1. GİRİŞ

Giriş ve Çalışmanın Amacı:

Bu çalışmada RFID olarak bilinen özelliğe sahip olan sistemler incelenmiş ve bu sistemler içerisinde şifreleme yapmaya uygun özellikte olanları belirlenerek bunların uygun bir şifreleme algoritması kullanılarak şifrelenmesi işlemi gösterilmek istenmiştir.

RFID sistemlerinin günümüzde pek çok alanda birçok uygulamada kullanıldığı bilinen bir gerçektir. Bu uygulamalara örnek olarak kapı girişlerinde personel kartı okutma, mağaza çıkışlarında kurulan alarm sistemleri ve güncel bir örnek olarak da İstanbul'da Avrupa kıtasından Asya kıtasına geçerken köprüde kullanılan OGS ve KGS sistemleri gösterilebilir. Görüldüğü üzere bu sistemlerde karşılıklı bir bilgi aktarımı söz konusudur. Bu sebepten bu uygulamalar güvenlik açığına sahip olma tehdidiyle karşı karşıyadır. Bu güvenlik açığı ise 3. kişi olarak isimlendirilen istenmeyen kişilerin bu bilgi aktarımının arasına girmesi, bir başka deyişle bu bilgileri ele geçirmesi veya değiştirmesidir. Bu istenmeyen durumun önüne geçilebilmesi için RFID sistemlerinin içerdikleri bilgiyi sadece doğru kişilere aktarması istenmektedir. Bunu sağlamanın yolu ise bu sistemin alıcı ve verici olmak üzere iki tarafı arasında işleyen bir protokol oluşturmak ve bu protokol sadece önceden belirlenmiş doğru bir sonucu ortaya koyduğunda bilgi aktarımına izin vermektir. Bu çalışmada yapılmaya çalışılan iş ise, uygun bir şifreleme algoritması kullanarak bir protokolü gerçekleştirmek ve bu protokolün sonucunda beklenen bir sonuç oluşması durumunda bilgi aktarımını başlatmaktır. Bu sayede, ele alınan RFID sisteminin kendi içinde haberleşmesinin güvenli hale geldiği ortaya atılacak ve son bölümde, önceden belirlenen güvenlik hedeflerine uyup uymadığı belirlenerek bu sistemin gerçek bir sistem olarak uygulanabilip uygulanamayacağı tartışılacaktır.

2. RFID SİSTEMLERİNİN İNCELENMESİ

2.1. RFID Sistemlerinin Tanımı ve Sınırları

RFID kelimesi İngilizce "*Radio Frequency Identification* " kavramının baş harflerinin birleşmesinden meydana gelir. Türkçeye *"Radyo Frekansı ile Tanımlama"* olarak da çevrilebilecek olan bu sistemlerin en temel özelliği sistem içindeki birimlerin birbirleriyle radyo frekansları olarak tabir edilen bir frekans aralığında haberleşmesidir. RFID sistemleri 135 kHz uzun dalgadan 5,8 GHz mikrodalgaya kadar olmak üzere çok çeşitli değişik frekanslarda çalıştırılabilirler [1]. Bu geniş frekans aralığında uygulamaya bağlı olarak uygun bir frekans seçilerek sistemin alıcı ve verici tarafı aynı frekansa ayarlanarak hava aracılığıyla uzaktan haberleşmeleri sağlanır. Bu frekanslar seçilirken uygulamanın tipi önemli olacağı gibi, yerel hukuki düzenlemeler de sınırlayıcı olmaktadır. Muhtelif ülkelerde 125 kHz ile 13,56 MHz arasında kalan frekanslar büyük ölçüde Standard haline getirilmiştir [2]. Her ne kadar RFID uygulamaları kısa menzil uygulamaları olarak bilindiği için lisans alınmasını gerektirmese de yaptıkları yayının farklı radyo frekansı uygulamaları ile karışmaması için pek çok ülke RFID uygulamalarının kullanabileceği frekans aralığını belirgin hale getirmiştir. Şu durumda bir RFID uygulamasını sınırlayan en temel etkenin frekans seçimi olduğu gözükmektedir. Bu seçim hem RFID sistemi için bir sınırlayıcıdır hem de ona ismini vererek bir RF uygulaması haline getirmektedir.

RFID sistemleri için genel bir tanım yapmak gerekirse, RFID teknolojisi, radyo frekansı kullanarak nesneleri tanımlama ve haberleşerek veri aktarma yöntemidir. RFID sistemlerini sınırlayan ve diğer tanıma sistemlerinden ayırt edilmesini sağlayan özellikleri ise bilgi taşıyıcı olarak RF frekansında elektromanyetik dalgaları kullanmalarıdır. RFID sistemlerinin çoğunda istenen önemli bilgi aktarımı tek yönlüdür. Bilgiyi taşıyan ve istendiğinde karşı tarafa gönderen birime **etiket**, etiketi sorgulayıp bilgisini isteyen birime ise **okuyucu** denir. RFID etiketleri, ürün seri kodları gibi bilgileri saklayabilirler ve istendiğinde okuyucuya radyo frekansında

elektromanyetik dalga üstünde gönderebilirler. En basit RFID sistemi bu iki birimin karşılıklı haberleşmesi ile oluşturulur.

2.2. RFID Sistemlerine Alternatif Uygulamalar

RFID sistemlerini diğer otomatik tanımlama sistemlerinden ayırmanın bir diğer yolu da "öteki" otomatik tanıma sistemlerini daha yakından incelemektir. Bu bölümde diğer otomatik tanımlama sistemleri incelenirken bir yandan da RFID ile olan farkları da tartışılacak ve RFID sistemlerinin üstün olan özellikleri de bu farklardan çıkarılacaktır.

İncelenecek olan ilk sistem barkod olarak bilinen ve çok fazla kullanılan bir tanımlama sistemidir. İngilizce "*bar code* " kelimesinden gelen barkod sözcüğü "çizgi şeklinde şifre" anlamına gelmektedir. Barkod teknolojisinde pek çok farklı kodlama türü olsa da temelde çalışma prensibi aynıdır. Bu çalışma prensibine göre bilgisi istenen **etiket** siyah çizgi ve boşlukların çeşitli kombinasyonları ile kodlanır. Her siyah çizginin kalınlığı ve bulunduğu yer onun nümerik bir karşılığı olarak kodlanır. Etiketin içerdiği bilgi olarak da barkodun üstündeki bu çizgi-boşluk yapısının nümerik karşılığı saklanır. **Okuyucu** yapısı olarak da ince bir lazer huzmesi gönderen bir aygıt kullanılır. Okuyucunun etiketi okuması işlemi şu şekilde yapılır: Lazer huzmesi barkod etiketinin üstüne düşüp de geri yansıdığı zaman lazer ışını lokal olarak en çok beyaz boşluklardan yansıyıp siyah çizgilerden daha az yansıyacağı için okuyucuya lazer ışını yerel anlamda farklı miktarlarda dönecektir. Bunun da neticesinde okuyucu, yansıyan ışın miktarlarına yapacağı nümerik atamalarla barkodun ürün kodunu kendisine bağlı bulunan bir ekranda gösterebilecektir. Bu şekilde uzaktan tanıma yapılabilir. Bu uzaktan tanımanın menzili ise sadece 50 cm' ye kadar çıkabilmektedir [1]. Bu açıdan barkod sistemi RFID' ye göre daha kısıtlayıcı bir sistemdir. Etiket ile okuyucu arasındaki mesafe oldukça sınırlıdır. Şekil 2.1.'de UPC olarak bilinen barkod etiketinin içeriği ve taşıdığı bilginin anlamı verilmiştir:

Şekil 2.1. Standard UPC. Kod parçaları şu şekilde etiketlenmiştir: (A) Uygulama kodu (B) Üretici kodu (C) Ürün kodu (D) Sağlama toplamı tamsayısı [3]

İncelenecek 2. sistem ise **akıllı kart** olarak bilinen uzaktan tanımlama sistemidir. Akıllı kart, kredi kartı büyüklüğünde plastik bir kart şeklinde kılıfa yerleştirilen elektronik veri depolama sistemidir. Bazı uygulamalarda ekstra hesaplama özelliği de bulunabilir. Akıllı kartların taşıdığı veriyi okuyucuya aktarması galvanik bağlantı yoluyla olur. Bu sistemlerde okuyucu ile akıllı kartın veri transferi için temas sağlaması zorunludur. Akıllı kartın ihtiyaç duyduğu enerji ve saat işareti okuyucudan sağlanır. Akıllı kartlar sahip oldukları işlevselliğe göre bellek kartları ve mikroişlemci kartları olmak üzere ikiye ayrılırlar.

Birinci kategoriye giren bellek kartları, sadece veri depolama kapasitesine sahiptirler. Genelde bu amaç için EEPROM kullanılır. Bu tip kartlarda ardışıl devre mantığı kullanılır. Bu kartlarda basit bir güvenlik algoritması da eklenebilir. Mikroişlemci ihtiva etmediği için kullanılabileceği uygulamalar sınırlıdır, ama sağladıkları fiyat performansı oldukça etkilidir.

İkinci kategoride yer alan mikroişlemci kartları ise içlerinde barındırdıkları mikroişlemci birimi sayesinde hesaplama yapma ve içlerinde depoladıkları verileri işleme tabi tutma yeteneklerine sahip olmaktadırlar. Bu sistemlerde EEPROM yanı sıra kartın işletim sistemi denilebilecek program kodu bir ROM biriminde saklanır. ROM biriminin içeriği sadece üretim esnasında belirlenir ve bir daha değiştirilemez. Mikroişlemci kartları barındırdıkları mikroişlemci sayesinde hesaplama yeteneklerinin yanı sıra veri güvenliğini de daha iyi sağlamaktadırlar. Bu tip kartların negatif yanı ise daha pahalı olmalarıdır.

Akıllı kartlar ile RFID sistemlerinde karşılaştırmak gerekirse, akıllı kartlar doğrudan temas gerektirdiğinden ve bu temas noktalarının kirlenmeye ve yıpranmaya da açık olduğu düşünülürse akıllı kart sistemlerinde hasar oluşması ihtimali daha fazladır. Bunun yanı sıra akıllı kart sistemleri yakın temas gerektirdiğinden ve yöne bağımlı

olduğundan RFID uygulamalarından daha az esnek bir çözüm sunar. Ayrıca RFID sistemlerinde verinin okuyucu tarafından okuma hızı yaklaşık 0,5 s sürerken bu süre akıllı kart uygulamalarında yaklaşık 4 s tutmaktadır [1]. Kısaca söylenebilir ki, RFID sistemleri akıllı kartlardan daha esnek ve hızlı bir veri transferi sağlamaktadırlar ve bu özellikleri sebebiyle tercih sebebi olmaktadırlar.

RFID sistemleri ile kıyaslanabilecek son tip otomatik tanımlama sistemleri ise biyometrik prosedürler olarak bilinen uygulamalardır. Bu sistemlerde insan vücudunun bir parçası temel alınarak tanımlama yapılmaya çalışılır. Bu sistemlere örnek olarak ses tanımlama, parmak izi prosedürleri ve retina tanımlama gösterilebilir. Her insanın kendine has özellikleri olacağından bu şekilde yapılan tanımlamalarda güvenlik faktörünün oldukça yükseleceği açıktır. Bu tip uygulamalar genelde belli özel alanlara girişin yapılacağı kapılarda kullanılabilir. Bu tip bir durumda giriş izni olan görevli personelin önceden ses kaydı, parmak izi veya retina örneği alınır ve okuyucu olarak nitelendirilebilecek bir birime bağlı olan bilgisayarda veritabanına kaydedilir. Bu kişi başka bir zamanda tekrar giriş yapmak istediğinde gene kendisine ait bilgiyi ses, parmak izi veya retina taraması yoluyla okuyucu ile paylaşır ve eğer sistem veritabanında bulunan ilk örnek ile kendi örneği uyuşuyorsa kapı açılır.

Bu uygulamalar arasında güvenlik faktörü düşük olanı ses tanıma sistemleridir. Bunun da sebebi sesin taklit edilebilmesi ve kişinin her durumda farklı ses çıkararak sistemin korelasyon(ilişki) kurmasını zorlaştırmasıdır. Normalde ilk tanımlama olarak kişinin sistemde ses kaydı yapılır ve veritabanına gönderilir. Aynı kişinin daha sonraki giriş denemelerinde ise verdiği ses örneği ile ilk tanımlanan ses örneği arasında bir korelasyon kurulmaya çalışılır. Bu korelasyon başarılı olursa kapı açılır. Ancak sesin kolay taklit edilebilir olması bu uygulamanın güvenlik faktörüne gölge düşürmektedir. Bu sebepten ses tanıma sistemlerinin güvenliğin önemli olduğu uygulamalarda kullanılması sakıncalar doğurabilir. En güvenli tanıma sistemi olarak retina taraması gösterilebilir ki bunun da sebebi mevcut tıbbi durumda retinayı taklit etmenin neredeyse imkansız olmasıdır.

Kısaca biyometrik uygulamalarla RFID uygulamaları kıyaslanırsa ortaya çıkan durumda biyometrik uygulamaların çok daha sağlam bir güvenlik ve taklit edilmesi zor bir tanımlama oluşturdukları doğrudur, ancak bu uygulamaların kurulabilmesi için gereken sistemlerin çok daha pahalı oldukları söylenebilir [1]. Ayrıca bu

sistemlerin okuma hızı da çok yavaştır (Yaklaşık olarak 5-10 saniyeden fazla bir süre tutabilmektedir) [1]. Bu durumda RFID sistemlerini daha üstün kılan özellikleri çok daha ucuz ve hızlı olmaları olarak özetlenebilir.

Muhtelif otomatik tanıma sistemlerinin kıyaslaması tablo 2.1. de verilmiştir.

Tablo 2.1. Muhtelif otomatik tanıma sistemlerinin karşılaştırılması

Sistem Parametreleri	**Barkod**	**Akıllı Kart**	**Biyometri**	**RFID**
Tipik Veri Miktarı(Byte)	1-100	16-64 k	-	16-64 k
Veri Yoğunluğu	Az	Çok Fazla	Fazla	Çok Fazla
Okunma hızı	Yavaş (~4 s)	Yavaş(~4 s)	Çok Yavaş (>5-10 s)	Çok Hızlı (~0,5 s)
Etiket ile Okuyucu arasındaki Maksimum mesafe	0-50 cm	Doğrudan temas	Doğrudan temas	0-5 m (mikrodalga)
Maliyet	Çok az	Az	Çok Fazla	Ortalama
Kir ve Yıpranmanın Etkisi	Çok Fazla	Mümkün (Temas Yüzeyi)	Yok	Etkisiz

2.3. RFID Sistem Elemanları

Otomatik Tanıma sistemlerinde kullanılan elemanlar üç parçada incelenebilir:

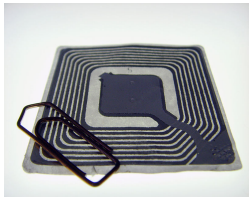
1. Veri taşıyıcı olan **etiket**
2. Veri sorgulayıcı olan **okuyucu**
3. Arka planda çalışan bir **veritabanı**

1. Etiket:

Etiket olarak tabir edilen parça, genel olarak istenen önemli veriyi taşıyan parçadır. Bu parça tipik olarak, veri saklamak amacıyla bir mikroçip ile bu veriyi istendiğinde radyo frekansında elektromanyetik dalgalar aracılığıyla okuyucuya göndermek üzere kullanılan bir antenden oluşur. Mikroçip ve anten ortak bir kılıfın içinde saklanırlar. Bu kılıf genelde seramik, plastik, epoksi veya cam olabilir. Etiketlerin sınıflandırılmasında kullanılan en temel özellikleri kullandıkları gücün kaynağıdır. Bu özelliğe göre etiketler aktif, pasif ve yarı aktif olmak üzere üç sınıfa ayrılırlar.

Aktif etiketlerin mikroçiplerinin üzerinde kendilerine ait bir güç kaynağı bulunur. Bu sayede aktif etiket, kendi inisiyatifiyle ve dışarıdan herhangi bir tetiklemeye gerek kalmadan kendi işlemlerini başlatabilir. Bu işlemler arasında veri manipülasyonu, şifreleme işlemleri veya menzildeki diğer etiketlerle haberleşme gibi eylemler bulunur. Ayrıca aktif etiketler kendi ürettikleri işaretleri okuyucuya kendi kararları neticesinde gönderebilirler. Aktif etiketlerin daha fazla veri depolama ve işleme kapasitesi olur ve bunun neticesinde şifreleme gibi ağır algoritmalar kullanan eylemlerde kullanılmaları daha uygun olur. Bunun yanı sıra aktif etiketler çok zayıf okuyucu sinyalleri ile de çalışabileceklerinden kullanılabilecekleri menzil daha geniştir ve bu da kullanıcıya daha fazla bir uygulama çeşitliliği sağlar. Aktif etiketler genelde okuyucudan yaklaşık 30 metre mesafeye kadar olan bir alanda işlem görebilirler [2]. Aktif etiketler genelde belli bir uzmanlık gerektiren bir amaç için kullanılırlar. Genelde mikroçipin içinde sahip oldukları verileri işleyebilmeleri için bir mikroişlemci, işledikleri verileri saklamak için bir oku-yaz bellek elemanı ve ne tür işlemler yapmaları gerektiğini bilmeleri için de etiketin işletim sistemini barındıran bir de sadece-oku bellek elemanı bulundururlar. Genelde pasif olan etiketlerden daha büyük hacme sahiptirler ve daha pahalıdırlar ama daha fazla veri depolayabilirler.

Aktif etiketler de enerji kullanımlarına göre ikiye ayrılırlar. Uyku moduna sahip olan etiketler, menzillerinde bir okuyucu olmadığı zaman uyku moduna geçerek enerji tüketimlerini sınırlandırırlar. Bu özelliği olmayan aktif etiketler ise sürekli çalışma halindedirler ve bu sebepten dolayı, onlar da enerji tüketimlerini düşük tutmak için daha düşük veri iletim hızı ve bellek alanı kullanmayı tercih ederler. Bu sayede enerji tüketiminde onlar da dengeyi korurlar. Şekil 2.2.'de örnek bir etiket gösterilmiştir:



Şekil 2.2. Örnek bir RFID etiketi

Pasif etiketlerin ise, aktif etiketlerden en büyük farkları kendi içlerinde bir güç kaynağı bulundurmamalarıdır. Bu sebepten dolayı, okuyucudan kendilerine gönderilen elektromanyetik dalga tarafından beslenirler. Aynı zamanda okuyucuya geri veri göndermek gerektiğinde de okuyucudan gelen bu dalgayı kullanırlar ve geri-saçılım denilen bir yöntemle istenen bilgiyi okuyucuya geri gönderirler. Pasif etiket çok sınırlı bir güçle beslendiğinden genelde iletebileceği veri çok sınırlıdır, genelde en çok da seri numarası gibi kimlik bilgileri gönderilir. Bunun yanı sıra pasif etiketlerin menzili de oldukça sınırlıdır, çünkü ilettikleri veriyi kuvvetlendirecek güçleri yoktur, bu da gönderdikleri verinin belli bir mesafe sonra gürültüye karışıp kaybolacağını gösterir. Bu özelliklerinden ötürü pasif etiketlerin içlerinde mikroişlemci gibi çok güç harcayan birimleri barındırması mümkün değildir. Bundan dolayı da pasif etiketler büyük miktarlarda veri depolamaya ve işlemeye muktedir olamazlar. Bunun sonucunda da şifreleme gibi bellek ve işlem gücü isteyen uygulamalarda kendilerine yer bulamazlar. Pasif etiketlerin kendine en rahat yer bulacağı uygulamalar güç kaynağının uygulanamadığı veya pil ömrünün daha önemli sayıldığı veya işlem kapasitesinin öncelikli olmadığı uygulamalardır. Bunlara örnek olarak mağazalardaki ürün kodlarını taşıyan etiketler veya insan bedenine yerleştirilen RFID takip cihazları verilebilir.

Aktif ve pasif etiketlerin yanı sıra bir de yarı aktif etiketler vardır. Bunlar pil yardımlı etiketler de denir. Bu türdeki etiketler mikroçip devreleri içerisinde bir güç kaynağı barındırırlar ama bu güç kaynağını sadece kendi devrelerine güç vermek için kullanırlar. Okuyucu ile haberleşmek için ise gene pasif etiketlerde bahsedilen yöntemi kullanarak (geri-saçılım yöntemi) kendi güç kaynaklarını kullanmaktan kaçınırlar. Bu tipteki etiketler kendi güç kaynaklarına dayandıklarından pasif etiketlerden çok daha fazla hesaplama gücüne sahiptirler ve pasif etiketlerden daha kısa bir sürede okuyucuya cevap vermeye hazır duruma geçerler, ancak daha fazla güç harcadıkları ve pahalı oldukları tahmin edilebilir. Ancak aktif etiketlerle kıyaslandıklarında okuyucuya kendi güçlerini kullanmadan cevap verdiklerinden daha az güç harcarlar ama aynı sebepten ötürü menzilleri daha kısadır. Üç tür etiketin kıyaslaması tablo 2.2. 'de verilmiştir.

Tablo 2.2. Aktif, yarı aktif ve pasif etiketlerin avantaj ve dezavantajlarını gösteren tablo

Özellik	Aktif etiket	Yarı-aktif etiket	Pasif etiket
Menzil	Uzun	Kısa	Kısa
Güç Tüketimi	Çok	Orta	Az
Maliyet	Yüksek	Orta	Düşük
İşlem Kapasitesi	Yüksek	Yüksek	Düşük
Bellek Kapasitesi	Yüksek	Yüksek	Düşük
Cevap süresi	Hızlı	Hızlı	Yavaş

Tablo 2.2. ' de verilen kıyaslamanın incelenmesi neticesinde güvenli yoldan, yani şifreleme yapılarak gerçeklenmek istenen bir RFID sistemin aktif etiket yapısında bir etiket kullandığında en iyi neticenin alınacağı görülebilir. Bu da demektir ki etiketin içinde mikroişlemci kullanılacaktır.

2. Okuyucu:

Bir RFID sisteminde okuyucunun görevi, antenini kullanarak etiketleri uyarmak, etiketlerin içerdiği veriyi okumak ve bir ağ aracılığıyla bu veriyi bir sunucu bilgisayara göndermektir [4]. Okuyucular da belleğe sahip olup bu bellekte veri saklayabilirler. Bu açıdan okuyucu kavramı yanıltıcı olmamalıdır. Okuyucu, yapılan uygulamaya göre stabil ya da mobil olabilir. Okuyucudan etikete giden kanala "*ileri kanal*", etiketten okuyucuya olan kanala ise "*geri kanal*" denir [3]. İleri kanalda okuyucu etikete elektromanyetik bir işaret göndererek, eğer etiket pasifse veya uyku modundaysa öncelikle onu uyandırır. Etiketin pasif olması durumunda etiketin içeriğini ihtiva eden veri geri-saçılım yöntemiyle okuyucuya geri gönderilir ve okuyucu da bu veriyi ya kendi üstünde kaydeder ya da kendisine bağlı arka planda çalışan bir bilgisayarın veritabanına kaydeder. Etiket aktifse, etikette bir takım hesaplamalar yapılabilir (şifreleme algoritması gibi) ve oluşturulan veri okuyucuya geri gönderilir. Bu şekilde sürdürülen haberleşmede okuyucu yöneten bir konumdadır. Okuyucunun performansını tarif eden bazı kavramlar Tablo 2.3. 'de verilmiştir.

Tablo 2.3. Okuyucu ile ilgili parametreler [4]

Özellik	Tanım
Tanımlama Menzili	Bir etiket grubunun tamamının tanımlanabildiği mesafe
Tanımlama Hızı	1 saniyede tanımlanabilecek etiket sayısı
Okuma Menzili	Bir etiket grubunun tamamının okunabildiği mesafe
Okuma Hızı	1 saniyede okunabilecek etiket sayısı

3. Veritabanı:

Bir RFID sisteminde okuyucu ve etiketin yanı sıra bir de okuyucuya bağlı olarak çalışan veritabanı bulunabilir. Okuyucu, etiketi sorgulamak amacıyla ona bir işaret gönderdiğinde, etiket bu işareti alarak uyanır ve kendi verisini okuyucuya geri yollar. Okuyucu geri aldığı bu cevabı, yani etiketin içeriğini alıp kendisine bağlı olan veritabanına yollar. Veritabanında bu veri kaydedilebilir veya bu verinin varlığı veri tabanında sorgulanabilir.

Örnek bir uygulamada önemli bir binanın girişi kilitlenmiş durumda olduğu düşünülsün. Bu kilidi sadece izinli personelin açıp girmesi isteniyorsa, basit bir RFID uygulaması yaratılmış olur. Bu uygulamada kapıda bir okuyucu bulunmakta, giriş izni bulunan personelin giriş kartında bir etiket bulunmakta ve okuyucuya bağlı olarak da arka planda bir veritabanı bulunmaktadır. Bu veritabanında sisteme önceden belli kart numaraları girilmiştir. Personel kartını okuyucuya doğru tuttuğunda okuyucu kartın bilgisini alır ve veritabanına yollar. Veritabanında mevcut kartın numarası olup olmadığı test edilir. Eğer numara var ise kapı açılır ve giriş izni verilir, ama eğer bilgisi yollanan kartın numarası sistemde yok ise kapı kilitli kalır ve geçiş izni verilmez. Bu tip bir uygulamayla sadece istenen kişilere giriş izni verilir. Bu uygulamada kartın üstünde kullanılan etiket pasif bir etiket olabilir, çünkü ondan tek istenen kimlik bilgisidir. Bu uygulamayı bir adım daha ilerletmek gerekirse giriş izni verildiği anda personelin kimlik numarası ve içeri girdiği saat ve tarih de sistemde kaydedilebilir.

Ancak bu uygulamalarda unutulmaması gereken bir şey de veritabanı ile okuyucu arasındaki veri iletiminin mevcut durumda güvenli olmadığıdır. Etiket ile okuyucu arasındaki güvenliğin şifreleme algoritmaları yardımıyla oluşturulabileceği önceden belirtilmişti, ancak veritabanı ile okuyucu arasındaki güvenliğin sağlanabilmesi için başka önlemlerin alınması gerektiği aşikardır.

2.4. RFID Sistem Ara Yüzü

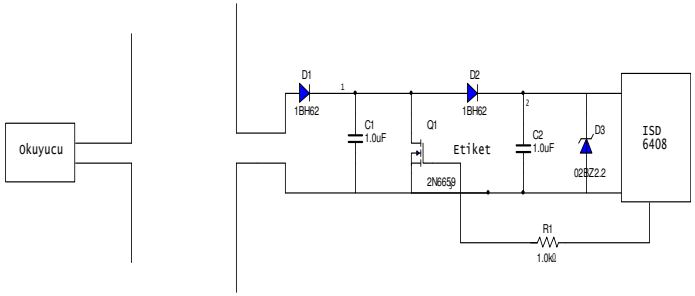
Önceki bölümde bir RFID sistemini meydana getiren elemanlar ve özellikleri tanıtılmıştı. Bu bölümde ise bu elemanların bir biri ile olan bağlantısı incelenecektir. Bu bağlamda, elemanların bir biri ile olan haberleşmesi ve bu haberleşmede kullanılan yöntemler incelenecektir. Doğal olarak bir RFID sistemini meydana

getiren başat iki eleman etiket ve okuyucu olduğundan ilk olarak bu ikisinin bir biri ile olan haberleşmesi incelenecektir.

Etiket-Okuyucu Bağlantısı:

Etiket ile okuyucu arasında radyo frekansında elektromanyetik dalgalar aracılığıyla bir haberleşme vuku bulmaktadır. İki elemanın da girişine aynı frekansta bir işareti alacak şekilde bir rezonans devresi eklenir ve böylelikle başka frekanslardan gelen istenmeyen işaretler bastırılmış olur. Bu rezonans devreleri bilindiği gibi birbirine paralel bağlanmış olan bir bobin ile bir kapasiteden oluşur. İşte havada ilerleyen elektromanyetik dalga ilk olarak bu bobin üzerinde bir akım meydana getirdiğinden etiket ile okuyucunun bu şekilde birbirine bağlanması durumuna endüktif bağlanma denir. Bobin üzerinde oluşan bu akım daha sonra kapasite üzerinde de bir gerilim oluşturur. Bu noktaya kadar etiket pasif de olsa aktif de olsa aynı olaylar yaşanır. Ancak bu noktaya gelindiğinde etiket aktif ise okuyucudan gelen bu işaret sadece etiketin uyandırılmasını sağlarken etiketin yarı aktif veya pasif olması durumunda ise üretilecek cevabın geri-saçılım yöntemiyle gönderilmesinde de işe yarar.

Geri-saçılım yöntemi RFID sistemlerinde etiketin pasif ya da yarı aktif olması durumunda sıkça kullanılan bir geri-yol (etiketten okuyucuya) iletim uygulamasıdır. Bu uygulamada, prensipte etiketin yük empedansı modüle edilerek okuyucudan gelen elektromanyetik dalganın yansıma miktarı değiştirilerek verinin etiketten okuyucuya aktarımı sağlanır [1]. Bu fiziksel olayın gerçekleşmesinde kullanılan yöntem mikrodalga frekansındaki elektromanyetik dalganın değişken yük empedansından değişik oranlarda yansımasıdır. Bu sayede etiketin göndermek istediği veri okuyucu tarafından alınır. Etiket, yük empedansını değiştirebilmek için girişte bulunan rezonans devresine paralel bağlanan bir FET tranzistorun geçit düğümüne kendi verisini göndererek savak-kaynak direncine doğrudan etki ediyor. Geçide gelen bir lojik ‘1’ savak-kaynak arası küçük direnç, geçide gelen lojik ‘0’ ise savak-kaynak arası büyük direnç olarak etkisini göstermektedir. Bu olgu Şekil 2.3.‘de gösterilmektedir.



Şekil 2.3. Geri-saçılım tekniğinin işleme prensibi. Etiketin çip empedansı, çipte bulunan FET anahtarlanarak modüle ediliyor [1].

Veri Kodlama:

Okuyucu ile etiket arasındaki iletişim bir önceki kısımda fiziksel açıdan incelenmişti. Bu iletişimin radyo frekansında elektromanyetik dalgalar aracılığıyla gerçekleştirildiği de belirtilmişti. Bu iletişim gerçekleştirilirken verinin olduğu gibi değil de bir kodlama yapılarak gönderilmesi ise verinin iletim kanalına tam olarak uyum sağlamasını sağlayacaktır. Bu şekilde verinin enterferans ve başka etiketlerin işaretleriyle çarpışma gibi olgulardan sıyrılması da sağlanacaktır [1].

Veri kodlama yapılırken gözetilmesi gereken kriterler, kodlanan işaretin etikete taşıyabildiği güç miktarı, sahip olduğu band genişliği ve diğer etiketlerin yol açtığı çarpışma olayına olan bağışıklığı olarak özetlenebilir [3].

Bu kriterler yakından incelendiğinde ilki için etikete taşınan gücün maksimum olması istendiği söylenebilir. İkinci kriter için ise kodlanmış işaretin az bir band genişliği kullanması istenmektedir ki bu sayede pek çok farklı işaret RFID uygulamasına ayrılmış sınırlı frekans bandında kendine yer bulabilsin. Son kriterde ise çarpışmaya olan bağışıklığın yüksek olması istenmektedir ki çok etiketin bulunduğu ortamlarda rahat çalışılabilinsin. Aslında 2. ve 3. kriterlerin çok sayıda etiketin bulunduğu ortamlar için geçerli olduğu söylenebilir ama 1. kritere her tür ortamda uyulması istenmektedir. 1. kritere uyan kodlama yöntemi olarak PPM ve

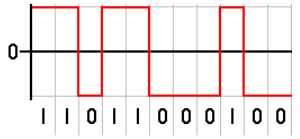
PWM kodlama yöntemleri verilebilir, çünkü bu teknikler bağıl olarak kararlı işaretler üretmektedirler. PPM ve PWM ikinci kritere de uygun sonuçlar sunmaktadır. Üçüncü kriterde bahsedilen çarpışmaya bağışıklık konusu ise bir çarpışma vuku bulduğunda bunu sistemin fark etmesine yönelik bir yaklaşımdır. Bu kriteri en iyi yerine getiren kodlama tekniği ise Manchester kodlama tekniğidir [3]. Tablo 2.4. 'de ileri ve geri yollarda bu kodlama tekniklerinin kullanım alışkanlığı gösterilmiştir.

Tablo 2.4. Kodlama Teknikleri [5]

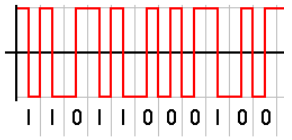
Kanal	Olağan Kodlama
İleri Kanal	Manchester veya NRZ
Geri Kanal	PPM veya PWM

Şekil 2.4. 'de ise ileri kanal kodlama tekniklerinin görsel olarak gösterimi verilmiştir.

Şekil 2.4. İleri Kanal Kodlama Teknikleri



NRZ kodlaması



Manchester kodlaması

Modülasyon:

İletim ortamı olan hava yoluyla verimli veri transferi sağlamanın ikinci önemli yöntemi de gönderilen veriyi modüle ederek göndermektir. Modülasyon işlemi, etiket ile okuyucunun tam olarak nasıl haberleşeceğini belirler. Radyo frekansında haberleşmede gönderilecek veri, modüle edilen bir taşıyıcı dalga üstünde taşınır. Üç tür sayısal modülasyon sınıfı vardır. Bunlar, genlik kaydırmalı anahtarlama (ASK), frekans kaydırmalı anahtarlama (FSK), ve faz kaydırmalı anahtarlamadır (PSK) . Her üç türün de güç tüketimi, güvenilirlik ve band genişliği kriterlerini sağlama karakteristiği farklıdır.

Okuyucudan etikete giden işaret, etiketin pasif olması durumunda etiketten okuyucuya geri dönen işaretten çok daha güçlü olacağından bu işareti bastırması ihtimali vardır. Bu ihtimali önlemek amacıyla etiketten okuyucuya geri döndürülecek işaretin genelde gelen taşıyıcı dalganın frekansının bir oranı olan farklı bir taşıyıcı dalga frekansında döndürülmesi sağlanır. Bunu sağlamak amacıyla etikette bir frekans bölücü devresi kullanılır. Geri dönen dalganın taşıyıcısına alt-taşıyıcı (sub-carrier) denir. Şekil 2.5. 'de RFID sistemlerinin haberleşmesinde kullanılan sayısal modülasyon teknikleri verilmiştir.

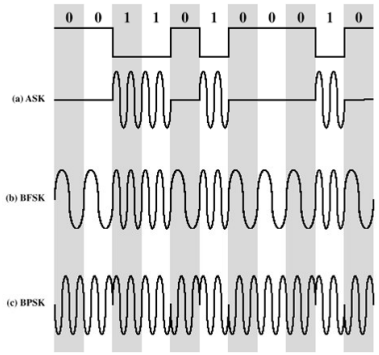


Figure 6.2 Modulation of Analog Signals for Digital Data

Şekil 2.5. RFID Sistemlerinin haberleşmesinde kullanılan sayısal modülasyon teknikleri

Çarpışma:

RFID sistemlerinin tasarımında karşılaşılan önemli bir problem de okuyucunun menzilinde olmasına rağmen etiketin okunamamasıdır. Bu tip bir problemle genelde çok sayıda etiketin bulunduğu ortamlarda karşılaşılır. Bu sorunun kaynağı, genelde etiketlerin aynı anda gönderdikleri verilerin birbiri ile karışması veya veri kaybına yol açmasıdır. Bu tip bir durumda etiketin sağlıklı bir şekilde okunabilmesinden bahsedilemez. Başka türde etkenler de "çarpışma" denilen olgunun ortaya çıkmasına yol açabilir. Üç tür çarpışma olayı betimlenebilir:

1. Tek okuyucu ve çok sayıda etiketin bulunduğu ortamda oluşan çarpışma
2. Tek etiket ve çok sayıda okuyucunun bulunduğu ortamda oluşan çarpışma
3. İki veya daha fazla sayıda okuyucunun aynı frekans aralığını kullanmaları neticesinde ortaya çıkan çarpışma olayı

Bu üç çarpışma türü arasında en yaygın olarak karşılaşılan veya gerçekleşmesi en olası olan çarpışma türü olan 1. kategoriye giren çarpışmalar ve çözüm yöntemleri incelenecektir.

Tek okuyucu ve çok sayıda etiketin bulunduğu ortamda oluşan çarpışma:

Gelişen uygulamalar ile birlikte RFID sistemlerinde çok sayıda etiketin aynı ortamı paylaştığı uygulamalar yaygınlaşmaktadır. Bunlara örnek olarak, kütüphanecilik, havaalanı bagaj sistemi veya marketlerde ürünlerin kodlanması gibi uygulamalar verilebilir [2]. İşte bu tip uygulamalarda okuyucular, bir ortamda çok sayıda etiketin varlığını algılayabilecek şekilde tasarlanmalıdırlar. Eğer bu algılama yapılamazsa okuyucu aynı anada birden çok sayıda etiketin verisini almaya çalışacaktır ki bu durumun da çarpışmaya yol açacağı açıktır.

Birden çok sayıda etiketin aynı kanal üzerinden haberleşmeye kalkması durumunda, çarpışmanın meydana geleceği ve bu durumun da veri iletimini olumsuz etkileyeceğinden bahsedilmişti. Bu çarpışmanın önüne geçilebilmesi için etiket ile okuyucu arasındaki iletişim için belli bazı kuralların belirlenmesi gerekmektedir. Bu kuralların tümüne *çarpışma önleme protokolü* denir [2]. Pasif etiketlerin sahip olduğu hesaplama yeteneği genelde düşük olduğundan ve birbirleriyle iletişim de kuramadıkları için pasif etiketleri içeren uygulamalarda çarpışmayı önleme meselesi ile okuyucu doğrudan sorumlu olacaktır. Genelde okuyucunun bu sorunu çözme

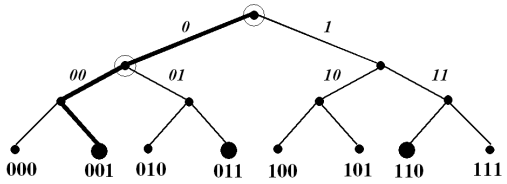
yöntemi olarak belirlenen süreçte önce ortamda menzile giren tüm etiketlerin belirlenmesi, daha sonra da bu etiketlerin tek tek tanımlanması gerekmektedir. Tek bir etiketi diğerlerinden tecrit ederek adresleme ve bu yolla tanımlama tekniğine *tekilleme* denir [2]. Tekilleme tekniği uygulayarak ortamda bulunan tüm etiketleri tanımlayan okuyucu daha sonraki aşamada istediği etikete bir tek onun adresini ya da tanımlama numarasını kullanarak ulaşabilir ve istediği veriyi çarpışma riski olmadan ondan alabilir. Okuyucu ile etiket arasındaki haberleşmede kullanılan çarpışma önleme protokolleri kullanılan frekansa ve uygulamaya göre standard hale getirilmeye çalışılmaktadır [2].

Çarpışma önleme protokolleri, belirleyici ve olasılılığa dayanan protokoller olarak ikiye ayrılırlar. Belirleyici protokollerde, her etiket tek bir kimlik numarasına sahip olmaktadır ve bu kimlik numarası üretim esnasında etiketin salt-oku belleğinde kaydedildiğinden değişmeden kalır. Olasılığa dayanan protokollerde ise zaman bölmeli çoklu erişim denilen bir altyapı kullanılır. Bu tip protokollerin çalışma prensibi oldukça basittir:

- Bir veri ne zaman gönderilmesi gerekiyorsa o zaman gönderilir.
- Eğer veri yolda çarpışmaya uğradıysa ve düzgün bir şekilde hedefe ulaşamadıysa veri başka bir zaman yeniden gönderilir.

Bu tip olasılığa dayanan protokollerde, bir çarpışma meydana geldiğinde okuyucu bunu fark edip tüm etiketlere bildirir ve etiketler de hepsi farklı bir sayaç oluşturarak bu sayaçlar sıfırlandığında yeniden veri iletimine geçecek şekilde beklemeye başlarlar. Tüm etiketlerin bekleme süresi farklı olarak ayarlandığında hepsi farklı süre aralıklarında iletime geçerek olası çarpışmaların önüne geçerler. Bu prensibin alt yapısı zaman bölmeli çoklu erişim olarak nitelendirilir.

Belirleyici yapıda çarpışma önleme protokollerine örnek olarak ağaç-yürüme algoritması verilebilir. Bu algoritmanın işleme prensibi 8 tane etiket tanımlama kapasitesine sahip olan bir okuyucu için şekil 2.6. 'da verilmiştir.



Şekil 2.6. 3 tane etiketin bulunduğu bir ortamda ağaç-yürüme algoritmasının işleme prensibi

Ağaç-yürüme algoritması şekil 2.6. üzerinde şu şekilde açıklanabilir:

- Ortamda 3 tane etiket vardır ve her biri ikili düzende bir sayıya karşılık gelecek 3 bitle kodlanmış bir kimlik numarasını salt-oku belleğinde taşımaktadır.
- Kodlama 3 bitle yapıldığı için okuyucunun aynı ortamdaki 8 farklı etiketi tanımlama olanağı vardır. Bu demektir ki 5 tane kod bu ortam için hiçbir etikete atanmamıştır.
- Okuyucu ilk olarak ilk bitinde 0 olan etiket olup olmadığını sorgular. 110 koduna sahip olan etiket bu durumda uyku moduna geçer ve protokol sonlanana kadar bir daha okuyucunun sinyallerine cevap vermez, yani tekrar tekrar okuyucunun karşısına çıkmaz.
- İkinci aşamada okuyucu ikinci bitinde 0 olan bir etiketin ortamda bulunup bulunmadığını sorgular. Bu durumda 011 koduna sahip olan etiket de uyku moduna geçer. Kalan tek etiket olan 001 kodlu etiket ise cevap verir.
- Üçüncü aşamada okuyucu üçüncü bitinde de 0 olan bir etiket olup olmadığını sorgular. Ortamda kalan son etiket olan 001 koduna sahip olan etiket de bu durumda cevap vermediğinden okuyucuya hiçbir cevap gelmez ve okuyucu sorgulamasını bir üst aşamada değiştirmesi gerektiğine karar verir.
- Dördüncü aşamada okuyucu sorgulamasını değiştirerek üçüncü bitinde 1 olan bir etiket olup olmadığını sorgular ve karşısına 001 kodlu etiket çıkar. Okuyucu bu sefer bu etiketi tam olarak tanımlamıştır. Bu şekilde ileri-geri manevraları sürdürerek okuyucu her üç etiketi de tanımlayabilir.

Olasılığa dayanan çarpışma önleme protokolleri daha az bir frekans bandının işgaline yol açtıklarından frekans bandının dar olarak düzenlendiği uygulamalarda kullanılmaya daha elverişlidirler. Belirleyici protokoller ise frekans bandının kısıtlayıcı olmadığı uygulamalarda kullanılabilirler.

Frekansla ilgili düzenlemeler:

Yerel hükümet düzenlemeleri, her ülkede RFID sistemler için kullanılabilecek elektromanyetik spektrum parçasını belirlemektedir. Pek çok RFID sistemi ISM (Industrial-Scientific-Medical) bandında çalışmaktadır [3]. ISM bandı kullanımı, düşük güç harcayan ve kısa menzile sahip RF uygulamaları için lisans gerektirmeyen bir özelliğe sahiptir. Bu bandlar ITU tarafından belirlenmiştir.

Dünya çapında RFID sistemleri için belirlenen en önemli taşıyıcı frekansları 0-135 kHz, 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz, 2.45 GHz, 5.8 GHz ve 24.125 GHz olarak belirtilmiştir [1]. Bu frekansların kullanılabilirliği her ülkenin kendi yasal düzenlemeleri tarafından belirlenmiştir. Tablo 2.5. 'de muhtelif ülkeler için belirtilen frekansların RFID sistemlerinde kullanımı gösterilmektedir [2].

Tablo 2.5. RFID Çalışma Frekansları

Frekans Bandı	Frekans	Sistem	Bölge/Ülke
LF	125-134 kHz	Endüktif	ABD, Kanada, Japonya ve Avrupa
VHF	13.56 MHz	Endüktif	ABD, Kanada, Japonya ve Avrupa
UHF	433.05-434.79 MHz	Yayınım	Avrupa'nın büyük kısmı, ABD ve Japonya
UHF	865-868 MHz	Yayınım	Avrupa, Ortadoğu, Singapur, Kuzey Afrika
UHF	866-869 ve 923-925 MHz	Yayınım	Güney Kore, Japonya,Yeni Zelanda
UHF	902-928 MHz	Yayınım	ABD, Kanada, Güney Amerika, Meksika, Tayvan, Çin, Avustralya, Güney Afrika
UHF	952-954 MHz	Yayınım	Japonya(Pasif etiketler için)
Mikrodalga	2.4-2.5 ve 5.725-5.875 GHz	Yayınım	ABD, Kanada, Avrupa, Japonya

3. RFID SİSTEMLERİNDE GÜVENLİK KAVRAMI VE GÜVENLİĞİN SAĞLANMASI

3.1. RFID Sistemlerinde Güvenlik Kriteri

Günümüzde pek çok alanda birçok uygulamada kullanılan RFID sistemleri güvenlik sorunuyla karşı karşıyadır. Bu sorunun kökeninde etiket ile okuyucu arasındaki veri transferinin gözlenebilir mahiyette olması yatmaktadır. Etiket ile okuyucu arasında gönderilen veri araya giren bir gözlemci tarafından gözlenebilir. Bu gözlemci eğer ilgili teçhizata sahipse arada durmanın yanı sıra iletilen veriyi kopyalayabilir veya değiştirebilir. Bu tür saldırılar önemli verilerin aktarıldığı RFID sistemleri için kabul edilemez bir durumdur. Bu durumun oluşmasını engellemek için güvenliği sağlanamamış bir ortam olarak kabul edilen etiket ile okuyucu arasındaki hava ortamında verinin şifreli bir şekilde gitmesi sağlanabilir. Bu şekilde en azından saldırganın havada aktarılan verinin içeriğine sahip olması engellenmiş olur. Bu şifreleme yöntemi sayesinde etiket bir şekilde taklit edilse bile okuyucu tarafından tanınmayacağından bu yolla yapılan denemeler başarısız olacaktır. Bu şekilde yapılan bir şifreleme neticesinde uzaktan kredi kartı ile ödeme veya izinli personel giriş kartı ile hedef binaya giriş yapma gibi uygulamaların güvenliği sağlanabilir. Ancak şifreleme yapmadan önce yapılacak uygulamaya da dikkat edilmelidir. Güvenlik işlevi olmasını gerektirmeyen ürün tanıma gibi uygulamalara güvenlik sağlamaya çalışmak boşu boşuna maliyetlerin artmasını sağlayacaktır. Öte yandan üstte belirtildiği gibi güvenlik gerektiren uygulamalarda da maliyetten kaçınmak ilerde daha büyük zararlara yol açabileceğinden bu hususa dikkat edilmelidir. Kısaca belirtmek gerekirse, bir RFID sisteminde güvenlik kriterinin ne kadar önemli olduğu kullanıldığı uygulamaya bağlıdır ve önce ilgili uygulamada güvenliğe ne derece ihtiyaç duyulduğu belirlenerek bu konuda ona göre tutum takınılmalıdır. Eğer ilgili uygulamada güvenlik sağlanmasına ihtiyaç var ise kullanılacak RFID sisteminin de özellikleri düşünülerek uygun bir şifreleme algoritması belirlenmeye çalışılır. Bu algoritma belirlenirken değerlendirilen temel ölçütler algoritmanın gerçekleştirilebildiği bellek alanı ile sisteme harcattığı güç miktarıdır. Tabi bu

ölçütler değerlendirilirken bir de algoritmanın sisteme sağladığı güvenlik de gözetilmesi gereken bir diğer etmendir. Sonuç olarak, kullanılacak algoritma belirlenirken ihtiyaç duyulan bellek alanı, harcanılan güç ve bunun karşılığında sağlanılan güvenlik bir denge oluşturacak şekilde en iyi çözümü sunan algoritma seçilmelidir.

Ancak RFID sistemlerine her koşul altında şifreleme yapmak kolay değildir, çünkü kullanıldıkları uygulamalarda küçük boyutlara sahip oldukları için sınırlı güç, bellek ve devre alanı sağlanabilen bir yapıdadırlar. Bu sebepten dolayı RFID sistemlerini güvenli olarak kurabilmek için şifreleme algoritmasına geçmeden önce öncelikli olarak önerilen bazı çözümler vardır. Bunlara bu kısımda değinilecektir.

Bu öncelikli olarak uygulanabilecek çözümlerden ilki *öldür* komutudur. Bu komut uygulanması durumunda etiket bir daha uyanmamak üzere işlevlerini durduracaktır. Bu komutun uygulanabilmesi için üretim aşamasında etiketin belli bir parolayı aldığı zaman tamamıyla deaktive olmak üzere programlanması lazımdır. Sonraki bir zamanda bu komutu aldığı anda işlevlerini durduracaktır [6].

Başka bir uygulamada ise etiketlerin klonlanmasının önüne geçmek amacıyla Faraday kafesi adı verilen bir uygulama yapılır. Bu uygulama neticesinde etiketin civarındaki bütün elektromanyetik dalgalardan tecrit edilmesi sağlanır. Bu şekilde etiketin koruduğu veriler de hiçbir şekilde sorgulanamaz, çünkü etiketten veri çıkışı imkansız hale gelmiştir [6].

Bir diğer uygulamada etiket sorgulanmak istemediği bir durumda etrafa normalde okuyucunun onu sorguladığı frekansta bir dalga yayarak olası sahte okuyucuların kendisi ile iletişime geçmesini engellemektedir [6].

Çok sayıda etiketin bulunduğu ortamlarda olası çarpışmaların önüne geçebilmek amacıyla 915 MHz taşıyıcı frekansında deterministik bir protokol olan ağaç-yürüme protokolü, 13.56 MHz taşıyıcı frekansında ise olasılığa dayanan bir protokol olan ALOHA protokolü uygulanabilir.

Yukarda bahsedilen öncelikli önlemleri almanın yanı sıra güvenliği sağlamak amacıyla geleneksel şifreleme yöntemleri de kullanılabilir. Bunlarda akla ilk geleni aktif bir etiketin şifrelenmiş bir kimlik bilgisini içinde barındırması ve sık sık şifreleme amacıyla kullandığı anahtarı değiştirmesidir. Ancak anahtarın çok sık

değiştirilmesi pil ömrünü oldukça hızlı tükettiğinden en fazla saatte bir anahtarın değiştirilmesi yöntemi önerilmektedir [6].

Geleneksel şifreleme yöntemleri arasında önerilen ikinci bir şifreleme yöntemi ise iki taraflı bir soru-cevap formatında bir şifreleme algoritması kullanmaktır. Buna örnek olarak AES algoritması verilebilir. AES, simetrik anahtar kullanan çok güçlü fakat fazla güç harcatan bir şifreleme algoritmasıdır. AES' in detaylı analizi bir sonraki kısımda yapılacaktır.

Konvansiyonel şifreleme yöntemleri arasında RFID sistemleri üzerinde kullanılması önerilen bir diğer yöntem de açık anahtar şifreleme yöntemidir. Bir sonraki kısımda bu yöntem de incelenecektir.

3.2. RFID Sistemlerinde Kullanılması Olası Şifreleme Algoritmalarının İncelenmesi:

RFID sistemlerinde kullanılması olası şifreleme algoritmalarının incelenmesine geçmeden önce şifreleme işleminin kullanılan anahtarın niteliğine göre ikiye ayrıldığından bahsedilmelidir. Bunlardan birincisi simetrik anahtarla şifreleme, ikincisi ise açık anahtarla şifrelemedir. Simetrik anahtarla şifreleme yapıldığında, şifreleme anahtarı olan *k* biliniyorsa şifrelenmiş veriyi deşifre eden anahtar olan *d*' yi *k*' yı kullanarak hesaplamak kolay olmaktadır. Simetrik anahtar denmesinin sebebi budur: Şifrelemede kullanılan anahtar ile deşifre etmede kullanılan anahtar birbirine simetrik kabul edilir [7]. Açık anahtarlamalı şifrelemede ise iletişimin taraflarından sadece biri, elinde protokolde kullanılacak olan şifreleme ve deşifre etme anahtarlarını bulundururken, şifreleme anahtarını diğer tarafa herkesin görebileceği şekilde güvenli olmayan yoldan gönderir. Diğer taraf da bu anahtarı alır, asıl istenen veriyi şifrelemede kullanır ve şifrelenmiş halde verisini güvenli olmayan yoldan karşı tarafa gönderir. Şifrelenmiş veriyi alan taraf ise kendi deşifre etme anahtarını kullanarak veriyi deşifre eder ve istediği veriyi elde eder. Bu iki şifreleme yöntemi arasındaki esas fark şifreleme anahtarının güvenli bir yoldan gönderilip gönderilmemesi meselesidir. Eğer bu anahtar güvenli olmayan bir yoldan gönderiliyorsa gözlemciler bu anahtara doğrudan ulaşabileceğinden deşifre etmeye yarayan anahtarın şifreleme anahtarı ile doğrudan bir bağı bulunmaması ya da

şifreleme anahtarına bakılarak hesaplanmasının pratik olarak imkansız olması istenmektedir.

Simetrik anahtar kullanan şifreleme algoritmaları, akan şifre ve blok şifre gibi uygulamalara sahiptirler. Akan şifre kullanıldığı takdirde şifrelenmesi istenen verinin her bir biti teker teker şifrelenerek karşı tarafa gönderilirken blok şifre kullanıldığı zaman şifrelenmesi istenen mesajın içerdiği bitler bloklar halinde alınıp şifrelenir ve karşı tarafa gönderilir. 64 bitten oluşan bloklar oldukça yaygın bir kullanıma sahiptirler [8]. Gelişmiş Şifreleme Standardı olarak bilinen AES ise 128 bitlik bloklar kullanır [8]. Açık anahtarlı şifreleme de ise şifreleme anahtarı güvenli olmayan ortamda yollanır ve gözlemci olan herkesin eline geçebilir ve bu anahtar eline geçen herkes sahip olduğu veriyi şifreleyip karşı tarafa gönderebilir, ancak bu anahtarı kullanarak deşifre etmeye yarayan anahtarı keşfedip de karşı taraftan şifreli gelen veriyi kıramazlar. Bu durumda simetrik anahtarlı şifreleme iki tarafın da eşit statüye sahip olduğu bir haberleşme türü iken asimetrik veya açık anahtarlı şifreleme taraflardan birinin bilgi açısından üstün olduğu ve karşılıklı iletişimi yönettiği bir haberleşme türüne benzemektedir.

İki şifreleme türünü kıyaslamak gerekirse, ilk planda simetrik anahtarlı şifrelemenin kullandığı algoritmaların yapılan hesaplamalar açısından asimetrik anahtarlı şifrelemeye göre çok daha az yoğun olduğu görülmektedir. Bu durum göz önüne alındığında simetrik anahtarlı şifrelemenin açık anahtarlı şifrelemeye göre 100 hatta 1000 misli daha hızlı olduğu söylenebilir [8]. Bu bilgi ışığında güvenli kartlı geçiş uygulamasında girilmek istenen bina pek çok insanın çalıştığı bir bina ise ve girişin şifreli yapılması isteniyorsa zaman kaybının önüne geçmek amacıyla simetrik anahtarlı bir şifreleme çözüm olarak önerilebilir.

Simetrik anahtarlı şifrelemenin temel problemlerinden biri ise anahtar dağıtımının yapılması problemidir. Simetrik anahtarlı şifrelemede bilgi paylaşımında yer alan her birimin paylaştığı gizli bir anahtar olduğu için ve bu şifreleme anahtarının her bir birime ayrı ayrı iletilmesi gerektiğinden anahtar dağıtımı esnasında problem yaşanacağı tahmin edilebilir. Bu sistemin güvenli olarak gerçekleştirilebilmesi için iletişimin taraflarına düzenli olarak yeni anahtarlar sağlanmalıdır, çünkü teorik olarak her anahtar kırılabilir. Bunu sağlamak için de periyodik olarak yeni bir anahtar dağıtımı yapmak gereklidir. Simetrik anahtarlı şifrelemede ise anahtar dağıtımı yapılan kanalın güvenli olması zorunluluğu ve her bir birime ayrı bir anahtarın

ulaştırılması zorunluluğu simetrik anahtarlı şifreleme sistemini anahtar dağıtımı açısından elverişsiz kılmıştır.

Sağladığı güvenlik açısından incelendiğinde asimetrik anahtarlı şifreleme yöntemlerinin daha güvenli bir uygulamayı destekleyebilecekleri fark edilmiştir. Bunun arkasında yatan sebep ise asimetrik anahtarlı şifrelemede açık anahtarı etrafa gönderen yetkin tarafın sadece kendisinin deşifre etme özelliğine sahip olmasıdır. Bu tip bir sistemde ortamda bulunan diğer birimler açık anahtarı kullanarak kendi verilerini şifreleyebilirler, ancak şifrelenmiş bir veriyi deşifre etme yeteneği sadece bahsedilen yetkin birime verilmiştir. Bu özelliği sayesinde asimetrik anahtarlı şifreleme uygulamalarında güvenlik faktörü daha iyi sağlanmaktadır.

Bu kısımda simetrik anahtarlı şifrelemeyi temsilen AES ile asimetrik veya açık anahtarlı şifrelemeyi temsilen ECC algoritmaları incelenecek ve karşılaştırmalı olarak avantaj ve dezavantajları belirtilerek bir RFID uygulaması için daha uygun olanının seçilmesine çalışılacaktır.

AES (Advanced Encryption Algorithm) bahsedildiği üzere simetrik anahtarlı şifreleme türünde bir algoritmadır. NIST tarafından 1997 yılında dünya çapında açılan bir şifreleme algoritmaları geliştirme yarışmasında iki Belçikalı kriptolog tarafından geliştirilmiştir ve 2003 yılında NSA tarafından gizli bilgi ve belgeleri şifrelemek için yeterli olduğu ilan edilmiştir [2]. AES algoritması 128-, 192- ve 256-bit olmak üzere üç şekilde gerçekleştirilebilir [2]. Bit sayısı arttırıldıkça şifrenin karmaşıklığı dolayısıyla sağladığı güvenlik artar. AES hem yazılımsal hem de donanımsal olarak hızlı ve kolay bir şekilde gerçekleştirilebilir ve az bir bellek alanını işgal eder. Bu özellikleriyle beraber AES, hızlı bir şekilde geniş ölçekli uygulamalarda kullanılmaya başlamakta ve simetrik anahtarlı şifreleme sistemlerinin yeni standardı olma yolunda hızla ilerlemektedir.

ECC algoritması ise yukarda değinildiği gibi asimetrik anahtarlı şifreleme türü bir algoritmadır. ECC algoritması, elips yapısındaki eğrilerin sonlu alanlar üstündeki cebirsel yapısına dayanan bir algoritmadır. Bir eliptik eğriyi tarif eden denklem, denklem 3.1.'de verilmiştir.

$$y^2 = x^3 + ax + b \qquad (3.1.)$$

Burada belirtilen a ve b parametreleri ise $4a3+27b2 \neq 0$ eşitsizliğini sağlayan katsayılardır. Elliptik eğrileri gerçekleyen bit sayısı herhangi bir sayı olarak seçilebilse de güvenli bir uygulama sağlayabilmek amacıyla günümüzde 163 ile 283 bit arasındaki uygulamalar bulunmaktadır [9]. ECC algoritmalarının açık anahtarlı şifreleme sistemlerinin sahip oldukları bütün faydalar sayesinde daha güvenli bir uygulama sağlayacakları ve anahtar dağıtımı problemini ortadan kaldıracakları açıktır. ECC algoritmalarının RFID sistemleri için kullanılmaları önündeki en büyük problem karmaşık bir algoritma oldukları için kullandıkları fazla bellek alanı ve harcadıkları güç sebebiyle yol açtıkları maliyet problemidir. Ancak sağladıkları güvenliğin derecesinin yüksek olmasını hesaba katarak yakın gelecekte RFID uygulamalarında da daha sık bir şekilde kullanılacak olmaları tahmin edilebilir [9].

3.3. Bir RFID Sistemi İçin ECC Algoritmasının Gerçeklenmesi

Bir sistem ECC ile şifreleneceği zaman eliptik eğri üzerinde bulunan bir nokta iki tane koordinatı olmak üzere belirlenir ve bu koordinatlara sahip olan nokta ile kullanılan anahtar çarpılarak bir sonuç parametresi elde edilir. Kurulan iletişim protokollerinde kullanılan işte bu sonuç parametresidir. Bir RFID sisteminde kurulacak olan ECC algoritmalı şifreleme sistemi doğal olarak karşılıklı işlemler yapan bir okuyucu ile aktif bir etiketten oluşacaktır. Aktif etiketin içinde şifreleme hesaplamaları yapabilmek için bir adet mikroişlemci ve yeteri kadar bellek alanı gerekmektedir. Bu çalışmada mikroişlemci birimi olarak Silicon Laboratories firmasının C8051F060 uygulama geliştirme kiti kullanılmıştır. Bu kitin içinde bulunan mikroişlemci ve RAM sayesinde gerekli şifreleme hesaplamaları yapılabilecektir. Bu kitte bir adet seri port bulunmaktadır ve şifreleme hesaplamaları yapıldıktan sonra karşı tarafa gönderilmesi istenen veri seri port üzerinden gönderilecektir. Seri porta da HAC-UM 96 RF modem bağlandığında üretilen veri hava yoluyla gönderilmeye hazır hale gelecektir. Karşı taraf için de benzer yapıda bir blok kurulduğunda güvenli yoldan bir RFID sistemi kurulmuş olacaktır. Bu kısımda önce bu sistem parçaları tanıtılacak daha sonra da bu sistem parçaları kullanılarak ECC şifreleme algoritmasının nasıl kurulacağı anlatılacaktır.

C8051F060 Mikrokontrolör Kiti ve HAC-UM96 RF Modem:

Bu çalışmada bir RFID sistemi ele alınarak güvenli şekilde gerçekleştirilmesi sorunu ele alınmıştır. Bu güvenlik sorununu çözebilmek için aktif bir etiket ile bir okuyucu arasında şifrelenmiş veri aktarımı sağlayarak bu sorunun çözülmesi önerilmiştir. Bu amaçla kullanılacak olan etiketin de okuyucu gibi kompleks şifreleme işlemlerini yapabilmesi istenmektedir. Bu sebepten iletişimin iki tarafı da hesaplama kapasitesi bakımından birbirine eş kabul edilmekte ve simetrik olacak şekilde hem etiketin içinde hem de okuyucunun içinde aynı mikrokontrolör birimi kullanılmıştır.

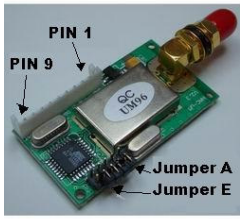
Kullanılan bu mikrokontrolör birimi Silicon Laboratories firmasının üretmiş olduğu C8051F060 isimli kitidir. Bu kitin içinde bir adet 8 bitlik 25 MHz sistem saatine sahip olan 8051 mikrokontrolörü, bir adet 4 kB'lık iç oku-yaz belleği, bir adet 64 kB'lık program kodunu saklayan Flash bellek, bir adet de 64 kB'lık dış oku-yaz belleği bulunmaktadır. Sistemin saniyede 25 milyon komutu işleme kapasitesi vardır. Ayrıca 2 adet UART bağlantısı ve 5 tane de 16 bitlik zamanlayıcısı vardır. Bu UART bağlantılarından biri RS-232 protokolünü kullanırken ,diğeri de CAN adı verilen protokolü kullanmaktadır. Bu çalışmada yapılan uygulamada mikroişlemci biriminde işlenen verinin dışarıya transferi RS-232 protokolü ile gerçekleştirilecektir [10].

Mikrokontrolörün dış dünya ile bağlantısı RS-232 protokolünü kullanan UART üzerinden bir RF modeme bağlanarak gerçekleştirilecektir. İşte sistemde kullanılacak bu RF modem HAC-UM96 olarak adlandırılmış bir RF modem modelidir. Bu modelin belirtilmiş olan bazı özellikleri şu şekilde belirtilmiştir:

- İletim sırasında aktarılan güç oldukça düşüktür ve 10 mW kadardır.
- 433 MHz civarında ayarlanabilen 8 kanal kullanan taşıyıcı frekansı kullanmaktadır.
- Gauss frekans kaydırmalı anahtarlama (GFSK) kullanan sistem havada meydana gelebilecek olan girişime (enterferans) ve iletilen bitlerde meydana gelebilecek hatalara karşı dayanıklıdır ve bit hata oranı oldukça düşük olmaktadır.
- 300 ile 500 metre arasında değişen güvenilir iletim menziline sahiptir.
- Modem, bir UART cihazıdır ve ona gönderilen veri uygun çerçeve içinde gönderilmelidir. Bu cihaz için uygun çerçeve saniyede 9600 bit olmaktadır.

- 2 tane seri portu ve 3 tane arayüzü bulunmaktadır. Kullandığı arayüzler, TTL düzeyinde UART, RS-232 ve RS-485'dir.
- Düşük güç tüketimine ve uyku modu özelliğine sahiptir. Veri gönderirken maksimum 40 mA akım kullanırken veri alırken maksimum 30 mA akım kullanır ve uyku moduna girdiğinde maksimum 20 µA akım çekmektedir [11].

RF modemin resmi ise şekil 3.1. ' de gösterilmektedir.



Şekil 3.1. HAC-UM96 RF modeminin resmi [11]

Mikrokontrolör birimi ve RF modem birimi, birlikte gerçekleştirilmek istenen RFID sisteminin donanım kısmını gerçekleştirirler. Sistemin yazılım kısmını oluşturan kısımlar olan ana protokol ile algoritma kısımları ise şimdi incelenecektir.

Ana Protokol:

Gerçekleştirilmeye çalışılan RFID sisteminin yazılım kısmının en önemli parçası sistemin şifrelemede kullandığı ana protokoldür. Ana protokol sistemin iki tarafı arasında veri transferi başlamadan önce iki tarafın da birbirini sınaması ve tanımlaması aşamasını barındırır. Bu sistemde kullanılan ana protokol şekil 3.2.' de verilmiştir [12].

Okuyucu		Etiket
X ⟵ r . P	X ⟶	
	⟵ e	
y = a.e + r mod n	y ⟶	Eğer y . P + e . Z = X ise kabul et, değilse reddet.

Şekil 3.2. Schnorr'un Tanımlama Protokolü [12]

Bu tanımlama protokolü gereği ilk aşamada kullanılan parametreler tanıtılmalıdır.

r…..okuyucunun kullandığı gizli şifreleme anahtarı
P……..eliptik eğri üzerinde tanımlanmış x ve y koordinatları olan bir nokta
e……...etiketin kullandığı açık parametre
a……...okuyucunun kullandığı gizli parametre
Z……...Z = - a . P işlemi sonucu ortaya çıkar. Bu işlem okuyucunun içinde yapılır ve işlemin sonucu olan Z parametresi etikete gönderilir.

1. Burada gösterilen X = r . P işlemi eliptik eğri nokta çarpma (ECPM) işlemidir. Önce bu işlem yapılır ve sonucu karşı tarafa gönderilir.
2. İkinci aşamada ise etiketten e parametresinin gelmesi beklenmektedir.
3. Üçüncü aşamada etiketten gelen e parametresi de kullanılarak y = a.e + r mod n işlemi gerçekleştirilir ve sonuç parametresi etikete gönderilir. Burada gerçekleştirilen işlem bilinen basit artimetik çarpma ve toplama işlemlerine modül işleminin uygulanarak sonucun sınırlandırılmasıdır.
4. Dördüncü aşamada okuyucuda Z = - a . P işlemi gerçekleştirilir ve ortaya çıkan Z parametresi etikete gönderilir. Burada yapılan işlem de birinci aşamadaki gibi eliptik eğri nokta çarpma işlemidir.
5. Beşinci ve son aşamada ise etiket y . P + e . Z işlemini yapar ve bu işlemin sonucunda ortaya çıkan iki koordinat X noktasının iki koordinatına eşit oluyorsa okuyucunun ilk başta göndermiş olduğu iletişim teklifini kabul eder ve ilgili veri transferini başlatır. Burada yapılan işlem ise iki tane eliptik eğri üzerinde nokta çarpımının eliptik eğri üzerinde nokta toplamı (ECPA) şeklinde tecelli etmektedir.

Burada bahsedilen parametrelein hepsi de 163 bit uzunluğundadır, yani 163 bitlik ECC uygulanmaktadır. Bu kısımın devamında ise eliptik eğri üzerinde nokta çarpma ve toplama işlemleri anlatılacaktır.

Eliptik eğri üzerinde nokta toplama ve çarpma işlemleri:

Eliptik eğri üzerinde nokta toplama işlemi, sonlu alanlarda toplama ve çarpma işlemlerine dayanmaktadır. Sonlu alan, içeriği sadece 1 ve 0'dan oluşan yani işlemlerini modül 2 üzerinde gerçekleştiren alanın ismidir. Bu sebepten dolayı öncelikle bu işlemlere değinilinmesi gerekmektedir. Sonlu alanlarda toplama işlemi

yapılan iki sayının toplamı iki sayının bit bit YADA (XOR) işlemine tabi tutulması anlamına gelmektedir. Sonlu alanlar üzerinde çarpma işlemi de toplama işlemine dayanır. Bu işlemde 1. çarpanın bitleri en yüksek anlamlı olandan başlanarak incelenir. Bu arada değeri sıfır olan geçici bir sayı oluşturulur ve bu geçici sayının içeriği 1. çarpanın incelenen her biti için sola kaydırılır ve bu arada 1. çarpanın incelenen bir biti '1' ise bu geçici sayı 2. çarpan ile toplanır. Bu şekilde devam eden süreçte bit sayısında bir taşma olursa bir indirgeme polinomunun yardımıyla sonlu alanda toplama yapılarak taşan bitin yok edilmesi sağlanır. Bu şekilde işlem tamamlanır.

Eliptik eğri üzerinde nokta toplama ve çarpma işlemi de işte sonlu alanda gerçekleştirilen bu iki işleme dayanmaktadır [13].

4. SONUÇLAR VE TARTIŞMA

Bu çalışmada ilk önce çeşitli RFID sistemleri incelenmiş ve bunlar arasından şifrelemeye en uygun olan bir güç kaynağı bulunan aktif bir etiket kullanan ve ISM bandında 433 MHz frekansını kullanan bir RFID sisteminin güvenli açıdan gerçekleştirilmesi için en uygun şifreleme türü olarak Açık Anahtarlı Şifreleme tercih edilmiş ve bu şifreleme türünün günümüzdeki en güçlü temsilcisi olan ECC algoritması 163 bit kullanılarak gerçekleştirilmiştir. Günümüzde yeterli bir güvenlik seviyesine ulaşabilmek için 160 bit kullanan bir ECC algoritmasının yeterli olduğu belirtilmiştir [14].

ECC algoritması, açık anahtarlı şifreleme türünde bir algoritma olduğu için simetrik anahtarlı şifreleme türüne göre bazı üstünlükleri bulunmaktadır. Bu üstünlükler,

1. Anahtar dağıtımı sorununu çözmüş olması,
2. Daha güvenli bir şifreleme sağlaması,

şeklinde özetlenebilir. ECC algoritmasının tek olumsuz özelliği yoğun bir hesaplama içeriğine sahip olduğundan AES gibi simetrik anahtarlı uygulamalardan daha yavaş bir işlem hızına sahip olmasıdır. ECC algoritması, açık anahtarlı şifreleme türünün de en üstün algoritmasıdır. 300 bitle gerçeklenen bir ECC, gene aynı türde bulunan RSA algoritmasının 2000 bitle sağlayabildiği güvenliği sağlamaktadır [14]. Bu da ECC 'nin açık anahtarlı şifreleme türleri içersinde en çok güvenilen algoritma olmasını, dolayısıyla da en çok tercih edilen uygulama hüviyeti kazanmasını açıklamaktadır.

Sonuç olarak bu çalışmanın ortaya çıkardığı bir gerçek de RFID sistemlerinin yaygın bir kullanıma sahip olmalarına karşın çoğu uygulamada yetersiz güvenlik önlemleriyle donatılmış olduklarıdır. Bu sorunu aşmanın yolu olarak da şifreleme algoritmaları kullanılması gerektiğine işaret edilmekte ve çözüm olarak da ECC algoritmasının 160 bitin üstündeki bir uygulaması gösterilmektedir.

KAYNAKLAR

[1] **Finkenzeller, K. ,** 2003. RFID Handbook, Carl Hanser Verlag, Münih.

[2] **Lehpamer, H. ,** 2008. RFID Design Principles, Artech House, Norwood.

[3] **Weis, S. A. ,** 2003. Security and Privacy in Radio-Frequency Identification Devices, *Master Thesis*, MIT, Massachusetts

[4] **Brown, D. E. ,** 2007. RFID Implementation, McGraw-Hill, New York.

[5] **Peris, P. , Hernandez, J. C. , Estevez, J. M. ve Ribogardo, Arturo,** 2006. RFID Systems: A Survey on Security Threats and Proposed Solutions, Computer Science Department, Carlos III University of Madrid.

[6] **Parmar, A. , Byambajav, D. , Englert, B. ,** 2007. Evaluating and improving the security of RFID tags in shipping containers, Final Report on METRANS Project, California State University Long Beach.

[7] **Menezes, A. , van Oorschot, P. ve Vanstone, S. ,** 1996**.** Handbook of Applied Cryptography, CRC Press.

[8] **Symmetric-Key Algorithm.** http://en.wikipedia.org/wiki/Symmetric-key_algorithm

[9] **Wolkerstorfer, J. ,** 2005. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags?, *Workshop on RFID and Lightweight Crypto*, Graz University of Technology, Graz, Austria, July 13-15, s. 78-91.

[10] **Silicon Laboratories** C8051F060/1/2/3/4/5/6/7 datasheet http://www.keil.com/dd/docs/datashts/silabs/c8051f06x.pdf

[11] **HACCOM UM96** Datasheet / User Manual http://www.sparkfun.com/datasheets/RF/UM96_Tutorial_Manual.pdf

[12] **Batina, L. , Guajardo, J. , Kerins, T. , Mentens, N. , Tuyls, P. ve Verbauwhede, I. ,** 2006. An Elliptic Curve Processor Suitable For RFID-Tags, Katholieke Universiteit Leuven, ESAT/COSIC, Belçika ve Philips Araştırma Laboratuarları, Eindhoven, Hollanda

[13] **Yalçın, S. B. Ö.,** 2005. Hardware Design of Elliptic Curve Cryptosystems and Side-Channel Attacks, *PhD Thesis*, Katholieke Universiteit Leuven, Belçika.

[14] **Namin, A. H. ,** 2005. Elliptic Curve Cryptography, Research Centre for Integrated Microsystems, Electrical and Computer Engineering, University of Windsor.

ÖZGEÇMİŞ

İ. Kaan Bulut 1985 yılında İstanbul' da doğdu. Orta öğrenimini 2004 yılında İstanbul Erkek Lisesi'nde tamamladı , lisans öğrenimini ise 2008'de İTÜ Elektronik Mühendisliği bölümünde tamamlayacaktır. İngilizce ve almanca dillerini bilmektedir.

Mayıs 2008