Tümleştirmeye Uygun Kaotik Osilatör Tabanlı Rastgele Sayı Üreteci

Vedat Tavas[1], Ahmet Şamil Demirkol[1], Selçuk Kılınç[2], Serdar Özoğuz[1], Ali Toker[1], Ali Zeki[1]

[1]Elektronik ve Haberleşme Mühendisliği Bölümü, İstanbul Teknik Üniversitesi, İstanbul

[1]e-posta: (tavas, demirkola, ozoguz, tokeral, zekia)@itu.edu.tr

[2]Elektronik-Elektronik Mühendisliği Bölümü, Dokuz Eylül Üniversitesi, İzmir

[2] e-posta: selcuk.kilinc@deu.edu.tr

Özet

Bu çalışmada tamamen tümleştirmeye uygun gerçek rastgele sayı üreteci (GRSÜ) devresi tasarlanmıştır. Tasarımda osilatör örnekleme yöntemi kullanılmıştır. RSÜ yapısında gerçek rastgeleliği sağlamak amacıyla belirsizlik kaynağı olarak sürekli zamanlı kaotik devre kullanılmıştır. Kaotik devre negatif-gm LC osilatör tabanlıdır. Kaotik işaret multivibratör kullanılarak seğirmeli kare dalga işarete çevrilmitir. Ardından darbe boşluk oranı 1 olan yüksek hızlı kare dalga işareti, seğirmeli kare dalga ile örneklenerek rastgele bit dizisi oluşturulmuştur. Örnekleme için D tipi flip-flop devresinden faydalanılmıştır. Devrenin bit üretim hızı 2Mbit/s'dir. Tasarımda 0.35µm CMOS teknoloji parametreleri kullanılmıştır. Tasarımı yapılan devrenin serimi çizilmiş ve serim sonrası analizleri yapılmıştır. Tasarlanan devre ±1.65V simetrik kaynakla beslenmektedir. Devre 0.25mm^2 kırmık alanı kaplamaktadır ve harcadığı güç 35mW'tır. Devre üretime yollanmıştır. Üretimden dönen örneklerle yapılacak deneylerin sonuçlarının konferans zamanına kadar yetişmesi durumunda, sonuçların konferansta sunulması hedeflenmektedir.

Abstract

In this work a true random number generator (TRNG) which is fully compatible for integration is designed. Oscillator sampling method is used in the design. Continuous time chaotic circuit is used in RNG to get full-truly randomness. Chaotic circuit is based on negative-gm LC oscillator. Chaotic signal changed to jittered square wave by voltage controlled oscillator and random bit string is done by sampling a fast square wave signal which has a mark space ratio is 1 with the jittered square wave. D type flip-flop is utilized for sampling. Throughput of the circuit is 2Mbit/s. 0.35µm CMOS technology parameters are used in the design. Layout of the designed circuit is drawn and post-layout analysis is done. Designed circuit powered by ±1.65V symmetric supply. Circuit area is 0.25mm^2 and power consumption is 35mW. Circuit was sent to fabrication. If results of experiments done with the fabricated chips reach to the conference, they will be presented in the conference.

Bu çalışma Türkiye Bilimsel ve Teknolojik Araştırma Kurumu TÜBİTAK tarafından desteklenmektedir.(Proje numarası 106E093.)

1. Giriş

Son yıllarda kaotik devreler rastgele sayı üreteçlerinde belirsizlik kaynağı olarak kullanılmaya başlanmıştır [1-4]. Tasarlanan devrelerin tümleştirmeye uygun olmaları, düşük güç harcamaları, yüksek frekanslarda ve düşük gerilimlerde çalışabilmeleri kullanım alanlarını genişletmektedir.

Bu çalışmada klasik negatif-gm LC osilatörden [5] türetilmiş bir kaotik devreyi belirsizlik kaynağı olarak kullanan gerçek rastgele sayı üreteci önerilmiştir. Sürekli zamanlı kaotik devrenin tasarımı [6]'da verilmiş ve bu devrenin üretilmiş halinin sonuçları [7]'de gösterilmiştir. Kaotik devre 50MHz'lere kadar salınım yapabilmektedir ve tamamen tümleştirmeye uygundur. Devrenin kaotik çalışma aralığını genişletmek için devre 15MHz merkez frekansında salınım yapacak şekilde düzenlenmiştir.

Ayrık zamanlı kaotik devreler RSÜ yapılarında kullanılmaktadır [1-3]. Son zamanlarda sürekli zamanlı kaotik devreler de RSÜ yapılarında kullanılmaya başlanmıştır [4]. Yüksek hızlı bit dizisi elde etmek için yüksek frekanslarda çalışan devreler kullanılmalıdır. Burada önerilen devrenin rasgele sayı üreteçlerinde kullanılabileceği deneysel olarak gösterilmiştir [7]. Bu devreden ortalama 2Mbit/s hızında veri elde edilmektedir. Bu bit dizisinin NIST-800-22 [8]'de verilen rastgele sayı testlerini geçtiği gösterilmiştir [7].

Burada ilk olarak kaotik devrenin serim sonrası sonuçları verilmiştir. Sonra bu devrenin 0.35µm CMOS teknolojisinde üretilmiş halinin ölçüm sonuçları verilmiştir. Son olarak da önerilen kaotik devre kullanılarak [7]'de verilen yöntemden farklı bir yöntemle gerçeklenmiş yeni bir rastgele sayı üreteci sunulmuştur. Tasarımı yapılan devrenin serimi çizilmiş ve analizleri yapılmıştır.

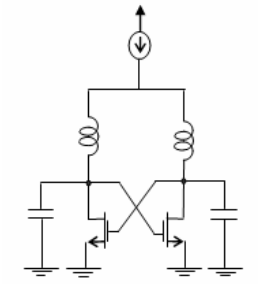
2. Önerilen Kaotik Devre

Önerilen kaotik devre Şekil 1a'da verilen klasik negatif-gm tank osilatöründen türetilmiştir. Bu temel yapıya bir çift paralel RC bölümü, fark kuvvetlendiricisi ve *K* kazançlı akım aynaları eklenerek Şekil 1b'de verilen kaotik osilatör türetilmiştir. Devreye K kazançlı akım aynalarının eklenmesi güç sarfiyatını arttırırken devrenin daha kararlı kaotik davranış göstermesini sağlamaktadır. Devredeki kapasite değerleri $C=C_1=C_2=0.5C_3=0.5C_4$ olacak şekilde seçilirse devrenin durum denklemleri aşağıdaki gibi elde edilir.

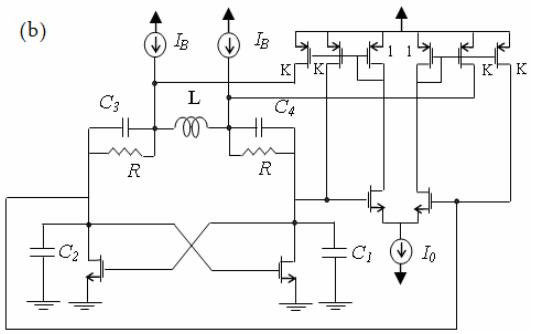
$$C(\dot{v}_{C2}-\dot{v}_{C1}) = -2i_L + 0.5\beta(v_{C2}-v_{C1})(v_{C2}+v_{C1}-2V_{TH})$$
$$C(\dot{v}_{C2}+\dot{v}_{C1}) = -2I_B + KI_0 - 0.25\beta\left[(v_{C2}-v_{C1})^2 + (v_{C2}+v_{C1}-2V_{TH})^2\right]$$
$$L\dot{i}_L = (v_{C2}-v_{C1}) - (v_{C4}-v_{C3})$$
$$2C(\dot{v}_{C4}-\dot{v}_{C3}) = 2i_L - (v_{C4}-v_{C3})/R + K\begin{cases} I_0 & , v_{C2}-v_{c1} \ge \sqrt{2}V_{sat} \\ g_m(V_{C2}-V_{c1})\sqrt{1-\left(\frac{v_{C2}-v_{c1}}{2V_{sat}}\right)^2} & , |v_{C2}-v_{c1}| < \sqrt{2}V_{sat} \\ -I_0 & , v_{C2}-v_{c1} \le \sqrt{2}V_{sat} \end{cases} \quad (1)$$

Burada $V_{sat} = \sqrt{I_0 L/\mu_n C_{ox} W}$ ve $g_m = \sqrt{I_0 \mu_n C_{ox} W/L}$ dir.

(a)



(b)

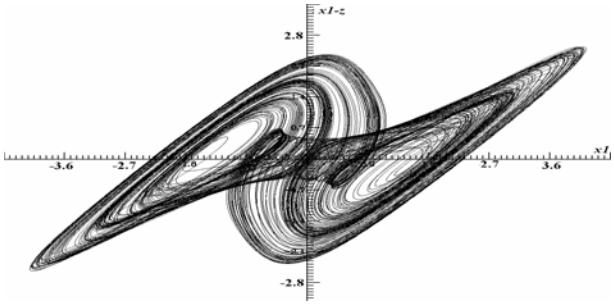


Şekil 1: a) Negatif-gm sinüs osilatörü b) Kaotik osilatör.

Normalize değerler olarak: $x_1 = (V_{C2}-V_{C1}) / 2V_S$, $x_2 = (V_{C2}+V_{C1}) / 2V_S$, $y = 2i_L R / V_S$, $z = (V_{C4}-V_{C3}) / 2V_S$, $t_n = t / 2RC$, $V_S = V_{TH}$ (V_{TH} eşik gerilimidir) seçilirse (1) denklemleri aşağıdaki gibi yazılabilir

$$\dot{x}_1 = -y + bx_1\left[x_2 - 1\right]$$
$$\dot{y} = x_1 - z$$
$$\dot{x}_2 = d - 0.5b\left[x_1^2 + (x_2-1)^2\right]$$
$$2\dot{z} = y - 2z + K\begin{cases} c & , x_1 > x_{sat} \\ \sqrt{2bc}\sqrt{1-\left(\frac{x_1}{\sqrt{2}x_{sat}}\right)^2} & , |x_1| < x_{sat} \\ -c & , x_1 < x_{sat} \end{cases} \quad (2)$$

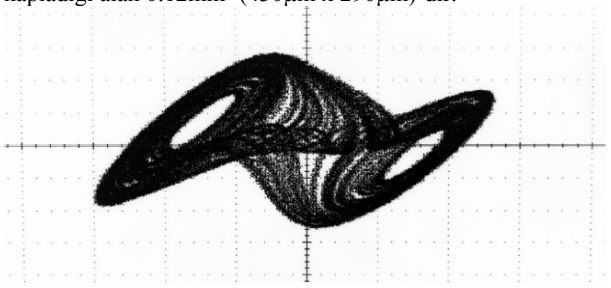
Yukarıda verilen denklemlerde $x_{sat} = V_{sat} / V_{TH}$, $b = \beta R_O V_{TH}$, $c = I_0 R / V_{TH}$, $d = 2 (KI_0-I_B)R / V_{TH}$ dir. Bu sistem farklı parametre kümesi için kaos oluşturmaktadır. Örneğin b = 0.4, c = 0.15, d = 0.8, k = 8 için elde edilen kaotik çekici Şekil 2'de gösterilmiştir.



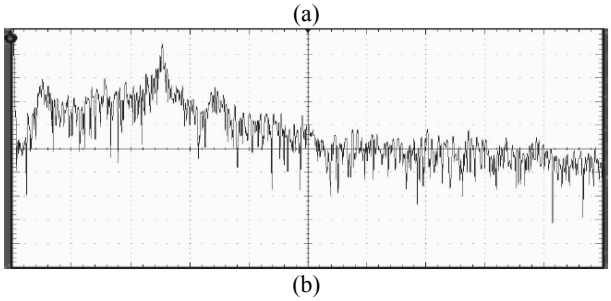
Şekil 2: (2)'de verilen sistemin sayısal analiz sonucu.

3. Kaotik Devrenin Benzetim ve Deneysel Sonuçları

Devrenin tümleşik olarak çalışmasını incelemek için Cadence tasarım ortamındaki Spectre benzetim aracı kullanılarak devrenin serimi çizilmiştir. Model parametreleri olarak AMS SiGe 0.35µm CMOS teknoloji parametreleri kullanılmıştır. Devrede eleman değerleri olarak C=10pF, R=350Ω, K=8 seçilmiştir. Devre ±1.65V ile beslenmiştir. Endüktans serimde çok yer kapladığı için devreye dışarıdan bağlanılması düşünülmüş ve serimin dışına alınmıştır. Endüktans değeri L=10µH seçilmiş ve kutuplama akım değerleri I_B=385µA, I_0=240µA olacak şekilde ayarlanmıştır. Bu değerlerle üretilmiş olan kaotik devreden elde edilen kaotik çekici ve frekans yelpazesi sırasıyla Şekil 3a ve Şekil 3b'de verilmiştir. Kaotik devre 11mW güç harcamaktadır ve kapladığı alan 0.12mm^2 (430µm x 290µm)'dir.



(a)



(b)

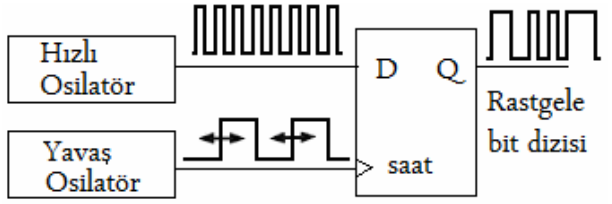
Şekil 3: a) Gözlemlenen kaotik çekici (V_{C2}-V_{C1}) ile V_L değişimi (X-ekseni=200mV/div, Y-ekseni=100mV/div) b) V_{C1}'re ait ölçülen frekans yelpazesi (X-ekseni=3MHz/div, Y-ekseni=10dB/div).

4. Rastgele Bit Üretimi

Rastgele sayı üreteçlerinde gerçek rastgeleliği elde edebilmek için sisteme belirsizlik kaynağı eklenmelidir. GRSÜ için kullanılan yöntem ve bloklar aşağıda verilmiştir.

4.1. RSÜ yapısında kullanılan yöntem

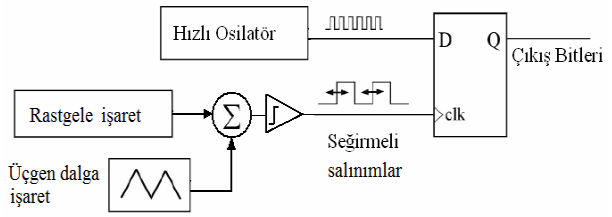
Bu çalışmada belirsizlik kaynağı olarak yukarıda anlatılan kaotik devre kullanılmıştır. Rastgele bit üretimi için temelde osilatör örnekleme yöntemi kullanılmıştır [9]. Bu yöntem Şekil 4'te gösterilmiştir.



Şekil 4: Osilatör örnekleme yöntemi temel gösterimi.

Osilatör örnekleme yöntemi temel olarak osilatör faz gürültüsünü rastgelelik kaynağı olarak kullanmaktadır. Sistemde serbest salınımlı biri hızlı biri yavaş olmak üzere iki osilatör bulunmaktadır. Hızlı olan osilatör yavaş olan tarafından bir D flip-flop kullanılarak örneklenmektedir. Eğer düşük frekanslı osilatörün periyodundaki standart sapma hızlı osilatörünkine göre çok büyükse, örneklenen osilatördeki iki ardışıl örnekleme ilişkisiz (uncorelated) kabul edilmektedir [10]. Sadece osilatör örnekleme yöntemi kullanılarak gerçeklenen RSÜ etkili bir rastgelelik sağlayamamaktadır [10]. Bundan dolayı sisteme başka bir belirsizlik kaynağı daha eklenmelidir. Belirsizlik kaynağı olarak direnç ısıl gürültüsü [10, 11] veya kaotik işaret kullanılabilmektedir [7]. Sisteme belirsizlik kaynağının eklenmesi ile gerçeklenen RSÜ yapıları rastgelelik testlerini geçebilmektedir [7,10,11].

Bu çalışmada Şekil 5'te blok şeması gösterilmiş RSÜ yapısından faydalanılmıştır [11]. Bu yapıda üçgen dalga işarete rastgele işaret eklenip bir karşılaştırıcıdan geçirilerek seğirmeli kare dalga işareti elde edilmektedir. Tasarlanan RSÜ yapısında multivibratör kullanılarak toplayıcı ve karşılaştırıcı kullanılmadan seğirmeli salınımlar elde edilmektedir.

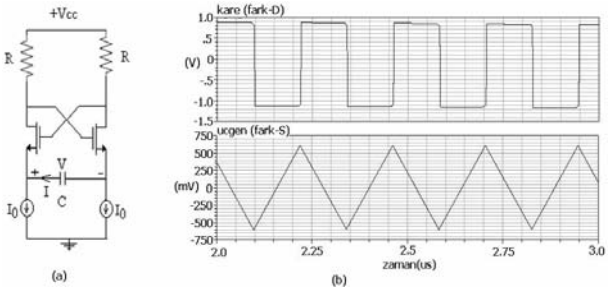


Şekil 5: RSÜ de kullanılan temel yöntem.

Osilatör örnekleme yönteminde, hızlı osilatör frekansı yavaş osilatör frekansının (veya belirsizlik kaynağının frekansının) 50 katından fazla olması yeterli rastgelelik sağlamakta; bu oran 100 veya üstünde olunca iyi rastgelelik sonuçları elde edilmektedir [13]. Ayrıca hızlı osilatör darbe boşluk oranın 1 olması iyi rastgelelik sağlamak için ayrı bir gerekliliktir [13].

4.1.1. Seğirmeli salınımların oluşturulması

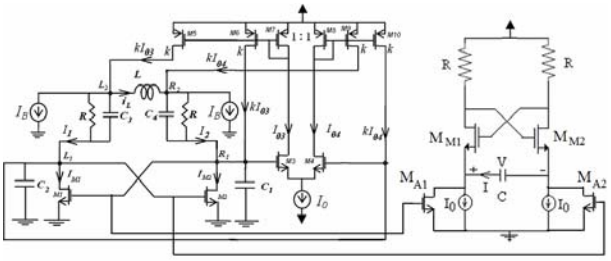
RSÜ yapısında seğirmeli kare dalga işaretini elde etmek için kullanılan multivibratör yapısı [14] ve devreden elde edilen dalga şekilleri Şekil 6'da verilmiştir. Üçgen dalga işareti MOS tranzistorların kaynak (S) uçları arasındaki gerilim farkından, kare dalga işareti MOS tranzistorların savak (D) uçları arasındaki gerilim farkından elde edilmektedir.



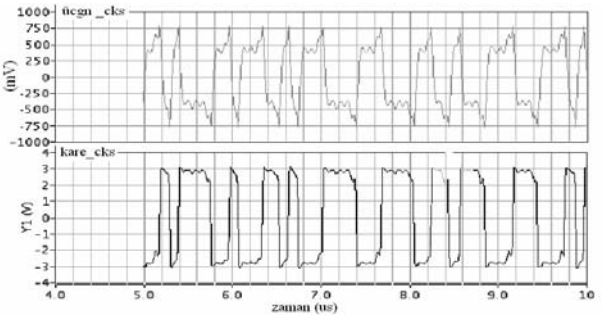
Şekil 6: (a) Multivibratör yapısı (b) çıkış dalga şekilleri.

Multivibratörden elde edilen kare dalga işaretinin frekansı kutuplama akımı I_0 ile değişmektedir. Bu akım değiştirilerek kare dalganın frekansında değişiklik yapılabilmektedir. Bu değişim kaotik işaret ile sağlanarak seğirmeli osilasyon işareti elde edilmesi amaçlanmıştır.

Seğirmeli osilatör işareti elde etmek için kaotik devre ile multivibratör devresi Şekil 7'deki gibi bağlanmıştır. Kaotik işaret M_{A1} ve M_{A2} taranzistorlarının geçitlerine bağlanmıştır. M_{A1} ve M_{A2} tranzistorlarından akan akım kaotik işaretin genliği ile değişmektedir. M_{A1} ve M_{A2} tranzistorlarından akan akım ile multivibratör kutuplama akımı I_0 akımının toplanması ile multivibratördeki C kapasitesinden akan I akımını değiştirilmektedir. M_{M1} ve M_{M2} taranzistorları savak uçlarında oluşan kare dalga işaretinin frekansı değişen I akımıyla kontrol edilebilmektedir ve böylece seğirmeli kare dalga işareti oluşmaktadır. Bu yapıdan elde edilen işaret Şekil 8'de verilmiştir.



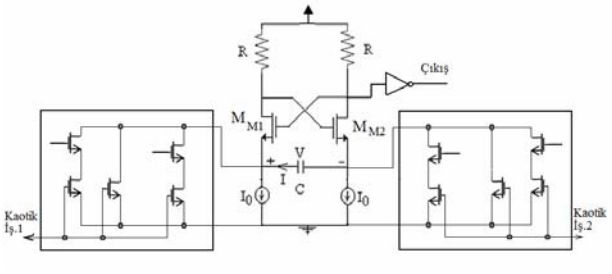
Şekil 7: Seğirmeli işaret üreten osilatör devresi.



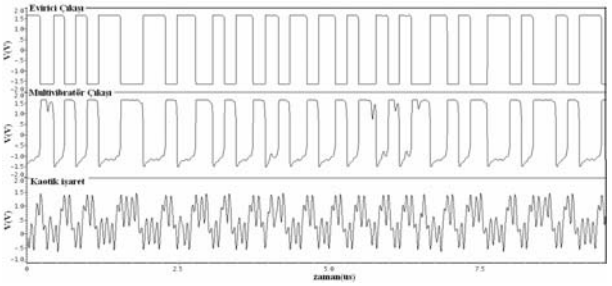
Şekil 8: Seğirmeli osilatör işareti.

Seğirmeli osilatör işaretinin düzgün kare olmadığı görülmektedir. Tepe değerlerinde gözlenen genlik değişimleri bazen osilatör örneklemesi sırasında D flip-flop çıkışında yanlış örneklemelere neden olmaktadır. Bundan dolayı multivibratörün çıkışına bir evirici eklenerek oluşan seğirmeli işaret genliklerinin tamamen besleme değerlerinde olması sağlanmıştır.

Devrenin incelenmesi sonucunda multivibratördeki direnç R = 10kΩ, çapraz bağlı tranzistor boyutları $(W/L)_{MM1,MM2}$ = 25µm/1µm, kapasite değeri C = 12pF için multivibratöre kaotik işareti taşıyan M_{A1} ve M_{A2} tranzistorlarının boyutlarının $(W/L)_{MA1,MA2}$ = 1µm/1µm ile $(W/L)_{MA1,MA2}$ = 4µm/1µm arasında olduğunda seğirmeli işaretin oluştuğu gözlenmiştir. M_{A1} ve M_{A2} tranzistorlarının kanal uzunluğu 1µm iken eşdeğer kanal genişlikleri 1.5µm, 2.5µm ve 3.5µm olacak şekilde tasarlanmıştır. Böylece kaotik işaret genliğinin multivibratöre etkisi değiştirilerek seğirme miktarı ayarlanabilmektedir. Multivibratörün kırmık üzerinde gerçeklenmiş hali Şekil 9a'da, elde edilen seğirmeli kare dalga işareti Şekil 9b'de verilmiştir.



(a)



(b)

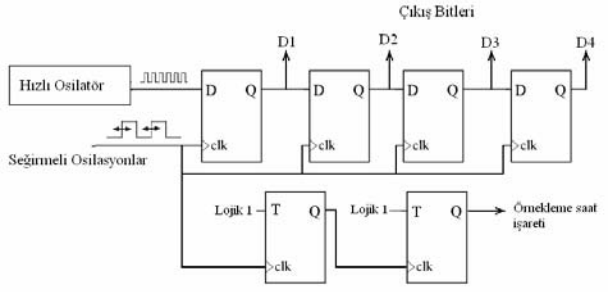
Şekil 9: a) Yeniden düzenlemiş multivibratör yapısı. b) Multivibratör çıkışındaki seğirmeli kare dalga işareti.

4.1.2. Hızlı osilatör

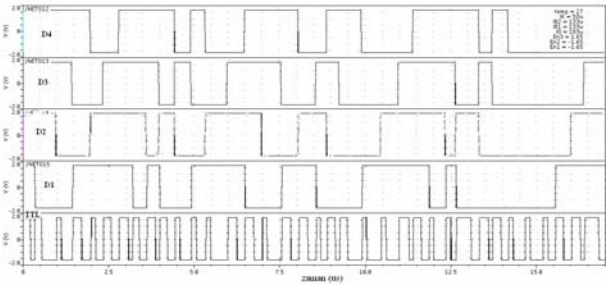
Seğirmeli kare dalga işaretin temel salınım frekansı 2MHz civarındadır. Hızlı osilatör olarak seğirmeli işaret frekansının 75 ve 100 katlarında salınım yapan 150MHz'lik ve 200MHz'lik iki ring osilatör tasarlanmıştır. Ring osilatör frekansı arttıkça, özellikle 200MHz'den sonra, işaretin darbe-boşluk oranı 1'den çok sapmaktadır. Bundan dolayı daha iyi bir darbe boşluk oranına sahip daha düşük frekansta salınım yapan ikinci bir osilatörün sisteme eklenmesi düşünülmüş ve 150MHz'lik ring osilatör sisteme eklenmiştir.

4.1.3. Örnekleme işlemi

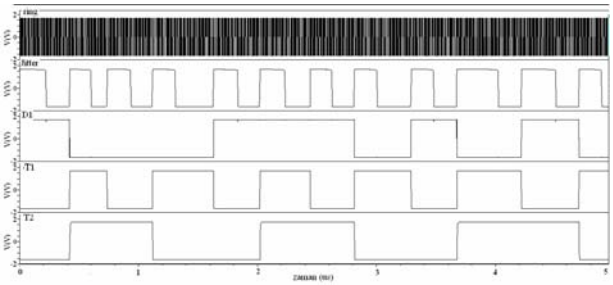
Yavaş osilatörün hızlı osilatörü örneklemesi için D flip-flop kullanılmıştır. Kırmıktan elde edilecek bit dizisinin paralel okuma yapılarak dışarıya alınması amaçlanmıştır. Şekil 10'da gösterilen çıkış katı ile dört bit veri oluşunca okuma yapılmaktadır. Şekil 11 ve Şekil 12'de devrenin benzetim sonucunda elde edilen çıkış işaretleri gösterilmiştir. RSÜ devresinin serimi Şekil 13'te verilmiştir.



Şekil 10: RSÜ çıkış katı.



Şekil 11: RSÜ çıkış bit dizisi.

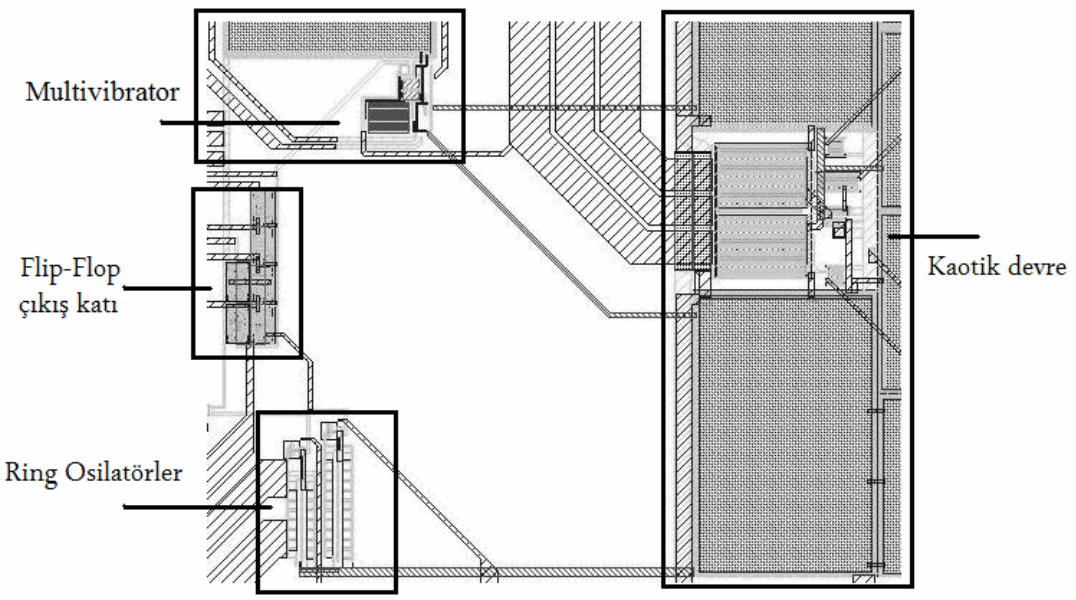


Şekil 12: T flip-flop çalışması.

5. Sonuçlar

Tümleştirilmiş RSÜ yapılarında bugüne kadar kullanılan kaotik yapılar ağırlıklı olarak ayrık zamanlı sistemlerdir. Sürekli zamanlı kaotik sistemlerin tümleşik GRSÜ yapılarında kullanılmaları ve yüksek hızda bit üretecek şekilde tasarlanmaları kaotik sistemlerin GRSÜ yapılarında kullanımında yeni bir kapı açacaktır. Yüksek bit üretimi için yüksek hızlı çalışan sistemlerin olması da kaçınılmazdır. Burada çalışma frekansı düşürülmüş sürekli zamanlı kaotik sistem kullanılarak tasarlanmış tümleşik RSÜ yapısı verilmiştir. Bu yapıdan 2Mbit/s hızda rastgele bit üretilmesi daha yüksek hızlarda rastgele bit üretilebileceğinin bir göstergesi olacaktır.

Devre üretime yollanmıştır. Üretimden dönen örneklerle yapılacak deneylerin sonuçlarının konferans zamanına kadar yetişmesi durumunda, sonuçların konferansta sunulması hedeflenmektedir.



Şekil 13: Rastgele sayı üreteci devresinin serimi

6. Kaynaklar

[1] Gerosa, A., Bernardini, R., Pietri, S., "A fully integrated chaotic system for the generation of truly random numbers", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* Cilt 49, Yayım 7, syf:993 - 1000, Temmuz 2002

[2] Delgado-REstituto, M., Medeiro, F., Rodriguez-VAzquez, A., "Nonlinear Switched current Cmos IC for RNG", *Electronics Letters,* Cilt: 29, No.25, Aralık 1993.

[3] Zhou, Tong; Yu, Mingyan; Ye, Yizheng; "A Robust High-Speed Chaos-Based Truly Random Number Generator for Embedded Cryptosystems", *49th IEEE International Midwest Symposium on Circuits and Systems, 2006. MWSCAS '06.* Cilt 2, syf:536 – 540.

[4] M.E.Yalcin, J.A.K.Suykens, and J.Vandewalle, "True Random Bit Generation from a Double Scroll Attractor", *IEEE Trans. Circuits Syst. I,* vol. 51, syf.1395-1404, 2004.

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

[6] Tavas, V., Özoğuz, S., ve Toker, A., 'Yeni bir tümleşik kaotik devre', *Elektrik-Elektronik-Bilgisayar-Biyomedikal Müh. 12. Ulusal Kongresi Bildiriler Kitabı*, 2007, syf. 253-256.

[7] Tavas, V., Demirkol, A. Ş., Özoğuz, S., Zeki, A., Toker, A., *"An integrated cross-coupled chaos oscillator aplied to random number generation"*, IET Circuits, Devices & Systems dergisinde yayımlanmak üzere kabul edilmiştir.

[8] National Institute of Standard and Technology, "*A Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications*", NIST800-22, Mayıs 2001.

[9] Fairfield, R. C., Mortenson, R. L., Coulthart, K.B., *"An LSI random rumber generator"*, Proc. Advances in Cryptolgy Conf. (CRYPTO '84), 1984, syf. 203-230.

[10] Petrie, C. S., Connelly, J. A., *"A noise based IC random number generator for applications in cryptography"*, IEEE Trans.Circuit & Systems, cilt. 47, no. 5, syf. 615-621, Mayıs 2000.

[11] Bucci, M., Germani L., Luzzi R., Trifiletti A., and Varanonuovo M., *"A high-speed oscillator-based truly random number source for crptographic applications on a smart card IC*", IEEE Transaction on computer. cilt.52, no 4, syf: 403- 409, Nisan 2003.

[12] National Institude of Standart and Technology, "Security requirements for cryptographic Modules", FIPS PUB 140-1, January 11, 1994.

[13] C. S. Petrie, J. A. Connelly, "*Modelling and simulation of oscillator-based random number generators*", Proc. ISCAS'96, Cilt. 4, Syf: 324-327, May 1996.

[14] Buonomo A., Schiavo A. L., "*Analysis of emitter (source)-coupled multivibrators*", IEEE transactions on circuits and systems-1. Cilt.53, No:6, Syf:1193-1202, Haziran 2006.