DOKUZ EYLÜL ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ
FEN VE MÜHENDİSLİK DERGİSİ
Cilt/*Vol.*:18■ No/*Number*:3■Sayı/*Issue*:54■Sayfa/*Page*:640-651■ EYLÜL 2016/*Sep 2016*
DOI Numarası (DOI Number): 10.21205/deufmd.2016185427

Makale Gönderim Tarihi (Paper Received Date): 21.01.2016 Makale Kabul Tarihi (Paper Accepted Date): 13.09.2016

RADYO FREKANSI İLE TANIMLAMA ETİKETLERİ İÇİN GERÇEK RASTGELE SAYI TABANLI ÜRETEÇ

(TRUE RANDOM NUMBER BASED GENERATOR FOR RADIO FREQUENCY IDENTIFICATION TAGS)

Gökhan DALKILIÇ[1]

ÖZ

Bu çalışmada, radyo frekansı ile tanımlama (RFID) teknolojisi kullanılarak ultra yüksek frekans (UHF) elektronik ürün kodu (EPC) 2. nesil (Gen2) standardı ile tasarlanmış etiketlerdeki güvenlik sorunlarının çözümüne yönelik rastgele sayı üretimi konusunda yeni bir yaklaşım önerilmiştir. Yaklaşımın en önemli farkı deneysel bir etiket olan kablosuz tanımlama ve algılama platformunun (WISP) üzerinde yer alan duyargaların gerçek rastgele sayı kaynağı olarak kullanılmasıdır. Gerçek rastgele sayı kaynaklarından elde edilen sayılar, geliştirilen basit bir sözde rastgele sayı üretecine tohum olarak verilmiştir. Elde edilen sayılar, rastgele sayı testlerinde bir standart olarak kullanılan Standartlar ve Teknoloji Ulusal Enstitüsü (NIST) test paketinden geçirilmiş ve başarılı sonuçlar elde edilmiştir.

Anahtar Kelimeler: RFID, WISP, GRSÜ, SRSÜ

ABSTRACT

In this study, a new random number generation approach has been proposed which will be useful for solving security problems on the radio frequency identification (RFID) tags that are designed with ultra high frequency (UHF) electronic product code (EPC) 2nd generation (Gen2) standard. The most important difference of this approach is using the sensors on an experimental tag, wireless identification and sensing platform (WISP), as the source of the true random number. The numbers obtained from true random number sources are given as seeds to a developed simple pseudo random number generator. The resulting numbers are passed through National Institute of Standards and Technology (NIST) test suite which is used as a standard in random number tests and successful results are obtained.

Keywords: RFID, WISP, TRNG, PRNG

[1] Dokuz Eylül Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, İzmir, dalkilic@cs.deu.edu.tr

1. GİRİŞ

Radyo frekansı ile tanımlama (radio frequency identification - RFID) etiketlerinde yapısal nedenlerden dolayı hesaplama kısıtları mevcuttur. Bu kısıtlar en büyük etkisini güvenlik alanında göstermektedir [1]. RFID etiketi üzerinden alınan verinin okuyucuya ve okuyucudan alınan verinin RFID etikete havadan iletilmesi aşamasında bilginin güvenli bir kanaldan ve güvenli bir yöntemle iletilmesi önem kazanmaktadır. Özellikle son zamanlarda ortaya çıkan, RFID teknolojisi ile bütünleşik duyargalar yapısına sahip etiketler, çok çeşitli alanlarda kullanılmaya başlanmıştır. Bunlar stok takibinden [2], sağlık verilerinin veya varlıklarının takibine kadar [3] geniş bir yelpazeye sahiptir. Sağlık, inşaat, madencilik, vb. yüksek risk içeren alanlarda bilginin doğru iletilememesi veya kötü niyetli kişiler tarafından müdahaleye açık olması çok ciddi zararlar ortaya çıkarabilir. Bu gibi sorunlar göz önünde bulundurulduğunda sistem kaynakları da dikkate alınarak güncel güvenlik tehditlerine karşı dirençli bir yapı kurulması çok büyük önem taşımaktadır.

RFID, bir nesne ya da bireye ait tanım verisini kablo kullanılmadan radyo dalgaları vasıtası ile iletmeye yarayan sistemleri tanımlayan genel bir terimdir [4]. RFID etiketleri güç kaynaklarına bakılarak üç sınıfa ayrılabilir. Bunlardan ilki aktif etiketlerdir. Bu etiketler dâhili olarak üzerlerinde bulunan bir enerji kaynağından (pil, batarya vb.) güç elde etmektedir. İkinci tür olan pasif RFID etiketlerinin kendi güç kaynakları yoktur ve genellikle etiketler okuyucu sinyallerini elektriksel kuvvete dönüştürmek yolu ile enerjilerini temin ederler [5]. Üçüncü tür ise yarı pasif (yarı aktif) etiketlerdir. Yarı pasif etiketlerde dâhili bir güç kaynağı vardır. Bu güç kaynağı sadece etiket üzerindeki duyarga vb. donanımların güç ihtiyaçlarının karşılanmasında kullanılır [6]. Okuyucuya gönderilecek radyo sinyalleri için pasif etiketlerde olduğu gibi okuyucunun anteninden gönderilen sinyalden güç elde ederler.

RFID etiketlerinden verinin okunabilmesi için özel okuyucuların kullanılması gerekmektedir [7]. RFID okuyucusu, etiketi okuyabilmek veya etiketin hafızasındaki veriyi elde etmek için öncelikle antenine enerji yükler. Anten enerji yüklemesi ile radyo dalgaları yaymaya başlar ve pasif etiketin aktif hale gelmesini sağlar. Aktif hale gelen etiket, üzerindeki veriyi serbest bırakır [4]. Serbest kalan ve radyo dalgaları ile ortamda yayılan veri, anten tarafından algılanarak RFID okuyucusuna iletilir. Okuyucu da bu veriyi ilgili bilgisayara gönderir. RFID etiketleri üzerinde toplanan veriler üretici kodu, ürün tipi, sıcaklık ve nem gibi bazı bilgileri içerebilir [8, 9]. Bu süreçte anten, RFID okuyucusu ve etiketi arasındaki iletişimi sağlayan temel araçlardan biridir. Antenin boyutuna ve şekline bağlı olarak çalışma frekansı ve diğer performans öğeleri farklılıklar gösterir [10].

Kablosuz tanımlama ve algılama platformu (wireless identification and sensing platform - WISP), bataryasız kablosuz duyargalar (sensörler) sınıfında yer almakta olup sıcaklık ve ivmeölçer duyargalarına sahip, oda büyüklüğündeki alanlarda ortamdaki radyo frekansı yayan okuyucudan gelen dalgalardan güç üreten pasif bir ultra yüksek frekans (ultra high frequency - UHF) RFID etiketidir. Bu basit yapı, çok çeşitli dağıtık algılama uygulamalarına izin verir. Ucuz ve küçük boyuttaki duyargalar, detaylı ve mütevazı ölçümleme yapabilmeleri ile son yıllarda daha fazla ilgi toplamaya başlamıştır [11]. Klasik pasif RFID etiket sistemlerinde, ortamdaki yüksek güçlü okuyucular, sadece tanımlayıcı bilgilerini okuyucuya dönebilen ve etiket olarak adlandırılan bataryasız cihazları sorgularlar. WISP ise RFID etiketlerini duyargalar ile zenginleştirmeyi amaçlamıştır. Bu sayede, ortamdan yapılan ölçümlemeler de okuyucuya iletilebilmektedir.

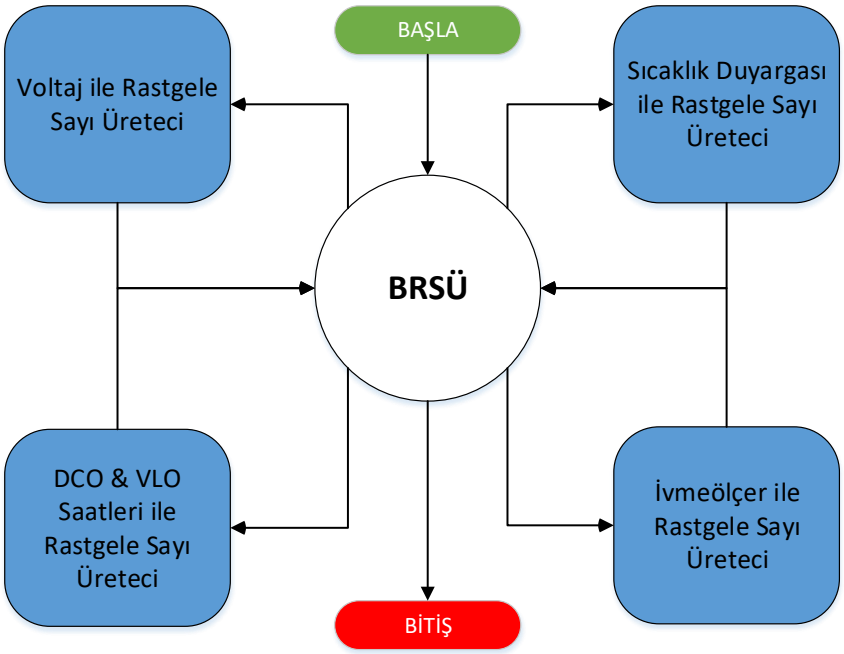
WISP etiketinin üzerinde sıcaklık, ivmeölçer gibi duyargalar bulunurken, kamera vb. cihazlarla birlikte çalışması da sağlanmıştır [12]. WISP üzerinde yer alan ivmeölçer ADXL362, 3 eksenli 2 µA'den daha az tüketimi olan çok düşük enerjili bir ivmeölçerdir ve bu entegre sıcaklık duyargasına sahiptir. [13].

Bu çalışmada, RFID etiketlerinin temel özellikleri ve özel bir UHF RFID etiketi olan WISP hakkında genel bilgilere yer verilerek bu bilgiler ışığında WISP etiketi ile okuyucu arasındaki güvenliğin sağlanmasında en temel konu olan rastgele sayı üretiminde kaynak kullanımı düşük bir öneri getirilmiştir.

2. bölümde çalışmada kullanılan 4 adet rastgele sayı kaynağı detaylı olarak anlatılmakta, ardından bu kaynaklardan elde edilen sayıların rastgeleliğini ölçmek için kullanılan test paketi açıklanmaktadır. 3. Bölümde, geliştirilen rastgele sayı fonksiyonu açıklanmakta ve fonksiyon çıktısı sayıların rastgele sayı test paketinden geçirilmiş sonuçları verilmektedir. Son bölümde ise elde edilen sonuçlarla ilgili youmlara ve gelecek çalışmalara yer verilmiştir.

2. DONANIMSAL GERÇEK RASTGELE SAYI KAYNAKLARI

Rastgele sayı üreteçleri (RSÜ), günümüzde bankacılıkta ve veri transferinde güvenliği sağlamak amacıyla devamlı olarak kullanılmaktadır. Üreteçleri üretiliş kaynaklarına göre grupladığımızda, karşımıza iki tip üreteç çıkmaktadır. Bunlardan ilki donanımın direkt olarak kullanılması ile oluşturulan gerçek rastgele sayı üreteçleri (GRSÜ), diğeri ise yazılım aracılığı ile oluşturulan sözde rastgele sayı üreteçleridir (SRSÜ). Yazılım vasıtası ile rastgele sayı üretmek genellikle daha hızlı fakat daha düşük rastsallığa sahiptir [14]. Diğer taraftan, donanım üzerinde üretim daha yavaş iken yazılımsal üreteçlere tohum (seed) değeri üretmek için kullanılırlar.



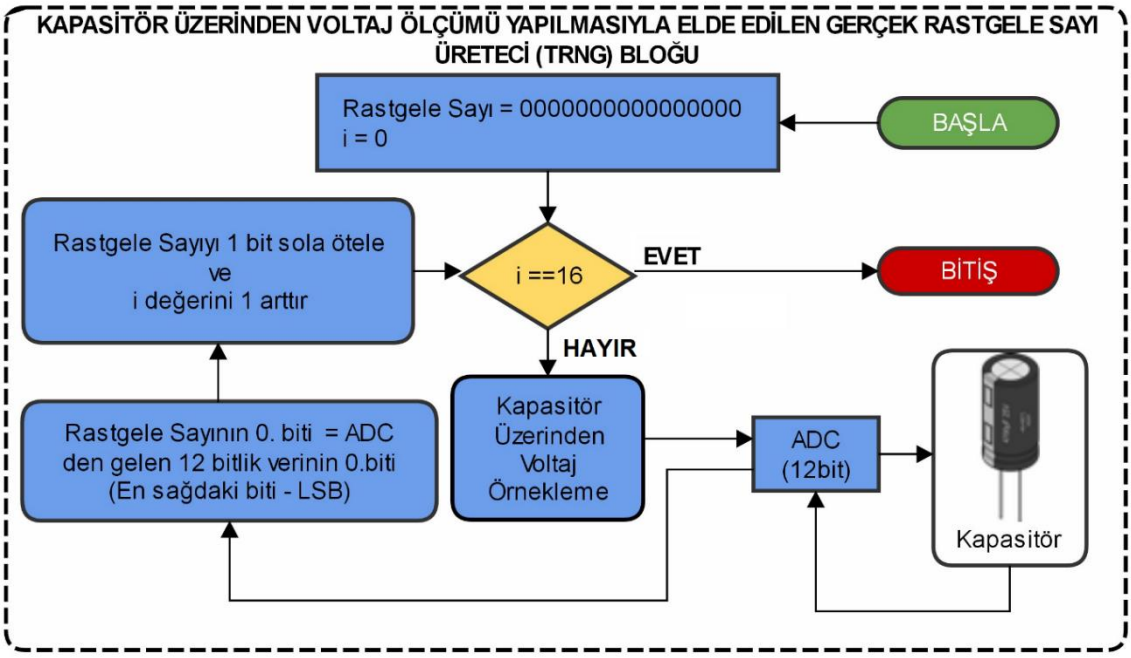
Şekil 1. Rastgele sayı üreteci genel görünümü

UHF Elektronik ürün kodu (electronic product code - EPC) 2. nesil (2^{nd} generation - Gen2) standardına sahip etiketlerin işlem gücünün her geçen gün artması ve EPC Gen2

standardına kriptografik algoritmaların da eklenmesiyle standart olarak kabul edilen kimlik doğrulama protokolü [15] üzerinde düzenlemeler ihtiyaç haline gelmiştir. WISP etiketi üzerinde rastgele sayı üretimi için kullanılan rand() fonksiyonu bulunmaktadır. Ancak, bu fonksiyonun rastgeleliği çok yetersizdir [16]. Bu çalışmada gerçek rastgele sayının elde edilmesi için WISP üzerindeki duyargalardan [17], birbirinden bağımsız iki farklı saatin saat farkından [16] ve voltaj ölçümünden yararlanılarak elde edilen birden fazla kaynaktan gelen veriler kullanılmıştır. Bu şekilde oluşturulmuş gerçek rastgele sayı üreteci Şekil 1'de görüldüğü gibi sırası ile kapasitör üzerinden yapılan voltaj örneklemesi ile oluşturulan üreteç, sıcaklık duyargasından elde edilen verilerle oluşturulan üreteç, sayısal olarak kontrol edilen osilatör (digitally controlled oscillator - DCO) ve çok düşük frekanslı osilatörün (very low frequency oscillator - VLO) saat farklarından faydalanılarak oluşturulmuş üreteç ve ivmeölçer duyargası ile oluşturulmuş üreteçtir.

2.1. Kapasitörden elde edilen rastgele sayı üreteci

WISP'in kapasitöründe biriken voltaj miktarını analog dijital çevirici (analog digital converter - ADC) üzerinden örnekleyerek sayısal değer elde edilebilmektedir. Rastgele sayı üretiminde ise voltaj değerinin tek veya çift olduğunu belirleyen sağdan ilk biti (least significant bit - LSB) kullanılmıştır [18]. 16 bitlik bir rastgele sayı üretebilmek için 16 örnekleme yapılmıştır. Her bir örnekleme işleminde elde edilen sayısal değerin sağdan ilk biti alınarak, rastgele sayımızın sağdan ilk biti olarak belirlenmiştir. Bu işlem sonrasında sayının tüm bitleri bir kez sola ötelenmiştir. Bu şekilde 16 çevrim sonucunda 16 bitlik bir rastgele sayı elde edilmiştir. Bu çevrimin her bir adımı Şekil 2'de görülmektedir.

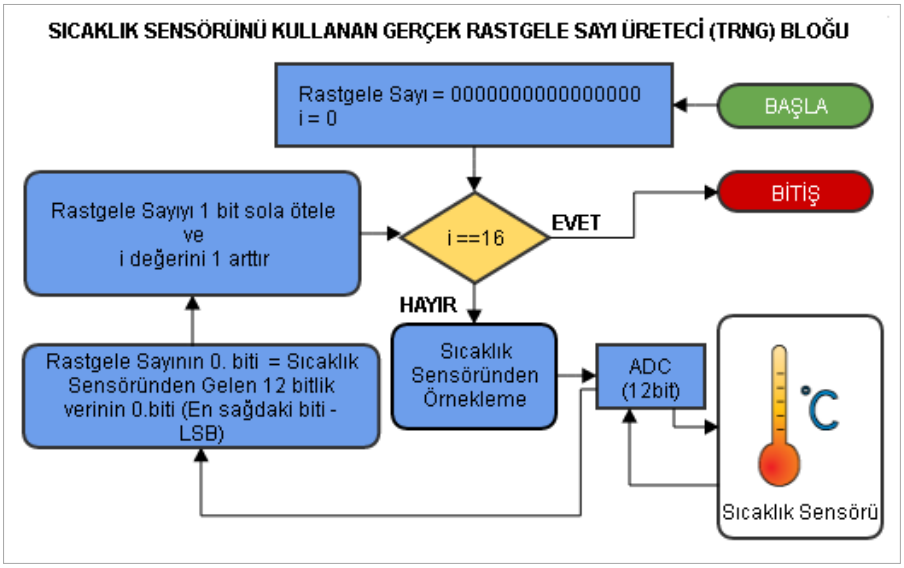


Şekil 2. Kapasitör üzerinden voltaj örneklemesi ile rastgele sayı üretilmesi

2.2. Sıcaklık duyargasından elde edilen rastgele sayı üreteci

Sıcaklık duyargası ile rastgele sayı üretimi (Şekil 3), kapasitörden elde edilen voltaj değeriyle rastgele üretimiyle aynı şekilde yapılmakta olup tek fark gerçek rastgele sayı

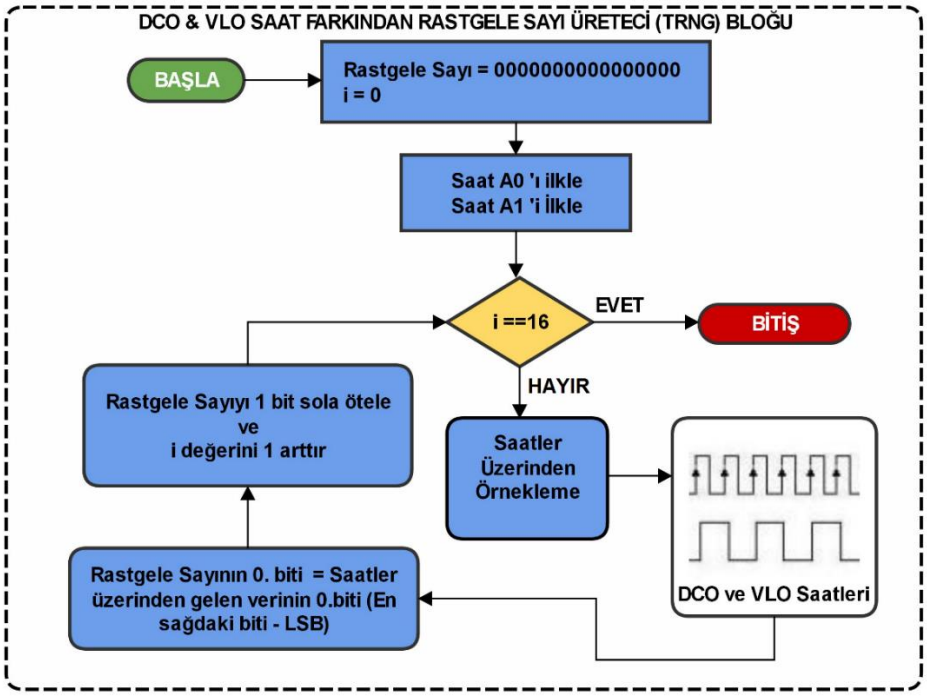
kaynağının sıcaklık duyargası olmasıdır. Bir önceki yöntemde olduğu gibi her seferinde 1 bitlik rastgele sayı elde edilir.



Şekil 3. Sıcaklık duyargası ile rastgele sayı üretilmesi

2.3. Saat farklarından elde edilen rastgele sayı üreteci

Bu durum için WISP üzerindeki MSP430 işlemcisinin iki farklı saatinden yararlanılmıştır. İki farklı saat, iki farklı süreölçere (timer) sinyal üretmek için kullanılır. Alt sistem ana saati (Subsystem master clock – SMCLK) DCO ile çalışmaktadır ve bu osilatör 1, 8, 12 ve 16 Mhz için sıfırlanabilir. Aynı şekilde yardımcı saat (Auxiliary clock – ACLK) VLO ile çalışmaktadır ve 12 Khz'de çalışan bu osilatör de sıfırlanabilir. Tüm bu işlemleri yapmak için gerekli yazmaçlar MSP430 işlemcisinde bulunmaktadır. Her iki saatin zaman farkı rastgele sayı üretimi için Şekil 4'te gösterildiği gibi kullanılmıştır [16].

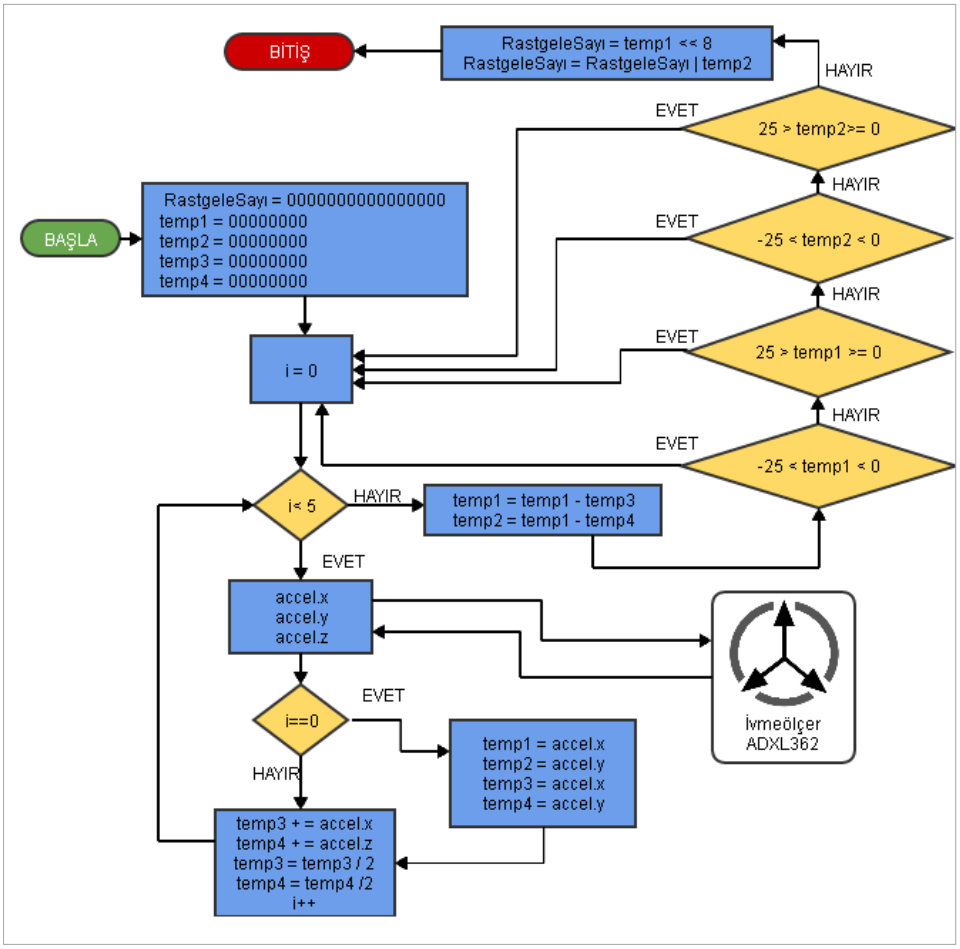


Şekil 4. DCO ve VLO saat farkından faydalanılarak rastgele sayı üretilmesi

2.4. İvmeölçer duyargasından elde edilen rastgele sayı üreteci

İvmeölçer duyargasında sayı üretimi diğer duyargalardaki yöntemden farklı bir yöntemle yapılmıştır. WISP'in hareketsiz kaldığı durumlarda en üst düzey hassasiyet ile her bir örneklemede farklı sayılar üretebilmek için bazı matematiksel işlemler yapılmış ve uygun sonuçlar elde edildiğinde bunlar rastgele sayı üretiminde kullanılmıştır. İlgili işlemin adımları Şekil 5'de ayrıntılı olarak gösterilmiştir.

Şekil 5'de gösterildiği şekilde öncelikle ivmeölçerden x, y ve z değerleri alınmıştır. 5 defa alınan ivmeölçer değerleri temp1, temp2, temp3 ve temp4 isimli değişkenlere atanmış ve her bir değişken üzerinde Şekil 5'de görülen matematiksel işlemler gerçekleştirilmiştir. Bu işlemlerin ardından temp1 ve temp3 değişkeni kullanılarak temp1 değişkeni, temp1 ve temp4 değişkeni kullanılarak temp2 değişkeni elde edilmiştir. temp1 ve temp2 değişkenlerinin değerleri -25 ve 25 aralığındaysa tüm işlemler baştan tekrarlanmıştır. Eğer bu aralıkta değilse, temp1 değişkeninin son 8 biti sola kaydırılarak temp2 değişkeninin son 8 biti ile değiştirilmiştir. Bu işlemin sonucunda ivmeölçerden gelen 3 değer kullanılarak 16 bitlik bir rastgele sayı üretilmiştir. WISP'in hareketsiz kalabileceği öngörüldüğünden bir döngü ile 5 kez ölçümleme yapılmış ve bu ölçümleme sonucunda yukarıda belirtilen matematiksel işlemlerle konumdaki değişiklik tespit edilmeye çalışılmıştır. Buradaki değişim farkının -25 ile +25 gibi bir aralıkta çıkması durumunda üretilen rastgele sayıların tekrar ettiği gözlemlenmiş ve bu nedenle değişimin yeteri kadar büyük olmadığı varsayılarak tekrar sayı üretimi yapılmıştır.



Şekil 5. İvmeölçer duyargası ile rastgele sayı üretilmesi

2.5. Rastgele sayı testi

4 farklı duyargadan elde edilen sayıların rastgeleliğini test etmek için her bir duyargadan 1 milyon adet 16 bit sayı elde edilmiştir. Elde edilen bu sayıların kabul görmüş rastgele sayı testi olan Standartlar ve Teknoloji Ulusal Enstitüsü (National Institute of Standards and Technology – NIST) [19] testine tabi tutulduğunda testten başarısız oldukları Çizelge 1'de görülmektedir. Çizelge 1'in üst kısmında verilmiş olan sonuçlar, 4 GRSÜ için de ortak olup tümünde sıfır sonucu elde edilmiştir. Bu da sayıların testlerden geçemediğini göstermektedir. Alt kısımda ise "Longest Run", "Nonperiodic Templates" ve "Linear Complexity" testlerinin bazılarında oluşan sıfırdan farklı değerler verilmiş, fakat sadece "Linear Complexity" testinden 3 üreteç geçmeyi başarmıştır. Çizelge 1'in ilk sütununda belirtilen testler NIST test paketini oluşturmaktadır ve bu testler hakkında detaylı açıklamalar NIST test paketi dokümanında [19] bulunmaktadır.

NIST testi sonuçlarından da açık ve net şekilde görüldüğü gibi bu üreteçlerin ürettiği sayılar, NIST test paketi içerisindeki tek bir test dışında tüm testlerden kalmaktadır. Sonuçlar, bu donanımsal kaynaklardan elde edilen sayıların direk olarak rastgele sayı kaynağı olarak kullanılamayacağını göstermektedir. Donanımsal kaynakları tohum olarak kullanan bir sözde rastgele sayı üreteci daha iyi sonuçlar üretebilir.

Çizelge 1. Gerçek rastgele sayı üreteçlerinin NIST sonuçları

İstatistiksel Test	**P-Değeri**				**Oran**				**Durum**			
Rastgele Sayı Üreteci	T1	T2	T3	T4	T1	T2	T3	T4	T1	T2	T3	T4
Frequency	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Block Frequency	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Cumulative Sums	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Runs	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Rank	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
FFT	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Overloading Templates	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Universal	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Apen	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Random Excursions	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Random Excursions Variant	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Serial	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	0,00000	X	X	X	X
Longest Run	0,00000	0,00000	0,00000	0,00000	0,28486	0,00000	0,00000	0,00000	X	X	X	X
Nonperiodic Templates	0,00000	0,00000	0,00000	0,00000	0,00170	0,00170	0,00170	0,00170	X	X	X	X
Linear Complexity	0,213309	0,000089	0,20443	0,21331	0,87500	1,00000	1,00000	1,00000	√	X	√	√

T1: Voltaj örneklemesi ile oluşturulmuş GRSÜ T2: Sıcaklık duyargası kullanılarak oluşturulmuş GRSÜ
T3: DCO-VLO farkı kullanılarak oluşturulmuş GRSÜ T4: İvmeölçer kullanılarak oluşturulmuş GRSÜ

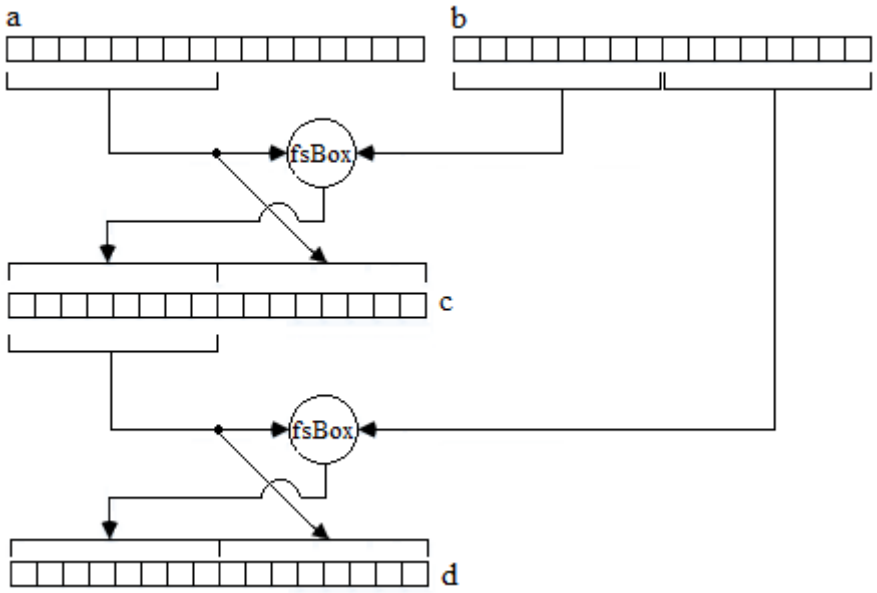
3. BASİTLEŞTİRİLMİŞ RASTGELE SAYI ÜRETECİ

Kullanılan donanımsal kaynakların rastgele sayı üretimi için yeterli olmadığı görüldüğünden, 4 farklı duyargadan gelen sayılar geliştirilen basitleştirilmiş rastgele sayı üreteci (BRSÜ) algoritmasına tohum olarak verilmiştir. BRSÜ algoritması aynı veri şifreleme standardı (data encryption standard - DES) şifreleme algoritmasında olduğu gibi Feistel yapısı [20] üzerinden şekillendirilmiştir. Yerine koyma kutuları (substitution box – sbox), özel veya (XOR) ve öteleme (shift) işlemlerinden oluşan ihtiyacı karşılayacak bu yeni algoritmanın meydana getirdiği SRSÜ aşağıdaki gibi tanımlanmıştır. BRSÜ algoritmasının temel adımlarından birini oluşturan sDES fonksiyonun şematik gösterimi ise Şekil 6'da verilmiştir.

```
uint32_t BRSU(uint16_t a,uint16_t b,uint16_t c,uint16_t d){
     uint16_t e,f;
     uint32_t m,n,x,y;

     e = sDES(a,b);
     f = sDES(c,d);
     m = e;
     n = f;
     m = (m<<16) | f;
     n = (n<<16) | e;
     x = (m^(m>>17)) ^ ((m^(m>>23))<<13);
     y = (n^(n>>22)) ^ ((n^(n>>17))<<11);
     return x ^ y;
}

uint16_t sDES(uint16_t a,uint16_t b){
     uint8_t leftside, rightside, rightsidenext;
     leftside  = ((a >> 8) & 255);   // ((a >> 8 ) & (0000000011111111))
     rightside = a & 255;            // (a & (0000000011111111))
     rightsidenext = leftside;
     leftside  = fsBox(leftside,((b >> 8) & 255));
     rightside = rightsidenext;
     rightsidenext = leftside;
     leftside  = fsBox(leftside,(b & 255));
     rightside = rightsidenext;
     return (leftside << 8 ) | rightside;
}
```



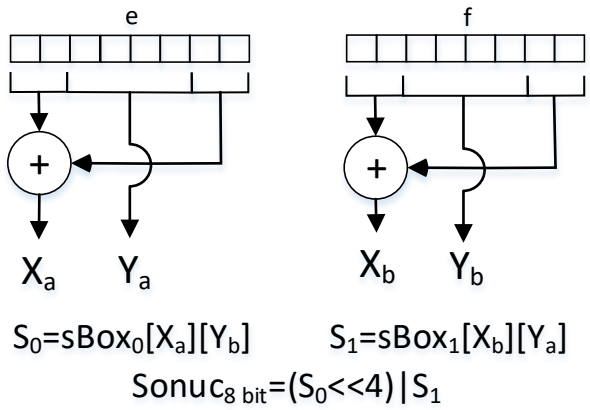
Şekil 6. sDES fonksiyonu yapısı

BRSÜ fonksiyonuna girdi olarak verilen değerler sırası ile voltaj örneklemesi ile elde edilmiş rastgele sayı, sıcaklık sensöründen elde edilmiş rastgele sayı, DCO ve VLO saat farkından elde edilmiş rastgele sayı ve ivmeölçerden elde edilmiş rastgele sayıdır. İlk çalıştırılan sDES fonksiyonunda (e = sDES(a,b)) voltaj değeri Şekil 6'da görülen a'yı; sıcaklık değeri ise Şekil 6'da ifade edilen b'yi oluşturmaktadır. a'nın ikinci sekiz biti (sol 8 bit) ve b'nin ikinci sekiz biti (sol 8 bit) Şekil 7'de gösterilmiş olan fsBox fonksiyonuna girdi olarak gönderilir. fsBox fonksiyonunun çıktısının ardına a'nın ikinci 8 biti eklenir ve c sayısı elde edilir. c'nin ikinci 8 biti ve b'nin ilk 8 biti fsBox fonksiyonuna girdi olarak verilir ve elde edilen çıktı d sayısının ikinci 8 bitini oluşturur. d'nin ilk 8 bitine c'nin ikinci 8 biti aynen aktarılır.

Çizelge 2. BRSÜ yerine koyma kutuları [21]

E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D
4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C

Şekil 7'de fsBox fonksiyonu verilmiştir. fsBox fonksiyonuna girdi olarak gelen 16 bit, tekrar e ve f olarak ikiye bölünür. e değerinin ilk 2 ve son 2 biti XOR işleminden geçirilerek X_a değeri, f değerinin ilk 2 ve son 2 biti XOR işleminden geçirilerek X_b değeri elde edilir. e değerinin ortadaki 4 biti Y_a'yı, f değerinin ortadaki 4 biti ise Y_b'yi oluşturur. X_a değeri Çizelge 2'nin üst kısmında belirtilmiş olan yerine koyma kutusunda ($sBox_0$) satır seçmek için, Y_b değeri ise sütun seçmek için kullanılır. Yerine koyma kutusundan 4 bitlik bir sayı elde edilir (S_0). X_b değeri Çizelge 2'nin alt kısmında belirtilmiş olan yerine koyma kutusunda ($sBox_1$) satır seçmek için, Y_a değeri ise sütun seçmek için kullanılır. Yerine koyma kutusundan 4 bitlik bir sayı elde edilir (S_1). S_0 değeri sola 4 bit kaydırılarak, sağ 4 bitine S_1 değeri yerleştirilir. Elde edilen sonuç fsBox fonksiyonunun çıktısıdır.



Şekil 7. fsBox fonksiyonu işlemleri

Tüm bu işlemlerin sonucunda BRSÜ algoritması 32 bitlik rastgele sayı üretmektedir. Üretilen bu sayılar, NIST test paketinde test edildiğinde Çizelge 3'de verilen sonuçlar elde

edilmiştir. Bazı testler için farklı değişkenlerle test tekrarlandığından bu testler için sonuç değerlerinin ortalamaları alınmıştır.

Çizelge 3'de elde edilen sonuçlara göre BRSÜ rastgele sayı üreteci NIST test paketindeki tüm testlerden geçmiştir. Algoritmada kullanılan 4 farklı gerçek rastgele sayı üretecinin sonuçlara olan etkisini araştırmak için 3 gerçek rastgele sayı üretecinin sonuçları aynı şekilde sDES fonksiyonundan geçirilmiş ve elde edilen sayılar NIST test paketiyle test edilmiştir. Bu testler sonucunda üretilen sayıların NIST test paketi içerisinde yer alan Frequency, BlockFrequency, CumulativeSums, Runs, OverlappingTemplate, ApproximateEntropy ve Serial testlerinden geçemediği gözlemlenmiştir. Kullanılan sDES fonksiyonu Feistel yapısından şekillendirilmiştir, ancak DES algoritmasında olduğu gibi 16 turdan oluşmamaktadır, Feistel yapısının daha basit halini içermektedir. Bunun nedeni WISP'in kaynaklarının sınırlı olmasıdır. WISP'in kaynak sınırlamasından dolayı Feistel yapısının basitleştirilmesi ile oluşan dezavantaj, 4 farklı gerçek rastgele sayı kaynağı kullanılarak giderilmiştir.

Çizelge 3. BRSÜ NIST sonuçları

İstatistiksel Test	P-Değeri	Oran	Durum
Frequency	0,122325	1,0000	**GEÇTİ**
Block Frequency	0,671779	1,0000	**GEÇTİ**
Cumulative Sums (Ortalama)	0,214797	0,9844	**GEÇTİ**
Runs	0,671779	1,0000	**GEÇTİ**
Longest Run	0,253551	1,0000	**GEÇTİ**
Rank	0,043745	0,8438	**GEÇTİ**
FFT	0,468595	1,0000	**GEÇTİ**
Nonperiodic Templates (Ortalama)	0,484277	0,9898	**GEÇTİ**
Overloading Templates	0,082177	1,0000	**GEÇTİ**
Universal	0,739918	0,9688	**GEÇTİ**
Apen	0,100508	0,9688	**GEÇTİ**
Random Excursions (Ortalama)	0,269708	1,0000	**GEÇTİ**
Random Excursions Variant (Ortalama)	0,369314	0,9974	**GEÇTİ**
Serial (Ortalama)	0,003495	0,8907	**GEÇTİ**
Linear Complexity	0,213309	1,0000	**GEÇTİ**

4. SONUÇLAR

NIST test paketinden elde ettiğimiz sonuçlara göre, ortaya koyulan BRSÜ adındaki yeni algoritmanın çıktısında oluşan sayıların tam bir rastgelelik sağladığı görülmektedir. NIST test paketinde yapılan test işlemi için WISP üzerindeki her bir duyargadan 1.000.000 adet rastgele sayı üretilmiştir. Rastgele sayı üretiminin zaman bakımından hesaplanabilmesi için fonksiyon 10.000 defa çalıştırılmış ve yapılan ölçümler neticesinde BRSÜ fonksiyonu ile bir adet rastgele sayı üretiminin yaklaşık 4,859 ms sürdüğü görülmüştür. Bu test sonuçlarından da anlaşılacağı üzere bu yeni üreteç, WISP üzerindeki kriptografik işlemlerde kullanılmak amacıyla rastgele sayı üretimi için güvenli ve hızlı bir yapı sunmaktadır. Ayrıca ortaya konulan çözümde uygulanan işlemlerin bit bazında olması, kaynakların kısıtlı olması dolayısıyla performans açısından da büyük avantajlar ortaya koymaktadır. WISP üzerinde yapılacak yeni çalışmalarda, elde edilen sonuçları geliştirmek amacıyla genetik algoritmalar, vb. yeni yöntemler denenecektir.

TEŞEKKÜR

Bu çalışma 215E225 no'lu araştırma projesi ile TÜBİTAK tarafından desteklenmiştir.

KAYNAKLAR

[1] Juels A., "Minimalist cryptography for low-cost RFID tags", The Fourth International Conference on Security in Communication Networks – SCN 2004, LNCS Cilt 3352, Springer-Verlag, 2004, s. 149–164.

[2] Zhonga R.Y., Huanga G.Q., Lana S., Daic Q.Y., Chend X., Zhange T., "A big data approach for logistics trajectory discovery from RFID-enabled production data", International Journal of Production Economics, Cilt 165, Temmuz 2015, s. 260-272.

[3] Özcanhan M.H., Dalkılıç G.**,** Utku S., Alkım E., Akis S., "Akıllı ambulans araçlarına doğru ilk adımlar: RFID ambulans varlıkları takibi", XIX. Türkiye'de İnternet Konferansı, 2014.

[4] Khong G., White S., "Moving right along: using RFID for collection management at the parliamentary library", Information-Online 12 th Exhibition & Conference, Sidney, 2005, s. 1-12.

[5] Manish B., Shahram M., "RFID field guide: deploying radio frequency identification systems", Prentice Hall PTR, ABD, 2005, s. 24-29.

[6] Nikitin P.V., Ramamurthy S., Martinez R., Rao, K.V.S., "Passive tag-to-tag communication," 2012 IEEE International Conference on RFID, Nisan 2012, s. 177-184, 3-5.

[7] Finkenzeller K., "RFID handbook: fundamentals and applications in contactless smart Cards and identification" 2nd ed., Rachel Waddington, John Wiley & Sons, Ltd, West Sussex, 2003, s. 1-393.

[8] Aggarwal C.C., Ashish N., Sheth A., "The internet of things: A survey from the data – centric perspective", Managing and Mining Sensor Data, Springer, 2013.

[9] Want R., "An introduction to RFID technology", Pervasive Computing, IEEE, cilt 5, sayı 1, 2006, s. 25-33.

[10] Dziadak K., Kumar B., Sommerville J., "Model ort he 3D location of buried assets based on RFID technology", J. Comp. Civil Eng., 2009, s. 148–159.

[11] Cullerand D.E., Mulder H., "Smart sensors to network the world", Scientific American, cilt 290, sayı 6, Haziran 2004, s. 84–91.

[12] Naderiparizi S., Parks A. N., Kapetanovic Z., Ransford B., Smith J. R., "WISPCam: A Battery-Free RFID Camera", IEEE RFID, 15-17 Nisan, 2015.

[13] ADXL362, http://www.analog.com/en/products/mems/mems-accelerometers/adxl362.html#product-overview, Erişim tarihi: 15.12.2015.

[14] Turner N., "Software vs. Hardware RNG's.", iGaming Business Magazine, 2005, http://www.tstglobal.com/assets/downloads/1268986797a16.pdf, Erişim tarihi: 20.01.2016.

[15] Özcanhan M.H., Dalkılıç G., Utku S. , "Analysis of two protocols using EPC Gen-2 tags for safe in patient medication", INISTA 2013: IEEE International Symposium on Innovations in Intelligent Systems and Applications, 2013, s. 1-6.

[16] Fujdiak R., Mišurec J., Petr M., Rášo O., "Random number generator in MSP430 x5xx families", Elektrorevue, cilt 4, sayı 4, 2013, s. 70-74.

[17] Voris J., Saxena N., Halevi T., "Accelerometers and randomness: perfect together", 4th ACM Conference on Wireless Network Security, 2011, s. 115-126.

[18] Buccini M., "An MSP430F11x1 sigma-delta type milli volt meter", 2000, http://www.ti.com/lit/an/slaa104/slaa104.pdf, Erişim tarihi: 20.01.2016.

[19] Rukhin A., Soto J., Nechvatal J., Smid M., Barker E., Leigh S.,Levenson M., Vangel M., Banks D., Heckert A., Dray J., Vo S. "A statistical test suite for the validation of random number generators and pseudo random number generators for cryptographic applications", 2010, http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html. Erişim tarihi: 20.01.2016.

[20] Feistel H., "Cryptography and computer privacy", Scientific American, Mayıs 1973, Cilt 228, Sayı 5, s. 15-23

[21] Sun H., Chiang T., Chen X., "Digital video transcoding for transmission and storage", CRC Press, 2004, s. 277-278.

ÖZGEÇMİŞ / CV

Gökhan DALKILIÇ; Yrd. Doç. Dr. (Asst. Prof. Dr.)

Bilgisayar Mühendisliği lisans derecesini 1997 yılında Ege Üniversitesi, İzmir, Türkiye'den, Bilgisayar Bilimleri yüksek lisans derecelerini 1999 yılında Güney Kaliforniya Üniversitesi, Los Angeles, Amerika'dan ve 2001 yılında Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü'nden ve Bilgisayar Mühendisliği doktora derecesini 2004 yılında Dokuz Eylül Üniversitesi, İzmir, Türkiye'den aldı. Ocak 2003'ten Aralık 2003'e kadar Orta Florida Üniversitesi, Florida, Orlando, Amerika'da misafir öğretim elemanıydı. Halen Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği, İzmir, Türkiye'de yardımcı doçent olarak görev yapmaktadır. Araştırma alanları hafif kimlik doğrulama protokolleri, kriptografi ve doğal dil işlemedir. 50'den fazla akademik yayını ve 4 kitabı bulunmaktadır.

He received the B.S. degree in Computer Engineering from Ege University, Izmir, Turkey, in 1997, the M.S. degrees in Computer Science from University of Southern California, Los Angeles, USA, in 1999, and from Ege University International Computing Institute, Izmir, Turkey, in 2001, and Ph.D. degree in Computer Engineering from Dokuz Eylul University, Izmir, Turkey, in 2004. He had been a visiting lecturer in University of Central Florida, Orlando, USA from January 2003 to December 2003. He has been an Assistant Professor of the Department of Computer Engineering of Dokuz Eylul University, Izmir, Turkey. His research areas are cryptography, statistical language processing and computer networks. His fields of studies are lightweight authentication protocols, cryptography, and natural language processing. He has over 50 papers and four books to his name.