İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

SÜREKLİ-ZAMANLI KAOS İLE RASTGELE SAYI ÜRETECİ TASARIMI

YÜKSEK LİSANS TEZİ

Müh. Koray ÖZDEMİR

Anabilim Dalı : ELEKTRONİK VE HABERLEŞME MÜHENDİSLİĞİ

Programı : ELEKTRONİK MÜHENDİSLİĞİ

HAZİRAN 2008

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

SÜREKLİ-ZAMANLI KAOS İLE RASTGELE SAYI ÜRETECİ TASARIMI

YÜKSEK LİSANS TEZİ

Müh. Koray ÖZDEMİR

(504061217)

Tezin Enstitüye Verildiği Tarih : 5 Mayıs 2008

Tezin Savunulduğu Tarih : 9 Haziran 2008

Tez Danışmanı : Doç. Dr. Serdar ÖZOĞUZ

Diğer Jüri Üyeleri Prof.Dr. Ece Olcay GÜNEŞ (İ.T.Ü.)

Prof. Dr. Herman SEDEF (Y.T.Ü.)

HAZİRAN 2008

ÖNSÖZ

Bu çalışmada benden değerli yardımlarını esirgemeyen tez danışmanım değerli hocam Doç. Dr. Serdar ÖZOĞUZ ve bu çalışmam aşamasında bana destek olan Yrd. Doç. Dr. Selçuk KILINÇ, Yük. Müh. Vedat TAVAS ve Yük. Müh. Ahmet Şamil DEMİRKOL' a teşekkürlerimi borç bilirim.

En son ama en önemli olarak bütün yaşantım boyuca benden desteklerini ve sevgilerini esirgemeyen sevgili aileme teşekkür ederim.

Mayıs 2008 **Koray ÖZDEMİR**

İÇİNDEKİLER

KISALTMALAR

RSÜ : Rastgele Sayı Üreteci

DES : Data Encryption Standard

RSA : Rivest, Shamir, Adleman

NIST : National Institute of Standard and Technology

SRSÜ : Sözde Rastgele Sayı Üreteci

GRSÜ : Gerçek Rastgele Sayı Üreteci

LEM : Lineer Eşlenik Metodu

D/A : Dijital Analog Dönüştürücü

VDC : Volts Direct Current

MOS : Metal Oxide Semiconductor

VCO : Voltage Controlled Oscillator

FIPS : Federal Information Processing Standards Publication

TABLO LİSTESİ

Sayfa No

ŞEKİL LİSTESİ

Sayfa No

SEMBOL LİSTESİ

α,β,γ	: Normalizasyon Sabitleri
B	: Diyot Kırılma Noktası Gerilimi
Cox	: Birim Geçit Oksit Kapasitesi
E	: Gürültü Gerilimi
f	: Frekans
Φ	: Poker Testi Sonucu
φ	: Saat Fazı
σ	: Gauss Dağılışı
τ	: Zaman Sabiti
K'	: MOS Geçiş İletkenliği Parametresi
KF	: Kıpraşma Gürültüsü Katsayısı
L,W	: MOS Kanal Boyutları

SÜREKLİ-ZAMANLI KAOS İLE RASTGELE SAYI ÜRETECİ TASARIMI

ÖZET

Bu çalışmada, tümleşik yapıda sürekli-zamanlı bir kaotik işaret üreteci kullanarak yeni bir rastgele sayı üreteci tasarımı ve bu tasarımın nümerik analizlerinden bahsedilmektedir. Bu yapıyı gerçeklerken kaos ve rastgele sayı üreteci tanımları incelemiş ve bu bilgiler doğrultusunda tasarım gerçeklenmiştir.

Kaotik devrelerden elde edilen işaretlerin kendine özgü özellikleri incelendiğinde bu işaretlerin rastgele karakterde işaretler olduğu görülmüştür. Bu bilgiden yararlanarak birçok rastgele sayı üreteci yapısında entropi kaynağı olarak kullanılan gürültü işaretinin yerine kaotik işaretin kullanılması düşünülmüştür. Bu sayede rastgele sayı üreteci yapılarında gürültü işaretinin işlenmesi için gereken karmaşık ve zor işlemlere gerek kalmamıştır.

Kaotik işaretin kaynak olarak kullanılabileceği ve tümleşik devre tasarımına yatkın rastgele sayı üreteci yapıları araştırıldığında en uygun yapının literatürde iyi bilinen çift osilatör örnekleme yapısı olduğu belirlenmiştir. Bu yöntemde D-tipi flip-flopun girişine hızlı osilatör uygulanırken saat girişine seğirmeli yavaş osilatör bağlanır ve seğirmeli yavaş osilatörün yükselen kenarlarında hızlı osilatör örneklenir. Bu yapının çıkışındaki rastgelelik yavaş osilatördeki seğirmenin rastgeleliğiyle ile sağlanmaktadır. Genelde fiziksel gürültü ile gerçeklenen yüksek seğirmeli salınım, bu çalışmada kaotik işaret kullanılarak elde edilmiştir. Seğirmeli yavaş osilatörün gerçeklenmesi kaotik işaret bindirilmiş üçgen işaretin karşılaştırıcıdan geçmesi ile sağlanmıştır.

Rastgele sayı üreteci yapısı tasarlandıktan sonra bu yapının matematiksel modeli çıkarılarak bu yapının tasarım parametrelerine olan duyarlılığı ve optimum çalışma noktaları nümerik analiz edilmiştir. Nümerik analizden elde edilen sonuçlar kullanılarak yeni tasarlana rastgele sayı üreteci laboratuar ortamında ayrık elemanlarla tasarlanmış ve gerçekleştirilen devreden elde edilen bit dizisi NIST'in NIST–800–22 dokümanında yer alan rastgelelik testine tabi tutulmuştur. Ve test sonuçlarından, üretilen bit dizisinin herhangi bir rastgele olmayan davranış göstermediği anlaşılmaktadır. Böylece kaos tabanlı yapılarla kullanarak rastgele sayıların üretilebileceği gösterilmiştir.

RANDOM NUMBER GENERATOR DESIGN USING CONTINUOUS-TIME CHAOS

SUMMARY

In this work, the design of a new random number generator circuit using continuous-time chaos in integrated circuit structure and this structure's numerical analyzes are described. While this structure is realized, definition of chaos and random number generator are studied and according to these studies design is realized.

When the specific characters of signals required from chaotic circuits are researched, these signals are appeared as random characterized signals. Utilizing this information, instead of noise signals which are used as an entropy source for lots of random number generators' architecture, use of a chaotic signal is considered. So there will be no need complex and difficult operations for noise signal processes in the random number generator structures.

When the random number generator using chaotic signals as source and capable of integrated circuit design are investigated, the best structure in the literature is determined as dual oscillator sampling technique. In this method, fast oscillator is applied in D-type flip flop's data in while jittered slow oscillator is applied in clock and at the rising edges of jittered slow oscillator, fast oscillator are sampled. Randomness of this structure's output is realized by jitter's randomness of slow oscillator. Generally high jittered oscillation realized by physical noise, is determined by using chaotic signal in this study.

After random number generator's structure is designed, by extracting the mathematical model sensitivity of this structure's design parameters and optimum operating points are numerically analyzed. Using the results of numerical analyzes, new designed random number generator is realized in the laboratory with discrete components and bit sequence is generated from the realized circuit. The level of the randomness of the obtained bit sequence is tested by NIST–800–22. The results of the test confirmed that the generated bit sequences do not show any nonrandom behavior. So by using chaos based structures random numbers can be produced is shown.

1. GİRİŞ

1.1. Kaos

Kaos kısaca başlangıç ve giriş koşullarına aşırı duyarlı dinamik sistemler olarak tanımlanabilir. Kaotik sistemlerin başlangıç ve giriş koşullarına olan bu duyarlılığından ötürü bu değerlerde yapılacak ufak değişimler sistemin çıkışının çok farklı noktalara gitmesine neden olmaktadır. Bu davranıştan dolayı kaotik yapılar deterministik sistemler olsalar dahi ancak kısa bir süreliğine sistemin davranışı hesaplanabilmektedir. Daha sonraki iterasyonlarda ise kaotik sistemlerin davranışları önceden kestirilemez bir hal almaktadır. Bu yüzden kaotik sistemler rastgele davranıyormuş gibi gözükmektedir. Kaotik sistemlerin rastgele benzeri davranış sergilemeleri sayesinde yeni modelleme ve analiz teknikleri geliştirilmiştir. Bu gelişmeler sayesinde dinamik sistem kuramı zenginleşmiş anlaşılması zor olan bazı fiziki ve doğa olayları açıklanabilmiştir.

Kaos kavramı matematiksel olarak 1900'lerde incelenmeye başlanmış ilk ciddi ve bilimsel çalışma Edward Lorentz'in 1961'de hava tahmini yapmak için oluşturduğu matematiksel meteorolojik modelin sonuçları sayesinde elde edilmiştir. 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. Bu gelişmenin doğrultusunda kaos teorisi o zamana kadar çözülemeyen bir çok fiziksel ve matematiksel problemlerin çözülmesini sağlamıştır. Günümüzde kaos kavramı astronomi, biyofizik, biyoloji, fizik, jeoloji, kimya, matematik, meteoroloji, mühendislik, plazma, tıp hatta sosyal bilimlerde açıklanması zor olan olguların modellenmesi ve çözülmesinde kullanılmaktadır.

Koatik davranışın elektronik olarak modellenmesi ise ilk defa Leon O. Chua tarafından elektronik elemanlar ve devreler kullanarak 1983'te gerçeklenmiştir. Tasarımcısının adını almış olan bu otonom Chua devresi elektronik olarak

anlaşılması ve tasarlanması çok basit bir devredir. Bu özelliklerinden dolayı Chua devresi defalarca incelenmiş birçok uygulamada kullanılmış ve günümüz kaotik devre çalışmalarına ışık tutmuştur.

1.2. Rastgele Sayı Üreteçleri

Donanımsal (fiziksel) veya yazılımsal (sayısal) metotlar kullanarak çıkışında korelasyon bulunmayan ve istatistiksel olarak birbirinden bağımsız sayılar üreten sistemlere rastgele sayı üreteci (RSÜ) denir. Bu üreteçler, önceki veriler yardımıyla daha sonraki verilerin tahmin ve öngörülemeyeceği rastgelelik seviyesinde çıkış üretebilen yapılardır. Rastgele sayı üreteçleri bu özelliklerinden dolayı birçok değişik alanda kullanılmaktadır. Monte Carlo metodunun kullanıldığı uygulamalar, bilgisayar benzetimleri ve modellemeleri, sayısal analiz uygulamaları, istatistiksel analizler ve özellikler kriptografide rastgele sayı gereksinimleri bu üreteçler tarafından karşılanmaktadır.

RSÜ'leri kendi aralarında gerçek rastgele sayı üreteçleri (GRSÜ) ve sözde rastgele sayı üreteçleri (SRSÜ) olmak üzere ikiye ayrılır. Fiziksel kaynaklar ya da gürültü gibi doğal kaynaklar kullanılarak gerçeklenen yapılar GRSÜ'leri oluşturmaktadır. SRSÜ'ler ise deterministik bir algoritma kullanarak sadece bir periyotluk rastgele sayı üretebilen yapılardır. Yüksek güvenlik gerektiren şifreleme gibi işlemler için rastgelelik kalitesi yüksek ve uzun rastgele sayı üretebilen GRSÜ'ler kullanılırken, yüksek rastgelelik kalitesi gerektirmeyen bilgisayar benzetimi ve modelleme gerektiren yapılarda ise SRSÜ'lerin kullanımı yeterli olmaktadır.

1.3. Kriptografi

Kriptografi bilimi kısaca belli bazı algoritma ve şifreler kullanarak göndericinin yollayacağı açık mesajın şifrelemesi, alıcı ve gönderici arasındaki iletim ortamının güvenliğinin sağlanması, şifreli bir mesajın çözülmesi gibi konuları ele alır.

Kriptografi kökeni çok öncelere dayanan bir bilim dalıdır. Kriptografinin kullanıldığı ilk çalışmalar eski Yunan dönemlerine kadar dayanmaktadır. Tarihteki ilk şifreleme örneği ise eski Yunan imparatoru Julius Caesar'ın askerlerine gizli mesaj göndermek için mesajdaki harflerin 3 sonraki harfler ile değiştirilmesiyle oluşturduğu gizli

mesajlarıdır. Modern zamana kadar ilerleyen ve gelişen şifreleme bilimi günümüzde ise simetrik ve asimetrik kripto sistemler olarak ikiye ayrılmaktadır.

1.4. Tezde İzlenen Yol

Bu tezin amacı, sürekli zaman kaotik osilatör girişli yeni bir gerçek rastgele sayı üreteci tasarımı ve tasarımının nümerik analizler kullanarak optimum değerlerinin ve çalışma sınırlarının belirlenmesidir.

İkinci bölümde kriptografi hakkında bilgi verilip günümüzdeki kripto yapıları anlatılırken bu bölümün sonunda rastgele sayı üreteçleri hakkında genel bir bilgi verilecektir.

Üçüncü bölümde kaos teorisi kuramsal ve matematiksel olarak incelenecek, elektronik olarak kaotik sistemlerin gerçeklenmesi de anlatılacaktır.

Dördüncü bölümde literatürde kullanılan tüm devre yapılı rastgele sayı üreteçleri tekniklerinden bahsedilecektir.

Beşinci bölümde kaotik osilatör tabanlı rastgele sayı üreteci yapısı, modellenmesi, bu modellerin nümerik sonuçları ve bu devreden üretilen rastgele sayıların istatistiksel test sonuçları incelenecektir.

Altıncı bölümde çalışmayla ilgili sonuçlara yer verilecek ve sonuçlarla ilgili yorum yapılacaktır.

2. KRİPTOGRAFİ

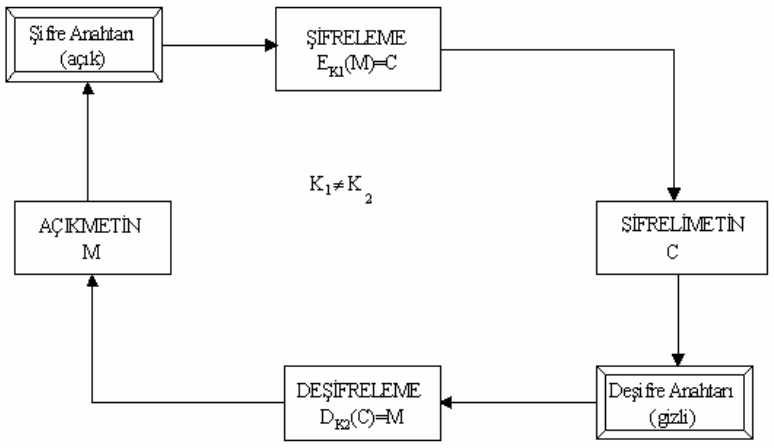
Kriptografi açık mesajı belli bir matematiksel veya donanımsal algoritma ve anahtar kullanarak şifreli mesaja çevirme, şifrelenmiş mesajı kırma, alıcı ve gönderici arasında güvenli iletimi sağlama gibi kavramları ele alan bir bilim dalıdır. Ancak kriptografi mantığına bakıldığında tam anlamıyla güvenli diyebileceğimiz bir algoritma, işlem, metot ya da şifre yoktur [1]. Bu yüzden ancak yüksek seviye ve güvenlikte bir şifreleme yapılması söz konusu olabilir.

Kriptografi metotlarına bakıldığında literatürde iki farklı metot söz konusudur. Bunlar simetrik ve asimetrik yapılardır. Simetrik yapılarda, gönderen açık mesajını gizli anahtarı (secret-key) kullanarak şifrelerken, şifrelenmiş mesajı alan kişi de aynı gizli anahtarı (secret-key) kullanarak şifrelenmiş mesajı çözer. Asimetrik yapılarda ise gönderen açık mesajını açık anahtar (public-key) kullanarak şifrelerken, mesajı alan ise farklı bir anahtar olan gizli anahtarla (private-key) şifreyi çözmektedir.

Modern anlamda kriptografinin kullanımına bakıldığında şifreleme ilk simetrik yapılar kullanarak gerçeklenmiştir. Bu yapılara en iyi örnek DES (Data Encryption Standard) algoritmasıdır. 1976 yılında asimetrik şifreleme metodunun bulunmasıyla şifreleme metoduna yeni bir boyut getirilmiştir. Asimetrik sistemlere en iyi örnek ise RSA (Rivest, Shamir, Adleman) olur [2].

Bu yapılara bakıldığında asimetrik yapıların algoritmalarının çözülme olasılığı simetrik yapılara göre daha zor olduğundan asimetrik yapıların güvenliği daha fazladır. Ancak bu özellikten dolayıdır ki asimetrik yapıların oluşturulması ve şifrelenmesi simetrik yapılara göre daha fazla zaman gerektirmektedir.

Şekil 2.1'e bakıldığında asimetrik ve simetrik yapıların genel bir akış diyagramı gözükmektedir. Eğer K_1 K_2'ye eşitse simetrik yapı eşit değilse asimetrik yapının tanımı yapılmış olur



Şekil 2.1: Asimetrik ve Simetrik Yapıların Genel Akış Diyagramı

2.1. Simetrik Kripto Sistemler

Gizli anahtarlı (simetrik) kripto sistemlerde şifreleme ve şifreyi çözme işlemleri için aynı anahtar kullanılmaktadır. Veriyi ileten ve alan da aynı anahtarı kullandığından bu anahtarların her iki tarafa da güvenli bir şekilde iletilmesi gerekmektedir. Bunun için bu anahtar verilerinin açık bir hattan değil de daha güvenli bir kanal üstünden aktarılması gerekmektedir. Bu noktada ise bir çelişki söz konusu olmaktadır eğer gizli anahtar güvenilir bir şekilde alıcıya gönderebiliyorsa simetrik kriptolama sisteminin bir anlamı kalmamaktadır. Bu sorunun üstesinden gelebilmek içinse güvenilir taşıyıcılar geliştirilmiştir [3].

Simetrik kriptolama sistemlerinde en yaygın kullanılan metot DES (Data Encryption Standard) metodudur. DES açık metni 64 bitlik bloklar halinde şifrelemekte kullanılan bir algoritmadır. Bu sistemlerde güvenlikler anahtarlar üzerinden gerçeklendiğinden güvenlik kullanılan anahtarın sayısına ve kalitesine göre değişmektedir. Ne kadar çok sayıda ve şifreleme kalitesi yüksek anahtarlar kullanılırsa, gönderilen mesajın güvenliği o kadar artmaktadır. DES metodu kısaca iki adet kombinasyon olan karıştırma ve dağılımdan meydana gelen bir çevrim bloğudur. DES algoritmalarında bu çevrim bloğu 16 kez tekrarlanarak şifrelenme sağlanmaktadır [4,5].

2.2. Asimetrik Kripto Sistemler

Açık anahtarlı şifreleme yönteminde şifrelemek için açık anahtar ve şifreyi çözmek için ise gizli anahtar olmak üzere iki ayrı anahtar kullanmaktadır. Farklı iki anahtarın kullanılması sayesinde güvenirlilik simetrik sistemlere göre daha başarılıdır.

Temelde açık anahtarlamalı şifrelemelerde alıcı açık-gizli anahtarları ve kullanılan algoritmayı tasarlar ve alıcının açık anahtarı ve kullanılan algoritmayı genel kullanımla paylaşır. Bu noktadan sonra mesajı iletmek isteyen kişi mesajı almak isteyen kişinin belirlediği açık anahtar ve algoritma ile kendi açık mesajını şifreledikten sonra mesajı gönderdiği hattın güvenirliliği söz konusu olmaksızın mesajı almak isteyen kişiye göndermektedir. Bu şifrelenmiş mesajı elinde gizli anahtarı ve algoritma tasarımını bulunduran alıcı ancak çözebilmektedir [6,7].

Günümüzde açık anahtarlama yönteminin en güzel örneği olarak RSA gösterilmektedir. Bu algoritma 1976 yılında Ron Rivest, Adi Shamir ve Leonard Adleman tarafından tasarlanmıştır. Bu metoda bakmak gerekirse:

1) P ve Q büyük değerli (1024 bit gibi) iki asal sayı olmalıdır.
2) 1<E<P*Q koşulunu ve (P-1)*(Q-1) ile aralarında asal olma koşulunu sağlayan bir E bulunmalıdır.
3) D*E = 1 (mod (P-1)*(Q-1)) koşulunu sağlayan bir D bulunmalıdır.

Bu değerler tasarlandıktan sonra gönderici tarafından C = (T^E) mod PQ işlemi ile T açık mesajı şifrelenmiş C mesajına çevrilmekte ve (C^D) mod PQ = T dönüşümü ile ise şifreli mesajı alıcı açık mesaja dönüştürmektedir. Bu işlemde E açık anahtar iken D gizli anahtar olarak kullanılır. Bu dönüşümü bir örnek ile göstermek gerekirse:

P = 61 - ilk asal sayı (P değeri E ve D tasarlandıktan sonra yok edilmeli)

Q = 53 - ikinci asal sayı (Q değeri E ve D tasarlandıktan sonra yok edilmeli)

P*Q = N =3233 - modül (paylaşıma açık)

E = 17 - açık anahtar (paylaşıma açık)

D = 2753 - gizli anahtar (sadece mesajı alan bilir)

T = açık mesaj

C = şifrelenmiş mesaj

şifrele(T) = (T^E) mod P*Q = C

çöz(C) = (C^D) mod P*Q = T

T=123 için;

şifrele(123) = (123^17) mod 3233

= 337587917446653715596592958817679803 mod 3233

= 855

çöz(855) = (855^2753) mod 3233

=123

Bu örnekte seçilen anahtar boyutları çok küçük olmasına rağmen çöz fonksiyonunda modüle edilmesi gereken sayı uzunluğu 8144 basamaklıdır. Böylece bu örnek RSA metodunun matematiksel olarak ne kadar güçlü olduğunu göstermektedir [8].

RSA sistemlerinde güvenlik kaliteli ve büyük P-Q asal sayıları üretimiyle sağlanmaktadır. Çarpanlarına ayırma işlemi zaman alan bir işlem olduğundan büyük bir sayının asal olup olmadığını anlamak çok fazla zaman almaktadır. Bu sayede büyük değerde P-Q asalları oluşturulabilirse N'nin de çarpanlarına ayrılması çok zor olacaktır. Böylece RSA sistemler çözülmesi çok zor ve zaman alan bir hale gelmektedir. N değeri oluşturulurken P ve Q asalları genelde büyük ve eş uzunlukta seçilir aksi takdirde asallardan biri küçük olursa N değerinin çarpanlarına ayrımı kolaylaşır [9].

Buradaki sıkıntı ise P ve Q olarak kullanılacak büyük asal sayıların nasıl üretileceğidir. Bu noktada asal sayı üretme kavramı devreye girer. Uygun büyüklükte rastgele bir sayı üretilmeli ve bu sayının asal olup olmadığı test edilmelidir. Bu testler sayesinde üretilen rastgele sayının kesinlikle asal olduğu ya da büyük olasılıkla asal olduğu belirlenebilmektedir.

Bir sayının %100 asal olduğunu belirleyen testler mevcuttur ama bu testler oldukça fazla zaman alan ve karmaşık testlerdir. Bu yüzden daha hızlı olan olasılıklı asal sayı testleri kullanılmaktadır ve bu testler %100 asaldır denemese de büyük olasılıkla asaldır denebilir ve bu testlerin hata olasılığı 2^{-100}'den azdır. RSA sistemleri için çok önemli olan büyük değerli asal sayı ya da büyük ve rastgele sayı ihtiyacı ise günümüzde RSÜ'ler tarafından karşılanmaktadır [9,10].

2.3. Rastgele Sayı Üreteci

Rastgele sayı üreteci, çıkışı rastgele sayılar olan sayısal veya fiziksel kaynaktan türetilmiş sistemlerdir. Rastgele sayı dizileri, istatistiksel olarak birbirinden bağımsız ve aralarında korelasyon bulunmayan sayılardan oluşur. Rastgele sayılar bu özelliklerinden dolayı birçok değişik alanda kullanılmaktadır. Karmaşık olguların modellenmesi ve benzetiminde, Monte Carlo metodunun kullanıldığı uygulamalarda, sayısal ve istatistiksel analiz uygulamalarında ve özellikle kriptografide (şifreleme) anahtar verisini oluşturmakta RSÜ'ler kullanılmaktadır [11,12].

Rastgele işlem kavramına bakarsak bu işlemlerin deterministik bir yapıya sahip olmadığı yani önceki çıkışlara bakarak daha sonraki çıkışların tahmin edilemeyeceği görülmektedir. Ancak RSÜ'lerin bir olasılık dağılımını takip ettiği söylenebilir. Bu yüzden RSÜ yapıların ürettiği sayı dizilerinin rastgeleliği rastgelelik testleri doğrultusunda kötü, iyi, çok iyi gibi dereceli olarak adlandırılmaktadır [13].

Rastgelelik uygulamalar arttıkça farklı rastgele veri üretime teknikleri oluşmuştur. Bu teknikler verinin ne kadar öngörülemez ve istatistiksel olarak rastgele üretilebileceğine göre değiştiği gibi ne kadar hızlı rasgele sayı ürettiğine de bağlı olarak çeşitlenmiştir. Bu doğrultuda RSÜ'leri kendi aralarında iki temel gruba ayırabiliriz: Sözde rastgele sayı üreteçleri (SRSÜ) ve gerçek rastgele sayı üreteçleri (GRSÜ).

2.3.1. Sözde Rastgele Sayı Üreteci

SRSÜ'ler belli bir algoritma, matematiksel formül ya da önceden hesaplanmış tablolar kullanarak rastgele gibi gözüken sayı dizileri oluşturan devrelerdir. SRSÜ'ler deterministik yapılardır ve sadece tek bir periyot boyunca rastgele davranışlı çıkışlar üretebilmektedir. Bir veya birkaç istatistiksel testten geçebilen SRSÜ dizileri oluşturulabilmesine rağmen SRSÜ'lerin birçoğu istatistiksel testlerden kalmakla beraber çok kolaylıkla da tahmin edilebilirdirler [14].

SRSÜ'lerine güzel bir örnek olarak lineer eşlenik metodu LEM (linear congruential generator (LCG))gösterilebilir [15].

$X_{n+1} = (a*X_n + c) \bmod m$

m modülo işlemiş 0<m,

a çarpma katsayısı $0 \leq a < m$,

c artan $0 < c < m$,

X_0 başlangıç koşulu, çekirdek $0 \leq X_0 < m$,

$a=5$, $c=1$, $m=7$ $X_0=2$ içi

sonuç 2, 3, 0, 1, 6, 7, 4, 5, 2, 3, 0, 1,…..

SRSÜ yapılarını özellikle kısa zamanda yüksek verimlilikle uzun boyutlu rastgele sayı üretimine ve aynı değerde anahtarlara ihtiyaç duyulduğunda kullanılmaktadır [16]. Ayrıca SRSÜ'ler kolay gerçeklenme ve düşük maliyetle üretilme gibi avantajlara da sahiptir. SRSÜ'lere bakıldığında sayıların periyodik olduğu görülmektedir bu özellik rastgeleliği etkilediğinden işlemler periyodu uzun olabilecek şekilde tasarlanmalıdır.

SRSÜ'nün bu özellikleri göz önüne alındığında bu teknik daha çok modelleme ve benzetim uygulamalarında kullanılmaktadır. Ancak SRSÜ uygulamalarında algoritma bilindiğin takdirde herhangi bir andaki değerine bakarak sonraki çıkışlar tahmin edilebileceğinden yüksek güvenlik, gizlilik ve öngörülememe gerektiren şifreleme işlemleri için ise yetersiz kalmaktadır [12].

2.3.2. Gerçek Rastgele Sayı Üreteci

SRSÜ'nün tersine GRSÜ'ler 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 rastgelelik 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 koşulları farklılıkları ve durum değişkenleri sapmaları sistemin öngörülemez bir hale gelmesini sağlamaktadır. GRSÜ'ler donanım ve yazılım tabanlı olmak üzere iki farklı teknikle gerçeklenebilirler [11,12]. GRSÜ yapımında kullanılan donanım bazlı mekanizmalara bakacak olursak:

1)Saçma gürültüsü: Elektronik devrelerdeki mekanik gürültüler olarak adlandırabilir. Örnek olarak foto diyota yansıtılan lambadaki fotonlar ele alındığında foto diyota ulaşan fotonların devrede oluşturduğu gürültü.

2)Nükleer bozulma radyasyonu: Sabit olmayan atom çekirdeklerinin elektromanyetik veya parçacık halinde radyasyon yaymasıyla oluşan enerji kaybı.

3)Termal gürültü: Direncin üstündeki ısıl değişimlerden dolayı oluşan elektriksek gürültüdür. Termal gürültünün karakteristiği beyaz gürültüye benzemekte ve bu özelliğinden dolayı rastgelelik uygulamalarında çok tercih edilmektedir.

4)Çığ gürültüsü: Zener diyodun ters kutuplandığı durumda bel verme noktasında oluşan gürültüdür.

5)Atmosferik gürültü: Doğal atmosferik olayların oluşturduğu radyo gürültüsüdür.

6)Diğer bir kaynak olarak da saat işaretinin sapması (osilatörün faz gürültüsü) gösterilebilir.

GRSÜ kaynaklarına baktığımızda bu kaynakların tamamıyle tahmin edilemez ve öngörülemez olduğu teorik olarak kabul edilmektedir. Ancak rasgele sayı kaynağının çalışması doğru gözüküyor gibi olsa da oluşturulan sayıların kutuplanmış olup olmadığı kontrol edilmelidir. Sıcaklıktaki değişimler, güç kaynağının gürültüsü, gövde etkileri, tasarlanan cihazın yaşı, manyetik ve diğer dış alan etkileri devrenin kutuplanmasına neden olabilmektedir. Bu koşullar tasarımcı tarafından giderilemediği takdirde oluşturulan sayı dizileri son-işleme (post-process) tabi tutularak rastgele sayının istatistiksel kalitesi arttırılmaktadır [12,14].

Yazılım tabanlı üreteçlerde ise mouse hareketleri arasındaki süreler, klavyeye basış zamanlaması gibi bilgisayar odaklı işletmeler entropi kaynağı olarak görev yapmaktadır. Ancak yazılım tabanlı RSÜ'leri gerçeklemek, donanım tabanlıları gerçeklemekten daha zahmetli dış ataklara daha açık ve daha az güvenilirdir.

3. KAOS

Kaos tanımı incelendiğinde başlangıç koşullarına üstel duyarlı, nonlineer, deterministik karakterli, uzun vadede periyodik olmayan dinamik sistemler olduğu görülmektedir [17,18]. Bu bilgiler doğrultusunda kaotik devrelerin yapısı hakkında bir taslak oluşturulabilir.

İlk olarak kaotik sistemler dinamik yapılardır yani zamana bağlı olarak değişim göstermektedir. İkinci olarak bu sistemler değişken ve aperiyodik yapılardır yani kendilerini tekrarlamazlar. Üçüncü olarak kaotik yapılar karmaşık yapılarmış gibi gözükse de aslında basit yapılardan meydana gelmektedir [19]. Dördüncü olarak bu sistemler nonlineer yapılardan oluşmaktadır. Son olarak kaotik sistemler deterministik yapılardır. Ama bu determinizm kavramı beraberinde bazı anlam kargaşalarını da beraberinde getirmektedir. Kaotik sistemler aperiyodik ve tahmin edilemez gibi gözükseler de deterministik kavramından dolayı bu sistemlerin rastgelelik gösterdiği söylenememektedir [20]. Yani kaotik sistemlerin bir andaki durumu tam olarak bilindiğinde, sonraki herhangi bir andaki durumu da tam olarak belirlenebilmelidir. Fakat kaotik sistemler kararsız ve giriş koşullarına üstel duyarlıdır böylece kaotik sistemler deterministik sistemler olmalarına rağmen bu özelliklerinden dolayı yapılacak perturbasyon sonuçları incelendiğinde sistemlerin rastgele davrandığı gözlenmektedir [21,22] .

Matematiksel olarak kaotik sistemler incelendiğinde bu sistemlerin başlıca özellikleri güç spektrumlarının gürültü spektrumlarına benzer bir yapıya sahip olması, Lyapunov üstellerinin pozitif değerler alması, otokorelasyon fonksiyonunun üstel olarak azalması ve Poincare kesit düzlemenin bir bölümünün tamamen ve düzensiz bir şekilde doldurması olarak görülmektedir [22].

Kaotik sistemler matematiksel modellemelerine göre ayrık zamanda kaotik sistemler ve sürekli zamanda kaotik sistemler olmak üzere ikiye ayrılır. Aynı şekilde kaotik sistemler gösterdikleri özelliklerden dolayı nonlineer farka dayalı sistemler ve

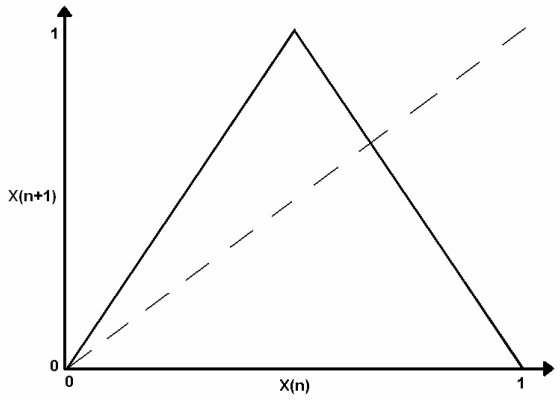
diferansiyel denkleme dayalı sistemler veya otonom ve otonom olmayan sistemler olarak ta gruplandırılabilir [23].

3.1. Ayrık Zamanda Kaos

Ayrık zamanda kaos, uygun bir f(x) nonlineer fonksiyonun iterasyonu sonucu oluşan genelde geri besleme özelliği gösteren kaotik özellikli dizilerin oluşturduğu bir sistemdir. Bu sistemlerin genel anlamda gösterimi Denklem 3.1'deki gibidir.

$$X_{n+1} = f(X_n) \quad \textbf{(3.1)}$$

Seçilen f(x) fonksiyonunun kaotik olması için, fonksiyonun başlangıç koşullarına yüksek duyarlılık göstermesi ve buna bağlı olarak x_n değerlerinin çok farklı değerlere gitmesi gerekmektedir. Ayrık zamanlı kaotik fonksiyonlara bakıldığında genelde bir boyutlu basit bir denklemle bu davranış sağlanabilmektedir. Bu fonksiyonlarda x_{n+1}, $f(x_n)$ değişkenlerinin kullanımıyla bir boyutlu haritalar oluşturulmakta ve bu fonksiyonlar geri besleme yapısına sahip olduğundan düzlemde V şeklinde bir form almaktadır [24]. Tent, lojistik, Bernoulli kaydırıcısı gibi fonksiyonlar bu davranışa sahip bazı kaotik haritalara örnektir.



Şekil 3.1: Tent Dönüşümü

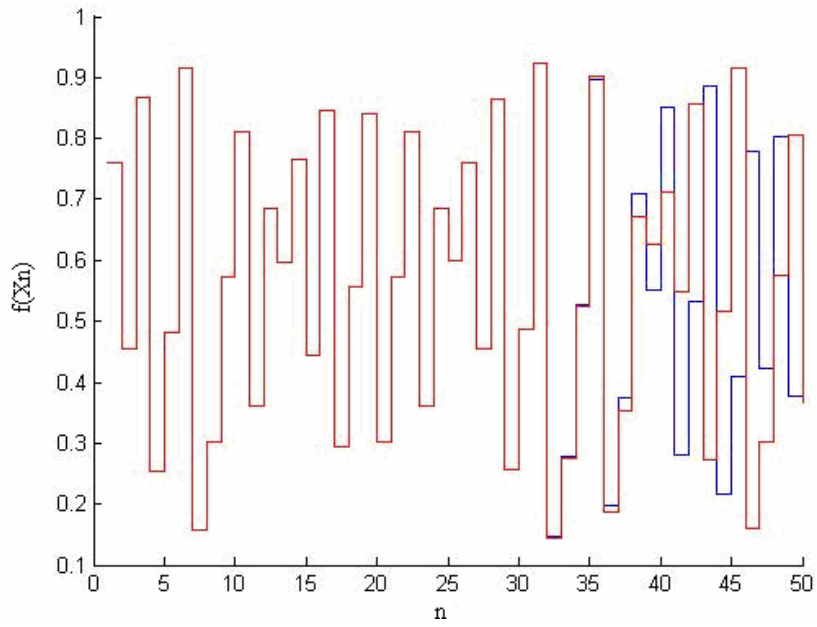
Ayrık kaotik dönüşümüne Denklem 3.2'de gösterilen ve literatürde çok iyi bilinen çadır dönüşümü örnek olarak verilebilir.

$$X_{n+1} = A*\min(X_n, 1- X_n) \quad \textbf{(3.2)}$$

Denklem 3.2'deki ifadeyi daha genel bir gösterim olan parça parça sürekli zaman fonksiyonuyla, Denklem 3.3'teki gibi de yazılabilir. Şekil 3.1'de de bu parçalı sürekli zaman dönüşüme ait grafik verilmiştir.

$$f(x)=\begin{cases}2x & 0\le x<0.5\\ 2-2x & 0.5\le x<1\end{cases},\ x_0\in[0,1) \qquad \textbf{(3.3)}$$

Bu koşullar altında Denklem 3.3'teki yapıyı başlangıç koşulu x_1=0.6 ve A=1.9 ayrıca ayrık kaotik yapıların duyarlılığını daha iyi gözlemleyebilmek için x_1=0.600000000001 seçilerek aynı iterasyon tekrardan uygulanmıştır. Bu koşullar altında $f(X_n)$ çıkış değeri, n iterasyon sayısı olmak üzere iki durum da Şekil3.2'deki gibi gösterilmektedir.



Şekil 3.2: Tent Dönüşümü Duyarlılığı

Denklem 3.3'deki dönüşümünde x_1=0.6 (mavi) ve x_1=0.600000000001(kırmızı) için iterasyonlar yapıldığında 32'ıncı iterasyondan sonra çıkış sonuçlarının değiştiği hesaplanmıştır. Bu örnekten de anlaşılacağı gibi ayrık zamanlı kaotik işaretler giriş değerlerine oldukça duyarlıdır.

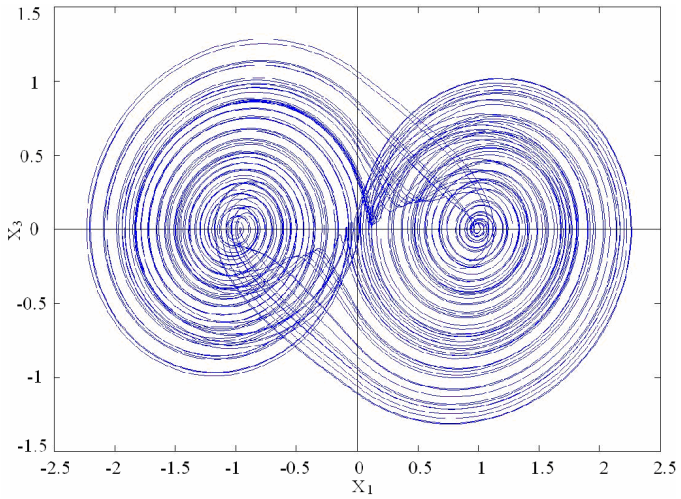
3.2. Sürekli Zamanda Kaos

Sürekli zaman kaotik yapılar, x(t) bir vektör olmak üzere $\frac{d(x(t))}{dt}=f(x(t))$ olacak şekilde adi diferansiyel denklemler ile ifade edilirler. Literatürdeki çalışmalar incelendiğinde kaotik bir sistem oluşturmak için basit yapıda üçüncü dereceden diferansiyel bir denklem takımı ve nonlineer bir yapı çoğu zaman yeterli olmaktadır [25]. Bilinen bir denklem takımıyla oluşturulan sistemin faz portresi çizdirilerek,

f(x)'in parametrelerine bağlı olarak kaotik davranışı detaylı olarak incelenebilir. Buna örnek olarak jerk sistemi Denklem 3.4'te verilmiştir.

$$\frac{d}{dt}\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -a & -a \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix} f(x_1), \quad f(x_1) = \begin{cases} 1 & x_1 \geq 0 \\ -1 & x_1 < 0 \end{cases} \tag{3.4}$$

Denklemde ayrıca değişken bir a parametresi vardır. Bu parametrenin değerini değiştirerek farklı faz portreleri elde etmek mümkündür. Jerk osilatörü için uygun a parametresi 0.5 ile 1 arasında yer almaktadır. Şekil 3.3'te örnek bir faz portresi normalize olarak verilmiştir.



Şekil 3.3: a=0.7 Değeri için Jerk Sistemi Çekici

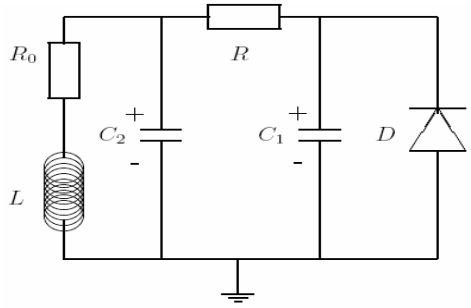
3.3. Elektronik Sistemlerde Kaos

Düzensiz, giriş koşullarına çok duyarlı, ufak farkların zamanla büyük farklılıklar getirmesi gibi rastgeleliği ve ön görülememeyi sağlayan özelliklere sahip olmalarından dolayı kaotik işaretler, son yıllarda elektronik sistemlerde gitgide yaygın kullanılmaya başlanmıştır [26].

Elektronik devre ile kaos olgusu ilk defa 1983'te Leon O. Chua tarafından gerçeklenmiştir. Chua iki direnç, iki kapasite bir endüktans ve bir adet diyot ile elektronik bir devrenin kaotik davranış gösterebilmesi için gerekli koşulları:

1) Bir ya da daha çok nonlineer eleman bulundurma
2) Bir ya da daha çok aktif direnç bulundurma
3) Üç ya da daha çok enerji tutabilen eleman bulundurma

gerçeklemiş ve basit bir nonlineer dinamik devre ile kaos elektronik olarak elde edilmiştir. Bu devre Şekil 3.4'te gösterilmektedir.



Şekil 3.4: Chua Devresi

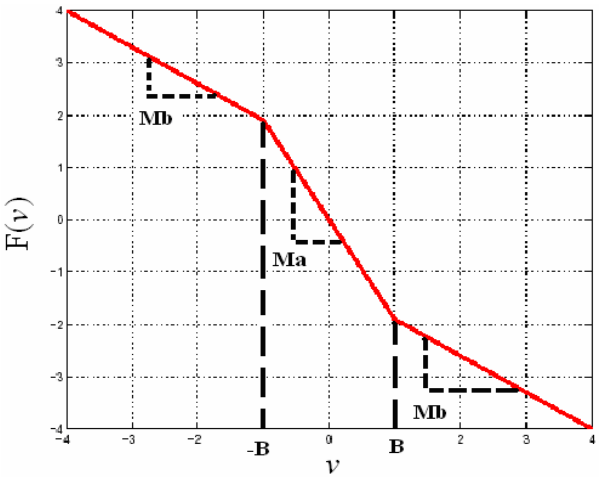
Kirchoff yasasına göre devrenin düğüm denklemleri çözüldüğünde:

$$C_1\dot{v}_{C1} = \frac{1}{R}(v_{C2} - v_{C1}) - F(v_{C1})$$
$$C_2\dot{v}_{C2} = \frac{1}{R}(v_{C1} - v_{C2}) + \imath_L \qquad \textbf{(3.5)}$$
$$Li_L = -Ro\imath_L + v_{C2}$$

Denklem 3.5'teki sonuç ortaya çıkacaktır. Nonlineer yapıyı oluşturan diyotun davranışı ise:

$$F(V) = m_b v + \tfrac{1}{2}(m_a - m_b)[|v + B| - |v - B|] \qquad \textbf{(3.6)}$$

olarak gösterilmektedir ki burada m_a ve m_b nonlineer yapının gerilim-akım karakteristiğinin eğimini gösterirken B ise kırılma noktasındaki gerilimi göstermektedir. Bu davranış karakteristiği Şekil3.5'te normalize olarak gösterilmektedir.



Şekil 3.5: Chua Devresi Diyot Karakteristiği

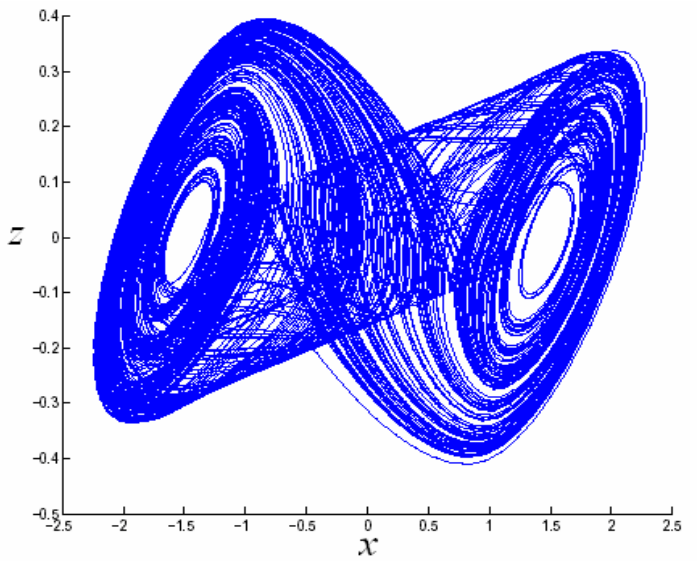
Tanım bağıntısını boyutsuz hale getirerek matematiksel olarak tanımlayabilmek için normalizasyona gerek duyulmaktadır bunun için;

$$x=\frac{V_1}{B} \quad y=\frac{V_2}{B} \quad z=\frac{R}{B}I \quad \alpha=\frac{C_2}{C_1} \quad \beta=\frac{R^2C_2}{L} \quad \gamma=\frac{RRoC_2}{L} \quad a=Rm_a \quad b=Rm_b \qquad \textbf{(3.7)}$$

olarak seçilir ve zaman sabiti $\tau=\frac{t}{RC_2}$ olarak seçilirse Chua devresinin diferansiyel denklemi

$$\begin{aligned}
&\dot{x}=\alpha(y-x-f(x))\\
&\dot{y}=x-y+z\\
&\dot{z}=-\beta y-\gamma z\\
&f(x)=bx+\frac{1}{2}(a-b)\left[|x+1|-|x-1|\right]
\end{aligned} \qquad \textbf{(3.8)}$$

olacaktır ve $\alpha\geq 0$, $\beta\geq 0$, $\gamma\geq 0$ ve $b < -1 < a < 0$ koşulu için devre kaosa girecektir [27]. Bu koşullar altında Chua devresinin faz eğrisi çıkarıldığında Şekil 3.6'daki davranış elde edilmektedir.



Şekil 3.6: Chua Devresi Faz Eğrisi

Kaosun elektronik yapılarda başlıca kullanım alanlarına bakıldığında öncelikle şifreleme ardından, analog işaret işleme, güç elektroniği, sayısal haberleşme ve gürültü işareti yerine kullanıldığı söylenebilir. Uygulama alanları daha detaylı incelendiğinde kaotik devreler sözde sinyal üreteçlerinin yerine sunulabilecek çok iyi bir alternatif olmaktadır. Ayrıca bu devreler konuşma işlemleri, dinamik davranışlı

elektronik devreler renkli ve beyaz gürültü işlemleri gerektiren yerlerde gürültü kaynağı olarak kullanılmaktadır. Diğer taraftan kaotik üreteçler analog sinyal uygulamalarında kıpırtı (dither) kaynağı olarak ta kullanılmaktadır ki bu sayede modülatörün taban gürültüsü beyazlatılmaktadır. Diğer bir uygulama alanı olan telemetre sistemlerinde ise periyodik olmayan kaos işareti zamanla çabuk değişen dekorelasyona sahip olması sayesinde yüksek çözünürlüklü radar sistemlerinin şifrelenmesinde kullanılmaktadır. Ve bütün bu kullanım alanlarıyla beraber kaotik işaretler en çok dijital haberleşmelerde gönderilen işaretin saklanmasında kullanılmaktadır [23].

Ayrık veya sürekli zamanda kaotik sistemler kullanılarak yukarıda belirtilen ihtiyaçları karşılayacak elektronik devreler tasarlanabilmektedir. Tez çalışması doğrultusunda incelemeler yapıldığında RSÜ'lerde kullanılmak üzere ilk olarak kaos, elektronik devrelerde ayrık kaotik yapılar kullanılarak gerçeklenmiştir. Bu yapılarda kaotik dönüşüm olarak uygun bir parça parça sürekli zaman yapısı seçilip bu dönüşüm aracılığıyla kaotik işaret üretilmiştir. Ancak ayrık kaotik fonksiyonların elektronik devrelerle oluşturulması karmaşık ve zor olmuştur. Ayrıca tasarlanan devrelerin saat ile kontrol edilme gereksiniminden dolayı bu yapıların hızları yetersiz kalmış ve bu yapının yerini alabilecek alternatif yöntemler aranmaya başlanmıştır.

Sürekli zamanda kaotik devrelerin kolay tasarlanabilmesi ve saat girişine gerek duymadan, çok yüksek hızda çalışabilmesi bu çalışmalar üstündeki ilgiyi arttırmıştır. Sürekli zamanda kaotik yapılar incelendiğinde temelinde bir osilatörün varlığı görülmektedir. Ana osilatör denklemine nonlineer özellik katan yeni elemanlar eklenerek yeni parametreler oluşturulmakta ve periyotları birbirinden farklı sonsuz harmonikler içeren sinüs osilatörü tabanlı kaotik osilatör elde edilmektedir. Bu devrelerdeki nonlineerlik ve çıkıştaki harmonik işaretlerin sayısı arttıkça işaret gürültüye benzemekte ve kaotik işaretin de kalitesi artmaktadır. Bu özellik, frekans spektrumu incelendiğinde de kolaylıkla saptanabilir.

4. TÜMDEVRE TASARIM ÖRNEKLERİ

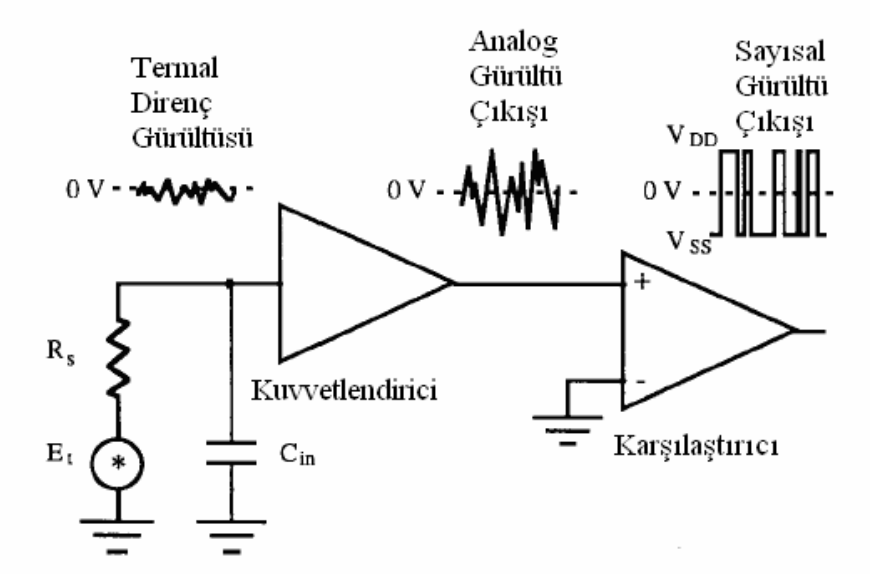
Birçok matematiksel algoritma, deterministik işlemler ve dijital devre kullanarak sözde rastgele sayı dizileri oluşturulmakta ve bu dizilere dayanan benzetim, devre testleri ve ölçümler yapılabilse de sözde rastgele kaynağı daha sıkı güvenlik ihtiyacı gerektiren veri şifreleme yapıları için yeterli olmamaktadır [28]. Çünkü sözde rastgele kaynakların çıkışındaki veri kökleri sabit bir entropiye sahip olmakta ve daha fazla geliştirilememektedir [29]. Ayrıca sözde rastgele yapılardan analog çıkış alabilmek içinde D/A (Dijital/Analog) çeviriciye ihtiyaç vardır. Buna karşın gerçek rastgele yapılar yüksek başarımda rastgeleliği basit yapılarla ve tümleşik olarak gerçekleyebilmektedir.

Günümüzde tümleşik rastgele sayı üreteçleri yapay sinir ağları, istatistiksel benzetim, dijital sistem uygulamalarında ve özellikle kriptografide kullanılmaktadır [30]. Ve tümleşik yapı sayesiyle daha kararlı çalışan, daha az güç tüketen ve daha az yer kaplayan devreler gerçeklenmek mümkündür.

Literatür incelendiğinde rastgele sayı üretimi için mevcut tümleşik devre örnekleri entropi kaynağına göre fiziksel gürültü kaynaklı ve kaos tabanlı olarak gruplandırılmıştır. Fiziksel gürültü kaynaklı tümleşik RSÜ yapılarına bakınca gürültünün doğrudan kuvvetlendirilmesi, çift osilatörlü yapı ve INTEL RSÜ elemanı gözükürken; kaos tabanlı yapılarda ayrık kaos tabanlı yapı ile sürekli zamanlı kaos tabanlı yapı gözükmektedir.

4.1. Gürültünün Doğrudan Kuvvetlendirilmesi

Bu metot tümleşik RSÜ teknikleri arasında en popüler olanıdır ve çalışma yöntemi Şekil 4.1'de yer almaktadır. Gürültünün doğrudan kuvvetlendirildiği yapılarda gürültü kaynağı olan ısıl ya da shot gürültüsünün küçük ac işaretleri yüksek kazançlı geniş bantlı bir kuvvetlendirici ile algılanabilir bir eşik seviyesine kadar kuvvetlendirilmektedir. Daha sonra kuvvetlendirilen gürültü işareti belirlenen bir referansla karşılaştırılıp rastgele '1' ve '0' bit dizisi çıkışı elde edilir [17].



Şekil 4.1: Gürültünün Doğrudan Kuvvetlendirilmesi Yöntemi

Tümdevre yapılar için uygun gürültü kaynağı arandığında çığ gürültüsünün elde edildiği zener diyotun 6VDC değerinin üstünde bir eşik gerilimine gerek duymasından ötürü gürültü kaynağı olarak kullanılmamaktadır. Diğer taraftan tümleşik olarak ısıl gürültüyü oluşturan ısıl direnç polisilikon veya difüzyon katlarının kullanımı ile kolaylıkla tasarlanabilmektedir [29] bu yüzden tümleşik yapılarda entropi kaynağı olarak direncin ısıl gürültüsünü kullanmak tasarımı daha kolaylaştırmaktadır. Fakat tümleşik olarak tasarlanan ısıl direncin rastgeleliğin elektromanyetik dalgalardan etkilenmesini engelleyebilmek için kaliteli bir kılıflandırılmaya ihtiyacı vardır [30].

Bu yapılarda rastgelelik başarımına bakıldığında beyaz gürültü kaynağı birim spektral gürültü yoğunluğuna sahip uygun bir Gauss dağılımı göstermektedir. Yani gürültü işareti kuvvetlendirildikten sonra bu işaretin ortalama değerinin altında ve üstünde bulunan değerlerin dağılıma olasılığı eşit olmaktadır. Bu sayede çıkıştan yüksek başarımda rastgelelik elde edilecektir [31].

İdealdeki davranışı böyle olması gerekirken gürültünün kuvvetlendirilmesi sonucu transistorlardan gelen 1/f gürültüsü kuvvetlendirilmiş beyaz gürültüye binmekte ve işaretin spektrum analizine bakıldığında 1/f gürültüsünün getirdiği kenar frekansı f_c , yaklaşık olarak 0Hz-100Hz aralığı, değerine kadar spektrum yoğunluğu birim özellik göstermemektedir.

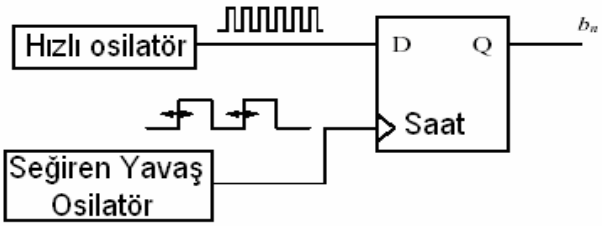
Bu yapıların tasarımındaki asıl zorluk kuvvetlendiricinin tasarımındadır. Kuvvetlendiricilerin yüksek kazançlı, geniş bantlı, düşük giriş kapasiteli ve çıkışında düşük 1/f gürültüsü üretmesi gereklidir. Bu sayede kuvvetlendirilecek gürültü beyaz gürültü özelliğini koruyabilecektir. Ancak kuvvetlendirici tasarımında bu dengeyi kurabilmek çok zordur. MOS yapılı kuvvetlendiricilerde 1/f gürültüsü MOS transistorun geçit alanının karekökü ile ters orantılıdır.

$$E_{ni}(1/f) = \sqrt{\frac{KF}{2fCoxWLK'}} \qquad \textbf{(4.1)}$$

Denklem 4.1'e göre 1/f gürültüsü azaltılmak istendiğinde MOS transistorun geçit alanı büyütülmek zorunda olduğundan kuvvetlendiricinin giriş kapasitesi büyüyecek ayrıca kuvvetlendiricini kazanç-bant genişliği çarpımı azalacaktır [29]. 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 yardımı ile süzülmekte ya da birim güç spektrumu seviyesine kadar bastırılmaktadır. Bu gereksinim de devrenin tasarım yükünü arttırmaktadır.

4.2. Çift Osilatör Yapısı

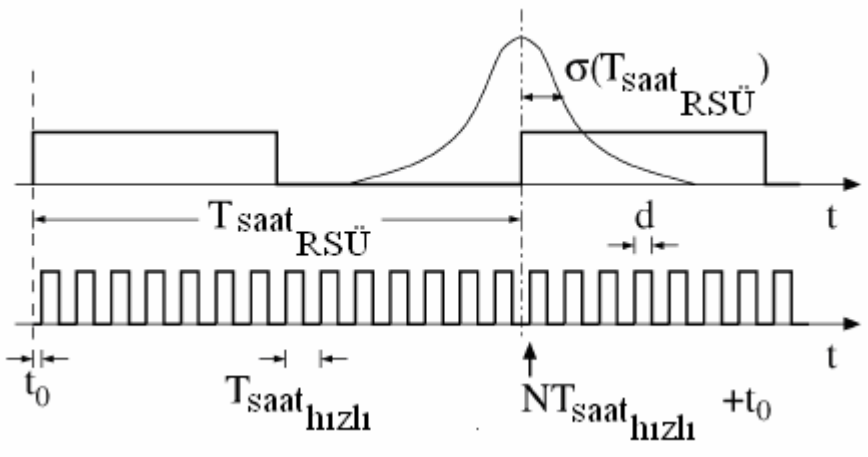
Çift osilatörlü yapıda rastgelelik serbest çalışan yavaş osilatörün faz gürültüsü sayesinde elde edilmektedir. Bu yöntemde hızlı osilatör D tipi flip flopun işaret girişine uygulanırken faz gürültüsüne sahip yavaş osilatör D tipi flip flopun saat girişine uygulanmakta ve faz gürültüsünün rastgeleliği sayesinde hızlı osilatör rastgele örneklenebilmektedir. Çift osilatörlü yapıdaki rastgelelik için hızlı ve yavaş osilatörün oranları uygun seçilmelidir [17].



Şekil 4.2: Çift Osilatör Yapısı

Bazı durumlarda yavaş osilatörün çıkışının seğirmesi yeterli rastgele dağılımı gösterememekte, gürültü kaynaklı ya da gerilim kontrollü osilatörler kullanılarak

seğirme seviyesi arttırılmaktadır. Şekil 4.2'de en temel uygulama bloğu verilmiştir [17].



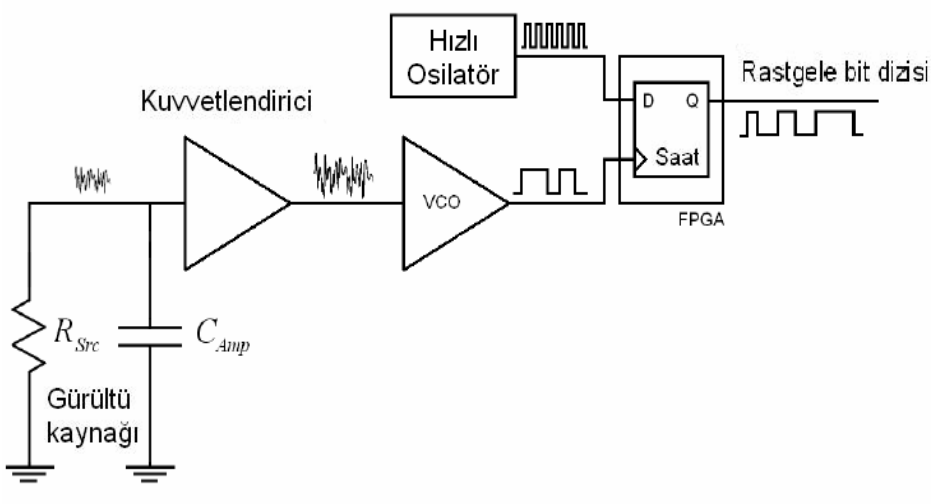
Şekil 4.3: Gürültünün Gauss Dağılımı

Tüm devre yapılarında osilatörler genelde ring osilatör yapıları kullanılarak gerçeklenmektedir [32]. Bu yapının çalışma kriterlerine bakıldığında yavaş osilatörün frekansını 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. Bu tip yapılarda istenilen rastgelelik oluşmayabilir. Bu durumlarda çıkış tekrar sözde rastgele bir algoritmadan geçirilerek tam rastgele bit dizileri elde edilir.

4.3. Intel RSÜ

Yukarıda bahsedilen iki ayrı yöntemin birleşmesiyle Intel firması RSÜ devresini meydana getirmiştir. Yöntemin blok diyagramı şekil 4.4'te gösterilmiştir.

Şekil 4.4'deki blok diyagramdan görüldüğü gibi, bir direncin ısıl gürültüsü kuvvetlendirilir ve bu işaret ilk yapıdaki gibi karşılaştırıcı yerine, bit üretmek için gerilim kontrollü bir osilatörün girişine uygulanır. Böylece ikinci yapıda oluşturulan seğirmeli yavaş osilatör gerilim kontrollü osilatörün çıkışından elde edilir. Daha sonra da hızlı bir osilatör, gerilim kontrollü osilatörün çıkışında oluşan yavaş osilatörle örneklenir [28].



Şekil 4.4: Intel RSÜ'nün Blok Diyagramı

INTEL'in ürettiği RSÜ'de yavaş osilatördeki seğirme yayılımı içine 10–20 adet hızlı osilatör alabilecek kadar olmaktadır. Fakat çıkış hala tam olarak rastgele olmamaktadır. Bu nedenle örnekleme sonucu oluşan bitler düzenleyici bir algoritma olan Von Neumann algoritmadan geçirilir ve tam rastgele bit dizisi elde edilmiş olur.

Tablo 4.1: Von Neumann Algoritması

Giriş Biti	Çıkış Biti
0,0	-
0,1	1
1,0	0
1,1	-

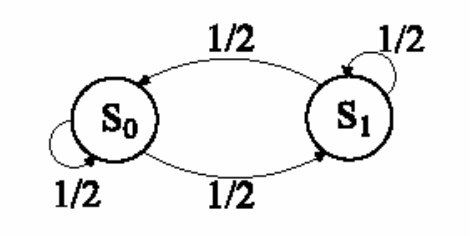
4.4. Kaos Tabanlı Yapılar

Düzensiz davranışları ve başlangıç koşullarına aşırı hassas oluşları nedeniyle, kaotik işaretler de rastgelelik kaynağı olarak değerlendirilmekte ve RSÜ yapımında kullanılmaktadırlar. Kaotik sistemleri ayrık ve sürekli olarak ikiye ayırmak mümkündür

4.4.1. Ayrık Kaos Tabanlı Yapı

Kaos kavramı ile üretilen ilk RSÜ devrelerinde ayrık kaotik tabanlı yapılar kullanılmıştır. Kaos kavramı ile RSÜ için ideal rastgeleliğe iyi bir örnek olan yazı-tura atma olayı incelendiğinde çıkış olasılığı hep ½ olan S_0 ve S_1 durumları

oluşmaktadır. S_0 için çıkışı "0" ve S_1 için çıkışı "1" olan bir yapı tasarlandığında rastgele bir bit üretici elde etmem mümkündür. Bu yapıya ilişkin durum diyagramı Şekil 4.5'te mevcuttur.



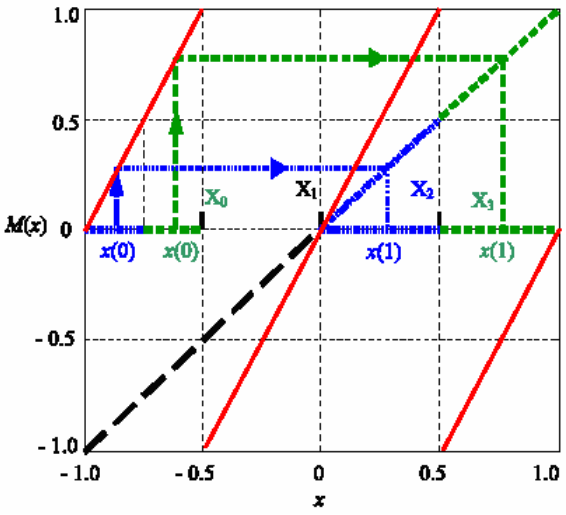
Şekil 4.5: Yazı-Tura Atma Olayına Karşılık Gelen Durum Diyagramı

Durum diyagramındaki davranışı daha anlaşılır ve tasarlanabilir boyuta getirebilmek için parça parça sürekli zaman dönüşümüne ihtiyaç vardır. Bu tip dönüşümler sonucu oluşan bir boyutlu ayrık zamanlı grafiklere Markov dönüşümü ($x_{n+1} = M(x_n)$) denmektedir.

Yazı-tura atma olayını Markov dönüşümü ile incelediğimizde;

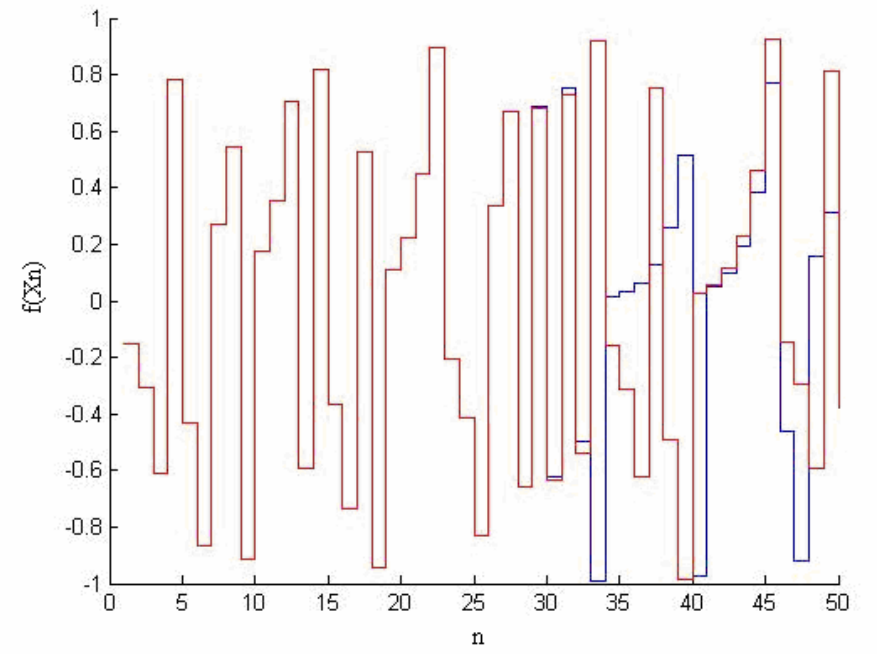
$$M(x_n) = (2x+1) \bmod 2 - 1 \quad \text{için,} \quad x(n+1) = \begin{cases} 2x(n) - 2, & x > 1/2 \\ 2x(n), & 1/2 > x > -1/2 \\ 2x(n) + 2, & -1/2 > x \end{cases} \qquad \textbf{(4.2)}$$

Denklem 4.2'deki eşdeğer oluşmaktadır. Markov dönüşümü ile oluşan durum değerleri X_0=[-1,-1/2], X_1=[-1/2,-0], X_2=[0,1/2] ve X_3=[1/2,1] şeklinde olacaktır [33]. Bu koşullarla oluşan Markov haritası Şekil 4.6'da dır.



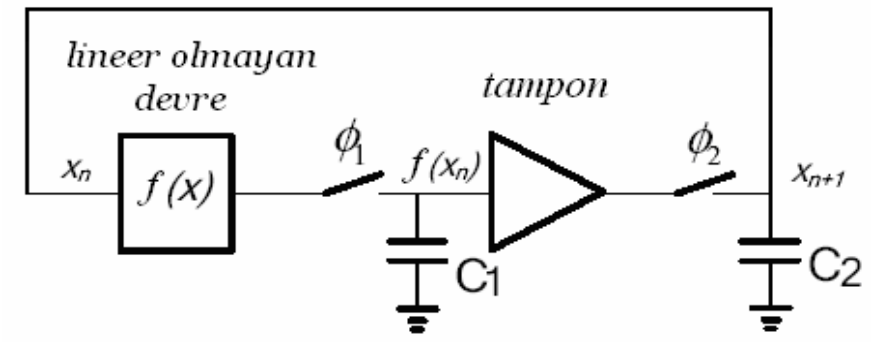
Şekil 4.6: Yazı-Tura Olayının Markov Haritası Dönüşümü

Şekil 4.6'daki Markov dönüşümünü kullanarak tasarlanan RSÜ devresinin dönüşüm sonucu başlangıç koşulları x(1)=-0.076 (mavi) ve x(1)=-0.0760000001 (kırmızı) için çıkış sonuçları incelenmiştir.



Şekil 4.7: Markov Dönüşümü Sonucu Oluşan Çıkış

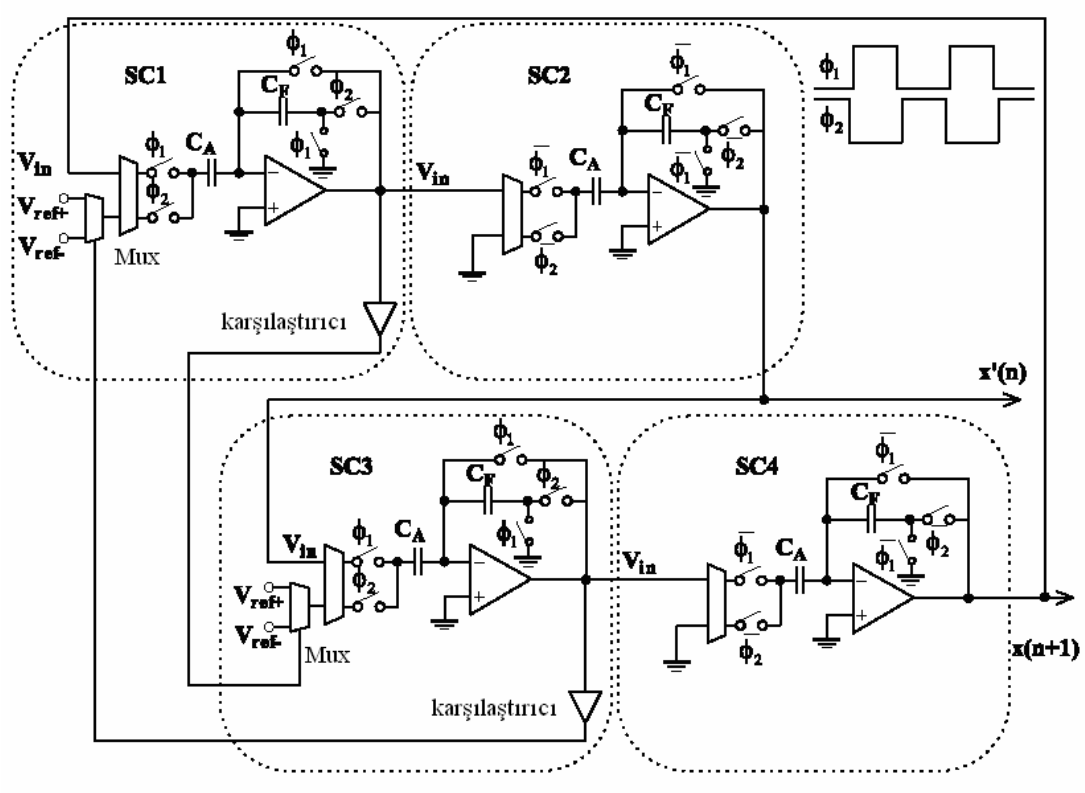
Matematiksel olarak modellenen ayrık kaos tabanlı yapı için tümleşik devre tasarlanması gerektiğinde denklem 3.1'deki iteratif yapının devre elemanları ile gerçeklenmesi gerekmektedir. Ayrık zamanda kaos üreteci oluşturabilmek için nonlineer olan devre yapısına ek olarak saklama ve geciktirme işlemlerini gerçekleyen iki analog yapıya da ihtiyaç vardır. Saklama işlemi için elektronik yapı olarak örnekle ve tut yapısını oluşturan anahtar-kapasite elemanları kullanılır. Gecikme işlemi için ise buffer elemanı yeterli olacaktır. Bu elemanlar kullanılarak oluşturulan ayrık zamanlı kaos için birim hücre yapısı Şekil 4.8'de yer almaktadır.



Şekil 4.8: Ayrık Zamanlı Kaos Üreteci Birim Hücresi

ϕ_1 fazında nonlineer devre x_n işaretini işler ve $y(x_n)$ çıkışı üretir ve bu veri C_1 kapasitesinde saklanır. ϕ_2 fazında ise saklana $y(x_n)$ verisi buffer üzerinden C_2 kapasitesine saklanmak üzere x_{n+1} verisi olarak iletilir ve iterasyon işlemleri böyle devam eder [34].

Bu bilgiler doğrultusunda denklem 4.2'deki yapının devre tasarımına bakmak gerekirse şekil 4.9'teki gibi bir yapıyla karşılaşılacaktır.

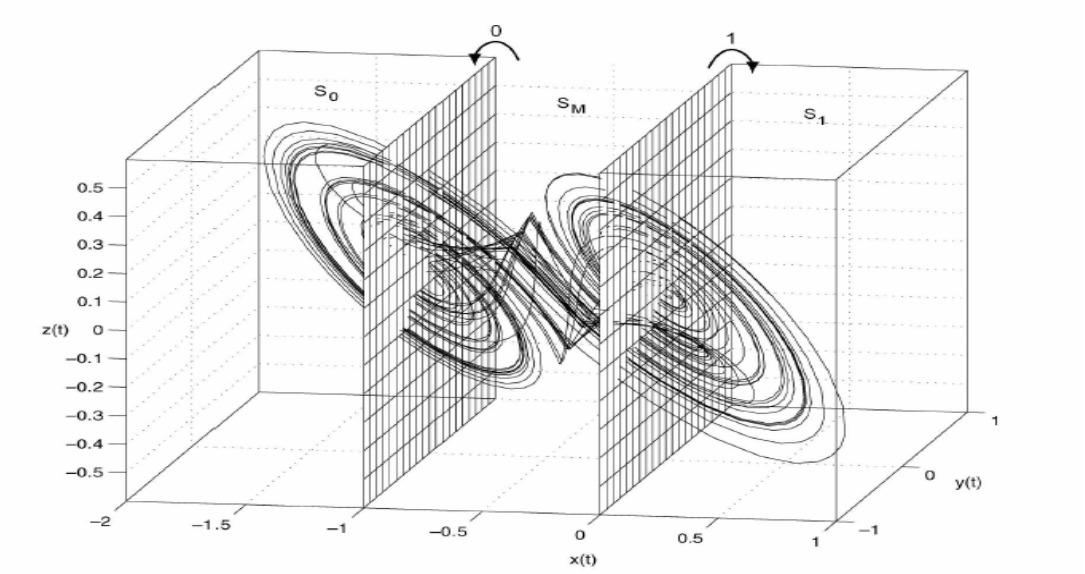


Şekil 4.9: Tümdevre Yapıları için Örnek bir Ayrık Zamanlı Kaos Üreteci

Bu yapıların dezavantajlarına baktığımızda tümdevre uygulamaları için oldukça karmaşık ve çalışma hızları olarak saate bağımlı olduğundan (literatürdeki örneklerde en fazla 500KHz) yavaş çalıştığı gözükmektedir [29].

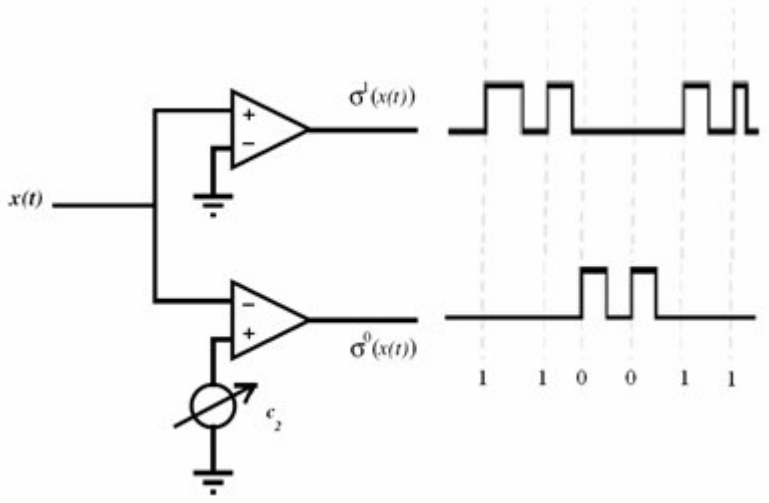
4.4.2. Sürekli Zamanlı Kaos Tabanlı Yapı

Sürekli zamanlı kaos ile tasarlanmış ilk RSÜ tekniği [11]'de gösterilmektedir. Bu çalışma incelenirse temelde entropi kaynağı olarak çift sarmal üreten kaotik osilatör kullanılmaktadır. Rastgele sayı elde etmek için kaotik osilatör devresinin çıkışı, biri denge noktasında ve ikincisi ise diğer denge noktası civarında olmak üzere, iki tane eşik değeri (0 ve -1) seçilir ve devrenin çıkışı 3 alt uzaya bölünmüştür.



Şekil 4.10: Çift Sarmallı Yapı ve Seçilen Eşik Değerleri

İlk karşılaştırıcı x(t) çıkış gerilimi pozitif değer aldığı yerlerde 1, aksi halde 0 çıkışı üretirken; ikinci karşılaştırıcı çıkış gerilimi -1V seviyesinin altında iken 1,aksi halde 0 çıkışı üretmektedir. Daha sonra bu iki bit dizisi düzeltici bir algoritma olan Von Neumann algoritmasıyla rastgele bit dizisi üretebilen bir yapı haline getirilir.



Şekil 4.11: Karşılaştırıcı Bloğu ve Bit Çıkışı

Ancak, karşılaştırılacak uygun eşik değerlerinin belirlenmesi oldukça zordur. Bunun için, bir yandan eşik parametresi değiştirilirken bir yandan da çıkışın entropisinin değişimi incelenerek doğru eşik değeri tespit edilmelidir. Bu yapının bir diğer dezavantajı ise çıkışın Von Neumann algoritmasına gereksinim duymasıdır ki bu işlem de çıkış hızını yaklaşık 4 kat yavaşlatmaktadır.

4.4.3. Ayrık ve Sürekli Zamanlı Kaos Tabanlı Yapıların Karşılaştırılması

Ayrık zamanlı kaos yapılarına baktığımızda (i) matematiksel modele dayanan yapılarından dolayı ayrık zamanlı yapıların çalışmalarının çok daha rahat kontrol edilebilmesi ve çok daha düzgün davranışlar gösterebilmesi (ii) çıkış sonucu oluşan bit değerlerini sonlandırıcı ve düzeltici bir matematiksel algoritmaya gerek duymaması (iii) ve saatle çalıştığından sabit bir değer elde edilebilmesi bu yapıların avantajlarını oluşturmaktadır.

Sürekli zamanlı kaos yapılarına baktığımızda ise (i) çok hızlı veri çıkışı üretebilmesi ve (ii) tümdevre yapıları için basit devreler oluşturabilmesi bu yapıların avantajlarını oluşturmaktadır [35].

4.5. Tümdevrede Karşılaşabilinecek Sorunlar

Tümdevre yapılı RSÜ yapıları incelenmiş ve bu yapılarda karşılaşılabilecek sorunlar irdelenmiştir. Bu sorunlara bakmak gerekirse örneğin tümdevre yapısı aşırı seviyede güç tüketiyorsa bu devreler çalışırken karmaşık güç tüketimi davranışları bazı yazılım tabanlı devreler sayesinde algılanabilmekte ve bu cihazlara güç analizi atağı uygulanabilmektedir. Bu güç tüketimi işaretleri RSÜ'lerinin çıkışlarındaki işaretlerle yüksek seviyede korelasyon gösterdiğinden bu tarz yapılar dış ataklara karşı korumasız kalmaktadır [32,36].

Donanımsal yapılı RSÜ'ler de ne kadar mükemmel tasarlanmış olsa da bant genişliği kısıtlamaları, fabrikasyon toleransları, eskime, ısıl sürüklenme, deterministik yapı etkileri gibi unsurlar sayesinde üretilen bit dizisi bu etkilerle korelasyon gösterebilmektedir. Aynı zamanda bu tümleşik yapılardaki taban gürültüsü ve besleme gürültüsü seviyelerinin getirdiği etki rastgeleliği sağlayan gürültü kaynağının da üstünde bir etki yaratarak kutuplama etkisi yaratarak rastgeleliği olumsuz etkilemektedir [17,32,36].

Oluşabilecek bu istatistiksel kusurları ortadan kaldırabilmek için RSÜ'nin çıkışındaki bit dizileri düzeltici ya da korelasyonu ortadan kaldırıcı algoritmalara sokulur. Bu sayede üretilen hızlı bit dizi akışı yavaşlatılsa da oluşan bit dizisinin kalitesi ve entropi yapısı iyileştirilmektedir [32,36].

5. SÜREKLİ-ZAMANLI KAOS ile RASTGELE SAYI ÜRETECİ TASARIMI

Son yıllarda kaotik işaretlerin haberleşme ve şifreleme [37,38] alanlarında kullanımının artmasıyla kaotik osliatör yapılarının tasarlanmasına büyük önem verilmeye başlanmıştır[23,35,39-43]. Tümleşik devre teknolojisinin gelişmesi ile birlikte düşük güç tüketimi, düşük gerilim ve yüksek frekans çalışmaları gibi özellikleri sağlayabilen kaotik tümdevre yapıları tasarlanabilmektedir.

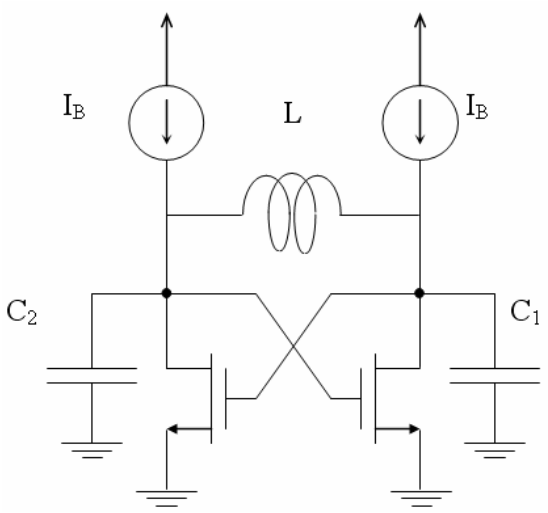
Bu bölümde yeni yapılan çalışmalar ele alınmaktadır. Bu çalışmada tümleşik devre yapısına uygun yeni bir çapraz bağlı LC kaotik osilatörü tanıtımı [44], tasarlanan bu osilatörün CMOS gerçeklemeye uygunluğu, tasarlanan kaotik işareti temelde entropi kaynağı olarak kullanabilecek uygun bir RSÜ yapı seçimi ve bu yapının çalışma prensibi anlatılmaktadır. Kullanılacak RSÜ ve kaotik işaretin matematiksel modelleri oluşturularak RSÜ'nün başarımı ile ilgili nümerik analizler gerçeklenmiş ve sonuçlar yorumlanmıştır. Önerilen metoda göre binary veriler toplanarak tasarlanacak RSÜ'nün FIPS-140-2 ve NIST-800-22 rastgelelik test sonuçları incelenmiştir.

5.1. RSÜ'de Kullanılan Kaotik Osilatör

Bu bölümde RSÜ yapısı için entropi kaynağı olarak iyi bilinen çapraz bağlı LC tank osilatörü temelli yeni bir kaotik osilatör devresi tanıtılmaktadır[44]. Önerilen bu yapı standart CMOS işlemi ile tamamen uyumlu bir şekilde tasarlanabilen ve bir kaç on megahertz gibi yüksek frekanslarda çalışabilecek yapıya sahiptir. Kaotik devrenin uygulanabilir olduğunu gösterebilmek için Cadence tasarım programı ile post-layoutu tasarlanmış, sonuçlar doğrultusunda 0.35μm ams CMOS teknolojisine göre devre üretilmiştir.

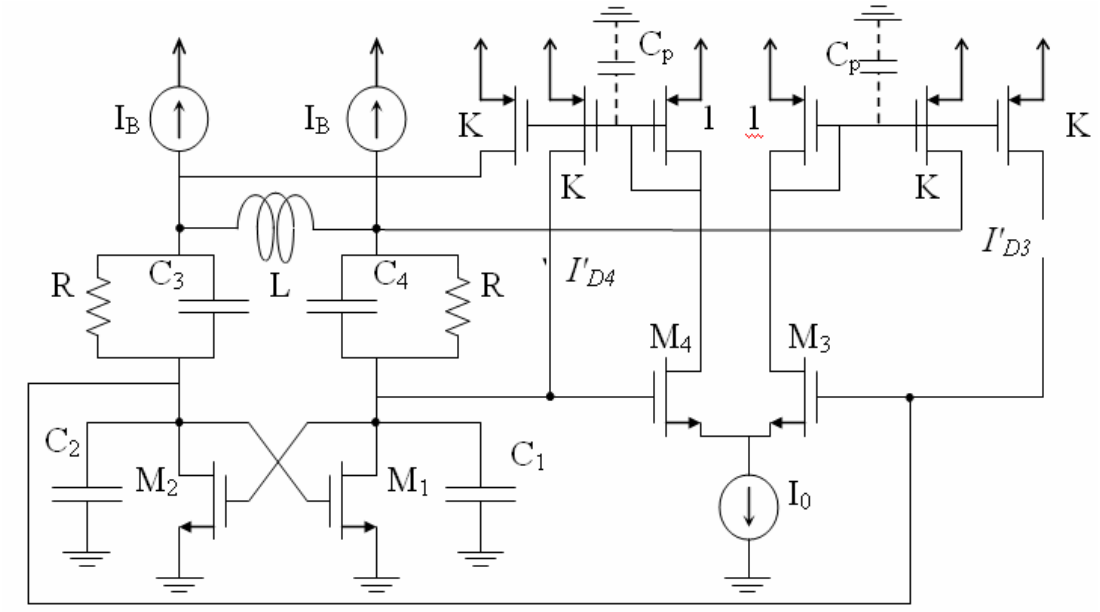
Aynı zamanda tasarlanan CMOS'lu kaotik osilatör yapısından elde edilen ikinci bir bipolar yapılı devre tanıtılmış ve bu yapının Cadence post-layout sonuçları incelenmiştir ki bu sayede bir kaç gigahertz gibi çok yüksek frekans değerlerinde kaotik işaret elde edilebileceği saptanmıştır ve bu yapının gerçeklenebilir olduğu gösterilmiştir.

Bu çalışmada kullanılan kaotik osilatör devresine bakmak gerekirse temelde Şekil 5.1'de çapraz bağlı transistor çifti ile oluşturulmuş negatif dirence paralel bağlanmış iyi bilinen LC tank osilatörü yapısı görülmektedir. Bu yapı literatürde sıkça kullanılan ve negatif-gm LC tank osilatörü olarak adlandırılan sinüzoidal osilatördür[44,45]. Deneyimler ve daha önceki devre yapıları göz önüne alındığında temeli negatif-gm LC tank osilatörü olarak alınarak bu yapıdan kaotik osilatör yapısının türetilebileceği görülmüştür. Ayrıca kaotik osilatör tasarlanırken çapraz bağlı LC tank osilatörü temelli yapının kendine özgü düşük güç tüketimi, yüksek frekans çalışımı ve kaynak gürültüsünün az etkilemesi gibi özellikleri sayesinde tümleşik tasarıma da yatkın olduğu görülmektedir.



Şekil 5.1: Negatif-gm LC Tank Osilatörü

Şekil 5.2'de tanıtılan kaotik yapı detaylı olarak görülmektedir. Bu yapı oluşturulurken Şekil 5.1'deki yapı temel alınmıştır. Devrenin derecesini arttırmak için iki adet paralel RC yapısı eklenmiş ve temel yapıya nonlineerlik kazandırmak için ise diferansiyel çifti katı eklenmiştir. Devrede PMOS transistorler tarafından gerçeklenen akım aynalaması devreye K kazancı sağlamakta ve bu kazanç sayesinde diferansiyel çiftindeki gerilim akım nonlineer karakteristiğinin eğimi kontrol edilmektedir. Devrenin simetrikliği bozulmadan Şekil 5.1'deki temel yapıya eklemeler yapılmıştır. Bu eklemelere rağmen temel yapının daha önce bahsettiğimiz özellikleri bozulmamıştır.



Şekil 5.2: Kaotik Devre

Şekil 5.2'deki yapı göz önüne alındığında, $C=C_1=C_2=0.5C_3=0.5C_4$, $C_p=0$ koşulları altında devrenin durum denklemleri çıkarıldığında denklem 5.1'deki eşitlikler ortaya çıkmaktadır.

$$C\Delta\dot{v}_{C2} = -2i_L + \frac{\beta}{2}\Delta v_{C2}(v_{C2} + v_{C1} - 2V_{TH})$$

$$C(\dot{v}_{C2} + \dot{v}_{C1}) = -2I_B + 2KI_0 - \frac{\beta}{4}\left[\Delta v_{C2}{}^2 + (v_{C2} + v_{C1} - 2V_{TH})^2\right]$$

$$L\dot{i}_L = \Delta v_{C2} - \Delta v_{C4} \qquad \textbf{(5.1)}$$

$$2C\Delta\dot{v}_{C4} = 2i_L - \Delta v_{C4}/R + K\begin{cases} I_0 & ,\Delta v_{C2} \geq \sqrt{2}V_{sat} \\ g_m\Delta v_{C2}\sqrt{1-\left(\Delta v_{C2}/2V_{sat}\right)^2} & ,|\Delta v_{C2}| < \sqrt{2}V_{sat} \\ -I_0 & ,\Delta v_{C2} \leq -\sqrt{2}V_{sat} \end{cases}$$

5.1'deki denklemdeki bilinmeyen parametreler ise $\Delta v_{C2}=v_{C2}-v_{C1}$, $\Delta v_{C4}=v_{C4}-v_{C3}$, $V_{sat}=\sqrt{I_0/\beta}$, $g_m=\sqrt{I_0\beta}$ geçiş iletkenliği parametresi, $\beta=\mu_n C_{ox} W/L$ ve V_{TH} MOS transistor eşik gerilimi olarak gösterilmektedir. Şekil5.2'deki C_p parazitik kapasitesi PMOS transistorun geçit-kaynak parazitik kapasitesini temsil etmektedir. Bu parazitik kapasitenin etkisi sahip olduğu değerden dolayı devreyi etkileyecektir ancak işlemlerin kolaylığı açısından denklemlere eklenmemiştir. Bu parazitik kapasitenin etkisinden daha sonra bahsedilecektir.

Denklem 5.1'deki yapı için normalizasyon değişkenleri: $x_1=\Delta v_{C2}/2V_S$, $x_2=(v_{C2}+v_{C1})/2V_S$, $y=2i_LR_0/V_S$, $z=\Delta v_{C4}/2V_S$, $t_n=t/2R_0C$, $V_S=V_{TH}$ ve $R_0{}^2=L/8C$, olarak

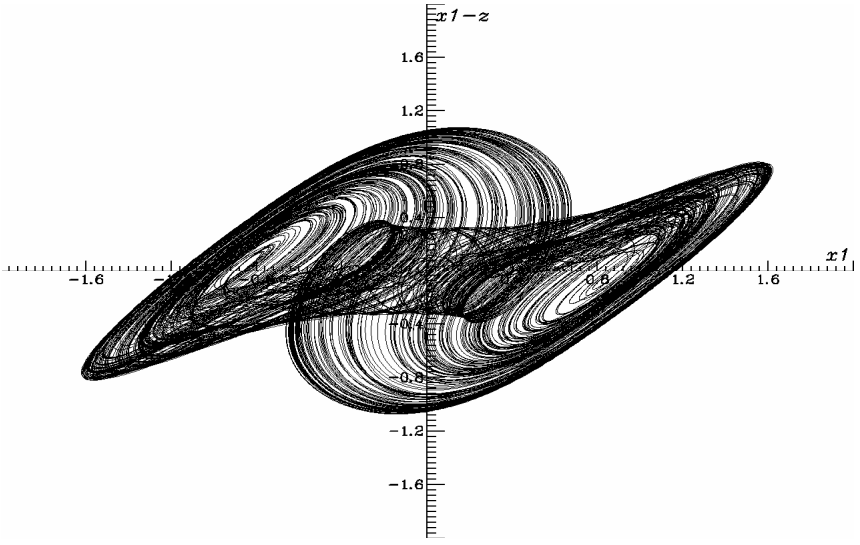
belirlenmiştir. Bu değişkenler doğrultusunda yeni denklem takımı 5.2'deki gibi:

$$\begin{aligned}
\overset{\circ}{x}_1 &= -y + bx_1[x_2 - 1] \\
\overset{\circ}{y} &= x_1 - z \\
\overset{\circ}{x}_2 &= d - 0.5b\left[{x_1}^2 + (x_2 - 1)^2\right] \\
2\overset{\circ}{z} &= y - 2mz + K\begin{cases} c & , x_1 > x_{sat} \\ \sqrt{2bc}\, x_1\sqrt{1-\left(\dfrac{x_1}{\sqrt{2}x_{sat}}\right)^2} & , |x_1| < x_{sat} \\ -c & , x_1 < -x_{sat} \end{cases}
\end{aligned} \qquad \textbf{(5.2)}$$

iken $x_{sat}=V_{sat}/V_{TH}$, $b=2\ \beta R_0 V_{TH}$, $c=I_0R_0/V_{TH}$ ve $d=2(KI_0-I_B)R_0/V_{TH}$, $m=R_0/R$ olmaktadır.

Akım aynaları ile sağlanan K parametresi devrenin güç harcamasını ve yüksek frekanslarda çalışma yeteneğini olumsuz etkilese de devrenin daha gürbüz bir yapıya sahip olabilmesi için gerektiği yapılan nümerik analizler sonucu ortaya çıkmıştır.

Bu devre değişik parametre takımları ile kaosa girebilmektedir. 5.2'deki denklem için Runge-Kutta Felberg metodu kullanıldığında parametreler b=0.26, c=0.146, d=1.2, K=8, m=1 seçildiğinde kaotik atraktör takımlarından $x_1 - (x_1\text{-}z)$ değerlerinin projeksiyonu Şekil5.3'teki gibi olmaktadır.



Şekil 5.3: Denklem 5.2'nin Numerik Analizi

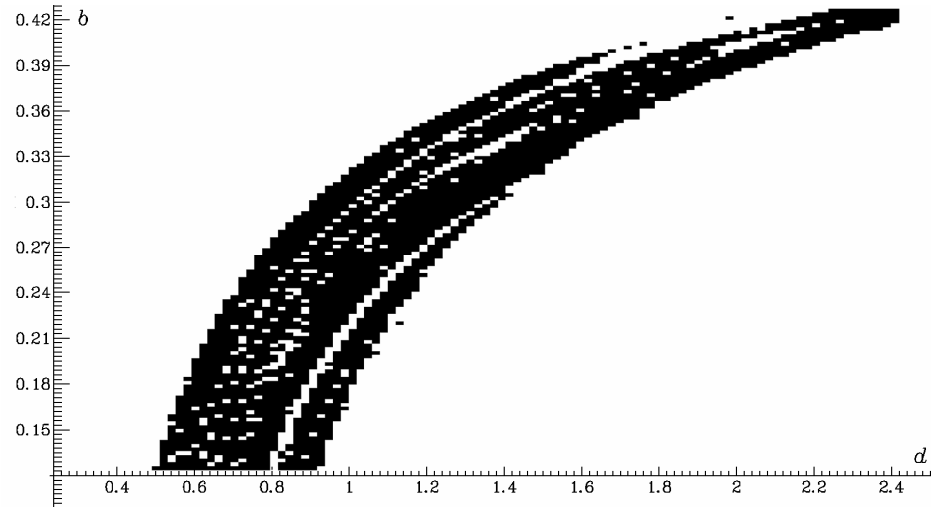
Nümerik olarak tasarlanan devrenin tümleşik devre olarak üretilmesi esnasında üretim toleranslarından kaynaklanan değer sapmaları oluşacaktır. Bu sıkıntılar devrenin hem kaosa girme parametrelerinin değişmesine hem de devrenin gürbüz

yapısının azalmasına neden olacaktır. Bu yüzden devre tasarımı bu sapmalar göz önüne alınarak gerçeklenmiştir. Üretim esnasında gerçeklenecek tolerans hatalarından dolayı b,c,d,K ve m parametreleri çalışma aralıkları incelenmiştir.

PMOS akım aynasının oluşturduğu K parametresi, akım aynasının çıkış katına K adet paralel transistor ve giriş katına aynı boyuttan bir adet diyot bağlı transistor bağlayarak gerçeklenmiştir. Tümdevre üretiminde aynı boyutlu transistor eşleri üretebilmek neredeyse hatasız bir şekilde mümkündür ve tam olarak K değeri ayarlanabilmektedir. Kaotik devrenin benzetim sonuçları gösteriyor ki K değerinde PMOS transistorun kanal boyu modulasyonundan kaynaklanan %3lük bir sapma mevcuttur. Bu hata kaskod akım aynası kullanarak daha da aşağıya çekilebilmektedir ancak nümerik analiz sonuçları 5.2'deki denklemde bu seviyedeki bir sapmanın çok ciddi bir bozulmaya neden olmayacağı belirlenmiştir. Böylece K parametresi nerdeyse hatasız bir şekilde imal edilebilmektedir.

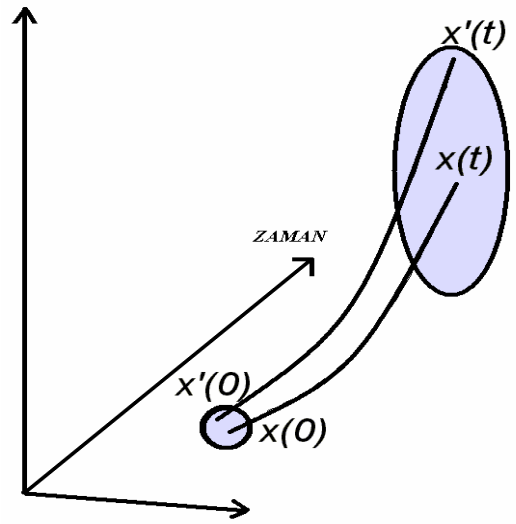
$c=I_0R_0/V_{TH}$ ve $d=2(KI_0-I_B)R_0/V_{TH}$ değişkenlerine bakıldığında I_0 ve I_B akımlarının DC olarak değişimi ile c ve d parametreleri ayarlanabilmektedir. Bu sayede c ve d parametreleri elektronik olarak kontrol edilebilir ve doğru bir şekilde istenilen değere ayarlanıp sabitlenebilir bir özelliğe kavuşmuştur.

K, c ve d parametreleri düzgün bir şekilde ayarlanabilirken tümleşik devre üretimi esnasında b parametresinin yani NMOS transistorun geçiş iletkenliği β değeri ve m parametresinin yani R direnci değeri istenilen değerlere tam veya yaklaşık olarak ayarlanamadığı gibi %30'lara varan sapmalarla üretim gerçeklenebilmektedir. Bu üretim kusurlarından dolayı sapma etkileri iki parametreli düzlemde nümerik olarak incelenmiş ve devrenin kaosa girme hassasiyeti ve aralığı ölçülmüştür. Denklem 5.2'deki yapıda b parametresi (0.12, 0.4) arasında değiştirilirken dışardan ayarlanabilen d parametresi (0.5, 2.5) arasında değiştirilirmiş, diğer parametrelerse Şekil 5.3'teki atraktörü gerçekleyen değerlerine sabitlenmiştir. Şekil 5.4'te b ve d parametrelerinin taratılması sonucu devrenin kaotik yapısı sorgulanmıştır. Şekildeki siyah bölgeler lyapunov üstelinin pozitif olduğu yani devrenin kaotik davrandığı bölgeleri göstermektedir.



Şekil 5.4: Kaotik Devrenin b ve d Parametrelerine Göre Kaotik Davranışı

Lyapunov üsteli kavramını açıklamak gerekirse ΔX_0 çok küçük bir değer olmak üzere aynı denklem için başlangıç koşulları X_0 ve $X_0+\Delta X_0$ olarak alındığında $f(X_0, t)$ ve $f(X_0+\Delta X_0, t)$ arasında oluşacak fark devrenin Lyapunov üstelini oluşturacaktır. Bu kavram Şekil5.5'te gösterilmektedir.



Şekil 5.5: Lyapunov Üsteli Kavramı

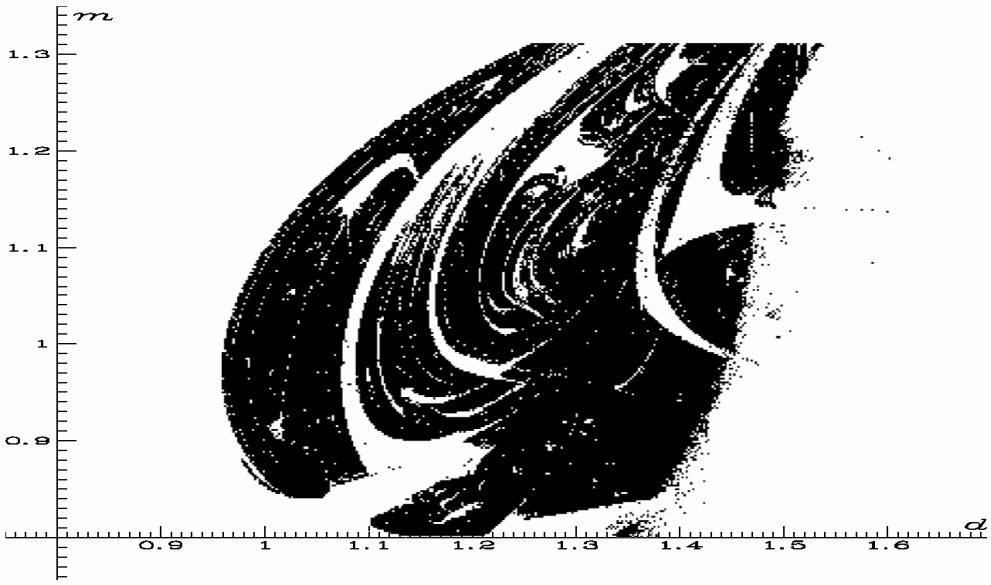
Lyapunov değerlerini hesaplamak gerekirse:

$$\lambda = \lim_{t\to\infty} \frac{1}{t} \ln \frac{\left| f(X_0 + \Delta X_0, t) - f(X_0, t) \right|}{\left|\Delta X_0\right|} \qquad \textbf{(5.3)}$$

olarak denklem 5.3'te hesaplanmaktadır ve hesaplanan lambda değerine göre sistemin davranışı hakkında bilgi edinilebilmektedir. Buna göre $\lambda<0$ için devre

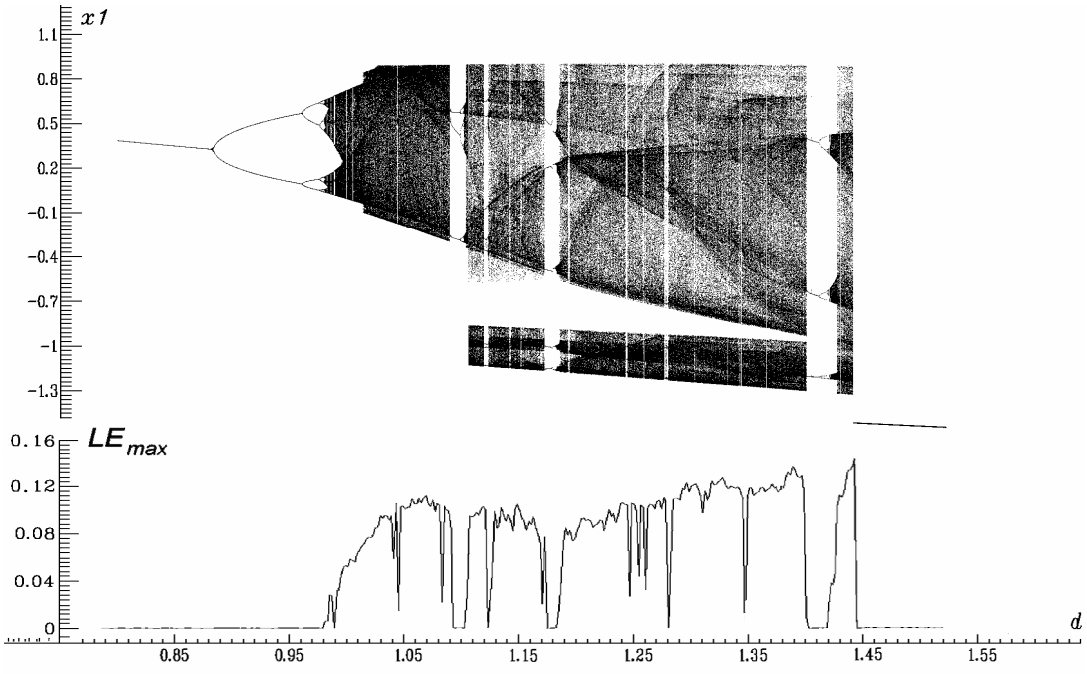
kararlı, $\lambda=0$ için devre korunumlu, $\lambda>0$ için ise devre kararsız davranış göstermektedir.

Aynı karakteristik m (0.7, 1.3) aralığında ve d (0.9, 1.6) aralığında gerçeklenmiş ve Şekil 5.6'daki karakteristik ortaya çıkmıştır. Bu çalışmalarda b parametresi %54'lük m parametresi ise %30'luk sapmalara göre taratılmıştır ve bu değerler içinde devrenin kaosa girdiği nümerik olarak hesaplanmıştır. Bu karakteristiklerden anlaşılacağı üzere üretim esnasında b veya m parametresini istenilen değerden sapması durumunda dışardan ayarlanan I_0 ve I_B kutuplama akımlarıyla d parametresi istenilen değere ayarlanabilmekte ve bu sayede devre tekrardan kaosa sokulabilmektedir.



Şekil 5.6: Kaotik Devrenin m ve d Parametrelerine Göre Kaotik Davranışı

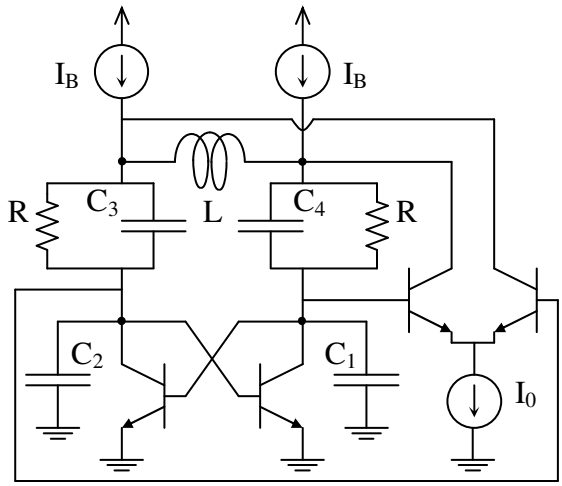
Devrenin kaotik davranışını belirleyebilmek için dallanma diyagramı kullanılmaktadır. Devrenin dallanma diyagramına bakabilmek için en uygun parametre ise d parametresi olarak belirlenmiştir. Çünkü devre denge noktasında iken çapraz bağlı transistorlerin üstünden akan akım $2(KI_0-I_B)$ olmakta başka bir deyişle endüktans kısa devre kapasitelerse açık devre iken transistorlerden akan akımın normalizasyon sonucu kolay bir şekilde $d=2(KI_0-I_B)R_0/V_{TH}$ olarak görülmektedir. Bu akım, transistorün geçiş iletkenliğini diğer bir deyişle devredeki negatif direncin değerini belirlemekte yani devrenin özdeğerinin reel kısmını oluşturmaktadır. Bu yüzden dallanma diyagramı için seçilen d parametresi sistemin dinamik davranışının gözlenmesi için en uygun değişken olacaktır. d parametresine göre sistemin dallanma diyagramı ve Lyapunov üstelinin karakteristiği Şekil5.7'de verilmektedir.



Şekil 5.7: Kaotik Devrenin d Parametresine Göre Dallanama Diyagramı ve Lyapunov Üsteli

Beklendiği üzere devre zengin bir dinamik yapı sergilemekte periyot-2, periyot-3 ve periyot-5 gibi dallanmalarla bölünmüş parçalı kaos davranışları Şekil5.7'de görülmektedir. Küçük d değerleri için devre periyot-2, periyot-4 ve tek sarmallı davranırken d parametresi 1.1'i geçince çift atraktörlü davranış sergilemeye başlamaktadır. d parametresi I_0 ve I_B kutuplama akımlarıyla ayarlanabildiğinden her türlü dinamik davranış bu akım değerlerinin değişimi ile elde edilebilmektedir.

Ayrıca Şekil 5.2'deki yapı temel alan ikinci bir devre tanıtılmaktadır. Şekil5.8'de önerilen devre bipolar yapıda tasarlanmıştır.



Şekil 5.8: Kaotik Devrenin Bipolar Versiyonu

Şekil 5.2'deki CMOS'lu devrede K ile gösterilen gerilim-akım nonlineer karakteristiğini sağlayan akım aynalı yapı bipolarlı yapıda yerini $I_C=I_S\ e^{VBE/VT}$ eşitliğine bırakmıştır. Böylece devrenin karmaşıklığı azaldığı gibi çalışma frekansıda CMOS'lu devreye göre oldukça yükselmiştir. $C=C_1=C_2=0.5C_3=0.5C_4$ koşulu altında devrenin durum denklemleri incelendiğinde:

$$
\begin{aligned}
C\,\dot{\Delta v}_{C2} &= -2i_L + I_S(e^{\frac{v_{C2}}{V_T}} - e^{\frac{v_{C1}}{V_T}}) - I_0 \tanh(\frac{\Delta v_{C2}}{2V_T}) \\
C(\dot{v}_{C2} + \dot{v}_{C1}) &= 2I_B - I_0 - I_S(e^{\frac{v_{C2}}{V_T}} + e^{\frac{v_{C1}}{V_T}}) \\
L\,\dot{i}_L &= \Delta v_{C2} - \Delta v_{C4} \\
2C\,\dot{\Delta v}_{C4} &= 2i_L - \frac{\Delta v_{C4}}{R} + I_0 \tanh(\frac{\Delta v_{C2}}{2V_T}).
\end{aligned}
\qquad \textbf{(5.4)}
$$

olarak belirlenmektedir. I_S transistorun saturasyon akımını gösterirken V_T ise ısıl gerilimi göstermektedir.

Denklem 5.4'teki yapı için normalizasyon değişkenleri: $x_1=\Delta v_{C2}/2V_S$, $x_2=(v_{C2}+v_{C1})/2V_S$, $y=2i_LR_0/V_S$, $z=\Delta v_{C4}/2V_S$, $t_n=t/2R_0C$, $V_S=V_T$ seçilmiş ve paramerteler $b=I_SR/V_T$, $c=I_0R/V_T$ ve $d=(2I_B-I_0)R/V_T$ olarak belirlenmiş ve normalize denklem 5.5'te elde edilmiştir.

$$
\begin{aligned}
\dot{x}_1 &= -y + b\left[e^{x2+x1} - e^{x2-x1}\right] - c\tanh(x_1) \\
\dot{y} &= x_1 - z \\
2\dot{z} &= y - 2z + c\tanh(x_1) \\
\dot{x}_2 &= d - b\left[e^{x2+x1} + e^{x2-x1}\right]
\end{aligned}
\qquad \textbf{(5.5)}
$$

Şekil 5.8'deki yapıya bakıldığında bu tasarıma ait denklem daha farklı bir parametre takımı ile kaosa girmektedir. $b=10^{-12}$, c=3, d=3.5 değerleri için Şekil5.3'tekine benzer bir karakteristik sergilendiği görülmüştür. Ayrıca bu yapının d parametresine göre taratılarak bakılan dallanma diyagramı karakteristiği de Şekil5.7'deki yapıya benzer bir karakteristik göstermiştir.

5.1.1. Parazitik Kapasitenin Kaotik Devreye Etkileri

Tanıtılan yapıda MOS yapılar kullanılması nedeniyle birçok parazitik kapasite yer almaktadır. Bu yüzden parazitik kapasitelerin devrenin çalışma performansını ne kadar etkileyeceği ya da kısıtlayacağı önem kazanmaktadır. Şekil5.2 doğrultusunda devreye bakıldığında M_3-M_4 transistorlerinin kaynak ucu ortak diferansiyel çiftine yani AC toprağa bağlıdır ayrıca M3-M_4 transistorlerin diğer parazitik kapasiteleri devrede C_1-C_2 kapasitelerine paralel gelmektedir bu yüzden bu parazitik etkiler ihmal edilir düzeydedir. Akım aynalama devresindeki çıkış katlarında bulunan PMOS'ların savak-kaynak ve savak-gövde etkileri ise yüksek frekanslarda devredeki C_3-C_4 kapasiteleri ile şöntlenmektedir ve etkileri ortadan kalkmaktadır. Bu bilgiler doğrultusunda ve yapılan benzetmeler sonucu devrenin çalışma performansını gerçekten etkileyebilecek parazitik nedenlerin endüktansın sonlu kalite faktöründen ve akım aynasındaki PMOS'ların geçit-kaynak parazitik kapasitesinden meydana gelmiştir. Akım aynalamaları sonucu K akım kazançlı yapılar oluşmakta ve büyük akım kazançları değerleri sonucu geçit kapasitelerinin sayısı artmakta ve PMOS'ların geçit-kaynak parazitik etkilerini katlamaktadır. Tüm bu parazitiklerin toplamı devrede C_P olarak gösterilmiştir. Ayrıca endüktansın sonlu kalite faktörünün getireceği L ye paralel gelen direnç r_Q olarak tanımlanmıştır. Bu ideal olmayan yapılar göz önüne alınarak ve iki yeni değişkenle beraber $w_1=2(I'_{D3}- I'_{D4})R/V_{TH}$, $w_2=2(I'_{D3}+I'_{D4})R/V_{TH}$ devre için yeni bir tanım bağıntısı ayarlamak gerekirse, $xsat=V_{sat}/V_{TH}$, $b=2\beta RV_{TH}$, $c=I_0R/V_{TH}$, $d'=-2I_BR/V_{TH}$, $\varepsilon_Q=r_Q/4R$, $\varepsilon=C_p/4C$ için

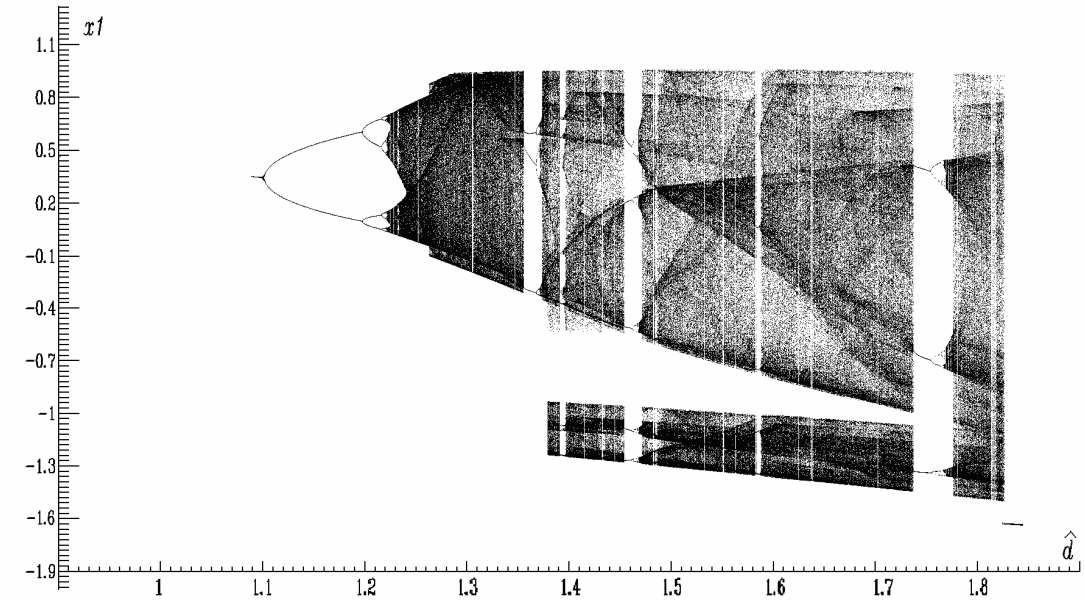
$$
\begin{aligned}
\dot{x}_1 &= -y + bx_1[x_2 - 1] \\
\dot{y} &= x_1 - z - \varepsilon_Q y \\
\dot{x}_2 &= d' + Kw_2 - 0.5b\left[x_1^{\,2} + (x_2 - 1)^2\right] \\
2\dot{z} &= y - 2z + 0.5Kw_1 \\
\varepsilon \dot{w}_1 &= \frac{\sqrt{b}}{32}\left[\sqrt{w_1 + w_2}\,(4c + 4f(x_1) - w_1 - w_2) - \sqrt{w_2 - w_1}\,(4c - 4f(x_1) - w_2 + w_1)\right] \\
\varepsilon \dot{w}_2 &= \frac{\sqrt{b}}{32}\left[\sqrt{w_1 + w_2}\,(4c + 4f(x_1) - w_1 - w_2) + \sqrt{w_2 - w_1}\,(4c - 4f(x_1) - w_2 + w_1)\right]
\end{aligned}
\qquad \textbf{(5.6)}
$$

$$f(x_1)=\begin{cases} c & ,x_1 > x_{sat} \\ \sqrt{2bc}\,x_1\sqrt{1-\left(\dfrac{x_1}{\sqrt{2}x_{sat}}\right)^2} & ,|x_1| < x_{sat} \\ -c & ,x_1 < -x_{sat} \end{cases}$$

olarak denklem 5.6'daki gibi gösterilir.

Denklem 5.6'da ε_Q endüktansın sonlu kalite faktörünün etkisini, ε ise PMOS'un getireceği parazitik etkileri modellemektedir. İdeal olmayan bu yapının davranışını görmek için denklem 5.6'daki d' parametresinin dallanma diyagramına bakılmalıdır. Ancak bu diyagramı Şekil5.7'deki dallanma diyagramı ile kıyaslayabilmek için yeni bir parametre olan $\hat{d} = d'+2Kc$ ile dallanma diyagramı çizilmelirid. Böylece $\hat{d} \equiv d$ eşitliği ile aynı düzlemde kıyaslama yapmak mümkün olmuştur. ε_Q ve ε değerlerinin etkilerini görmek için (ε_Q , ε)=(0.05, 10^{-6}) ve (ε_Q , ε)=(10^{-6}, 0.075) değerleri ile iki farklı dallanama diyagramı elde edilmiştir.

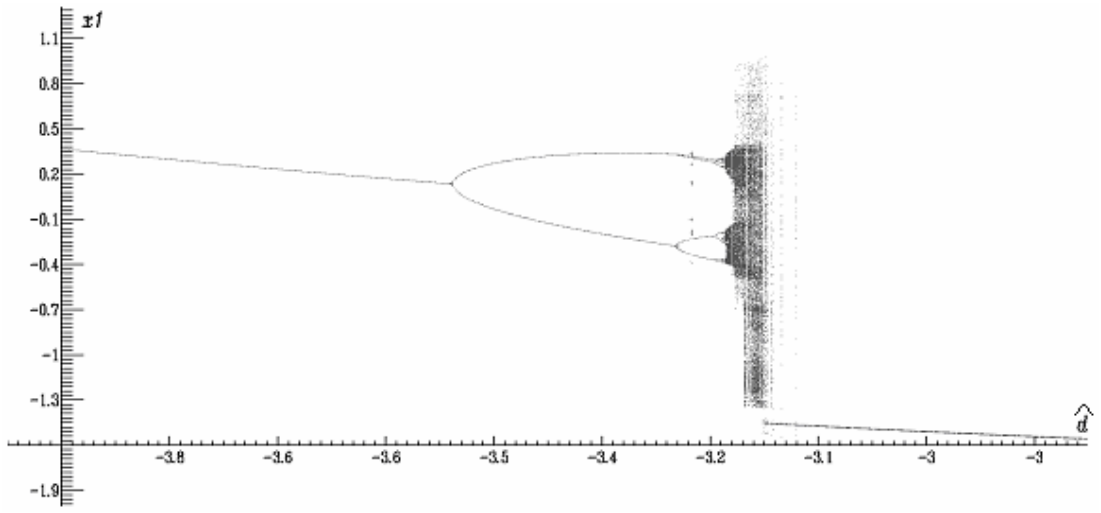
(ε_Q , ε)=(0.05, 10^{-6}) koşulunda endüktansın sonlu kalite faktörü denklemde etkisini gösterirken parazitik kapasitenin etkisi yok sayılacak kadar azdır. Böylece sırf endüktansın devre üstündeki etkisi incelenebilmektedir. Şekil5.9'da endüktansın sonlu kalite faktörünün $\hat{d}$ parametresi ile dallanma diyagramı karakteristiği görülmektedir.



Şekil 5.9: Endüktansın Sonlu Kalite Faktörünün $\hat{d}$ Parametresi Dallanması

Şekil5.9'dan da anlaşılacağı gibi devrede endüktansın son kalite faktörünü Şekil 5.7 ile kıyaslandığında dallanma diyagramı karakteristiğini değiştirmediği sadece aynı karakteristik için daha büyük bir $\hat{d}$ parametresine gerek duyduğu görülmektedir. Bu değer $\hat{d} = 2(KI_0 - I_B)R/V_{TH}$ eşitliğinden de anlaşılacağı gibi I_O ve I_B akımlarıyla ayarlanabilmektedir. I_B akımın denklemdeki etkisi KI_O değerine göre çok ufak kalacağından $\hat{d}$ parametresi Io akımını ile doğru orantılı bir şekilde kontrol edilmektedir. Ancak devrenin kaosa girebilmesi için daha büyük bir $\hat{d}$ parametresine yani daha büyük bir Io akımına ihtiyaç duyulacaktır ki bu işlem devrenin güç harcamalarının artmasına neden olacaktır.

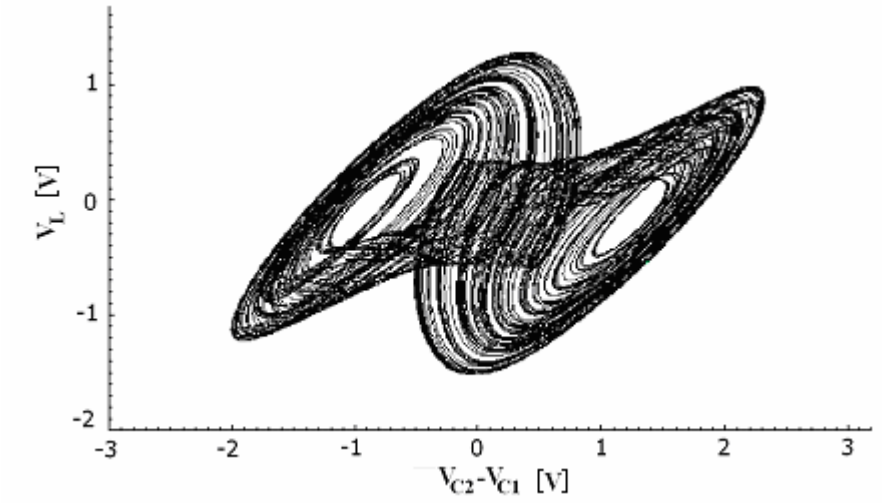
$(\varepsilon_Q , \varepsilon)=(10^{-6}, 0.075)$ koşulunda endüktansın sonlu kalite faktörü denklemde etkisi yok sayılacak düzeyde iken parazitik kapasitenin devre üstündeki etkisi incelenmiştir ve dallanama diyagramı karakteristiği Şekil 5.10'da gösterilmiştir. Şekilden de anlaşılacağı gibi seçilen ε değeri için devre çok dar bir alanda kaosa girmektedir. Yani ε dolayısı ile C_P devrenin çalışma frekansı için bir üst limiti oluşturmaktadır. Ancak bu kısıtlamanın üstesinde devrenin normalizasyonunda kullanılan zaman sabitinin R_0C'nin azaltılması ile gelinebilir ve böylece daha yüksek frekanslarda tekrardan işlem gerçeklenir. Ancak R_0 değerinde yapılacak her hangi bir azaltma b ve c parametrelerinin korunabilmesi için I_O ve I_B akımlarının arttırılmasına ve böylece devrenin güç tüketiminin de artmasına neden olacaktır. Bu sorunun da üstesinden gelebilmek için ise R_0 değeri yerine C değeri ufaltılmalıdır ancak bu seferde C değeri ufalınca ε değeri artacağından devrenin gürbüz yapısı zayıflayacaktır.



Şekil5.10: C_P Parazitik Kapasitesinin $\hat{d}$ Parametresi Dallanması

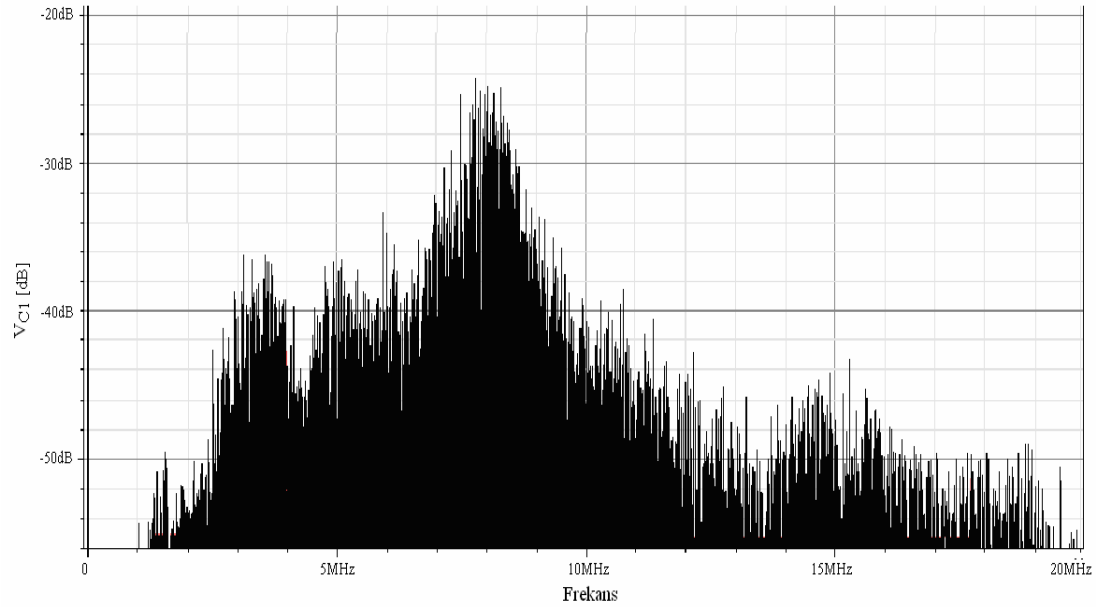
5.1.2. Kaotik Devrenin Benzetim ve Deneysel Sonuçları

Kaotik devrelerin uygunluğunu ve performansını görmek için Cadence programı kullanarak 0.35μm SiGe BiCMOS üretim tekniği ile devrelerin tasarımları yapılmıştır. Her iki devrede 0.35μm üretim tekniği gereği ±1.5V besleme gerilimi ile beslenmektedir. Şekil5.2'deki CMOS'lu yapı için pasif eleman değerleri L=10μH, C=10pF, R=350Ω olarak seçilirken kutuplama akımları I_B=370μA, I_0=230μA olarak belirlenmiştir. K değerinin ayarlanması için ise akım aynasının çıkış katına eş boyutlu 8 transistor paralel bağlanırken giriş katına aynı boyutlara sahip bir adet diyot bağlı transistor bağlanarak K değeri 8'e ayarlanmıştır. Tasarımda NMOS transistorlerin boyutları W/L=12μm/1μm olarak seçilmiştir. Benzetim sonuçlarına bakıldığında NMOS transistorun geçit iletkenliği 55 $\mu A/V^2\mu m$ eşik gerilimi ise 0.57V olarak bulunmuştur. Tüm bu veriler kullanılarak denklem 5.2'deki parametreler hesaplandığında b=0.26, c=0.143, K=8, d=1.82 ve m≈1 olarak bulunmaktadır ki bu değerler neredeyse Şekil5.3'ü oluşturan parametrelerle mükemmel benzerlik göstermektedir. Bir tek d parametresi olan değerinden büyüktür ancak bölüm 5.1.1'de de anlatıldığı gibi endüktansın sonlu katsayı faktöründen dolayı d parametresinn büyük olma gereksinimi bu farklılığın yaratacağı sorunları ortadan kaldırmaktadır. Bu parametreler kullanılarak faz eğrisi için düzlemler (v_{C2}-v_{C1})'e v_L seçildiğinde Şekil 5.11'deki normalize atraktör davranışı ortaya çıkmıştır. Bu davranış Şekil5.2'deki yapı ile örtüşmektedir.



Şekil 5.11: Cadence Benzetiminde CMOS Devrenin Kaotik Atraktör Davranışı

Kaotik işaretin frekans spektrumu ise Şekil5.12'de verilmektedir. Şekilden de anlaşılacağı gibi kaotik işaretin DC seviyeden 15MHz'e kadar uzanan geniş bir frekans karakteri mevcuttur.



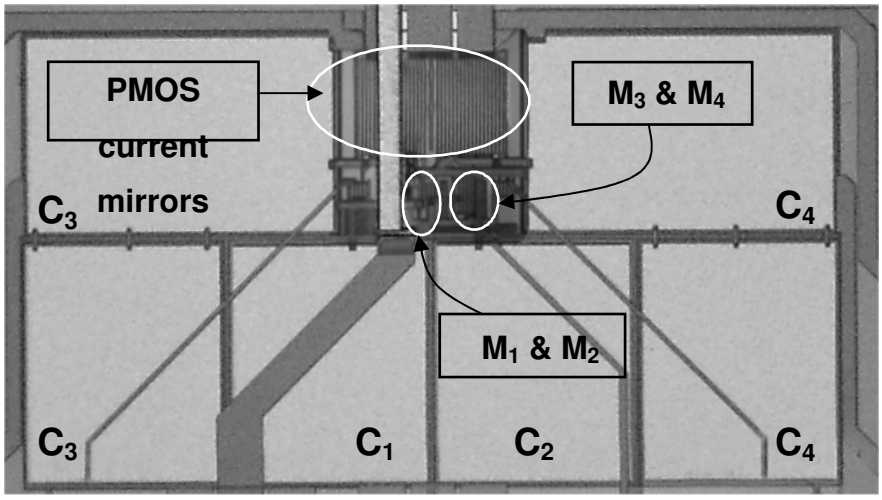
Şekil 5.12: Cadence Benzetiminde CMOS Devrenin Frekans Spektrumu

Bu şekilden yola çıkarak güç tüketimi yoğunluğunun tek bir frekans noktası olan 8MHz civarında yoğunlaştığı görülmektedir. Daha önceki [42] otonom yapılı kaotik işaretlerin frekans spektrumlarına da bakıldığında kaosun temelde var olan sinüs osilatörünün merkez frekans ve bu işaretin pertürbasyonlarıyla birlikte oluştuğu görülmektedir. Yani güç spektrumu sinüs osilatörünün merkez frekansının etrafına yayılmaktadır. Şekil5.2'de tanıtılan devre yapısında var olan sinüs osilatörünün merkez frekansının 8MHz olduğu görülmekte ve bu tepe frekansı kaotik osilatör için $f_{0,kaos}$ olarak adlandırılmaktadır.

Devrenin benzetim modeline bakıldığında parazitik kapasite C_p = 500fF olarak görülmektedir. Denklem 5.6'dan yola çıkarak ε değerinin üst limiti 0.05 olarak seçilirse devrede kullanılması gereken en küçük kapasite değeri C = 2.5pF olmalıdır. Eğer devre alabileceği en küçük kapasitif değer ile tasarlanırsa kaotik işaretin merkez frekansı 32MHz'e kadar artacaktır. Benzetimler boyunca kapasite ve endüktans değerleri daha küçük değerlere çekilerek 30MHz merkez frekanslı kaos işaretleri elde edilmiştir. Ancak bu koşullar altında devre çok dar bir aralıkta kaosa girmektedir. Bu yüzden üretim için devrenin daha gürbüz ve daha güvenli çalışacağı aralığı garantileyen C=10pF ve L=10µH değerlerini alarak tasarlanmıştır.

Cadence benzetim programında ayrıca Şekil5.8'de gösterilen önerilen devrenin bipolar versiyonu da tasarlanmıştır. Bu yapı için uygun pasif eleman değerleri ve kutuplama akımları ise L=7nH, C=350fF, R=100Ω ve I_B=800μA, I_0=50μA olarak seçilmiştir. Bu yapının da atraktör davranışı Şekil5.10'daki CMOS'lu yapı ile aynı karakteristiği sergilemiştir. Ayrıca yapılan frekans spektrumu analizleri sonucu bu yapının 6GHz'e kadar çalışabileceği güç harcamasına ise 2.7mW olacağı hesaplanmıştır.

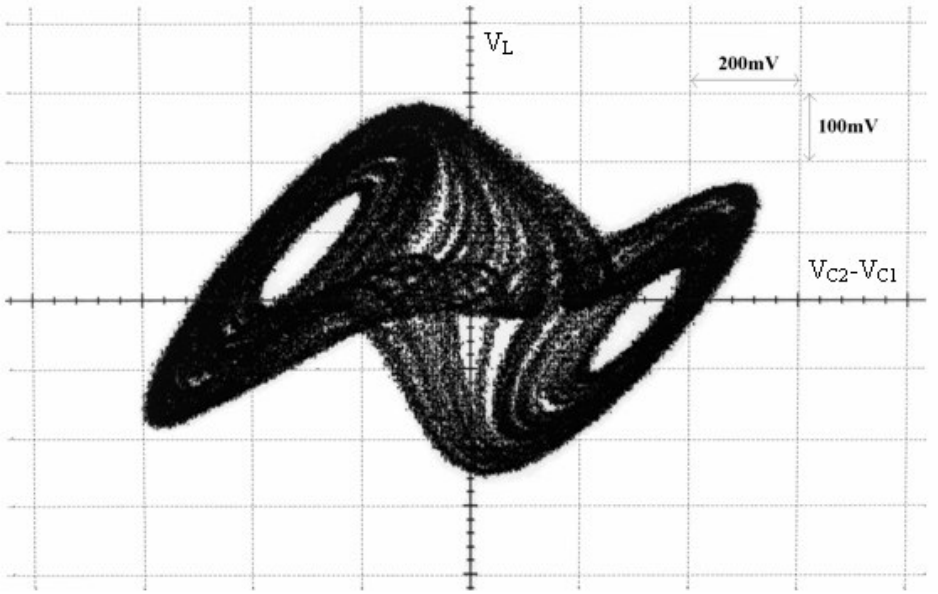
Şekil5.13'te önerilen CMOS devresi 0.35μm n-kuyulu CMOS tekniği kullanılarak üretilmiştir[44]. Tasarlanan çipin görüntüsü Şekil5.12'de gösterilmektedir. Çip toplamda 11mW güç tüketmekte ve 0.12mm^2 (430μm x 290μm) alan kaplamaktadır. CMOS'lu devrede aynalama akımı bloğunun kutuplanması gerektiğinden bipolarlı yapıdan çok daha fazla güç harcamaktadır. Ayrıca biplarlı yapıda kullanılması gereken endüktans değeri de imal edilen CMOS'lu yapının gerektirdiği endüktans değerinden daha ufaktır. CMOS'lu yapının tüm bu dezavantajlarına rağmen üretime gönderilme nedeni ise elimizde var olan ölçüm cihazlarının GigaHertz değerlerini desteklemesidir ancak daha yüksek frekansta çalışılabileceği gösterilmiştir.



Şekil 5.13: 0.35μm n-kuyulu CMOS Devresi

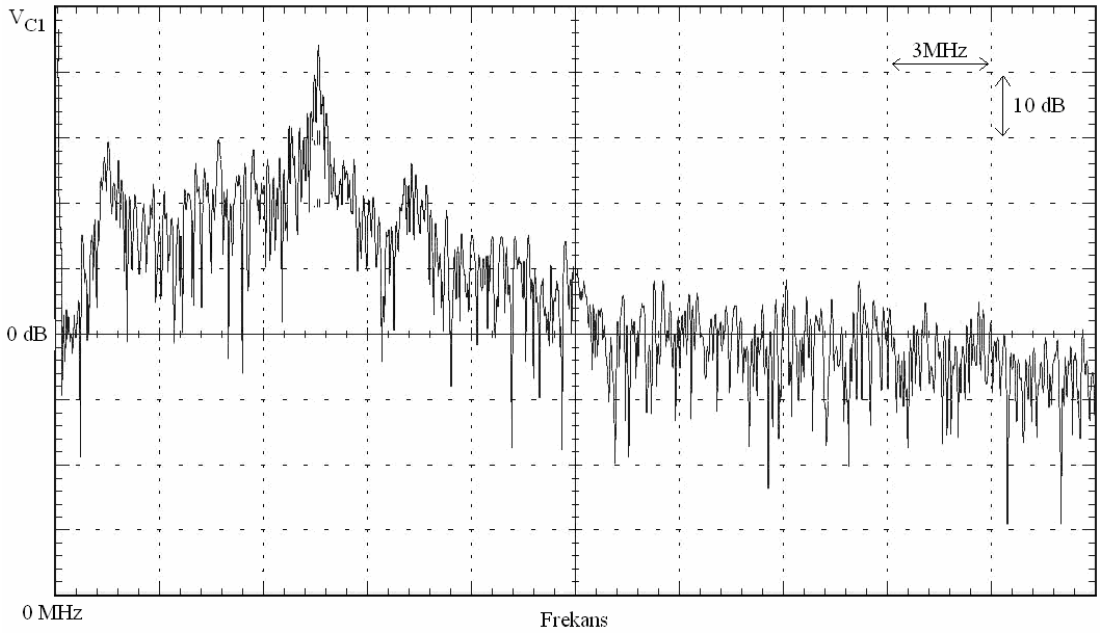
Üretilecek devrenin daha rahat kaosa sokulabilmesi için endüktansı dışardan bağlamak ve kutuplama akımlarınıda dışardan ayarlı bir şekilde vermek daha doğru bulunmuştur. Ayrıca endüktasın tümleşik olarak üretimi esnasında gerçekleşecek zorluklar böylece ortadan kalkmıştır. Bu doğrultuda tanıtılan devreye endüktans L=10μH olarak dışardan bağlanmış kutuplama akımları I_B=385μA, I_0=240μA olacak şekilde devreye akıtılmıştır ve imal edilen çipten Şekil 5.14'teki atraktör

karakteristiği ortaya çıkmıştır ve bu şekil teoride hesaplana Şekil 5.11 ile bire bir örtüşmektedir.



Şekil 5.14: Kaotik Atraktör V_{C2}-V_{C1} ile V_L

Seçilen kutuplama akımları sonucu parametreler d=1.9, c=0.149 değerlerine gelmiştir. Ayrıca ürettirilen 10 adet çipin kaotik yapılarının gürbüz olup olmadığı kontrol edilmiş ve üretilen tüm çipler Şekil5.14'te gösterilen karakteristiği sergilemiştir. Üretilen çipin frekans spektrumu ise Şekil5.15'te gösterilmektedir ve benzetimde de hesaplandığı gibi 15MHz'e kadar uzanan bir frekans aralığında devre kaos işareti üretmektedir.



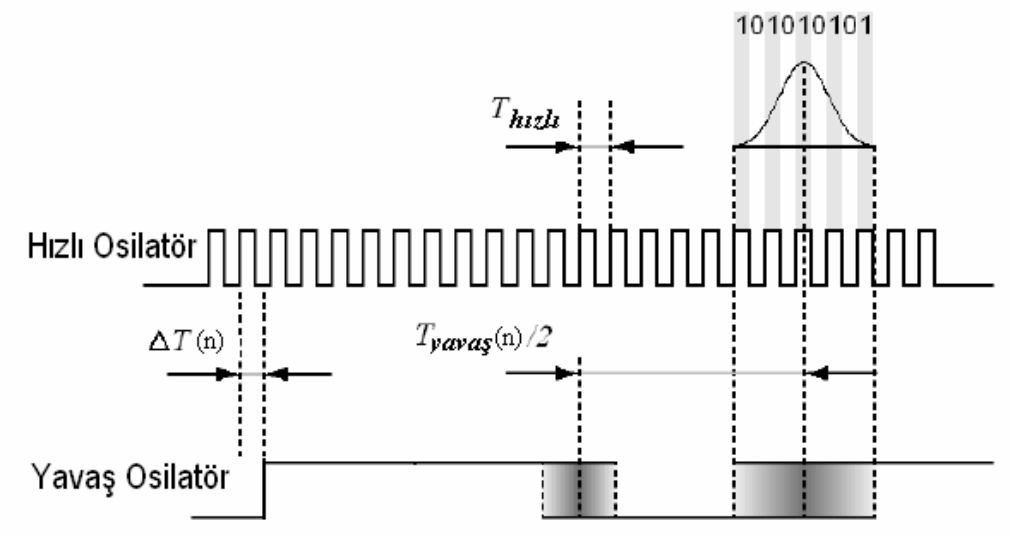
Şekil 5.15: Üretilen Devrenin V_{C1} Frekans Spektrumu

5.2. Kaos Tabanlı Rastgele Sayı Üreteci

Daha önceki kaotik sistem çalışmalarından esinlenerek [11,26,33,38,46-48] rastgele sayı üretimi için kaos tabanlı yapı tasarımı ele alınmıştır.

Literatürdeki birçok RSÜ yapısına bakıldığında entropi kaynağı olarak fiziksel gürültüden yararlanıldığı görülmektedir. Kaotik işaretlerin gürültü davranışına benzer düzensiz bir yapıya sahip olması ve zamanla çabuk kaybolan otokoralasyon fonksiyonlarından dolayı kaotik işaretlerin RSÜ yapılarında entropi kaynağı olarak kullanılan gürültü kaynaklarının yerine kullanılması düşünülmüştür.

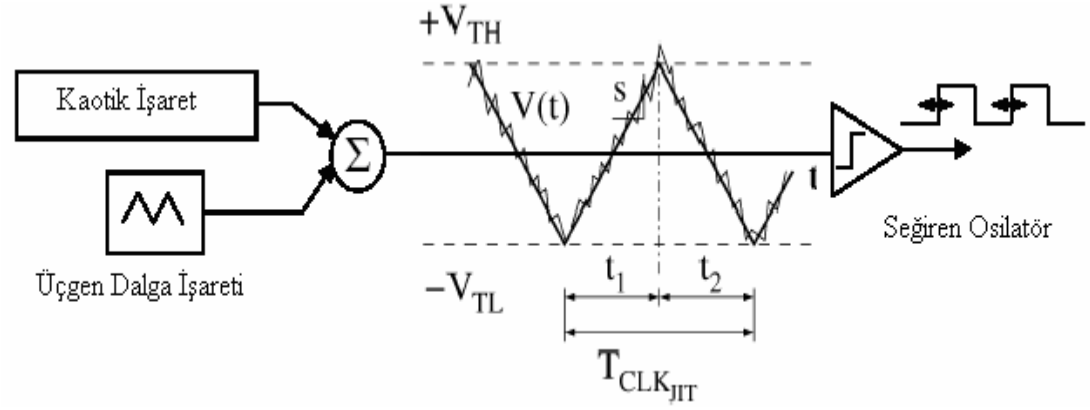
Bu bilgiler doğrultusunda kaos tabanlı rastgele sayı üreteci tasarımında Şekil 4.2'de yer alan rastgele sayı üretimi için osilatörün faz gürültüsünü kullanan ve literatürde iyi bilinen çift osilatörlü yapı [28] kullanılmıştır. Çift osilatörlü rastgele sayı üreteci tekniğine bakıldığında hızlı osilatör, yavaş osilatörün faz gürültüsündeki rastgeleliği kullanarak örneklenmektedir. D tipi flip-flopun saat girişine giren yavaş çalışan seğirmeli osilatörün yükselen kenarlarında hızlı osilatör örneklenmekte ve elde edilen çıkış bitleri rastgele davranış sergilemektedir. Bu yapının davranışı daha detaylı bir şekilde Şekil 5.16'da gösterilmiştir.



Şekil 5.16: Çift Osilatör Yapısının Girişi

Bu tekniğin kısıtlaması ise yavaş osilatördeki seğirme seviyesinin rastgele sayı üretimi için yetersiz olmasıdır. Literatürde seğirmeli yavaş osilatör tasarımlarına bakıldığında kuvvetlendirilmiş fiziksel gürültünün gerilim kontrollü osilatörüden geçirilmesi [28] veya gürültü eklenmiş üçgen işaretin karşılaştırıcıdan geçirilmesi ile

[32] gerçeklenen yapılar vardır. Ve bu yapılarla yavaş osilatördeki seğirme seviyesindeki yetersizlik ortadan kaldırılabilmektedir. Rastgeleliği düzelten bu iki yapı ele alınarak karşılaştırıldığında gerilim kontrollü osilatör, devre karmaşıklığını arttıracaktır. Büyük bir bant genişliğine sahip olan gürültü kaynağı işlenebilir bir düzeye getirilmesi için yüksek kazançlı kuvvetlendiriciye ihtiyaç duymaktadır. Ancak kuvvetlendirici tasarlarken kazanç artarken kuvvetlendiricinin bant genişliği daralacaktır. Bu yüzden gürültü işaretinin yüksek frekanstaki değerleri kuvvetlendirilemeyecek ve bu kayıplar rastgeleliği olumsuz etkileyecektir. Bu kısıtlama yüksek hızlı RSÜ üretimi için engeller oluşturacaktır. Ama kaotik işaretin genliği seçilen pasif eleman değerleriyle istenilen seviyeye ayarlanabileceğinden dolayı gürültü kaynağını güçlendirmeye yarayan kuvvetlendirici elemanına [28, 32] da gerek kalmamaktadır. Böylece fiziksel gürültü yerine daha önceden de belirttiğimiz gibi gürültünün yerini almasını beklediğimiz kaotik işaret kaynak olarak kullanılabilir.Bu yüzden tasarlanan devre için üçgen işaretli yapının kullanılması daha uygun görülmüştür ve tasarlanan yeni yapı Şekil 5.17'de gösterilmektedir.



Şekil 5.17: Seğirmeli Yavaş Osilatör Tasarımı

Tasarlanan yapıda seğirmeli yavaş osilatörün ana frekansı üçgen dalganın merkez frekansı ile belirlenirken, seğirme ise üçgen dalgaya eklenen kaotik işaret sayesinde oluşturulur. Bu tasarımda seğirmeli yavaş osilatörü gerçeklerken kaotik işaretin genliği eleman değerleri uygun seçilerek yeterince büyük yapılabildiğinden, fiziksel gürültüde gereken kuvvetlendiriciye [32] veya seğirmeyi arttırmak için kullanılan VCO' ya [28] gerek duymamaktadır.

5.2.1. Kaos Tabanlı Rastgele Sayı Üretecinin Modellenmesi

Bu bölümde kaos tabanlı rastgele sayı üretecinin tasarımı nümerik metotlar kullanılarak anlatılmıştır. Şekil 4.2'deki hızlı ve yavaş osilatörden oluşan yapının matematiksel modellenin analizi özellikle hızlı osilatörün yavaş osilatöre oranı arttıkça çok zaman gerektiren modellemelere dönüşmüştür. Bu yüzden Şekil 4.2'deki karakteristiği gerçekleyen başka bir matematiksel model geliştirilmiştir. Bu yapının matematiksel modeline bakmak gerekirse Şekil 5.16'daki zaman diyagramında görüldüğü gibi $\Delta T(n)$ iki osilatör arasındaki faz farkını göstermektedir. Matematiksel ifadeyle, $T_{yavaş}(n)$ seğirmeli yavaş osilatörün periyotlarını ve $T_{hızlı}$ da hızlı osilatörün periyodunu belirtmek üzere yeni model

$$\Delta T(n) = (\Delta T(n-1) + T_{yavaş}(n)) \bmod T_{hızlı} \qquad \textbf{(5.7)}$$

olarak denklem 5.7'deki gibi açıklanabilir.

Böylece çift osilatörlü yapı modüler aritmetik kullanılarak kolayca gösterilebilir. Örnekleme sonucu oluşan b_n çıkışı da (5.8)'de gösterilmiştir.

$$b_n = \left\{ \begin{array}{l} 1\ ,\ \Delta T(n) < T_{hızlı}/2 \\ 0\ ,\ \Delta T(n) \geq T_{hızl}/2 \end{array} \right\} \qquad \textbf{(5.8)}$$

Bu modelleme gerçeklenirken kaliteli çıkış bitleri elde edebilmek için hızlı osilatörün %50'lik mükemmel bir işaret oranına sahip olması gerekir.

RSÜ'yü tasarlamak için önce denklem 5.2'deki diferansiyel denklem nümerik olarak gerçeklenmiş sonra genliği ve frekansı ayarlanabilen üçgen dalga ile toplanarak Şekil 5.17'deki yapı tasarlanmış böylece seğirmeli yavaş osilatör modellenmiştir. Daha sonra denklem 5.7 ve 5.8 kullanılarak çıkış bitlerini oluşturulmuştur. Bu modellerle tasarlanan RSÜ başarılı bir şekilde gerçeklenmiştir.

5.2.2. Modellin Nümerik Analizleri

Önceki çalışmalarda yapılan analizler ve çift osilatör yapısından elde edilmiş bilgiler [17,28,32] doğrultusunda RSÜ devresinin karakteristiğini etkileyen 5 etken ortaya çıkmaktadır. Bunlar:

1) Kaotik sistemin parametreleri {b, c, d, K, m}.
2) Yavaş osilatörün hızlı osilatöre oranı ($T_{yavaş}$ / $T_{hızlı}$).

3) Kaotik işaretin genliğinin üçgen işarete oranı. Bu oran modüle edilmiş yavaş osilatörün standart sapmasını($\sigma_{yavaş}$) belirler.

4) Kaotik işaretin frekansının yavaş osilatöre oranı. Bu oranda kaotik işaretin frekansı spektrum analizinde tepe yaptığı nokta $f_{0,kaos}$ kaos işaretinin frekansı olarak seçilir ve bu oran $f_{0,kaos}$ / $f_{yavaş}$ olarak gösterilir. Bu değer RSÜ çıkış hızı için üst sınırı belirlemektedir.

5) Hızlı osilatörün işaret oranının dengesi. Bu dengesizlik RSÜ çıkışındaki bitlerin kutuplanmasına neden olmaktadır.

RSÜ için en uygun tasarımın bulunması için devrenin tasarımında kritik görülen ve yukarda belirtilen 5 etken modellemede parametrik olarak taratılmış ve bit çıkışları elde edilmiştir. Bu sonuçlar rastgelelik seviyesinin belirlenmesinde kullanılan denklem 5.9'de belirtilen poker testine [49] tabi tutularak sonuçlar elde edilmiştir.

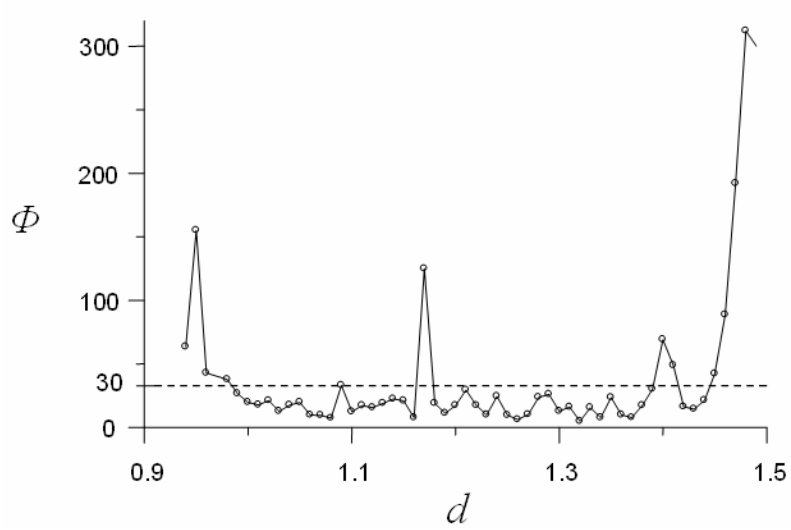
$$\phi = \frac{2^m}{k}\left(\sum_{i=1}^{2^m} n_i^{\,2}\right) - k \qquad \textbf{(5.9)}$$

Devreden N bit veri toplanmaktadır. Bu veri m bit uzunluklu verilere ayrıştırılarak birbirleriyle çakışmayan k adet dizi oluşturulur. n(i) değeri ise N sayılı veri dizisinde $1 \le i \le 2^m$ koşulunda yer alan i değerlerinin bulunma olasılığını göstermektedir. ϕ değeri ise standart χ^2-testinde N veri dizisinde m bit uzunluklu sayıların dağılımını göstermektedir. FIPS–140–2 testi doğrultusunda $N=20000$, $m=4$ ve $k=N/m=5000$ seçildiğinde testin geçer seviyede yer alması için $\phi < 46.17$ koşulunun sağlanması gerekmektedir. Ancak bu çalışma boyunca eşik değeri daha zor bir seviye olan ϕ <~30 koşuluna göre analiz edilmiştir.

Nümerik analizler boyunca aksi söylenmediği taktirde tüm analizlerde kaotik osilatör parametreleri b=0.26, c=0.146, d=1.2, K=8, m=1 ve Şekil4.2'deki çift osilatör yapısı içinde parametreler $T_{yavaş}/T_{hızlı}$=100, $f_{0,kaos}=4f_{yavaş}$, $\sigma_{yavaş}$=6 $T_{hızlı}$ ve $T_{yavaş}=1/f_{yavaş}$= 25 zaman birimi olarak seçilmiştir.

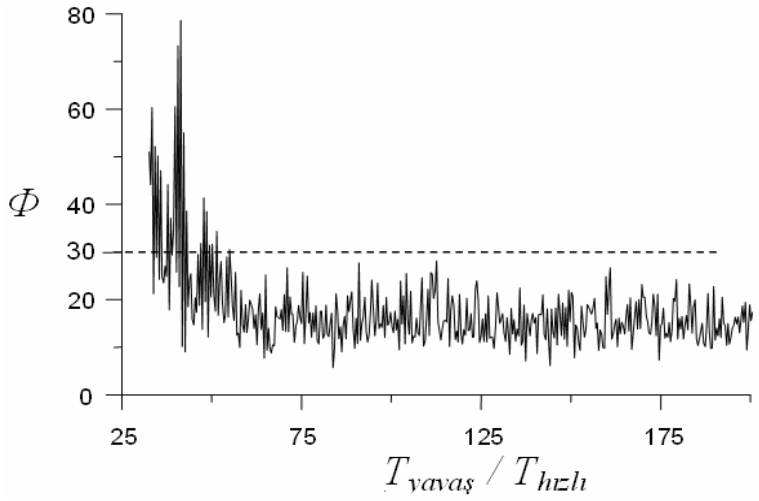
Şekil5.18'de ϕ = 30 seviyesi ile RSÜ devresinin çıkışının d parametresine göre davranışı gösterilmektedir. Şekilde5.18'de yüksek tepe yapan noktalar ile Şekil5.7'deki dallanma diyagramında periyodik olan alanlar yani kaotik devrenin kaostan çıktığı yerlerdeki d parametrelerinin örtüştüğü görülmektedir. Burdanda

anlaşılıyor ki devre kaosta olmadığı zaman RSÜ devresinin istatistiksel başarımı zayıf, diğer koşullarda ise başarılı olduğu görülmektedir.



Şekil 5.18: RSÜ Devresinin d Parametresine Göre Benzetim Sonuçları

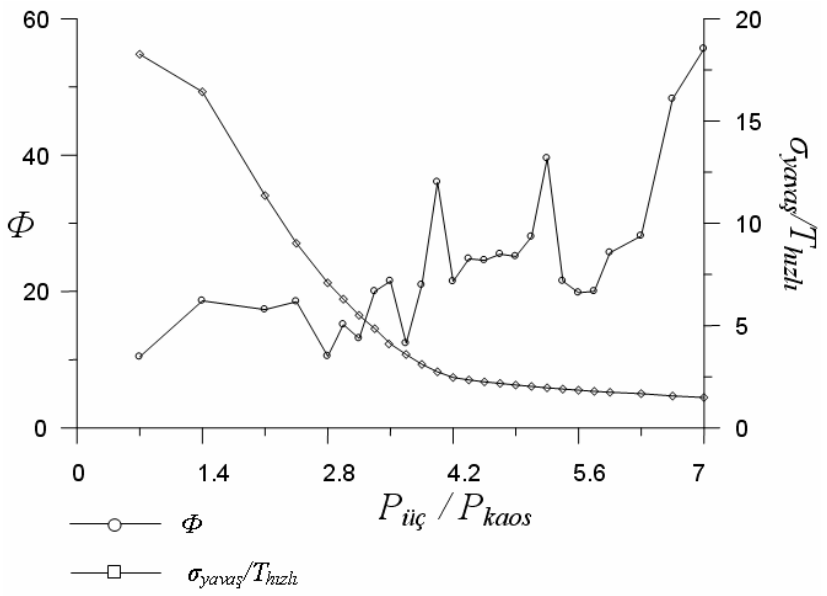
RSÜ devresinin yavaş osilatörün hızlı osilatöre oranına göre performansı ise Şekil 5.19'da gösterilmektedir.



Şekil 5.19: RSÜ Devresinin $T_{yavaş}$ / $T_{hızlı}$ Parametresine Göre Benzetim Sonuçları

Nümerik analiz doğrultusunda istenilen seviyede çıkış elde edebilmek için $T_{yavaş}$ / $T_{hızlı}$ oranının 60'tan büyük olması gerekmektedir. Bu oran ne kadar düşürülebilir ise o kadar hızlı çalışan RSÜ'leri tasarlamak mümkün olacaktır. Çünkü RSÜ'lerinin çalışma hızını yavaş osilatör belirler ve $T_{yavaş}$ / $T_{hızlı}$ oranı ne kadar az olursa daha yüksek frekanslarda çalışan yavaş osilatörler devrede kullanılabilir. Bu konular hakkında yapılan çalışmalarda entropi kaynağı fiziksel gürültü olan devrelerde [17, 28] ideal oran 100 olarak önerilmektedir.

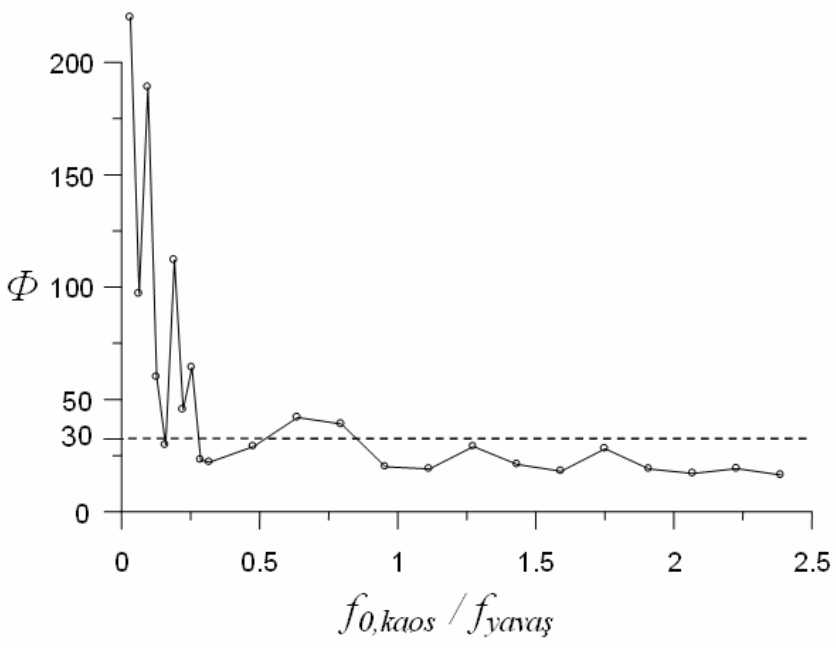
Kaotik işaretin genliğinin üçgen işaretin genliğine oranına göre RSÜ'nün rastgelelik performansı ise Şekil5.20'de gösterilmektedir.



Şekil 5.20: RSÜ Devresinin $P_{üç}$ / P_{kaos} ve $\sigma_{yavaş}$ / $T_{hızlı}$ Parametresine Göre Benzetim Sonuçları

Bu hesaplama boyunca kaotik işaretin genliği sabit tutularak üçgen işaretin genliği taratılmıştır. Aynı grafikte yavaş osilatörde oluşacak standart sapmaya da ($\sigma_{yavaş}$) yer verilmiştir. Bu doğrultuda kaotik işaretin genliği sabitken üçgen işaretin genliği arttırıldığında standart sapma ($\sigma_{yavaş}$) değerinin azaldığı görülmektedir. $P_{üç}$ / P_{kaos} >3 veya $\sigma_{yavaş}$ / $T_{hızlı}$ <5 koşullarında ϕ değeri yükselme eğilimi göstermekte ve RSÜ devresinin istatistiksel başarımı azalmaktadır. Bu yüzden başarımı iyi bir RSÜ tasarlayabilmek için $\sigma_{yavaş}$ / $T_{hızlı}$ > 5 koşulunu sağlayan bir tasarım yapmak gerekir ki bu değer [28]'deki makalede de 10–20 arası olarak önerilmiştir.

$f_{0,kaos}$ / $f_{yavaş}$ oranının RSÜ üzerine etkisini görebilmek için ise bu oran 0.01 ile 3.3 arasında taratılmıştır. Bu taratma esnasında $f_{yavaş}$ değeri sabit tutulurken $f_{0,kaos}$ değeri değiştirilmiştir. Sonuçlar Şekil 5.21'de gösterilmektedir. Şekilden de anlaşılacağı üzere $f_{0,kaos}$ > $f_{yavaş}$ koşulu sağlandığı sürece ϕ değeri 30'un altında kalmakta ve RSÜ başarılı çalışmaktadır. RSÜ devresinin hızını yavaş osilatörün hızı belirlediğinden ve iyi bir rastgelelik sonucu elde edilmesi gerektiğinden bulunan sonuç doğrultusunda kaotik işaretin bantgenişliği RSÜ için bir üst sınır belirlemektedir.

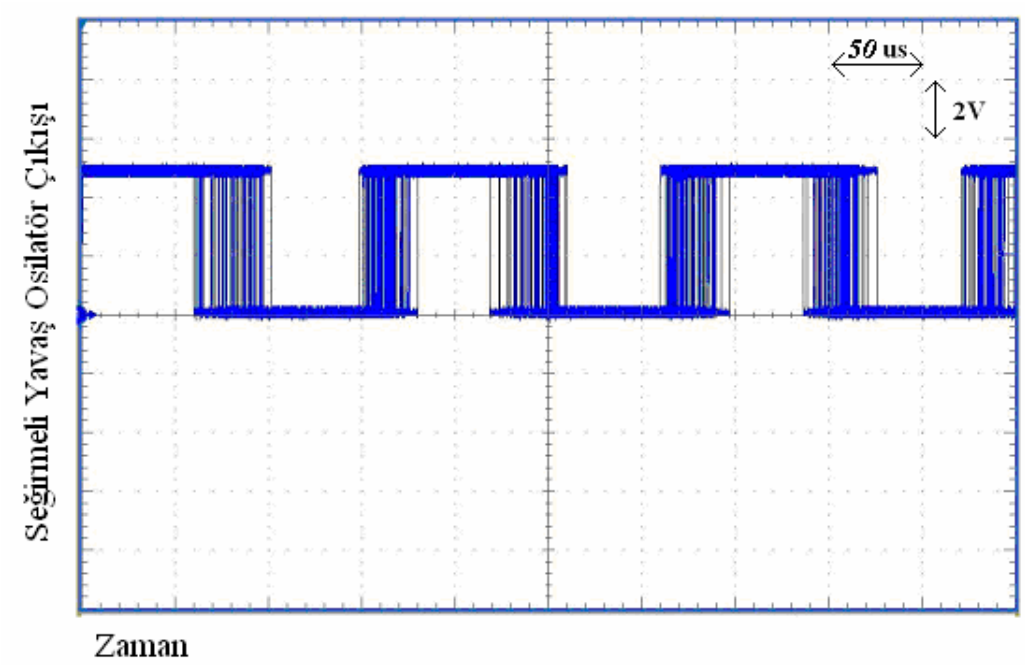


Şekil 5.21: RSÜ Devresinin $f_{0,kaos}$ / $f_{yavaş}$ Parametresine Göre Benzetim Sonuçları

Ayrıca çift osilatör tabanlı RSÜ devrelerinin performansı için hızlı osilatörün işaret oranının çok belirleyici olduğu iyi bilinmektedir. Eğer bu oran düzgün bir şekilde %50 olarak ayarlanmazsa RSÜ yapısının çıkışlarından elde edilecek verilerde kutuplanma meydana gelecektir ki bu kutuplanmada rastgeleliği bozmaktadır. Bu tarz kutuplanma etkilerini yok edebilmek için literatürde genelde Von Neumann [50] algoritması kullanılmaktadır. Bu algoritmanın elektronik olarak adapte edilebilmesi için ise Şekil4.2'de önerilen D-tipi flip-flop yerine T-tipi flip-flopun [32] kullanılması yeterli olacaktır. Böylece Von Neumann algoritmasının çalıştırıldığı bir işlemciye gerek kalmamakta ve bu işlemin çıkış sonucunu etkileyen yavaşlatıcı etkileri de ortadan kalkmaktadır.

Yapılan nümerik analizlerle RSÜ yapısı için en uygun değerler belirlenerek tasarım gerçeklenmiştir. Bu aşamada yüksek hızlarda veri toplama imkanı mevcut olmadığından Şeki5.2'deki kaotik devre, Şekil 5.17 ve Şekil 4.2'deki bloklar ayrık elemanlar kullanılarak gerçeklenmiş ve daha düşük frekansta çalışan rastgele sayı üretecinden veri toplanmıştır. Şekil 5.2'deki kaotik devresi ayrık elemanlarla gerçeklenirken MOS yapıları National Instrument'ın CD4007 eşlenik transistor çiftiyle gerçeklenirken pasif eleman değerleri L=10μH, C=4.7nF, R=430Ω olarak seçilmiş kutuplama akımları da I_B=860μA, I_0=100μA olarak ayarlanmıştır. Seçilen bu değerlerle ayrık yapıda kurulan kaotik devre kaosa girmiştir. Şekil 5.17'deki bloğu gerçeklerken toplama işlemi için Analog Devicen'in AD844 kuvvetlendiricisi

kullanılırken karşılaştırma işlemi National Instrument'ın LM311 elemanı ile gerçeklenmiştir. Kaotik işaret $f_{0,kaos}$ değeri 24KHz olarak ölçülmüştür. Yukarda elde edilen tasarım kriterlerinden $f_{0,kaos} > f_{yavaş}$ koşulu gereği 24KHz yavaş osilatörün ve buna bağlı olarak RSÜ devresinin çıkış hızının üst limitini oluşturmaktadır. RSÜ devresinden elde edilen bit dizisinin kaliteli bir rastgelelik gösterebilmesi için 6KHz'lik yavaş osilatör frekansı uygun görülmüştür. Seğirmeli yavaş osilatörün çıkışından elde edilen işaret formu Şekil5.22'de gösterilmektedir. Bu işaret formundan yavaş osilatörün standart sapması 15μs olarak ölçülmüştür ki bu değer hızlı osilatörün periyodunun 5.42 katı kadarlık bir zaman dilimini içermektedir ve $\sigma_{yavaş} / T_{hızlı} > 5$ koşulunu sağlamaktadır. Hızlı osilatörün merkez frekansı 360KHz seçilerek $T_{yavaş} / T_{hızlı}$ oranı seçilebilecek en küçük ve en iyi değer olan 60'a ayarlanmıştır. Bu koşullar eşliğinde RSÜ yapısı en uygun değerlere ayarlanmıştır.



Şekil 5.22: Seğirmeli Yavaş Osilatörün Çıkış İşaret Formu

RSÜ devresinin istatistiksel kalitesinin belirlenmesi için üretilen bit dizisi PCI veri toplama kartı ile bilgisayara aktarılarak NIST'in FIPS-140-2 [49] ve NIST-800-22 [13] testlerine tabi tutulmuştur. Testler için 70Mbit veri toplanmıştır. FIPS-140-2 testi için toplana veri 20000 bit uzunluklu 3500 bloğa ayrılarak 4 basit teste (monobit,poker,runs,long run) sokulmuş ve tüm bloklar testte başarılı bulunmuştur.

NIST-800-22 testi için toplanan veri 100000 bit uzunluklu 700 bloğa ayrılarak tam NIST testine sokulmuştur. Bu testin sonucu Tablo5.1'de görülmektedir. Bu tabloda

uygulanan testlerin adları ilk sütunda yer almaktadır. Her test herbir bloğa uygulanmakta ve 700 adet p-değeri elde edilmektedir. P-değeri 0-1 arası bir dağılım göstermekte ve bu testin başarılı olabilmesi için gereken alt sınır 1/blok sayısı=0.00142'dir. P-değeri 0.00142'den büyük olan blokların dağılımı ise son sütunda yer almaktadır. Test sonuşlarına bakıldığında ise oluşturulan sayıların NIST testinden geçtiği ve rastgele sayı davranışı sergiledikleri görülmektedir.

Tablo 5.1: NIST–800–22 Test Sonuçları

İstatistik Testler	P-değeri İstikrarı	Başarılı Blokların Dağılımı
Block-frequency	0.004581	0.9800
Linear-complexity	0.176657	0.9862
Runs	0.853761	0.9843
Fft	0.020724	0.9862
Apen	0.005193	0.9829
Serial	0.739918	0.9871
Serial	0.138408	0.9971
Cumulative-sums	0.839261	0.9957
Cumulative-sums	0.690492	0.9986
Longest-run	0.009535	0.9814
Frequency	0.453247	0.9957
Rank	0.364541	0.9929
Universal	0.061841	0.9875
Overlapping-templates	0.002700	0.9786
Nonperiodic-templates	0.030515	0.9757

6. SONUÇ

Bu tezin amacı, girişinde sürekli zaman çift sarmallı kaotik osilatörden elde edilen işaret ile kaotik işaret tabanlı yeni bir gerçek rastgele sayı üreteci (GRSÜ) tasarlamaktır. Tezde parametreleri kontrol edilebilen türden yeni bir negatif-gm LC kaotik osilatör yapısı tanıtılmıştır. Bu yapını değişik parametrelerde benzetimleri ve deneysel sonuçlar incelenmiş bipolar teknolojisi ile daha yüksek frekanslarda gerçeklenebileceğini gösterilmiştir. RSÜ için literatürde iyi bilinen çift osilatör yapısının kullanılması önerilmiştir. Çift osilatörlü yapıda entropi kaynağı olarak negatif-gm LC kaotik osilatörden elde edilen kaotik işaret kullanılarak RSÜ tasarımı gerçeklenmiştir. RSÜ için önemli parametrelerin etkileri tasarlanan nümerik modellerle incelenmiş ve kaliteli rastgele sayı elde edebilmek için optimum değerler belirlenmiştir. Bu değerler doğrultusunda entropi kaynağı çipten diğer tasarım kısmı ayrık elemanlardan oluşan RSÜ oluşturulmuştur.

Bu tasarımı kullanarak literatürde daha önce önerilen devrelerde gereksinim olan fiziksel gürültüyü kuvvetlendirmede kullanılan büyük kazançlı geniş bantlı kuvvetlendirici [17] ve seğirme dağılımını düzenleyen VCO elemanına [28] gerek kalmadan rastgele sayı üreteci gerçeklenmesi sağlanmıştır.

Sonuç olarak tasarlanan devreden elde edilen bit dizileri rastgele sayı testleri FIPS-140-2 ve NIST-800-22'ye sokulmuş ve bu testlerden başarıyla geçmiştir. Ayrıca bu çalışmada tasarlanan GRSÜ' nün çıkışı herhangi bir algoritmaya gerek duymadan rastgeleliği sağlamıştır. Böylece yeni bir kaos tabanlı RSÜ tasarımı gerçeklenmiştir.

KAYNAKLAR

[1] **Rankl, W. ve Effing, W.,** 2000. Smart Card Handbook, *John Wiley&Sons*, New York.

[2] Cryptography, 2008. *http://en.wikipedia.org/wiki/Cryptography*

[3] **Schneier, B.,** 1996. Applied Cryptography, *John Wiley&Sons*, New York **.**

[4] **Stinson, D. R.,** 1995. Cryptography Theory and Practice, **CRC Press Inc**., London.

[5] **Rhee, M. Y.,** 1994. Cryptography and Secure Communications, *McGraw-Hill Series*, Singapore.

[6] **Hellman, M. E.,** 2002. An Overview of Public Key Cryptography, *IEEE Communications Magazine*, Volume **40**, Issue 5, Page(s):42 – 49.

[7] **Salomaa, A.,** 1990, Public-Key Cryptograpy, *Springer-Verlag*, Heidelberg, Berlin.

[8] The Mathematical Guts of RSA Encryption**,** 2008. *http://world.std.com/~franl/crypto.html*

[9] **Aslan, B.,** 1999. Sayısal İmza Sistemlerinin İncelenmesi (Digital signature schemes), *Yüksek Lisans*, İTÜ, İstanbul.

[10] RSA Laboratories FAQ on Cryptography, Chapter 3 Techniques in Cryptograpyh, *http://www.rsa.com/rsalabs/node.asp?id=2152*

[11] **Yalçın M., Suykens J. ve Vandewalle J.,** 2004. True Random Bit Generation from a Double Scroll Attractor, *IEEE Trans. Circuits Syst. I*, **51**, 1395-1404.

[12] Random, 2008. *http://www.random.org/randomness/*

[13] National Institute of Standard and Technology, A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications, NIST800-22, 2001. *http://csrc.nist.gov/rng/SP800-22b.pdf*

[14] Hardware Random Number Generator, 2008. *http://en.wikipedia.org/wiki/Hardware_random_number_generator*

[15] Linear Congruential Random Number Generator, 2008. *http://www.cse.msu.edu/~nandakum/nrg/Tms/Probability/Probgenerator.htm*

[16] **Kocarev L. ve Jakimoski G.,** 2003. Pseudorandom Bits Generated by Chaotic Maps, *IEEE Trans. Circuits and Systems I,* **50**, 123-26.

[17] **Petrie C. ve Connelli J.,** 2000. A Noise-Based IC Random number Generator for Applications in Cryptography, *IEEE Trans. Circuits and Systems I,* **47**, 615-621.

[18] **Stephen K.,** 1998. In the Wake of Chaos: Unpredictable Order in Dynamical Systems (Chicago, University of Chicago Press, 1993), *The Case of Chaos, in Mathematics Teacher Magazine*, Crayton Bedford

[19] **Williams G. P.,** 1997. Chaos Theory Tamed, *Joseph Henry Press*, Washington, D.C.

[20] **Gleick J.,** 1987. Chaos : Making a New Science, *Viking Press*, New York

[21] Chaos Theory, 2008. *http://en.wikipedia.org/wiki/Chaos_theory*

[22] **Strogatz S.,** 2001. Nonlinear Dyanamics and Chaos, *Westview Press,* Cambridge.

[23] **Delgado-Restituto M. ve Rodriguez-Vazquez A.,** 2002. Integrated Chaos Generators, *Proc. of IEEE*, vol. **90**, no. 5, pp. 747-767.

[24] **Juncu V.D., Rafiei-Naeini M. ve Dudek P.,** 2006. Integrated Circuit Implementation of a Compact Discrete-Time Chaos Generator, *Journal Analog Integrated Circuits and Signal Processing* , Vol **46**, No 3 , pp.275-280.

[25] **Chua L., Wu W., Huang A. ve Zhong G.,** 1993. A Universal Circuit for Studying and Generating Chaos-Part I: Routes to Chaos, *IEEE Trans. Circuits and Systems I,* **40**, 732-744.

[26] **Gerosa A., Bernardini R., ve Pietri S.,** 2002. A Fully Integrated Chaotic System for the Generation of Truly Random Numbers, *IEEE Trans. Circuits and Systems I*, vol. **49**, no. 7, pp. 993-1000.

[27] **Weiland S.,** 2005. Chaos in the Chua Circut, *Project for the Course on Dynamical Systems*, Technische Universiteit Eindhoven, Eindhoven.

[28] **Jun B. ve Kocher P.,** 1999. The Intel Random Number Generator, *White Paper Prepared for Intel Corporation*, *http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.*

[29] **Holman W. T., Connelly J. A., ve Downlatabadi A. B.,** 1997. An Integrated Analog/Digital Random Noise Source, *IEEE Trans. Circuits and Systems I*, vol. **44**, no. 6, pp. 521-528.

[30] **Petrie, C.S., Connelly, J.A.,** 1996. Modeling and Simulation of Oscillator-Based Random Number Generators. *Proc. IEEE International Symp. Circuits and Systems (ISCAS)*, Vol. 4, pp. 324-327.

[31] **Motchenbacher C. D. ve Connelly J. A.,** 1993. Low-Noise Electronic System Design, *John Wiley&Sons* ,New York.

[32] **Bucci M., GermaniL., LuzziR., Trifiletti A., ve Varanonuovo M.,** 2003. A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC, *IEEE Trans. Comput*., vol. **52**, pp. 403- 409.

[33] **Drutarovsky M. ve GalajdaP.,** 2006. Chaos-Based True Random Number Generator Embedded in a Mixed-Signal Reconfigurable Hardware, Journal of Electrical Engineering, Vol. **57**, No. 4, 218–225.

[34] **Dudek P., ve Juncu V.D.,** 2005. An area and power efficient discrete-time chaos generator circuit, *Circuit Theory and Design, Proceedings of the 2005 European Conference*, Volume 2, Issue , 28 Aug.-2 Sept. Page(s): II/87 - II/90 vol. 2.

[35] **Özoğuz S., Elwakil A.S., ve Ergün S.,** 2006. Cross-coupled Chaotic Oscillators and Application to Random Bit Generation, *IEE Proc. Circuits Devices Syst*., vol. 153, no. 5, pp. 506-510.

[36] **Bucci M., Germani L., Luzzi R., Tommasino P., Trifiletti A. Ve Varanonuovo M.,** 2003. A High-Speed IC Random-Number Source for SmartCard Microcontrollers, *IEEE Trans. Circuits and Systems I,* **50**, 1373-1380.

[37] **Kolumban G., Kennedy M.P., ve Chua L.O.,** 1997. The role of synchronization in digital communications using chaos. I. Fundamentals of digital communications, IEEE Trans. Circuits Syst. I, 44, pp. 927-935.

[38]**Callegari S., Rovatti R., ve Setti G.,** 2005. Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos, IEEE Trans. Signal Process., 53, pp. 793-805.

[39] **Cruz J.M. ve Chua L.O.,** 1993. An IC chip of Chua's circuit, IEEE Trans. Circuits Syst. II-Analog & Digital Signal Processing, 40, pp. 614–625.

[40] **Gonzales O. A., Han G., de Gyvez P., ve Sinencio E.S.,** 2000. Lorenz-based chaotic cryptosystem: a monolithic implementation, IEEE Trans. Circuits Syst. I, 47, pp. 1243-1247.

[41] **Elwakil A.S., ve Kennedy M.P.,** 2001. Construction of generic classes of chaotic oscillators using passive-only nonlinear devices, IEEE Trans. Circuits Syst. I, 48, pp. 289-307.

[42] **Elwakil A.S., ve Kennedy M.P.,** 2000. Chua's circuit decomposition: A systematic design approach for chaotic oscillators, J. Franklin Inst., 337, pp.251–265.

[43] **Delgado-Restituto M., ve Rodriguez-Vazquez A.,** 1998. Design considerations for integrated continuous-time chaotic oscillators, IEEE Trans. Circuits Syst. I, 1998, 45, pp. 481-495.

[44] **Tavas V., Demirkol A.S., Özoğuz S., Zeki A., ve Toker A.,** 2008. An Integrated Cross-Coupled Chaos OscillatorApplied to Random Number Generation, IET Circuits,Devices and Systems, Hakem değerlendirmesinde.

[45] **Craninckx J., ve Steyaert M.,** 1997. A 1.8-GHz low-phase-noise CMOS VCO using optimised hollow spiral inductors, IEEE J. Solid-State Circuits, 32, pp. 726–744.

[46] **Delgado-Restituto M., Medeiro F., ve Rodriguez-Vazquez A.,** 1993. Nonlinear Switched-current CMOS IC for Random Signal Generation, Electron. Lett., 29, pp. 2190-2191.

[47] **Addabbo T., Alioto M., Fort A., Rocchi S., ve Vignoli V.,** 2006. 'A feedback strategy to improve the entropy of a chaos-based random bit generator, IEEE Trans. Circuits Syst. I. ,53, pp. 326-337.

[48] **Ergün S., ve Özoğuz S.,** 2007. 'A Chaos-Modulated Dual Oscillator-Based Truly Random Number Generator', in Proc. 2007 IEEE Int. Symp. Circuits Syst., New Orleans, U.S.A. , pp. 2482-2485.

[49] Security Requirements for Cryptographic Modules. Federal Information Processing Standards Publication 140-2, U.S. Department of Commerce/NIST, 1999. http://www.nist.gov.

[50] **Von Neumann J.,** 1951. Various Techniques Used in Connection With Random Digits, Applied Math Series., Notes by G.E. Forsythe, In National Bureau of Standards, 12:36-38.

ÖZGEÇMİŞ

Koray Özdemir, 1984 yılında Kayseri'de doğdu. Lise öğrenimini 2002 yılında İstanbul Hüseyin Avni Sözen Anadolu Lisesinde, lisans öğrenimini ise 2006 yılında İstanbul Teknik Üniversitesi Elektronik Mühendisliği bölümünde tamamladı. Aynı yıl, İ.T.Ü. Fen Bilimleri Enstitüsü Elektronik Mühendisliği programında yüksek lisans eğitimine başladı. 2006 yılından beri, Gömülü Sistemler Laboratuarında proje görevlisi olarak çalışmaktadır.