İSTANBUL TEKNİK ÜNİVERSİTESİ

ELEKTRİK-ELEKTRONİK FAKÜLTESİ

GÜVENLİ BİR RFİD PROTOKOLÜ GERÇEKLENMESİ VE TEST EDİLMESİ

BİTİRME ÖDEVİ

CUMHUR ERDİN

040090414

Bölümü: Elektronik ve Haberleşme Mühendisliği Bölümü

Programı: Elektronik Mühendisliği

Danışmanı: Doç. Dr. Sıddıka Berna ÖRS YALÇIN

MAYIS 2014

ÖNSÖZ

Öncelikle bitirme projem boyunca bana yardım eden, bilgilerini, önerilerini, vaktini ve desteğini hiçbir zaman esirgemeyen hocam Doç. Dr. Sıddıka Berna ÖRS YALÇIN'a çok teşekkür ederim.

Bu çalışma sırasında yardımcı olan arkadaşlarıma ve İstanbul Teknik Üniversitesi Gömülü Sistemler Tasarımı Laboratuvarına teşekkür ederim.

Son olarak, her zaman yanımda olan ve destekleriyle güç bulduğum aileme sonsuz teşekkürlerimi sunarım.

Cumhur ERDİN

MAYIS 2014

İÇİNDEKİLER

KISALTMALAR

RFID : Radio Frequency Identification
FPGA : Field Programmable Gate Array
EDK : Embedded Development Kit
SDK : Software Development Kit
ISE : Integrated Synthesis Environment
XPS : Xilinx Platform Studio
TEA : Tiny Encryption Algorithm
SPI : Serial Peripheral Interface
LUT : Look-up Table
CRC : Cyclic Redundancy Check
LRC : Longitudinal Redundancy Check

ŞEKİL LİSTESİ

GÜVENLİ BİR RFİD PROTOLOLÜ GERÇEKLENMESİ VE TEST EDİLMESİ

ÖZET

Radyo frekansı ile tanımlama (Radio frequency identification, RFID) teknolojisi bugün kolay uygulanabilen ve etkin bir sistem olduğundan tüm dünyada yaygın bir kullanım alanına sahiptir ve bu kullanım her geçen gün artmaktadır. RFID protokolünün güvenliği gelişen teknoloji ile birlikte çok daha önemli hale gelmiştir. RFID sistemleri çok çeşitli alanlarda (kredi kartı gibi) kullanılmaktadır. RFID sistemlerinde bulunabilecek güvenlik açıkları, bu gibi sistemlerin taşıdıkları bilginin kıymetli olmasından dolayı önem taşır ve giderilmesi gerekir. Örneğin kimlik bilgilerinin ortaya çıkması, veri tabanlarına ve sistemlere erişilebilmesi, finansal verilere yapılabilecek olan bir takım etkiler bunların sadece bir kısmıdır. Bunu geliştirmek için Alanda Programlanabilir Kapı Dizileri (field-programmable gate array, FPGA) üzerinde RFID protokolü gerçekleştirilmiş, bu sisteme çeşitli saldırılarda bulunulmuş ve tedbir önerilerinde bulunulmuştur.

Sistemde donanım olarak küçük şifreleme algoritması (Tiny Encryption Algorithm - TEA), rastgele sayı üreteci kullanılmıştır. MicroBlaze kullanılarak sistemin kontrolü sağlanmıştır. Kablosuz haberleşmenin sağlanabilmesi için FPGA üzerine RF modüller yerleştirilmiş, haberleşme olarak seri çevresel birim ara yüzü (Serial Preperial Interface – SPI) kullanılmıştır.

Sisteme ilk olarak servisin engellenmesi saldırısı uygulanmış, bunun sonucunda etiket ve okuyucu arasındaki kimlik doğrulama protokolünün engellenmesi sağlanmıştır. Daha sonra, sisteme atak olarak “yeniden oynatma” atakları yapılmıştır. Bu ataklar ile asıl etiketin yerine geçilerek okuyucunun gerçek etiket ile haberleştiğine inandırılması amaçlanmıştır. Rastgele sayılar çok fazla olduğu için belirli bir kısmına olan cevaplar kaydedilmiş ve bu rastgele sayılar geldiğinde atak cihazı etiket yerine geçmeyi başarmıştır.

IMPLEMENTATION AND TEST OF A SECURE RFID PROTOCOL

SUMMARY

Translation of özet

1. GİRİŞ

RFID teknolojisinin çok yaygın kullanılması ve hayatımızda kilit noktalarda bulunması konunun seçilmesinde etkili olmuştur [1]. Personel kontrolü, ürün takibi, güvenlik bunlardan sadece birkaçıdır. RFID kartların yüksek güvenliğe sahip olanları Dünya'da kimlik kartı ve kredi kartı olarak da kullanılmaktadır. RFID sistemin kullanım alanları detaylandırılırsa; stok kontrolü ve envanter yönetiminde, kapı geçiş sistemlerinde (otoparklarda, sitelerde), kamuda bina giriş çıkışlarında, araç takibinde, para ve pasaport içine yerleştirilen etiketlerde, tedarik zinciri uygulamalarında kullanılmaktadır. Gelecekte de aynı şekilde sağlık, turizm, mağazacılık, eğitim, hizmet sektörü, inşaat, kamu, tarım ve hayvancılık sektörlerinde kullanılacak ve kullanım alanları gitgide yaygınlaşacaktır. Bu yüzden bu yaygın sistemin gerçeklemesi ve özellikle de güvenliğinin sağlanması çok önemlidir. Bu kullanılan sistemler hayatımıza büyük kolaylık sağlamaktadır ama güvenlikleri ve kötü amaçlar için kullanılmalarını engellemek amacıyla bu proje seçilmiştir.

RFID sistemleri temel olarak okuyucu ve etiket olmak üzere iki parçadan oluşmaktadır. Bitirme çalışması kapsamında okuyucu ve etiket kısımlarının yanı sıra atak cihazı da FPGA üzerinde gerçeklenmiştir. Sistem üzerinde şifreleme için küçük şifreleme algoritması (Tiny Encryption Algorithm - TEA) kullanılmıştır. Güvenli bir haberleşme sistemi oluşturulması amacıyla sistemde rastgele sayı üretecinden yararlanılmış ve bu rastgele üretilen sayılar sistemde şifrelenerek iletilmiştir. Bu iletilen verilerin doğruluğu, okuyucu ve etiketin aynı şifreleme ve şifre çözme özelliklerine sahip olması kimlik doğrulama işleminin yapılması için kullanılmıştır. Etiket ve okuyucunun sorunsuz haberleşiyor olduktan sonra sistem üzerinde çeşitli atak işlemleri denenmiştir.

Sisteme servisin engellenmesi saldırısı yapılmıştır. Programlanan atak cihazı yardımıyla etiket ve okuyucunun veri akışına rastgele üretilen sayılar verilmiştir. Diğer bir atak olarak tekrarlama saldırısı kullanılmıştır. Atak cihazı bu sefer etiket ve okuyucu arasındaki haberleşmeyi kaydetmiş, okuyucudan gelen sinyallere karşı etiketin hangi sinyalleri gönderdiğini tespit etmiştir. Okuyucunun gönderdiği rastgele

üretilmiş olan sayıları kendi sisteminde kaydettiği sayılar ile karşılaştırıp etiketin üreteceği veriyi tespit edip etiketin yerine geçmeye çalışılmıştır.

Şifreleme, şifre çözme, rastgele sayı üreteci devreleri donanım olarak FPGA üzerinde gerçeklenmiştir. Haberleşme ve modüllerin kontrolü işlemleri yazılım ile MicroBlaze işlemcisinden yararlanarak sağlanmıştır. Kablosuz haberleşmenin sağlanması için FPGA üzerine RF modülleri eklenmiş, seri çevresel birim ara yüzü (Serial Preperial Interface – SPI) kullanılarak haberleşme sağlanmıştır.

Bitirme çalışması içerisinde sistemin neden seçildiği, testlerin nasıl yapıldığı, donanım ve yazılım kısımları, konu ve parçalar ile ilgili bilgilere değinilmiştir.

Tez içerisinde yer alan bölümler açıklanacak olursa; tezin ikinci bölümünde radyo frekans ile tanımlama sistemlerinin ne olduğundan genel olarak bahsedilmiş, kullanım alanlarına değinerek önemi vurgulanmak istemiştir. İkinci bölümün son kısmında da etiket yapılarının çeşitleri anlatılmıştır. Üçüncü bölümde ise donanım ve yazılım tasarımın yapıldığı araç, kullanılan diller ve kullanılan ortamlar anlatılmıştır. Dördüncü bölüm içerisinde RFID sistemlerinin güvenlikleri ve bu sistemlere karşı saldırı yöntemleri anlatılmıştır. Beşinci bölümde gerçeklenecek RFID protokolünden bahsedilmiş, altıncı bölümde de yapılan tasarımlar anlatılmıştır. Yedinci bölümde sisteme yapılan saldırılar ve tedbirler ele alınmıştır.

2. RADYO FREKANSI İLE TANIMLAMA SİSTEMLERİ

2.1. Radyo Frekansı ile Tanımlama Sistemleri ve Özellikleri

Ürünlerin otomatik olarak tanımlanmasında farklı yöntemler var olmasına rağmen, radyo frekans kullanan sistemler son yıllarda diğer yöntemlere göre çok daha tercih edilmektedir. Barkot sistemlerinin kullanımları kolaydır fakat veri depolama konusunda oldukça kısıtlıdırlar. Bunun yanı sıra barkot üzerindeki etiketin değerinin değiştirilmesi de mümkün değildir. Bu esnek olmayan kullanımın çözümü mikroçiplerin kullanılmasıdır. Okuyucu ile mekanik temas gerektiren akıllı kartların aksine kablosuz haberleşme ile iletişim sağlanır. Radyo frekans yardımı ile veri ve enerji gönderilir. Bu sistemler radyo frekansı ile tanımlama sistemleri (Radio frequency identification, RFID) olarak isimlendirilir [3].

Sistemin bilimsel olarak anlaşılması 1600'lü yıllara kadar çok yavaş ilerlemiştir. 1600 ve 1800 yılları arasında elektrik, manyetizma ve optik ile beraber, matematik ile ilgili gözlemler, konuyla ilgili bilgi düzeyini arttırmıştır. RFID fikrinin doğuşu olarak 1948 yılında Harry Stockman tarafından yayınlanan "Communication by Means of Reflected Power" varsayılabilir. 1964 yılında R.F. Harrington RFID ile ilgili elektromanyetik teorisini yayınladı. Daha sonra konuyla ilgili icatlar geniş ölçekte ilerlemeye başladı. Genel olarak incelenmek istenirse:

1940-1950 Radar tanımlandı ve kullanılmaya başlandı (özellikle 2. Dünya Savaşında) RFID 1948'de icat edildi.

1950-1960 RFID teknolojisinin ilk keşifler araştırmaları ve laboratuvar deneyleri yapıldı.

1960-1970 RFID teorisinin geliştirilmesi, çeşitli alanlarda uygulamaları denenmeye başlandı.

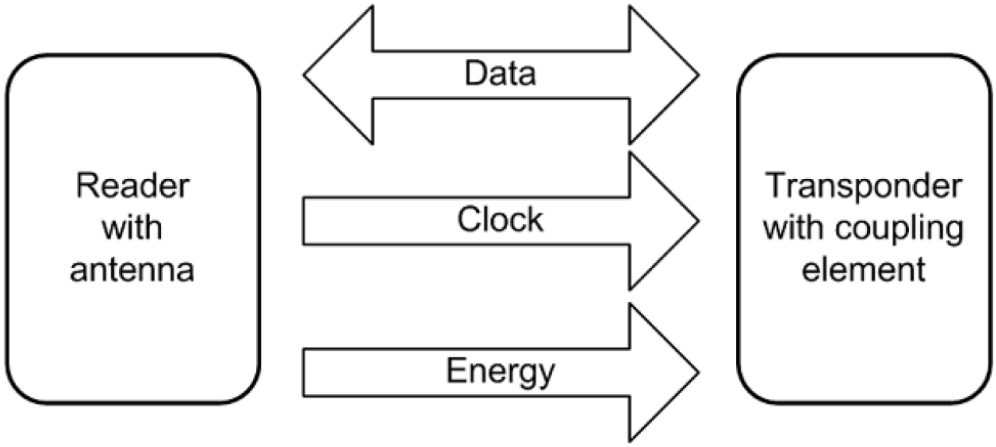
1970-1980 RFID teknolojisinin gelişiminde artış, RFID testleri hızlandı, RFID'nin ilk uygulamaları benimsendi.

1980-1990 RFID ticari uygulamalara dahil oldu.

1990-2000 RFID standartları ortaya çıktı, RFID yaygın şekilde kullanılmaya ve hayatın bir parçası haline gelmeye başladı.

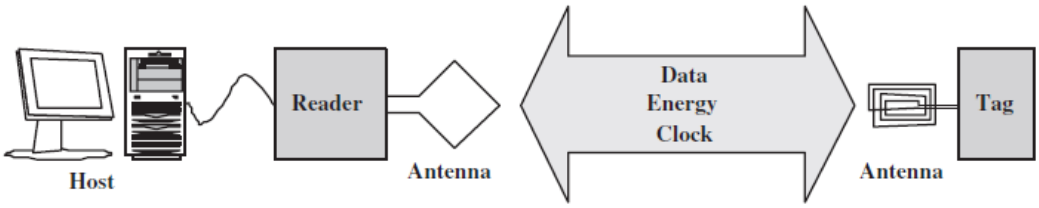
2000- RFID'nin kullanımı artmaya devam ediyor [5].

RFID sistemleri iki temel bileşenden oluşur. Bunlar anteni de içeren okuyucu ve ürünün kimliğini belirten etikettir. Bunlar arasındaki haberleşmede radyo frekansı ve protokol kullanılır. RFID sisteminde okuyucu ve pasif etiket arasındaki hatlar şekil 2.1 de görülmektedir. Veri okuyucu ve etiket arasında çift taraflı olarak aktarılır, saat işareti okuyucudan etikete gönderilir. Pasif etiket ise okuyucudan etiketi aktif hale getirmek için enerji gönderir. RFID sistemlerde okuyucular aynı zamanda kendi veri tabanlarına sahip olabilirler ve etiketlerden alınan veri ile veri tabanları karşılaştırılıp etiketin kayıtlı olup olmadığı sorgulanabilir [3].



Şekil 2.1 : Okuyucu ve etiket arasındaki iletişim [3].

RFID sistemlerini temel olarak incelemek gerekirse nesneye küçük bir devreden oluşan RFID etiket yerleştirilir. Etiketin içerisinde bilgi depolanır ve bu bilgi okuyucu tarafından otomatik olarak alınabilir. Bu yerleştirilen etiket, yerleştirilen nesnenin kimliğini oluşturur. RFID sistemin yapısı şekil 2.2. deki şekilde görülebilir. Bilgisayar okuyucu yardımıyla etiketten bilgiyi radyo frekansı yardımıyla alabilir. Bunu gerçekleştirirken önce bir istek gönderir, daha sonra eğer etiket okuyucunun okuyabildiği alanın içerisinde ise cevap gönderebilir. Etiketten alınan cevap uygulamaya göre bilgisayarda işlenir [6].



Şekil 2.2 : RFID sistem yapısı [6].

Etiketler fonksiyonları bakımından aktif, yarı pasif ve pasif olmak üzere üçe ayrılır. Etiketler ile detaylı bilgi 2.4. başlığının altında daha detaylı olarak verilecektir. Okuyucuları etiketlerden ayıran en önemli özellik birden fazla etiketi okuyabilir ve okuyucular pasif etiketlerin aksine kendi güç kaynaklarına sahiptirler.

Etiket ve okuyucunun hangi formatlarda haberleşeceği, haberleşirken hangi modülasyonu kullanacakları, girişim engelleme metotları ve protokol parametreleri ISO/IEC 18000-3 standardında tarif edilmiştir. Bu standarda göre, RFID okuyucu ve etiket 13.56 MHz frekansında haberleşmektedir [7].

2.2. Radyo Frekansı ile Tanımlama Sistemlerinin Kullanım Alanları

RFID günümüzde birçok alanda hayatımızın içerisindedir. Bu konu başlığı altında en yaygın kullanım alanları olan lojistik, bilet, ulaştırma sektörü, sağlık, güvenlik ve tanımlama sistemlerinden bahsedilecektir.

2.2.1. Tedarik Zincirinde Kullanımı

En önemli RFID uygulama alanlarından biri tedarik zinciri yöntemindedir. RFID etiketler sayesinde ürün zincirindeki tüm nesnelere RFID sistemler sayesinde üretimden satış noktasına kadar takip edilir. Örneğin, lojistik sektöründe dünyada ilk 100 şirket içerisinde olan Megatrux şirketi ürün takibinde Motorola RFID sistemleri kullanmaya başladı. Bu sayede müşteri servisleri gelişti ve giderleri büyük miktarda azalma gösterdi.

RFID uygulamaları bunun dışında teslimatlarda sıklıkla kullanılmaya başlandı. RFID etiket sayesinde gönderiden teslime kadar yeri anlık takip edilebilir. Avustralya da 2005 yılından itibaren yurtiçi postalarında RFID etiketli zarflar kullanmaya başladı. Bu sistem sayesinde paketlerin sıcaklık, konum hatta nem seviyeleri tespit edilmesi amaçlanıyor [8].

2.2.2. Sağlık Sektöründe Kullanımı

Sağlık sektöründeki ilaçların dağıtımı, taşınması ve işlenmesi yüksek oranda doğruluk gerektirmektedir. Ayrıca sağlık sektöründe çıkan problemlerin insan hatalarından kaynaklı olduğu rapor edilmiştir. Bu sorunların çözümünde RFID sistem kullanılmaya başlanmıştır. Hasta ve ilaç takibi hangi hastanın hangi ilacı kullandığı ve bunların iletişimi otomatik olarak sağlanabilmektedir. Bunun yanı sıra görevlilerin ve hastaların giriş çıkışları RFID kart sistemi ile kontrol edilip gerekli yerlere giriş izinleri ile girilmemesi gereken yerlere giriş engellenebilir. Ayrıca envanter yönetimi ve gerekli malzemelerin teminine karar verilmesi yine RFID sistemler tarafından kontrol edilir. İlaçların gerçek olup olmadığı ve gerçek zamanlı stok kontrolü yapılabilir. Sağlık sektöründe bunun gibi yaygın bir kullanım alanına sahiptir. Tahminlere göre Amerika sağlık sektöründe market değeri 2010 yılında 86.3 milyar dolara ulaşmıştır [8].

2.2.3. Ulaşım Sektöründe Kullanımı

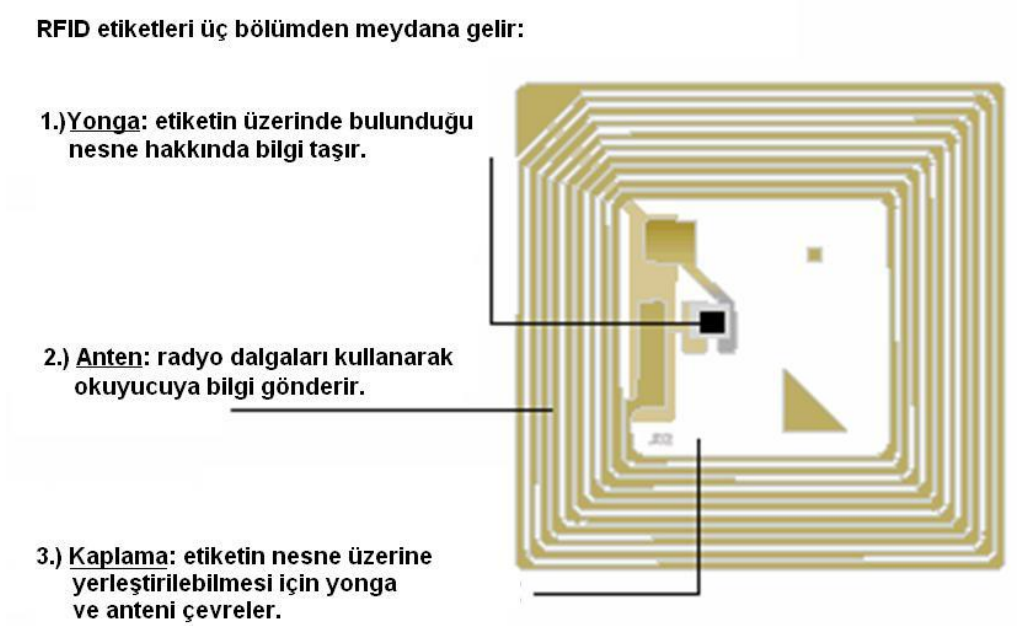
Ulaşım sektöründe de RFID teknolojileri yaygın olarak kullanılmaktadır. Özellikle otoyollar ve araba park yerlerinin hemen hepsinde rahatlıkla görülebilir. Ülkemizde paralı yollarda arabaların trafik sıkışıklığı yaratmadan ücretlerinin alınması yine bu sistem ile yapılmaktadır. Araç içerisindeki etiket okuyucu yardımı ile okunup aracın kimliği tespit edilir ve geçtiği yolun uzunluğuna ve arabanın cinsine göre ücret belirlenir. Araba park yerlerinde, belirli bölgeye girerken ve çıkarken yine RFID sistemlerinden yararlanılır. Araç içine yerleştirilen etiket yardımı ile aracın kimliği belirli olur ve yetkisi olan veya ücreti ödemek karşılığı ile RF okuyucunun olduğu kapı sisteminden geçiş sağlanır.

2.2.4. Güvenlik ve Tanımlama Sistemlerinde Kullanımı

Personel kimlik kartlarında da RFID sıklıkla kullanılmaktadır. Kullanıcının kimliği kullandığı kart içerisinde saklanmaktadır. Amerika da pasaportların içerisinde RFID etiketler kullanılmaktadır. Son zamanlarda yeni tip öğrenci kimlik kartlarının içerisinde de RFID sistem kullanılmaya başlanmıştır. Bu kullanılan RFID etiketler manyetik şeritli kimlik tanımlama depolama sistemlerine göre çok daha güvenilirdirler. Birçok şirket RFID kartlar sayesinde çalışanların iş yerlerine giriş

çıkış saatlerini kontrol etmekte ve sadece yetkisi olduğu alanların girişine izin vermek diğer bölgelere girilmesini engellemektedir. Bunun dışında e-bilet sistemlerinde de RFID kullanılmaktadır [8].

2.3. RFID Etiket Yapısı



Şekil 2.3 : RFID Etiket yapısı [9].

RFID etiketi şekil 2.3'te görüldüğü gibi temel olarak 3 kısımdan meydana gelmektedir. Radyo frekansı kullanılarak yapılan sorguya cevap verme özelliğine sahiptir. Etiketler kullanım yerlerine bağlı olarak değişik boyut ve fonksiyonda olabilmektedirler. RFID etiketler fonksiyonları açısından incelendiğinde aktif etiketler, yarı pasif etiketler ve pasif etiketler olmak üzere üçe ayrılır [10].

2.3.1. Aktif Etiketler

Aktif RFID etiketleri bir verici ve bir güç kaynağına sahiptir. Güç kaynağı mikroçipin devrelerini harekete geçirerek, okuyucuya (reader) sinyal gönderilmesini sağlar (Cep telefonunun baz istasyonuna sinyal göndermesi gibi).

Aktif etiketler kendi yapılarında bulunan güç kaynağı sayesinde devrelerinin çalışmasını ve haberleşme için sinyal üretimlerini sağlarlar. Kendi içinde barındırdıkları piller yani güç kaynakları sayesinde daha uzak haberleşme mesafeleri ve daha iyi çalışma performanslarına sahiptirler. Taşımacılıkta da kullanılabilen bu

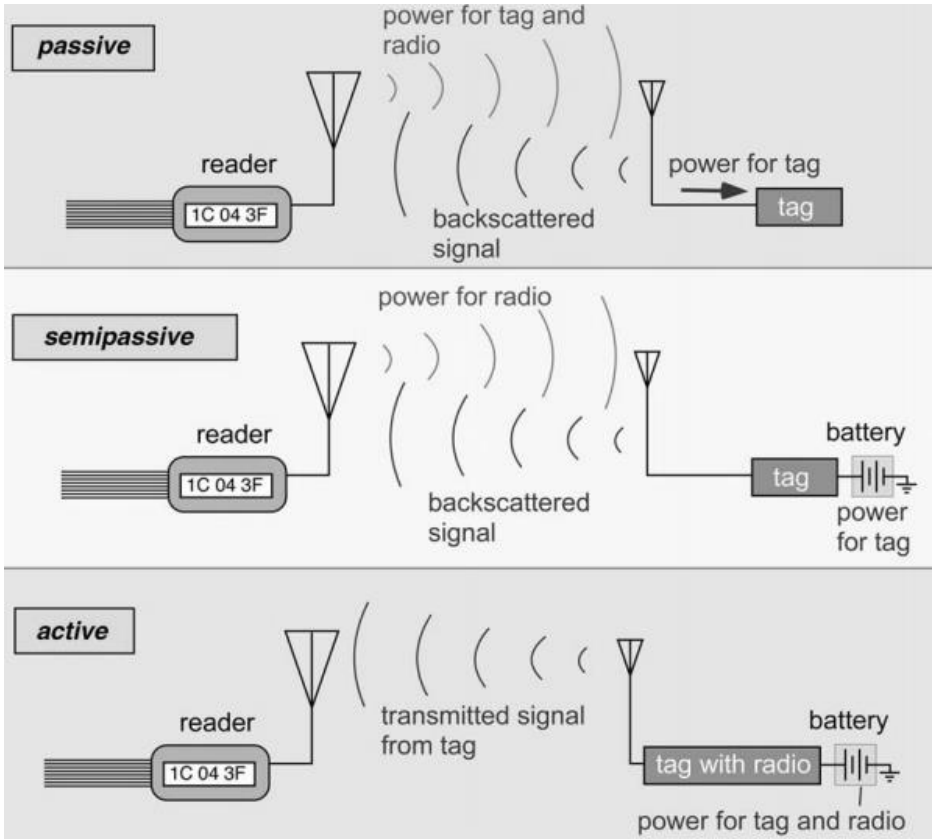
etiketler GPS ve uydu haberleşme sistemleri ile uyumlu çalışabilmeleri sayesinde dünya üzerinde takip edilebilmektedirler. Dezavantaj olarak, pil içermelerinden dolayı bakım gerektirdiklerinden maliyetleri yüksektir [10].

2.3.2. Yarı Pasif Etiketler

Yarı pasif etiketler de aktif etiketler gibi kendi güç kaynaklarını içerirler fakat yarı pasif etiketler çipin devrelerini harekete geçirmek için güç kaynağı kullanırken, iletişim kurmak için okuyucudan uyarı alırlar [10].

2.3.3. Pasif Etiketler

Pasif etiketler güç kaynağına sahip değildir. Elektromanyetik dalgalar göndererek etiketin antenini uyaran okuyucudan, güç alırlar. Güç kaynakları içermemeleri daha kısa mesafeli haberleşmeler için kullanılmasına neden olur. Ucuz ve basit yapıda olduklarından tercih edilirler. Bu sebeple güç kaynağının uygulanamadığı, pil ömrünün daha öncelikli olduğu ve işlem kapasitesinin ikinci planda olduğu alanlarda kullanılırlar [10].

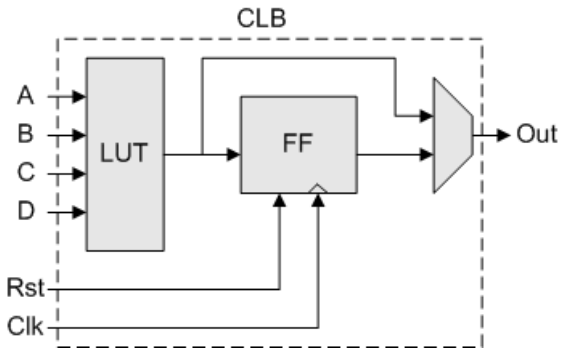


Şekil 2.4 : RFID Etiket çeşitleri [2].

3. GERÇEKLEME ORTAMLARI

3.1. Alanda Programlanabilir Kapı Dizinleri

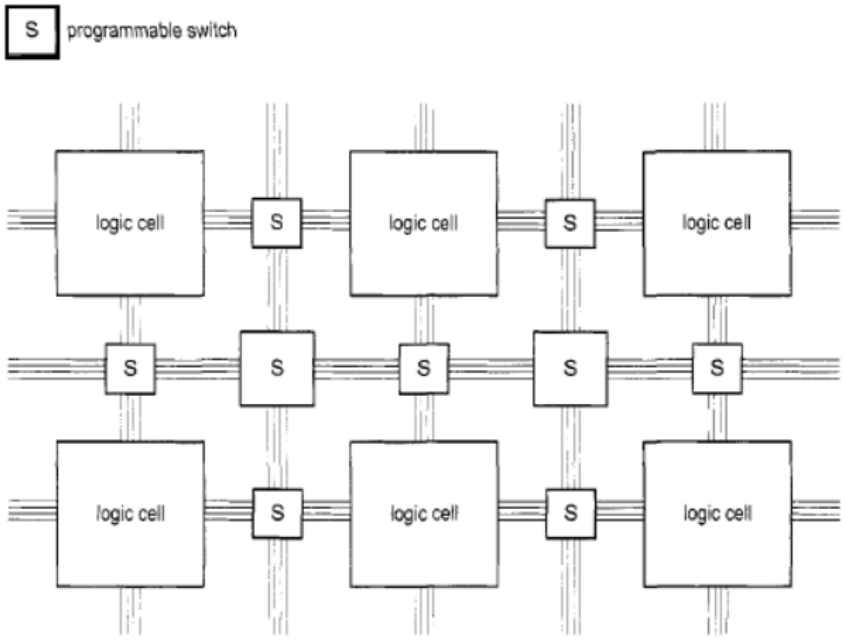
FPGA yönetilebilir anahtarların ve programlanabilir mantık hücrelerinin iki boyutlu olarak dizilmesi ve programlanabilir anahtarların yerleştirilmesi ile oluşturulur. Mantık hücreleri basit bir fonksiyonu gerçeklemek üzere yapılandırılabildiği gibi programlanabilir anahtarlar ile mantık hücreleri arasında bağlantılar kurulabilir. Özel tasarımlar her bir mantık hücresinin ve anahtarların programlanması ile elde edilir. Donanım tanımlama dilleri kullanılarak devrenin tasarımı yapıldıktan ve sentezlenmesinin ardından istenilen lojik hücre ve anahtar yapılandırılmasının yer aldığı veri dizisi kablo yardımıyla FPGA'ya gönderilerek devre gerçeklenmiş olur [11].



Şekil 3.1 : Mantık hücresi yapısı [11].

Mantık hücreleri Şekil 3.1'de görüldüğü gibi programlanabilir kombinezonsal devre ve bir adet D tipi flip-flop içerir. Genellikle programlanabilir kombinezonsal devrelerde LUT (Look-up Table) kullanılır. LUT'lar aslında bir mantık işlemini yerine getiren küçük belleklerdir. N girişli bir LUT 2^N boyutlu bellek elemanına karşılık düşmektedir. LUT'un içerisine gerekli kod yazılarak herhangi bir n girişli kombinezonsal fonksiyon elde edilebilir [11].

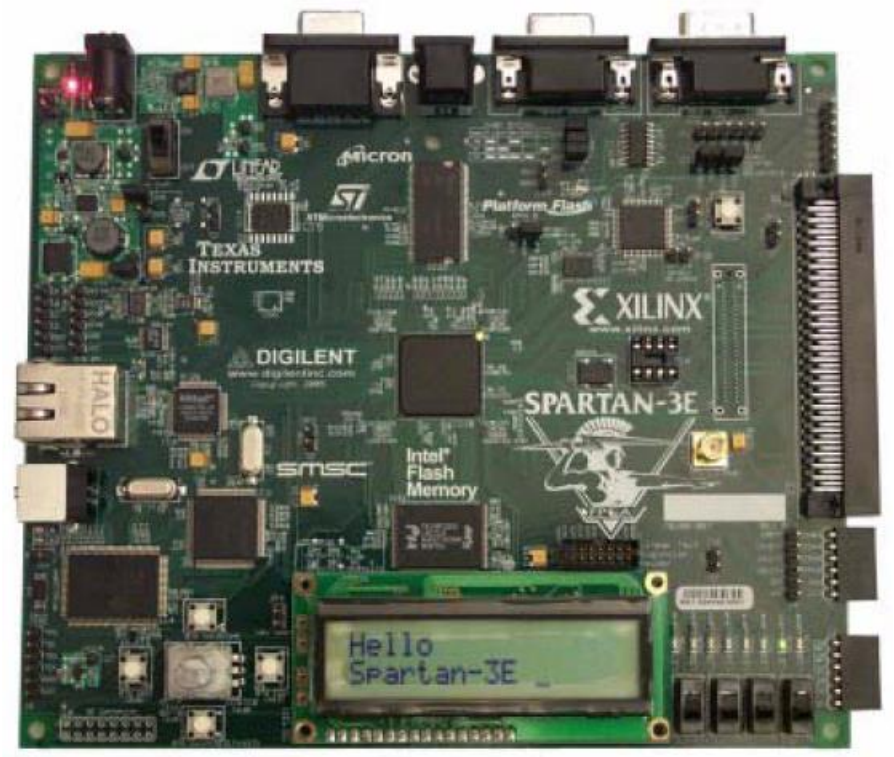
Mantık hücreleri ve anahtarlardan oluşan FPGA'in genel görüntüsü şekil 3.2'de görülmektedir.



Şekil 3.2 : FPGA İç Yapısı [11].

FPGA temel olarak içinde bulundurduğu elemanlar yardımıyla tasarımcının ihtiyaç duyduğu mantık işlevlerini gerçekleştirme amacına yönelik olarak üretilmiştir. Dolayısıyla FPGA içerisinde bulunan her bir mantık bloğunun işlevi kullanıcı tarafından düzenlenebilmektedir. FPGA isminin kaynağı olan alanda programlanabilir isminin verilmesinin nedeni, mantık bloklarının ve ara bağlantıların imalat sürecinden sonra programlanabilmesidir. Bunun yanı sıra FPGA paralel işlem yapabilme özelliğine sahiptir. FPGA içerisindeki yapılar sayesinde içerisine mikroişlemci de gömebilmek mümkündür. FPGA donanım ve yazılımın bir arada gerçekleştirilmesine olanak sağlamaktadır. Tümleşik ve daha hızlı bir yapıya sahip olmasından dolayı bu proje içerisinde FPGA kullanılmaya karar verilmiştir.

3.2. Xilinx Spartan-3E Başlangıç Kiti



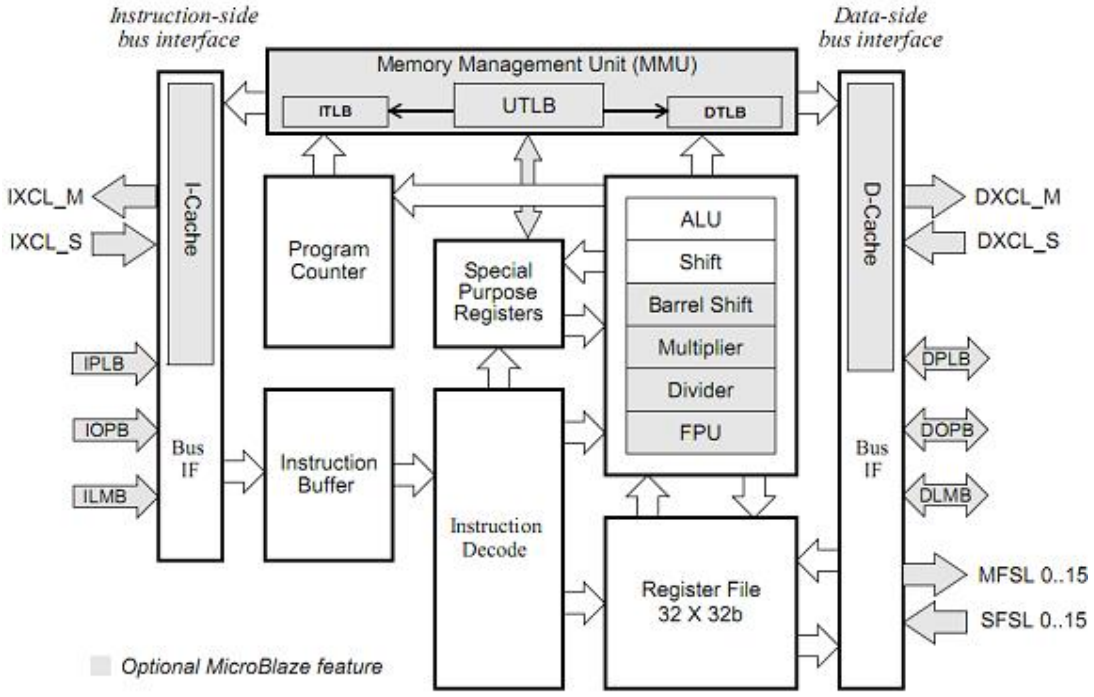
Şekil 3.3 : Spartan-3E Başlangıç Kiti [12].

Projede kit olarak Spartan-3E başlangıç kiti kullanılmaktadır. Bu başlangıç kiti, Xilinx firmasının Spartan3E FPGA kullanıcılarına hızlı bir başlangıç yapmaları için hazırlanmış geliştirme karttır. FPGA kitinin genel görünümü Şekil 3.3'te görülmektedir. Bu başlangıç kitinin başlıca 50 MHz kristal saat üreteci, paralel flash, 64 MByte Çift Veri Oranlı Senkron Dinamik Rastgele Erişimli Hafıza, Ethernet, iki adet seri port, 4 adet kayan anahtar, 8 adet led, 4 adet anlık temaslı buton, 100-pin genişlemeli bağlantısı ve 500.000 kapıya sahip FPGA'e sahiptir [12].

3.2.1. MikroBlaze İşlemcisi

Sistemin gerçeklenmesi için FPGA üzerine MikroBlaze gömülmüştür. MikroBlaze gömülmesinin sebebi; MikroBlaze FPGA üzerinde kullanılabilen yazılım temelli mikroişlemcidir, bu işlemci bazı özellikler dışında kullanıcıya istediği çevreseli ekleme ve çıkarma olanağı sağlayabilmektedir. Ayrıca fiziksel olarak kartın üzerinde bulunmaz. Gömülü yazılım (Embedded Development Kit, EDK) tasarım aracı sayesinde FPGA üzerinde oluşturulur. Ayrıca bu kurulan MikroBlaze tasarımın tüm

kontrolünden ve akışından sorumlu olacaktır. MikroBlaze çekirdeğinin blok diyagramı şekil 3.4 de gösterilmektedir.



Şekil 3.4 : MikroBlaze çekirdeği blok diyagramı [13].

Microblaze 32-bit İndirgenmiş Komut Takımı Bilgisayarı (Reduced Instruction Set Computing, RISC) Harvard bellek mimarisine sahiptir. Program ve veri erişimi ayrı bellek alanlarından sağlanır. Her bir adres alanı 32 bit ile adreslenir [13].

MicroBlaze işlemcisi son derece yapılandırılabilir olup, kullanıcının özellikleri tasarımın gerekliliklerine göre rahatlıkla değiştirebilmesini sağlamaktadır. 32 bitlik 32 adet genel amaçlı kaydedicileri (registers) ve 32 bit adres yolu gibi özellikleri sabit iken, iş hattı (pipeline) derinliği, veri yolu sayısı ve türleri, kayan noktalı sayı birimi (Floating Point Unit, FPU) ve bellek idare birimi (Memory Management Unit, MMU) gibi özellikleri ile FPGA için optimize edilmiş bir mikroişlemcidir [13].

3.3. Donanım Tanımlama Dilleri

3.3.1. Verilog Donanım Tanımlama Dili

Elektronik sistemleri modellemek için kullanılan donanım dillerinden biri verilogdur. Verilog 1983-1984 yıllarında Phil Moorby ve Prabhu Goel tarafından icat edilmiştir. 1985 yılında ise donanım modelleme dili olarak değiştirilmiştir. Yapısal olarak C dili

ile olan yakınlığı nedeniyle sayısal sistem tasarımı geliştiricilerinin sıklıkla tercih ettiği donanım tanımlama dili haline gelmiştir. Dil küçük büyük harf duyarlılığına sahiptir. Verilog geleneksel programlama dilleri gibi basamakları ardışık bir şekilde yürütmez. Ayrıca verilog diliyle oluşturulan modüller arasında bir hiyerarşi söz konusudur. Eğer yazılan verilog kodu sentezlenebilir ifadeler içeriyorsa bu tasarımın donanımda gerçekleştirilecek temel bileşenleri ve bağlantıları oluşturulabilir.

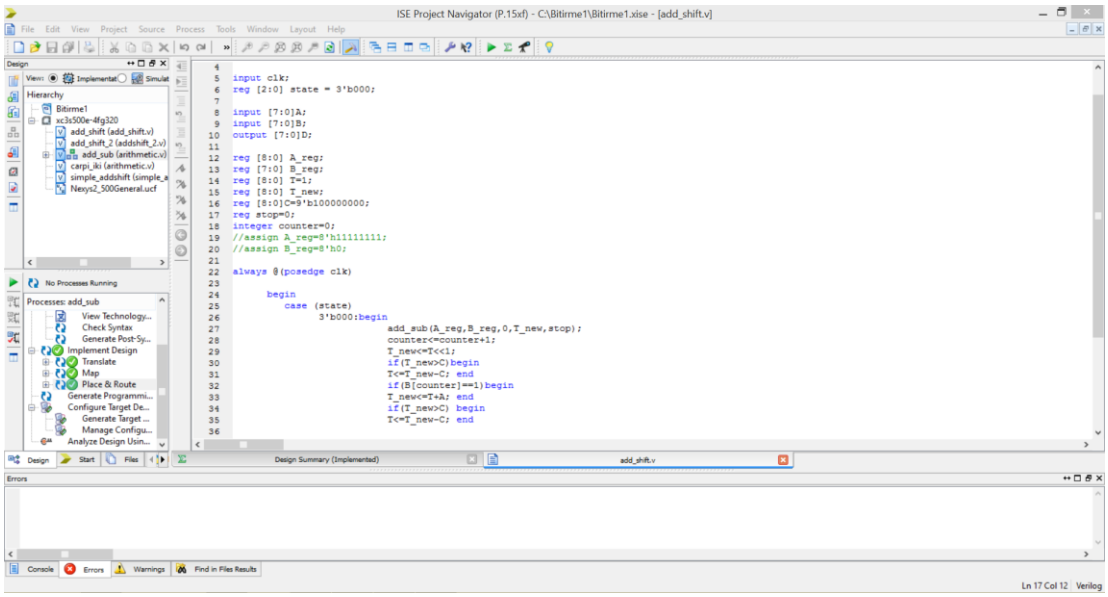
3.3.2. VHDL Donanım Tanımlama Dili

Sayısal devrelerin tasarlanması ve denenmesi amacıyla yaygın olarak kullanılan bir diğer donanım tanımlama dilidir. Açılımı Very High Speed Integrated Circuit Hardware Description Language olan VHDL en çok kullanılan donanım tasarlama dillerinden biridir. VHDL temel olarak Amerika Savunma bakanlığı tarafından ortaya çıkarılmıştır. Daha sonra bu programlama dili 1980'lerden beri kullanılmakta olup sürekli geliştirilmiş ve IEEE tarafından da standart olarak kabul edilmiştir. VHDL genel olarak paralel programlama dili olarak kullanılmaktadır. VHDL, tasarımda hiyerarşinin bulunması, her bir tasarım elemanının iyi tanımlı bir ara yüze ve hatasız davranış tanımlamasına sahip olması gibi özelliklere sahiptir.

3.4. Xilinx ISE Ortamı

Tümleşik Yazılım Ortamı (Integrated Software Environment, ISE) 7 serisi dahil Xilinx ürünlerinin programlanabilmesi için geliştirilmiş bir programdır. ISE ortamında yerleştirme ve FPGA görüntüsü oluşturmak dahil birçok işlem gerçekleştirilebilmektedir. Verilog ve VHDL gibi donanım dilleri ile beraber tasarım tamamlandıktan sonra FPGA içine gömme işlemi yapılabilmektedir. Bunun dışında yazılan programa test kodu eklenerek, devreye verilen uygun giriş değerleri için çıkış değerleri çeşitli benzetim şekillerinde gözlenebilir. Bunlar davranışsal benzetim, sentez sonrası benzetim, FPGA üzerinde gerekli yerleşimler yapıldıktan ve yollar çizildikten sonra gecikmelerin de dahil edildiği benzetim elde etmek mümkündür. Bu test aşamasında hangi değişkenin hangi aralıkta nasıl değiştiği benzetim sonucunda incelenerek yazılan kodun testi yapılabilmektedir. Bu özelliklere ilave olarak devrenin özelliklerini anlatan çeşitli raporlar oluşturmaktadır. Sentez raporu, çeviri sonrası raporu, eşleştirme sonrası raporu, yerleşim sonrası rapor, statik zamanlama raporu gibi detaylı raporları kolaylıkla elde edebiliriz. Tasarım sonucu penceresi

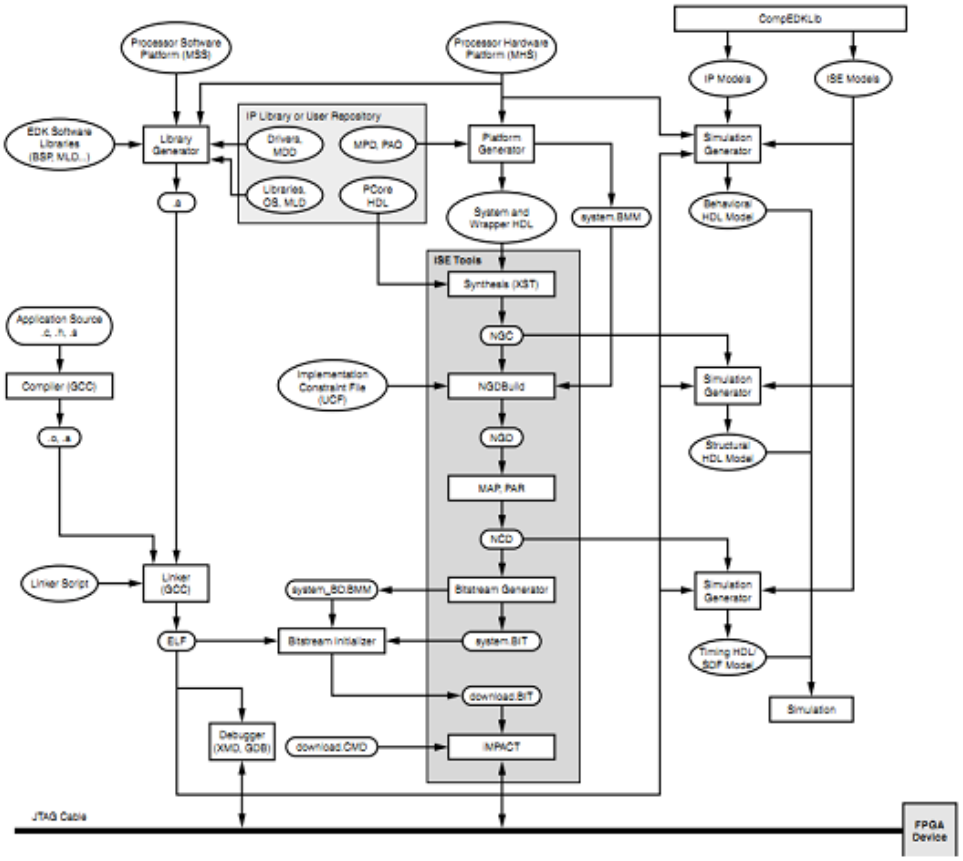
incelendiğinde kullanılan elemanlar ve ne kadar sayıda ve oranda kullanıldıkları, bunun yanı sıra hatlar arası gecikmeler yine ISE aracılığı ile elde edilebilir. Tasarım bittikten sonra FPGA görüntüsünü, nerede hangi elemanın kullanıldığını ve bağlantı hattını inceleyebiliriz.



Şekil 3.5 : Xilinx ISE Programının Görüntüsü.

3.5. Xilinx EDK Ortamı

EDK (Embedded Development Kit) ortamı Xilinx firmasının ürettiği FPGA'lar üzerinde mikroişlemci tabanlı sayısal sistemler geliştirmek üzere kullanıma sunulmaktadır. EDK çevre birimlerinin ve FPGA donanımlarının bağlanması, sistemin adreslenmesi, haberleşme protokollerinin yazılması gibi işlerle uğraşmak yerine sadece donanım ve yazılım tasarımına odaklanmayı sağlar [21]. Şekil 3.6'da FPGA içerisindeki mikroişlemciyi kullanarak tasarlanan bir sistemin tasarım akış diyagramı görülmektedir. EDK ortamının bir önemli avantajı proje süresini kısaltmasıdır. Bu şekilde görülen geliştirme aşamaların hepsini tek bir ara yüz programı ile kullanıcıya sunarak çok zahmetli ve karmaşık sistemleri daha kolay tasarlanabilir hale getirir.



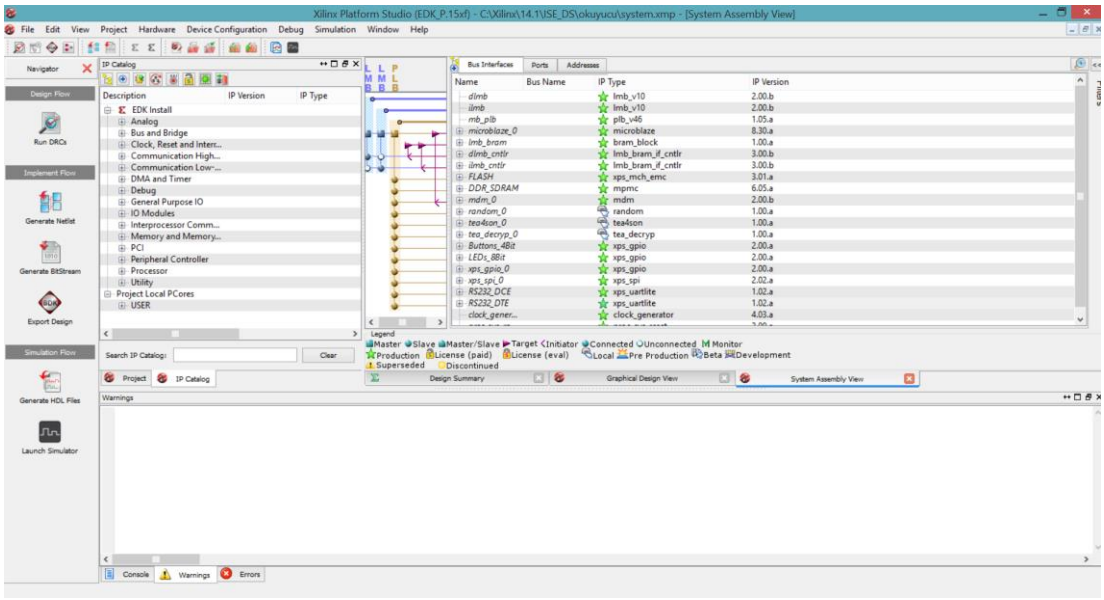
Şekil 3.6 : EDK Sistem Geliştirme Araçları [21].

EDK geliştirme ortamında “soft core” (Microblaze) veya “hard core” (PowerPC) gibi mikroişlemci temelli donanım projelerine FPGA kartı üzerinde bulunan çevre birimleri ve giriş-çıkış birimleri eklenebileceği gibi Xilinx tarafından geliştirilmiş donanımlar ve kullanıcının ISE aracılığıyla oluşturduğu kendi donanımları eklenebilmektedir [21].

EDK ile tasarım oluştururken EDK’nın bize sağladığı Temel Sistem Oluşturucu (Base System Builder, BSB) ile tasarımcıya kendi tasarım sisteminin tabanını kolay bir şekilde oluşturmasını sağlar. BSB yardımıyla tasarımcı kolaylıkla FPGA kartı üzerindeki istediği donanımların hazır İnternet Protokollerini (Internet Protocol, IP) seçerek tasarımına ekleyebilmektedir. Bu kısmı donanım, donanım oluştur ve donanım ekle kısımları kullanılarak yapılabilir. Ayrıca tasarımcı kendi donanımları ve eklediği bu IP’leri EDK’nın sunmuş olduğu veri yolları ile kolayca bağlayarak sistemi oluşturabilir. Bunu yaparken ara yüzden bağlantılar kolay bir şekilde

bağlanabilir. Bununla beraber adres kısmına geçerek sağ üstteki düğme yardımıyla adreslenmemiş kısım için adresleme işlemi de tamamlanabilir. Portlar kısmından bağlı olan portlar ve detayları incelenebilir.

Tasarım yapılırken dikkat edilmesi gereken noktalar arasında seçilen kaydedicilerin uygun sayıda seçilmesidir. Yeterli sayıda giriş, çıkış biti tanımlanması gerekmektedir. Yapılan çalışma içerisinde _cntlr ve RAM blokları sisteme her durumda eklenmiştir. "user logic" içerisinde gerekli değişimler ve atamalar yapılır, kullanılacak fonksiyon çağırılır.



Şekil 3.7 : Xilinx XPS Programının Görünümü.

EDK donanım projesinin yapılandırılmasında XPS (Xilinx Platform Studio) programı kullanılmaktadır. XPS'de Microblaze mikroişlemcisine bağlanan çevre birimleri Microblaze tarafından adreslenmektedir. Sistemin adres haritası üretildikten sonra XPS ortamında ya da ISE ortamında tasarlanan projeye sentezleme ve gerçekleme aşamaları uygulanmaktadır. Son olarak bu aşamadan sonra donanım tasarımı bitirilerek bu donanımı kontrol etmek için kullanılan Microblaze ya da PowerPC gibi mikroişlemcilerin yazılımının tasarlanması aşamasına geçilmektedir. Daha sonra buradan, burada yaptıklarımız SDK'ya aktarılarak geri kalan işlem SDK ortamında devam edilir.

3.5.2.Xilinx SDK Ortamı

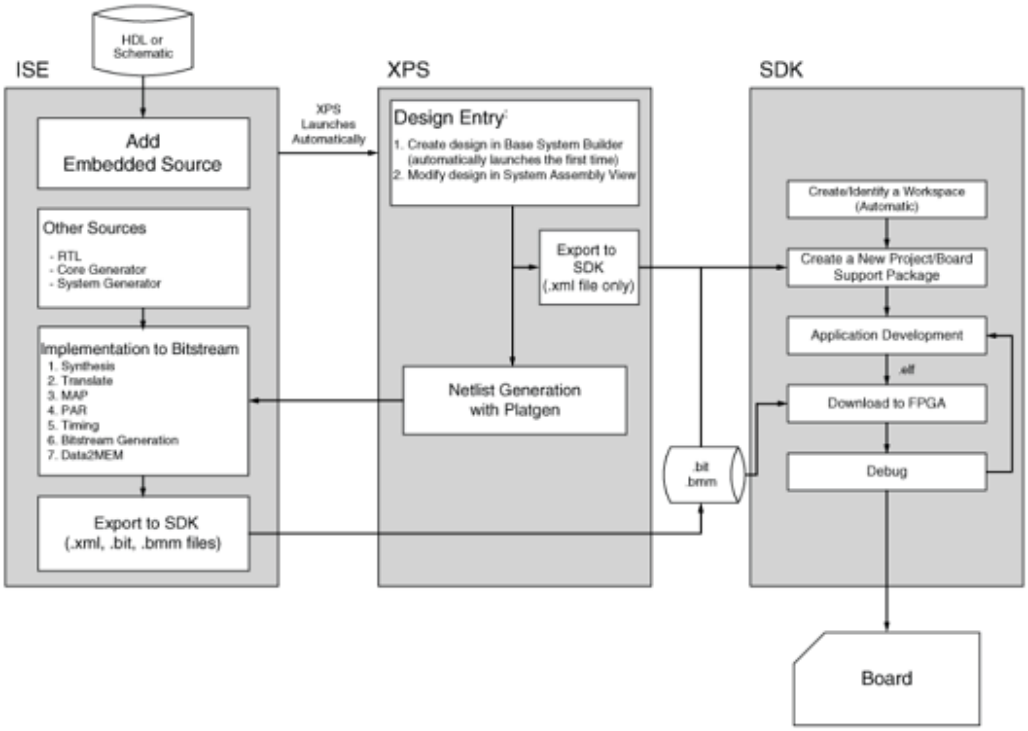
Yazılım Geliştirme Kiti (Software Development Kit, SDK) Xilinx firması tarafından EDK ortamında tasarlanan mikroişlemci merkezli sayısal sistem tasarımlarının yazılım tasarımını gerçeklemek için geliştirilen ara yüz ortamıdır. Xilinx'in tasarım ortamlarının eski sürümlerinde SDK, XPS geliştirme ortamı içerisinde yer almaktaydı. ISE13 sürümünden sonra Xilinx firması SDK'yı XPS ortamından ayırarak XPS'i sadece donanım tasarlama ortamına dönüştürmüştür. SDK ise sadece tasarlanan donanımlara yazılım tasarımı yapmak amacıyla kullanılmaktadır. EDK ortamında tasarlanan sisteme ait kullanıcı donanımları ve çevre birimlerinin kütüphaneleri üretilerek yazılım tasarımına ilk adımın atılması sağlamaktadır. Aynı zamanda, SDK tarafından üretilen kütüphanelerin söz konusu yazılım projesine eklenmesiyle kullanıcıya mikroişlemciyi kolayca kontrol etme olanağı sağlanmaktadır.

- Zengin özellikli C/C++ kod editörü ve derleme ortamı
- Proje yönetimi
- Tasarım yapılandırması uygulaması ve otomatik Makefile üretimi
- Hata navigasyonu
- Kaynak düzeyinde hata ayıklama ve gömülü hedeflerin görünüşü için iyi tümleştirilmiş ortam
- Kaynak kodu sürümü kontrolü

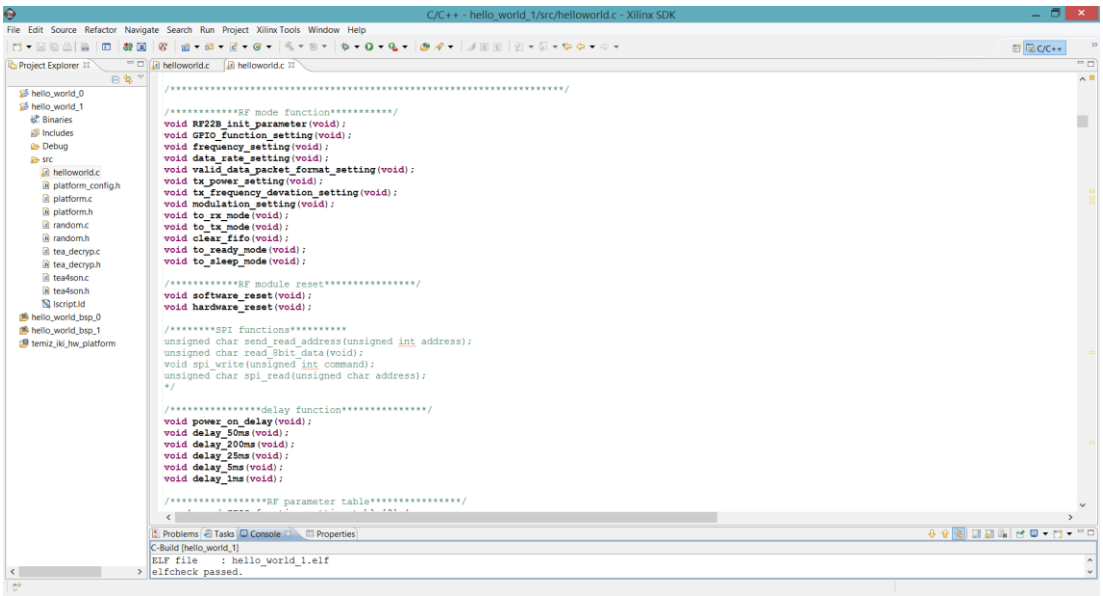
SDK tarafından kullanıcılarına sunulmuş başlıca özelliklerdir [22].

ISE, EDK ve SDK ortamları kullanılarak sıfırdan bir sistem tasarımının akışı Şekil 3.8'de gösterilmektedir. Tasarım akışından bahsedilecek olursa öncelikle ISE ortamında donanım tanımlama dilleri ya da şematik çizimlerle tasarlanan donanımlar EDK ortamında kullanıcı donanımı olarak tanımlanır. EDK ortamında kullanıcı donanımına IP verilerek mikroişlemci merkezli sayısal sistem tasarımına eklenmek istenen diğer hazır IP'lerle birlikte eklenmektedir. EDK ortamında donanım yapısı tamamlanan sistem SDK ortamına gönderilerek bu aşamada otomatik olarak

kütüphaneleri üretildikten sonra yazılım tasarımı yapılmaktadır. Son olarak, donanım ve bu donanımları kontrol etmek için yapılan yazılım da tamamlandıktan sonra SDK aracılığıyla, donanım bilgilerini içeren "bit" uzantılı donanım dosyası ve "elf" uzantılı yazılım dosyası birleştirilerek FPGA'ya gönderilir.



Şekil 3.8 : Sistem Tasarım Akışı [23].



Şekil 3.9 : Xilinx SDK Programının Görüntüsü.

4. RFID SİSTEMLERİNDE GÜVENLİK

RFID sistemleri diğer kimlik tanımlama sistemlerine göre görüş alanına ihtiyaç duymaması kolay takip edilebilirlik açısından çok daha avantajlıdır. Bu özellikler ile beraber RFID kullanımı gün geçtikçe artmakta ve bu kullanım alanlarındaki artış güvenlik, gizlilik gibi konuları ortaya çıkarmıştır.

4.1. Güvenlik

4.1.1. Gizlilik

RFID etiketleri okuyucunun sorgusuna etiketi kullanan veya taşıyan kişiye uyarı vermeden cevap verirler. Bu yüzden okuma sınırları içerisine giren etiketler gizlice taranıp bilgilerinin alınması tehlikesi ile karşı karşıyadırlar. Çoğu RFID etiket kendisine özgü bir tanımlayıcıya sahiptir, bu veri şifrelenmiş bir algoritma ile korunuyor olabilir. Ama buna rağmen RFID etiket etraftaki okuyuculara belirli bir dizi sayı gönderir ve bu numara rastgele üretilmiş olsa ve asıl bilgiyi içermese bile, RFID etiketin takip edilmesi mümkündür. Bu problem etiketin kişi ile ilgili bilgi taşıması durumunda çok daha büyük bir problem haline dönüşür [14].

Bazı RFID etiketler boyut olarak çok küçüktür ve bu etiketler giysilere, ayakkabılara, anahtarlıklara ve birçok yere yerleştirilebilirler. Herhangi biri bu etiketten yararlanıp kişinin nerede alışveriş yaptığını, nerde yaşadığını hatta hangi hastalık için hangi ilacı kullandığını dahi öğrenebilir. Bu gibi durumlarda kişinin bireysel hakları zarar görür [1].

4.1.2. Takip Edilebilirlik

RFID sistemlerinin kolay takip edilebilir olması diğer bir güvenlik unsuru olan takip edilebilirlik konusunu gündeme getirmiştir. RFID sistemlerinin kişileri takip etmekte kullanılması birçok kesim tarafından tepki ile karşılanmasına rağmen Amerika'da RFID öğrenci kartları uygulamaya geçilmiştir. Bu uygulama ile beraber öğrencilerin yerleri anlık takip edilmeye başlanmıştır. Bu kullanılan RFID öğrenci kartları sadece

pasif çipler gibi okuyucu tarafından okunduğu zaman veri göndermiyor, aynı zamanda içerisinde bulunan pil sayesinde dışarıya sabit bir sinyal yayınlayarak öğrencilerin konumunun takip edilmesini sağlıyor. Sistemin kullanım amacı öğrencilerin yerlerinin takip edilerek, derslere katılan öğrencilerin ve eğitimin veriminin arttırılması ama öğrencilerin takip edilmeleri kişilik hakları açısından endişe verici bir durum olarak gözüküyor [15].

Şekil 3.10 : Öğrenci Kartlarına Uygulanan RFID Etiket.

RFID sistemler ile takip hayatımızın birçok alanında yer almaktadır. Bunlara bir diğer örnek ise "Lucile Packard Çocuk Hastanesi"nde (Lucile Packard Children's Hospital, LPCH) kullanılmaktadır. Geleneksel olarak bu hastanede yeni doğan çocuklara anne ile aynı numarayı taşıyan bir bant yerleştirilerek çocukların karışması engelleniyordu. Hastane güvenliğin arttırması için RFID etiket sistemine 2001 yılında geçiş yaptı. Bu yeni sistem ile yeni doğan bebeğin ayak bileğine aktif RFID etiket yerleştiriliyor. Bu aktif RFID etiketlerin hepsi kendine özgü bir numaraya sahip ve bu sistemde anne ve bebeğin ismi ile beraber kayıt ediliyor. Bu etiket 433 MHz de çalışırken sadece 1.3x1.5x0.6 inç boyutuna sahip, bu özelliğin yanı sıra etiket çıkarılmaya kalktığı zaman gerekli görevli kişiler için uyarı sistemi çalışıyor. RFID etiket düzenli olarak RF sinyalleri göndererek eğer RF sinyalleri kesilmeye çalışılırsa yine uyarı sistemini harekete geçiriyor ve bu sayede bebeğin gerekli izinleri almadan hastaneden ayrılması engellenmiş oluyor [16].

4.2.RFID Saldırı Yöntemleri

RFID sistemlerinin yüksek güvenlik gerektiren uygulamalarda kullanımı artmaktadır. Bunlara örnek olarak erişim sistemleri, ödeme sistemleri ve bilet düzen sistemleri verilebilir. RFID sistemlerin bu gibi önemli uygulamalarda kullanılmasından dolayı RFID sistemin olası ataklara karşı güvenilir olması gerekmektedir. Aksi takdirde insanlar RFID sistemi yanıltıp erişim izni olmayan yerlere giriş yapabilir ve ödemedikleri hizmetleri alabilirler [17]. RFID sistemine yapılacak olası atak sistemleri farklı şekillerde yapılabilir. Bunlar başlıca etikete yapılan saldırılar ve RF ara yüzüne yapılan saldırılar diye sınıflandırılabilir.

4.2.1. Etikete Uygulanacak Saldırılar

4.2.1.1. Etiketlerin Kalıcı Olarak Devre Dışı Bırakılması

RFID etiketler yok edilebilir veya çalışmasına zarar verilebilir, bu tip durumlar etiketin kalıcı olarak devre dışı bırakılmasına yol açar.

Etiketlerin çıkarılması ve değiştirilmesi bu kalıcı olarak devre dışı bırakma türlerinden biridir. RFID etiketler fiziksel olarak zayıf bir güvenlik sistemine sahiptirler. Nesnenin içine gömülmemiş olan etiketler kolaylıkla çıkarılabilir ve başka bir nesneye yerleştirilebilir. Bu olaya en basit örneklerden biri fiyatların değiştirilmesi olarak verilebilir. Bu hırsızlık yöntemi ile ucuz olan nesne ile pahalı olan nesnenin etiketi değiştirilir ve bunun sonucunda aynı nesne daha az para verilerek alınmış olunur. Etiket değiştirildiği için RFID etiket takip edilemez ve değiştirildiği kolay anlaşılamaz. Bu kolaylıkla yapılabilecek önemli bir teknik bilgi gerektirmeyen bir güvenlik problemidir ama bu problem ile çok fazla karşılaşılmamaktadır.

İkinci kalıcı olarak devre dışı bırakma yöntemi olarak etikete hasar verilmesi örnek gösterilebilir. Bu yöntem de etiketlerin çıkarılması ile benzer özellik gösterir. RFID etiketlerin zayıf fiziksel güvenliğe sahip olması, bu etiketlerin fiziksel olarak kolay bir şekilde hasar alabilmesine neden olmaktadır. RFID etiketine insanları rahatsız etmek, RFID sisteminin çalışmasını engellemek gibi sebepler ile zarar verilebilir. Bu basınç, çekme kimyasal madde uygulama, görünebilen RFID anteni çıkarma gibi şekillerde yapılabilir. Bunu sonucunda nesneyi almak isteyen kişi RFID etikete zarar verdiği için kontrol noktalarından ve RFID okuyucuların bulunduğu noktalardan geçerek ürünü dışarıya çıkarabilir. Bunun yanı sıra RFID etiketler olumsuz çevre

şartlarından da etkilenebilirler. Yüksek ve düşük sıcaklık gibi sebepler RFID etiketin bozulmasına yol açabilir. İlave olarak aktif etiketler kendi pillerine sahiptirler ve bu pillerin çıkarılması veya zamanla bitmesi etiketlerin çalışmaz hale gelmesine neden olabilir. Bu durum pasif etiketler gerekli gücü RFID okuyucudan aldıkları için onlara geçerli değildir. Son etki olarak da bu tip etiketler elektrostatik yüklenmeye karşı aşırı duyarlıdırlar ve ani şekilde uygulanacak bir enerji yüzünden kalıcı olarak kullanım dışı kalabilirler [17].

4.2.1.2. Etiketlerin Geçici Olarak Devre Dışı Bırakılması

RFID etiketler kalıcı olarak devre dışı tehdidini atlatmış olsa bile bu etiketlerin geçici olarak devre dışı bırakılma durumu vardır. Faraday kafesi kullanarak elektromanyetik dalgalara karşı koruma sağlanabilir ve RFID okuyucu olan yerden bu şekilde geçici şekilde etiketi devre dışı bırakarak geçilebilir. RFID etiketler kasıtlı olmadan çevresel şart nedeni ve radyo dalgaları nedeniyle geçici olarak devre dışı kalabilir. Bunun dışında pasif olarak bulunan sinyali bozan etmenler de ortaya çıkabilir, çevre şartlarında sinyali engelleyecek gürültü seviyeleri, gürültü üreten elektronik kaynaklar ve çeşitli metaller radyo frekanslarının sapmasına, kesin ve verimli iletişimin sağlanmasını engelleyebilir. Bu pasif bozucu etkenler bu sisteme saldırmak istenen kişi tarafından da aynı şekilde kullanabilir. RFID etiketin sinyalini bozan elektromanyetik alan veya etiketin karşı verdiği tepki sinyalin geçici olarak engellenmesini sağlayabilir [17].

4.2.1.3. Etiketlerin Kopyalanması

RFID etiketler elektromanyetik alana girdikleri zaman herhangi bir doğrulama yapmadan tepki verirler. Bu durum saldırmak isteyen kişiler tarafından kullanılabilir. Uygun bir okuyucu tasarlandığında etiketin okuyucuya tepkisi dinlenir ve veri kaydedilir. Daha sonra elde edilen bilgi başka bir etiket üzerine gömülerek asıl etiket ile yerleri değiştirilip okuyucu kandırılabilir. Bu sayede kopyalanan etiket eğer aynı veriyi gönderebilir ise kopyalanan etiket ile gerçek etiket arasındaki fark okuyucu tarafından algılanamaz. Bunu engellemek için ulaşılabilir hafızaya sahip olan etiketler kopyalamaya karşı doğrulama protokolüne sahiptirler ve anahtarlama şifre koyma ve doğrulama sayesinde bu kopyalama durumu engellenmeye çalışılır [1] [17].

4.2.2. RF Ara Yüzüne Saldırılar

Haberleşme sırasında veri etiket ve okuyucu arasında hava aracılığı ile iletilir ve bu bağlantı çeşitli saldırı çeşitlerine açıktır. Bu saldırı çeşitleri dört ana başlık altında incelenebilir.

4.2.2.1. Dinleme (Eavesdropping)

RFID haberleşme sisteminin kablosuz haberleşme şeklinde sağlanması, bu haberleşmenin dinlenmesinin en ciddi ve yaygın tehlike haline getirmiştir. Bu hattın dinlenmesi yetkisi olmayan kişisel bir anten aracılığı ile RFID etiket ve okuyucu arasındaki iletişimin kayıt edilmesi ile yapılır. Bu tip atak iki yönde de gerçekleştirilebilir. Hem etiket ve okuyucu arasındaki iletilen sinyallerin dinlenmesi, hem de tersine okuyucu ile etiket arasındaki sinyallerin dinlenmesi şeklinde uygulanabilir ama okuyucu sisteminin çok daha güçlü bir şekilde bilgi aktarması okuyucudan çıkan bilginin daha rahat bir şekilde daha uzak yerlerden ve daha geniş açılardan dinlenebilmesine olanak sağlar. Daha sonra bu yöntem ile elde edilen bilgi daha sonra bahsedilecek olan farklı atak şekillerinde kullanılabilir [18].

4.2.2.2. Yayını Bozma (Jamming)

Çeşitli olumsuz şartlar altında pasif olarak yayının kendiliğinden kesilebileceği gibi, bu yayını kesmeye sebep olacak etki sisteme saldırmak isteyen kişi tarafından da kullanılabilir [18]. Bu yayını bozan cihazlar belirli bir frekans bandında sistemin iletişimini kesmek için gürültü üretirler, bu çeşitli yollarla yapılabilir yakın mesafeden okuyucu ve etiket arasına girilip bunların haberleşmesi engellenebilir ya da uzak bir mesafeden daha güçlü bir etki uygulayarak yayın bozulabilir.

Yayını bozma teknikleri yasalar tarafından engellenmiştir ve bu bozucu sinyallerin kaynağı kolaylıkla tespit edilebilir [1].

4.2.2.3. Servisin Engellenmesi (Denial of Service)

RFID etiketlerin normal çalışma koşullarını herhangi bir gerekli durum altında engelleyici etiketler bulunabilir. Bu etiketlere sistemi kilitleyici etiketler veya RFID koruyucuları denebilir. Bu etiketler RFID iletişiminin gizliliğini korumak için kullanılabileceği gibi kasıtlı olarak sistemin kilitlenmesini sağlamak amacıyla da kullanılabilir. Sisteme çok sayıda veri gönderen bu etiketler okuyucu tarafından sistemde çok fazla etiket olduğu varsayımı oluşturabilir ve bu çok sayıda bitler içeren veri okuyucunun kilitlenmesine sebep olabilir ve böylelikle servis engellenmiş olur [18].

4.2.2.4. Yeniden Oynatma Saldırısı

RFID etiketler güvenliklerini sağlamak için genellikle gizli ve kimliklerini eşleştiren bir cevap oluştururlar ama bu yöntemin sıklıkla karşılaşılan problemi yeniden oynatma saldırısıdır. Yeniden oynatma saldırısı yönteminde etiketin okuyucuya karşı oluşturduğu şifrelenmiş ve gizli bilgi kaydedilir ve bu kayıtlı bilgiden yararlanarak okuyucuya sanki gerçek gizli bilgi içeren etiket varmış izlenimi yaratılır. Bu yöntemin kullanımının tipik örneği sınırlandırılmış ve yetkisi olmayan kişilerin girmesini engellemek için kurulmuş olan RFID okuyucu içeren kapı sistemleridir. Bu kapı sistemlerinde gerçek etiketin yani kartın gönderdiği sinyal kopyalanır ve tekrar oynatılırsa okuyucu sistem gerçek kart varmış gibi kapı açılmasına yetki verecek ve güvenlik kırılmış olacaktır [18].

4.2.2.5. Trafik Analizi Saldırısı

RFID haberleşmesi trafik analizi saldırısına da uğrayabilir. Bu saldırı tipinde dinleme saldırısı kullanarak elde edilen mesajlar içerisinden gerekli bilgiler elde edilir. Bu bilgiler şifreleme ve doğrulama teknikleri içerse bile hala trafik analizi saldırısına uğrayabilirler. Bu saldırı tipinde ne kadar fazla bilgi elde edilebilirse iletişimin nasıl sağlandığı o kadar kolay anlaşılabilir [18].

4.2.2.6. Şifrelemeye Saldırı

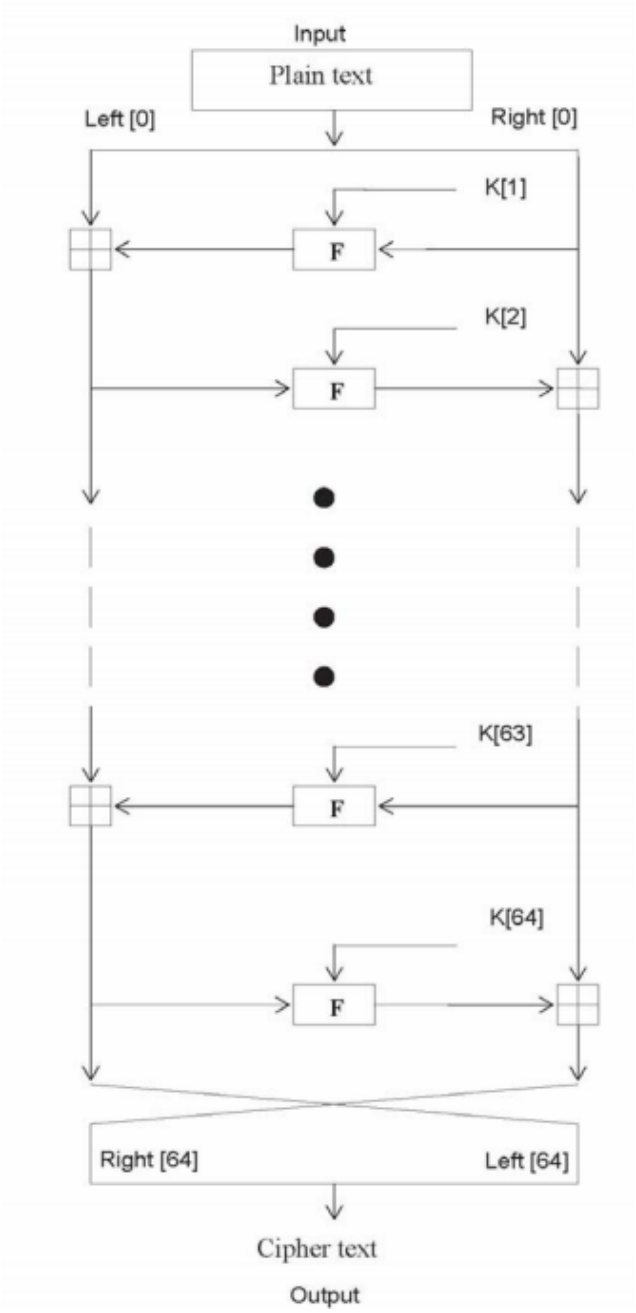
RFID etiket içerisinde önemli bilgiler saklanırsa bu bilgiler ne kadar şifreli olsa bile şifrelerin kırılma ihtimali vardır. Çeşitli şifre kırma algoritmaları ile RFID etiketin şifreleme tekniği kırılması denenebilir [18].

5. GERÇEKLENECEK RFID PROTOKOLÜ

5.1. TEA Algoritması

Şifreleme iletilecek mesajın güvenliğini sağlayan yöntemdir. TEA (Tiny Encryption Algorithm) Wheeler ve Needham tarafından 1994 yılında şifreleme için tasarlanmış bir algoritmadır [19]. TEA algoritması yüksek performans gerektiren gömülü sistemlerde kullanılması açısından uygundur. TEA kolay gerçeklenebilmesi, hızlı olması, düşük enerji tüketimi, düşük masraflı ve güvenli olması sebebi ile tercih edilmektedir [20].

TEA algoritması Feistel türü şifrelemedir ve karışık matematiksel gruplardan yararlanarak işlemleri gerçekleştirir. Çiftli kaydırma yöntemi kullanarak anahtar ve verinin tüm bitlerini sürekli olarak karıştırmaktadır. Anahtar yerleşim algoritması basittir. 128 bitlik anahtar K olsun bu K 4 tane 32 bitlik bloğa ayrılarak işleme sokulur. Bu bloklar K = (K[0], K[1], K[2], K[3]) şeklindedir. TEA algoritması ayrımsal şifre analizine (Differential Cryptanalysis) oldukça dirençli gözükmektedir ve çalışma alanındaki zaman performansı etkileyicidir [19].

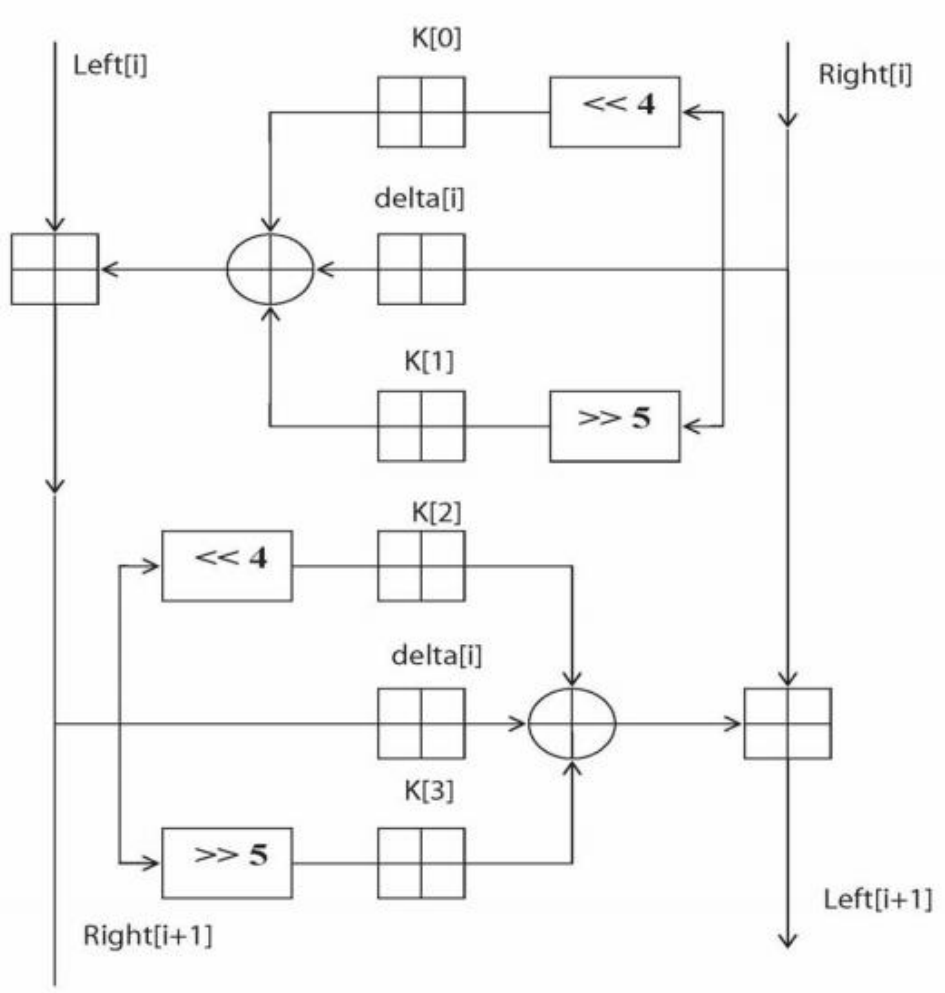


Şekil 5.1 : TEA Şifreleme Yapısı [19].

Şekil 5.1 TEA şifreleme rutinini göstermektedir. Şifrelemenin girişleri "Plain Text" bloğu ile gösterilmiştir. Burada K anahtardır. Burada kullanılan anahtarlar her aşamada farklılık göstermektedir. Bu anahtarlar oluşturulurken "delta" sabitinden yararlanılır. Bu sabit, altın orandan üretilmiştir ve bu oran sayesinden alt anahtarların hepsi birbirinden farklı olduğu ve bunun kesin değeri kriptografik öneme sahip değildir. Delta sabiti denklem 5.1'deki gibi hesaplanmaktadır [19].

$$\text{delta} = (\sqrt{5} - 1)*2^{31} = 9E3779B9_h \qquad (5.1)$$

Şekil 5.1'deki yapı daha detaylı incelenirse 64 adet Feistel döngüsünden oluşmaktadır. Bu döngülerin iç yapısı da şekil 5.2'de görülebilir. İki şekil karşılaştırıldığında anlaşılabileceği gibi şekil 5.2 iki adet Feistel döngüsü içermektedir ve her bir Feistel döngüsünün içerisinde toplama, ayrıcalıklı veya , mantıksal kaydırma işlemleri yapılmaktadır.

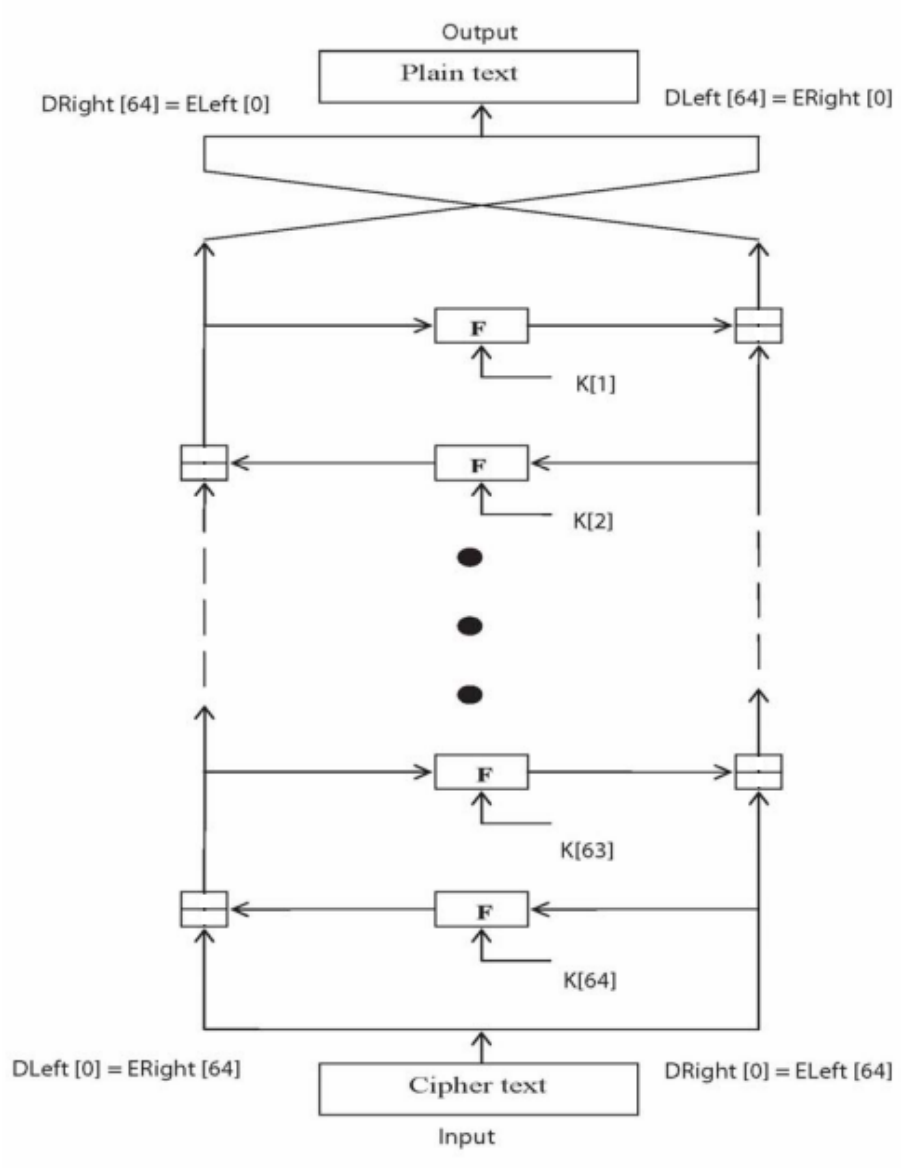


Şekil 5.2 : TEA Şifreleme Yapısı [19].

Şifreleme yapısı incelenirse, Right[i] ilk Feistel döngüsüne girer, bu şifresiz bilgi üç kola ayrılır. Bunlardan bir tanesinde 4 bit sola kaydırılarak K[0] anahtarıyla toplanır. Diğer kolda ise 5 bit sağa kaydırılarak K[1] anahtarıyla topla işlemine dahil olur. Üçüncü kolda da gelen bilgi yukarıda açıklanan delta ile toplanarak hepsi beraber XOR işlemine girerler. Bu döngünün çıkışı sol taraf ile bağlanmaktadır. Daha sonra bu solda elde edilen bilgi toplanarak 2. Feistel döngüsüne girer ve aynı işlemler diğer Feistel döngüsünde de devam eder. Bunun çıkışı da sağ tarafa giderek oradaki veri

ile toplanır. Bu işlem aynı şekilde birbirini 32 kez takip eder. Tüm işlemler tamamlandığında sağ ve sol tarafta şifrelenmiş bilgi elde edilir.

Şifre çözme işlemi de aslında şifreleme ile aynı işlemleri göstermektedir. Şifre çözme işleminde şifrelenmiş metin giriş olarak kullanılır ve bu sefer anahtarlar ters sıra ile birbirini takip eder. Şifre çözme algoritması da şekil 5.3'de yer almaktadır [19].

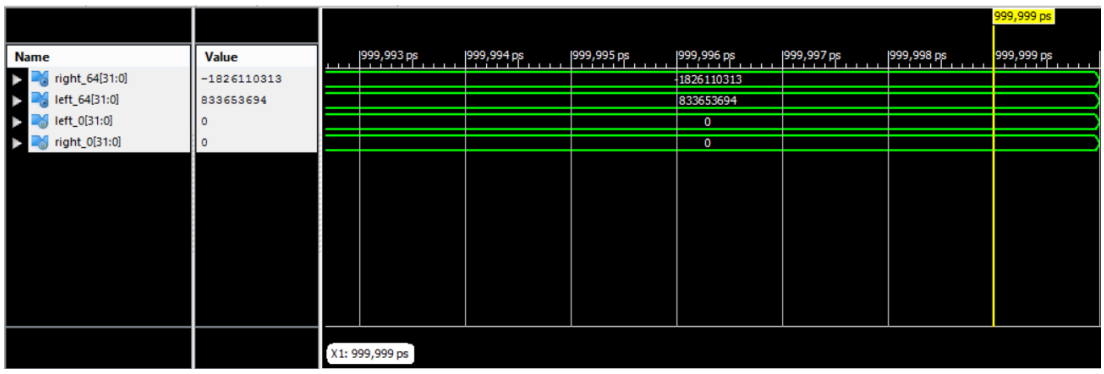


Şekil 5.3 : TEA Şifre Çözme Yapısı [19].

5.1.1. TEA Algoritmasının Test Edilmesi

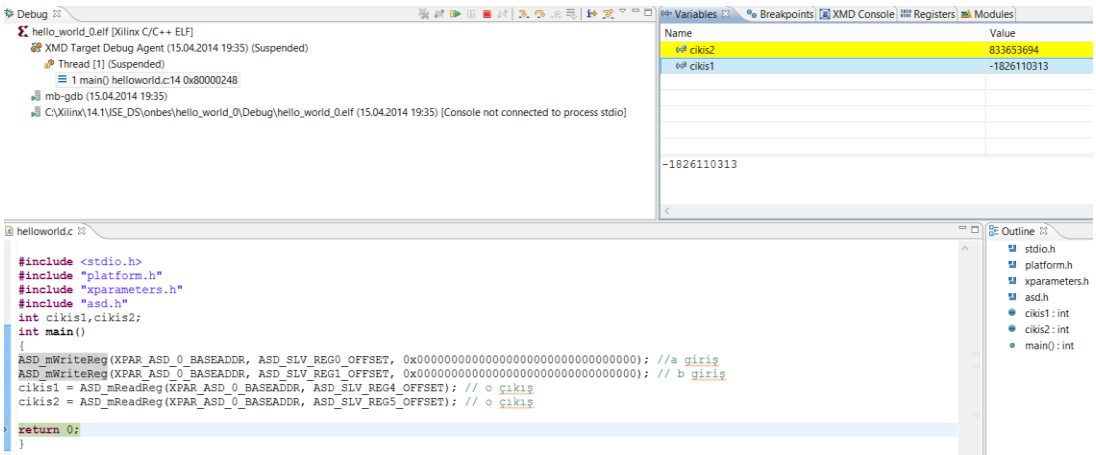
TEA algoritması 5.1'deki yapı kullanılarak gerçeklenmiş ve test edilmiştir.

Xilinx ISE ortamında kod yazıldıktan sonra test vektörleri uygulanmış ve davranışsal analiz sonucunda şekil 5.9'daki test sonucu elde edilmiştir. Şekilde sol ve sağdaki girişin değerlerinin sıfır verildiği TEA algoritmasının uygulanması sonucunda sağ ve sol değerin elde edildiği görülmektedir.



Şekil 5.4 : Xilinx ISE Tea Test.

Yazılan kod Xilinx ISE aracılığı ile test edildikten sonra FPGA üzerinde gerçeklenmesi yapılmıştır. TEA modülü FPGA üzerinde MicroBlaze ile kontrol edilecek şekilde donanım olarak eklenmiştir. SDK aşamasına geçildikten sonra program FPGA üzerine gömülmüştür. Xilinx'teki "debug" aracılığı ile şekil 5.10'da sol altta gözüken kod adım adım koşturulmuş, "cikis1" ve "cikis2" isimleri verilen çıkış verileri gözlemlenmiş, elde edilen veriler ışığında Xilinx ISE sonucu ile Xilinx SDK sonucu olması gereken şekilde aynı değerler olarak elde edilmiştir.



Şekil 5.5 : Xilinx SDK Tea Test.

5.2. Rastgele Sayı Üreteci

Doğrulama mekanizmasının sağlanması için ve okuyucu etiketin kimliği tanımlama yapabilmesi için rastgele sayı üreterek etikete göndermesi gerekmektedir. Bu işlemi gerçekleştirmek için rastgele sayı üretici donanımı tasarlanmıştır. Kullanılan rastgele sayı üretecinin saat, sıfırlama ve tetik girişi bulunmaktadır. Çıkış olarak ta işlemin tamamlandığını belirten hazır, k ve rastgele oluşturulmuş sayı elde edilir. Bu elde edilen rastgele sayı 64 bitten oluşmaktadır. Rastgele sayı kullanılırken hafızada değer tutucular 32 bitlik olduğundan dolayı rastgele sayı iki parçaya ayrılmış, iki ayrı rastgele sayı olarak değerlendirilmiş ve etikete o şekilde gönderilmiştir. Etiketten şifreli olarak rastgele sayı okuyucu üzerinde şifresi çözülerek, gönderilen rastgele sayılar ile aynı sayıların gelip gelmediği tespit edilmiş ve bunun sonucunda etiketin kimlik doğrulama aşaması tamamlanmıştır.

6. OKUYUCU VE TRANSPONDER TASARIMI

6.1. RFM22B Alıcı ve Verici Modülü

Sistemde RF haberleşmenin sağlanması için HOPE Microelectronic şirketi tarafından üretilen RFM22B isimli modül kullanılacaktır. Bu modül 433/470/868/915 MHz frekans aralığında ISM bandında çalışmaktadır. -121 dBm duyarlılığa sahiptir ve çıkış güç seviyesi en yüksek değerde +20dBm'dir. Modülün diğer özellikleri ise düşük güç tüketimine sahip olması, veri aktarma oranının 0.123 ten 256 kbpsye kadar değer alabilmesidir. Boş bir alanda oldukça uzak mesafelere kadar iletişim sağlanabilmektedir.

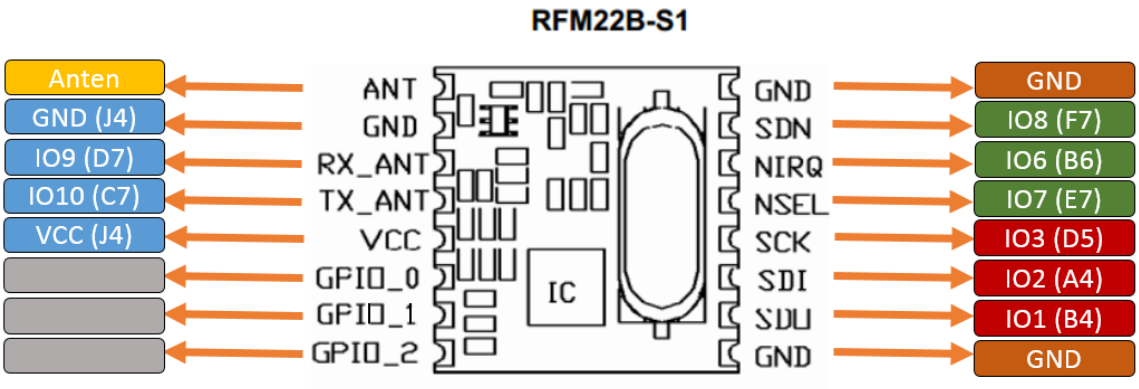
Özelliklerinden de anlaşılabileceği gibi bu modül farklı frekans aralıklarında çalışabilmektedir. Bu sahip olduğu özellikler sayesinde farklı uygulama alanlarında kullanılabilmektedir. Uzaktan kumanda sistemleri, ev güvenliği ve alarm sistemleri, telemetri, kullanıcı giriş kayıtlarının tutulması, ürün takip sistemi, lastik basıncı izlenmesi, kablosuz bilgisayar çevre birimleri, uzaktan anahtarsız giriş, ev otomasyonu, endüstriyel kontrol sistemleri, sensör bağlantıları, etiket ve okuyucu sistemleri gibi alanlarda kullanılabilmektedir [24].

Proje içerisinde etiket okuyucu sistemlerin haberleşmesinde bu alıcı verici modülünden yararlanılmıştır. Modül farklı özelliklere sahip olduğundan bunlar arasında seçim yapılmıştır. Kod yazılırken belirlenen değerlere göre veriler girilmiştir. Veri aktarım oranı 9.6kbps ve merkez frekansı 868 MHz olarak belirlenmiştir.

RFID sistemlerde çalışma frekansı uygulamanın amacına sistemin çalışacağı ortama ve çevre şartlarına göre değişmektedir.

Bitirme projesi kapsamında yapılacak olan uygulamada RFID sistemin haberleşmesinin uzak mesafelerde uygulanması amaçlanmıştır. Bu nedenle UHF frekans bandında bir frekans bandında haberleşme yapılmasına karar verilmiştir. UHF bandı 300 MHz frekansından başlayarak 3 GHz banına kadar uzanan geniş bir

bant aralığına sahiptir. Sistemin merkez frekansının belirlenmesinde UHF bandı üzerindeki RFID düzenlemeleri göz önüne alınmıştır. Dünya üzerinde farklı düzenlemeler ve hükümetler tarafından farklı kısıtlamalar getirilmiştir. Avrupa genelinde UHF RFID haberleşmesi için kullanılan aralık 865 ile 868 MHz frekansları arasındadır. Bu düzenlemelere uymak için merkez frekans 868 MHz seçilmiştir. Kullanılan RF modülün bağlantı şeması ve bitirme çalışmasında FPGA üzerinde bağlantıların yapıldığı yerlerin detaylı gösterimi şekil 6.1'de görülmektedir.



Şekil 6.1 : RFM22B FPGA Bağlantı Şeması.

Haberleşme sağlanırken FPGA üzerinde yer alan seri çevresel birim ara yüzü (Serial Peripheral Interface, SPI) kullanılmıştır.

RFM22B modülündeki bağlantılar:

Anten: Sarı ile gözüken kısım ile anten bağlantısı yapılmıştır.

GND ve VCC: Modülün toprak ve güç kaynağı bağlantılarını oluşturmaktadır.

RX_ANT: Antenin alıcı mı verici mi olduğunun saptanmasında kullanılmaktadır. RX_ANT=1 değerini alırsa anten RX modunda çalışmaktadır

TX_ANT: RX_ANT çalışma mantığının tam tersi şeklinde çalışmaktadır. TX durumunda çalışılmak isteniyorsa değeri 1 olmalıdır.

SDN: Kapatmak için kullanılan giriş pinidir. SDN=1 durumunda devre kendini kapatmakta ve kayıtlı veriler kaybolmaktadır.

NIRQ: Mikroişlemcinin kesme oluşturan çıkışıdır.

NSEL: Seri arayüz seçim girişidir. 4 hatlı seri veri yolu üzerinde seçim ve etkinleştirme için kullanılır.

SCK: Seri saat girişidir.

SDI: Seri veri girişidir. 0 ile Vcc V arasında sayısal giriş yapılır. 4 hatlı seri veri yolunda veri akışını sağlar.

SDO: 0 ile Vcc V arasında sayısal çıkış verir. İç kontrol için seri geri okuma fonksiyonu sağlar [24].

6.2. Haberleşme Protokolü

RFID sistemlerinde etiket ve okuyucu arasında güvenli bir doğrulama ve iletişimin sağlanması için standartlar doğrultusunda çeşitli yöntemler kullanılmaktadır. Bu proje kapsamında Martin Heldhofer tarafından 2004 yılında sunulan doğrulama protokolü kullanılacaktır. Veri tabloları başlangıç çerçeveleriyle başlayıp, bitiş çerçeveleri ile bitmektedir.

Start of Frame	Flags	0xA0	MfgCode	User ID	Random Number	CRC	End of Frame
	8 bit	8 bit	8 bit	64 bit	128 bit	16 bit	

Şekil 6.2 : Okuyucunun Gönderdiği Veri Tablosu [4].

Bayraklar (Flags): İletilen verinin ilk byte'ını oluştur. Veri oranı ve taşıyıcı frekans bilgisi gönderir.

0xA0: Yorum satırı olarak kullanılır. Beklenen komut ile ilgili bilgi verir.

Üretici Kodu (MfgCode): Üreticiye özgü komutlar burada yer alır. Kopyalama ve yanlış anlaşılmanın engellenmesi sağlanır.

Kullanıcı Kimliği (User ID): Kullanıcının kimliğini belirtir ve etiketin özgün verisidir.

Çevrimsel Hata Denetimi (Cyclic Redundancy Check, CRC): Hataların tespitinde kullanılır. İletilen veride bir değişiklik olup olmadığının kontrolünde kullanılır. Denetim seti olarak bir dizi kod gönderilir. Alıcı taraf iletilen veri ile aynı denetim işlemlerini gerçekleştirerek alınan veride hata olup olmadığını tespit eder. Elde edilen iki sonuç birbiri ile aynı değilse iletimde bir hata olduğu anlaşılır.

Start of Frame	Flags	User ID	Signed Data	CRC	End of Frame
	8 bit	64 bit	64 bit	16 bit	

Şekil 6.2 : Etiketin Gönderdiği Veri Tablosu [4].

Etiketin gönderdiği veri daha kısadır. Yorum kısmı ve üreticinin bilgilerini içermez ve gerekli bilgiyi iletmede kullanılır.

Doğrulama olarak sistemde 64 bitlik rastgele sayı etiket üzerine gönderilir. Alınan bu veri şifrelenir ve geri gönderilir. Okuyucu bu şifrelenmiş veriyi alır ve şifreyi çözer ve kendi gönderdiği veri ile karşılaştırır. Eğer gönderdiği veri ile şifresi çözülmüş veri aynı ise okuyucu ile etiket arasında doğrulama sağlanmış olur.

6.3. Kimliklendirme Protokolü

Kullanılan sistemde kimliğin doğruluğu iki yönlü kimlik sorma yanıt yapısı kullanılarak gerçekleştirilmiştir. Bu protokol Martin Feldhofer tarafından aşağıdaki şekildeki gibi ifade edilmiştir [6].

$$
\begin{aligned}
A \leftarrow B: &\quad r_B \\
A \rightarrow B: &\quad E_K(r_A, r_B) \\
A \leftarrow B: &\quad E_K(r_B, r_A)
\end{aligned}
$$

Şekil 6.3 : Kimliklendirme Protokolü [6].

Şekilde A ve B olmak üzere iki adet birbiri ile ilişki kuracak sistem bulunmaktadır. Çift taraflı kimliklendirme protokolü gereğince; A ve B ikisi de aynı özel anahtara sahiptir. B rastgele sayı üreterek A'ya gönderir. A bu sayıyı ikisinin ortak olarak bildiği şifreleme yöntemi ile şifreler ve B'ye geri gönderir. Bunun ile beraber kendisi

bir rastgele sayı üretir ve şifreleyerek bu bilgiyi de B'ye gönderir. B gelen şifreli mesajı çözer ve kendi gönderdiği sayının doğru gelip gelmediğini kontrol eder. Daha sonra çözülen veriyi tekrar şifreleyerek yerlerini değiştirir ve A'ya gönderir. Bu sayede A sonucu kanıtlar ve B'nin kimliğini tanımlamış olur. Gerçeklenen sistemde B olarak gözüken okuyucu sistem, A ise etiketi temsil etmektedir. Şifreleme tekniği olarakta tea algoritmasından yararlanılmıştır.

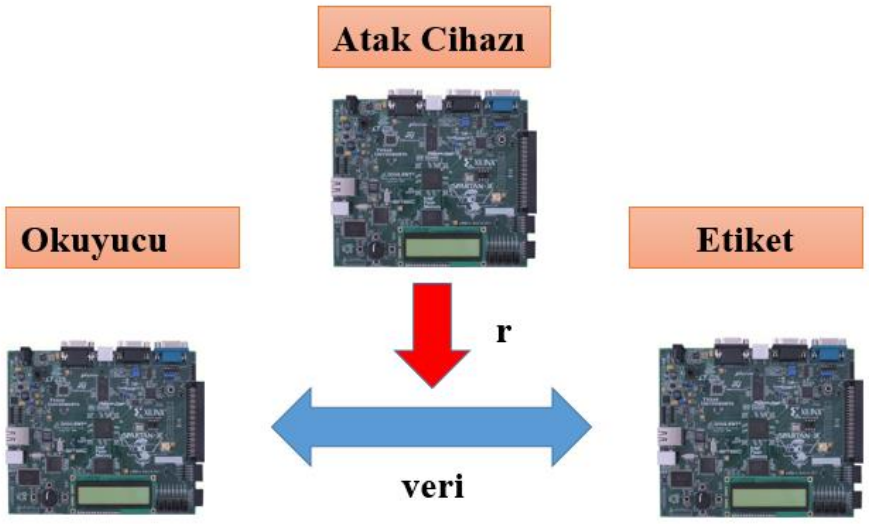
6.4. Yatay Fazlalık Denetimi (Longitudinal Redundancy Check, LRC)

Haberleşme sistemlerinde kullanılan denetim mekanizmalarından biridir. Her bir bit dizisinin paralel gruplar halinde işleme sokulması ile oluşturulur ve bunun için de gelen veri ayrı bloklar halinde ele alınmalıdır. Bu sistem sayesinde verinin doğru geldiği bir başka yoldan kontrol edilmiş olur. Yöntem temel olarak ayrılan bitlerin sürekli olarak birbirleri ile ayrıcalıklı veya işlemi uygulanmasından oluşmaktadır. Bu hesaplama sonucunda elde edilen veri ile LRC kontrolü gerçekleştirilmiş olur.

7. PROTOKOLÜN GERÇEKLENMESİNE SALDIRILAR

7.1. Servisin Engellenmesi Saldırısı

Sisteme RFID sistemlerinde güvenlik başlığının altında RF arayüzüne saldırılar kısmında anlatılan servisin engellenmesi saldırısı uygulanmıştır. Oluşturulan atak sistemi rastgele sayı üretmekte ve bu sayıları devamlı olarak sisteme vermektedir. Bu rastgele verilen sayılar okuyucu ve etiket arasındaki akan veri arasına karışarak sistemin çalışmasını engellemektedir. Şekil 7.2'de oluşturulan sistem yer almaktadır.

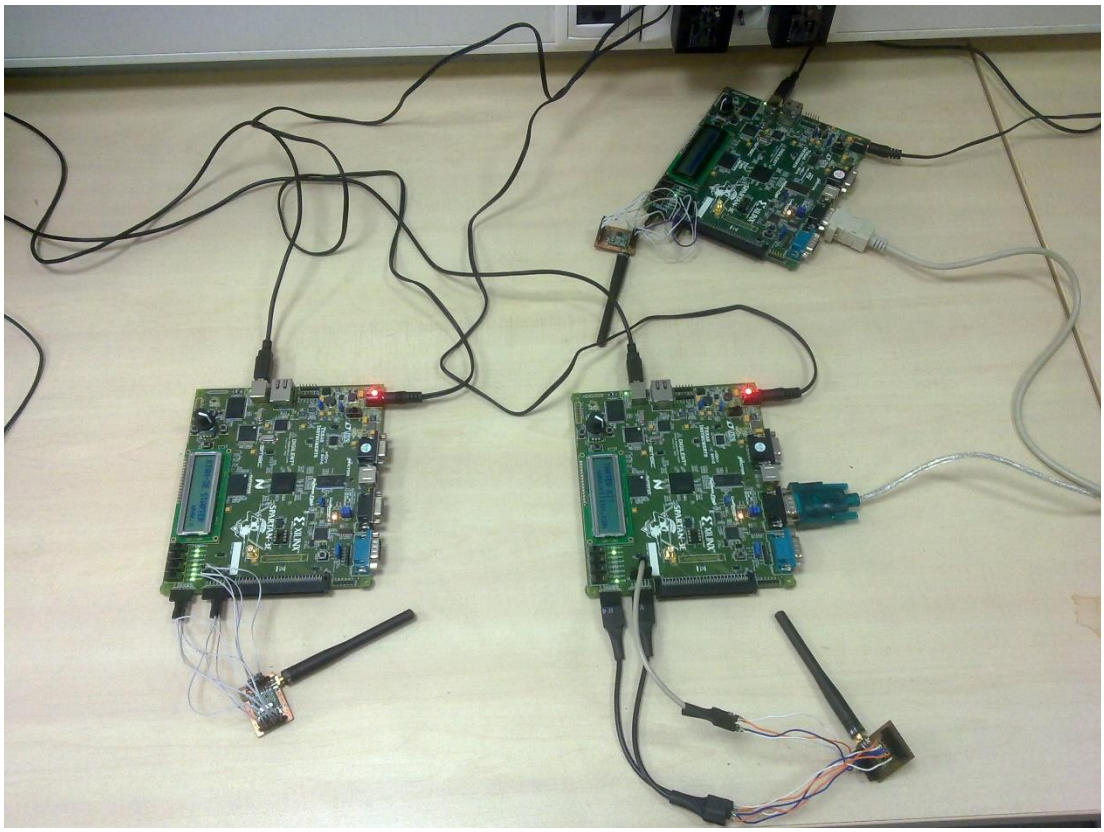


Şekil 7.1 : Servisin Engellenmesi Sistem Gösterimi.

Kullanılan okuyucu ve etiket sistemlerinde verilerin doğruluğunu kontrol etmek için yatay fazlalık denetimi yöntemi kullanılmaktadır. Ortama giren atak cihazı yayınladığı rastgele sayılar ile akan veri arasına kendi ürettiği rastgele sayıları karıştırarak okuyucu ve etiketin LRC hatası vermesine sebep olmaktadır. Bu oluşan hatadan dolayı etiket ve sistem kimlik doğrulama sıkıntısı ile karşılaşmaktadır.

7.2. Yeniden Oynatma Saldırısı

Sisteme RFID sistemlerinde güvenlik başlığının altında RF arayüzüne saldırılar kısmında anlatılan yeniden oynatma saldırısı uygulanmıştır. Kullanılan sistemde etiket ile okuyucu arasında var olan haberleşme dinlenip, alınan veriler kaydedilmiştir. Tasarlanan sistemde okuyucunun gönderdiği rastgele üretilen sayıya karşılık, etiket bu gelen rastgele sayıyı şifrelemekte ve okuyucuya geri göndermektedir. Kullanılan üçüncü FPGA, yani atak cihazı yardımıyla her üretilen rastgele sayıya karşılık şifrelenmiş halinin hafızada saklanması ve okuyucu daha önceden kayıt edilmiş rastgele sayılardan gönderdiği zaman, ona karşılık yine kaydedilmiş olan şifrelenmiş halini gönderip atak cihazının, etiket yerine geçmesi planlanmıştır.



Şekil 7.2 : Gerçeklenen Sistem.

Sistemde etiket ve okuyucu tarafında kullanılan rastgele sayı üreteci, rastgelelik oranı yüksek bir üreteç olduğu için $2^{bit\ sayisi}$ kadar farklı rastgele sayı üretilecektir. 64 bitlik rastgele sayı üreteci kullanıldığı için sistem 2^{64} adet rastgele sayı üretecektir. Atak cihazının tüm bu rastgele sayıları ve bunlara karşı vereceği cevabı kaydetmesi

gerekmektedir. Sistemde bu miktarda veri kaydedilemeyeceği için sistemin test aşaması belirli rastgele sayıların kaydedilmesi ve bunlara karşı şifrelerin kaydedilmesi şeklinde gerçekleştirilmiştir. Bunun sonucunda okuyucudan gelen rastgele sayı ile bu rastgele sayıya karşı etiket tarafından üretilen cevap kaydedilmiştir. Okuyucu aynı rastgele sayıyı gönderdiğinde ortamda etiket olmasa bile atak cihazı etiket yerine geçerek okuyucunun etiket ile haberleştiğini varsaymasını sağlamıştır.

7.3. Saldırılara Karşı Alınabilecek Tedbirler

Yaratılan ataklara karşı RFID sistemlerde güvenliğin geliştirilmesi açısından çeşitli tedbirlerden yararlanılmaktadır.

7.3.1. Zaman Bilgisi Kullanarak Atakların Engellenmesi

Zaman bilgisinin gönderilen veriye eklenmesi atağın engellenmesinde kullanılan en kolay çözümlerden biridir. Bu teknikte okuyucu zaman bilgisini gönderilen veriye ekleyerek gönderir. Daha sonra etiket gelen zaman bilgisini değiştirmeden gönderilen cevap çerçevesine ilave eder. Okuyucu gelen veri çerçevesindeki zaman bilgisi ile zaman değişkenini karşılaştırır. En uzun iletişim süresini hesaplayarak gelen zaman verisi ile bu iletişim süresini kullanarak kimlik doğrulama işlemini gerçekleştirir. Burada kritik nokta aradaki geçen zamanın en uzun iletişim süresinden kısa olması gerekliliğidir. Zaman bilgisinin eklenmesi güvenliği büyük ölçüde arttırmaktadır ama oluşturulan sistemin gerekli hesaplamaları yapacak güce sahip olması gerekmektedir.

7.3.2. RF Yön Seçiciliği Kullanarak Atakların Engellenmesi

Okuyucu sistemde RF alan koruması kullanılarak ataklar engellenebilir. Bu teknikte temel olarak radyo sinyallerinin algılanabileceği yönler kısıtlanır. Genel olarak radyo dalgalarını incelersek, bu tip dalgalar anten üzerinden her yöne yayılma özelliğine sahiptirler. Saldırmak isteyen taraf bu geniş bir alana yayılmış radyo dalgalarını çok uzun mesafeden dinleyerek aktarılan verilere ulaşabilir. Bunu engellemek için RF dalgalarının yayılacakları yön etiket ve okuyucu yapısında belirlenerek iletilen dalgaların yayılma yönü belirlenip, iletilen dalgaların çok yönlü yayılması engellenebilir. Bu sayede çeşitli ataklara karşı sistem güvenliği sağlanmış olur.

7.3.3. Rastgele Üretilen Sayı Kullanarak Atakların Engellenmesi

Sistemler arasında doğrulamak için kullanılan rastgele sayıların ne kadar rastgele üretildiği ve kaç bit olduğu önemli bir faktörü oluşturmaktadır. Eğer üretilen sayı tamamen rastgele üretilebiliyorsa atak cihazının üretilen rastgele sayı kadar gelen veri ve bunlara karşı cevap kaydetmek zorunda kalacaktır. Atak cihazının daha fazla veri kaydetmesi ve buna hızlı bir şekilde cevap vermesi daha da zorlaşacak ve güvenli bir haberleşme sistem oluşturulmuş olacaktır.

7.3.4. Sinyalin Gücünden Yararlanarak Atakların Engellenmesi

Gelen sinyalin gücünün hesabından yararlanarak atakların engellenmesi RF sistemine yapılan atakların engellenmesinde kullanılan bir diğer yöntemdir. Bu yöntem ile sisteme girmeye çalışan diğer izini olmayan okuyucu ve etiketler tespit edilerek sistemin haberleşmesinin bozulması engellenir. Bu yöntem ile alınan sinyalin gücünün hesaplanması güvenlik açısından önemli bir yarar sağlarken, bu sistemin kullanılması tasarımın maliyetini arttırmaktadır.

8. SONUÇLAR VE TARTIŞMA

Radyo frekans uygulamaları hayatımızın her yerinde karşılaşacağımız ve gün geçtikçe sayısı artan bir uygulamadır. Bu artan uygulama alanı ve kullanımı sistemin güvenliği ve gizliliği ilgili büyük bir endişe uyandırmaktadır. Çok farklı alanlarda kullanılan bu RFID sistemlerin güvenliğini arttırmak için çeşitli güvenlik önlemleri alınmakta ve güvenlik sistemleri geliştirilmektedir. Bu güvenlik önlemlerinin başında şifreleme ve farklı protokoller kullanımı gelmektedir. Son zamanlarda RFID sistemleri için güçlü şifreleme algoritmaları geliştirilmiştir. Bununla beraber yüksek sayıda yeni protokol geliştirilmiş ve güvenliğin artması için geliştirilmeye devam etmektedir. Buna rağmen RFID sistemlerin güvenliklerinin arttırılması için bu alanda daha fazla çalışılması gerekmektedir.

Yapılan bitirme çalışmasında güvenli bir RFID sistemi tasarlanması ve bu sisteme çeşitli ataklarda bulunarak güvenliğinin test edilmesi amaçlanmıştır. Bu amaç ile üç adet Spartan3E Starter FPGA kartı kullanılarak donanım ve yazılım gerçeklemesi yapılmıştır. Sistemin kontrolü için MicroBlaze işlemcisinden yararlanılmıştır. Sistemde şifreleme açısından yer ve hız bakımından verimli bir sistem olan TEA şifreleme algoritması kullanılmıştır. Sistemin güvenliğinin arttırılması açısından oluşturulan sistemlere rastgele sayı üreteçleri eklenmiştir. Sistem kullanılan RFM22B isimli alıcı ve verici RF modül sayesinde kablosuz olarak haberleşmektedir. Haberleşme protokolü olarak çift taraflı kimlik doğrulama protokolü okuyucu ve etiket üzerinde kullanılmaktadır. Bu protokolde okuyucu 64 bitlik rastgele sayıyı şifrelemeden etikete göndermektedir. Alınan veri şifrelenerek geri gönderilir, aynı zamanda etiket de rastgele sayı üretip şifreleme işlemini tamamlayıp okuyucuya gönderir. Okuyucu bu şifrelenmiş veriyi alır ve şifresini çözer. Çözülen şifrelenmiş sayı ile kendi ürettiği rastgele sayının aynı olup olmadığını kontrol eder ve gelen verilerin yerini değiştirerek etikete geri gönderir. Etiket gelen verinin şifresini çözer ve kendi gönderdiği rastgele sayının doğru olduğundan emin olur, böylelikle çift taraflı doğrulama protokolü gerçeklenmiştir.

Atak çalışmaları için üçüncü bir Spartan3E Starter Board kullanılmıştır. İlk olarak servisin engellenmesi saldırısı yapılmıştır. Atak cihazında sürekli olarak rastgele sayı üretilip RF modül üzerinden yayın yapılmıştır. Bu gönderilen rastgele sayı, aralarında haberleşen okuyucu ve etiket verileri arasına karışarak okuyucu ve etiketin kimlik doğrulama yapmasını engellemektedir.

İkinci olarak atak cihazında yeniden oynatma saldırısı yapılmıştır. Etiket ve okuyucu arasında gidip gelen veri kaydedilmiş. Okuyucunun gönderdiği veriye karşılık, etiketin hangi veriyi ürettiği tespit edilip etiketin yerine geçilmeye çalışılmıştır. Okuyucunun ürettiği rastgele sayı miktarı çok fazla olduğu için sistem sadece belirli rastgele sayılar geldiğinde çalışacak şekilde uygulanmıştır. Çalışmanın sonunda yapılan bu saldırılara karşı alınabilecek tedbirler açıklanmıştır.

Güvenli bir RFID sistemi tasarlanmış ve çeşitli ataklar denenerek sistem güvenlik açısından test edilmiştir. Gelecek çalışmalar için yeni saldırı teknikleri geliştirilebilir ve bu saldırılara karşı tedbirler alınarak oluşturulan güvenli RFID sisteminin güvenliği daha da arttırılabilir.

KAYNAKLAR

[1] **Ozen, O.E., Ors, S.B., Yagci, H.B**., 2013. Design and implementation of a secure RFID system on FPGA, *Signal Processing and Communications Applications Conference (SIU), 2013 21st* , vol., no., pp.1,4.

[2] **Dobkin, D.M.,** 2006. The RF in RFID, Elsevier Inc.

[3] **Feldhofer, M.,** 2004. An authentication protocol in a security layer for RFID smart tags, Electrotechnical Conference, 2004. MELECON 2004. Proceedings of the 12th IEEE Mediterranean, **2**, pp. 759- 762.

[4] **Ozen, O.E., Ors, S.B., Yagci, H.B., 2013.** Design and implementation of a secure RFID system on FPGA.

[5] **Landt, J.,** 2005. The history of RFID, *Potentials, IEEE* , vol.24, no.4, pp.8,11, Oct.-Nov.

[6] **Feldhofer, M., Dominikus, S., Wolkerstorfer, J.**, 2004. Strong Authentication for RFID Systems Using the AES Algorithm, *Cryptographic Hardware and Embedded Systems - CHES 2004*, pp. 357-370, 6th International Workshop Cambridge, MA, USA.

[7] **ISO/IEC 18000-3,** 2003. Information Technology AIDC Techniques - RFID for Item Management, International Organization for Standardization.

[8] **Dong-Liang Wu; Ng, W.W.Y.; Yeung, D.S.; Hai-Lan Ding**, 2009. A brief survey on current RFID applications, *Machine Learning and Cybernetics, 2009 International Conference on* , vol.4, no., pp.2330,2335.

[9] **TOBB GS1 Türkiye**, [Alıntı Tarihi: 10 Nisan 2014], http://gs1.tobb.org.tr/images/rfid_etiketi.JPG.

[10] **Kavas, A.,** 2007. Radyo Frekans Tanımlama Sistemleri, **430,** s. 74-80.

[11] **Chu, Pong P.**, 2008. FPGA Prototyping by VHDL Examples. Wiley-Interscience, New Jersay.

[12] **Xilinx,** 2006. Spartan-3E Starter Kit Board User Guide.

[13] **Xilinx**, 2007. MicroBlaze Processor Reference Guide.

[14] **Juels, A.,** 2006. RFID security and privacy: a research survey, *Selected Areas in Communications, IEEE Journal on* , vol.24, no.2, pp.381,394.

[15] **Christina DesMarais**, 2013. http://www.pcworld.com/article/2025170/radio-frequency-id-chip-case-ruling-favors-texas-school-district.html

[16] **Jonathan Collins,** [Alıntı Tarihi: 10 Nisan 2014], RFID Delivers Newborn Security, http://www.rfidjournal.com/articles/view?1372/2

[17] **Finkenzeller, K.** 2010. RFID Handbook, John Wiley & Sons, Ltd., 3. edition.

[18] **Mitrokotsa, A., R.M.R. and Tanenbaum, A.S**., 2008. Classification of RFID Attacks, Proceedings of the Second International Workshop on RFID Technology, pp.73–86.

[19] **Andem, V.R.,** 2003. A Cryptanalysis of the Tiny Encryption Algorithm, MSc. Thesis, The University of Alabama, ALABAMA.

[20] **Abdelhalim, M.B., Elhennawy, A., Ayyad, M.and El-Mahallawy, M.,** 2011. Implementation of a Modified Lightweight Cryptographic TEA Algorithm in RFID System, VI. International Conference on Internet Technology on Secured Transactions, Abu Dhabi, 11-14 December, pp. 509-513.

[21] **Xilinx,** 2007. Embedded System Tools Reference Manual.

[22] **Xilinx,** Software Development Kit Help Contents, [Alıntı Tarihi: 11 Mayıs 2014],http://www.xilinx.com/support/documentation/sw_manuals/xilinx12_2/SDK_Doc/index.html.

[23] **Xilinx,** 2011. EDK Concepts, Tools and Techniques.

[24] **Hope Microelectronics,** RFM22B/23B ISM TRANSCEIVER MODULE, data sheet

ÖZGEÇMİŞ

Adı Soyadı: Cumhur ERDİN

Doğum Yeri ve Tarihi: Edirne, 1991

Lise: Edirne Süleyman Demirel Fen Lisesi; 2005-2009

Lisans: İstanbul Teknik Üniversitesi, Elektronik Mühendisliği; 2009-2014