KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

UHF RFID ETİKETLER İÇİN SRAM TABANLI DONANIMSAL RASTGELE SAYI ÜRETECİ TASARIMI

YÜKSEK LİSANS TEZİ

Elektrik-Elektronik Müh. İhsan SOLAK

Temmuz 2008
TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

UHF RFID ETİKETLER İÇİN SRAM TABANLI DONANIMSAL RASTGELE SAYI ÜRETECİ TASARIMI

Elektrik-Elektronik Müh. İhsan SOLAK

Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsünce
"Elektronik Yüksek Mühendisi"
Unvanı Verilmesi İçin Kabul Edilen Tezdir.

Tezin Enstitüye Verildiği Tarih : 06.06.2008
Tezin Savunma Tarihi : 10.07.2008

Tez Danışman : Yrd. Doç. Dr. İsmail KAYA
Jüri Üyesi : Doç. Dr. Temel KAYIKÇIOĞLU
Jüri Üyesi : Yrd. Doç. Dr. Hüseyin PEHLİVAN

Enstitü Müdür V. : Doç. Dr. Salih TERZİOĞLU

Trabzon 2008

ÖNSÖZ

Radyo frekans tanımlama (RFID) sistemleri radyo frekanslarını kullanarak durağan yada hareket halinde bulunan canlılar ve nesneleri tekil veya çoğul halde tanımlamakta kullanılmaktadır. RFID sistemlerinin uygulama alanlarına örnek olarak: ürün dağıtım zinciri uygulamaları, üretim, envanter muhasebesi ve kontrolü, hastane, hasta tanımlama, tedavi ve tıbbi kayıtların kontrolü, kütüphane, müze, gıda ve ilaç sanayinde özellikleri son kullanım tarihlerinin izlenmesi ve sahte ilaçların takibinde, ilaç tanımlamada, hayvanların kimlik ve aşı bilgilerinin izlenmesi ve pasaport uygulamaları verilebilir. Bu çalışmada EPC C1 G2 RFID standardında belirtilen çarpışma önleyici algoritma için kullanılması gereken bir rastlantısal sayı üreteci tasarlanmıştır. Bu tasarımın standardın getirdiği kriterlere uygun olup olmadığı araştırılmıştır.

Çalışmalarım boyunca bana değerli zamanını ayıran ve verdiği fikirler ile beni yönlendiren değerli hocam sayın Yrd. Doç. Dr. İsmail Kaya'ya ve hayatım boyunca her türlü maddi ve manevi desteklerini hiçbir zaman esirgemeyen aileme sonsuz şükranlarımı sunarım.

İhsan SOLAK
Trabzon 2008

İÇİNDEKİLER

Sayfa No

ÖZET

Radyo frekans tanımlama (RFID) sistemleri radyo frekanslarını kullanarak durağan yada hareket halinde bulunan canlılar ve nesneleri tekil veya çoğul halde tanımlamakta kullanılmaktadır. RFID sistemlerinin uygulama alanlarına örnek olarak: ürün dağıtım zinciri uygulamaları, üretim, envanter muhasebesi ve kontrolü, hastane, hasta tanımlama, tedavi ve tıbbi kayıtların kontrolü, kütüphane, müze, sanat galerisinde ürün tanımlama, kontrol ve güvenlik uygulamaları, gıda ve ilaç sanayinde özellikleri son kullanım tarihlerinin izlenmesi ve sahte ilaçların takibinde, ilaç tanımlamada, hayvanların kimlik ve aşı bilgilerinin izlenmesi ve pasaport uygulamaları verilebilir.

RFID sistemlerde birden çok etiket okuma alanı içerisine girdiğinde aynı anda cevap verdiklerinden bunların ayrıştırılıp okunabilmesi için çarpışma önleyici algoritmaların kullanılması gerekir. Bunun için bir çok algoritma geliştirilmiştir. Bu çalışmada EPC C1 G2 RFID standardında belirtilen çarpışma önleyici algoritma için kullanılması gereken bir rastlantısal sayı üreteci tasarlanmıştır. Bu tasarımın standardın getirdiği kriterlere uygun olup olmadığı araştırılmıştır.

Her bir etikette bulunacak olan bu rastlantısal sayı üreteci diğer etiketlerden bağımsız olarak değişik sayılar üretecek ve bir sayıcı tarafından kullanılacak bu sayılar, etiketin diğer etiketlerden değişik zaman aralıklarında cevap vermesini sağlayacaktır.

Anahtar Kelimeler: RFID, Rastlantısal Sayılar, RFID Etiketi, SRAM, EPC C1G2 VHDL, FPGA, RNG

SUMMARY

Design of SRAM Based Hardware Random Number Generator for UHF RFID Tag Applications

Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify people or objects. The most common applications are payment systems, access control and asset tracking. Increasingly, retail and pharma companies are looking to use RFID to track goods within their supply chain, to work in process and for other applications.

Tag collision occurs when more than one tag reflects back a signal at the same time, confusing the reader. Different designs have used different systems for having the tags respond to the reader one at a time. These involve using algorithms to "singulate" the tags. Since each tag can be read in milliseconds, it appears that all the tags are being read simultaneously. For that reason, many algorithms have been developed. In this study, a hardware random number generator is designed to use in EPC C1G2 RFID standard based tags applications. It is researched that this design is suitable for standard or not.

Key Words: RFID, Hardware Random Number Generator, RFID Tag, SRAM EPC C1G2, VHDL, FPGA, RNG

ŞEKİLLER DİZİNİ

Sayfa No

SEMBOLLER DİZİNİ

2D : İki boyutlu
ABD : Amerika Birleşik Devletleri
AES : Kriptolama Algoritması
ASIC : Uygulamaya Dönük Tümleşik Devre
CATA : Kanada Hava Taşımacılık Şirketi
Ce : Chip Enable
CEPT : Avrupa Posta ve Telekomünikasyon Birliği
EPC : Elektronik Ürün Kodu
FFT : Hızlı Fourier Dönüşümü
FC : Faraday Kafesi
FPGA : Alanda Programlanabilen Kapı Dizisi
G : Giga
GaAs : Galyum-Arsenid
Gen : Nesil
GRSÜ : Gerçek Rartgele Sayı Üreteci
HDL : Donanım Tanımlama Dili
HF : Yüksek Frekans
Hz : Hertz
I : Çerçeve antenden akan akım
IC : Tümleşik devre
ID : Kimlik
ISO : Standard
KET : Kısa Mesafe Erişimli Telsiz Cihazlarının Kurma ve Kullanma Esasları
k : Kilo
LCD : Likit Kristalli Ekran
LF : Düşük Frekans
LFSR : Doğrusal Geribeslemeli Kaydırmalı Hafıza
m : Mili
M : Mega
MOSFET : Metal-Oxide-Semiconductor-Field-Effect Transistor

MRAM : Manyetik Rastgele Erişimli Bellek

N : Çerçeve anten sarım sayısı

NXP : Firma adı

ODTÜ : Ortadoğu Teknik Üniversitesi

OE : Output Enable

R : Anten Yarıçapı

RF : Radyo Frekans

RAM : Rastgele Erişimli Bellek

RFID : Radyo Frekans Tanımlama

RNG : Rastgele Sayı Üreteci

ROM : Sadece Okunabilen Hafızasında

SHF : Süper Yüksek Frekans

SRAM : Static Rastgele Erişimli Bellek

SRSÜ : Sözde Rastgele Sayı Üreteci

UHF : Ultra Yüksek Frekans

W : Watt

WE : Write Enable

x : Anten düzlemine dik doğrultudaki alıcı uzaklığı

XST : Xilinx Synthesis Tool

1. GENEL BİLGİLER

1.1. Giriş

Radyo frekans tanımlama (RFID) sistemleri radyo frekanslarını kullanarak durağan yada hareket halinde bulunan canlılar ve nesneleri tekil veya çoğul halde tanımlamakta kullanılmaktadır. RFID sistemleri ilk olarak 1940 lı yılların başlarında İngiltere'de dost ve düşman uçaklarının tanımlanmasında kullanılmıştır. Bunu 1970 li yıllarda nükleer malzeme izleme uygulamaları takip etmiş, ticari uygulamaları 1990 lı yıllarda başlamıştır. RFID sistemlerinin uygulama alanlarına örnek olarak: ürün dağıtım zinciri uygulamaları, üretim, envanter muhasebesi ve kontrolü, hastane, hasta tanımlama, tedavi ve tıbbi kayıtların kontrolü, kütüphane, müze, sanat galerisinde ürün tanımlama, kontrol ve güvenlik uygulamaları, otomotiv endüstrisinde ürün özellikleri ve bakım bilgi kayıtlarının takibinde, akıllı kart uygulamalarında, ürün satın alma, seyahat kartları uygulamaları, polis ve emniyet uygulamaları (delillerin ve delil noktalarının kayıtları), taşımacılıkta (konteyner ve bagaj bilgileri takibinde), değerli ürün üretimi ve değerli ürün izlenmesinde, kamu taşımacılığı, spor karşılaşmaları, kayak pist kullanımı gibi bilet gerektiren uygulamalar, karayolları geçiş ücretlerinin toplanması, gıda ve ilaç sanayinde özellikleri son kullanım tarihlerinin izlenmesi ve sahte ilaçların takibinde, ilaç tanımlamada, hayvanların kimlik ve aşı bilgilerinin izlenmesi ve pasaport uygulamaları verilebilir [1].

Radyo frekans tanımlama sistemleri, tanımlama uygulamasını radyo dalgalarını kullanarak gerçekleştirdiğinden alıcı ve verici arasında doğrudan temas ve doğrudan görüş şartına gerek duymamaktadır.

RFID ticari uygulamalarının en önemlilerinden biri olan kamu taşımacılığı 1995 yılında Fransa (Paris) otoyol ücretlendirilmesinde, 1997 de Kore'de "otobüs kartı" uygulamasında ve Thailand (Bangkok) metro ücretlerinin toplanması uygulamasıyla başlanmıştır. Ekim 2004 yılında Japonya'da (Tokyo) cep telefonlarına gömülü RFID çip vasıtasıyla taksi ücretlerinin telefon sahibinden kredi kartından alınması pilot uygulama olarak başlatılmıştır.

RFID erişim ve güvenlik uygulamaları, laboratuar, hava limanları, okullar gibi güvenlik bedeniyle erişimin kontrollü olarak uygulandığı alanlarda gerçekleştirilmektedir. Mart 2004 yılında Kanada hava taşımacılık şirketi (Canadian Air Transport Authority

CATA) havalimanlarında erişimin kontrollü olarak verildiği alanlarda RFID teknolojisi ile erişim uygulaması başlatmıştır.

Nisan 2005 yılında Japonya Tokyo Rikkyo ilkokulunda öğrencilerin gerçek zamanlı okula geliş gidişlerinin takibi için RFID kart uygulaması başlatmıştır. RFID kartlarının öğrencilerin kişisel eşyelarına (çanta, mont vb) monte edilmesi istenmiştir. Aktif RFID etiketleri dolayısı ile öğrencilerin okula geldiği ve okuldan ayrıldığı saatler gerçek zamanlı olarak tespit edilebilmektedir. Yine kullanılmakta olan aktif etiketler 10 metre uzaklıktan okunabildiği için okula okula giriş ve çıkışlarda öğrencilerin durdurulmalarına özel giriş-çıkış kapısına ve özel yollara gerek duyulmamaktadır. Öğrenci erişim kontrolünde kullanılmakta olan RFID kartlar öğrenciye ait özel bir numara ile tanımlanmakta öğrencilerin kişisel tanımlama bilgilerini içermemektedir. Böylece kartın kaybolması durumunda kimlik bilgilerine erişme mümkün olmamaktadır. Yine RFID uygulaması sayesinde okula geliş-gidiş kontrolünün tanımlanmış web sitesi üzerinden takibi ve aktif RFID etiketlerinin gerçek zamanlı olarak hangi konumda (sınıfta, kantinde, kütüphanede vb) olduğu bilgisi kamera görüntüsü ile izlenebilmektedir. Diğer yandan kaza veya doğal afet olaylarında acil elektronik posta tabanlı bilgilerle okul idaresi ve aileler zamanında uyarılabilmektedir.

RFID ürün dağıtım zinciri uygulamasında; RFID etiketler ürün dağıtım zincirinde yer alan ürünlerin doğrudan izlenmesini sağlar. Üreticinin ön kapısı ile satıcının arka kapısı arasında gerçekleşen kayıp ve çalıntı olaylarını engeller. RFID uygulaması ile ürünün bulunduğu noktaların izlenmesi mümkün olmaktadır.

RFID Tıp ve eczacılık uygulamalarında; hastalara uygulanmış küçük RFID etiketler ile özellikle yeni doğanlar, zihinsel özürlü hastalar ve yaşlıların uzun vadeli tedavilerinin takibi ve hasta bakımları mümkün olmaktadır. Özellikle bilinci kapalı konuşma özrü olan hastalara uygulanmış RFID etiket sayesinde daha önce uygulanmış tedavilere erişilebilmektedir.

Eczacılık uygulamalarında ilaçların izlenmesi, doğru adrese yönlendirilmesi, yasal yollarla üretilmemiş olan ilaçların tedarik zincirine girmesinin engellenmesi, kullanım süresi dolmuş olan ilaçların raflardan alınması RFID etiketlerle mümkün olmaktadır.

RFID tarım ve gıda endüstrisi uygulamalarında; RFID etiketleri ile tarladan alınan ürünlerin satış noktasına ulaşıncaya kadar geçirdiği aşamalar ve bekleme süreleri zarfında oluşacak bozulmalar takip edilmektedir.

RFID gıda endüstrisinde özellikle et ve et ürünleri gibi soğuk zincir gerektiren

uygulamaların takibinde uygulama alanı bulmaktadır. RFID tarım uygulaması Kasım 2004 de Namibia'dan İngiltere'ye dondurulmuş et ithalatında gerçekleştirilmiştir. RFID etiketleri ile et yüklü konteynerin yolculuk sırasında açılıp açılmadığı bilgisi, mühürlerin kırılma bilgisi, konteynerlerin yolculukları sırasında tanımlanmış güzergahlarda kalış süreleri bilgilerinin takibi mümkün olmuştur.

RFID e-devlet uygulamalarında; ehliyet ve pasaportların RFID etiket taşıması, evsizlerin RFID etiketlerle takibi, şehirde yaşayanlarla şehre dışarıdan gelenlerin izlenmesi suretiyle terörizmin önlenmesi, paraların üzerine konacak RFID etiketlerle çalıntı ve tahribatın önlenmesi uygulamaları verilmektedir.

RFID savunma ve gizlilik uygulamalrında; kişilerin kimliklerinin RFID etiketleri ve biyometrik uygulamalarla belirlenmesi böylece yetkisiz kişilerin bilgiye erişiminin engellenmesi ile savunmanın güçlendirilmesi hedeflenmektedir.

RFID kütüphane uygulamarı; ödünç verilen ve rafta bulunan kitapların gerçek zamanlı olarak izlenmesi için RFID teknolojisinden faydalanılır. 2003 yılından beri Japonya'da (Tokyo) 2004 yılından beri Hollanda'da kütüphanelerde RFID uygulaması gerçekleştirilmektedir.

RFID spor uygulamaları; araba yarışlarında arabalara yerleştirilen RFID etiketleri maraton yarışlarında sporcunun ayakkabısına monte edilen RFID etiketleri ile yarışı kazanan hassas olarak belirlenebilmektedir. Bunlara ek olarak özellikle kayak pistleri gibi ellerin bağımsız olarak kullanıldığı uygulamalarda RFID etiketleri kullanılmaktadır.

İngiltere Manchester futbol kulübü RFID etiketleri kullanarak taraftarlarının biletsiz olarak stadyuma girmesini sağlayan ilk futbol kulübüdür.

RFID tüketici uygulamaları; RFID günlük hayatımızda paralı yollarda, bürolarda ve kütüphanelerde aktif olarak kullanılmaktadır. Yakın gelecekte alışveriş merkezlerinde ve spor karşılaşmalarında da uygulama alanı bulacaktır.

RFID kişisel refah ve güvenlik uygulamaları; hastaların bakım ve tedavilerinde RFID teknolojisi kullanılmaktadır. Diğer taraftan RFID etiketlerin konuma duyarlı bilgisinin gerçek zamanlı olarak elde edilmesiyle kişisel güvenlik ve kişilerin (özellikle çocuk ve yaşlıların) ev dışında, parklarda ve şehirde takibini mümkün kılmaktadır.

1.2. Radyo Frekans Kimlik Tanıma Sistem Bileşenleri

Radyo frekans tanımlama sistemleri, radyo frekansı ile yapılan sorguları almaya ve

cevaplamaya olanak tanıyan etiket (transponder, tag), okuyucu (alıcı-verici) ve alınan bilgilerin depolandığı veri tabanından oluşmaktadır.

Radyo frekans kimlik tanıma sistem haberleşmesinde okuyucu radyo frekans sinyallerini gönderir. Okuyucunun radyo frekans alanına girmiş bulunan pasif etiket, haberleşmesi için gerekli olan enerjiyi bu alandan alır. Etiket haberleşmesi için gerekli olan enerjiyi aldığında, üzerinde depolanmış bilgiye göre taşıyıcı sinyali modüle eder. Modüle edilmiş taşıyıcı etiketten okuyucuya gönderilir. Okuyucu modüle edilmiş sinyali algılar, şifresini çözer ve okur. Son olarak alınan bilgi veri tabanının bulunduğu bilgisayara aktarılır.

Okuyucunun görevleri:

- Etikete enerji sağlar,
- Taşıyıcı sinyali gönderir,
- Etiket tarafından modüle edilmiş sinyali algılar, şifresini çözer ve okur.

Etiketin görevleri:

- Okuyucunun gönderdiği enerjiyi alır,
- Etiket içinde depolanmış bilgiye göre taşıyıcı sinyali modüle ederek okuyucuya gönderir.

1.3. RFID Etiketleri

RFID etiketi, radyo frekansı kullanılarak yapılan sorgulamaları alan cevaplayan sınırlı kapasitede belleğe sahip, taşınabilen, içinde bilgi barındıran, mikro yonga, anten ve taban malzemesinden oluşmaktadır. Mikro yonga etiketin üzerinde yer aldığı nesneye ilişkin bilgileri depolar. Anten radyo frekansı kullanarak nesneye ait bilgilerin okuyucuya gönderilmesini sağlar. Taban malzemesi ise etiketin nesne üzerine yerleştirilebilmesi için mikro yonga ve anteni çevreler. Etiketler kullanım yerlerine bağlı olarak değişik boyut ve fonksiyonda olabilmektedir.

RFID etiketleri fonksiyonları bakımından

- Aktif etiketler
- Pasif etiketler
- Yarı pasif etiketleri

olarak sınıflandırılırlar.

Aktif etiketler, devrelerinin çalışması ve cevap sinyali üretebilmelerini sağlayan güç

kaynağı içerirler. Etiket üzerinde yer alan pil dolayısıyla performansları ve haberleşme mesafeleri yüksektir. 1 km uzaklığa kadar sinyal gönderen aktif etiketler mevcuttur. Özellikle demiryolları ve denizyolları endüstrisi taşımacılığında kullanılan aktif etiketler GPS ve uydu haberleşme sistemleri ile uyumlu çalışarak üzerine monte edildikleri ürünün dünya üzerinde izlenmelerine olanak tanımaktadır. Pil içermeleri dolayısı ile bakım gerektirmekte olup maliyetleri diğer etiket çeşitlerine göre yüksektir.

Pasif etiketler, kendi güç kaynakları yoktur. Okuyucudan aldıkları güçle çalışırlar. Haberleşme mesafeleri küçük olmalarına rağmen bakım gerektirmemeleri basit ve ucuz olmaları dolayısı ile tercih edilmektedirler.

Yarı-pasif etiketler güç kaynağı içerirler. Üzerlerinde yer alan pil sadece mikro yonganın devrelerine sağlamaktadır. Haberleşme pasif etiketlerde olduğu gibi okuyucudan gelen sinyallerle aktif olan etiketle sağlanır. Sözkonusu etiketler sıcaklık ve hareket bilgisi gibi algılayıcı (sensör) giriş bilgilerini depolamak için kullanılırlar. Yarı pasif etiketlerin haberleşme mesafeleri büyük olup güvenilirdirler. Üzerlerinde yer alan güç kaynağı dolayısı ile okuyucuya daha hızlı cevap verebilmektedirler. RFID etiketleri depoladıkları bilgiler açısından

- Sadece okunabilen
- Okunabilen/Yazılabilen
- Okunabilen/Yazılabilen/Yeniden yazılabilen

olarak sınıflandırılırlar.

Sadece okunabilen etiketler, genellikle pasif RFID etiketleridir. Bilgi depolama kapasiteleri küçüktür. Üretim sırasında üzerlerine yazılan bilgiyi saklarlar ve bu bilgi değiştirilemez. Bu nedenle uygulamalarda tanıtıcı etiket olarak kullanılmaktadırlar. Sadece okunabilen etiketlerin sistemlerde merkezi bilgisayar sistemi ve veritabanı radyo frekans tanımlama sisteminde kullanılan nesnelerle ilgili tüm işlemlerin kontrolünü gerçekleştirir.

Okunabilen/Yazılabilen etiketler, bilgi depolama kapasiteleri yüksek etiketlerdir. Yazılabilme özelliği olan bu etiketlere okuyucu kapsama alanındayken yeni bilgiler eklenebilir yada etiket üzerinde var olan bilgiler değiştirilebilir. Bu özellikleri dolayısı ile hareketli veri tabanı gibi davranabilirler. Maliyetleri sadece okunabilen etiketlere göre yüksektir.

Okunabilen/Yazılabilen/Yeniden yazılabilen etiketler üzerindeki bilgilerin değiştirilebilme özelliği ve yüksek depolama kabiliyetleri dolayısıyla geniş uygulama alanına sahiptirler. Haberleşme açısından cevap verme süreleri kısadır. Maliyetleri diğer

etiketlere göre fazladır.

1.4. RFID Okuyucu İşlevi

Okuyucu etiketle haberleşebilmek için gerekli enerjiyi, radyo frekans kimlik tanıma sisteminin çalışma frekansına bağlı olarak seçilen çalışma frekansında zamanla değişen manyetik alan yaratarak sağlamaktadır. Okuyucu ürettiği, zamanla değişen manyetik alanı genellikle çerçeve anten vasıtasıyla etikete gönderir. Okuyucunun dairesel çerçeve anteninden akım aktığında çerçeve antene dik düzlemde oluşan manyetik alan şiddeti

$$H = \frac{INR^2}{2\left(R^2 + x^2\right)^{3/2}} \tag{1}$$

olarak hesaplanmaktadır [2,3]. Burada

I = Çerçeve antenden akan akım

N = Çerçeve anten sarım sayısı

R = Anten yarıçapı

x = Anten düzlemine dik doğrultudaki alıcı uzaklığını tanımlar.

Denklemden de görüleceği üzere manyetik alan şiddeti mesafenin küpü ile ters orantılıdır. Endüktif bağlaşım prensibine dayanan radyo frekans kimlik tanıma sistemlerinde alanın mesafenin küpüyle ters orantılı olarak zayıflaması ana sınırlayıcı faktördür.

Okuyucu tarafından gönderilen radyo frekans enerjisi etiketin fonksiyonlarını yerine getirebilmesi için taşıyıcı sinyal içermektedir. Taşıyıcı sinyal etikete enerji sağlamanın yanı sıra, etiketteki bilgilerin okuyucuya gönderilmesini ve haberleşmenin senkronizasyonunu sağlar. Etiket okuyucu tarafından gönderilen sinyali alır ve modüle ederek tekrar okuyucuya gönderir. Etiket tarafından gönderilen okuyucu antenine gelen sinyaller geri saçılım sinyalleri olarak adlandırılır. Okuyucu doğrultusunda geri saçılan sinyaller okuyucu tarafından şifresi çözülerek alınır.

1.5. Okuyucunun Tasarım ve Performansı

Okuyucu aynı zamanda alıcı-verici olduğundan alıcı ve verici kısımlarını içermektedir. Verici sinyali osilatörde üretir, kuvvetlendirir, filtreler ve akord devresi

yardımıyla antenden etiket doğrultusunda gönderir. Alıcı kısımda ise etiketin göndermiş olduğu bilgiler zarf dedektörü ile işlenir, filtrelenir ve kuvvetlendirilerek mikro kontrolöre veri tabanına gönderilmek üzere iletilir.

(1) ifadesine göre anten yarıçapı artırıldığında manyetik alan şiddeti de artmaktadır. Diğer taraftan NI da artırıldığından H da artacaktır. Manyetik alan şiddetinin artırılması için her iki durumda da sınırlamalar mevcuttur.

Anten yarıçapı büyütüldüğü zaman okuyucu portatif özelliğini kaybedecek ve maliyeti artacaktır.

NI değeri artırıldığında okuyucu anten endüktansı artacak, yüksek endüktans yükü de büyük oranda geriye yansıyan güce sebep olacaktır.

Sonuç olarak NI çarpanını mümkün olduğu kadar küçük tutup haberleşme için gerekli manyetik alan şiddeti seviyesini elde edecek sistem tasarlanmalıdır.

1.6. RFID Frekans Bandları

Radyo frekans tanımlama sistemleri için spektrum kullanımı Avrupa Posta ve Telekomünikasyon Birliği (European Conference of Postal and Telecommunications Administrations-CEPT) tarafından düzenlenmiş ve standartlar tanımlanmıştır. Spektrumun Türkiye'de kullanımı ise 06.03.2004 tarih 25394 sayılı Resmi gazetede yayınlanan "Kısa Mesafe Erişimli Telsiz Cihazlarının (KET) Kurma ve Kullanma Esasları" yönetmeliği uyarınca Telekomünikasyon Kurumu tarafından belirlenmştir [4].

RFID sistemleri kısa mesafe uygulamaları için Düşük Frekans (LF) 120-135kHz; akıllı kart ve etiket uygulamaları için Yüksek Frekans (HF) 13.56MHz; aktif düşük güçlü etiket uygulamaları için Ultra Yüksek Frekans (UHF) 433MHz ve tedarik zinciri uygulamaları için Ultra Yüksek Frekans (UHF) 860-960MHz ve aktif etiklerle daha büyük haberleşme nesafeleri ve daha yüksek hızlarda veri iletimi için Süper Yüksek Frekans (SHF) 2450MHz frekans bandlarını kullanmaktadır.

Avrupa Posta ve Telekomünikasyon Birliği RFID haberleşmesi için Avrupa Standardı olarak Eylül 2004 de ETSI EN 302 208 standardının uygulanmasına karar vermiştir. ETSI EN 302 208 standardı 865-868 MHz frekans bandını kullanan 3 MHz band genişliğine sahip Söylemeden Dinle (LBT) protokolü ile 2W eşdeğer izotropik radyasyon güç seviyelerinde haberleşmeyi öngörmektedir.

Spektrumun Türkiye'de kullanımı ise 06.03.2004 tarih 25394 sayılı Resmi gazetede

yayınlanan "Kısa Mesafe Erişimli Telsiz Cihazlarının (KET) Kurma ve Kullanma Esasları" yönetmeliği uyarınca, fabrika, depo, antrepo ve büyük alışveriş merkezleri gibi kapalı lokal alanlarda ya da mülkiyeti kullanıcıya ait kampüs veya açık alanda frekans sinyalleri yoluyla, veri iletimi, dosyalama, depolama, yer belirleme, depo arşivleme, yakınlık sensörü, el cihazlarından data transferi, kablosuz etiket vb. işlemleri yapan ve sadece dahili kullanıma izin verilen sistemler, 500 mW eşdeğer izotropik radyasyon güç seviyelerinde haberleşmeyi öngörmektedir.

1.7. Karşılaşılan Problemler ve Çözümler

Radyo frekans tanımlama teknolojisi ile akıllı evler ve akıllı şehirler geliştirilmeye başlanmıştır. Mart 2004 de Kore hükümeti Seul'de akıllı ev müzesi açmıştır. Bu müzede; evde yiyecekleri sipariş veren buzdolabı ağı, kablosuz güvenlik sistemleri, gün ışığına göre aydınlatmanın otomatik olarak yanıp söndüğü saydınlatma sistemleri, akıllı çamaşır makinaları (çamaşırların üzerinde yer alan RFID etiketlere göre çamaşırları yıkayan) ve yaşlıların/fiziksel engelli kişilerin evde tek başına yaşayabilmelerini sağlayan RFID etiketleri ile yaşam sergilenmektedir. Evde yaşayan yaşlı ve fiziksel engelli kişilerin üzerlerinde yer alan RFID etiketler yardımıyla hasta kişilerin ilaçlarını alıp almadıkları, tansiyon ve nabız bilgileri, evdeki konum bilgileri (banyoda, odada veya bahçede) ve sağlık durumu bilgileri kontrol edilmektedir.

Evler akıllı evlere doğru geliştikçe insanlarda daha akıllı olmaya doğru donanımsal olarak gelişim göstermektedir. Washington Üniversitesi ve Intel işbiliği sonucunda geliştirilen akıllı saat sayesinde evden/kamusal alandan ayrılırken yanımıza almamız gerekenleri (anahtar, para cüzdanı, gözlük, cep telefonu vb.) hatırlatmaktadır.

Kısaca radyo frekans tanımlama sistemleri mağazalardaki ürün uygulamalarından çıkıp hızla sosyal yaşantımıza girmekte ve yaşamımızın tüm kesimlerinde yer almaktadır.

Günlük hayatta uygulama yeri ve fonksiyonları açısından RFID etiketleri barkodlara göre pahalı olabilmektedir. RFID sistemlerinin mevcut envanter sistemlerine entegrasyonu yatırım maliyeti gerektirmektedir. (Okuyucu, uygun yazılım, uygun veri tabanı) Metal, sıvı içeren kablar, dielektrik özellik gösteren malzemeler üzerine monte edilen RFID etiketlerinin interferans etkileri nedeniyle okunamaması radyo frekans tanımlama sistemlerinin dezavantajı olarak gözükmektedir.

Değişik ülke ve bölgelerde çalışan RFID sistemlerinin çalışma frekansları ve çıkış

güçleri açısından birlikte çalışılabilirlik özelliği taşımaması şimdilik sorun olarak yer alsa bile sistemler arası uyum çalışmaları devam etmektedir. Özellikle pasif etiketlerin okuma mesafelerinin kısa olması radyo frekans tanımla sistemleri için dezavantaj oluşturmaktadır. Aynı anda birden çok RFID etiketinin okunabilmesi için çakışma önleyici algoritmaların ve şifreli okuma yazma algoritmalarının geliştirilmesi gerekmektedir.

1.8. RFID Standartları

Yüksek frekans çözümleri için standardizasyon tamamlanmış olmakla birlikte, ultra yüksek frekans konusunda çalışmalar halen devam etmektedir. Yüksek frekans için tamamlanmış standart ISO 14443 ve ISO 15693 olarak tanımlanmıştır. Ultra yüksek frekans için çalışmaları devam eden standart ISO 18000 ve EPC Class 0, Class 1 ve Gen2 olarak belirlenmiştir.

EPC ile ürün tanımlamasında kullanılan RFID teknolojisinin kullanılmasını küresel boyutta düzenlemek amacıyla, RFID etiketlerinde ve okuyucularında kullanılmak üzere Class 1 Gen 2 (Sınıf 1 Nesil 2) standardını geliştirmiş ve söz konusu standardın dünya genelinde uygulanabilmesi için çeşitli frekans aralıkları belirlemiştir.

İkinci nesli (Gen2) önemli yapan birkaç unsur vardır. Birincisi, ortaya çıkarılabilecek RFID altyapı elemanlarının, dünya çapında birlikte kullanılabilirliğini de sağlayarak, temellerini oluşturur. Ayrıca şu an kullanılan “Class 0” ve “Class 1” okuyucu ve etiketlerle karşılaştırıldığında daha hızlı okuyabilme özelliği ve kısıtlara karşı daha az duyarlılık gibi işlevsel ilerlemeleri beraberinde getirir. Güvenlik kavramı da daha gelişmiş şifreleme teknolojileri, şifre koruma ve yetkilendirme ile yapılmaktadır.

1.9. RFID Güvenliği İçin Önerilen Çözümler

Güvenlik ve gizliliğin sağlanması için farklı çözüm yöntemleri önerilmektedir. Bu yöntemler burada derinlemesine incelenmeyecek olsa da önemli olarak görülenler üzerinde durulacaktır.

“Kill” Komutu: Bu çözüm Auto-ID Center ve EPCglobal tarafından önerilmiştir. Her bir tagın tekil bir şifresinin olduğu, örneğin 24 bit, ve üretim aşamasında programlandığı bir yöntemdir. Doğru şifre verildiğinde tag tamamen kullanılamaz hale gelmektedir.

“Faraday Cage” Yaklaşımı: Bir diğer yöntem tagların herhangi bir elektromanyetik dalgaya maruz kalmasının engellenmesidir. Faraday Kafesi (FC) adı verilen metal bir ağ veya folyodan yapılmış olan bir kap birçok frekanstaki sinyali kırabilmektedir.

“Aktif Sinyal Bozma” Yaklaşımı: FC’ye alternatif olarak, elektromanyetik dalgaların engellenmesinin bir diğer yolu da radyo kanalının rahatsız edilerek, RF sinyal bozma yönetimin uygulanmasıdır. Bu işlem, aktif olarak radyo sinyalleri yayan bir cihaz kullanılarak yapılabilir. Böylece RFID okuyucuların okuma işlemi yapmaları engellenmiş olacaktır.

Blogger Tag: Bir okuyucu tarafından gönderilen sorguyu birden çok tag yanıtlarsa, okuyucu çakışma olduğunu varsayacaktır. Tag okumada kullanılan en önemli protokoller “ALOHA” (13.56 MHz) ve “tree- walking” protokolleridir (915 MHz). Bunlardan, kısa frekans kullanan “tree- walking” protokolünün çalışma mantığı kullanılarak pasif bir sinyal bozma yöntemi geliştirilmiştir. “Blocker tag” adı verilen bu yöntem ile yeniden tasarlanan bir tagın, olası tüm seri numaralarının benzetimini yapması ve RFID okuyucuyu yanıltması sağlanmıştır.

Ahlaki Kanun Tasarıları: Garfinkel tarafından ortaya konulan RFID ahlaki değerleri, RFID sistemler kullanılırken uyulması önerilen bazı maddeler içermektedir. Garfinkel, bu değerleri kanun haline getirme amacı olmasa da, firmaların uymasını önermektedir.

Klasik Şifreleme: Her tagın anonim(isimsiz) bir ID'ye sahip olması, E(ID) gibi, böylece gerçek ID nin saklanması düşüncesini savunur. Genel veya simetrik anahtar şifreleme algoritması içerebilir veya tag ID'sine bağlanmış rastgele bir sayı olabilir. İzlenme sorununu çözmek için, tag içerisindeki anonim ID yeniden şifreleme ile sıkça değiştirilmelidir. Feldhofer tarafından önerilen yetkilendirme mekanizması, basit bir iki taraflı sorun-yanıt algoritması üzerine kuruludur. Bu yaklaşımın sorunu, RFID tagın AES özelliğinin olmasına ihtiyaç duymasıdır. Genel anahtar şifreleme kullanan yeniden şifreleme üzerine kurulu yapılar da vardır.

Hash fonksiyonlarına dayanan yöntemler: Güvenlik sorunlarını aşmak için daha yaygın şekilde kullanılan bir çözümde hash fonksiyonlarıdır.

Temel PRF özel yetkilendirme yöntemleri: Molar tarafından önerilen yöntem, tag ve okuyucular arasında ortak bir yetkilendirme mantığı üzerine kuruludur. Bu protokol, tag ve okuyucu arasındaki mesajların korunması için paylaşılan bir anahtar ve Pseudo-Random Function (PRF) kulllanır.

Ağaç tabanlı özel yetkilendirme ve atama ağacı: Hash yöntemlerinin önemli bir

olumsuz yanı, tagların tanımlanabilmesi için sunucuya fazla yüklenilmesidir. Molnar, bu yükün azaltılabilmesi için "Tree-Based Private Authentication" isimli bir yöntem önermiştir [5].

1.10. RFID'nin Geleceği

Birçok alanda kullanılabilen RFID "tag"ları ve okuyucuların, mobil öğrenmenin temel taşlarından olan taşınabilir bilgisayarlar ve cep bilgisayarları ile birleştirilmesiyle, öğrenme sürecine çevresel farkındalık, uyarlanabilirlik ve tepki verebilme yeteneğinin de kazandırılabilmesi mümkün olacak ve öğrencilerin konum bilgilerine göre ayrı ayrı öğrenme içeriklerine ulaşabilmesi sağlanabilecektir.

Radio Frequency Identification (RFID) halen gelişmekte olan bir teknoloji olduğundan kullanım modelleri ve bütünleşik mimarisi sürekli değişmektedir. RFID hzlı bir şekilde geleceğe hazırlanmakta; teknolojik gelişmeler, endüstriyel standartlardaki gelişmeler ve bu alana yapılan yatırımlar da RFID yi parlak bir geleceğin beklediğini işaret etmektedir.

Birbiriyle uyumsuz RFID standartları bu teknolojinin daha yavaş büyümesine sebep olmaktadır. Çoğu öncü RFID üreticisi kendi sistemini farklı frekans ve protokollerle üretmektedir. Yinede hem ABD'de hem de Avrupa'da bazı kurumlar RFID kullanımı için standartlar geliştirmeye çalışmaktadır.

RFID kullanımında küresellik gözönünde bulundurulmalı, RFID veri yapısı standarlara uygun olmalıdır. Standartların kullanımı okuyucu ve etiketlerin fiyatlarını düşüreceği gibi yeni buluşlarında artmasını sağlayacaktır. Bugün RFID kullanılan en yaygın standart "electronic product code (EPC)" olarak bilinen elektronik ürün kodudur.

Bugün RFID çalışmaları yönünü, radyo vericilerinin daha iyi yayın yapmasını sağlayabilecek olan Nano teknoloji kullanmaya doğrultmuştur.

RFID teknolojisi, hücresel telefonlardan sonra en hızlı gelişecek kablosuz teknoloji olarak görülmektedir ve 2009 yılına kadar %120 lik bir artış beklenmektedir. RFID kullanımının yaygınlaşması için anahtar gereklilik 0.3-0.5 Dolar civarında olan tag fiyatlarının düşmesidir. Nano teknolojinin bu seviyeyi 0.05 Dolara kadar düşürmesi ve RFID'nin yaygın kullanımını sağlaması beklenmektedir.

RFID tagların bir çoğu bakır veya alüminyum antenler kullanmaktadır. Nano teknoloji üreticileri ise bu antenleri nano boyutlarda parçalardan oluşan mürekkep baskı

kullanarak yapmayı başarmak için uğraşmaktadırlar. Kağıt üzerine antenler basmak daha hızlı ve ucuz üretim sağlayacaktır.

RFID tagların maliyetinin yarısını üzerlerindeki çipler oluşturmaktadır, bu nedenle araştırmalar bu çip kullanım yönteminin nano boyutlarda çözülmesi üzerine çalışmaktadırlar.

RFID mikro çiplerin kapasite attırımı konusunda ise Micromem firması "magnetic RAM" veya MRAM üzerinde çalışmaktadır. MRAM, RFID teknolojisine büyük yenilikler ve fırsatlar getirecektir. Elektrik enerjisini saklamak mantığına dayalı varolan bilgisayar belleklerinin aksine, MRAM, nano boyutlardaki manyetik bit dizileri ile bilgiyi saklar. MRAM üzerine yazma işlemi, her bir bit'in manyetik kutuplarını değiştirerek yapılır ve bu değer elektrik gereksinimi duymadan saklanabilir.

Bunun yanında, "flash memory" olarak tabir edilen hafıza cihazlarının aksine MRAM'ler radyasyona karşı da dirençlidirler. Bu özelliği ile MRAM'lerin, havayolları ve askeri alanlar gibi yerlerde bulunabilen X- ışını uygulamalarında kullanılabilirlikleri daha yüksektir.

Gelecekteki nanoteknoloji uygulamaları, mürekkep tabanlı RFID devrelerini mümkün kılarak silikon çip gereksinimini ortadan kaldırabilecektir. Bunun en iyi örneği tamamen mürekkepten geliştirilen bir prototip olan "Organic ID" dir ve maliyeti 0.01 doların altındadır. Organic ID'nin 5-10 yıl arasında yaygınlaşması beklenmektedir.

RFID, insanların, taşıdıklarının veya satın aldıklarının uzaktan ve habersiz izlenebilmelerini sağlayabildiği için özel yaşamı tehdit unsuru olarak görülebilmektedir ve kullanım karşıtları da bulunmaktadır. Ancak geliştiriciler ikinci nesil RFID'nin bu konuları da dikkate alarak gerçekleştirildiğini söylemektedirler; yeni nesil RFID etiketleri istenildiğinde okunamaz veya bir daha kullanılamaz hale getirilebilmektedirler.

RFID teknolojisi, konum bilgisinin kullanılması yoluyla öğrenme içeriğinin tek birey için uyarlanarak öğrenmenin daha etkin yapılabilmesini sağlayacak, dolayısıyla öğrenme sürecinin verimliliğini arttıracaktır.

1.11. RFID Performans Kriterleri

RFID çiplerinin kopyalanması oldukça zordur. Her etiket, güvenlik amacıyla üretici firma tarafından belirlenen ve değiştirilemeyen bir kimlik koduna sahiptir. Etiketteki bilgiler üzerine birden fazla koruma seviyesi eklenmektedir. Yeni Gen 2 standardındaki 32

bitlik şifreleme sayesinde yetkisiz kişilerin çip içerisindeki bilgilere ulaşması engellenmekte, çip kitlenmekte ve gerekirse kullanılmaz hale getirilmektedir.

RF etiketler üretim aşamasında kağıt yüzeyler arasına yerleştirilebildiği gibi sağlam plastik maddelerin içine de koyulabilmektedir. Böylece ürün takibi yapılacak zorlu ortamlarda maksimum dayanıklılık ve uzun etiket ömrü sağlamaya olanak tanınmaktadır.

Radyo frekans teknolojisi ile okuma yapılırken barkotta olduğu gibi etiketin okuyucuya yakın bir mesafede olması gerekmemektedir. Bunun nedeni radyo sinyellerinin maddeler arasından geçebilme özelliğidir. Bu sayede toplu sayımlar çok hızlı bir şekilde yapılabilmektedir. Palet ve kasalara yerleştirilen kutuların teker teker okutulması zorunluluğu ortadan kalkmaktadır. Bununla birlikte nesnelerin belli bir düzen içinde dizilmediği ortamlarda yapılacak uygulamalarda da önem taşımaktadır. Havaalanı bagaj takibi, postane paket düzenleme bu uygulamalardan bazılarıdır. Birden fazla RF etiketin bulunduğu ortamlarda bir okuyucunun tüm etiketleri okuyabilmesi de çok önemli bir diğer özelliktir. Bu özelliğe ek olarak okuyucular birçok etiketin arasından yalnız belirlenmiş olan etiketi okuma yeteneğine de sahiptir.

RFID okuyucusunun okuma kapasitesi; çipin frekansına, gücüne, etiketin aktif ya da pasif olmasına ve antenin yön hassasiyetine göre değişmektedir. Ortamda metal ya da sıvıların olması da okuma/yazma performansını etkilemektedir. Okunup yazılabilen etiketlerde, okuma kapasitesi genelde yazmadan daha yüksektir. Aktif etiketler de pasiflere göre daha geniş kapsama alanına sahiptirler.

RF etiketler barkoda göre çok daha yüksek hızda okunabilmektedir. RF okuyucular saniyede 50 etiket ve daha fazlasını okuyabilecek kapasiteye sahipken barkod tarayıcılar her defasında ancak bir barkod okuyabilmektedir. RF teknolojisinin bu özelliği çok sayıda nesnenin hızlı bir şekilde takibinin gerektiği uygulamalarda çok büyük avantaj sağlamaktadır. Buna bağlı olarak bilgi toplanması sürecinde zaman kaybı ve çalışan masrafları minimuma indirilebilmektedir.

RF etiketler barkoddan çok daha yüksek miktarda bilgi depolayabilmektedir. Linear/1D barkod yaklaşık 20 alfa nümerik karakter, 2D barkod ise maksimum 2,000 karakter depolayabilirken, çok gelişmiş RF etiketler 1Mbyte (bir milyon karakter) hafıza alanına sahiptir. Bu belirgin üstünlük daha fazla bilginin depolanmasına, daha fazla ürün özelliğinin izlenmesine ve takip kayıtlarının tutulmasını mümkün kılmaktadır.

RF etiketler frekans aralıklarına bağlı olarak da gruplandırılmaktadır. Değişik frekansların değişik özelliklerinden dolayı bazı değişik uygulamalara tatbik edilmesi daha

yararlı olur. Örneğin alçak frekans etiketleri daha az güç kullanma gereksinimleri olduğundan metalik olmayan maddelere daha etkili ulaşabilir. İçerdiği su oranı yüksek olan maddelerde (meyveler gibi) ideal kullanma alanı bulmakla beraber algılama mesafeleri oldukça düşüktür (0,33 metre).

Yüksek frekans etiketleri ise metalden oluşan objeler ve daha yüksek su içeren maddeler için kullanılabilir (1 metre). UHF frekansları ise her iki frekanstan daha uzun ve daha iyi veri transferi yapabilmektedir. Ne var ki UHF daha fazla güç ve arada metal engel olmamasını gerektirir. Bu nedenle burada okuyucu ile etiket arasında temiz bir alan olması gerekmektedir. UHF etiketleri üretim bitiş aşamasından malların stoklara devrine kadar verimli olarak kullanılabilir.

Alçak Frekans (LF) (<135 KHz) Pasif

- Sadece okunabilir veya okunup yazılabilir
- Daha uzun ve pahalı bakır anten
- Metal ve sıvılara bağlı performans kaybı daha düşük
- Kısa okuma mesafesi
- Büyük boyutlu

Yüksek Frekans (HF) (13.56 MHz) Pasif

- Sadece okunabilir, okunup yazılabilir veya bir kez yazılıp sürekli okunabilir
- Temassız akıllı kartlarda kullanım
- Alçak frekansa göre daha ucuz
- Metal ve sıvılara bağlı performans kaybı daha düşük
- Alçak frekansa göre daha uzun okuma mesafesi
- Büyük boyutlu
- Birden fazla etiketin okunabilmesi
- Yüksek haberleşme sürati

Ultra Yüksek Frekans (UHF) (868 MHz - 915 MHz) Pasif ve Aktif

- Sadece okunabilir, okunup yazılabilir veya bir kez yazılıp sürekli okunabilir
- Temassız akıllı kartlarda kullanım
- Yüksek frekansa göre daha ucuz
- Metal ve sıvılara bağlı performans kaybı düşük
- Yüksek frekansa göre daha uzun okuma mesafesi
- Büyük boyutlu

Mikrodalga (2.45GHz, 5.8GHz) Pasif ve Aktif

- Sadece okunabilir, okunup yazılabilir veya bir kez yazılıp sürekli okunabilir
- Ultra yüksek frekansa göre daha pahalı
- Metale bağlı performans kaybı daha düşük
- Sıvılara bağlı performans kaybı daha yüksek
- Ultra yüksek frekansa göre daha uzun okuma mesafesi
- Yüksek haberleşme sürati

1.12. Eski Bir Teknoloji: Barkod

Barkod; değişik kalınlıktaki dik çizgi ve boşluklardan oluşan ve verinin otomatik olarak ve hatasız bir biçimde başka bir ortama aktarılması için kullanılan bir yöntemdir. Barkod, ürünün kodu veya ürün ile ilgili açıklamalar içermemelidir. Barkod sadece o ürüne ait bir referans numarası içermelidir. Bu referans numarası bilgisayara tanıtılır ve ürüne ait detaylı bilgiler bilgisayarda tutulur. Daha sonra bu referans numarası kullanılarak o ürüne ait bilgiye erişilir.

Barkod ve RF etiketler arasındaki en önemli farklardan biri barkod teknoljisinde baskılı bir etiket optik bir okuyucu tarafından okunurken, RFID teknolojisinde yarı iletken bir etiketin radyo frekans teknolojisi kullanılarak sorgulanmasıdır. Bir barkod okuyucusu, barkodu okuyabilmek için barkodu görmelidir.

Teknolojileri karşılaştırırken dikkate alınması gereken konular okuma kapasitesi, okuma mesafesi, etiket dayanıklılığı, bilgi depolama kapasitesi, bilgi esnekliği, güvenlik, maliyet, standartlar, eğitim ve servis olarak belirlenebilir.

Barkodlu veri toplama uygulamaları ile karşılaştırıldığında RFID teknolojisinin bazı üstün yönleri mevcuttur;

- Zor çevre koşullarında kullanılabilmesi
- Kar, sis, buz, boya gibi çevresel faktörlerden etkilenmemesi
- RFID etiketlerinin içerdiği bilginin bir yardımcı elemana gerek olmadan okunabilmesi
- Aynı anda birçok etiketin okunabilmesi
- Tek bir etiketin bir defadan daha fazla kullanılabilmesi

1.13. Donanım Tanımlama Dili, HDL

HDL genel olarak programlanabilir ya da özel üretilmiş tümdevreler için tasarım dili olarak bilinen ve sayısal devre otomasyonunda kullanılan programlama dilidir. Tümdevre tasarımı ise belirli bir amaca hizmet eden özelleşmiş mantık ve devre tasarımını kapsayan elektrik mühendisliği alt dalıdır.

Tümdevre tasarımı analog ve sayısal tasarım olarak ikiye ayrılır. Analog tasarım güç devreleri, radyo dalgası devreleri gibi konularla ilgilenirken, sayısal tasarım ise mikroişlemciler, programlanabilir tümdevreler (FPGA), hafızalar (RAM, ROM, flash bellek) ve ürüne özel tümdevreler (ASIC) üretmek için kullanılmaktadır. Analog tasarım daha çok yarı-iletken cihazların verim ve kazanç gibi fiziksel özellikleriyle ilgilenmekte ve tümdevrelerde çok daha yüksek oranda fiziksel alan kaplamaktadır. Gelişmiş tümdevrelerde analog ve sayısal bölümler birlikte kullanılmaktadır.

Günümüzde kullanılan tümdevreler oldukça karmaşık bir yapıya haiz olmakla birlikte, hazır üretilen programlanabilir tümdevrelerde (FPGA) 300 binden fazla sayısal hücre bulunmaktadır ve bu hücrelerin her birinde 1000'den fazla transistör mevcuttur. Özel üretilen tümdevrelerde (ASIC) ise üst sınır bulunmamakta ve entegre içerisindeki transistör sayısı milyarları geçmektedir. Intel'in ürettiği ve yalnızca hafıza işlemleri için kullanılan SRAM tümdevresinde 2 milyar transistör ve bir Quad Core işlemci çekirdeğinde 800 milyon transistör bulunmaktadır.

Tümdevre tasarımı genellikle silikon taban üzerinde transistör, direnç, kapasite gibi elektronik bileşenlerin oluşturulması ve iletken metallerle bu bileşenlerin birbirine bağlanması işlemidir. Bu bileşenler birbirinden izole edilerek ve gerektiği yerlerde elektron yapılarıyla oynanarak (doping) istenilen özelliklere göre düzenlenir.

Özelleşmiş tasarımlarda (ASIC), gerekli silikon tipinin (GaAs...vb de kullanılabilir) seçimiyle başlayan bu süreç, FPGA tasarımlarında FPGA seçimiyle başlar. Akabinde tasarımın işlevsel testleri yapılır ve tasarım istenilen tümdevre tipine göre silikon üzerine yerleştirilerek, metal hatlar çekilir. FPGA tasarımında üretilen karta yüklenmesiyle (download) işlem biterken, ASIC tasarımlarda bu süreç tasarımın özel olarak ABD, Avrupa ya da Güneydoğu Asya'daki fabrikalara ürettirilerek, uygun şekilde paketlenmesiyle son bulur.

Tümdevre tasarımında genellikle HDL dillerinden uygun olanı kullanılır. (Hardware Description Language – Donanım Tanımlama Dili) Çeşitli şirketlerde/kurumlarda VHDL,

Verilog, iHDL gibi farklı fakat hepsi birbirine çok yakın programlama dilleri yoğun olarak kullanılmakta iken, C++ ile de bu tasarımlar artık yapılabilmektedir. Elbette C++'ın yapısının donanım tasarlamak için çok uygun olmaması nedeniyle, en yoğun olarak dünyada (ve silikon vadisinde) Verilog kullanılmaktadır. Ülkemizde daha yoğun olarak VHDL kullanılmaktadır, bu tercihin sebebi ise VHDL tasarım paketinin maliyetinin çok daha düşük olmasıdır. iHDL, Intel tarafından Pentium 4'lerin geliştirilmesi sırasında 90'lı yılların sonunda tasarlanan ve kısa bir süre kullanılan bir tasarım dilidir; fakat Intel bile artık kendi geliştirdiği iHDL'i bırakmış, endüstri standartlarıyla tasarım yapmaktadır. Cadence, Synopsys, Celoxica gibi büyük şirketler, SystemC adı verilen C/C++ ile donanım tasarımını ön plana çıkartmakta ve paralel programlama imkanı veren C/C++ kütüphaneleriyle tasarım sürecini hızlandırmaya çalışmaktadırlar. Ayrıca VEE/LABVIEW gibi programların geçtiğimiz yıllarda FPGA desteklerini artırmaları sayesinde, grafiksel veri akış çizelgeleriyle tasarım yapma imkanını, yazılım mühendislerine sağlamaları da sektör için büyük bir gelişmedir.

Türkiye'de ASIC tasarım yapan firma/kurum sayısının oldukça az olması sebebiyle; çoğu büyük şirket ve KOBİ, FPGA üzerinden VHDL ile tasarıma yönelmiş durumdadır. Özellikle tasarım sürecinin hızlanması ve yeniden programlanabilme imkanı nedeniyle FPGA tasarımları pratiklik ve işlevsel güncelleme imkanı sağlamaktadır. Gerek savunma sanayinde, gerekse telekomünikasyon sektöründe her ölçekten çok sayıda yerli firma FPGA kullanarak üretim yapmaktadır. Ankara'da ODTÜ Teknokent'te ve Bilkent Cyberpark'ta kurulu firmaların yanı sıra İstanbul'da ve İzmir yakınlarında da bu tür tasarımlar yapan çok sayıda KOBİ mevcuttur.

Son yıllarda sayısal tasarım teknolojilerinin gelişmesiyle, tasarımların içerisine yerleştirilen ve "çekirdek" (core) adı verilen yapıların alım-satımı da hızlanmıştır. Örneğin bir sinyal işleme kutusu üretilirken, tasarıma eklenecek FFT (Hızlı Fourier Dönüştürücüsü) çekirdeği çok çeşitli firmalardan satın alınıp, kara kutu olarak kodun içerisine yerleştirilebilmektedir. Entegre içerisinde orijinal tasarım şekli bozulmadan yerleştirilmeleri durumunda garanti edilen saat frekansında çalışabilen bu kara kutular, yeterli boş yer olmadığı durumlarda tüm entegre çapında dağıtılabilmekte, fakat azami saat frekansları düşmektedir.

Yazılan tümdevre tasarım kodları (Verilog/VHDL) öncelikle "sentezleme" adı verilen bir işlemden geçirilmekte ve "sayısal mantık devresi" haline getirilmektedir. Bildiğimiz anlamda "ve", "veya", "ve değil"...vb sayısal kapılardan oluşan bu sayısal

mantık devresinin, kullanılması istenilen entegre türüne göre (özelleşmiş ya da programlanabilir) önce sentezlenmesi (synthesis), daha sonra ise tümdevre içerisindeki "yerleşimi" yapılmakta (floorplanning) ve "hatları çekilmekte"dir. (place&route) Böylece fonksiyonel işlevselliği doğrulanan tümdevre tasarımı, FPGA üzerine yüklenerek gerçek zamanlı testlere başlanabilmektedir.

Yüksek hızlı karmaşık sinyalleri işlemesi gereken ürünlerde, tasarımcının MATLAB ortamında Xilinx (en büyük FPGA üreticilerinden birisi, www.xilinx-.com) firmasının "System Generator" arayüzü ile tasarlayıp MATLAB'da simülasyonunu gerçekleştirdiği sistemlerin, doğrudan FPGA üzerine yüklenebilmeleri ya da yukarıda bahsedildiği gibi "kara kutu" haline getirilip koda entegre edilebilmeleri de olasıdır. Benzer ürünler diğer büyük üretici olan Altera (www.altera.com) tarafından da kullanıma sunulmuştur (DSP Builder, SOPC Builder).

Elektronik tümdevre tasarım otomasyonu şirketleri içerisinde en yoğun olarak kullanılan ürünler Cadence, Synopsys, Mentor Graphics ve Synplicity şirketlerinin ürünleridir. Baskı devre kartı tasarım yazılımı üzerine çok çeşitli firmalar mevcuttur, fakat yazılan Verilog/VHDL kodunun sentezlenmesi her iki tümdevre tipi seçiminde de ortak olduğu için sentezleyici yüksek önem taşımaktadır. Xilinx firmasının çok uygun maliyetle kullanıcılarına sunduğu XST de (Xilinx Synthesis Tool), yüksek performansla çalışmakta ve Xilinx marka FPGA'ler için pratik bir çözüm olarak karşımıza çıkmaktadır.

Tasarım aşamasında, kodu yazmaya başladığımız andan itibaren Mentor Graphics firmasının geliştirdiği ve endüstriyel standart olan Modelsim Verilog/VHDL simülasyon ortamı da tasarımcının ilk ihtiyaçları arasındadır. Modelsim, kodun yazıldığı şekliyle teorik simülasyonunu yapmakla beraber, FPGA/ASIC üzerine yerleştirildikten sonra, hatları çeken programın çıktı olarak sağladığı zamanlama bilgilerini de girdi olarak kullanabilmekte ve bu sayede tasarımın FPGA/ASIC üzerinde gerçek zamanlı (1ns çözünürlükle) simülasyonunun yapılabilmesini de tüm gerekleriyle birlikte sağlamaktadır. Benzer simülasyon ortamları Xilinx, Altera, Actel, Aldec, Lattice ve Blue Pacific şirketlerinin ürünleriyle de sağlanmaktadır; fakat Mentor Graphics şirketi, Modelsim isimli ürünüyle tüm dünyada bu alandaki en büyük isim olmayı başarmıştır.

Verilog/VHDL dillerinin bir diğer büyük üstünlüğü test arayüzü sağlamalarıdır. Tasarım kodu yazılırken, ayrı bir "entity" (varlık-kod grubu) olarak da "testbench" adı verilen test arabirimleri yazılabilmekte ve simülasyon sırasında tasarıma istenilen her türlü girdilerin (sinyal ya da vektör, analog ya da sayısal) bu testbench'ler yoluyla girilmesi ve

çıkışların analizi sağlanmaktadır. Böylece yapılan tasarım tek bir tuşla tüm testlerden geçirilip sonuç alınabilmekte ve test bilgileri testbench arayüzüyle her türlü yazılıma da aktarılabilmektedir.

Programlanabilir tümdevreler (FPGA) elbette genel kullanım için üretilmeleri nedeniyle, uygulamaya özel üretilen tümdevrelere (ASIC) göre daha yavaş kalmakla beraber, piyasadaki yeni FPGA'ler ortalama 500 megahertz saat frekansı ile çalışabilmeleri ile yüksek hız gereksinimi olan telekomünikasyon ve radar cihazları dahil her türlü cihazın tasarımında rahatlıkla kullanılmaktadırlar. FPGA'lere çalışmaları için gerekli voltaj ilk verildiği anda, belirli bir arayüz vasıtasıyla kart üzerindeki flash bellekten yüklenerek programlanmaktadırlar. Ayrıca CPLD (karmaşık programlanabilen mantık devresi) adı verilen, daha basit ve flash bellek kullanımıyla hafızası istenmedikçe silinmeyen programlanabilir entegreler de kullanılmaktadır. CPLD'ler çok daha düşük frekanslarda çalışmakta ve basit kontrol devrelerinin tasarımında kullanılmaktadırlar. Batarya ile çok uzun süre çalışabilen CPLD çeşitleri de mevcuttur.

Son birkaç yıl içinde, FPGA üreticilerinin, programlanabilir entegre içerisine mikroişlemci/powerpc işlemcisi (hatta çok sayıda işlemci) yerleştirerek ürün çeşitliliğine gittikleri de görülmektedir. Bu işlemciler bazı firmalarda doğrudan donanımın içerisine işlemciyi (işlemcileri) gömerek üretmek şeklinde olurken, bazı firmalarda/ürünlerde ise bu işlemcilerin yazılım olarak "kara kutu" şeklinde satıldığı gözlenmektedir. Xilinx, Altera, Altium, Lattice, Virginia Tech ve Pablo Bleyer şirketleri kendi geliştirdikleri "kara kutu" işlemcileri satışa sunmuş başlıca şirketlerdir.

Yüksek sıcaklık, titreşim, radyasyon gibi zorlu koşullara özel üretilen (elbette daha yüksek maliyetli) FPGA tipleri de mevcuttur. Bir ASIC tümdevreyi üretirken çalışacağı koşulların önceden belirlenmesi önem arz ederken, proje gereksinimlerine göre FPGA ve diğer devre elemanlarının seçimi de özenle yapılmalı, yüksek sıcaklık ve radyasyon gibi unsurlar tasarımın her aşamasında dikkate alınmalıdır. Örneğin radyasyona maruz kalabilecek tasarımlarda (uydu...vb cihazların elektronik kartları), doğru malzeme seçilmemesi telafi edilemez sonuçlar doğurabilmektedir.

Gelişen teknolojinin üretimde sağladığı yüksek olanakları kullanmamız, özellikle kontrol ve sinyal işleme teknolojilerinde KOBİ'lerin dünya liderleriyle yarışabilmelerine olanak sağlamaktadır. Düşük maliyetleri, yüksek hızları ve kısa tasarım süreçleriyle FPGA'ler, tüm tasarımlarımızda çok büyük başarılara ve esnek tasarımlara olanak sağlamıştır.

1.14. SRAM'in İç Yapısı

Durağan Rastgele Erişimli Bellek (SRAM - Static Random Access Memory) yarı-iletken bir bellek türüdür.

Durağan (“static”) kelimesi, sürekli tazelenmesi gereken devingen RAM’in (DRAM) aksine, belleğe güç verildiği sürece belleğin içeriğini koruduğunu belirtir. (Bununla beraber, SRAM, salt okunur bellek ROM ve flaş bellek ile karıştırılmamalıdır.)

Rastgele Erişim (“Random access”) hafızanın içerdiği konumlara, daha önce erişilmiş olan konumlara bakılmaksızın erişilebileceğini yani yazılıp okunabileceğini belirtir.

SRAM içindeki her bit; her biri, iki adet çapraz eşlenmiş tersleyici(inverter) oluşturan transistörlerden dört tanesi üzerine kurulmuştur. Bu hafıza hücresi(bit), genelde “1” ve “0” ifade etmek için kullanılan iki durağan duruma sahiptir. İki adet fazladan erişim (access) transistörü, okuma ve yazma işlemleri sırasında hafıza hücresine erişimi denetlemek üzere hizmet verirler. Bir hafıza hücresini(bit) saklamak için özellikle altı adet MOSFET (Metal-Oxide-Semiconductor Field-Effect Transistor) gerekmektedir.(4:okuma-yazma 2:erişim)

Bakışımlı (simetrik) devre yapısı bir hafıza konumdaki değerin DRAM’e göre çok daha hızlı okunmasına olanak tanır. SRAM’in daha hızlı olmasını sağlayan, DRAM’le arasındaki bir başka fark ise tüm adres bitlerini bir kerede alan özel çiplerdir. Buna karşılık DRAM’lerin sahip olduğu yarar iki yarım parça halinde çoklanmış adresler kullanmasıdır. İki parça halinde çoklanması demek aynı paket içerisindeki pinler üzerinde, boyutları ve maliyeti düşürmek üzere küçük değerli bitlerin yüksek değerli bitleri izlemesi demektir.

SRAM, synchronous (zamanuyumlu) DRAM anlamında olan SDRAM ile karıştırılmamalıdır. SDRAM tamamen SRAM’den farklıdır. Ayrıca pseudostatic (pseudo: yalancı static:durağan) RAM (PSRAM) denen, kendini SRAM’miş gibi maskeleyen DRAM’le karıştırılmamalıdır.

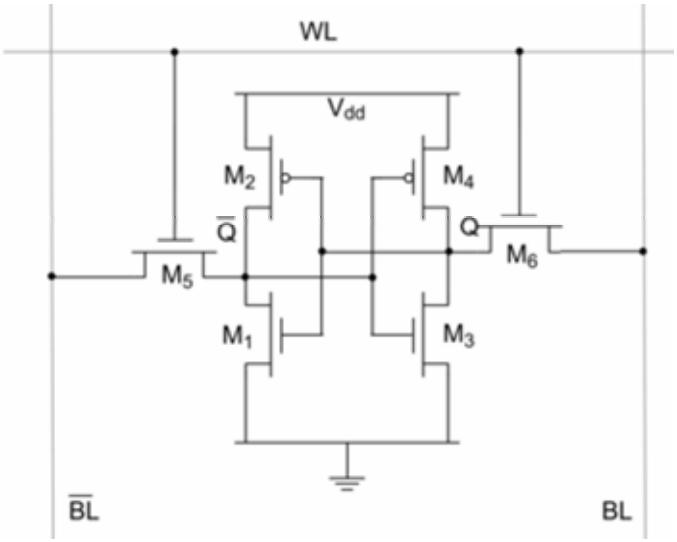
Random Access; son erişilen bellek yeri önemsenmeksizin, bellek içindeki yerlerin herhangi bir sırada yazılabilmesi veya okunabilmesi demektir. SRAM içindeki her parça, 2 cross-couplet tersleyici yapıda olan 4 transistörde toplanır. Bu depo hücresi, 0 ve 1'i göstermek için kullanılan iki kararlı duruma sahiptir. İki ek erişimsel transistör, okuma ve yazma işlemleri boyunca depo hücresinde erişimi kontrol etmeye yardımcı olur. Bu yüzden tek bir parça bellek depolamak için tipik olarak 6 tane MOSFET alır. Şekil 1.'de görüldüğü

gibi, hücreye erişim, [BL] ve BL, iki line-bit‘e bağlanıp bağlanmaması gerekmediğini içe doğru kontrol eden M5 ve M6, iki erişim transistorünü kontrol eden (örnek WL) word-line tarafından sağlanır. Bunlar hem okuma hem de yazma işlemleri için bilgi transferinde kullanılırlar. İki line-bit’e katı bir biçimde sahip olması gerekli değilken hem işareti hem de ters sonucu, noise margins’i (gürültü tolerans payı) geliştirdiğinden, tipik olarak sağlanır. Okuma erişimi boyunca, line-bit’ler RAM hücresi içinde tersleyiciler tarafından aktif olarak yüksek ve alçak olarak sürdürülür. Bu işlem, DRAM’lere nazaran SRAM hızını arttırır. Line-bit’ler depo kapasitecileriyle bağlanır ve şarj paylaşımı, line-bit’lerinin aşağı yukarı sallanmasına neden olur. SRAM’lerin simetrik yapısı, ayrıca daha kolay incelenebilen küçük voltaj oluşturan, farklı işaretlemelere izin verir. m yolu ve n data-line ile bir SRAM’ın boyutu, 2m words ya da 2m ×n bit’dir.

Bir SRAM, üç ayrı durumda incelenir: yedek(devre işlemiyorsa), okuma (bilgilerin istendiği), yazma(içeriği güncelliyorken). Bu 3 durumu şu şekilde gerçekleştirir:

a) Yedek: Eğer word-line öne sürülmüyorsa, erişim transistorleri M5 ve M6 bit-line’lardan hücreye bağlanmaz. M1-M4 tarafından şekillenen 2 cross-couplet tersleyicilerin dış dünyayla bağlantısı kesildiğinde de, birbirlerini desteklemeye devam edeceklerdir.

b) Okuma: Sanılır ki; bellek içeriği Q’da depolanan 1’dir. Okunan devre şarj etme öncesi her iki bit-line tarafından başlatılır. Değerler Q’da depolandığında, 2.adım gerçekleşir. [Q],



Şekil 1. SRAM hücre yapısının basit gösterimi

BL ayrılarak bit-line'a transfer edilir. BL tarafında, M4 ve M6 transistörleri, bit-line'ı, VDD'ye çeker. Eğer bellek içeriği sıfır olursa, tam tersi yaşanır ve [BL], 1'e doğru çekilir.

c) Yazma: Bir yazma devresi, bit-line'a yazılan değere göre başlar. Eğer 0 yazmak istiyorsak, bit line'a 0 uygularız. 1, bit-line'nın değerlerini terse çevirerek yazılır. Sonra WL ön plana geçer ve depolananın değerine bağlanır. Input sürücüleri kullanım süresi, dayanıklılığından dolayı daha uzundur.

Uygulanışları ve kullanımı bakımından SRAM'leri incelediğimizde şu başlıklar altında toplayabiliriz.

a) Özellikleri:

SRAM, DRAM'den biraz daha pahalıdır; fakat daha hızlı ve oldukça az güce ihtiyaç duyar. Bu yüzden, hız, güç ve her ikisi açısından tercih edilir. Ayrıca SRAM'i kontrol etmek daha kolaydır ve genellikle diğer modern DRAM türlerinden, daha doğru bir random access'e ulaştırır. Daha karmaşık bir iç yapıya neden olduğundan SRAM, DRAM'den daha az yoğundur ve bunun için kişisel bilgisayarların ana belleğindeki gbi düşük maliyetli uygulamalar, yüksek kapasite için kullanılmaz.

b) Saat Hızı ve Gücü:

SRAM'ın güç tüketimine sıklıkta erişildiğine bağlı olarak bir çeşitlilik gösterir; sıkça kullanıldığında ve bazı IC'ler full hızda birçok watt harcadığında, dinamik RAM kadar güce ihtiyacı olabilir. Diğer bir yandan RAM daha yavaş bir tempoda kullanılarak enerji tasarrufu sağlanabilir (tıpkı mikro işlemcilerde yapılan uygulamalardaki gibi).

Statik RAM öncelikle;

- Genel amaç ürünüdür.
- Asynchronous olanlar (28 pin 32k×chips ve 16m bitlik benzer ürünlerdir.)
- Synchronous olanlar (genellikle caches ve burst transferi gerektiren diğer uygulamalar için kullanılır.) (18m bit[256k×72])
- Chip'e entegre edilenler.
- Mikrokontrolör'deki cache veya RAM hafızası gibi (genellikle yaklaşık 32 bytes'tan 128 kilobytes'a kadar olanlar)
- Mikro işlemcilerin içindeki ilk cacheler gibi (×86 grubu ve diğerleri)(8k2dan birkaç megabyte 'a kadar)
- Belirli bir IC ve ASIC uygulamalarında (genellikle kilobyte sırasıyla)
- FPGA ve CPLD'de (genellikle birkaç veya daha az kilobyte sırasıyla)

c) Yerleştirilmiş Kullanımı:

Endüstriyel ve bilimin alt sistemlerinin bazı kategorileri, otomative elektronik ve benzer sistemler static RAM içerir. Bazı miktarlar (kilobyte ve daha az) oyuncaklarda da pratik olarak kullanılır. Birkaç megabyte, cep telefonları, dijital kameralar…vb karmaşık yapıdaki ürünlerde de kullanılabilir.

d) Bilgisayarlarda:

SRAM ayrıca kişisel bilgisyarlar, workstationlar, routerlar ve çevresel ekipmanlarda (iç CPU cache ve dış burst mode SRAM caches, hard disk tamponlar, router tamponlar..vb) Ayrıca LCD ekranlar ve yazıcılarda da gösterilen imgeyi tutan static RAM'ler kullanılır. Küçük SRAM tamponları CDROM'larda ve CDRW sürücülerinde bulunur. (genellikle 256k bytes veya daha fazlası, tek bir değer yerine blokları transfer eden track data kullanılır. Aynısını modem kablolarına ve bilgisayara bağlı benzer ekipmanlara uygular. CMOS-RAM olarakta adlandırılır. Fakat günümüzde daha sık EEPROM veya flaş bellek kullanımlarına uygulanır.)

e) Hobi olarak ilgilenenler:

Hobi olarak ilgilenenler sıklıkla SRAM'i tercih eder. Güncellemeye gerek olmadığından, kullanımı DRAM'lerden çok daha basittir. Ayrıca SRAM genellikle 3 kontrole gerek duyar: Chip Enable(Ce), Write Enable(WE) and Output Enable(OE).

SRAM türleri bakımından üçe ayrılır.

a) Transistör olarak:

- Bipolar Junction Transistör (TTL ve ECL 'de kullanılır.), oldukça hızlıdır fakat çok güç harcar.
- MOSFET (CMOS'da kullanılır.), düşük enerjili ve günümüzde yaygın olan bir türdür.

b) Fonksiyon olarak:

- Asychronous, zamandan bağımsızdır; bilgi içi ve dışı transition tarafından kontrol edilir.
- Synchronous, her an zamana göre çalışır. Bilgi ve diğer kontrol sinyalleri zaman sinyalleri ile beraber çalışır.

c) Özellik olarak:

- ZBT, zaman miktarı zaman devre sayısı kadardır. Yazma-okuma ve okuma-yazma işlemlerinden SRAM'e ulaşımının değişmesi kadar bir zaman alır.
- SyncBurst (syncBurst sram ya da synchoronous –burst SRAM)

1.15. Rastlantısal Sayı Üretimi

Rasgele sayılar bir anlamda gelişigüzel, bilinemeyen, tahmin edilemeyen sayılar olarak düşünülebilir. Kuralsal matematik tanımına göre eğer bir katarı ifade etmek için katarı kendisi ile ifade etmekten başka daha kısa bir yol bulunamıyorsa o katar rasgeledir denir. Başka bir deyişle, katar eğer sıkıştırılamıyorsa rasgeledir. Buradan sıkıştırma işleminin bir rasgeleleştirme fonksiyonu olduğuna dikkat edin. Bilgisayarlarla çalıştığımız için rasgele sayıları rasgele bitler ya da rasgele bitlerin bir katarı olarak düşünebiliriz. Bu bitleri daha sonra birlikte gruplar ve üzerinde modülolar, çeşitli aritmetik ve lojik işlemler gerçekleştiririz ve değişik formlarda kullanırız. İstatistik bize rasgele bitler hakkında birkaç şey şöylemektedir: "Bir rasgele bit katarında sıfırlar birler kadar sık olmalıdır. Sıfır çiftleri tek bir sıfırın yarısı kadar sıklıkta olmalıdır ve bir çiftlerinin de sıklığında olmalıdır. Bir üçlü ise bir ikilinin yarı sıklığında ve tek bir bitin çeyrek sıklığında oluşmalıdır. Benzer şekilde bir rasgele katardan çiftler halinde (x ve y diye) örnekler alınırsa ve bu çiftlerden bir grafik oluşturulursa bu grafikte kümelenmeler olmamalıdır". Bir sayı katarı üzerinde ne kadar rasgele olduklarını ya da olmadıklarını göstermek üzere gerçekleştirilebilecek ki-kare (chi-squared) testi gibi başka istatistiksel testler de mevcuttur. Bir bit katarının bu istatistiksel biçimi izleme derecesi onun entropikliğinin de derecesidir. Bu entropikliğin katı matematiksel tanımıdır. Entropik ve bilinemeyen birşey için iyi tanımlanmış bir terim olmadığına dikkat edin. Birçok insan gayri resmi olarak "entropik" terimini istatistiksel olarak rasgele ve bilinemeyen anlamında kullanmaktadır [9]. Shannon'a göre, herhangi bir mesaj ya da durumun H entropisi:

$$H = -K\sum_{i=1}^{n} p_i \log(p_i) \tag{2}$$

ile verilmektedir. Burada K, birimsel dönüşümü sağlamak amacıyla konulmuş seçime bağlı bir sabittir, 1/log(2) bit gibi. p_i ise olası n durum içinden olası i durumunun oluşması olasılığıdır. k bitlik bir ikili sonuç üreten bir rasgele sayı üreteci olması durumunda, $0 \le i < 2^k$ olmak üzere, p_i bir çıkışın i'ye eşit olmasının olasılığıdır. Mükemmel bir rasgele sayı üreteci için, $p_i = 2^{-k}$ ve çıkışın entropisi k bite eşittir. Bu tüm olası çıkışların eşit olasılıklı olması ve ortalamada çıkışta bulunan bilginin de k bitten daha kısa bir dizi ile temsil edilememesi anlamına gelmektedir [10]. Güçlü şifreler de aynı zamanda birer rasgeleleştirme fonksiyonudur. Bu fonksiyonların şifremetin çıkışları

rasgeledir, ideal durumda mükemmel derecede rasgeledir. Bütün istatistiksel testlere uyar ve etki olarak gürültü gibi görünür. Rasgele sayılar güçlü (mükemmel rasgele sayılar en güçlüleridir) ya da zayıf ve bilinebilir ya da bilinemez olabilir. Bu konuda daha ayrıntılı bilgi için [11]'e başvurulabilir.

1.15.1. Sözde Rasgele Sayı Üreteçleri

Bir sözde rasgele sayı üreteci (SRSÜ) davranışları gerçek rasgele sayılara çok fazla benzeyen sayıları üretmek için kullanılan bir formüldür. Tohum denen bir başlangıç durumundan bir dizi çıkış üretmek için deterministik prosesleri kullanır. Çıkışın tamamen tohum datanın bir fonksiyonu olmasından dolayı, çıkışın gerçek entropisi tohumun entropisini asla aşamaz. Üretilen sözde rasgele dizi rasgele gibi görünür ve gerçek rasgele dizilerden mümkün olduğu kadar ayırt edilemez olmalıdır. Örneğin, sıkıştırılamaz olmalıdır, sıfırlar birler kadar sık olmalıdır, vb. Bu özellikler deneysel olarak ölçülebilir ve daha sonra bir ki-kare testi kullanılarak istatistiksel beklentilerle de karşılaştırılabilir. Bir sözde rasgele sayı üreteci sadece aşağıdaki özelliği mutlaka sağlar [12]:

Rasgele gibi görünür. Yani rasgeleliğin bilinen bütün istatistiksel testlerini geçer. Pek çok uygulama için sözde rasgele sayılar oldukça tatmin edicidir. Bununla birlikte kriptografik uygulamalar için en güçlü hasımlar tarafından bile tahmin edilemeyecek sözde rasgele bitlerin kullanılması çok önemlidir. Kriptografik uygulamalar rasgele sayı üreteçlerinin özelliklerine aşırı derecede duyarlıdır. Bir rasgele sayının bilinememesi kavramı kriptografik çalışmalarda temeldir. Kriptografide kullanılacak bir sözde rasgele sayı üretecinin ilave olarak aşağıdaki özelliği de sağlaması gerekir:

Tahmin edilemezdir. Yani, diziyi oluşturan algoritma ya da donanıma ilişkin tüm bilgi ve akıştaki tüm önceki bitler verilse dahi bir sonraki rasgele bitin ne olduğunu tahmin etmek hesapsal açıdan olanaksızdır.

1.15.2. Gerçek Rasgele Sayı Üreteçleri

Bir gerçek rasgele sayı üreteci (GRSÜ) tamamen rasgele sayılar üreten bir donanımdır. Alışılmış yöntem bir direnç ya da yarı-iletken diyod tarafından üretilen gürültüyü (Johnson gürültüsü) güçlendirmektir ve bunu bir karşılaştırıcıya ya da Schmitt

tetikleyiciye vermektir. Eğer çıkış örneklenirse (çok hızlıca değil) istatistiksel olarak bağımsız bir dizi bit alınır ya da almak ümit edilir. Bunlardan daha sonra sekizliler, tamsayılar ya da kayan noktalı sayılar ve eğer gerekliyse diğer dağılımlardan rasgele sayılar elde edilebilir.

Bir gerçek rasgele sayı üreteci yukarıdakilere ilave olarak aşağıdaki özelliği de mutlaka sağlar[12].

Güvenilir bir şekilde tekrar üretilemez. Yani dizi üretici tam olarak aynı (en azından elden geldiği kadar aynı) girişle iki kere çalıştırılırsa, sonuçta iki ilişkisiz rasgele dizi elde edilir.

Burada şunu da belirtmek gerekir ki, çıkışları gerçek bir rasgele sayı üretecinden hesapsal olarak ayırt edilemeyecek kadar yüksek kalitede SRSÜ'ler olması durumunda bile, belki inşa edilebilirler, bu SRSÜ'lerin yine de GRSÜ'ler kullanılarak tohumlanması gerekecektir. Genellikle, rasgele sayı üretiminde ana amaç bazı entropik sayılar elde etmek ve daha sonra bunları bir sözde rasgele sayı üretecini başlatmakta (tohumlamakta) kullanmaktır. Bununla birlikte, sürekli olarak entropik sayılar örnekleyen bir süreç hazırlamak ve sürekli ve toplamsal olarak bir sözde rasgele sayı üretecini beslemek daha da iyi bir çözümdür.

İyi rasgele sayıların üretilmesi zor bir problemdir. Gerçek rasgele sayılar elde etmek için çeşitli yollar vardır. Örnek olarak, gürültü içeren donanım cihazları üretilmesi, kozmik ışın değişiminin gözlemlenmesi ve tuzağa düşürülmüş civa atomlarından olan ışık emisyonlarının gözlenmesi verilebilir. Kuantum mekaniği de rasgeleliğin gerçek dünyada olduğunu söylemektedir.

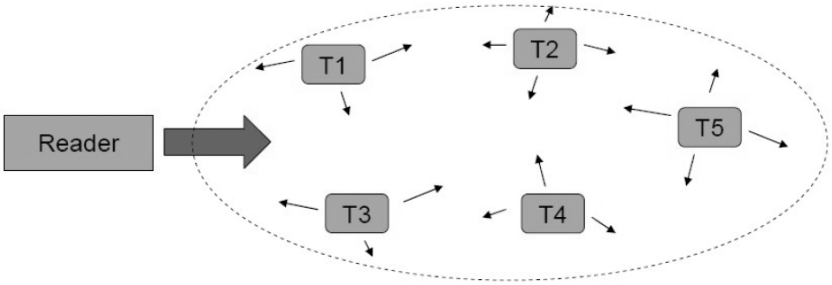
Klasik bilgisayarlarla tamamen rasgele birşeyler üretmek olanaksızdır. Bilgisayarlar deterministik sistemlerdir. Bir girişi ve bir çıkışı vardır ve içeride tamamen tahmin edilebilir işlemler gerçekleşir. Bir bilgisayara aynı giriş iki defa uygulanırsa ikisinde de aynı sonuç alınır. İki özdeş bilgisayara aynı giriş uygulanırsa ikisinden de yine aynı sonuç alınır. Bir bilgisayar yalnızca sonlu sayıda (büyük bir sonlu sayı ama yine de sonlu) bir durumda bulunabilir ve çıkış her zaman giriş ile bilgisayarın o anki durumunun deterministik bir fonksiyonu olacaktır. Bu, bir bilgisayar (en azından bir sonlu durum makinesi) üzerindeki herhangi bir rasgele sayı üretecinin tanım olarak periyodik olması anlamına gelmektedir. Periyodik olan bir şey ise tanım olarak tahmin edilebilirdir. Ve eğer birşey tahmin edilebilirse rasgele değildir. Bir gerçek rasgele sayı üretecinin rasgele bir girişi olmak zorundadır ve bir bilgisayar bu koşulu sağlayamaz.

Bununla birlikte bilgisayar kullanıcıları varolan en entropik şeyler arasındadır. Klasik bilgisayarlarla tamamen rasgele birşeyler üretmek amacıyla kullanıcının klavye kullanımından (tuş basımları arasındaki zamanlamadan) ve fare kullanımından (tuş basımları arasındaki zamanlamadan, farenin konumundan) yararlanılabilir.

Hiç kullanıcınız olmaması durumunda ise bir entropi kaynağı olarak donanım da kullanılabilir. Saatine bakılabilir, diske bakılabilir, bir mikrofondan alınan veriler kullanılabilir, bilgisayarın video belleği okunabilir, ağda gidip gelen verilere bakılabilir, bilgisayarın o anki durumu kullanılabilir, vb. Bu konuda daha fazla bilgi için [11]'e başvurulabilir.

1.16. Çakışma Önleyici Algoritmalar

RFID etiket çakışması, aynı anda birden fazla etiket okuyucuya sinyal gönderdiği zaman meydana gelir. Etiketin okuyucuya tek bir anda cevap vermesi için değişik sistemler geliştirilmiştir[8]. Bu sistemler etiketleri tekilleştiren algoritmaları içerir. Her etiket saniyenin binde birinde okunduğu için, eş zamanlı okunuyorlarmış gibi görünür. Bu durumu Şekil 2.'de daha rahat görebilmekteyiz.

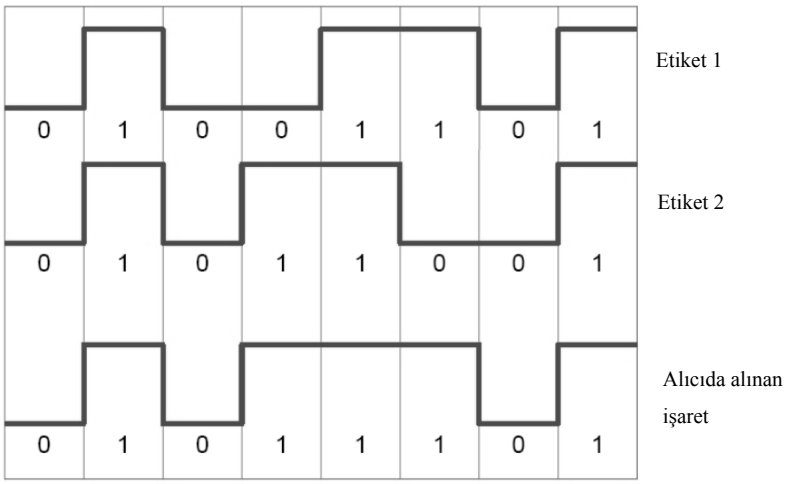


Şekil 2. Çakışma probleminin gösterimi

Bunun yanında bir de okuyucu çakışması vardır. Bu problemi çözmenin bir yolu zamanı birçok geçiş için bölmektir. Bu basit olarak okuyucuların farklı zamanlarda etiket ile iletişim kurmasıdır. Bu birbirleri ile çatışmalarını engeller. Ancak bu aynı zamanda iki okuyucunun çakıştığı bir yerde bir RFID etiketinin iki defa okunması anlamına da gelebilir. Bu yüzden sistem, bir etiket bir okuyucu tarafından okunduğu zaman diğer okuyucunun tekrar okumaması şeklinde kurulmalıdır.

Çakışma probleminde bit bazında neler olduğunu daha iyi anlayabilmek için Şekil

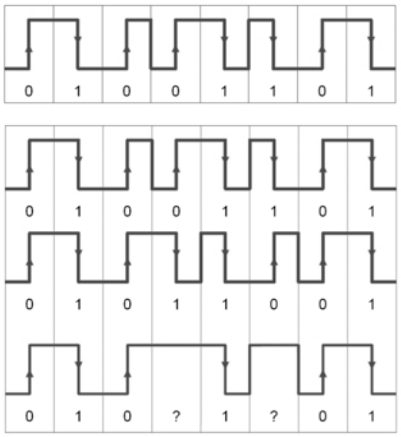
3.’de gösterilen herbir etiketin davranışının nasıl olacağını iyi bir şekilde görmekteyiz.



Şekil 3. Bit bazında çakışma problemi

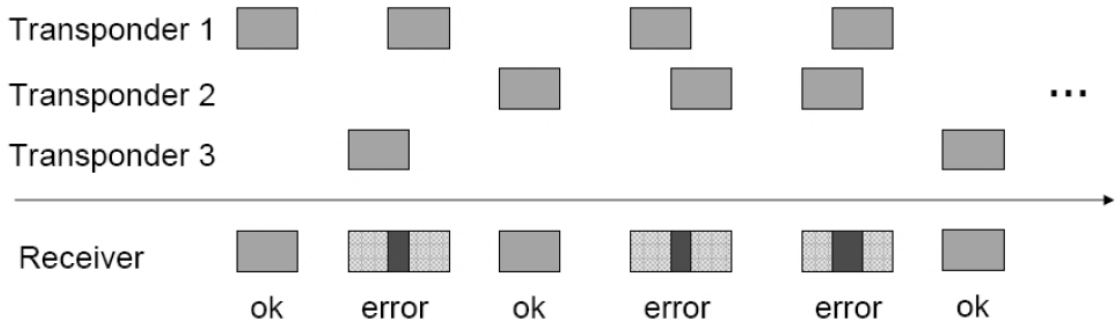
Şekil 3.’de de görüldüğü üzere farklı etiketlerin aynı anda gönderdikleri bitler birbiri ile karışacak ve böylece okuyucunun farklı bitleri almasına sebep olacaktır. Bu durumu engellemek için bir algoritma kurulması gerekir. Çoğu zaman bu algoritmalar etiketlerin farklı zamanlarda cevap vermesi ilkesine dayanan sistemleri kullanırlar.

Şekil 4.’de gösterilen durum herbir etiketin kodlanmış veri kullanarak haberleşmesini ve böylece okuyucunun hangi bitte çakışma olduğunu algılaması ve bu biti düzeltici bazı tedbirler alması ile çakışma probleminden kurtulunabilinir.

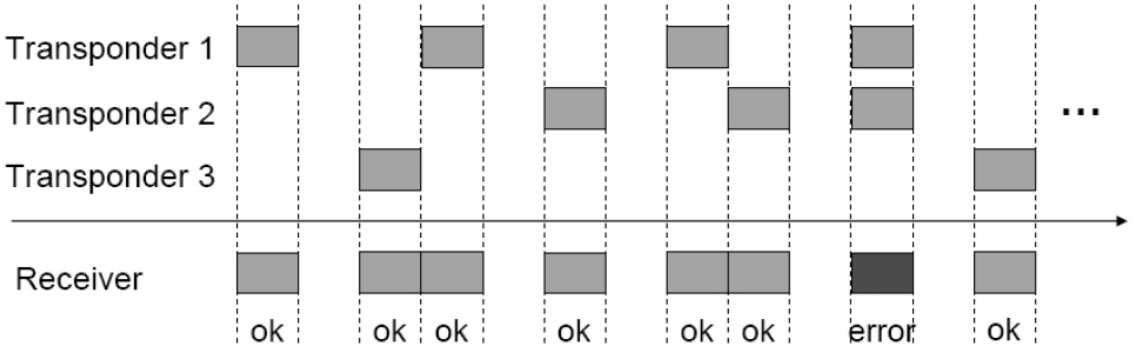


Şekil 4. Manchester kodlama ile çakışan bitin tesbiti

Eğer etiket cevabını rastlantısal bir şekilde yolluyorsa Şekil 5.'deki durum söz konusu olur, Şekil 6.'de ise rastlantısal ancak belirli zaman aralıklarında cevabını yollamasının diğerinden ne kadar iyi olduğunu görebiliyoruz. İşte bu yüzden sistemler "slot counter" adında zaman aralıkları ile çalışan ancak yine de rastlantısal olarak bu aralıkları kullanan algoritmaları kullanırlar.



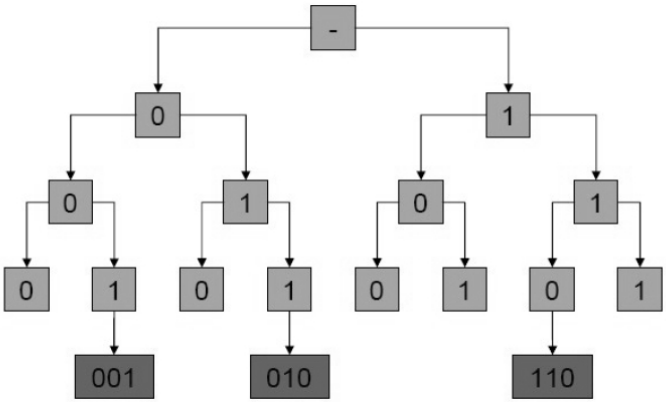
Şekil 5. Etiketler cevablarını rastlantısal olarak yolluyor



Şekil 6. Etiketler cevablarını belli zaman aralıklarında yolluyor

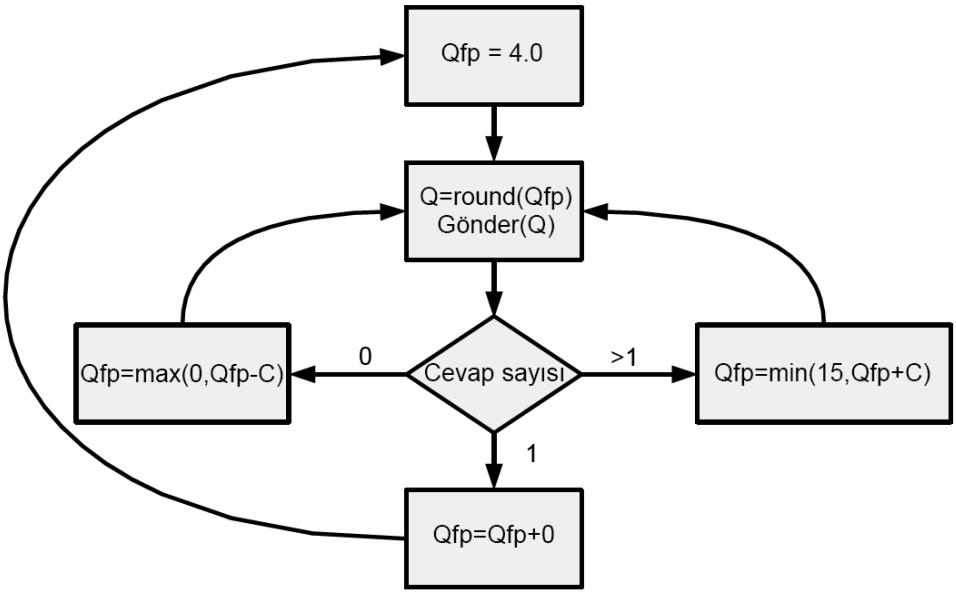
Rastlantısal olarak uygulanan algoritmalardan bazıları deterministik yöntemler kullanır. Bunların en önemlisi "binary search" algoritmasıdır. Bu algoritmada en anlamsız veya en anlamlı bit ile başlanarak bir arama algoritması kurulur. Uygun olan etiketlerin cevap vermesi ile diğer bitlere geçen okuyucu algoritması tüm etiketlerin okunmasına kadar her bir bit için tüm olasılıkları dener. Ancak bu algoritmaların dezavantajı yavaş çalışıyor olmalarıdır. Şekil 7.'de binary search algoritmasına ait bir blok şema verilmiştir. Burada 3 bitlik etiket ID'lerinden oluşan sistem her bir etiketi bulmak için tün olasılıkları

deniyor. Bir olasılıktan diğer olasığa geçmeyi çakışma olduğu zaman gerçekliyor. Çakışmayı ise yine manchester kodlama kullanarak anlıyor.



Şekil 7. Binary Search Algoritması Blok Şeması

Olasılıksal yöntem kullanan algoritmalarda dikkat edilemesi gereken bir hususda ortamda bulunan etiket sayının dikkate alınarak bir uzunluk biriminin hedeflenmesidir. Bu uzunluk birimi Q bit olarak adlandırılmaktadır. Q'nun belirlenmesi ile daha hızlı okuma yapılması hedeflenmektedir. Rastlantısal sayılar bu Q bit ile belirli bir kural çarçevesinde slot belirleyicilere yüklenerek daha kısa süre içerisinde etiketlerin cevap vermesini böylece etiket sayısı ile zaman aralıkları arasında iyi bir ilişki kurulmasını, özellikle sayı bakımından, sağlar. Şekil 8.'de bu yapının akış diyagramı görülmektedir.



Şekil 8. Olasılıksal yöntem ile çakışma önleyici algoritma akış diyagramı

Q'nun büyük değerleri için C'nin küçük değerleri, Q'nun küçük değerleri için C'nin büyük değerleri kullanılır. Tipik C değerleri ise 0.1 ila 0.5 arasındadır.

Bu bölümde çakışma önleyici algoritmaların kullanılmasının nedenlerini görmüş olduk. Özellikle bazı algoritmaların rastlantısal olarak cevap vermesi gerektiğini ve bu yüzden etiketlerin bünyesinde bir rastlantısal sayı üretecinin olması gerektiğini gördük. İşte bu tezin içeriğinde yapılan çalışmalarda böyle bir rastlantısal sayı üretecinin diğer tasarımlardan çok daha basit ve az güç harcayan yapının oluşturulmasını içermektedir. RFID etiketinin çok az güç seviyesinde çalışma zorunluluğu tasarımda kullanılacak olan yapıların çok basit ve az güç harcaması zorunluğu vardır.

1.17. RNG Tasarımı

[13]'de yapılan çalışmada rastlantısal sayı üretiminde SRAM yapısı incelenmiş ve enerji verildiğinde her bir bitin aynı değeri almayıp değişik değerler aldığı gözlemlenmiş ve bunun rastlantısal sayı üretimine ne kadar uygun olduğu araştırılmıştır. Bu noktadan yola çıkılarak bu çalışmada bir SRAM kullanılarak bu değerlerin kriterleri sağlamada bize ne sunduğu araştırılmıştır.

NXP firmasına ait LPC2138 mikro kontrolörü içerisindeki RAM bloğunun yapısı SRAM tipidir. Buradan alınan byte ve word uzunluğundaki blokların incelemesi yapılmıştır.

EPC C1G2 [14] standardında rastlantısal sayıların üretilmesi ve belli kriterlere uygunluğu istenmektedir. Birinci kriter üretilen herbir sayının olasığının $0.8/2^{16}$ ila $1.25/2^{16}$ arasında olmasıdır. İkinci kriter ise 10,000 adet etiket topluluğunda aynı sayının üretilmesi durumu 10 adeti geçmemelidir. Üçüncü kriter ise üretilen rastlantısal sayıların tahmin edilebilmesi ile ilgilidir ve 100,000 adet üretilen sayıların ardı ardına tahmin edilebilmesi 25 adeti geçmemesi gerekir.

SRAM'den alınan değerler 2 adet 16-bitlik LFSR bloklarının birbirine parallel bağlanması ile oluşturulan ve VHDL dili kullanılarak bunun donanıma hazır hale getirilmesi sağlanmıştır. Bu bloğun ürettiği rastlantısal sayılar grafiklerle daha görsel hale getirilmiş ve başka rastlantısal sayı üreteçleri ile karşılaştırılmıştır. Bu karşılaştırma sonucunda üretilen rastgele sayıların durumu incelenmiş ve tasarımın ne kadar RFID mikro yongasına uygun olduğu konusu incelenmiştir. Kullanılan kaynak miktarından, tüketilen enerji miktarı ve kapladığı yere kadar her türlü detay incelenmiş ve RFID'de olmazsa

olmaz enerji kriteri sağlanıp sağlanmadına bakılmıştır. Ne kadar performans getirdiği, işlem kapasitesi bakımından diğer tasarımlardan ne ölçüde farklı olduğu noktaları incelenmiş ve önemli sonuçlara varılmıştır.

RNG, etiketin içerisinde bulunduğu elektromanyetik alan şiddetinden bağımsız olmalıdır. Aynı zamanda okuyucu etiket arasındaki haberleşme altyapısından da bağımsız olmalıdır. Bunlara ek olarak etiket içerisindeki bilgiye ve bilgi yoğunluğundan ve benzeri durumlardan bağımsız olmalıdır [14]. Bu bağlamda bu çalışmada ortaya konulan tasarım tüm bu kriteleri sağlamış ve herhangi bir özelliğe bağlı kalmadığını kanıtlamıştır.

RNG bloğu aynı zamanda üretiği 16-bitlik rastlantısal sayılardan Q-bit boyutunda yeni sayılar üretebilme kapasitesine sahiptir. Bu Q-bit sayılar etiketin değişik zaman aralıklarında cevap vermesini sağlaması açısından sayıcıya yüklenecek olan sayılardır. Etiket aynı zaman da enerji geldiğinde iki adet rastlantısal sayıyı depolayıp daha sonra kullanmak üzere hafızasında tutma özelliğine sahiptir. Tüm bunlar EPC C1G2 standardında istenen RNG bloğuna ait özellikler olduğu için bu çalışmaya dahil edilmiş ve uygulamada çıkan problemler giderilerek tasarım sonlandırılmıştır.

2. YAPILAN ÇALIŞMALAR, BULGULAR VE TARTIŞMA

2.1. Giriş

RFID sistemlerde birden çok etiket okuma alanı içerisine girdiğinde aynı anda cevap verdiklerinden bunların ayrıştırılıp okunabilmesi için çakışma önleyici algoritmaların kullanılması gerekir. Bunun için bir çok algoritma geliştirilmiştir [8]. Bu çalışmada EPC C1 G2 RFID standardında belirtilen çakışma önleyici algoritma için kullanılması gereken bir rastlantısal sayı üreteci tasarlanmıştır. Bu tasarımın standardın getirdiği kriterlere uygun olup olmadığı araştırılmıştır.

Her bir etikette bulunacak olan bu rastlantısal sayı üreteci diğer etiketlerden bağımsız olarak değişik sayılar üretecek ve bir sayıcı tarafından kullanılacak bu sayılar, etiketin diğer etiketlerden değişik zaman aralıklarında cevap vermesini sağlayacaktır.

Bu bölümde literatürde yer alan RFID etiket için tasarlanmış rastlantısal sayı üreteçlerinin nasıl çalıştığını ve ardından bizim kullanacağımız SRAM tabanlı rastlantısal sayı üreteci ile ilgili testlere yer vereceğiz. Bu testlerin içeriğini rastlantısallık özelliğini kullanacağımız SRAM yapısı ile ilgili ve SRAM'den aldığımız verileri çakışma önleyici algoritma süresince tekrar rastlantısal sayı üretmek için kullanacağımız LFSR yapısının incelenmesi ve test edilmesi oluşturmaktadır. Birinci bölümde RNG tasarımı başlığı altında RNG'nin hangi kriterlere uygun olması gerektiği verilmiştir. İlerleyen bölümlerde bu kriterleri sağlamada yapılan testler ve sonuçları irdelenmiştir.

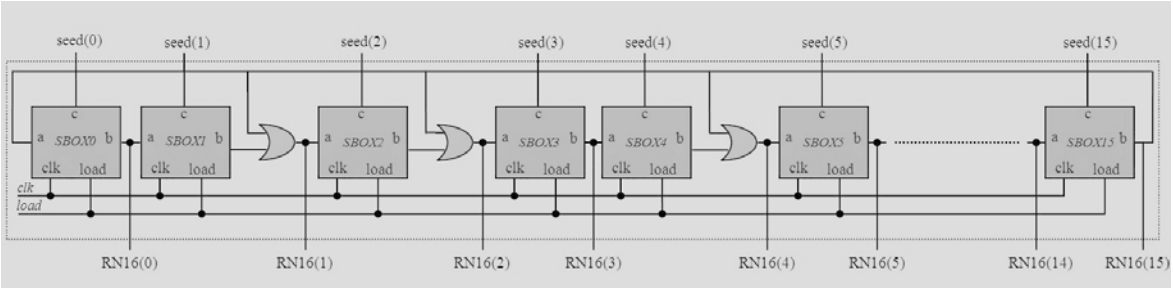
SRAM'den alınan değerler 16-bit uzunluğundaki LFSR yapısına çekirdek değer olarak giriş yapılır. Böylece ilk durumda üretilecek olan rastlantısal sayı daha sonraki bölümlerde saat darbesini aldıkça başka rastlantısal sayılar üretmeye başlıyacaktır. Herbir teste yapılan çalışmanın hangi işlemlerden geçerek yapıldığı anlatılmıştır. Testlerin içerisinde sadece testlere yer verilmemiş aynı zaman da yapılan testin tasarıma ne gibi etkisi olduğu anlatılmıştır. Böylece test başlıkları altında bazı tasarım bilgilerine yer verilmiştir.

İkinci ve üçüncü kriter testlerinde kriterlerin bazı metodları çok fazlasıyla sağlandığı görülüyor, ancak bu tasarımda acaba bu kadar iyi sonuçlara ihtiyaç var mı. Tabiki standardın getirdiği kriterler tartışılabilir. Biz tasarımın karmaşık olmasını istemiyoruz. Bu yüzden paralel yapıdan uzak olan tek LFSR'yi uygulamak en iyisidir.

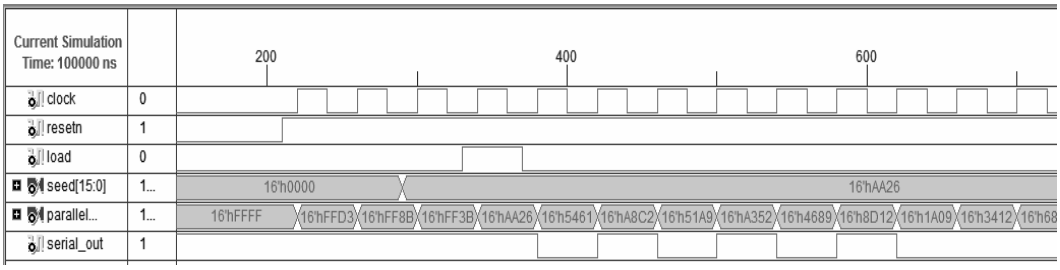
LFSR yapısının en fazla uzunlukta tekrarlaması için 1., 2., 4. ve 15. bitler exorlanarak kaydırma işlemi uygulanmıştır. Başlangıç değerleri ilk önce exorlama işlemi yapılmadan load pini kullanılarak SRAM'den alınan değerler blok içerisine kaydedilir ve daha sonra exor yapıları aktif edilerek girilen bu çekirdek değeri ile LFSR'nin her saat darbesinde paralel çıkış alınır ve elde edilen sayılar tekrarlamalı rastlantısallık özelliği gösterir. SRAM'den alınan değerler bir saat darbesi süresince alınıp tamamlandığından, RNG'nin hızlı çalışma özelliği ön plana çıkmaktadır, diğer tasarımlar çekirdek değerlerini LFSR bloklarına çoğu zaman seri olarak girmekte buda 16 adet saat darbesinden sonra LFSR bloğu hazır hale gelmektedir. Bu bakımdan bu tasarım tek saat darbesi ile çok hızlı bir şekilde sayısını üretmekte ve böylece enerjinin kısa süre içerisinde boşa harcanması engellenmiş olmaktadır. Etiket tasarımında bu ve benzeri noktalar tasarımın olmazsa olmazları arasında yer alır. Tasarımcı bu noktaları çok iyi bir şekilde değerlendirmeli ve uygulamalıdır. Bu çalışmanın ana temelini bu mantık oluşturmaktadır. Bir işi yapan bir devre değil, aynı işi çok daha hızlı ve lojik olarak daha baist bir şekilde yapan devrenin tasarımı söz konusudur. Çünkü imkanlar sınırlıdır ve rahat olma durumu söz konusu değildir.

LFSR yapısı VHDL dili kullanılarak donanımsal olarak tasarlanmadan önce basit bir LFSR bloğu C dili kullanılarak oluşturulmuş ve SRAM'den alınan çekirdek değerleri ile rastlantısal sayılar ürettirilip sonuçlar gözlemlenmek üzere kod içerisinde tekrar kullanılmıştır.

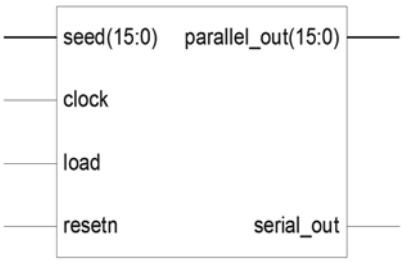
Buradaki SRAM içeriği direkt olarak RNG'nin ürettiği rastlantısal sayılar olmayacaktır. Bu değerler parallel oluşturulmuş LFSR yapısına çekirdek (başlangıç) değeri olarak verilecektir. Şekil 9.'de basit ve tek olan LFSR yapısı görülmektedir. Bu yapının VHDL dili ile donanımsal uygulaması ve yazılan kod bölüm sonunda verilmiştir. Bu haliyle donanım başlangıç değerini SRAM'den değil içerisindeki bir hafıza biriminden almaktadır. İleriki aşamada oluşturulacak olan RAM bloğu, FPGA içerisinde uygulanacağından, ve kullanılacak olan FPGA, SRAM esaslı olacağından bu RAM birimi enerji geldiğinde daha önceki yapılara uygun olarak değişik değerler alacak ve böylece RNG için başlangıç değerini oluşturacaktır.



Şekil 9. RNG bloğunun genel yapısı



Şekil 10. RNG bloğunun simülasyon sonuçları



Şekil 11. RNG bloğunun sembolik gösterimi

Şekil 10.'da LFSR bloğunun simülasyon sonuçlarını vermektedir. Şekil 11. ise LFSR bloğunun sembolik gösterimini içermektedir. Bu gösterimde giriş ve çıkışlar belli olmaktadır. SRAM'den alınan değerler seed pininden girilecektir. Çıkış ise rastlantısal sayıdır ve "paralle_out" olarak adlandırılan pinden alınır.

2.2. Literatür Çalışması

Bu bölümde literatürde yapılan donanımsal rastlantısal sayı üreteçlerine yer verilecektir. Burada amacımız diğer tasarımlar hakkında bilgi sahibi olup, bu tezde yapılan

çalışmanın ne kadar basitlik ve diğer unsurlarda ne kadar gelişmiş olduğunu görmek. Literatür araştırmasında özellikle RFID sistemleri için olan rastlantısal sayı üreteçlerini araştırdık. Çünkü RFID için üretilmesi gereken bu yapı diğer tüm tasarımlardan yapı olarak farklılık göstermektedir. Çok daha basit bit yapıya sahip olmalıdır. Yani lojik olarak daha az eleman kullanmalıdır.

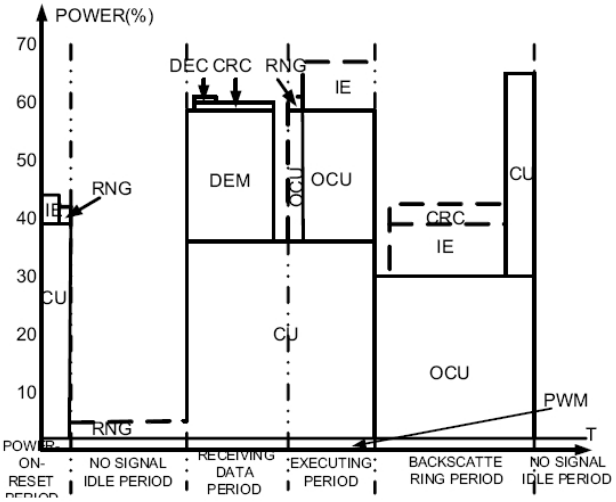
Literatür incelendiğinde karşımıza çıkan RNG üreteçleri etiketin okuyucu alan içerisine girmesiyle çalışmaya başlamakta ve çekirdek değerlerini etiketin EPC kodunu alarak ve bunun CRC datasını üreterek kullanırlar. Ardından herbir etikete yeni bir komut gelene kadar çalışıp her saat darbesinde yeni bir rastlantısal sayı üretirler. Ancak bu yapının sonuçları, bu tezde incelenen kriterlerler bu yayınlarda yer almamaktadır. Bu yüzden bu çalışma böyle bir sistemin sonuçlarını verme açısından bir ilkdir. [26] çalışmasında kullanılan rastlantısal sayı üreteci EPC kodunu kullanmaktadır. Ancak bu tezde EPC C1G2 standardı kullanıldığından, RNG bloğunun bazı kriterleri yerine getirmesi gerekir. Bunlardan bir tanesi EPC kodunun kullanılamaz olmasıdır. Bu yüzden [26] çalışması EPC C1G2 için uygun bir donanım sunmamıştır. RNG etiketin okuyucu alanının içerisine girmesiyle çalışmaya başlamakta ve komut gelene kadar çalışmaktadır bu da donanım için boş bir enerji harcama durumu ortaya koymaktadır. Ancak tezimizde ortaya koyduğumuz yapı rastlantısal sayıya ihtiyaç duyduğumuz anda tek saat darbesi ile sayı ütetilip kullanılabilir. Ve enerji konusunda böylece çok daha az güç harcayan ifadesini kullanabiliyoruz. [26] çalışmasında üretilen sayılar ile ilgili herhangi bir grafik, kriter testi, rastlantısallık testi ortaya konulmamıştır. Bu haliyle üretilen sonuçların çakışma önleyici algoritma için ne kadar uygun olduğu kapalıdır. Üretilen chip tek adet olduğundan bizim çalışmamızda ortaya konulan binlerce adet test kriterleri sağlanamamıştır.

Literatürde RFID için yapılan çalışmalarda özel olarak sadece RNG üretimini amaçlıyan ve sonuçlarına yer veren yayınlara rastlanmamıştır. Bunun yerine RFID etiket içerisinde analog ve digital yapının tasarımına dönük çalışmalar mevcuttur. Bu çalışmalarda RNG ile ilgili yaygın bir kullanım vardır. Bu yüzden [20..27] çalışmaları incelenmiş ve RNG üretimine ait tarafları karşılaştırma yapabilmek için anlaşılmaya çalışılmıştır. Ama sayısal bazı sonuçların verilmemesi, bu tasarımların karşılaştırılmasını zorlaştırmıştır.

[26] çalışmasından alınan ve Şekil 12.'de gösterilen grafik RNG'nin sürekli çalıştığını göstermektedir.

Şekil 12.'den de görüldüğü gibi, power-on-reset dediğimiz, enerjinin gelmesi ile

reset alan sistem, ilk olarak CU ve RNG birimlerini çalıştırmaktadır. CU, kontrol birimidir. Daha sonra etiket komut alana kadar yani "idle" konumunda bulunduğu sürece RNG'nin çalıştığını görüyoruz. Bunun yanında bazı küçük süreli RNG kullanımı görülmektedir. İşte bu tezde yapılan çalışmada bu küçük kullanım zamanlarının haricinde etiket "idle" konumda iken RNG çalışmamaktadır. Bu çalışmanın en önemli avantajı budur.



Şekil 12. RNG'nin sürekli çalıştığını gösteren grafik

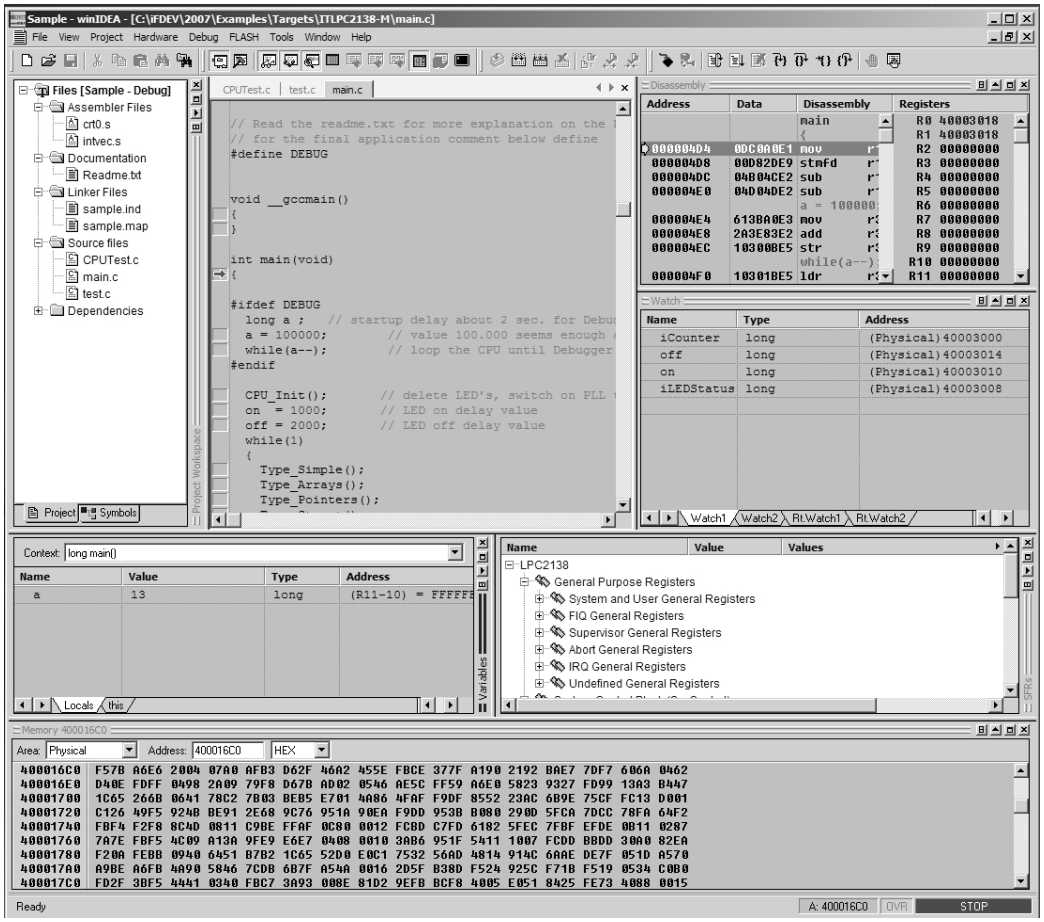
2.3. Yapılan Testler

LPC2138 mikro kontrolöründe bulunan SRAM içeriği incelenmesi için WinIDEA debugger programı ve emülatör kullanılarak bilgisayar ortamına alındı. Şekil 13. ve 14.'de WinIDEA ve LPC2138'in emülatör donanımı görülmektedir.

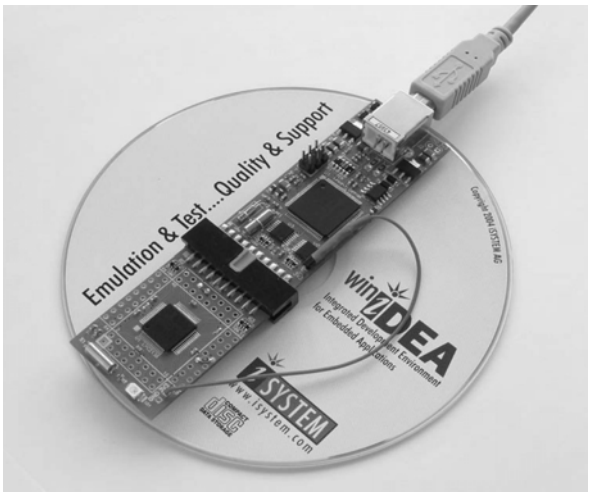
2.3.1. SRAM Testleri

WinIDEA programının Memory pencerisi kullanılarak mikro kontrolörün SRAM bloğu gözlemlenmiştir. Burada tüm donanımın enerjisi kesilip tekrar verildiğinde değişik değerler alan bitlerin durumunda renk değişikliği ile tekrar gösterildiği görülmüştür. Bu değerler göz ile kontrol edilmiş ve byte formatından word formatına kadar rastlantısal sayı üretiminde kullanılabileceği öngörülmüştür. Böylece sayısal olarak verilerin incelenmesine başlanmıştır.

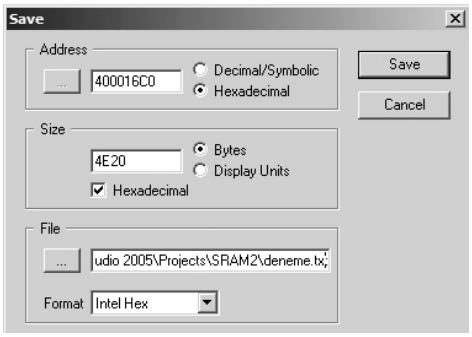
Aynı pencerinin verileri kaydetme özelliğinden yararlanılarak SRAM içeriği istenilen miktarda hex formatında kaydedilmiş ve bu formattan işe yarayan verilerin alınıp C kodu ile işlem yapabileceğimiz Microsoft Visual C++ 2005 Express Edition ortamına alınabilmesini sağlayan bir kod yazılmıştır. Kaydetme işlemine ait pencere Şekil 15.'de görülmektedir. Verilen kod aynı zamanda verileri sinyal işleme programı olan DADiSP ortamına almak için uygun formatta kayıt işleminide yapmaktadır. DADiSP ortamına alınan verilerin grafikleri çıkarılmış ve hazır olan rastlantısal sayı üreteçleri ile grafiksel olarak karşılaştırılmaları yapılmıştır.



Şekil 13. WinIDEA programından bir görünüm

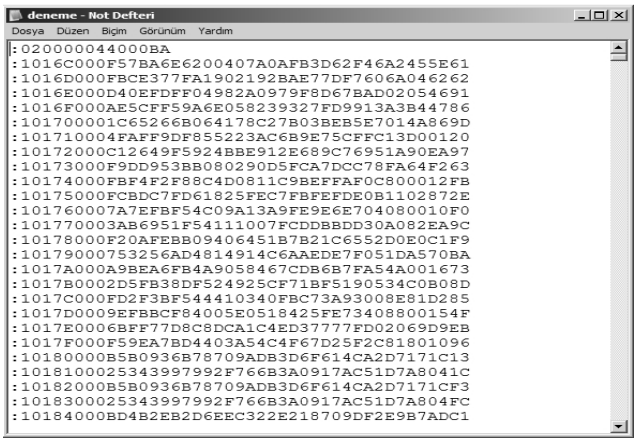


Şekil 14. LPC2138 mikrokontrolör emülatörü



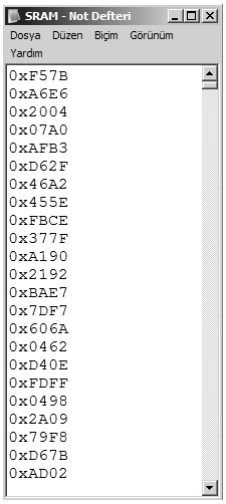
Şekil 15. Kayıt penceresi

Kaydetme işleminden sonra oluşturulan deneme.txt dosyasından bir görünüm Şekil 16.'de gösterilmiştir. Burada hex dosya formatına dikkat edilmesi gerekecektir.



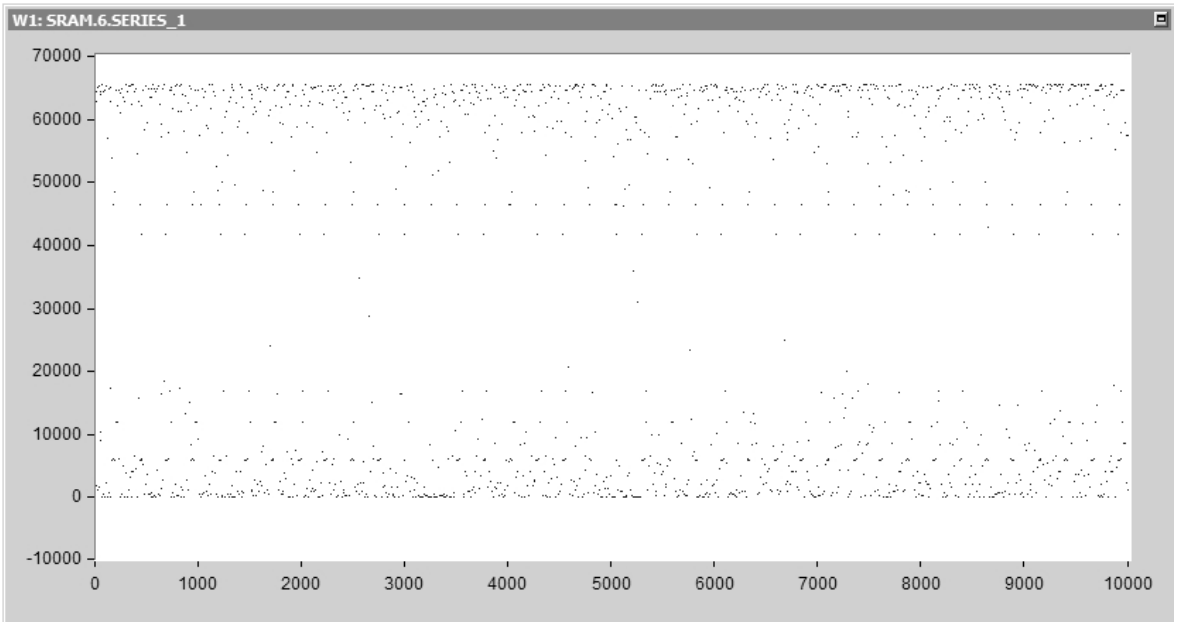
Şekil 16. Hex formatında kaydelilen SRAM içeriği

Buradaki kayıt hex formatında olduğundan, gerekli olan SRAM bitlerinin alınması için kullanılan kod bloğu verilen kodun içerisindedir. Böylece Şekil 17.'da görüldüğü gibi SRAM içeriği elde edilmiş olunur.

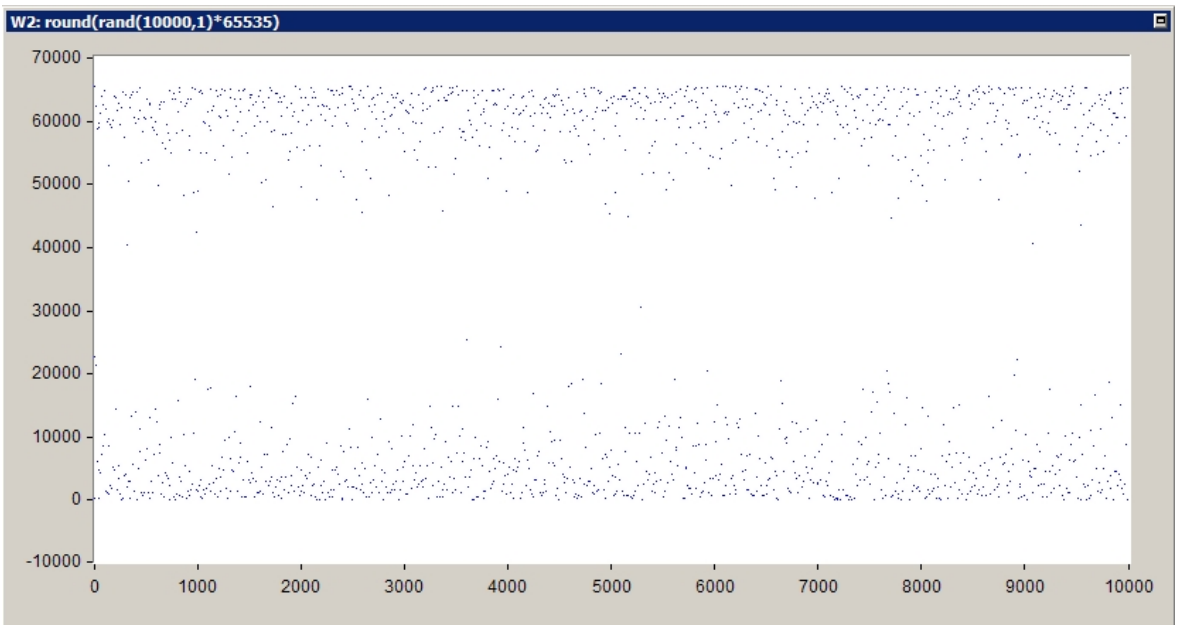


Şekil 17. SRAM içeriği

Şekil 18.'de SRAM bloğundan alınan 16-bit uzunluğundaki 10 bin adet sayının grafiksel olarak gösterimi yapılmıştır. Şekil 19.'de DADiSP ortamında bulunan hazır rastlantısal sayı üreteci kullanılarak üretilen sayıların grafiği gösterilmiştir. Bu grafiklerden SRAM'in 16-bitlik farklı bloklarının birbirinden rastlantısal olarak ne kadar farklı olduğu başka bir rastlatısal kaynak ile karşılaştırılınca daha iyi ortaya çıkmış oluyor. Tabiki arada bir fark var. Ama ileride antılacak olan sayısal işlemlerle bu farkın standardın istediği kriterleri yerine getirmede bir sorun oluşturmadığı görülecektir.



Şekil 18. SRAM'den alınan verilerin grafiği



Şekil 19. Hazır RNG üretecinin ürettiği sayılar

2.3.2. Birinci Kriter Testi

Tasarımda birinci kriter olan, bir üretecin ürettiği sayıların olasılığı ile ilgili istenen değerleri sağlamak için 2 adet LFSR yapısı paralel bağlandığında olasılık 0.5 değerine düşmektedir. Standarda göre bu sayının 0.8 olması istenmektedir. Bu yüzden en fazla

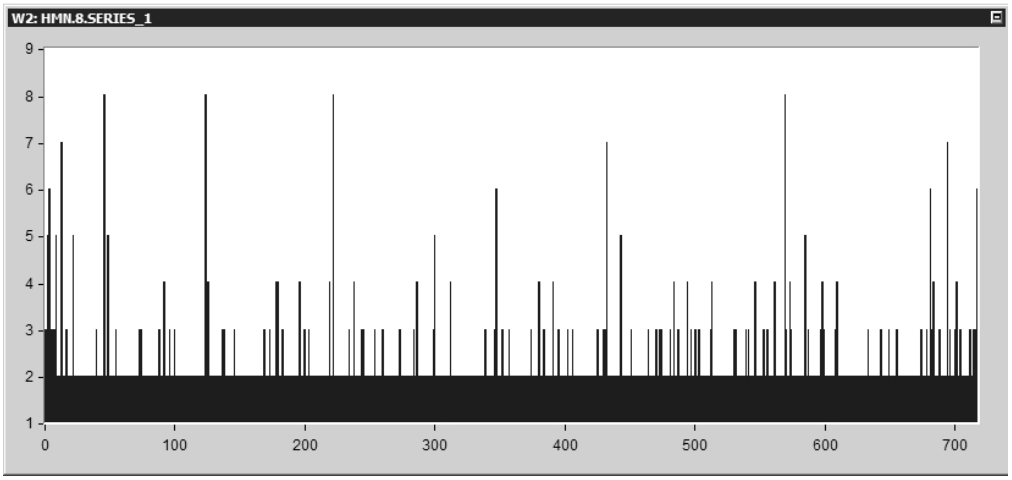
uzunlukta tekrar yapmak için seçilen exorlanacak bitler daha başka bitler kullanılarak bu değerin aşağıya indirilmesi ve böylece olasılık değerinin 0.5 den 0.8 e yükseltilmesi gerekmektedir.

Ancak geçekte, etiket içerisine uygulanacak olan bu yapı aslında tek LFSR bloğunun kullanılması ile daha performanslı bir blok olacağı aşikardır. İstenilen düşük olasılık değeri biraz yüksekte tutularak daha basit bir devre tasarımı ön plana çıkarılabilir. Böylece daha az enerji tüketimi de sağlanabilir. Paralel yapının her iki LFSR bloğuda SRAM'den farklı değerler alacağından 10 bin adet içerisinde 10 adet aynı sayı üretme kriteri çok iyi sağlanmış oluyor. Ancak tek LFSR yapısında bu kriter 10 adetin üstüne çıkıyor. Yine burada da kriterden ödün verip daha basit bir tasarımı ön plana çıkarmak için tek LFSR yapısı kullanılabilir. Paralel LFSR 2 adet 16 bit SRAM verisi kullandığından mevcut olan etiket içerisinde kullanılacak SRAM bloğunun bunun için çok yeterli olduğunu söyleyebiliriz. Protokolün getirdiği haberleşme altyapısını oluştururken kullanılması gereken geçici hafıza birimlerinin SRAM teknolojisi ile üretilmesi şu anda mevcut olan bir teknolojidir. Dolayısıyla bu RNG bloğu zaten var olan sistem gereksimini kullandığından diğer tasarımlarda olduğu gibi ek bloklara ihtiyaç duymamaktadır.

2.3.3. İkinci Kriter Testi

16-bit uzunluğundaki verilerin 10 bin adet SRAM bloğunda kaç adetinin birbiri ile aynı olduğu Şekil 20. ve 21.'de görülmektedir. Şekil 20.'de 20 adetin üstünde aynı olan sayıları ve bunların kaç adet olduğunu görebiliyoruz. Şekil 21.'de ise 10 adetin altında kaç sayı olduğunu görüyoruz. 10 bin adet sayıdan 700 civarında 10'un altında sayılmış. Tüm bunlar 16-bit alındığında yani paralel LFSR kullanılmadığında SRAM'den alınacak olan verilerin göstereceği özelliklerdir. Paralel yapı kullanıldığında ise 32-bit'e ulaşan çekirdek değerin artık bir benzerini bulmak çok zorlaşıyor. Yapılan simülasyon çalışmasında 32 bit en fazla 2,000 adet sayı ile çalışıldığından ne kadar sayının aynen üretildiği testini ancak 2,000 adet sayıda bakabildik ve test sonucu aynı sayının olmadığını gösterdi. Bu demek oluyor ki 2 adet 16-bit LFSR ve çekirdek değeri olarak kullanılan SRAM değerleri ile oluşturulan blokda birbirinin aynı olan sayıların sayısı neredeyse sıfırdır ve böylece kriter çok iyi sağlanmış olur.

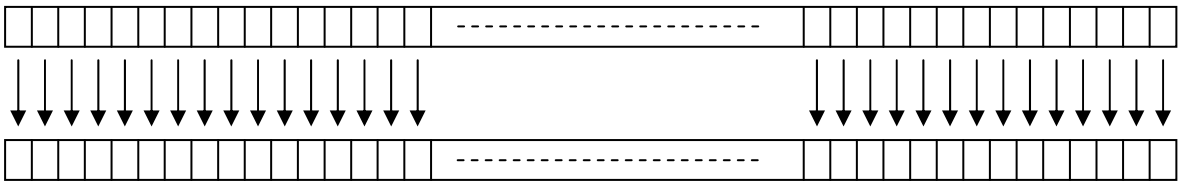
Şekil 20. SRAM değerlerinden 10 adet üzeri olanlarının gösterilmesi



Şekil 21. SRAM değerlerinden 10 adetin altında olanlarının gösterilmesi

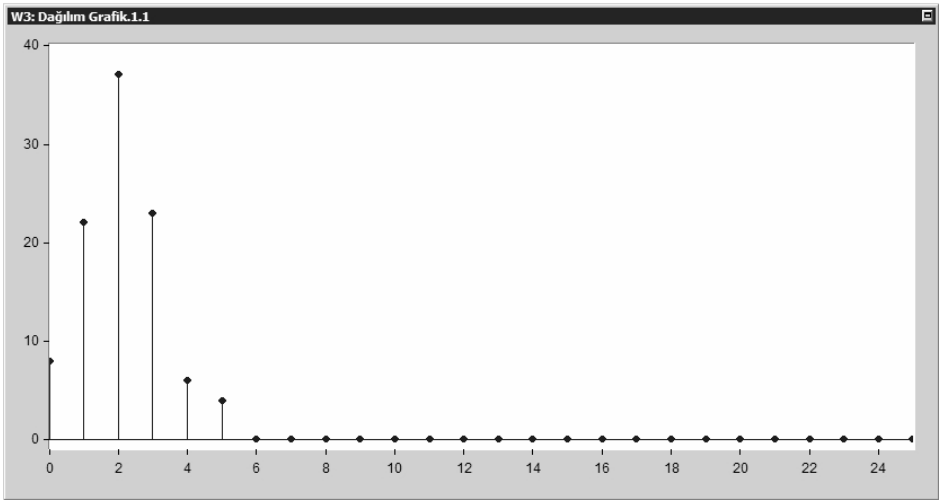
2.3.4. Üçüncü Kriter Testi

Bu kriterde her bir etiket üzerinde bulunan rastlantısal sayı üreteçlerine ait üretilen sayıların tahmin edilebilme olasılıkları araştırılmaıştır. Kritere uygun olup olmadığına bakılmıştır. EPC C1G2 standardının üçüncü kriteri olan bu olasılık değeri 100 bin adet sayı içerisinde 25 edeti geçmemesi yönündedir. Yapılan testlerde tahmin edilebilme olasılığının kriter değerinden çok aşağılarda olduğu görülmüştür. Şekil 22.'de tahmin edilebilme olasılığının nasıl test edildiğine dair bir grafik bulunmaktadır. Çalışmada kullanılan rastlantısal sayı üretecinden alınan 100 bin sayı ile hazır bir üreteçden alınan 100 bin sayı karşılıklı olarak karşılaştırılıp aynı olan değerlerin sayılması ile tahminlik derecesi ortaya çıkmış oluyor.



Şekil 22. Tahmin edilme olasılığı şematize eden gösterim

Şekil 23.'de tahmin edilebilme olasılıklarının dağılım grafiği görülmektedir. Bu dağılım kriterden yani 25 edetten ne kadar uzakta olduğu görülmektedir. Böylece bu çalışmada kullanılan bu sayı üreteci üçüncü kriteri sağlamış oluyor. Şekil 15.'de 100 defa yapılan testlerin sonuçlarından yararlanılmıştır.



Şekil 23. Tahmin edilebilme olasılığının dağılım grafiği

2.4. Simülasyon Çalışması

Simülasyon çalışmasında değişken sayıda etiket ortamı oluşturularak herbir etikete SRAM'den aldığımız değerlerin kullanıldığı rastlantısal sayı üretimi sonucunda ortaya çıkan çakışma miktarı ile hazır bir rastlantısal sayı üreteci ile oluşturulmuş ortamdaki çakışma miktarı karşılaştırılmıştır. Şekil 24.'de bu simülasyonun sonuçlarını içermektedir. Etiket sayısı rastlantısal olarak değişmekte ve her durumda iki sayı üretecinin durumu kayıt altına alınmaktadır. Aynı sayıda olan etiket denemeleri aslında birbirlerinden

tamamen farklı olan etiketler ile yapıldığından çakışma sayılarının farklılığı bundan dolayıdır.

Etiket Sayısı	**Bu çalışmada kullanılan SRAM tabanlı RNG**	**C kütüphanesinden alınan RNG fonksiyonu**
526	33	12
554	49	9
148	29	2
211	0	4
812	39	20
433	21	4
55	0	0
27	0	0
256	18	1
302	48	4
358	30	13
459	7	18
430	34	14
35	0	0
75	5	2
88	4	1
105	3	0

Şekil 24. Farklı sayıda etiketin çakışma durumları

3. SONUÇLAR

Bu çalışmada, UHF RFID sistemlerinde kullanılan etiket üzerinde yer alan RFID mikro yongasında kullanılmak üzere basit, az güç harcayan, standardın getirdiği kriterlere uygun bir rastlantısal sayı üretecinin tasarımı yapılmıştır. Ayrıca kriterlere uygunluk noktasında yapılan ölçümlere yer verilmiştir. Tasarımın uygulama noktasında dikkat edilmesi gereken noktalara değinilmiş ve performanstan ödün vererek daha basit bir yapıya nasıl ulaşılabilineceği anlatılmıştır.

Yapılan deneysel testlerin hangi ortamlarda ve hangi programlar kullanılarak yapıldığı gösterilmiş ve böylece diğer araştırmalara iyi bir altyapı oluşturması amaçlanmıştır.

Tasarımın FPGA içerisinde de uygulanabilir olması, RFID siteminin FPGA içerisinde simülasyon amaçlı olarak kurulması esnasında çok rahatlıkla kullanılmasını sağlamaktadır. Bu, tasarımın hem basit hem de sayısal tasarımda mevcut teknolojileri kullanmasından kaynaklanmaktadır.

Kısaca özetlersek:

- Basit bir tasarım
- Az güç harcayan tasarım
- Standardın kriterlerine uygun
- Tek saat darbesinde rastlantısal sayı üretiliyor, çok hızlı
- FPGA ortamında simülasyon amaçlı uygulanabilir
- Sayısal tasarımda mevcut yöntemleri kullanıyor
- SRAM, diğer sayısal blokların yapısında mevcut olabiliyor
- Protokol içermiyor, uygulaması kolay

4. ÖNERİLER

Kullanılan SRAM bir mikro kontrolörün içerisinde bulunan RAM bloğu kullanılarak ölçümler yapılmıştır. Farklı SRAM donanımları kullanılarak davranış biçimleri karşılaştırılabilir. Sadece SRAM odaklı bir hafıza yongası ile ölçümler tekrarlanabilir.

SRAM'in rastlantısal aldığı değerlerin hangi kriterlere bağlı olduğu ve mirko yapıda hangi çalışmaların bu değerlere etki edeceği araştırılabilir. Böylece ileri düzeyde rastlantısal sayı üretimine önemli ölçüde basitlik getirecek yeni bir yöntem ve yapı oluşturulabilir.

RFID sistemlerinde şifreleme önemli bir problem olarak karşımıza çıkmaktadır. Bu problemi çözmek için bir çok şifreleme algoritması etiket yonga içerisine uygun olacak şekilde yeniden tasarlanmaktadır. Bu algoritmalara istenilen düzeyde, rastlantısal sayı üretmede yapılan tasarımın ne kadar uygun olduğu araştırılabilir. Böylece mevcut olan tasarımın herhangi bir geliştirme olmaksızın uygunluğu görülebilir. Aksi durumda ise blok daha iyi tasarlanmak için yapısı değiştirilerek yeni bir çalışma ortaya konulabilir.

5. KAYNAKLAR

1. "The Case of Radio Frequency Identification" International Telecommunication Union Workshop on Ubiquitious Network Societies, Document UNS/04 April 2005.

2. Klaus Fınkenzeller “RFID Handbook” John Wiley&Sons ISBN 0-740-84402-7, 2003

3. John D. Kraus, Ronald J. Marhefka “Antenna for All Applications” McGraw-Hill, ISBN 0-07-232103-2, 1996

4. "Kısa Mesafe Erişimli Telsiz Cihazlarının (KET) Kurma ve Kullanma Esasları" yönetmeliği 06.03.2004 tarih 25394 sayılı Resmi Gazete

5. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda, "RFID Systems: A Survey on Security Threats and Proposed Solutions", 2004

6. John K., "Various techniques used in connection with random digits", Applied Mathematics Series, no. 12, (1951) 36-38.

7. Peterson Ivars. "*The Jungles of Randomness: A Mathematical Safari",* Wiley, NY, 1998, ISBN 0-471-16449-6

8. Dong-Her Shih, Po-Ling Sun, David C. Yen, Shi-Ming Huang, "Taxonomy and survey of RFID anti-collision protocols", IEEE Computer Communications, 29 (2006) 2150–2166,

9. http://www.merrymeet.com/jon/usingrandom.html, "Using and Creating Cryptographic- Quality Random Numbers", 02/03/2007.

10. Jun, B. and Kocher, P., “The Intel Random Number Generator”, Cryptography Research. Inc white paper, 22/04/2007.

11. http://www.merrymeet.com/jon/usingrandom.html, "Using and Creating Cryptographic-Quality Random Numbers", 11/03/2007.

12. Schneier, B., *Applied Cryptography: Protocols, Algorithms and Source Code in C*, John Wiley & Sons. Inc, 1996.

13. Daniel E. Holcomb, Wayne P. Burleson, and Kevin Fu, Initial SRAM State as a Fingerprint and Source of True Random Numbers for RFID Tags, University of Massachusetts, Amherst MA 01002, USA, 2007

14. EPCTM, Radio-frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860MHz 960MHz, 2005

15. Franklin Prosser ve David Winkel, "The Art of Digital Design - An Introduction to Top-Down Design," second edition, Prentice-Hall, 1987

16. Z. Navabi, "VHDL: Analysis and Modeling of Digital Systems", McGraw-Hill, 1993.

17. Jean-Pierre Deschamps, Gėry Jean Antoine Bioul, Gustavo D. Sutter, "Synthesis of Arithmetic Circuits: FPGA, ASIC and Embedded Systems", John Wiley & Sons, Inc., Publication. 2006.

18. Richard Munden "ASIC and FPGA Verification : A Guide to Component Modelling", Elsevier, 2005.

19. Volnei A. Pedroni, "Circuit Design with VHDL", MIT Press, 2004.

20. Y. Fukumizu, M. Nagata, S. Ohno, K. Taki, A Design of Transponder IC for Highly Collision Resistive RFID Systems: IEEE Asia-Pacific Conference on Advanced System Integrated Circuits, (AP-ASIC) / Aug. 4-5, 2004

21. Y. Yu, Y. Yang, N. Yan, H. Min, A novel design of secure RFID tag baseband: SAINT Workshops 2006, International Symposium; Digital Object Identifier, 10.1109/SAINT-W.2006.15

22. A. Jones, R. Hoare, S. Dontharaju, S. Tung, R. Sprang, J. Fazekas, J. Cain, M. Mickle, An automated FPGA-based reconfigurable, low-power RFID tag: Proceedings of the 6th International Conference on VLSI and CAD, 2005, pp. 107-116.

23. S. W. Man, E. S. Zhang, H.Chan, V. Lau, C. Y. Tsui, H. C. Luong, Design and Implementation of a Low-power Baseband-system for RFID Tag: SAINT Workshops 2006.

24. Y. Niu, M. B. Nejad, H. Tenhunen, L. Zheng, Design of a Digital Baseband Processor for UWB Transceiver on RFID Tag: Proceeding of ISCAS2007, 2007.

25. A. Ricci, M. Grisanti, I. Munari, P. Ciapolini, Design of a Low-Power Digital Core for Passive UHF RFID Transponder: IEEE Journal of Solid-State Circuits, Kasım 2005, 40(11): 2193-2201.

26. H. Yan, H. Jianyum, L. Qiang, M. Hao, Design of Low-power Baseband-processor for RFID Tag: Solid-State Circuits, IEEE Journal of Volume 36, Issue7, July 2001.

27. A. Ashry, K. Sharaf, Ultra Low Power UHF RFID Tag in 0.13 um CMOS: Proc. Int.'l Symp. Circuits and Systems (ISCAS 2005), IEEE Press, 2005.

5. EKLER

Ek 1. VHDL dili kullanılarak tanımlanmış RNG bloğuna ait kodun bir bölümünden alıntı.

```
library IEEE;
use IEEE.STD_Logic_1164.all;
--use IEEE.std_logic_textio.all;
USE ieee.std_logic_arith.ALL;
USE ieee.std_logic_unsigned.ALL;
--use STD.textio.all;

entity LFSR_GENERIC is
port (clock: in std_logic;
resetn: in std_logic;                                    -- active low reset
load: in std_logic;                                      -- active high load
seed: in std_logic_vector(15 downto 0);          -- parallel seed input
parallel_out: out std_logic_vector(15 downto 0);  -- parallel data out
serial_out: out std_logic);                  -- serial data out (From last shift register)
end entity LFSR_GENERIC;

architecture RTL of LFSR_GENERIC is
signal Taps: std_logic_vector(15 downto 0) :=        "1000000000010110";
begin
        LFSR: process (clock)
        -- internal registers and signals
        variable LFSR_Reg: std_logic_vector(15 downto 0);
        variable Feedback: std_logic;
--file my_output : TEXT open WRITE_MODE is "C:\file_io_LFSR.txt";
--variable my_line : LINE;
--variable my_output_line : LINE;
begin
if resetn='0' then
```

Ek 1.'in devamı

```
LFSR_Reg := (others=>'1');
elsif load = '1' then
for index in seed'range loop
if seed(index) = '1' then
LFSR_Reg := seed;
end if;
end loop;
elsif rising_edge(clock) then
--write(my_output_line, conv_integer(LFSR_REG));
--writeline(my_output, my_output_line);
Feedback := LFSR_Reg(15);
for N in 15 downto 1 loop
if (Taps(N-1)='1') then
LFSR_Reg(N) := LFSR_Reg(N-1) xor Feedback;
else
LFSR_Reg(N) := LFSR_Reg(N-1);
end if;
end loop;
LFSR_Reg(0) := Feedback;
end if;
parallel_out <= LFSR_Reg;   -- parallel data out
serial_out <= LFSR_Reg(15);                -- serial data out
end process;
end RTL;
```

Ek 2. Yapılan deneysel simülasyonlar için C dili kullanılarak yazılmış kod.

```
// SRAM.cpp
#include "stdafx.h"
#include "stdlib.h"
#include <stdio.h>
#include <process.h>
using namespace System;
int main()
{
        unsigned __int16 addnum;
        unsigned __int16 seed[10000];
        unsigned __int16 test[65536];
        unsigned __int16 show[1000];
        unsigned __int16 LFSR_Reg[16] =
{0x1,0x1,0x1,0x1,0x1,0x1,0x1,0x1,0x0,0x1,0x0,0x1,0x0,0x0,0x0,0x0};
        unsigned __int16 LFSR[200000];
        unsigned __int16 Feedback;
        unsigned __int16 Taps[16] = {0,1,1,0,1,0,0,0,0,0,0,0,0,0,0,1};
    int i, ch, k, n, m, g, p, d, h;
        int tc = 0;
        int fc = 0;
        unsigned __int16 Random[10000];
        unsigned __int16 Randomdadisp[200000]; // DADiSP round(rand(100000,1))
    FILE* fp;
        FILE* RAM;
        FILE* GRA;
        FILE* RND;
        FILE* RANDOM;

    fopen_s(&fp, "C:\\Documents and Settings\\Administrator\\Belgelerim\\Visual
Studio 2005\\Projects\\SRAM2\\deneme.txt", "r");
```

Ek 2.'nin devamı

```
if (!fp)
   {
     printf("Failed to open file deneme.txt\n");
     exit(1);
   }
      fopen_s(&RAM, "C:\\Documents and Settings\\Administrator\\Belgelerim\\Visual Studio 2005\\Projects\\SRAM2\\SRAM.txt", "w");
   if (!RAM)
   {
     printf("Failed to open file SRAM.txt\n");
     exit(1);
   }
   fopen_s(&GRA, "C:\\Documents and Settings\\Administrator\\Belgelerim\\Visual Studio 2005\\Projects\\SRAM2\\HMN.txt", "w");
   if (!GRA)
   {
     printf("Failed to open file HMN.txt\n");
     exit(1);
   }
   fopen_s(&RND, "C:\\Documents and Settings\\Administrator\\Belgelerim\\Visual Studio 2005\\Projects\\SRAM2\\random.txt", "w");
   if (!RND)
   {
     printf("Failed to open file random.txt\n");
     exit(1);
   }
  fopen_s(&RANDOM, "C:\\Documents and Settings\\Administrator\\Belgelerim\\Visual Studio 2005\\Projects\\SRAM2\\randomdadisp.txt", "r");
   if (!RANDOM)
   {
     printf("Failed to open file randomdadisp.txt\n");
```

Ek 2.'nin devamı

```
exit(1);
   }
       fseek( RANDOM, 0L, SEEK_SET );
       for( i = 0;   i < 200000;i++ )
       {
       fscanf( RANDOM, "%d", &Randomdadisp[i] );
       }
       for( i = 0;   i < 10000;i++ )
       {
       Random[i]=(rand() << 8)|rand();
       fprintf( RND, "%d\n", Random[i] );
       }
       k=1;// to catch 16-bit data
       for(n=0;n<10000;n++) seed[n]=0x0000;
       for(h=0;h<1000;h++) show[h]=0x0000;
       for(n=0;n<200000;n++) LFSR[n]=0x0000;
       n=0;
   m=0;
       g=0;
       p=1;
       h=0;
       while ( (ch = getc(fp)) != EOF )
   {
      if(m<=8) goto K1;
                       switch (ch)
                       {
                       case 48: addnum = 0x0000; break;
                       case 49: addnum = 0x0001; break;
                       case 50: addnum = 0x0002; break;
                       case 51: addnum = 0x0003; break;
                       case 52: addnum = 0x0004; break;
                       case 53: addnum = 0x0005; break;
```

Ek 2.'nin devamı

```
                    case 54: addnum = 0x0006; break;
                    case 55: addnum = 0x0007; break;
                    case 56: addnum = 0x0008; break;
                    case 57: addnum = 0x0009; break;
                    case 65: addnum = 0x000A; break;
                    case 66: addnum = 0x000B; break;
                    case 67: addnum = 0x000C; break;
                    case 68: addnum = 0x000D; break;
                    case 69: addnum = 0x000E; break;
                    case 70: addnum = 0x000F; break;
                    }
                    // put char into file code
                    putc(ch, RAM);
                    if(p>3) {putc('\n', RAM); p=0; putc('0', RAM); putc('x', RAM);}
                    p++;
                    //
                    if(k==1) seed[n]=seed[n]+(addnum<<12);
                    if(k==2) seed[n]=seed[n]+(addnum<<8);
                    if(k==3) seed[n]=seed[n]+(addnum<<4);
                    if(k==4) {seed[n]=seed[n]+addnum; k=0; n++; g++;}
                    k++;
                    if(g==8)
                    {
                              while ( (ch = getc(fp)) != '\n' ){}
                              m=-1;
                              g=0;
                    }
K1:
                    m++;
          }

          for(d=0;d<65536;d++)
```

Ek 2.'nin devamı

```
test[d]=0;
        for(n=0;n<10000;n++)
        {
                for(d=0;d<65536;d++)
                        if(seed[n]==d) test[d]++;
        }

        for(d=0;d<65536;d++)
        {
                if(test[d]>20)
                {
                        show[h]=test[d];
                        fprintf( GRA, "%d\n", show[h] );
                        h++;
                }
        }
        fcloseall();
        for(int p=0;p<200000;p++)
        {
                Feedback = LFSR_Reg[15];
                for(int s=15;s>=1;s--)
                {
                        if(Taps[s-1]==1)
                                LFSR_Reg[s] = LFSR_Reg[s-1]^Feedback;
                        else
                                LFSR_Reg[s] = LFSR_Reg[s-1];
                }
                LFSR_Reg[0] = Feedback;

                for(int t=15;t>=1;t--)
```

Ek 2.'nin devamı

```
{
                                LFSR[p] = LFSR[p] + (LFSR_Reg[t]<<t);

}
                LFSR[p] = LFSR[p] + LFSR_Reg[0];
        }

        for(int p=0;p<200000;p++)
        {
                if(LFSR[p]==0xAA98) fc++;
        }

        for(int p=0;p<200000;p++)
        {
                if(LFSR[p]==Randomdadisp[p]) tc++;
        }
}
```

ÖZGEÇMİŞ

İhsan SOLAK 1982'de Trabzon'da doğdu. İlk ve orta öğrenimini Trabzon'da yaptı. 2001 yılında Karadeniz Teknik Üniversitesi, Mühendislik Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü'nde Lisans Programı'na başladı ve 2005 yılında bu bölümden mezun oldu. Aynı yıl Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü Elektronik Mühendisliği Ana Bilim Dalı'nda Yüksek Lisans Programı'na başladı. Yabancı dil olarak İngilizce bilmektedir.