiro-Wilk normal dağılım testi uygulanması sonucunda elde edilen P-değerleri (P-values obtained as a result of applying the Shapiro-Wilk normal distribution test for the GTT values of 511 LCA rul




**Şekil 8**. 511 adet DHÖ kuralına ait BST değerleri için Shapiro-Wilk normal dağılım testi uygulanması sonucunda elde edilen P-değerleri (P-values obtained as a result of applying the Shapiro-Wilk normal distribution test for the BST values of 511 LCA rules)

## 6. Sonuçlar (Conclusions)

İki boyutlu doğrusal tek tip hücresel özdevinirlerin başlangıç durum yoğunluklarının sözde rastgele sayı üretimlerine olan etkisi deneysel olarak incelenmiştir. Aday 512 üretecin 19 farklı başlangıç durum yoğunluğu oranları için iki kademe halinde önce NIST istatistiksel test süiti sonrasında AIS31 ve TestU01 süiti testleri uygulanmıştır. Ayrıca, dikkate alınan 512 hücresel özdevinirin her birine 19 adet farklı başlangıç doluluk oranı için geçilen test toplamı ve başarı skor toplamı ölçüm sonuçları ayrı ayrı dikkate alınarak normal dağılım kontrolü amaçlı Shapiro-Wilk testi uygulanmıştır. Bu testler sonucunda farklı özdevinirler için kayda değer sayıda özdevinir için dağılımın tek düze değil normal dağılım özelliği gösterdiği olduğu gözlemlenmiştir. Literatürde dikkate alınmayan ve farklı başlangıç durum yoğunlukları için değişkenlik göstermeyip tek düze dağılım niteliğinde olduğu düşünülen hücresel özdevinirlerin rastgele sayı üretim performans sonuçları, başlangıç durum yoğunluğunun dikkate alınması gereken önemli bir unsur olduğunu ortaya koymaktadır. Spesifik olarak, NIST testinden geçen en başarılı 7 adet özdevinire ait tüm farklı başlangıç durum yoğunlukları dikkate alındığında, özdevinir ne olursa olsun başlangıç yoğunluk oranı %25 ile %70 arasında olması durumunda, başarılı rastgele sayı üretimi gözlemlenmiştir. Bu çalışmada elde edilen iki temel sonuç vardır:

1. Doğrusal hücresel özdevinirlerin nitelikli rastgele sayı üreteçleri oldukları bilinmektedir ancak döngü boyu kısalığı sebebiyle doğrudan kriptografik amaçlı uygulamalarda kullanımları uygun değildir. Literatürde bilinen bu sonuç iki boyut bağlamında deneysel olarak doğrulanmıştır.
2. İki boyutlu doğrusal hücresel özdevinirler bağlamında deneysel olarak ortaya koyulduğu üzere başlangıç durum yoğunluğu rastgele sayı üretiminde önemlidir ve göz ardı edilmemelidir.

## Teşekkür (Acknowledgement)

Atılım Üniversitesi Metal Şekillendirme Mükemmeliyet Merkezi'ne; TÜBİTAK ULAKBİM Yüksek Başarımlı ve Grid Hesaplama Merkezi başuzmanı ve araştırmacısı Dr. Hakan Bayındır'a; Atılım Üniversitesi öğretim üyelerinden Dr. Öğr. Üyesi Beytullah Yıldız'a; Ozan Can Acar, Buğra Yener Şahinoğlu, İbrahim Tarakçı ve Ömer Durukan Kılıç'a faydalı soru, yorum ve desteklerinden dolayı teşekkür ederim.

## Kaynaklar (References)

1. Stipčević M., Koç Ç.K., True random number generators, In: Koç Ç.K., editor. Open Problems in Mathematics and Computational Science. Berlin, Germany: Springer, 275-315, 2014.
2. **2.**Tuna M., Fidan C.B., A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems, Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (2), 473-491, 2018.
3. Tuncer, T., Avaroğlu, E., Türk, M., Ozer, A.B., Implementation of Non-periodic Sampling True Random Number Generator on FPGA, Informacije Midem, 44 (4), 296-302, 2014.
4. Ozkaynak, F., A Novel Random Number Generator Based on Fractional Order Chaotic Chua System, Elektronika ir Elektrotechnika, 26 (1), 52-57, 2020.
5. Akkaya S., Pehlivan İ., Akgül A., Varan M., The design and application of bank authenticator device with a novel chaos based random number generator, Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (3),1171-1182, 2018.
6. Avaroğlu,E., Pseudorandom number generator based on Arnold cat map and statistical analysis, Turk. J. Elec. Eng. & Comp. Sci., 25, 633-643, 2017.
7. Knuth D.E., The Art of Computer Programming, Addison-Wesley, Reading, Mass., ABD, 1981.
8. Wolfram S., Random sequence generation by cellular automata, Adv. Appl. Math., 7, 123-169, 1986.
9. Park SK,Miller KW,Random number generators:good ones are hard to find, Com. of ACM 31,1192-1201, 1988.
10. Bakiri M., Guyeux C., Couchot J.F., Oudjida, A.K., Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses, Comput. Sci. Rev., 27, 135-153, 2018.
11. Bhattacharjee K., Das, S., Search for good pseudo-random Number Generators: Survey and Empirical Studies, Computer Science Review 45 (2022), 100471.
12. Sipper M., Evolution of Parallel Cellular Machines: The Cellular Programming Approach, Lecture Notes in Computer Science - 1194, Springer-Verlag, Berlin, Heidelberg, Germany, 1997.

**13.** Faraoun K.M., A genetic strategy to design cellular automata based block ciphers, Expert Syst. Appl., 41 (17), 7958-7967, 2014.

**14.** Guan, S.U., Zhang, S., Quieta, M.T., 2-D CA variation with asymmetric neighborship for pseudorandom number generation, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 23 (3), 378–388, 2006.

**15.** Hanin C., Omary F., Elbernoussi S., Boulahiat B., Design of new pseudo-random number generator based on non-uniform cellular automata, International Journal of Security and its Applications, 10 (11), 109-118, 2016.

**16.** Shin S.H., Kim D.S., Yoo K.Y., A 2-Dimensional Cellular Automata Pseudorandom Number Generator with Non-linear Neighborhood Relationship, Networked Digital Technologies, Springer-Verlag, 293, 355-368, 2012.

**17.** Temiz F., Siap I., Akın H., On Pseudo Random Bit Generators via Two-Dimensional Hybrid Cellular Automata, Acta Phys. Pol. A, 125 (2), 534-537, 2014.

**18.** Hosseini S.M., Karimi H., Jahan M.V., Generating pseudo-random numbers by combining two systems with complex behaviors, Journal of Information Security and Applications, 19 (2), 149-162, 2014.

**19.** Szaban, M., (2019), Pseudorandom number generator based on totalistic cellular automaton, 15th International Conference on Parallel Computing Technologies (PaCT), Springer Series, Lecture Notes in Computer Science (LNCS) 11657, 360-370, 2019.

**20.** Nayyeri A., Dastghaibyfard G., An Information Theoretic Analysis of Random Number Generator based on Cellular Automaton, International Journal of Advanced Computer Science and Applications, 9 (1), 321-329, 2018.

**21.** Bhattacharjee K., Paul D., Das S., Pseudo-random number generation using a 3-state cellular automaton, Int. J. Mod. Phys. C, 28 (6), 1750078, 2017.

**22.** Bhattacharjee K., Das, S., Random number generation using decimal cellular automata, Commun. Nonlinear Sci. Numer. Simul., 78, 104878, 2019.

**23.** Guan S.U., Tan S.K., Pseudorandom number generation with self-programmable cellular automata, IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., 23 (7), 1095-1101, 2004.

**24.** Roy S., Gupta R.K., Rawat U., Dey N., Crespo R.G., PCHET: An efficient programmable cellular automata based hybrid encryption technique for multi-chat client-server applications, Journal of Information Security and Applications, 55, 102624, 2020.

**25.** Petrica L., FPGA optimized cellular automaton random number generator, J. of Parallel Distrib. Comp.,111, 251-259, 2018.

**26.** Baetens J.M., Gravner J., Stability of Cellular Automata Trajectories Revisited: Branching Walks and Lyapunov Profiles, J. Nonlinear Sci., 26, 1329–1367, 2016.

**27.** Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., Vo, S., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications", National Institute of Standards and Technology (NIST) Special Publication 800-22 (Revision 1a, L. E. Bassham III), 2010.

**28.** Killmann, W., Schindler W., A proposal for: Functionality Classes for Random Number Generators AIS20 / AIS31 Version 2.0, September 18, 2011.

**29.** L'Ecuyer, P., Simard R., TestU01: A C Library for Empirical Testing of Random Number Generators, ACM Transactions on Mathematical Software, Vol. 33, No. 4, Article 22, August 2007.

**30.** Packard N.H., Wolfram S., Two-Dimensional Cellular Automata, J. Stat. Phys., 38 (5-6), 901-946, 1985.

**31.** Martinez G.J., Seck-Tuoh-Mora J.C., Zenil H., "Wolfram's Classification and Computation in Cellular Automata Classes III and IV", In: Zenil H. (eds) Irreducibility and Computational Equivalence. Emergence, Complexity and Computation, Springer, Berlin, Heidelberg, 2, 2013.

**32.** Zenil H., Compression-based Investigation of the Dynamical Properties of Cellular Automata and Other Systems, Complex Syst., 19 (1), 1-28, 2010.

**33.** Culik K, Yu S., Undecidability of CA classification schemes, Complex Syst., 2 (2), 177-190, 1988.

**34.** Tomassini M., Sipper M., Perrenoud M., On the Generation of High-Quality Random Numbers by Two-Dimensional Cellular Automata, IEEE Trans. Comput., 49 (10), 1146-1151, 2000.

**35.** Sulak F., Uğuz M., Koçak O., Doğanaksoy A. On the Independence of Statistical Randomness Tests Included in the NIST Test Suite, Turk. J. Elec. Eng. & Comp. Sci., 25, 3673-3683, 2017.

**36.** French Information Systems Security Center, Using AIS31 Method, Application Note/05.3, http://osgug.ucaiug.org/utilisec/embedded/Shared%20Documents/Device%20Security/RNG/NOTE-05_Evaluation_AIS31_en.pdf, Yayınlanma/Güncelleme Tarihi: 07.03.2007, Erişim Tarihi: 19.10.2022.

**37.** Matsumoto, M., Nishimura, T., Mersenne Twister: a 623-dimensionally Equidistributed Uniform Pseudo-Random Number Generator, ACM Transactions on Modeling and Computer Simulation, 8 (1), 3–30, 1998.

**38.** Zarezadeh, Z., Cellular Automaton-Based Pseudorandom Number Generator, Complex Systems, 26 (4), 373-389, 2017.

**39.** Bhattacharjee, K., Das, S., A list of tri-state cellular automata which are potential pseudo-random number generators, International Journal of Modern Physics C, 29 (9), 1850088, 2018.

**40.** Shapiro, S.S., Wilk, M.B., An analysis of variance test for normality (complete samples), Biometrika, 52 (3-4), 591-611, 1965.