Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki Etkisinin İncelenmesi

Erdinç AVAROĞLU, Mustafa TÜRK

***ÖZET*— Rasgele sayı üreteçlerinden elde edilen sayılar bilgi güvenliği anlamında kriptoloji alanında güvenlik açısından bir zorunluluktur. Bu güvenliğin sağlanabilmesi için elde edilen sayıların kestirilememesi, tekrar üretilememesi ve iyi istatistiksel özellikleri sağlaması gerekmektedir. Bu gereksinimlerin sağlaması amacıyla gerçek rasgele sayı üreteçleri kullanılmıştır. Ancak gerçek rasgele sayı üreteçlerinden elde edilen bit dizilerinin bazıları zayıf istatistiki özellikler göstermiştir. Bu nedenle bu eksikliğin giderilmesi amacıyla çeşitli son işlem algoritmaları uygulanmıştır. Bu çalışmada, yeni bir son işlem algoritması önerilmiş ve bunun kısmi istatiksel analizi yapılmıştır.**

Anahtar Kelimeler — Rasgele sayı Üreteçleri, Son işlem, Kaotik çekerler.

***ABSTRACT*— The numbers which are obtained from random number generator is a obligation for the sense of security in the field of information security cryptology. To maintain this security, the numbers which are obtained must be unpredictable, unproducible second time and provide good statistical properties. To provide these needs, true random number generators are used. But some of the sequences from true random number generators have shown poor statistical futures. In order the eliminate this deficiency, various post processing algorithms have been applied. In this study, a new post processing algorithm was proposed and its partial statistical analysis was carried out.**

Keywords: Random number generator, Post Processing, Chaotic attractor

I. GİRİŞ

Rasgele sayı üreteçlerinden elde edilen sayılara istatistikte örnekleme, simülasyon, nümerik analiz, eğlence gibi alanlarda ve kriptografide ihtiyaç duyulmuştur. Özellikle rasgele sayılar çeşitli kriptografik uygulamalar için zorunluluktur. Çünkü kriptografi anahtarların üretimi ve dağıtımında, başlangıç vektörü oluşturulmasında, kimlik doğrulama protokollerinde, asal sayı ve şifre üretiminde rasgele sayılara ihtiyaç duyar. Bir kriptografik sistemin güvenliği elde edilen sayıların gerçek rasgeleliliğine dayanmaktadır. Bu sebepten dolayı kriptografik sistemlerde kullanılan rasgele sayıların bazı sıkı gereksinimleri sağlamaları gerekmektedir. Bu gereksinimler kestirilememe (tahmin edilememe), tekrar üretilememe ve iyi istatistiksel özelliklerdir [1].

E.Avaroğlu, İnönü Üniversitesi Bilgi İşlem Daire Başkanlığı, Malatya, TÜRKİYE. (Telefon: 04223773266, e-posta: erdinc.avaroglu@inonu.edu.tr)
M.Türk, Fırat Üniversitesi Elektrik Elektronik Mühendisliği, Elazığ, TÜRKİYE (Telefon: 424-2370000-5208, e-posta: mturk@firat.edu.tr)

Bu rasgele sayıların elde edilebilmesi amacıyla çeşitli rasgele sayı üreteçleri (RSÜ) geliştirilmiştir. Bu rasgele sayı üreteçleri gerçek rasgele sayı üreteçleri (GRSÜ), sözde rasgele sayı üreteçleri (SRSÜ) ve hibrit rasgele sayı üreteçleri olmak üzere sınıflandırılmıştır.

Sözde rasgele sayı üreteçleri herhangi bir başlangıç (tohum) değeri olmadan başlayamaz. Tohum rasgele seçilmiş olmalıdır. Belirlenen tohum değeri belirli bir algoritmaya tabi tutularak uzun rasgele sayı dizileri üretilmiştir. SRSÜ'nün avantajlı yanı diğer uygulamalara oranla ucuz olması, kolay gerçeklenebilir olması, hızlı olması ve donanım ihtiyacına gerek duymamasıdır. Ancak SRSÜ'ler ile üretilen sayılar tohum değeri tespit edildiğinde veya sistemde kullanılan fonksiyonlar yeterince karmaşık olmadığı taktirde tahmin edilebilmiştir. Ayrıca belli bir süre sonra üretilen dizi kendini tekrar etmeye (periyodiklik) başlamıştır. Belirtilen bu eksiklikler nedeniyle SRSÜ'ler kriptografik uygulamalar için uygun değildir [2-4].

Gerçek rasgele sayı üreteçleri gürültü kaynağı olarak kontrol edilemeyen ve kestirilemeyen gerçek fiziksel süreçleri kullanarak rasgele sayı üretmiştir. GRSÜ tarafından üretilen rasgele sayıların özellikleri ve rasgeleliliği fiziksel süreçlerin rasgeleliliğine bağlıdır. Kontrol edilemeyen fiziksel süreçler olduğu taktirde üretilen sayılarda kestirilemez ve kontrol edilemez. Ancak bazı üretilen bit dizisi istatistiki zayıflıklar göstermişlerdir. Bu zayıflıkların giderilmesi amacıyla üretilen bit dizisi son işleme tabi tutulmuştur. Son işlem uygulamaları zayıflıkları giderirken bit oranında azalmaya sebep olmuştur. GRSU yavaş, maliyetli ve donanıma bağımlı olması dezavantajlı tarafıdır. Ancak GRSÜ'ler kriptografik uygulamalar için zorunlu olan kestirilememe, tekrar üretilememe ve iyi istatistiki özellikleri sağlaması sebebiyle kriptolojide birçok uygulamada kullanılmıştır [1].

Hibrit rasgele sayı üreteci GRSÜ'den elde edilen rasgele sayının SRSÜ'de tohum değeri kullanılmasıyla her iki sistemin birlikte çalıştığı rasgele sayı üretecedir.

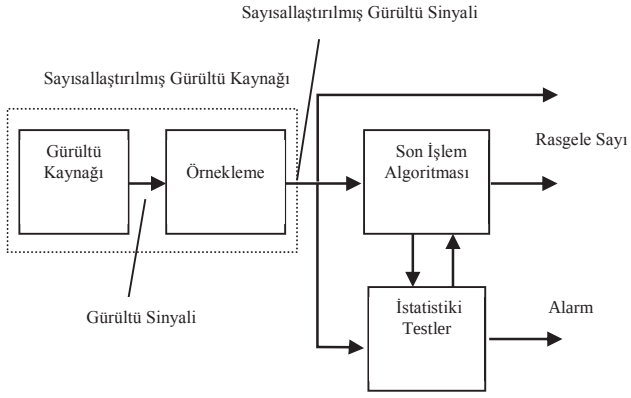
Kaotik sistemlerin en önemli özelliği başlangıç şartına bağlı olmalarıdır. Bu sistemler uzun dönemlerde tahmin edilemez davranışlar ve periyodik olmayan özellikler göstermişlerdir [5]. Kaotik sistemlerde elde edilen işaretlerin rasgele özellikler göstermesi (gürültü benzeri işaretler olması) nedeniyle gerçek rasgele sayı üreteçlerinde gürültü kaynağı olarak kullanılmışlardır. Ayrıca kriptolojide de kaos bir çok uygulamada kullanılmıştır [6,7].

Bölüm 2 de gerçek rasgele sayı üreteçlerinden ve son işlemden bahsedilmiştir. Bölüm 3'te rasgele sayı üretiminde kullanmış olduğumuz kaotik çekerlerden ve örnekleme işleminin nasıl yapıldığı açıklanmıştır. Bölüm 4'te elde edilen

bit dizisinin saf halinin ve son işlemden geçirilmiş halinin istatistiksel test sonuçları incelenmiştir. Bölüm 5'te sonuç verilmiştir.

II. GERÇEK RASGELE SAYI ÜRETECİ

Şekil1.'de GRSÜ genel tasarımı gösterilmiştir. GRSÜ'lerde entropi (gürültü) kaynağı deterministik olmayan doğal fiziksel olaylar olarak tanımlanmış ve rasgele sayı üretmede kullanılmıştır. Genellikle analog gürültünün dijital sinyale dönüşümünü içerir. İyi tasarlanmış bir GRSÜ'de bu entropi kaynağı, son işlemden geçirilen istatistiksel bağımsız bit dizilerini elde etmek için örneklenmiş ve gerçek rasgele sayı dizileri ile sonuçlanmıştır. Üretilen rasgele bitten bir sonraki bit tahmin edilememelidir ve aynı rasgele bitin üretilmesi engellenmiş olmalıdır. GRSÜ'lerde örnekleme işleminden sonra elde edilen rasgele bit dizisinde bulunan potansiyel zayıflıkları (bitler arası korelasyon olması) gidermek amacıyla elde edilen bit dizisi son işleme tabi tutulmuştur. Ancak bu işlem bit dizisinde ki zayıflıkları giderirken çıkıştaki bit oranını azaltmakta ve çalışma hızını düşürmekte olduğuna dikkat edilmelidir. Bu yüzden güçlü gürültü kaynakları kullanmak gerekmektedir [2,3,8].



Şekil 1. GRSÜ Genel Tasarımı

Gerçek rasgele sayı üretecinin temel blokları aşağıda açıklanmıştır.

A. *Gürültü (Entropi) Kaynağı*

GRSÜ'lerde kullanılan çeşitli tiplerde gürültü kaynakları bulunmaktadır. GRSÜ için entropi kaynağı fiziksel rasgelilik kaynağıdır. GRSÜ'lerde kullanılan gürültü kaynakları:

- Elektriksel Gürültü: Isıl gürültü, termal gürültü, saçma gürültüsü ve titreme gürültüsü kullanılmaktadır.
- Fotonların kuantum mekanik özellikleri
- Mekanik sistemler
- İnsan kaynaklı etkileşimler: fare ve klavye hareketleri

B. *Örnekleme(Sayısallaştırıcı)*

Örnekleyici gürültü sinyalinin gerekli örneklemesini yapmış ve fiziksel gürültü kaynakları için üretim mekanizması (Harvesting Mechanism) olarak adlandırılmıştır. Analog sinyalden sayısallaştırılmış sinyal üretir. Genellikle D-tip flip flop örnekleyici olarak kullanılmıştır. Gerilim kontrollü osilatörde bazı gürültü kaynakları için kullanılmıştır.

C. *Son İşlem (Post Processing)*

Son işlem genellikle sinyaldeki rasgeleliliği artırmak için kullanılmıştır. Son işlem uygulanmış sinyal değerleri saf sinyal ile karşılaştırıldığında düzenli (uniform) dağılımlıdır. Örneklenmiş rasgele sayı başına entropi artacaktır. Son işlemin aktif hata ve yan kanal analizi saldırılarından dolayı daha da önem kazanan ikinci amacı, saldırgan kurcalamaları ve çevresel değişikliklere karşı dirençli hale getirmesidir. Son işlem algoritmasına bağlı olarak üretecin güvenliği artmıştır. Xor doğrulama [9], von neumann doğrulama [10], H fonksiyonu [11] ve resilient fonksiyonlar [12] gibi çeşitli son işlem algoritmaları uygulanmıştır. Bu uygulamalardan en çok kullanılan 2 son işlem aşağıda açıklanmıştır ve yeni bir son işlem uygulaması önerilmiştir.

- **Xor Son İşlem :** Xor doğrulama bir çıkış biti üretmek amacıyla n bit (n=2) blok üzerinde xor işleminin uygulandığı basit doğrusal bir fonksiyondur. Çıkış bitindeki korelasyonu giderirken bir yandan da çıkış bit verimini 1/n kez azalmasına neden olmuştur. Ancak, çıkış bit dizisindeki korelasyon giriş bitlerinin bağımsız olması şartıyla düşmüştür. Bu doğrulamanın avantajı, basitliği ve sabit çıkış bit hızını sağlama olasılığıdır.
- **Van Neumann Son İşlem :** En eski ve en basit son işleme yöntemidir. Bit dizisindeki düzensizlikleri gidermiştir. Tablo 1'de gösterildiği gibi Van neumann düzgün dağılımlı 0 ve 1 bitleri üretmiştir. GRSÜ'den gelen eşzamanlı çiftleri dikkate almıştır. Eğer bit dizisi (1,0) ise 1 biti üretmiş, eğer bit dizisi (0,1) ise 0 biti üretmiştir. (0,0) ve (1,1) bit dizileri atılmıştır. Bu doğrulama entropiyi ideal değer 1'e yaklaştırarak ürettiği bitler ile entropinin iyileştirilmesine katkıda bulunmuştur. Ancak, GRSÜ'den gelen bazı bit dizilerinin atılmasından dolayı Van neumann çıkış bit hızı GRSÜ'nün çıkışına bağlıdır ve bundan dolayı sabit değildir. Bit hızı giriş bit hızının 1/4'ü kadar azalmıştır.

Tablo 1. Van Neumann Son İşlem

Girilen Bit Çiftleri	Van neumann çıkışı
00	Çıkış yok
01	0
10	1
11	Çıkış yok

- **Önerilen Son İşlem :** Önermiş olduğumuz sistemde van neumann tarafından önerilen sistemde atılan 00 ve 11 bitleri yerine 00 bitleri 0, 11 bitleri 1 olarak alınmıştır. Bu şekilde alınması ile van neumann son işleminde bit dizisi 1/4 oranında azalırken önerdiğimiz son işlemde azalma 1/2 oranında meydana gelmiştir.

Tablo 2. Önerilen Son İşlem

Girilen Bit Çiftleri	Önerilen son işlem çıkışı
00	0
01	0
10	1
11	1

Gerçek rasgele sayı üreteçleri iyi istatistiksel özellikler göstermesi ve elde edilen rasgele sayıların kestirilememesi sebebiyle kriptografik uygulamalarda kullanılmıştır. Ancak bu iyi özellikler yanında donanımsal tasarımlarının zor olması ve sistemin SRSÜ'lere göre çok daha yavaş çalışması dezavantajlı yanıdır. Bu yüzden kaotik sistemler kullanılmaya başlanmıştır. Çünkü kaotik devrelerin donanımsal olarak uygulanması daha kolay olmuştur. Ayrıca üretilen kaotik işaretler daha iyi rasgele özellikler ve performans göstermişlerdir.

III.KOATİK ÇEKERLER

Kaotik sistemlerin en önemli özelliği başlangıç şartına bağlı olarak uzun dönemlerde kestirilemeyen davranışlar ve periyodik olmayan özellik göstermesidir. Kaotik sistemlerde elde edilen işaretlerin gürültü benzeri işaretler olmasından dolayı rasgele sayı üretiminde gürültü kaynağı olarak kullanılmaktadır. Kaotik işaretler geniş aralıklarla örneklenerek kullanılması testlerde başarılı sonuçlar vermiştir. Kaotik işaretler kullanılarak yapılan çeşitli çalışmalar mevcuttur [13]. İlki sürekli zamanda çift sarmallı kaotik yapı [14] diğeri de osilatör örnekleme yöntemidir [15].

Bu çalışmamızda 2+2 çeker kullanılarak gerçekleştirilmiştir.

A. 2+2 çeker elde edilmesi

Bu çalışmamızda kullanmış olduğumuz genelleştirilmiş Chua devre denklemleri (1) 'de gösterilmiştir.

$$\begin{aligned} \dot{x} &= y + f_1(y) \\ \dot{y} &= z \\ \dot{z} &= -a \cdot x - a \cdot y - a \cdot z + f_2(x) \end{aligned} \qquad (1)$$

Burada

$$f_1(y) = \sum_{i=1}^{M_1} g_{\frac{(-2i+1)}{2}}(y) + \sum_{i=1}^{N_1} g_{\frac{(2i+1)}{2}}(y)$$

$$f_2(x) = \sum_{i=1}^{M_2} g_{\frac{(-2i+1)}{2}}(x) + \sum_{i=1}^{N_1} g_{\frac{(2i+1)}{2}}(x)$$

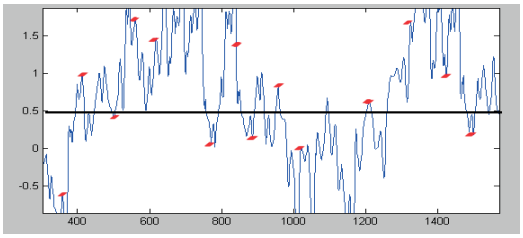
$$g_\theta(\alpha) = \begin{cases} 1 & \alpha \geq \theta, \theta > 0 \\ 0 & \alpha < \theta, \theta > 0 \\ 0 & \alpha \geq \theta, \theta < 0 \\ -1 & \alpha < \theta, \theta < 0 \end{cases}$$

Şeklinde olup, $M_1, N_1, M_2, N_2, i, j \in \Re^+$'dır. $f_1(y)$ sisteme etkisi ihmal edilmiştir ve a değeri 0.4 alındığında sistem çift çeker davranış göstermiştir. $f_1(y)$ ve $f_2(x)$ çok kırılma noktalı parçalı doğrusal elemanları temsil etmekte olup aynı özelliklere sahiptir. Y durum değişkeni $f_1(y)$ etkiler, x durum değişkeni de $f_2(x)$'i etkiler. M ve N parametrelerine bağlı olarak bu elemanlar dinamik yapı gösterirler. M ve N değerleri ile kırılma noktaları sayısı ve yerleri belirlenir.

Sistemde, x ve y=-ax+b doğruları boyunca kaotik çekiciler oluşacaktır. $f_2(x)$ etkisi altında olan kaotik sarmallar x ekseni boyunca oluşur, $f_1(y)$'nin etkisi altındaki kaotik sarmallar y=-ax+b doğrusu boyunca oluşur. Her iki yönde de kaotik çekiciler oluştuğu için bu davranış tipi n+n çekici olarak adlandırılır. İlk n değeri x ekseni diğer n değeri de y=-ax+b doğrusu boyunca oluşan toplam sarmalları gösterir.

Denklem (1) 'de verilen diferansiyel denklem çözülerek sistemin davranışı elde edilmiştir. Matlab programı kullanılarak, 4 adımlı Runge-Kutta metodu kullanılmıştır. Durum değişkenlerinin başlangıç değerleri (x_0,y_0,z_0)=(0.1,0.1,-0.1) ve a değeri 0.4 alınmıştır. 2+2 çeker elde etmek için M_1=1, N_1=2, M_2=0 ve N_2=1 alınmıştır[16]. 2+2 çekerden elde edilen X durum değişkeninden ilk 500 sayıdan itibaren 300 adımda bir değer alınmıştır. Elde edilen bu değerlerde aşağıdaki Şekil 2'de gösterildiği gibi ve (2)'de gösterilen kural (0.5 değeri simülasyon sonucu ortaya çıkan minimum ve maksimum değerlerin ortalaması olarak belirlenmiştir) uygulanarak herhangi bir son işleme tabi tutulmadan 108418 bit dizisi elde edilmiştir. Elde edilen bit dizisi [17]'deki çalışmamızda herhangi bir son işlem uygulamadan sadece istatistiksel testlere tabi tutulmuştur. Buradaki çalışmamızda elde edilen bit dizisi yukarıda açıklanan son işlemlerden geçirilerek saf bit dizisi üzerindeki etkileri incelenmiştir.

$$S(x) = \begin{cases} 0 & x < 0.5 \\ 1 & x >= 0.5 \end{cases} \qquad (2)$$



Şekil 2. 2+2 çekerin belli bir alanının simülasyonu

IV. SON İŞLEM SONRASI İSTATİSTİKSEL TEST SONUÇLARI

Gerçek rasgele sayı üreteçlerinden elde edilen bit dizileri sıcaklık,basınç gibi çevresel etkenler nedeniyle zayıflıklar gösterebilir. Bu zayıflıkların giderilmesi amacıyla son işlem uygulanmıştır. Elde edilen bit dizilerinin rasgele olup olmadığına geçerli istatistiksel testler uygulanarak karar verilebilmiştir. Bilinen en geçerli test Ulusal Standartlar ve Teknoloji Enstitüsünün yayınladığı NIST 800-22'dir. Bu testlerin yazılımı yazılmış olup elde edilen sonuçlar aşağıdaki tabloda gösterilmiştir.

Tablo 3. Elde edilen bit dizileri

Saf Bit Dizisi	108418 Bit
Xor Son İşlem	54209 Bit
Önerilen Son İşlem	54209 Bit
Van Neumann	27009 Bit

Tablo 4. 2+2 çeker için NIST testi sonuçları

Test Adı	**Saf bit Dizisi P değeri**	**XOR p değeri**	**Van neumann p değeri**	**Önerilen Son İşlem P değeri**	**Sonuç**
Frekans	0.151	0,412	0,421	0,112	Başarılı
Blok Frekans	0.484	0,086	0,835	0,789	Başarılı
Akış	**0.028**	**0,548**	**0,199**	**0,641**	**Başarılı**
Blok İçindeki En Uzun Birler Akışı	0.069	0,521	0,850	0,236	Başarılı
İkili Matris Rankı	0.675	0,021	0,177	0,725	Başarılı
Ayrık Fourier Dönüşümü	0.442	0,774	0,215	0,880	Başarılı
Örtüşmeyen Şablon Eşleştirme	0.086	0,557	0,832	0,705	Başarılı
Örtüşen Şablon Eşleştirme	0.778	0,698	0,744	0,928	Başarılı
Maurer'in Evrensel İstatistik	0.050	0,231	0,324	0,493	Başarılı
Doğrusal Karmaşıklık	0.580	0,950	0,997	0,320	Başarılı
Seri	0.246	0,400	0,926	0,850	Başarılı
	0.594	0,530	0,940	0,928	
Yaklaşık Entropi	0.106	0,241	0,383	0,414	Başarılı
Kümülatif Toplam	0.085	0,288	0,659	0,093	Başarılı

Elde edilen sonuçlar incelendiğinde her ne kadar saf bit dizisi istatistiksel test sonuçlarını geçmiş olsa bile son işlem uygulandığı taktirde bit dizisi kalitesinin arttığı gözlenmiştir. Son işlem bitleri daha düzgün dağılımlı hale getirmiştir. Bu düzelme üçüncü test olan akış testi ile anlaşılmıştır. Akış testi 0 ve 1'ler arasındaki değişime bakmaktadır. Sonuç değeri ne kadar büyük ise 0 ve 1' ler arası geçişin çok olduğunu ve aralarındaki korelasyonun az olduğunu göstermiştir. Tablo 4'de üçüncü teste bakıldığında son işlemin ne kadar etkili olduğu görülmüştür ve önerdiğimiz son işlemde sonuç çok daha iyi çıkmıştır.

V. SONUÇ

Bu çalışmamız da gerçek rasgele sayı üretecinden elde edilen bit dizilerine son işlem uygulanması ve bu uygulamanın sonuçları üzerinde durulmuştur. Saf bit dizileri her ne kadar testleri geçmekte olsa bile kriptografik güvenlik için gerekli olan kaliteli bit dizilerin son işlem sonrası elde edileceği ve gerçek rasgele sayı üretiminde son işlemin önemli bir aşama olduğu görülmüştür. Önermiş olduğumuz son işlemde sonuçlar başarılı olmuştur. Van neumann son işlemini iyi sonuç vermesine rağmen çıkış bit oranını 1/4 oranında azaltmaktadır. Ancak önerdiğimiz sistemde bu oran 1/2 olmuş ve daha iyi sonuçlar vermiştir. Daha ileriki çalışmalarda bit oranını düşürmeyen daha iyi sonuçlar alınabilecek son işlem algoritmaları önerilmesi düşünülmektedir.

KAYNAKLAR

[1] Koç, C.K.,"Cryptographic Engineering", *Springer*, 2009

[2] Akram, R.N., "Pseudorandom Number Generation in Smart Cards: An Implementation, Performance and Randomness Analysis", *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, 1-7, 7-10 May 2012

[3] Yıldırım S., Bazlamaccı C., "A True Random Number Generator and Test Platform Built in FGPA.", *International Information Security and Cryptology Conference - ISCTURKEY 2012, Ankara*, Turkey, pp.262-267, May 17-18, 2012

[4] Sobotka, J. and Zeman, V., "Design of the true random numbers generator", *Elektrorevue*, 2(3):1-6, September 2011

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

[6] Özkaynak,F., Özer, A. B., Yavuz, S.,"Cryptanalysis of A Novel Image Encryption Scheme Based on Improved Hyperchaotic Sequences", *Optics Communications*, 285(24): 4946-4948, 2012

[7] Özkaynak,F. and Özer, A. B.," A method for designing strong S-Boxes based on chaotic Lorenz system", *Physics Letters A*, 374(36): 3733-3738, 2010/8/9

[8] Murphy, J.P., "Field-programmable true random number generator", *Electronics Letters*, 48(10):565 - 566,10th May 2012

[9] Davies, R.B., "Exclusive OR (XOR) and Hardware Random Number Generators", February 28, 2002, 1{11, http://webnz.com/robert

[10] Suresh,V.B., Burleson, W.P., "Entropy Extraction in Metastability-based TRNG", *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on* ,135-140, 13-14 June 2010

[11] Dichtl, M., "Bad and Good Ways of Post-Processing Biased Physical Random Numbers", *Fast Software Encryption Lecture Notes in Computer Science Volume 4593*, 137-152,2007

[12] Sunar, B., Martin, W.J., and Stinson, D.R.,"A Provably Secure True Random Generator with Built-In Tolerance to Active Attacks", *in IEEE Transaction On Computers*, vol. 56, No.1, January 2007

[13] Yalçın, M.E. , "Şifreleme için çok sarmallı kaotik çekici temelli rastgele sayı üreteci tasarımı ve elektronik gerçeklenmesi", *Tübitak Proje(108E219)*, Eylül 2011

[14] Ergün, S. and Özoğuz, S., "A chaos-modulated dual oscillator-based truly random number generator.", *In Proceedings, International Symposium on Circuits and Systems*, 2482–2485, 2007

[15] Yalcın, M. E., Suykens, J. A. K. and Vandewalle, J., "True random bit generation from a double scroll attractor.", *IEEE Trans. Circuits and Systems-I*, 51(7):1395–1404, 2004

[16] Türk, M. and Ata, F., "The multi-mode chaotic behaviours: N+N and 2D N-scroll chaotic attractors", *COMPEL: The nternational Journal for Computation and Mathematics in Electrical and Electronic Engineering* , 25(4):929-939, 2006

[17] Avaroglu, E., Türk,M.," Random number generation using multi-mode chaotic attractor", *Signal Processing and Communications Applications Conference (SIU)*, 2013 21st ,1-4, 2013