Journal of the Faculty of Engineering and Architecture of Gazi University 33:2 (2018) 473-491

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

A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems

Murat Tuna[1*], Can Bülent Fidan[2]
[1]Department of Electrical, Kirklareli University, Kirklareli, 039100, Turkey
[2]Department of Mechatronics Engineering, Karabuk University, Karabuk, 078050, Turkey

Highlights:

- Latest developments about chaotic systems and random number generators in the literature
- Analysis and the studies on chaos-based true random number generators in the literature
- The importance of chaos based true random number generators on FPGA and their general situation in the literature

Keywords:

- Chaos and chaotic systems
- Random number generator
- True random number generator
- Field programmable gate array

Article Info:

Received: 03.11.2016
Accepted: 29.03.2017

DOI:

10.17341/gazimmfd.416355

Acknowledgement:

Correspondence:

Author: Murat Tuna
e-mail: murat.tuna@klu.edu.tr
phone: +90 288 214 1845

Graphical/Tabular Abstract

Chaos-based systems look like unstable because of producing noise-like signals, exhibiting a-periodic behavior and sensitive dependence on initial conditions. Due to these features, have attracted the attention of electronics engineering applications such as secure communication, cryptography and random number generation. In recent years, the great efforts are being made in the area of developing the chaos-based TRNG structures due to noise-like features and the ability of hiding informatory sign of chaotic oscillators. The general structure of chaos-based TRNG is shown in Fig.1. Chaos based TRNG's within the digital circuits are an effective alternative to the traditional chaos-based analog structure. Because TRNG systems that use analog chaotic signal generator are difficult to be synchronized with the transmitter and receiver. In addition, the weak resources that generates physical noises like thermal or scattering are used on the implementation of these circuits.

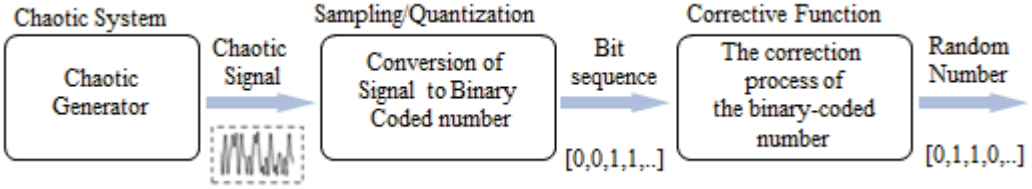


Figure 1. The block diagram of chaotic random number generating system

Purpose: In this study, performance differences between conventional method of TRNG that used chaotic system and recently designed FPGA based chaotic systems have been compered.

Theory and Methods: TRNGs that is used in the field of cryptography and secure communications require fast, secure and intensive process of the physical methods that do not have deterministic character are used as entropy source. These methods are direct reinforcement, dual oscillator and chaos-based applications.

Results: TRNG designs are proposed in the literature with different features. These designs show considerable changes relative to their use rather than entropy sources and production techniques. The technical characteristics of TRNG structures designed using different methods are given in Table 1. According to this, the CMOS-based TRNG designs have a working frequency of 1-25 MHz and a bit production rate of 1-40 Mbit/s maximum. The operating frequencies of the TRNG structures implemented with FPGA based classical oscillators are 20-300 MHz and bit production speeds drop to 1-40 Mbit/s due to the oscillators and method used. TRNG structures implemented using chaotic systems on FPGAs are seen to have higher bit rates at both 400 MHz and operating frequencies than other methods.

Table 1. Technical features of TRNGs designed using different methods

Method Used	Realization	Applied Tests	Operating frequency (MHz)	Bit production speed (Mbit/s)
Oscillator sampling	CMOS	NIST-800-22	1,24	10
Oscillator sampling	CMOS	DieHard	20	10-20
Ring oscillator	FPGA	NIST-800-22	300	7,14
Metastability	FPGA	NIST-800-22	22	50
Chaotic oscillator	FPGA	NIST-800-22	401	132
Chaotic oscillator	FPGA	NIST-800-22	293	58,76

Conclusion: In this article, firstly the differences between the methods used in TRNG constructions are explained. Secondly, the hardware characteristics and performance of the chaotic oscillators designed with on FPGA are mentioned. Third, the literature has focused on the characteristics of TRNG structures implemented chaos-based on FPGAs and the high performance that occurs when compared to traditional methods. Finally, TRNG structures and new chaotic oscillators with different characteristics are designed to give acceleration to the design work. Designed on chaos-based FPGAs, the TRNGs have an important potential to improve the information security capacity in cryptography and secure communications.

Journal of the Faculty of Engineering and Architecture of Gazi University 33:2 (2018) 473-491

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

Kaotik sistemler ve FPGA tabanlı kaotik osilatörlerin gerçek rasgele sayı üretimindeki (GRSÜ) önemi üzerine bir araştırma

Murat Tuna[1]*, Can Bülent Fidan[2]

[1]Kırklareli Üniversitesi, Teknik Bilimler Meslek Yüksekokulu, Elektrik Programı, Kırklareli, 39100, Türkiye
[2]Karabük Üniversitesi, Mühendislik Fakültesi, Mekatronik Mühendisliği, Karabük, 78050, Türkiye

ÖNEÇIKANLAR

- Kaotik sistemler ve rasgele sayı üreteçleri hakkında literatürdeki son gelişmeler
- Literatürde kaos tabanlı gerçek rasgele sayı üreteçleri üzerine yapılan çalışmalar ve analizleri
- FPGA üzerinde kaos tabanlı gerçek rasgele sayı üreteçlerinin önemi ve literatürdeki genel durumu

Makale Bilgileri
Geliş: 03.11.2016
Kabul: 29.03.2017

DOI:
10.17341/gazimmfd.416355

Anahtar Kelimeler:
Kaos ve kaotik sistemler,
Rasgele sayı üreteçleri,
Gerçek rasgele sayı üreteçleri,
Alan programlanabilir kapı dizileri,

ÖZET

Rasgele sayı üreteçleri kriptografi, Monte-Carlo metodunun kullanıldığı uygulamalar, bilgisayar benzetimleri ve modellemeleri ile sayısal analiz uygulamaları gibi birçok alanda kullanılmaktadır. Hızlı, güvenli ve yoğun işlem gerektiren kriptografi ve güvenli haberleşme alanlarında kullanılan GRSÜ'lerde entropi kaynağı olarak deterministik karaktere sahip olmayan yöntemler kullanılmaktadır. Bu yöntemler doğrudan kuvvetlendirme, çift osilatör ve kaos tabanlı uygulamalardır. Kaotik osilatörlerin gürültü benzeri özellikler taşımaları ve bilgi işaretini gizleyebilme gibi özelliklerinden dolayı kaos tabanlı GRSÜ yapıların geliştirilmesi üzerine son yıllarda büyük çabalar sarf edilmektedir. Sayısal devre üzerinde kaos tabanlı GRSÜ'leri geleneksel kaos tabanlı analog yapılarına göre etkili bir alternatiftir. Çünkü analog kaotik işaret üreteci kullanan GRSÜ sistemlerinde verici ile alıcının çok iyi şekilde senkronize edilmesi zordur. Bunların devre gerçeklemelerinde ısıl veya saçılma gürültüsü gibi fiziksel gürültü üreten zayıf kaynaklar kullanılmaktadır. Sayısal tabanlı FPGA çipleri yüksek performans ve işlemci gücü gerektiren kriptoloji ve güvenli haberleşme gibi uygulamalarda bilgi güvenliği kapasitesini iyileştirmede önemli bir potansiyele sahiptir. Bu çalışmada son yıllarda tasarlanan kaotik sistemler ile FPGA üzerinde tasarlanan kaos tabanlı GRSÜ'lerinin detaylı bir araştırılması ve geleneksel yöntemlerle performans karşılaştırılmaları yapılmıştır.

A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems

HIGHLIGHTS

- Latest developments about chaotic systems and random number generators in the literature
- Analysis and the studies on chaos-based true random number generators in the literature
- The importance of chaos based true random number generators on FPGA and their general situation in the literature

Article Info
Received: 03.11.2016
Accepted: 29.03.2017

DOI:
10.17341/gazimmfd.416355

Keywords:
Chaos and chaotic systems,
Random number generator,
Ture randon number generator,
Field programmable gate array,

ABSTRACT

The random number generators are used in many areas such as cryptography, the applications where the Monte-Carlo method is used, the application of numerical analysis with computer simulations and modeling. TRNGs that is used in the field of cryptography and secure communications require fast, secure and intensive process of the physical methods that do not have deterministic character are used as entropy source. These methods are direct reinforcement, dual oscillator and chaos-based applications. In recent years the great efforts are being made in the area of developing the chaos-based TRNG structures due to noise-like features and the ability of hiding informatory sign of chaotic oscillators. Chaos based TRNG's within the digital circuits are an effective alternative to the traditional chaos-based analog structure. Because TRNG systems that use analog chaotic signal generator are difficult to be synchronized with the transmitter and receiver. In addition, the weak resources that generates physical noises like thermal or scattering are used on the implementation of these circuits. The digital-based FPGA chips have a significant potential in improving the information security capabilities in some applications as cryptology and securing the communication which requires high performance and processor power. In this study, performance differences between conventional method of TRNG that used chaotic system and recently designed FPGA based chaotic systems have been compered.

*Sorumlu Yazar/Corresponding Author: murat.tuna@klu.edu.tr / Tel: +90 288 214 1845

1. GİRİŞ (INTRODUCTION)

Dünyada doğrusal olmayan sistemlerin, birbirleriyle olan ilişkilerini ortaya koyan ve bu sistemleri modellemeye çalışan bilim doğrusal olmayan (nonlineer) bilim olarak adlandırılmaktadır. Bu sistemlerde çok önemsenmeyen bir davranış veya etki sistemde öngörülemeyecek kadar büyük değişimlere ve tepkilere neden olabilmektedir [1]. Doğrusallık sadece belirli sınırlar arasında geçerli olabilmektedir. Günümüzde üzerinde pek çok araştırma ve çalışmalar yapılan doğrusal olmayan bilim alanlarından birisi de kaos bilimi veya kaotik sistemlerdir [2, 3]. Kaotik sistemler başlangıç koşullarına hassas bağlı, karmaşık ve düzensiz görünümlüdür ve deterministik doğrusal olmayan zamanla değişen sistemlerde ortaya çıkarlar [4]. Bu sistemlerin araştırılması ve uygulanmasına yönelik bilimsel ve endüstriyel alanlarda önemli çalışmalar gerçekleştirilmektedir. Mühendisliğin pek çok alanında kaotik sistemlerin varlığının ortaya çıkarılması, bu konuda yapılan yoğun çalışmalar ve yaşanan gelişmeler kaotik sistemlerin birçok uygulama alanında kullanılabileceğini göstermiştir [5]. Bu uygulama alanlarına biyomedikal [6, 7], haberleşme [8], görüntü işleme [9, 10], optik elektronik ve elektromanyetik [11], bulanık mantık [12, 13], güç elektroniği [14], optimum kontrol [15, 16], mekatronik, yapay sinir ağları gibi alanlar örnek olarak verilebilir.

Kaotik işaretlerin gürültü benzeri işaretler üretmesi, periyodik olmayan davranış sergilemeleri, başlangıç koşullarına hassas bağlı olmaları vb. özellikleri sebebiyle kaotik sistemler son yıllarda bilgi güvenliği amacıyla kriptografi [17] ve güvenli haberleşme [18] alanında sıklıkla kullanılmaya başlanmıştır. Kriptografinin tanımına bakıldığında bir bilginin şifrelenmesi ve bu şifrenin çözülmesi için uygulanması gereken yöntemler olarak tanımlanmaktadır. [19, 20] Kaotik işaretlerin elektronik mühendisliğindeki önemli araştırma ve uygulama alanları arasında ise güvenli haberleşme düzenekleri oluşturma [21], gürültü üreteçleri, şifreleme [22] ve rasgele sayı üreteçleri (RSÜ) bulunmaktadır [23]. RSÜ'leri tarafından üretilen rasgele sayılar bilgi güvenliği sistemlerinde anahtar olarak kullanılmaktadır. Fakat anahtarların sistem dışında kontrolsüz ortamlarda üretimi sistemin güvenilirliğini azaltmaktadır [24, 25]. Bu dezavantajı ortadan kaldırmak için donanımsal kriptolojinin ve güvenli haberleşmenin gelişimi programlanmış kripto aritmetiğinin DSPs (Digital Signal Processors (Sayısal İşaret İşlemciler)) [26, 27], ASIC (Application Specific Integrated Circuits (Uygulamaya Özel Tümleşik Devreler)) [28, 29] ve FPGA (Field Programmable Gate Array (Alan Programlanabilir Kapı Dizileri)) [30, 31] gibi entegre içerisinde gerçekleştirilmesi yönündedir. FPGA çipleri bu problemin üstesinden gelmekle birlikte aynı zamanda bu işlemleri yüksek frekanslarda da gerçekleştirebilmektedir. FPGA yüksek hız ve kapasiteleri nedeniyle özellikle yüksek performans ve işlemci gücü gerektiren kriptoloji ve güvenli haberleşme gibi uygulamalarda bilgi güvenliği kapasitesini iyileştirmede önemli bir potansiyele sahiptir [32, 33]. Kaotik osilatörlerin FPGA tabanlı modellenmesine yönelik çalışmalara literatürde oldukça fazla önem verilmektedir [34]. Alçın vd. [35] 2016 yılında yaptıkları çalışmada PU kaotik sistemini YSA (Yapay Sinir Ağları) yöntemiyle Xilinx Virtex-6 FPGA çipinde IEEE 754 kayan nokta standardında VHDL dilinde tasarlamışlardır. Sistemin yapılan test sonuçlarına göre çalışma frekansı 266,429 MHz olarak verilmiştir. Alınan çip istatistiklerine ve test sonuçlarına göre bu çalışma sonucunda önerilen kaotik sistem FPGA üzerinde YSA yöntemi ile başarılı bir şekilde modellenmiştir. Tuna vd. [36] 2015 yılında yaptıkları çalışmada literatüre yeni sundukları kaotik sistemini FPGA üzerinde sayısal olarak gerçekleştirmişlerdir. Sunulan yeni kaotik sistem, FPGA üzerinde IEEE-754-1985 kayan noktalı sayı formatında, Heun algoritması kullanılarak VHSIC HDL (Very High Speed Integrated Circuit Hardware Description Language (Çok Yüksek Hızlı Tümleşik Devre Donanım Tanımlama Dili)) dili ile gerçekleştirilmiştir. Tasarlanan sistem Xilinx Virtex-6 FPGA çipinde sentezlenmiş ve test edilmiştir. Test sonuçlarına göre FPGA-tabanlı yeni kaotik işaret üretecinin çalışma frekansı 390 MHz olarak belirlenmiş ve çip istatistikleri ile performans sonuçları verilmiştir. Diğer bir çalışmada Koyuncu vd. [37] 2014 yılında yaptıkları çalışmada literatüre yeni sundukları Pehlivan-Wei kaotik sistemini Xilinx firmasının üretmiş olduğu Virtex-6 FPGA kiti üzerinde gerçekleştirmişlerdir. Yeni kaotik sistemi VHDL dilinde üç farklı nümerik algoritma (Euler, Heun ve RK4) kullanarak tasarlayıp FPGA bordunun çip istatistiklerini karşılaştırmışlardır. Gerçekleştirdikleri tasarımın çalışma frekansını 463,688 MHz olarak belirtmişlerdir.

Azzaz vd. [38] yaptıkları çalışmada 3 boyutlu kaotik sistemi Xilinx Virtex-II XC2VP30FFG896-7 FPGA bordu üzerinde VHDL dilinde 32 bit (16Q16) sabit noktalı sayı formatında tasarımını gerçekleştirmişlerdir. Sürekli zamanlı kaotik sistemini sayısallaştırmada Euler nümerik algoritmasını kullanmışlardır. Tasarımın çalışma frekansı 38,86 MHz olarak belirtmişlerdir. Merah vd. [39] yaptıkları diğer bir çalışmada bilgi güvenliği uygulamaları için Lorenz kaotik sistemini FPGA üzerinde modellemişlerdir. Lorenz kaotik sisteminin tasarım aşamasında donanım tanımlama dillerinden birisi olan VHDL kullanılmıştır. Tasarlanan kaotik sistem Xilinx firmasının Spartan-3 FPGA ailesi çipinde gerçeklenmiştir. Tasarımın çalışma frekansı yaklaşık olarak 18 MHz olarak ifade edilmiştir. Koyuncu vd. [40] Burke-Shaw kaotik sistemini Xilinx Virtex-6 XC6VCX75T FPGA üzerinde 32 bit IEEE-1985-754 kayan nokta sayı standardını kullanarak VHDL dilinde tasarlamışlardır. Kaotik sistemi sayısallaştırmada RK5-Butcher nümerik algoritmasını kullanmışlardır. Sistemin çalışma frekansını 373,094 MHz olarak belirtmişlerdir. Diğer bir çalışmada De micco vd. [41] RK4 algoritmasını kullanarak Lorenz kaotik sistemini FPGA'de gerçeklemişlerdir. Kaotik sistem tasarımında IEEE-1985-754 kayan noktalı sayı standardı kullanılmıştır. Test aşamasında kaotik sistem Altera EP3C120F7 bordu ile test edilmiş ve sistemin çalışma frekansı yaklaşık 1 MHz olarak belirtilmiştir. Sadoudi vd.

[42] güvenli kaotik haberleşme sistemleri için Chen kaotik sistemini FPGA de modellemişlerdir. Bu çalışmada, 32-bit kesirli sayı standardı ile RK4 algoritması kullanılmış ve tasarım bir adet Xilinx Virtex-II çip içeren XCV1000FG456-4 bordu ile test edilmiştir. Yapılan tasarımdan elde edilen sinyaller ile Matlab sonuçları karşılaştırılmıştır. Sistemin çalışma frekansı 22,85 MHz olarak belirtilmiştir. Eroğlu yaptığı tez çalışmasında [43] Lorenz, Chua, Rössler, Linz ve Sprott kaotik sistemlerini Xilinx Virtex-4 FPGA kiti üzerinde tasarlamıştır. Yukarıda bahsettiğimiz ve son yıllarda FPGA tabanlı gerçekleştirilen kaotik çekerlerin özellikleri, kullanılan algoritma ile çalışma frekansı gibi teknik özellikleri Tablo 1'de verilmiştir.

Rasgele sayı üreteçleri Sözde Rasgele Sayı Üreteçleri (SRSÜ), Gerçek Rasgele Sayı Üreteçleri (GRSÜ) ve Hibrit Rasgele Sayı Üreteçleri (HRSÜ) olmak üzere 3 sınıfa ayrılmaktadır. GRSÜ'leri belirsizlik kaynağı olarak gerçek entropi kaynakları kullanmaktadır. Bu yapı daha güvenli bir kaynak oluşturduğu için kriptografide anahtar olarak öngörülemeyen bit dizisi oluşturmada sıklıkla kullanılmaktadır [44]. GRSÜ'lerinde entropi kaynağı olarak deterministik olmayan fiziksel olaylar kullanılmaktadır. Bunlar SRSÜ'lerine nazaran yavaş, maliyetli ve donanıma bağımlı olması gibi dezavantajlara sahiptir. Ancak GRSÜ'lerin kriptografik uygulamalar için zorunlu olan kestirilememe, tekrar üretilememe ve istatistiksel rasgelelik testlerinden oldukça başarılı bir şekilde geçmesi onun kriptolojide birçok alanda kullanımını arttırmıştır. Literatürde GRSÜ uygulamaları için çeşitli yöntemler sunulmuştur. Bu yöntemler; gürültü kaynağının doğrudan kuvvetlendirmesi, yüksek frekanslı osilatörün seğirmeli (jitter osilatör) düşük frekanslı osilatörle örneklenerek oluşturulan çift osilatör yapı ve kaotik sistem tabanlı sürekli ve ayrık zamanlı devre uygulamalardır. Bu uygulamalarda; elektronik gürültünün kullanımındaki en önemli kısıtlama gürültü genliğinin küçük olmasından dolayı rastgele sayı üretilirken geniş bantlı ve düşük gürültülü bir kuvvetlendiriciye ihtiyaç duyulmasıdır [45]. Bunun yanında ayrıca ısıl gürültü tabanlı GRSÜ yapıları bulunduğu sistemin içinde oluşan elektromanyetik alandan, sıcaklıktan, besleme gürültüsünden ve kuvvetlendiricinin gürültüsünden etkilenmektedir. Osilatör örnekleme yöntemine göre gerçekleştirilen GRSÜ'lerin ortalama bit üretim hızlarının belirli bir hızın üzerine çıkamaması [46, 47] ve gerçeklenen RSÜ'nin etkili bir rasgelelik sağlayamaması [48, 49] gibi dezavantajlara sahiptir. Ayrıca analog elemanlar kullanılarak sürekli zamanda gerçekleştirilen osilatörlerin çalışma

Tablo 1. Literatürde FPGA tabanlı gerçekleştirilen kaotik osilatörler ve teknik özellikleri
(The chaotic oscillators realized FPGA-based and their technical specifications in literature)

Çalışmayı Yapan	Kullanılan Kaotik Çeker	Kullanılan Algoritma	Kullanılan Sayı Stand.	FPGA Özellikleri	Çalışma Frekansı (MHz)
Alçın vd., [35], 2016	PU (Pehlivan-Uyaroglu) kaotik sistemi	YSA	IEEE-754 Floating-point 32 bit	Xilinx Virtex-6 XC6VCX240T	266,429
Tuna vd., [36], 2015	Yeni bir kaotik sistem	Heun	IEEE-754 Floating-point- 32bit	Xilinx Virtex-6 XC6VCX75T	390
Koyuncu vd. [37], 2014	Pehlivan-Wei chaotic systems	Euler, Heun, and RK4	IEEE-754 Floating-point- 32bit	Xilinx Virtex-6 XC6VCX75T	463,688
Azzaz vd. [38], 2013	3D Hybrid chaotic sys. Lorenz, Lü, Chen and Liu-Chen)	Euler	32 bits (16Q16) Fixed-point	Xilinx Virtex-II XC2VP30FFG896	38,86
Merah vd. [39], 2013	Lorenz	RK4	32 bits (12Q20) Fixed-point	Xilinx Spartan-3	18
Koyuncu vd. [40], 2013	Burke-Shaw	RK5-Butcher	32 Bit IEEE-754 Floating-point	Xilinx Virtex-6 XC6VCX75T	373,094
De Micco vd. [41], 2011	Lorenz	RK4	IEEE-754	Altera Ciclone III EP3C120F7	1
Sadoudi vd. [42], 2009	Chen	RK4	IEEE-754 Floating-point- 32 bit	Xilinx Virtex-II XCV1000FG456-4	22,85
Eroğlu [43], 2007	Lorenz, Chua Rössler, Linz and Sprott,	Simulink and Xilinx Systems Generator	IEEE-754 Floating-point- 32 bit	Xilinx Virtex-4 XC4VSX35-668	------
Tlelo-Cuautle vd. [44] 2016	50-scroll chaotic attractor	------	-----	Altera Cyclone IV FPGA DE2i- 150	66

frekanslarının düşük olması ve bu yapıların sistem parametrelerinin değişimine dirençli olması gibi problemleri de ortaya çıkmaktadır [50, 51]. Gerçek rastgele sayı üretiminde kullanılan ilk iki yöntemin olumsuz yönlerini iyileştirmek, ana kaynağın entropisini daha da arttırmak [52] ve yüksek çalışma frekansı ile yüksek bit üretim hızında daha gerçeksi ve güvenli rasgele sayı dizileri elde etmek [53] amacıyla kaotik devre tabanlı RSÜ [54, 55] sistemlerin kullanımı en uygun alternatiftirler.

2. KAOS VE KAOTİK SİSTEMLER
(CHAOS AND CHAOTIC SYSTEMS)

Kaos tanımı incelendiğinde başlangıç koşullarına üstel duyarlı, nonlineer, deterministik karakterli ve uzun vadede periyodik olmayan dinamik sistemler olduğu görülmektedir [56, 57]. En kısa tarifiyle ise, düzensizliğin düzeni şeklinde tanımlanan ve doğrusal olmayan olayları açıklamaya yarayan bir bilim dalıdır. Karmaşık, ama kendi iç düzenine sahip bir süreçtir [58]. Özellikle dikkat edilmesi gereken bir nokta, kaosun rasgelelik olmadığıdır. Dinamik sistemlerde bilinen en karmaşık kararlı hal davranışı kaos'tur [59]. Kaos ile ilgili çalışmalar, doğrusal olmayan dinamik sistemler teorisinin bir kısmıdır. Bu durum daha çok "deterministik kaos" olarak bilinir [60, 61]. 18. yüzyılın sonlarında, 1892 yılında Fransız matematikçi Henri Poincare yeni ufuklar açan bir araştırma ile basit dinamik kuralların çok karmaşık kararlı-hal davranışlarına yol açabileceğini ve zamana göre değişimi Hamilton denklemleri ile yönlendirilen mekanik sistemlerin karmaşık davranışlar gösterebileceğini keşfetti [62]. Günümüzde bu davranışlar "kaotik davranışlar" olarak adlandırılmaktadır. Kaos kavramı matematiksel olarak 19. yüzyılda incelenmeye başlanmış ve ilk ciddi bilimsel çalışma M.I.T. bilimcisi Edward Lorentz'in 1963'de hava tahmini yapmak için oluşturduğu matematiksel meteorolojik modelin sonuçları sayesinde elde edilmiştir [63]. Edward Lorentz bilgisayarla yaptığı modelde sayısal analizlerden elde ettiği sonuçları hızlandırmak için aldığı verileri yuvarlayarak kullanmıştır. Ancak sonuçlar çok hızlı bir şekilde değişerek tahmin edilemez bir hal almıştır. Böylece Lorentz, farkında olmadan kaos teorisinin temellerini atmıştır. Lorenz'in keşfinin önemi, yayınlanmasından çok yıl sonralara kadar anlaşılamamıştır. Ancak 1975 yılında, Li ve Yorke bu çeşit davranışı belirtmek için "kaos" terimini kullanmayı önermişlerdir [64]. Rössler 1976 yılında Lorenz sistemine göre daha basit 7 terimli bir kaotik sistem önermiştir [65]. Kaotik davranışın analog devre tabanlı modellenmesi ise ilk defa Leon O. Chua tarafından elektronik elemanlar ve devreler kullanarak 1983'te gerçeklenmiştir [66, 67]. Tasarımcısının adını almış olan bu sürekli otonom Chua devresi [68] elektronik olarak anlaşılması ve tasarlanması çok basit bir devre olmasından dolayı literatürde defalarca incelenmiş [69, 70] ve birçok uygulamada kullanılarak günümüz kaotik devre çalışmalarına ışık tutmuştur [71, 72]. Literatürde çok sayıda otonom kaotik devre geliştirilmiş olsa da üzerinde en çok çalışma yapılan ve kaotik dinamikleri en iyi bilinen otonom sistemler Lorenz, Chua, Rössler, Lü, Liu, Duffing, Chen, Rabinovich, Rikitake ve Burke-Shaw sistemleridir [73, 74].

Kaotik sistemler ayrık zamanda kaotik sistemler ve sürekli zamanda kaotik sistemler olmak üzere ikiye ayrılır [75, 76]. Ayrık zamanda kaos, uygun bir *f(x)* nonlineer fonksiyonun iterasyon sonucu oluşan genelde geri besleme özelliği gösteren kaotik özellikli dizilerin oluşturduğu bir sistemdir. Ayrık zamanlı kaotik fonksiyonlara bakıldığında genelde bir boyutlu basit bir ifade ile bu davranış sağlanabilmektedir. Eş. 1'de gösterilen x_{n+1} ve $f(x_n)$ değişkenlerinin kullanımıyla bir boyutlu haritalar oluşturulmakta ve bu fonksiyonlar geri besleme yapısına sahip olduğundan düzlemde ters V şeklinde bir form almaktadır [77, 78]. Tent, lojistik, çadır, Bernoulli kaydırıcısı gibi fonksiyonlar bu davranışa sahip bazı kaotik haritalara örnektir [79, 80].

$$x_{n+1} = f(x_n) \tag{1}$$

Sürekli zamanlı kaotik sistemler genellikle adi diferansiyel denklemlerle ifade edilirler. Sürekli zamanlı n tane birinci dereceden adi diferansiyel denklem sistemi i=1, 2, 3, ….., n olmak üzere Eş. 2 ile verilebilir [81, 82]. Bu bağıntıda x, n boyutlu bir vektördür. Literatürdeki çalışmalar incelendiğinde sürekli zamanlı kaotik bir sistem oluşturmak için basit yapıda üçüncü dereceden (n≥3) diferansiyel bir denklem takımı ve nonlineer bir yapı çoğu zaman yeterli olmaktadır [83, 84].

$$\begin{aligned} \frac{dx(t)}{dt} &= f(x(t)) \\ \frac{dx^i}{dt} &= f_1\left(x^i, x^{i+1}, \cdots\cdots x^n\right) \end{aligned} \tag{2}$$

Günümüzde son birkaç yılda kaosun uygulama alanlarının gelişmesi ile literatürde yeni kaotik osilatör tasarımlarına yönelik araştırmalarda önemli artışlar görülmektedir [85, 86]. Yu vd. 2012 yılında yaptıkları çalışmada yeni bir üç boyutlu kaotik sistemi sunmuşlardır [87]. Bu sistem 6 terim, 4 paremetre, bir adet quadratik üstel doğrusal olmayan terim ve bir adet quadratik karesel çapraz terim içermektedir. Ahmed vd. 2014 yılında yaptıkları çalışmada Chen kaotik sisteminden türettikleri sürekli zamanlı, üç boyutlu, bir tane doğyusal olmayan terim, bir adet doğrusal olmayan exponansiyel terim, quadratik çapraz çarpımlı terim olmak üzere 8 terim ve 3 paremetreden oluşmaktadır [88]. Kaçar 2016 yılında literatüre sunduğu çalışmasında sürekli zamanlı dört boyutlu yeni kaotik sistem 12 terim, 5 paremetre ve 2 adet kübik doğrusal olmayan terim içermektedir [89]. Tuna vd. 2016 yılında yaptıkları çalışmada altın oran denge noktalarına sahip, sürekli zamanlı, otonom, üç boyutlu, 2 adet ikinci dereceden doğrusal olmayan ifade olmak üzere 8 terim ve 2 paremetre içermektedir [90]. Leng vd. sundukları çalışmada dört boyutlu memristor tabanlı hiperkaotik bir sistem tasarlayarak kaos analizlerini gerçekleştirmişlerdir [91]. Akgül vd. (2016) yeni üç boyutlu 9 terimli, 9 parametreli ve 4 doğrusalsızlık içeren kaotik çeker önermişlerdir [92]. Önerdikleri sistemin temel kaos dinamik özelliklerini inceleyerek hem yazılım tabanlı (OrCAD-PSpice) hem de analog devre üzerinde devre gerçekleştirmesini yaparak aldıkları ekran ve osilaskop

sonuçlarını karşılaştırmışlardır. Abooee vd. (2013) yeni üç boyutlu otonom kaotik sistemini tanıtmışlardır [93]. Yaptıkları çalışmada yeni kaotik sistemin dinamik denklemlerini çıkartarak denge kararsızlığı, garip çeker, başlangıç koşullarına hassasiyeti, Lyapunov üstelleri ve fraktal boyut analizi gibi sistemin bazı temel dinamik özelliklerini incelemişlerdir. Ayrıca sistemin OrCAD-PSpice yazılımda simülasyonu ve analog devre elemanları ile devre gerçekleşmesini yaparak sonuçları karşılaştırmışlardır. Deng vd. (2014) yeni üç boyutlu 7 terimli, 3 parametreli ve sadece bir tane pozitif değer içeren otonom kaotik sistemini sunmuşlardır [94]. Önerdikleri yeni çekerin basit dinamik özellikleri olan faz portesini, denge noktasını, Lyapunov üstellerini, Poincare haritalama ve çatallanma diyagramını incelemişlerdir. Çiçek vd. (2016) üç boyutlu 9 terimli, 4 parametre ve 4 doğrusal olmayan terimli yeni otonom sürekli zamanlı bir kaotik çeker önemişlerdir [95]. Önerdikleri sistemin denge noktalarını, Lyapunov üstelleri, fraktal boyut, çatallaşma diyagramı gibi dinamik davranışlarını hem nümerik hem de analitik olarak incelemişlerdir. Ayrıca yeni kaotik sistemin OrCAD-PSpice yazılımında simülasyonu ve analog devre elemanları ile gerçekleşmesini yaparak sonuçları karşılaştırmışlardır. Buna ek olarakta aynı çalışmada güvenli haberleşme uygulamaları için kaotik maskele metodu ile etkin kontrol senkronizasyonunu gerçekleştirmişlerdir. Pehlivan vd. (2012) üç boyutlu sürekli zamanlı 8 terim, 2 parametre ve 2 kuadratik doğrusalsızlık içeren yeni bir otonom kaotik sistemi tanıtmışlardır [96]. Bu kaotik sistemin dinamik yapısını ve dinamik davranışlarını analitik ve nümerik olarak incelemişlerdir. Ayrıca kaotik devrenin Matlab ve Orcad-PSpice simülasyon sonuçlarını doğrulamak ve devrenin uygulanabilirliğini göstermek için elektronik elemanlarla devreyi gerçekleştirerek sonuçları karşılaştırmışlardır. Tablo 2'de literatüre son yıllarda yeni sunulan kaotik sistemlerin teknik özellikleri, diferansiyel denklemleri ve faz portreleri verilmiştir.

3. RASGELE SAYI ÜRETEÇLERİ (RSÜ)
(RANDOM NUMBER GENERATORS (RNG))

Donanımsal veya yazılımsal metotlar kullanarak çıkışında otokorelasyon bulunmayan ve istatistiksel olarak birbirinden bağımsız sayılar üreten sistemlere RSÜ denir. Bu üreteçler, önceki veriler yardımıyla daha sonraki verilerin tahmin ve öngörülemeyeceği rasgelelik seviyesinde çıkış üretebilen yapılardır. RSÜ bu özelliklerinden dolayı birçok değişik alanda kullanılmaktadır. Monte-Carlo metodunun kullanıldığı uygulamalar, bilgisayar benzetimleri ve modellemeleri, sayısal analiz uygulamaları, istatistiksel analizler ve özellikler ile kriptolojide rastgele sayı gereksinimleri bu üreteçler tarafından karşılanmaktadır. Bilgi güvenliği alanındaki kriptolojik sistemler, belirli devre ve aritmetik işlemlerin birleşiminden oluşmaktadır. Günümüzde donanımsal kriptolojinin gelişimi, kriptolanmış aritmetik yazılımın bir çip içerisine gömülerek gerçekleştirilmesi yönündedir. FPGA ve genel amaçlı mikroişlemciler ile donanımsal olarak rasgele sayı üreten

Tablo 2. Son yıllarda literatürdeki yeni kaotik osilatör tasarımları
(The new chaotic oscillator designs in literature in recent years)

Çalışmayı Yapan	Tasarım için kullanılan Kaotik Sistemin Özellikleri	Tasarlanan Kaotik sistemin Diferansiyel Denklem Özellikleri
Cicek, 2013, [76]	Ayrık kaotik sistem Tek boyutlu Lojistik fonksiyon	$x(n+1) = Rx(n)\ (1-x(n))$
Cicek, 2014, [102]	Ayrık kaotik sistem Tent fonksiyon Tek boyutlu	$x_{n+1} = A * \min(x_n,\ 1-x_n)$ $f(x) = \begin{cases} 2x & , 0 \le x < 0.5 \\ 2-2x & , 0.5 \le x < 1 \end{cases}, x_0 \in [0,1)$
Akgul, 2016, [92]	Otonom 3 boyutlu 9 terimli 9 parametreli	$\dot{x} = p_1 y - p_2 x + p_3 xz$ $\dot{y} = -p_4 xz - p_5 x + p_6 yz + p_7 x$ $\dot{z} = p_8 - p_9 y^2$
Abooee vd., 2013, [93]	Otonom 3 boyutlu 7 terimli 6 parametreli	$\dot{x} = a(y-x) + byz^2$ $\dot{y} = cx + dxz^2$ $\dot{z} = hz + kx^2$
Deng vd., 2014, [94]	Otonom 3 boyutlu, 7 terimli, 3 parametreli	$\dot{x} = -x - 2 \cdot y$ $\dot{y} = -x \cdot z - b \cdot y - a \cdot x$ $\dot{z} = x \cdot y - c \cdot z$
Çiçek vd., 2016, [95]	Otonom 3 boyutlu 9 terimli 4 parametreli	$\dot{x} = y + ax + bxz$ $\dot{y} = cxz + dx + yz + 1$ $\dot{z} = 1 + xy$
Pehlivan vd., 2012, [96]	Otonom 3 boyutlu 8 terimli 2 parametreli	$\dot{x} = y - x - a \cdot z$ $\dot{y} = x \cdot z - x$ $\dot{z} = -x \cdot y - y + b$

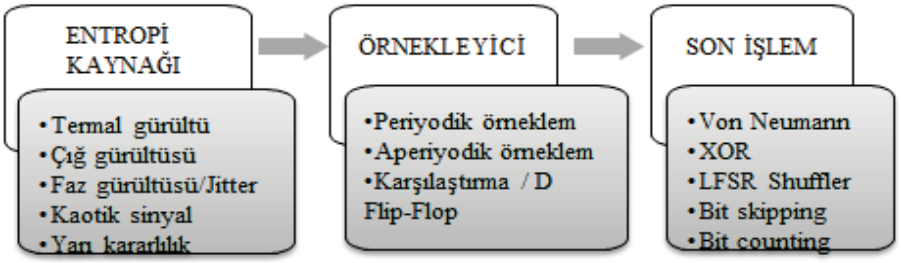
yapıların geliştirilmesi alanında oldukça büyük çabalar sarf edilmektedir. Rasgele sayılar çeşitli kriptografik uygulamalar için zorunluluktur. Çünkü kriptografi; anahtar üretimi ve dağıtımında, başlangıç vektörü oluşturulmasında, kimlik doğrulama protokollerinde, asal sayı ve şifre üretiminde rasgele sayılara ihtiyaç duyar [97]. Bir kriptografik sistemin güvenliği elde edilen sayıların gerçek rasgeleliğine dayanmaktadır. Bu sebeple, RSÜ birçok güvenlik alanlarının en önemli bölümünü oluşturur. Rasgelelik içermek amacıyla genelde binlerce bitten oluşan geniş bir havuz kullanılır ve havuzdaki her bir bit giriş gürültüsünün her bir bitine ve havuzdaki diğer her bite kriptografik olarak güçlü bir yolla bağımlı yapılır. RSÜ'leri Sözde RSÜ, Gerçek RSÜ ve Hibrit RSÜ olmak üzere üç ana sınıfa ayrılmaktadır [98].

3.1. Gerçek Rasgele Sayı Üreteçleri (GRSÜ)
(True Random Number Generators -TRNG)

Rasgele sayıların tamamının güvenilir bir kaynaktan sağlanması amacıyla kriptolojide GRSÜ'leri diğer yöntemlere nazaran daha çok kullanılmaktadırlar [99, 100]. Çünkü bu yapılar entropi kaynağı olarak deterministik karaktere sahip olmayan doğal fiziksel olayları kullanmaktadır. Bu sayede GRSÜ tekniği ile üretilen sayılar periyodik ve tahmin edilebilir olmayan bir yapıya kavuşmakta ve oluşan sayının rasgelelik kalitesi olabildiğince artmaktadır. Bu öngörülemeyen rastgele sayı üretiminin temelinde kararsız dinamik sistemler bulunmaktadır. Bu sistemlerin davranışı kaos teorisi ile açıklanmaktadır. Bu teorinin temeline bakıldığında işlemler deterministik gözükse dahi gerçek hayatta saptanamayacak kadar küçük seviyelerdeki giriş koşul farklılıkları ve durum değişkenleri sapmaları sistemin öngörülemez bir hale gelmesini sağlamaktadır. GRSÜ'ler donanım ve yazılım tabanlı olmak üzere iki farklı teknikle gerçeklenebilirler [101]. Gerçek rasgele sayılar kriptografik uygulamalar için çok önemlidir. Rasgele sayılar kriptografide başlangıç vektörü, özel ve gizli anahtarların oluşumunda, SRSÜ'de tohum üreteci olarak kullanılır. Bu kullanılan rasgele sayıların tahmin edilememesi, iyi istatistiksel özellikler göstermesi ve düzgün dağılımlı olması kriptografik açıdan çok önemlidir. Şekil 1'de gösterildiği gibi GRSÜ'leri gerekli rasgeleliği üreten entropi kaynağı, örnekleyici ve son işlemci olmak üzere üç bloktan oluşmaktadır [102]. Son işlem genellikle sinyaldeki üretim hataları ya da toleransları nedeniyle karşılaşılan istatistiksel kusurları düzeltmek ve rasgeleliği arttırmak için kullanılır. Son işlemin diğer bir amacı saldırgan kurcalamaları ve sıcaklık, basınç gibi çevresel etkenler nedeniyle elde edilen bit dizilerini daha dirençli hale getirmesidir [76, 103]. Son işlem algoritmasına bağlı olarak üretecin güvenliği artacaktır. Sayısal olarak gerçeklenen son işlemlerin en yaygın kullanılanları XOR fonksiyonu, Von Neumann algoritması, extractor fonksiyon, H fonksiyonu, özet fonksiyonu, resilient fonksiyonu ve lojistik harita gibi çeşitli son işlem algoritmaları uygulanmıştır [102, 103]. Bu işlemden sonra sayı üreteçlerinin çıkışının rasgele olduğu, matematiksel olarak kanıtlanamamasına rağmen, geçerli istatistiksel testleri uygulayarak, sayı dizilerinin rasgele olup olmadığını söyleyebiliriz. Bu testler, üretecin çıkışının gerçek bir rasgele diziden beklenenleri karşılayıp karşılamadığını söyler. Ayrıca testlerin sonuçlarına bakılarak RSÜ'nin kalitesi hakkında yorum yapılabilir. Bir sayı dizisinin rasgele olduğunu söylemek için, tüm testlerden geçmesi gerekir. Sadece bir tane test başarısız olsa bile dizi rasgele kabul edilemez. Bu amaçla literatürde geliştirilmiş FIPS-140-1 [29, 31], FIPS-140-2 [45, 46], NIST-800-22 [47, 48], AIS31 [51, 52], DIEHARD [76, 77] ve Test-U01 [97, 98] gibi çeşitli uluslararası istatistiksel testler kullanılmaktadır [102, 103]. Tasarlanan RSÜ'leri için kullanım amacına uygun olarak bu testlerden bir veya bir kaçı tercih edilebilir. Ayrıca GRSÜ'leri Gürültü İşaretinin Doğrudan Kuvvetlendirilmesi Dayalı RSÜ, Osilatör Örnekleme Yöntemine Dayalı RSÜ ve Kaos Tabanlı RSÜ'leri olmak üzere üç ana başlık altında incelenmektedirler.

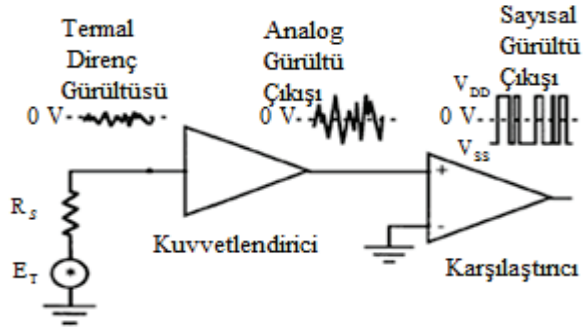
3.1.1. Gürültü işaretinin doğrudan kuvvetlendirilmesi yöntemi ile GRSÜ
(TRNG with the method of direct reinforcement of noise)

Gürültünün doğrudan kuvvetlendirilmesine dayan RSÜ'nin devre gerçeklemelerinde Şekil 2'de görüldüğü ısıl veya saçılma gürültüsü gibi fiziksel gürültü üreten kaynaklar kullanılmaktadır [104]. Daha sonra kuvvetlendirilen gürültü işareti belirlenen bir referansla karşılaştırılıp rastgele '1' ve '0' bit dizisi çıkışı elde edilir. Bu yapıların tasarımındaki asıl zorluk kuvvetlendiricinin tasarımındadır. Kuvvetlendiricilerin yüksek kazançlı, geniş bantlı, düşük giriş kapasiteli ve çıkışında düşük 1/f gürültüsü üretmesi gerekmektedir. Bu sayede kuvvetlendirilecek gürültü beyaz gürültü özelliğini koruyabilecektir. Ancak kuvvetlendirici tasarımında bu dengeyi kurabilmek oldukça zordur. Bu sorunların üstesinden gelmek için giriş kapasitesi ve kazanç-bant genişliği çarpımı istenilen büyüklükte tasarlanmakta ve oluşacak olan yüksek seviyedeki 1/f gürültüsü bir filtre



Şekil 1. Geleneksel GRSÜ blok şeması (Traditional TRNG block diagram)

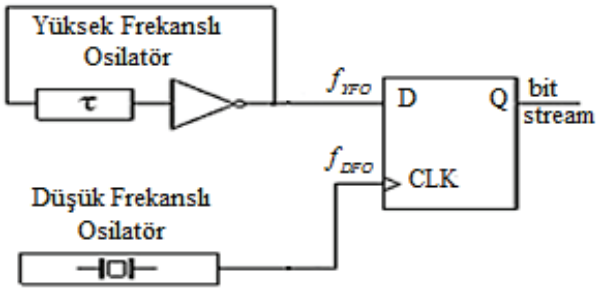
yardımı ile süzülmekte ya da birim güç spektrumu seviyesine kadar bastırılmaktadır. Bu gereksinim de devrenin tasarım yükünü arttırmaktadır. Ayrıca bu tür kaynakların devre üzerinde gerçekleşmesinin bazı sakıncaları ortaya çıkmıştır. Bu sakıncalardan en temel olanı devre içinde var olan gürültü kaynaklarının ürettikleri işaretlerin çok düşük güçlü olmaları, dolayısıyla devredeki istenmeyen işaretlerden etkilenmeleridir [105]. Analog ve sayısal blokların birlikte gerekçelendiği karışık devre yapılarında, besleme ve toprak uçlarındaki muhtemelen periyodik olan istenmeyen işaret seviyelerinin, fiziksel gürültü işaretlerinin ürettiği gürültünün tipik seviyelerin çok üstünde olduğu bilinmektedir. Bu nedenle fiziksel gürültünün kuvvetlendirilerek kullanıldığı tümleşik RSÜ'lerinde, bu tür rastlantısal olmayan istenmeyen işaretlerin etkilerini en aza indirmek için, gürültünün ürettiği alt devreye çok dikkatli bir şekilde elektromanyetik ekranlamanın uygulanması gerekmektedir [106]. Ancak üretilen fiziksel gürültü bu etkilerden mutlaka biraz etkileneceğinden, tüm devre ortamında üretilen fiziksel gürültünün aslında bozulmuş gürültü işareti olduğu düşünülmelidir [107].



Şekil 2. Gürültünün Doğrudan Kuvvetlendirilmesi Yöntemi ile RSÜ devresi [104].
(RNG circuit with the method of direct reinforcement of noise)

3.1.2. Çift osilatör örnekleme yöntemi ile GRSÜ
(TRNG with a dual oscillator sampling method)

Çift osilatörlü GRSÜ yapılarında rasgelelik serbest çalışan yavaş osilatörün faz gürültüsü (seğirme (jittered)) sayesinde elde edilmektedir. Bu yöntemde hızlı osilatör D tipi flip flopun işaret girişine uygulanırken faz gürültüsüne sahip yavaş osilatör D tipi flip flopun saat girişine uygulanmakta ve faz gürültüsünün rasgeleliği sayesinde hızlı osilatör rastgele örneklenebilmektedir. Şekil 3'te basit bir çift osilatör yapısı verilmiştir. Çift osilatörlü yapıdaki rasgelelik için hızlı ve yavaş osilatörün oranları uygun seçilmelidir. Yapıda seğirmeli yavaş osilasyonu üretmek için kullanılan alt devreler (ring osilatör, PLL, ısıl gürültü, termal veya johnson gürültüsü, saçma gürültüsü, kaotik işaret, Metastability vs.) değişmektedir. Bazı durumlarda yavaş osilatörün çıkışının seğirmesi yeterli rastgele dağılımı gösterememekte, gürültü kaynaklı ya da gerilim kontrollü osilatörler kullanılarak seğirme seviyesi arttırılmaktadır. Bu tür tümdevre yapıları genelde entropi kaynağı olarak ring osilatör yapıları kullanılarak gerçeklenmektedir. Bu yapının çalışma kriterlerine bakıldığında yavaş osilatörün frekansı çıkış hızını belirlemektedir ve bu frekansı düşük tutmak çıkış hızını düşürmektedir. Çıkış hızını arttırmak için yavaş osilatörün frekansı arttırılmalıdır. Ancak buna bağlı olarak hızlı osilatörün frekansını da arttırmak gerekir ki bu işlem tümleşik yapıların tasarımını zorlaştırmaktadır. Sadece osilatör örnekleme yöntemi kullanılarak gerçeklenen RSÜ etkili bir rasgelelik sağlayamamaktadır. Bundan dolayı sisteme başka bir belirsizlik kaynağı daha eklenmelidir [108]. Belirsizlik kaynağı olarak direnç ısıl gürültüsü veya kaotik işaretler kullanılabilmektedir [48, 48]. Literatürde çok değişik şekillerde çift osilatör yöntemine dayalı çalışmalar mevcuttur [109, 110].



Şekil 3. Faz gürültüsü kullanılarak gerçekleştirilen çift osilatör örnekleme yapısı [49].
(The dual oscillator sampling structure realized by using phase noise)

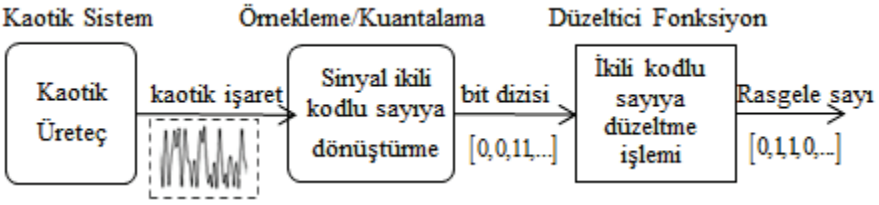
3.1.3. Kaotik devre tabanlı sistemler ile GRSÜ
(TRNG with chaotic circuit-based systems)

Son yıllarda yapılan çalışmalar GRSÜ devrelerinin gerçeklemesinde gürültü kaynağı olarak kaotik sistemlerin kullanılabileceğini göstermiştirler [110, 111]. Bu yapılarda kullanılan kaotik sistemler başlangıç değerlerine üstel olarak duyarlı sistemler olup, bunların çözümlerinin uzun zaman aralıkları için öngörülmesi mümkün olmamaktadır. Bunun yanında kaotik işaretlerin periyodik olmamaları nedeniyle, frekans spektrumları sürekli ve geniştir. Tüm bu özellikler kaotik sistemlerin yüksek başarımlı GRSÜ devrelerinde kullanılabileceğini göstermektedir. Kaotik sistemleri ayrık ve sürekli zamanlı olarak ikiye ayırmak mümkündür. Her iki tip sistemle oluşturulan GRSÜ yapıları vardır [111]. Kaos üreticine dayalı GRSÜ'lerin genel yapısı Şekil 4'te gösterilmektedir. Bu sistemde öncelikle osilatör çıkışı belirli bir frekansta örneklenir, çıkış değerleri kuantalanır, daha sonra da elde edilen bit dizisine düzeltici algoritmalar uygulanarak rastgele sayı üretimi sağlanır. Kaos tanımı incelendiğinde başlangıç koşullarına üstel duyarlı, doğrusal olmayan, deterministik karakterli, uzun vadede periyodik olmayan dinamik sistemler olduğu görülmektedir. Düzensiz davranışları ve başlangıç koşullarına aşırı hassas oluşları nedeniyle, kaotik işaretler de rasgelelik kaynağı olarak değerlendirilmekte ve RSÜ yapımında kullanılmaktadırlar. Şekil 5'te örnek bir kaotik devrenin 2 ve 3 boyutlu faz portreleri (*x-y, x-z, y-z* ve *x-y-z*) verilmektedir [93]. Kaotik sistemleri, otonom ve otonom olmayan kaotik sistemler olarak iki grupta sınıflandırabiliriz. Otonom olmayan kaotik osilatörler zamana bağlı periyodik bir kaynak fonksiyonu *f(t)*

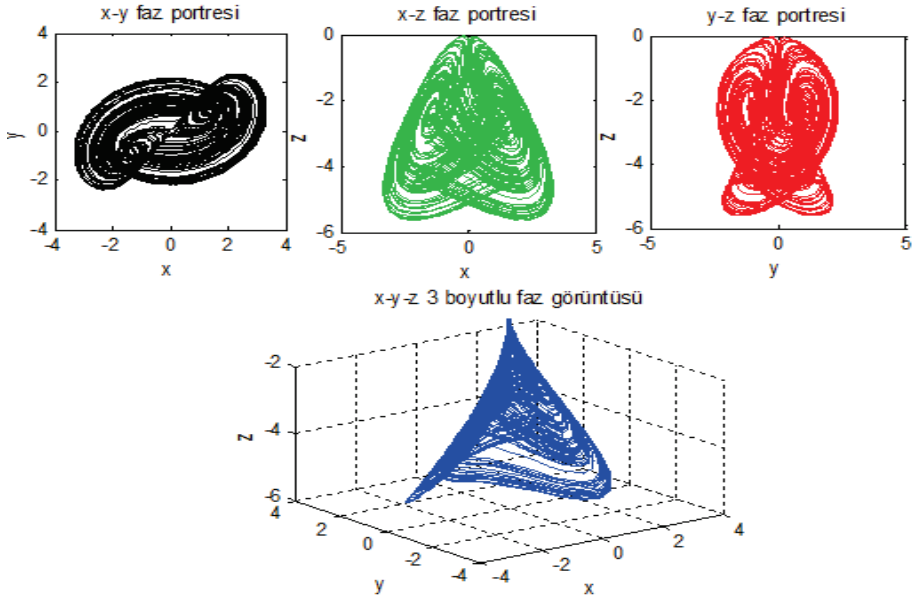
içeren lineer olmayan bir diferansiyel denklem sistemi ile modellenebilmektedir. Bu sistemlerde ise diferansiyel denklemin sağ tarafı "*t*" zaman değişkenine bağlı olmaktadır [112]. Bu zaman değişkeni fazladan bir durum değişkenine karşı geldiğinden, otonom olmayan sistemlerin kaos üretebilmesi için, bunların en azından ikinci dereceden olmasının gerektiği sonucuna kolaylıkla varılabilir. Fakat otonom bir sistemin kaos üretebilmesi için, Poincare Bendixson Teoremi sonucu olarak sistemin en azından üçüncü dereceden olması gerekmektedir [112].

4. LİTERATÜRDEKİ GRSÜ TASARIMLARI
(TRNG DESIGN ON LITERATURE)

GRSÜ tipik uygulanması Şekil 1'de görüldüğü gibi üç ana bölümden oluşmaktadır. İlk olarak, bir FPGA'nın tipik olarak seğirme veya yarı kararlılık durumunda fiziksel rasgele gürültü kaynağıdır. İkinci olarak, sayısallaştırıcı, entropi kaynağından rasgelelik toplar ve ikili bit dizisi üretir. Üçüncü olarak son işlem, korelasyonu azaltarak ve veri sıkıştırması yaparak, rasgele bit dizisinin istatistiksel özelliklerini geliştirir. Literatürde birçok GRSÜ uygulamaları önerilmiştir. Bu çalışmada analog CMOS (Complementary Metal Oxide Semiconductor (Analog Bütünleyici Yarı İletken Metal Oksit)) tabanlı gürültü devreleri, klasik osilatörler ve kaotik sistemler kullanılarak çok farklı tekniklerle gerçekleştirilen GRSÜ tasarımları karşılaştırılacaktır. Bu karşılaştırmalar sonucunda son yıllarda FPGA'ler üzerinde kaotik sistemler kullanılarak sayısal olarak tasarlanan GRSÜ'lerinin teknik üstünlükleri ortaya konulacaktır. Tavas vd. yaptıkları çalışmada [49] RSÜ devresinde kullanılabilecek ve tümleştirilmeye uygun yeni kaos üreteci önerilmiştir. Ayrıca tasarım ortamında yapılan benzetimlerden sonra bu devrelerin 0.35 µm AMS CMOS prosesi ile tümleşik devre üretimleri yapılmış ve GRSÜ oluşturulmuştur. Üretilen kaotik devrelerden 16 MHz ile 25 MHz arasında değişen bant genişlikli kaotik işaretler elde edilmiştir. GRSÜ yapısının doğrulanması için FIPS-140-1 rastgele sayı testi uygulanmıştır. Üretimi yapılan GRSÜ devresinin ortalama bit üretim hızı 2 Mbit/s olarak verilmiştir. Ergün vd. yaptıkları çalışmada [113] otonom olmayan kaotik sistem kullanılarak CMOS teknolojisi ile GRSÜ yapısı önerilmiştir. Önerilen yapının çalışma frekansı 1,24 MHz ve bit üretim hızı 10 Mbit/s olarak belirtilmiştir. Sunulan çalışmadan elde edilen rasgele dizinin NIST-800-22 testlerinden başarılı bir şekilde geçtiği vurgulanmıştır. Çiçek vd. sunduğu çalışmada [114] CMOS teknolojisi ile ayrık zamanlı kaos tabanlı yeni bir tasarım metodu kullanılarak GRSÜ yapısı geliştirilmiştir. GRSÜ yapısında bulunan kaotik sistem için tek boyutlu harita kullanılmıştır. Yapılan tasarımdan elde edilen rasgele bitler NIST testlerine tabi tutulmuş ve 11 testten geçtiği belirtilmiştir. Farklı bir çalışma



Şekil 4. Kaotik rastgele sayı üreten sistemin blok diyagramı [111].
(The block diagram of chaotic random number generating system)



Şekil 5. Örnek bir kaotik sistemin 2 ve 3 boyutlu faz portrelerinin görüntüsü.
(The display of 2D and 3D phase portraits of a sample chaotic system)

Pareschi vd. tarafından yapılmıştır [116]. Yapılan çalışmada kriptografik uygulamalar için yeni bir kaos tabanlı GRSÜ sunulmuştur. Tasarımın prototipi 0.35 µm CMOS teknolojisi ile gerçekleştirilmiş ve çalışmanın doğrulanması için sisteme NIST testleri uygulanmıştır. Yapılan testlerde sistemin bit üretim hızı 40 Mbit/s'ye kadar çıkmaktadır. Son yıllarda CMOS tabanlı gerçekleştirilen GRSÜ tasarımlarda kullanılan yöntemler, uygulanan testler, çalışma frekansları ve bit üretim hızları ile ilgili bilgiler Tablo 3'te verilmiştir. Literatürde FPGA tabanlı klasik osilatörlerle gerçekleştirilen GRSÜ tasarımları da önemli yer almaktadır. Kohlbrenner vd. [31] yaptıkları GRSÜ tasarımında her biri iki açık tutucu, bir tampon ve bir tümleyenden oluşan osilatör halkası kullanmışlardır. Entropi kaynağı olarak osilatör halkadan üretilen saat sinyalindeki seğirme kullanılmıştır. Halka osilatör saatlerindeki seğirme halka osilatör döngüsü içeren mantık kapılarının kararsız yayılma gecikmelerinden ileri gelmektedir. Örnekleyici devre, diğer halka çıkışı saat girişi ile bağlı iken osilatör halkalardan birinin çıkışı veri girişine bağlı olan D flip-flop'tur. Rasgele bitin çıkışına örnekleyici devre karar verir. Bu kurulumun doğru çalışması için; iki osilatör halkasının sıklığı, tamamen aynı veya doğru bir şekilde eşleşmiş olmalıdır. Bu GRSÜ'nün çıkışı XOR son işlemine tabi tutulmuştur. Çıkış oranı düşüktür ve elde edilen bit 1 Mbit/s den daha azdır. Çıkış dizisi istatistiksel olarak NIST testine tabi tutularak doğrulanmıştır. Bu tasarımın avantajı, bütün FPGA'lerin ortak kaynaklarını kullanması, matematiksel model uygulanabilmesi, çok az lojik kaynaklar kullanması ve düşük güç tüketimidir. Danger vd. [47] yaptıkları çalışmada klasik PLL ve Ring osilatörlerin sınırlı bant aralığına sahip olduklarını ve bu osilatörler ile oluşturulan GRSÜ'lerinin bit üretim hızlarının birkaç Mbit/s'yi geçmeyeceğini belirtmişlerdir. Bu probleme çözüm olarak daha yüksek bit üretim hızı sağlayan yeni bir yapı sunulmuş ve bu yapı FPGA ile gerçeklenmiştir. FPGA'de açık döngü yarı kararlılığına dayanan bir GRSÜ önermişlerdir. Bu tasarımın prensibi gecikme dizisidir ve dizideki birkaç kademe noktasından örneklenmiş sinyaller birlikte XOR edilerek rasgele bir sinyal oluşturmak için örneklenmektedir. Elemanlar arasındaki gecikme önemli ve bu duruma karşı özel özen gösterilmelidir. Bu GRSÜ'nün rapor edilen bit oranı 20 Mbit/s'dir. Sunulan yeni yapının doğrulanması NIST testleri ile yapılmıştır. Sonuç olarak yapının çalışma frekansı 20 MHz olarak verilmiştir. Bir diğer çalışma István vd. [52] tarafından FPGA tabanlı klasik jitter osilatör yöntemi kullanılarak yapılmıştır. Önerilen yöntemin doğruluğu NIST ve TestU01 testleriyle sağlanmıştır. Sistemin çalışma frekansı 50 MHz bulmakla beraber, kullanılan osilatör nedeniyle sistemin bit üretim hızı 1,92 Mbit/s'yi aşmamaktadır. Schellekens vd. [120] çoklu ring osilatörünü FPGA'de modellemişlerdir. FPGA çipi olarak Xilinx firmasının Virtex-II çipi kullanılmıştır. Tasarımı yapılan sistemin örnekleme zamanı 40 MHz olarak verilmiştir. Tasarımın rasgelelik kontrolü standart NIST-800-22 testleri ile yapılmıştır. Test sonuçlarına göre GRSÜ'nin bit üretim hızı 2,5 Mbit/s olduğu ifade edilmiştir. Dichtl vd. [121] FPGA'de Fibonacci ve Galois ring osilatörünü modellemişlerdir. Tasarımın gerçeklenmesi Xilinx firmasının üretmiş olduğu FPGA çiplerinden Spartan-3 çipini içeren Starter kit kullanılarak yapılmıştır. Sistemin ürettiği bit üretim hızı 12,5 Mbit/s olarak verilmiştir. Diğer bir başka çalışmada Fischer vd. [122] PLL tabanlı osilatörü FPGA çipleriyle gerçekleştirmişlerdir. GRSÜ yapısı VHDL'de tanımlanmış ve Altera firmasının Quartus-II programı kullanılarak gerçeklenmiştir. Kriptografik uygulamalar için tasarlanan GRSÜ'nin performans analizi

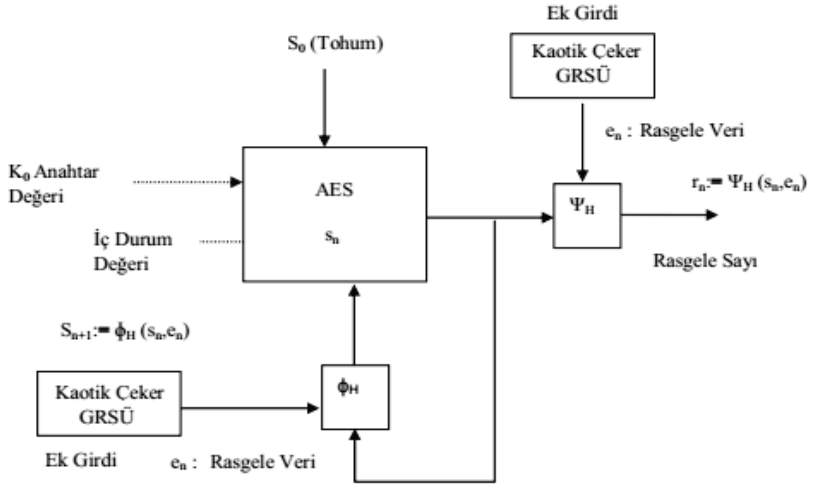
Tablo 3. Literatürde CMOS tabanlı gerçekleştirilen GRSÜ tasarımları ve teknik özellikleri
(TRNG designs and technical specifications realized CMOS-based in literature)

Çalışmayı Yapan/ Kaynak	Kullanılan Yöntem	Uygulanan Testler	Tasarım	Çalış. Frek. (MHz)	Bit Üretim Hızı (Mbit/s)
Tavas vd., 2010, [49]	Osilatör örnekleme	FIPS-140-1	CMOS teknolojisi	----	2
Bucci vd., 2016, [106]	Ayrık zamanlı kaos tabanlı	AIS31	CMOS teknolojisi	50	12,5
Ergün vd., 2007, [113]	Osilatör örnekleme	NIST-800-22	CMOS teknolojisi	1,24	10
Çiçek vd., 2014, [114]	Ayrık zamanlı kaos tabanlı tek boyutlu harita (Lojistik, Tent, Bernoulli)	NIST-800-22	CMOS teknolojisi	-----	-----
Ning vd., 2015 , [115]	Ring Osilatör örnekleme	DieHard	CMOS teknolojisi	20	10-20
Pareschi vd., 2010, [116]	Osilatör örnekleme	NIST-800-22	CMOS teknolojisi	-----	40
Dhanuskodi vd., 2014, [117]	Osilatör örneklem yöntemi	NIST-800-22	CMOS teknolojisi	-----	127
Aguilar vd., 2014, [118]	Ayrık Zamanlı kaos tabanlı tek boyutlu harita	NIST-800-22 FIPS-140-2	CMOS teknolojisi	-----	0,250
Park vd., 2015, [119]	Ayrık Zamanlı Boolean kaotik osilatör	NIST-800-22	CMOS teknolojisi	300	-----

NIST testleri ile yapılmıştır. Testlerden elde edilen sonuçlara göre tasarlanan sistemin bit üretim hızı 70 Kbit/s olarak elde edilmiştir. Kolay tasarım ve uygulamaları, sentezin bütünüyle FPGA araçları içinde yapılabiliyor olması, sabit çıkış hızına sahip olması ve düşük güç tüketimi bu tasarımın avantajları olarak gösterilebilir. Düşük çıkış hızı ve bu GRSÜ tasarımının, analog PLL içeren FPGA'lerde sınırlandırılmış olması bu yapının dezavantajlı yanıdır. Sunar vd. [126] tarafından 2007 yılında halka osilatöre dayalı FPGA tabanlı yeni bir GRSÜ tasarımı önerilmiştir. Temel olarak serbest salınımlı halka osilatörlerin çıkışları XOR işlemi ile birlikte toplanır ve sonra örneklenir. Rasgelelik kaynağı faz seğirmesidir. Halka osilatör tek sayıda tümleyen içeren gecikmelerin birleşimsel döngüsüdür. Bu tasarımda her biri 13 tümleyenden oluşan 114 adet halka osilatör kullanılmaktadır. Kullanılan halka osilatörlerin sayısı, ölçülür seğirmelere göre belirlenir. Tüm halka osilatörlerin çıkışları yüksek frekanslı rasgele sinyal almak için XOR işlemine girişi yapılır. XOR işleminin çıkışı da düşük frekanslı saat frekansı ile örneklenir. Daha sonra resilient fonksiyon son işlemi kullanılarak, rasgele sinyaldeki birler ve sıfır arasındaki orantısızlıklar düzeltilebilir. Bu GRSÜ'de son işlemi de içererek başarılan bit oranı 2,5 Mbit/s'dir. Çıkış bit dizileri Diehard ve NIST testleri kullanılarak doğrulanmıştır. Bu tasarım Dichtl vd. tarafından eleştirilmiştir. Bu eleştiriler arasında örnekleme oranı ve halka osilatörlerin bağımsızlık varsayımı vardır. Örnekleme hızı kolay düşürülmüş olsa da, çok sayıda halka kullanıldığında halka osilatörlerin bağımsızlığını doğrulamak oldukça zordur. Küçük sayıda halka için, dikkatli yerleşim ve yönlendirme ile diğerleri ile etkileşimden halkalar yeterince izole edilebilir. 2008 yılında Wold vd. [125] yaptıkları çalışmada Sunar tasarımının [126] her bir osilatör halkasına D flip-flop ekleyerek ve XOR'lar arasındaki hız sorununu giderecek yeni bir yapı önermişlerdir. Burada önerilen GRSÜ'de sadece 25 halka osilatör kullanarak Diehard ve NIST istatistiksel testlerini başarılı bir şekilde geçmişlerdir. Elde edilen çıkış hızı 100 Mbit/s olmuştur. Tuncer ve Avaroğlu yaptıkları çalışmalarında [127, 128] GRSÜ'lerinin çıkış hızını düşürmeden, istatistikî zayıflıkları gideren yeni bir son işlem algoritması önermişlerdir. Bu uygulamada entropi kaynağı olarak halka osilatörler tarafından üretilen faz seğirmesi kullanılarak FPGA ortamında donanımsal olarak GRSÜ gerçekleştirilmiştir. Önerilen son işlem kaotik davranış sergileyen lojistik haritadır. Lojistik harita 1. dereceden bir denklem olup bir başlangıç koşulu ve bir kontrol parametresine gerek duymaktadır. Bu sebepten dolayı donanım üzerinde gerçekleştirilmesi kolaydır. Gerçekleştirilen RO tabanlı bir GRSÜ sisteminde lojistik haritanın üretilen sayılara etkisini gözlemleyebilmek için dört farklı senaryo geliştirilmiştir. GRSÜ sisteminde kullanılan RO sayıları ve RO'ler deki tümleyen sayıları sırasıyla (114,13) (25,3) (10,3) (5,3) seçilmiştir. Tüm senaryolarda son işlem olarak lojistik harita kullanılmış olup her bir sistem Altera'nın EP4CE115F29C7 tabanlı FPGA bordunda gerçekleştirilmiştir. Burada lojistik haritanın son işlem olarak kullanımını gösterebilmek için Sunar tarafından önerilen [126] RO tabanlı GRSÜ sistemi kullanılmıştır. Sunar tarafından üretilen sistemde entropi kaynağından üretilen rasgele bit dizilerinde korelasyon olması nedeniyle son işlemsiz olarak testleri geçememiştir. Bunun sonucunda resilient fonksiyonu olarak adlandırılan son işleme tabi tutulmuş olup çıkış hızı ve oranı 1/16 oranında azalmıştır. Bu amaçla sistemin entropi kaynağında bulunan olası eksikliği gidermek için lojistik harita son işlem olarak önerilmiştir. Lojistik haritanın rasgeleliğinin tahmin edilememe ve rasgelelik özellikleri katması nedeniyle GRSÜ sisteminin güvenliği artacaktır. Sunar sisteminde çıkış hızı 2,5 Mbit/s iken geliştiren sistemde yaklaşık 20 Mbit/s olmuştur. Her bir sistem tarafından elde edilen sayıların istatistiksel testleri NIST 800.22 testine göre elde edilmiştir. Test sonuçlarına göre lojistik haritanın son işlem olarak kullanılabileceği gösterilmiştir. Halka osilatör tabanlı GRSÜ'lerin avantajı, bağımsız teknoloji, kolay tasarım ve uygulamaları, sentezin bütünüyle FPGA araçları içinde yapılabiliyor olması, nispeten sabit ve yüksek çıkış hızına sahip olmalarıdır. Ancak halka osilatör sayısının çokluğundan dolayı yüksek güç tüketimi, halka osilatörlerin bağımsız olmaması rasgelelik kalitesinin düşmesine ve çıkışın korelasyonlu olması, resilient fonksiyonundan dolayı saldırıların tespit edilemeyecek olması, güç tüketimi dolayısıyla aşırı lokal ısınmalar tasarımın dezavantajlarıdır. Klasik osilatörler kullanılarak son birkaç yılda FPGA üzerinde gerçekleştirilen GRSÜ tasarımlarında kullanılan osilatör, FPGA kart özellikleri, uygulanan testler, çalışma frekansı ve bit üretim hızı gibi teknik özellikler Tablo 4'te verilmiştir. Ayrıca literatürde saf SRSÜ'lerine FPGA üzerinde kaos tabanlı tasarlanan GRSÜ'lerin ek girdi olarak kullanıldığı ve Şekil 6'da gösterilen yeni Hibrit SRSÜ'leri yer almaktadır. Bu önerilen çalışmalardaki amaç saf SRSÜ'lerin deki geçerli iç durum değerinin gerçek rasgele veri (GRSÜ) ile güncellenerek sisteme tahmin edilemem özelliği katması ile SRSÜ sistemlerinin kriptografik uygulamalarda kullanılmasını uygun hale getirmektir. Avaroğlu yaptığı tez çalışmasında [129] AES blok şifreleme standartı kullanılarak oluşturulan saf SRSÜ, Xilinx FPGA üzerinde Burke-Shaw kaotik osilatör kullanılarak tasarlanan GRSÜ ek girdi olarak eklenmiştir. Sistemde her bir adımda rasgele üretilen 128 bit tohum değeri ve anahtar değeri AES'e girilerek şifreli elde edilen 128 bit şifreli tohum değeri ile Burke-Shaw kaotik çekerden elde edilen 128 bit rasgele veri XOR işlemi yapılarak çıkışa verilmiştir. Yeni iç durum değeri ise şifreleme sonucu AES'ten elde edilen veri ile kaotik çekerden elde edilen verinin XOR yapılarak sisteme girilmiştir. Bu sayede hem iç durum değeri hem de çıkış değeri FPGA üzerinde kaos tabanlı tasarlanan GRSÜ ile desteklenmiştir. GRSÜ ünitesi 32 bit IEEE 754-1985 kayan nokta sayı standardına uygun olarak Virtex-6 FPGA çipinde VHDL dilinde RK5-Butcher algoritması ile kodlanmıştır. Sistemin çalışma frekansı 373 MHz olarak verilerek tasarlanan Hibrit SRSÜ'inin tüm NİST testlerini başarılı bir şekilde geçtiği verilmiştir. Özkaynak yaptığı çalışmada [130] kaos tabanlı GRSÜ ünitesini saf SRSÜ tasarımına ek girdi olarak girerek önerdiği Hibrit RSÜ'nin kriptografik uygulamalarda kullanılabileceğini göstermiştir. Avaroğlu vd. yaptıkları diğer bir çalışmada [131] FPGA üzerinde ring osilatör tabanlı tasarladıkları kaotik GRSÜ ünitesini saf SRSÜ ek girdi olarak kullanarak Hibrit SRSÜ tasarlamışlardır. Tasarladıkları sistemin NİST 800-22 istatistiksel testlerden başarılı bir şekilde geçtiğini göstermişlerdir.

Tablo 4. Literatürde FPGA tabanlı Klasik osilatörlerle gerçekleştirilen GRSÜ tasarımları ve teknik özellikleri
(TRNG designs and technical specifications realized by FPGA-based classic oscillators in literature)

Çalışmayı Yapan	Kullanılan Teknik	FPGA Özellikleri	Uygulanan Testler	Çalışma Frek. (MHz)	Bit Üret. Hız (Mbit/s)
Kohlbrenner vd., 2004, [31]	Ring osilatör	Xilinx Virtex XCV1000	NIST-800-22	-----	< 1
Danger vd., 2009, [47]	Yeni bir yapı	Xilinx Spartan-3	NIST-800-22	20	20
Jessa vd., 2010, [50]	Ring osilatör	Xilinx Virtex-5	NIST-800-22	300	7,14
Wold vd., 2009, [51]	Ring osilatör	Altera Cyclone II	NIST-800-22 DIEHARD	300	-----
Istvan vd., 2009, [52]	Klasik jitter	Xilinx Spartan3E	NIST-800-22 TestU01	50	1,92
Çiçek vd., 2014, [102]	Ayrık Kaotik sistem (Bernoulli map--FPAA)	Xilinx Spartan XC3S1600E	NIST-800-22	2	1,5
Schellekens vd., 2006, [120]	Çoklu ring osilatör	Xilinx Virtex II	NIST-800-22	40	2,5
Ditchtl vd., 2008, [121]	Ring osilatör	Xilinx Spartan-3	NIST-800-22	-----	12,5
Fischer vd., 2002, [122]	PLL osilatör	Altera Quartus II	NIST-800-22	-----	1
Wieczorek vd., 2014, [123]	Çift kararlı Flip/Flop	Xilinx Spartan3E	NIST-800-22	50	5
Lozach vd., 2013, [124]	Open Loop Metastability	Xilinx Virtex-5 XC5VLX50T	AIS.31 NIST-800-22	22	20
Wold vd., 2008, [125]	Ring osilatör	Altera Cyclone II	NIST-800-22 DIEHARD	-----	100
Sunar vd., 2007, [126]	Ring osilatör	Xilinx Virtex-2	NIST-800-22 DIEHARD	-----	2,5
Tuncer ve Avaroğlu, 2015, [127-128]	Ring osilatör	Altera EP4CE115F29C7	NIST-800-22 TESTU01	450	25



Şekil 6. Önerilen Hibrit SRSÜ genel tasarımı [129].(General design of the proposed Hybrid PRNG)

Farklı bir çalışmada Merah vd. [132] kaotik Chua devresini FPGA üzerinde tasarlayarak GRSÜ tasarımı gerçekleştirmişlerdir. Tasarladıkları kaos tabanlı GRSÜ ünitesini saf SRSÜ için ek girdi olarak kullanarak kriptografik uygulamalar için şifreleme açısından güvenli Hibrit SRSÜ tasarlamışlardır. Avaroğlu vd. yaptığı bir diğer çalışmada [133] kriptografik sistemler için Hibrit SRSÜ tasarlamışlardır. Bu çalışmada FPGA üzerinde Sprott 94 G

kaotik çeker tabanlı GRSÜ tasarımını Hibrit SRSÜ için ek girdi olarak kullanmışlardır. Kaotik sistemin donanımsal tasarımında Xilinx Virtex-6 FPGA üzerinde 32-bit IEEE 754-1985 kayan nokta standardında VHDL dilinde RK5-Butcher nümerik algoritmasını kullanarak gerçekleştirmişlerdir. Tasarladıkları sistemin NİST testlerinden başarılı bir şekilde geçtiğini ve sistemin çalışma frekansını 339 MHz olarak vermişlerdir. Literatürde son birkaç yılda FPGA üzerinde kaos tabanlı gerçekleştirilen GRSÜ tasarımlarının Hibrit SRSÜ'lerine ek girdi olarak kullanıldığı çalışmaların teknik özellikleri Tablo 5'te verilmiştir. Literatürde FPGA üzerinde tamamen sayısal diferansiyel kaotik sistemleri kullanarak GRSÜ tasarımları yer almaktadır. Zidan vd. [134] yaptıkları çalışmada gömülü, tamamen sayısal diferansiyel kaosa dayalı GRSÜ önermişlerdir. Sayısal devrenin çıkışı maksimum Lyapunov üslerinin çıkış zaman serilerini hesaplayarak kaotik olduğunu kanıtlamıştır. Sistemin çözümünde dördüncü dereceden Runge Kutta, orta nokta ve Euler tekniği olmak üzere üç faklı metot kullanılmıştır. Sistem, VHDL'de kodlanarak ve Xilinx Virtex 4 FPGA çipi üzerinde gerçekleştirilmiştir. Devre oldukça küçük bir alan kaplamış ve çıkış hızı 2,1 Gbit/s olarak elde edilmiştir. Yeni önerdikleri son işlemden geçirildikten sonra NIST testine tabi tutulmuş ve başarıyla geçmiştir. Koyuncu vd. [135] yaptıkları çalışmada Sprott 94G kaotik sistemini Euler nümerik algoritması ile IEEE-754-1985 kayan nokta sayı formatında VHDL programlama dilini kullanarak Xilinx Virtex-6 FPGA çipinde tasarlamışlardır. Yaptıkları tasarımda kuantalama ünitesinden çıkan ikili sayı bitleri üzerine düzeltici fonksiyon olarak XOR yöntemini uygulamışlardır. Tasarım sonucunda elde ettikleri sayı dizilerinin rasgeleliğini kanıtlamak için uluslararası test standartları olan NIST-800-22 ve FIPS 140-1 testlerini uygulayarak testlerden başarılı bir şekilde geçtiklerini yaptıkları çalışmada göstermişlerdir. Diğer bir çalışmada Koyuncu [111] doktora tezinde 2 adet yeni kaotik sistemi 4 farklı algoritma ile 3 ayrı kuantalama tekniği kullanarak VHDL dilinde 32 bit IEEE-754-1985 kayan nokta sayı standardında Xilinx Virtex-6 FPGA çipi üzerinde GRSÜ tasarlamıştır. Tasarım sonucunda 24 adet farklı GRSÜ sonuçları elde etmiştir. Elde ettiği sonuçlar üzerine uluslararası rasgelelik testleri olan NIST 800-22 ve FIPS 140-1 testlerini uygulayarak optimum sonucu veren kuantalama ve algoritmayı ortaya çıkarmıştır. Son birkaç yılda kaotik tabanlı sistemleri kullanarak FPGA üzerinde tasarlanan GRSÜ'lerinin teknik özellikleri Tablo 6'da detaylı bir şekilde verilmiştir.

5. SONUÇLAR VE TARTIŞMALAR
(RESULTS AND DISCUSSIONS)

Tablo 3, 4, 5 ve 6'da ki çalışmalarda belirtildiği gibi literatürde farklı özelliklerde birçok GRSÜ tasarımları önerilmiştir. Bu tasarımlar kullanım yerine, entropi kaynakları ve üretim tekniklerine göre önemli ölçüde değişiklikler göstermektedirler. Her tasarımın güçlü ve zayıf yanları vardır. Bu özelliklerin bazıları performans ile ilgili bazıları ise güvenlik ve sağlamlıkla ilgilidir. GRSÜ olarak kullanılan kaotik sistemler kriptoloji ve bilgi güvenliği sistemlerinde anahtar olarak kullanılabilmektedir. Ancak anahtarların sistem dışında kontrolsüz ortamlarda üretimi sistemin güvenilirliğini azaltmaktadır. Bu dezavantajı ortadan kaldırmak için günümüzde donanımsal kriptografinin ve güvenli haberleşmenin gelişimi, programlanmış kripto aritmetiğinin bir entegre içerisinde gerçekleştirilmesi yönündedir. Bundan dolayı anahtarların sayısal devre tabanlı FPGA gibi programlanabilir donanımlarda üretilmesi gittikçe popüler olmaktadır. Programlanabilir FPGA çipleri yüksek hız ve kapasiteleri nedeniyle özellikle yüksek performans ve işlemci gücü gerektiren kriptoloji ve güvenli haberleşme gibi uygulamalarda bilgi güvenliği kapasitesini iyileştirmede önemli bir potansiyele sahiptir. GRSÜ gerçek entropi kaynaklı tamamen rasgele sayılar üreten bir donanımdır. Tablo 3'te incelenen analog CMOS tabanlı GRSÜ tasarımlarının çalışma frekansları 1-25 MHz kadar, bit üretim hızları da maksimum 1-40 Mbit/s'ye kadar çıkabilmesine rağmen donanımsal olarak üretilen GRSÜ sistemlerinin çok altında kalmaktadır. FPGA tabanlı klasik osilatörlerle gerçekleştirilen ve Tablo 4'te incelenen GRSÜ tasarımlarının çalışma frekansları 20-300 MHz seviyelerine kadar çıkabilirken kullanılan osilatörler ve yöntemden dolayı bit üretim hızları 1-40 Mbit/s'ye kadar düşmektedir.

Tablo 5. Literatürde Hibrit SRSÜ'lerine ek girdi olarak FPGA tabanlı kaotik sistemlerle gerçekleştirilen GRSÜ tasarımları ve teknik özellikleri
(TRNG designs and technical specifications realized by FPGA-based chaotic systems as additional input to hybrid PRNG in the literature)

Çalışmayı Yapan	Kullanılan Teknik	FPGA Özellikleri	Uygulanan Testler	Çalışma Frek. (MHz)	Bit Üretim Hız (Mbit/s)
Avaroğlu, 2014, [129]	Kaotik osilatör Burke-Shaw	Xilinx Virtex-6 XC6VLX550T	NIST-800-22	373	------
Özkaynak, 2014, [130]	Ayrık zamanlı kaotik fonksiyon	FPGA	NIST-800-22	------	------
Avaroğlu, 2014, [131]	Ring osilatör 5R+3İ	FPGA	NIST-800-22	------	------
Merah, 2013, [132]	Kaotik osilatör devresi	Xilinx Spartan-6 XC6SLX45	NIST-800-22	30,02	1,9 G
Avaroğlu, 2015, [133]	Kaotik osilatör Sprott 94 G	Xilinx Virtex-6 XC6VLX550T	NIST-800-22	339	------

Tablo 6. Literatürde FPGA üzerinde tasarlanan tamamen sayısal diferansiyel kaotik devre tabanlı GRSÜ
(Fully digital differential chaotic circuit based TRNG designed on FPGA in literature)

Çalışmayı Yapan	Kullanılan Kaotik Sistem ve tasarım özellikleri	Son işlem	FPGA Özellikleri	Uygulanan Testler	Çalış. Frek. (MHz)	Bit Üretim Hızı
Koyuncu, 2014, [111]	2 adet yeni kaotik sistem, 4 farklı Algoritma, 3 farklı Kuantalama, VHDL 32bit IEEE 754-1985	XOR	Xilinx Virtex-6 XC6VLX550T-2FF1759	NIST-800-22 FIPS 140-1	339-401	53-132 Mbit/s
Zidan vd., 2011, [134]	Lyapunov üslerinin çıkış zaman serileri, 3 Farklı algoritma, Verilog HDL	Yeni son işlem önerilmiş	Xilinx Virtex 4	NIST-800-22	-----	2 Gbit/s
Koyuncu vd., 2014, [135]	Sprott 94G Euler algoritma, 32bit IEEE 754-1985	XOR	Xilinx Virtex-6 XC6VCX75T	NIST-800-22, FIPS 140-1	400	-----
Wang vd. 2016, [136]	Yüksek boyutlu sayısal kaotik sistem	XOR	Altera DE2	-----	50	-----
Fatemi, vd., 2016, [137]	Kaotik harita (Bernoulli Map)	XOR	FPGA	NIST-800-22	-----	-----
Wang, vd., 2016, [138]	Çapraz ring osilatörlerin kaotik davranışı (CROs)	XOR	Altera Cyclone IV	NIST-800-22, Diehard	-----	240 Mbit/s
Koyuncu vd., 2016, [139]	SPCS kaotik sistemi Runge-Kutta (RK-4) VHDL 32bit IEEE 754-1985	XOR	Xilinx Virtex-6 C6VLX240T-1-FF1156	FIPS-140-1 NIST-800-22	293	58,76 Mbit/s

Yukarıda özetlenen çalışmalardan da gözlemlendiği gibi geleneksel GRSÜ yöntemlerinde çözümlenemeyen bazı önemli sorunlar ortaya çıkmaktadır:

- Analog elemanlar kullanılarak gerçekleştirilen osilatörlerin çalışma frekanslarının düşük olması
- Isıl veya saçılma gürültüsü gibi fiziksel gürültü üreten kaynaklarının ürettikleri işaretlerin çok düşük güçlü olmaları ve dolayısıyla devredeki istenmeyen işaretlerden etkilenmeleri
- Ayrıca analog elemanlar kullanılarak gerçekleştirilen yapıların sistem parametrelerinin değişimine dirençli olması
- Klasik osilatörlerin çalışma frekanslarının yüksek olmasına rağmen yapısından kaynaklanan ortalama bit üretim hızının belirli bir hızın üzerine çıkamaması.

Geleneksel rasgele sayı üretiminde yukarda belirtilen olumsuz etkileri yok etmek, daha hızlı ve güvenli rasgele diziler elde etmek için tamamen sayısallaştırılmış gömülü kaos tabanlı GRSÜ'leri alternatif olarak görülmüş ve son bir kaç yılda bu alanda önemli çalışmalar yapılmıştır. Bu çalışmalarda kaotik işaret üreteçlerinin kendilerine has özelliklerinden dolayı GRSÜ'lerin de gürültü kaynağı yerine kullanılabileceği gösterilmiştir. Tablo 6'de FPGA üzerinde kaotik sistemleri kullanarak gömülü olarak gerçekleştirilen GRSÜ'lerinin hem çalışma frekanslarının 400 MHz seviyelerinde hem de bit üretim hızlarının diğer yöntemlere göre çok daha yüksek olduğu görülmektedir. FPGA tabanlı sayısal kaotik sistemler rasgele sayı üretimi, kriptoloji ve güvenli haberleşme alanlarında bilgi güvenliği kapasitesini iyileştirmede önemli bir potansiyele sahiptir. Bu kapsamlı araştırma ile ilk olarak, GRSÜ kullanılan yöntemler arasındaki farklılıklara dikkat çekmek istenmektedir. İkinci olarak, FPGA üzerinde sayısal tabanlı tasarlanan kaotik osilatörlerin donanım özelliklerine ve çalışma performanslarına yer verilmiştir. Üçüncü olarak son yıllarda literatürde GRSÜ kullanılan FPGA üzerinde gerçekleştirilen kaos tabanlı yapılarının özelliklerine ve geleneksel yöntemlerle karşılaştırıldığında ortaya çıkan yüksek çalışma performanslarına dikkat çekmektir. Son olarakta farklı özelliklere sahip yeni kaotik osilatörlerin ve GRSÜ yapılarının tasarımlarına yönelik çalışmalara ivme kazandırmaktır.

6. SİMGELER (SYMBOLS)

GRSÜ : Gerçek Rasgele Sayı Üreteçleri
DSPs : Sayısal İşaret İşlemciler
ASIC : Uygulamaya Özel Tümleşik Devreler

FPGA	: Alan Programlanabilir Kapı Dizileri
VHSIC HDL	: Çok Yüksek Hızlı Tümleşik Devre Donanım Tanımlama Dili
RSÜ	: Rasgele Sayı Üreteçleri
SRSÜ	: Sözde Rasgele Sayı Üreteçleri
HRSÜ	: Hibrit Rasgele Sayı Üreteçleri
M.I.T.	: Massachusetts Teknoloji Enstitüsü
CMOS	: Analog Bütünleyici Yarı İletken Metal Oksit
NIST	: Ulusal Standartlar ve Teknoloji Enstitüsü
FIPS	: Federal Bilgi İşleme Standartları
XOR	: Özel Veya
AES	: Gelişmiş Şifreleme Standardı

KAYNAKLAR (REFERENCES)

1. Yılmaz D., Güler N.F., A Study on the Chaotic Time Series Analysis, Journal of the Faculty of Engineering and Architecture of Gazi University, 21 (4), 759-779, 2006.
2. Banerjee S., Kurths J., Chaos and Cryptography: A new dimension in secure communications, The European Physical Journal Special Topics, 223 (8), 1441-1445, 2014.
3. Jin L., Mei J., Li L., Chaos control of parametric driven Duffing oscillators, Appl. Phys. Lett., 104 (13), 1011-1015, 2014.
4. Hoang T.M., Tran D., Cryptanalysis and security improvement for selective image encryption, The European Physical Journal Special Topics, 223 (8), 1635-1646, 2014.
5. Akgul A., Calgan H., Koyuncu İ., Pehlivan İ., Istanbullu A., Chaos-based engineering applications with a 3D chaotic system without equilibrium points, Nonlinear Dyn., 84, 841-495, 2016.
6. Xiong A., Zhao X., Han J., Liu G., Application of the chaos theory in the analysis of EMG on patients with facial paralysis, Robot Intelligence Techlogy and Applications, 2 (274), 805-819, 2014.
7. Zhengxing H., Wei D., Huilong D., Haomin L., Similarity measure between patient traces for clinical pathway analysis: problem, method, and applications, IEEE J. Biomed. Health. Inf., 18 (1), 4−14, 2014.
8. Zexin K., Jiang S., Lin M., Yanhui Q., Shuisheng J., Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication, IEEE J. Quantum Electron., 50 (3), 148-157, 2014.
9. Barakat M.L., Mansingka A.S., Radwan A.G., Salama K.N., Hardware stream cipher with controllable chaos generator for colour image encryption, IET Image Proc., 8 (1), 33-43, 2014.
10. Anees A., Siddiqui A.M., Ahmed F., Chaotic substitution for highly auto correlated data in encryption algorithm, Commun. Nonlinear Sci. Numer. Simul., 19 (9), 3106-3118, 2014.
11. Ji Y., Zhang M., Wang Y., Wu Y., Zhang Y., Microwave-photonic sensor for remote water-level monitoring based on chaotic laser, Int. J. Bifurcation Chaos, 24 (3), 321-327, 2014.
12. Zheng G.W., Peng S., Hongye S., Jian C., Sampled-data fuzzy control of chaotic systems based on a T–S fuzzy model, IEEE Transaction on Fuzzy Systems, 22 (1), 153-163, 2014.
13. Yu S.H., Kang H.S., Kim Y.T., Hyun C.H., Park M., Fuzzy adaptive modular design of uncertain chaotic duffing oscillators, International Journal of Control Automation and Systems, 12 (1), 188-194, 2014.
14. Deivasundari P., Uma G., Ashita S., Chaotic dynamics of a zero average dynamics controlled DC-DC Cuk converter, IET Power Electron., 7 (2), 289-298, 2014.
15. Wan L., Luo X.S., Zeng S.Y., Zhang B., Global exponential stabilization for chaotic brushless DC motors with a single input, Nonlinear Dyn., 77, 209-212, 2014.
16. Pomares J., Perea I., Torres F., Dynamic visual servoing with chaos control for redundant robots, IEEE/ASME Trans. Mechatron., 19 (2), 423-431, 2014.
17. Jakimoski G., Kocarev L., Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps, IEEE Trans. Circuits Syst. I: Fundamental Theory and Applications, 48 (2), 163-169, 2001.
18. Çavuşoğlu Ü., Akgül A., Kaçar S., Pehlivan İ., Zengin A., A novel chaos-based encryption algorithm over TCP data packet for secure communication, Security Comm. Networks, 9 (22), 1285-1296, 2016.
19. Keyman E., Yıldırım M., Kriptolojiye Giriş Ders notları, Uygulamalı Matematik Enstitüsü**,** Kriptorafi Bölümü-ODTÜ, Türkiye, 2004.
20. Atar E., Ersoy O.K., Özyılmaz L., Hybrid data compression and optical cryptography with orthogonal matching pursuit, Journal of the Faculty of Engineering and Architecture of Gazi University, 32 (1), 131-139, 2017.
21. Çavuşoğlu Ü., Kaçar S., Pehlivan İ., Zengin A., Secure image encryption algorithm design using a novel chaos based S-Box, Chaos, Solitons Fractals, 95 (2017), 92-101, 2017.
22. Çavuşoğlu Ü., Zengin A., Pehlivan İ., Kaçar S., A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system, Nonlinear Dyn., 87, 1081-1094, 2017.
23. Avaroğlu E., Pseudorandom number generator based on Arnold cat map and statistical analysis, Turkish Journal of Electrical Engineering & Computer Sciences, 25, 633-643, 2017.
24. Ferguson N., Schneier B., Kohno T., Generating Randomness, Cryptography Engineering: Design Principles and Practical Applications, Wiley Publishing**,** Indianapolis, 137-141, 2010.
25. Zhong Z., Guanrong C., Simin Y., Hyperchaotic signal generation via DSP for efficient perturbations to liquid mixing, Int. J. Circuit Theory Appl., 37, 31-41, 2009.
26. Kharel R., Busawon K., Aggoune W., Ghassemloy Z., Implementation of a secure digital chaotic communication scheme on a DSP board, 7th International Symposium on Communication Systems

Networks and Digital Signal Process, Newcastle-England, 212-216, 21-23 July, 2010.
27. Te S., Guosheng R., Yang Z., Song Z., Design method for Duffing system based on DSP builder, IEEE International Conference on Industrial and Information Systems, Yantai-China, 121-124, 06-09 August, 2012.
28. Delgado R.M., Acosta A.J., Rodriguez V.A., A mixed-signal integrated circuit for FM-DCSK modulation, IEEE J. Solid-State Circuits, 40 (7), 1460-1471, 2005.
29. Güler U., Ergün S., A high speed fully digital IC random number generator, AEU Int. J. Electron. Commun., 66, 143-149 2012.
30. Kohlbrenner P., Gaj K., An Embedded True Random Number Generator for FPGAs, SIGDA 12th international symposium on Field programmable gate arrays, New York-USA, 71-78, 22-24 February, 2004.
31. Yiwei Z., Zexiang L., Xinjian Z., A chaos-based image encryption ASIC using reconfigurable logic, IEEE Asia Pacific Conference on Circuits and Systems, Macao-China, 1782-1785, 30-3 December, 2008.
32. Koyuncu İ., Design and Implementation of High Speed Artificial Neural Network Based Sprott 94-S System on FPGA, International Journal of Intelligent Systems and Applications in Engineering, 4 (2), 33-39, 2016.
33. Xiang F., Chen X., A Method to Generate Chaotic Attractors Based on FPGA, Applied Mechanics and Materials, 66 (68), 1301-1304, 2011.
34. Koyuncu İ., Özcerit A.T., Pehlivan İ., FPGA-Based A Chaotic Oscillator Design and Implementation, Nonlinear Dyn, 77 (2), 49-59, 2014.
35. Alçın M., Pehlivan İ., Koyuncu İ., Hardware design and implementation of a novel ANN-based chaotic generator in FPGA, Optik, 127 (2016), 5500-5505, 2016.
36. Tuna M., Koyuncu İ., Fidan C.B., Pehlivan İ., Real Time İmplementation of a novel Chaotic Generator on FPGA, IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı, Malatya-Türkiye, 604-607, 16-19 Mayıs, 2015.
37. Koyuncu I., Özcerit A.T., Pehlivan I., Implementation of FPGA-based real time novel chaotic oscillator, Nonlinear Dyn., 75 (2), 49-59, 2014.
38. Azzaz M.S., Taugast C., Sadoudi S., Fellah R., Dandache A., A new auto-switched chaotic system and its FPGA implementation, Commun. Nonlinear Sci. Numer. Simul., 18 (7), 1792-1804, 2013.
39. Merah L., Pascha A., Said A., Mamat N.H., Design and FPGA implementation of Lorenz chaotic system for information security issues, Application Mathematics Sciences, 7 (5), 237-246, 2013.
40. Koyuncu İ., Özcerit A.T., Pehlivan İ., An analog circuit design and FPGA-based implementation of the Burke-Shaw chaotic system, Optoelectron. Adv. Mater. Rapid Commun., 7, 635-638, 2013.
41. De micco L., Larrondo H.A., FPGA implementation of a chaotic oscillator using RK4 method, IEEE VII Southern Conferences on Programmable Logic, Cordoba-Spain, 185-190, 13-15 April, 2011.
42. Sadoudi S., Mohamed S.A., Mustapha D., Mustapha B., An FPGA real-time implementation of the Chen's chaotic system for securing chaotic communications, International Journal of nonlinear Science, 7 (4), 467-474, 2009.
43. Eroğlu C., Implementation of synchronized chaotic systems by FPGA, Master Tezi, İzmir Yüksek Teknoloji Enstitüsü, İzmir, 2007.
44. Tlelo-Cuautle E., Pa-Azucena A.D., Rangel-Magdale J.J., Carbajal-Gomez V.H., Rodriguez-Gomez G., Generating a 50-scroll chaotic attractor at 66 MHz by using FPGAs, Nonlinear Dyn, 85 (4), 1-15, 2016.
45. Xingyuan W., Xue Q., Lin T., A novel True Random Number Generator Based on Mouse Movement and a One-Dimensional Chaotic Map, Mathematical Problems in Engineering, 2012, 1-9, 2012.
46. Stipčević M., Quantum random number generators and their use in cryptography, IEEE 34th International Convention of Proceedings, Opatija-Croatia, 1474-1479, 23-27 May, 2011.
47. Danger J.L., Guilley S., Hoogvorst P., High speed true random number generator based on open loop structures in FPGAs, Microelectron. J., 40 (11), 1650-1656, 2009.
48. Zidan M.A., Radwan A.G., Salama K.N., Random number generation based on digital differential chaos, IEEE 54th International Midwest Symposium on Circuits and Systems, Seoul-South Korea, 1-4, 7-10 August, 2011.
49. Tavas V., Demirkol A.S., Ozoguz S., Kilinc S., Toker A., Zeki A., An IC Random Number Generator Based on Chaos, International Conference on Applied Electronics, Pilsen-Czech Republic, 1-4, 8-9 September, 2010.
50. Jessa M., Jaworski M., Randomness of a Combined TRNG Based on the Ring Oscillator Sampling Method, The İnternational Conference on Signals and Electronic Systems, Poznan-Poland, 323-326, 7-10 September 2010.
51. Wold K., Petrovic S., Optimizing Speed of a True Random Number Generator in FPGA by Spectral Analysis, IEEE Fourth International Conference on Computer Sciences and Convergence Information Techlogy, Seoul-South Korea, 1105-1110, 24-26 September, 2009.
52. Istvan H., Suciu A., Cret O., FPGA based TRNG using automatic calibration, IEEE 5th Conferences on Intelligent Computer Communication and Processing, Cluj-Napoca, 373-376, 27-29 August, 2009.
53. Ergun S., Özoğuz S., A Chaos-Modulated Dual Oscillator-Based Truly Random Number Generator, IEEE International Symposium on Circuits and Systems, New Orleans-USA, 2482-2485, 27-30 May, 2007.
54. Stojavski T., Kocarev L., Chaos-Based Random Number Generators—Part I: Analysis, IEEE Trans. Circuits Syst. I Regul. Pap., 48 (3), 281-288, 2001.
55. Stojavski T., Pihl J., Kocarev L., Chaos-Based Random Number Generators-Part II: Practical Realization, IEEE Trans. Circuits Syst. I Regul. Pap., 48 (3), 382-385, 2001.
56. Yardım F.E., Afacan E., Simulation of A Communication System Using Lorenz Based

Differential Chaos Shift Keying (DCSK) Model, Journal of the Faculty of Engineering and Architecture of Gazi University, 25 (1), 101-110, 2010.

57. Pehlivan İ., Uyaroğlu Y., Chaotic Circuit Design and Analyze of A New Chaotic Attractor, 6th International Advanced Techlogy Symposium, Elazığ-Turkey, 351-355, 16-18 Mayıs, 2011.

58. Tuna M., Fidan C.B., Electronic circuit design, implementation and FPGA-based realization of a new 3D chaotic system with single equilibrium point, Optik, 127 (24), 11786-11799, 2016.

59. Piper J.R., Sprott J.C., Simple Automous Chaotic Circuits, IEEE Trans. Circuits Syst. II Express Briefs, 57 (9), 730-734, 2010.

60. Sprott J.C., Simple chaotic systems and circuits, American Journal Physics, 68 (8), 758-763, 2000.

61. Çavuşoğlu Ü., Uyaroğlu Y., Pehlivan İ., Design of A Continuous Time Autonomous Chaotic Circuit and Application of Signal Masking, Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (1), 79-87, 2014.

62. Holmes P.J., Poincare celestial mechanics, dynamical-systems theory and chaos, Phys. Rep., 193 (3), 138-163, 1990.

63. Lorenz E.N., Deterministic non-periodical flow, Journal Atmospheric Sciences, 20, 130-141, 1963.

64. Li T., Yorke J., Period three implies chaos, American Mathematical Monthly, 82, 985-992, 1975.

65. Rössler O.E., An equation for continuous chaos, Physics Letters, 57 (5), 397−398, 1976.

66. Matsumoto T., Chua L.O., Tanama S., Simplest chaotic automous circuit, Physical Review, 30, 1155−1157, 1984.

67. Matsumoto T., A chaotic attractor from Chua's circuit, IEEE Trans. Circuits Syst., 31 (12), 1055–1058, 1984.

68. Merah L., Pacha A.A., Said N.H., Mamat M., A Pseudo Random Number Generator Based on the Chaotic System of Chua's Circuit and its Real Time FPGA Implementation, Applied Mathematical Sciences, 7 (55), 2719-2734, 2013.

69. Yamaçlı V., Abacı K., Köse E., Chua Devresinin Gerçeklenmesi ve Simülasyonu, 6th International Advanced Techlogies Symposium, Elazığ-Türkiye, 82-86, 16-18 Mayıs, 2011.

70. Jesus M., Simulation of Chua's Circuit by Automatic Control of Step-Size, Appl. Math. Comput., 190, 1526-1533, 2007.

71. Razminia A., Sadrnia M.A., Chua's Circuit Regulation Using a nonlinear Adaptive Feedback Technique, International Journal of Electrical, Robotics, Electronics and Communications Engineering, 1 (10), 1508-1512, 2007.

72. Kiliç R., Autonomous Chua's Circuit: Classical and New Design Aspects, A Practical Guide For Studying Chua's Circuits, World Scientific Publishing Nonlinear Science, Singapore, USA, 1-6, 2010.

73. MuraliI K., Lakshmanan M., Chua L.O., Controlling and Synchronization of Chaos in The Simplest Dissipative n-automous Circuit, Int. J. Bifurcation Chaos, 5, 563-571, 1995.

74. Ameer L.F.A., Implementation of Digital Chaotic Signal Generator Based on Reconfigurable LFSRs for Multiple Access Communications, Aust. J. Basic Appl. Sci., 4 (7), 1691-1698, 2010.

75. Milani M.M.R.A, Pehlivan H., Pour S.H., Kaos Tabanlı Bir Şifreleme Yöntemi ve Analizi, XIII. Akademik Bilişim Konferansı Bildirileri, Malatya-Türkiye, 487-493, 2-4 Şubat, 2011.

76. Cicek I., Pusane A.E., Dundar G., Random number generation using field programmable analog array implementation of logistic map, 21st Signal Processing and Communications Applications Conference (SIU), Girne-Cyprus, 1-4, 24-26 April, 2013.

77. Juncu V.D., Rafiei-Naeini M., Dudek P., Integrated Circuit Implementation of a Compact Discrete-Time Chaos Generator, Journal Analog Integrated Circuits and Signal Processing, 46 (3), 275-280, 2006.

78. Özdemir, K., Sürekli-Zamanli Kaos ile Rastgele Sayi Üreteci Tasarımı, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2008.

79. Lakshmanan M., MuraIi K., Chaos in nonlinear Oscillators, Control and Synchronization, World Scientific, 1996.

80. Chua L., Wu W., Huang A., Zhong G., A Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos, IEEE Trans. Circuits Syst. I Regul. Pap., 40, 732-744, 1993.

81. Akgul A., Hussain S., Pehlivan İ., A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications, Optik, 127 (2016), 7062-7071, 2016.

82. Li J., Liu F., Guan Z.H., Li T., A new chaotic Hopfield neural network and its synthesis via parameter switching's, Elsevier Neurocomputing, 11, 33-39, 2013.

83. Akgul A., Pehlivan İ., A new three-dimensional chaotic system without equilibrium points, its dynamical analyses and electronic circuit application, Technical Gazette, 23 (1), 209–214, 2016.

84. Pehlivan İ., Yeni Kaotik Sistemler: Elektronik Devre Gerçeklemeleri, Senkronizasyon ve Güvenli Haberleşme Uygulamaları, Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, 2007.

85. Liu C., A novel chaotic attractor, Chaos, Solitons Fractals, 39, 1037-1045, 2009.

86. Zhou P., Huang K., A new 4-D n-equilibrium fractional-order chaotic system and its circuit implementation, Commun. Nonlinear Sci. Numer. Simul., 19 (2014), 2005-2011, 2014.

87. Yu F., Wang C., A novel Three Dimension Automous Chaotic System with a Quadratic Exponential nonlinear Term, Engineering, Techlogy & Applied Science Research, 2 (2), 209-215, 2012.

88. Ahmed I., Mu C., Zhang F., A New Chaotic Attractor with Quadratic Exponential nonlinear Term from Chen's Attractor, International Journal of Analysis and Applications, 5 (1), 27-32, 2014.

89. Kaçar S., Analog circuit and microcontroller based RNG application of a new easy realizable 4D chaotic system, Optik, 127 (2016), 9551-9561, 2016.

90. Tuna M., Fidan C.B., Koyuncu İ., Pehlivan İ., Real Time Hardware Implementation of the 3D Chaotic Oscillator which having Golden-Section Equilibra, IEEE Sinyal İşleme ve İletişim Uygulamaları Kurultayı, Zonguldak-Türkiye, 1309-1312, 16-19 Mayıs, 2016.

91. Leng J., Cao Y., Zhao K., Dynamics Analysis of Hyperchaotic Circuit, Applied Physics Frontier, 2 (2), 8-11, 2014.

92. Akgul A., Moroz I., Pehlivan İ., Vaidyanathan S., A new four-scroll chaotic attractor and its engineering applications, Optik, 127 (2016), 5491-5499, 2016.

93. Abooee A., Yaghini-Bonabi H.A., Jahed-Motlagh M.R., Analysis and circuitry realization of a novel three-dimensional chaotic system, Commun. Nonlinear Sci. Numer. Simul., 18, 1235-1245, 2013.

94. Deng K., Yu S., Estimating ultimate bound and finding topological horseshoe for a new chaotic system, Optics, 125 (20), 1-5, 2014.

95. Çiçek S., Ferikoğlu A., Pehlivan İ., A new 3D chaotic system: Dynamical analysis, electronic Circuit design, active control synchronization and chaotic masking communication application, Optik, 127 (2016), 4024-4030, 2016.

96. Pehlivan İ., Uyaroğlu Y., A new 3D chaotic system with golden proportion equilibra: Analysis and electronic circuit realization, Comput. Electr. Eng., 38, 1777-1784, 2012.

97. Ahadpour S., Sadra Y., Fard Z.A., A novel Chaotic Encryption Scheme based on Pseudorandom Bit Padding, International Journal of Computer Science Issues, 9 (1), 449-456, 2012.

98. Kocarev L., Jakimoski G., Pseudorandom bits generated by chaotic maps, IEEE Circuits and Systems I: Fundamental Theory and Applications, 50 (1), 123-126, 2003.

99. Cret O., Gyorfi T., Suciu A., Implementing True Random Number Generators Based on High Fault Nets, Romanian Journal Of Information Science And Techlogy, 15 (3), 277-298, 2012.

100. Drutarovsky M., Simka M., A Simple PLL-Based True Random Number Generator for Embedded Digital Systems, Computing and Informatics, 23, 501-515, 2004.

101. Yalcin M.E., Suykens J.A.K., Vandewalle J., True random bit generation from a double-scroll attractor, IEEE Trans. Circuits Syst. I Regul. Pap., 51 (7), 1395-1404, 2004.

102. Cicek I., Pusane A.E., Dundar G., A novel design method for discrete time chaos based true random number generators, Integration the VLSI journal, 47 (1), 38–47, 2014.

103. Avaroğlu E., Türk M., Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki etkisinin İncelenmesi, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara-Türkiye, 291-294, 20-21 Eylül, 2013.

104. Özdemir K., Kılınç S., Özoğuz S., Sürekli-Zamanlı Kaos ile Rastgele Sayı Üreteci Tasarımı, IEEE 16th Signal Processing Communication and Applications Conference, Aydın-Türkiye, 1-4, 20-22 April, 2008.

105. Zhun H., Hongyi C., A Truly Number Generator Based on Thermal, IEEE Asicon, Shanghai-Chine, 862-864, 23-25 October, 2001.

106. Bucci M., Luzzi R., A Fully-Digital Chaos-Based Random Bit Generator, Lect. Notes Comput. Sci., 9100, 396-414, 2016.

107. Demirkol A.Ş., Kaotik Osilatör Girişli ADC Tabanlı Rastgele Sayı Üreteci, Master Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2007.

108. Tavas V., Tümleştirmeye Uygun Rastgele Sayı Üreteçleri, Doktora Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2011.

109. Tavas V., Demirkol A.S., Ozoguz S., Zeki A., Toker A., Integrated cross-coupled chaos oscillator applied to random number generation, IET Circuits Devices Syst, 3 (1), 1-11, 2009.

110. Demirkol A.Ş., Tavas V., Özoğuz S., Toker A., High frequency chaos oscillators with applications, IEEE 18th European Conference on Circuit Theory and Design, Seville-Spain, 1026-1029, 27-30 August, 2007.

111. Koyuncu İ., Kriptolojik Uygulamalar için FPGA tabanlı Yeni Kaotik Osilatörlerin ve Gerçek Rasgele Sayı Üreteçlerinin Tasarımı ve Gerçeklenmesi, Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, 2014.

112. Güven P., Otonom Olmayan Kaotik Sistemlerde Rasgele Sayı Üretiminin İncelenmesi, Master Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 2006.

113. Ergün S., Özoguz S., Truly random number generators based on an n-automous chaotic oscillator, AEU Int. J. Electron. Commun., 61, 235-242, 2007.

114. Cicek I., Pusane A.E., Dundar G., A new dual entropy core true random number generator, Analog Integration Circuit Signal Process, 81 (1), 61-70, 2014.

115. Ning L., Ding J., Chuang B., Xuecheng Z., Design and validation of high speed true random number Generators based on prime-length ring oscillators, The Journal of China Universities of Posts and Telecommunications, 22 (4), 1-6, 2015.

116. Pareschi F., Setti G., Rovatti R., Implementation and testing of high-speed CMOS TRNGs sased on chaotic systems, IEEE Trans. Circuits Syst. I Regul. Pap., 57 (12), 3124−3137, 2010.

117. Dhanuskodi S.N., Vijayakumar A., Kundu S., A Chaotic Ring Oscillator based Random Number Generator, IEEE International Symposium on Hardware-Oriented Security and Trust, Arlington-USA, 160-165, 6-7 May, 2014.

118. Aguilar Angulo J.A., Kussener E., Barthelemy H., Duval B., Discrete Chaos Based Random Number Generator, IEEE Faible Tension Consommation, Novotel Monte-Carlo-Monaco, 1-4, 4-6 May 2014.

119. Park M., Rodgers J.C., Lathrop D.P., True random Number generation using CMOS Boolean chaotic Oscillator, Microelectron. J., 46 (2015), 1364-1370, 2015.

120. Schellekens D., Preneel B., Verbauwhede I., FPGA Vendor Agstic True Random Number Generator, International Conference on Field Programmable Logic and Applications, Madrid-Spain, 1-6, 28-30 August, 2006.

121. Dichtl, M., Golic, J., "High-speed TRNG with logic gates only", Lect. Notes Comput. Sci., 4727, 45-62, 2007.

122. Fischer V., Drutavosky M., Simka M., Bochard N., High performance TRNG in Altera stratix FPLDs, Field Programmable Logic and Application, 3203, 555–564, 2004.

123. Wıeczorek P.Z., Golofit K., Dual-metastability time-competitive TRNG, IEEE Trans. Circuits Syst. I Regul. Pap., 61 (1), 134−145, 2014.

124. Lozach F., Ben R.M., Graba T., Danger J.L., FPGA design of an open-loop TRNG, Euromicro Conferances on Digital Systems Design, Santander-Spain, 615-622, 4-6 September, 2013.

125. Wold K., Tan C.H., Analysis and Enhancement of Random Number Generator in FPGA Based on Oscillator Rings, International Journal of Reconfigurable Computing, 2009, 1-8, 2009.

126. Sunar B., Martin W.J., Stinson D.R., A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks, IEEE Trans. Comput., 56 (1), 109-119, 2007.

127. Tuncer T., Avaroğlu E., Türk M., Ozer A.B., Implementation of non-periodic Sampling True Random Number Generator on FPGA, Journal of Microelectronics, Electronic Components and Materials, 44 (4), 296-302, 2014.

128. Avaroğlu E., Tuncer T., Özer A.B., Ergen B., Türk M., A Novel chaos-based post-processing for TRNG, Nonlinear Dyn., 81, 189-199, 2015.

129. Avaroğlu E., Donanım Tabanlı Rasgele Sayı Üretecinin Gerçekleştirilmesi, Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, 2014.

130. Özkaynak F., Cryptographically secure random number generator with chaotic additional input, Nonlinear Dyn., 78, 2015-2020, 2014.

131. Avaroglu E., Tuncer T., Özer A.B., Türk, M., A new method for hybrid pseudo random number generator, J. Microelectron. Electron. Compon. Mater., 4 (4), 303-311, 2014.

132. Merah L., Ali-Pacha A., Said N.H., Mamat M., Pseudo Random Number generator Based on the Chaotic System of Chua's Circuit, and its Real Time FPGA Implementation, Applied Mathematical Sciences, 7 (55), 2719-2734, 2013.

133. Avaroğlu E., Koyuncu İ., Özer A.B., Türk M., Hybrid pseudo-random number generator for cryptographic systems, Nonlinear Dyn, 82, 239-248, 2015.

134. Zidan M.A., Radwan A.G., Salama K.N., Random number generation based on digital differential chaos, IEEE 54th International Midwest Symposium on Circuits and Systems, Seoul-South Korea, 1-4, 7-10 August, 2011.

135. Koyuncu İ., Özcerit A.T., Pehlivan İ., Avaroğlu E., Design and implementation of chaos based true random number generator on FPGA, IEEE Signal Processing and Communications Applications Conference, Trabzon-Turkey, 236-239, 23-25 Nisan, 2014.

136. Wang Q., Yu S., Li C., Lü J., Fang X., Guyeux C., Bahi J.M., Theoretical Design and FPGA-Based Implementation of Higher-Dimensional Digital Chaotic Systems, IEEE Trans. Circuits Syst. I Regul. Pap., 63 (3), 401-4012, 2016.

137. Fatemi-Behbahani E., Ansari-Aslı K., Farshidi E., A New Approach to Analysis and Design of Chaos-Based Random Number Generators Using Algorithmic Converter, Circuits Systems and Signal Processing, 35 (11), 3830-3846, 2016.

138. Wang Y., Li S., A High-Speed Digital True Random Number Generator Based on Cross Ring Oscillator, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E99-A (4), 806-818, 2016.

139. Koyuncu İ., Özcerit A.T., The design and realization of a new high speed FPGA-based chaotic true random number generator, Comput. Electr. Eng., 2016, 1-12, 2016.