İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

YAKIN ALAN HABERLEŞMESİ İLE GÜVENLİ UYGULAMALAR İÇİN DONANIM/YAZILIM ORTAK SİSTEM TASARIMI VE GERÇEKLENMESİ

YÜKSEK LİSANS TEZİ

Subutay Giray BAŞKIR

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

OCAK 2015

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

YAKIN ALAN HABERLEŞMESİ İLE GÜVENLİ UYGULAMALAR İÇİN DONANIM/YAZILIM ORTAK SİSTEM TASARIMI VE GERÇEKLENMESİ

YÜKSEK LİSANS TEZİ

Subutay Giray BAŞKIR
(504111218)

Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Elektronik Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Sıddıka Berna ÖRS YALÇIN

OCAK 2015

İTÜ, Fen Bilimleri Enstitüsü'nün 504111218 numaralı Yüksek Lisans Öğrencisi **Subutay Giray BAŞKIR**, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı **"YAKIN ALAN HABERLEŞMESİ İLE GÜVENLİ UYGULAMALAR İÇİN DONANIM/YAZILIM ORTAK SİSTEM TASARIMI VE GERÇEKLENMESİ"** başlıklı tezini aşağıda imzaları olan jüri önünde basarı ile sunmustur.

Tez Danışmanı :	**Doç. Dr. S. Berna ÖRS YALÇIN** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Güneş KARABULUT KURT** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Yard. Doç. Dr. Nerhun YILDIZ** Yıldız Teknik Üniversitesi	.....

Teslim Tarihi : **15 Aralık 2014**
Savunma Tarihi : **20 Ocak 2015**

Aileme,

ÖNSÖZ

Yüksek lisans eğitimimin başından sonuna geçen dönemde değerli vaktini benimle paylaşan, anlayışlı tavrı ve sağladığı imkanlar ile beni destekleyen saygıdeğer hocam ve tez danışmanım Doç. Dr. Sıddıka Berna Örs Yalçın'a teşekkürlerimi sunmayı bir borç bilirim.

Ayrıca bu çalışma süresince teknik ve manevi destekleriyle gerektiği her durumda yanımda olan arkadaşlarım; Akif Özkan ve Sercan Tuncay'a içten teşekkürlerimi sunarım.

Son olarak tüm eğitim ve çalışma hayatımından çok daha fazlasını kapsayan yaşantımın her evresinde yanımda olup beni destekleyen ve yol gösteren annem Aynur Başkır ve babam Levent Ülvi Başkır'a minnettar olduğumu belirtmek isterim.

Aralık 2014

Subutay Giray Başkır
Elektronik Mühendisi

İÇİNDEKİLER

Sayfa

ÖNSÖZ ..... **vii**
İÇİNDEKİLER ..... **ix**
KISALTMALAR ..... **xi**
ÇİZELGE LİSTESİ ..... **xiii**
ŞEKİL LİSTESİ ..... **xv**
ÖZET ..... **xvii**
SUMMARY ..... **xix**
1. GİRİŞ **1**
2. YAKIN ALAN HABERLEŞMESİ **5**
2.1 Yakın Alan Haberleşmesi Uygulamaları 8
2.1.1 Ödeme uygulamaları 8
2.1.2 Biletleme uygulamaları 8
2.1.3 Servis sorgulama uygulamaları 9
2.1.4 Eşten eşe bağlantı uygulamaları 9
2.2 Yakın Alan Haberleşmesi'ne Karşı Yapılabilecek Ataklar 9
2.2.1 Hattın dinlenmesi 9
2.2.2 Veri bozma 10
2.2.3 Veri değiştirme 10
2.2.4 Veri ekleme 10
2.2.5 Ortadaki adam saldırısı 10
3. MATEMATİKSEL ÖN BİLGİLER **13**
3.1 Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü 13
3.1.1 Davies-Meyer özet fonksiyonu 16
3.2 Küçük Şifreleme Algoritması 17
3.3 Doğrusal Geribeslemeli Kaydırma Yazmacı 21
4. GELİŞTİRME ORTAMI BİRİMLERİ **23**
4.1 TRF7970A Analog Uç Birimi 23
4.2 MSP430 Geliştirme Kiti 25
4.3 Digilent Atlys FPGA Geliştirme Kiti 26
5. YAKIN ALAN HABERLEŞMESİ GELİŞTİRME ORTAMI TASARIMI **33**
5.1 Yakın Alan Haberleşmesi Etkin Cihaz Alt Birimleri 33
5.2 NFC Alt Sistem Tasarımı ve Gerçeklenmesi 34
5.3 Kontrol Birimi Gerçeklemesi 38
5.3.1 MSP430 geliştirme kiti kontrol birimi ile tasarım 40
5.3.2 Atlys Spartan-6 geliştirme kiti kontrol birimi ile tasarım 43
6. DOĞRULAMA PROTOKOLÜNÜN GERÇEKLENMESİ **51**
6.1 Gerçeklenen Donanım Alt Modülleri 51
6.1.1 Küçük şifreleme algoritması modülleri 52
6.1.1.1 Kullanılan alt bloklar 52
6.1.1.2 Küçük şifreleme algoritmasi şifreleme modülü 53

6.1.1.3 Küçük şifreleme algoritmasi şifre çözme modülü 55
6.1.2 Özet fonksiyonu modülü 57
6.1.3 Doğrusal geribeslemeli kaydırma yazmacı modülü 59
6.2 Doğrulama Protokol Gerçeklemesi 60
6.3 Doğrulama Protokolünün NFC Veri Trasfer Akışı ile Entegrasyonu 62
7. SONUÇ VE ÖNERİLER 65
KAYNAKLAR 67
EKLER 71
EK A 73
EK B 75
EK C 77
EK D 79
ÖZGEÇMİŞ 81

KISALTMALAR

NFC	**:** Near Field Communication
KBPS	**:** Kilobit per Second
FPGA	**:** Field Programmable Gate Array
RF	**:** Radio Frequency
MITM	**:** Man in the Middle Attack
RFID	**:** Radio Frequency Identification
TEA	**:** Tiny Encryption Algorithm
P2P	**:** Peer to Peer
POS	**:** Point of Sale
TI	**:** Texas Instruments
LLCP	**:** Logical Link Control Protocol
NDEF	**:** NFC Data Exchange Format
SNEP	**:** Simple NDEF Exchange Protocol
RAM	**:** Random Access Memory
EDK	**:** Embedded Development Kit
SDK	**:** Software Development Kit
SPI	**:** Serial Peripheral Interface
UART	**:** Universal Asynchronous Receiver/Transmitter
USB	**:** Universal Serial Bus
I2C	**:** Inter-Integrated Circuit
FIFO	**:** First In, First Out
DEP	**:** Data Exchange Format

ÇİZELGE LİSTESİ

Sayfa

Çizelge 3.1 : Veri bankası etiket tablosu. 14
Çizelge 5.1 : Örnek NFC analog uç birimleri. 35
Çizelge 6.1 : TEA şifreleme modülüne dair giriş ve çıkış değerleri. 55
Çizelge 6.2 : TEA şifre çözme modülüne dair giriş ve çıkış değerleri. 57

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1 : İki aktif NFC cihazı arasında kurulan aktif haberleşme yapısı. 6
Şekil 2.2 : Aktif ve pasif cihazlar arasında kurulan pasif haberleşme yapısı. 6
Şekil 2.3 : NFC özellikli cihazlar için NFCIP-1 protokol akışı. 7
Şekil 2.4 : Ortadaki adam saldırısı. 11
Şekil 3.1 : Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü. 13
Şekil 3.2 : Davies-Meyer özet fonksiyonu blok diyagramı. 16
Şekil 3.3 : TEA şifreleme rutini. 18
Şekil 3.4 : TEA i. Döngüsü. 19
Şekil 3.5 : TEA şifre çözme rutini. 20
Şekil 4.1 : TRF7970A blok diyagramı. 23
Şekil 4.2 : TRF7970A uygulama devresi. 24
Şekil 4.3 : Kart emülasyon modu için NFC yığın mimarisi. 24
Şekil 4.4 : Eşten eşe bağlantı modu için NFC yığın mimarisi. 25
Şekil 4.5 : MSP430 geliştirme kiti. 26
Şekil 4.6 : Atlys FPGA geliştirme kartı. 27
Şekil 4.7 : Microblaze mimarisi. 28
Şekil 4.8 : Xilinx araçlarının gömülü sistem tasarım aşamalarında kullanımı. 29
Şekil 4.9 : XPS ekran görüntüsü. 30
Şekil 4.10 : SDK programına ait ekran görüntüsü. 31
Şekil 5.1 : NFC alt sistem ve kontrol birimi. 34
Şekil 5.2 : NFC Alt Sistem Kartı blok diyagramı. 36
Şekil 5.3 : NFC anten yapısı. 37
Şekil 5.4 : TI firması tarafından önerilmiş NFC anten yapısı. 37
Şekil 5.5 : NFC Alt Sistem Kartı tasarım görüntüsü. 38
Şekil 5.6 : Dizgi işlemi tamamlanmış NFC Alt Sistem Kartı. 38
Şekil 5.7 : MSP430 geliştirme kartı ile gerçeklenen tasarım platformu blok diyagramı. 40
Şekil 5.8 : MSP430 geliştirme kartı ile gerçeklenen tasarım platformu. 40
Şekil 5.9 : Kart emülasyon modu protokol katmanları. 41
Şekil 5.10 : Kart emülasyon modu akış diyagramı. 41
Şekil 5.11 : SM130 modülü ile KGS kartı kimlik bilgisi okunması. 42
Şekil 5.12 : SM130 modülü, MSP430 geliştirme kiti kontrol birimi ve NFC Alt Sistem Kartı'nın birlikte çalıştırılması. 42
Şekil 5.13 : NFC Alt Sistem Kartı ve Atlys Spartan-6 geliştirme kiti kontrol birimi yapısı. 43
Şekil 5.14 : NFC Alt Sistem Kartı ve Atlys Spartan6 geliştirme kiti kontrol birimi. 44
Şekil 5.15 : Eşten eşe modu için Microblaze işlemcisi ve çevre birimlerine dair blok diyagram. 45
Şekil 5.16 : Eşten eşe bağlantı modu protokol katmanları. 46
Şekil 5.17 : Eşten eşe bağlantı modu akış diyagramı. 47

Şekil 5.18 : Eşten eşe bağlantı modu ile NFC özellikli cep telefonuna aktarılmış JPG formatlı resim dosyası. 47
Şekil 5.19 : Eşten eşe bağlantı modu ile NFC etkin bir cep telefonuna resim dosyası aktarımı. 48
Şekil 5.20 : İki adet Atlys Spartan-6 geliştirme kiti kontrol birimi ile NFC alt sistem kartı ikilisi kullanılarak gerçekleştirilen eşten eşe bağlantı görüntüsü... 49
Şekil 6.1 : Saat işaretli TEA şifreleme modülü. 54
Şekil 6.2 : Saat işaretli TEA şifre çözme modülü. 55
Şekil 6.3 : Özet fonksiyonu modülü 58
Şekil 6.4 : Doğrusal geri beslemeli kaydırma yazmacı bloğu. 59
Şekil 6.5 : Doğrulama protokolü gerçeklemesi için Microblaze işlemcisi ve çevre birimlerine dair blok diyagram. 60
Şekil 6.6 : NFC eşten eşe modu için düzenlenen doğrulama protokolü adımları. 61
Şekil 6.7 : Cihazlar arası anahtar paylaşımına dair ekran görüntüsü. 62
Şekil 6.8 : NFC ile güvenli haberleşme kanalı üzerinden veri aktarımına dair protokol akışı. 63
Şekil 6.9 : Doğrulama protokolü sonrasında NFC eşten eşe haberleşmesine dair mesaj akışı. 64
Şekil A.1 : NFC Alt Sistem Kartı şematik tasarımı. 73
Şekil B.1 : Saat işaretli TEA şifreleme modülü simülasyon sonuçları. 75
Şekil C.1 : Saat işaretli TEA şifre çözme modülü simülasyon sonuçları. 77
Şekil D.1 : Özet fonksiyonu modülü simülasyon sonuçları. 79

YAKIN ALAN HABERLEŞMESİ İLE GÜVENLİ UYGULAMALAR İÇİN DONANIM/YAZILIM ORTAK SİSTEM TASARIMI VE GERÇEKLENMESİ

ÖZET

Yakın alan haberleşmesi (Near Field Communication - NFC) kısa mesafelerde bilgi alışverişini sağlayan bir kablosuz haberleşme teknolojisidir. Bu haberleşme sisteminin en önemli özelliği cep telefonuna entegre bir biçimde kullanıma olanak sağlamasıdır. Günümüzde yaygınlaşmış cep telefonu kullanımı göz önünde bulundurulduğunda NFC birçok kullanım alanında kullanıcılara daha öncesinde üstlerinde taşımak zorunda oldukları kart veya bilet gibi ödeme ya da geçiş için kullanılan cihazları kullanmadan zaten sürekli yanlarında taşıdıkları bir cep telefonu ile bu işleri yerine getirmelerine imkan vermektedir. Bu teknoloji ülkemiz dâhilinde pek sıklıkla olmasa da hali hazırda birçok ülkede ödeme, ulaşım, kontrollü giriş çıkış gibi birçok uygulama alanında kullanılmaktadır. Ancak NFC'nin kullanıldığı bu uygulamalar güvenlik açısından incelediğinde ve çeşitli saldırılara tabi tutulduğunda sahip olduğu güvenlik açıkları ortaya çıkmaktadır. Literatürde işlenen güvenlik açıkları iki NFC özellikli cihazın arasındaki haberleşmenin dinlenmesi, veri bozulması, veri eklenmesi ve veri değiştirilmesidir.

Bu tez çalışmasında söz konusu ataklara karşı NFC özellikli cihazların güvenli bir haberleşme kanalı üzerinden veri aktarmalarına imkan sağlayacak bir sistem tasarımı ve gerçeklemesi yapılmıştır.

Tasarımın NFC standartlarına sadık kalınarak yapılması amacıyla öncelikle bir gerçekleme ortamı altyapısı oluşturulmuştur. Bu alt yapı içerisinde bir NFC özellikli cihazın içinde bulunan NFC teknolojisi ile ilişkili alt birimlere karşılık düşecek iki adet haberleşme kartı tasarlanmış ve gerçeklenmiştir. Bu kartlar ile birlikte NFC kontrol birimi için iki adet FPGA geliştirme kartı üzerinde Microblaze işlemcisi kullanılmış ve NFC kontrol birimi yazılım tasarımı yapılmıştır. Yapılan tasarımların entegre edilmesi ile birimler arasında kablosuz NFC veri transfer hattı kurulmuştur.

Söz konusu haberleşme kanalının güvenli hale getirilmesi amacıyla donanım / yazılım ortak sistem tasarımı yöntemi ile FPGA üzerinde bir doğrulama protokolü gerçeklenmiştir. Bu aşamada cihazlar arasında NFC bağlantısı kurulmasından önce karşılıklı olarak cihazların doğrulanması ve anahtar paylaşımı gerçekleştirilmiştir. Bu amaç doğrultusunda gerçeklenen donanım kısmında kapı seviyesinde çeşitli kriptografik algoritmalar, yazılım kısmında ise donanım olarak gerçeklenen kriptografik algoritmaların kullanılmasıyla söz konusu doğrulama protokolu gerçeklenmiştir. Sonrasında bu doğrulama protokolü NFC veri transfer akışı ile entegre edilmiş, haberleşme akışı dahilinde aktarılan mesaj, doğrulama protokolünün çalıştırılmasıyla üretilen anahtarlar kullanılarak şifreleme ve şifre çözme işlemlerine tabi tutulmuştur. Bu yol ile NFC özellikli birimler arasında güvenli bir haberleşme kanalı üzerinden veri aktarımı gerçekleştirilmiştir.

HARDWARE/SOFTWARE CODESIGN AND IMPLEMENTATION FOR SECURE NEAR FIELD COMMUNICATION APPLICATIONS

SUMMARY

Near Field Communication (NFC) is a wireless communication technology, which provides short distance data, sharing. The capability of mobile phone integrated usage is the most important feature of this communication system. Considering the usage of mobile phone at the present time; NFC provides a system that people can use their mobile phones in many different application areas instead of carrying a large number of cards which are credit cards, tickets for payments or access control devices. Although in Turkey, this protocol has not a wide usage area, in many countries people perform various activities such as payment and ticketing by using that technology. On the other hand, when the applications, which depend on NFC technology, are investigated by being exposed to cryptographic experiments and attacks; it is seen that this technology has severe vulnerabilities. In the literature, related vulnerabilities are investigated as eavesdropping, data corruption, data insertion and data modification.

In this thesis, a system design and implementation is carried out for secure data transfer between NFC enabled devices over a secure communication channel in order to prevent the attacts, which are mentioned.

In order to make the design appropriate to NFC standards, primarily an implementation environment infrastructure is built. For this infrastructure, two communication cards are designed and implemented.

These cards, which are called NFC subsystem cards, are equvalent to NFC enabled devices' NFC subsystem. Analog front end and NFC antenna are the main parts of these cards. For the analog front end integrated circuit a product of Texas Instruments which is called TRF7970A is preffered by comparing other similar products. For NFC antenna design NFC Forum POLLER-3 type antenna is implemented on printed circuit board.

Along with communication cards, two different NFC control unit software are designed besides. At the first design, NFC card emulation mode protocol layers are implemented on a microcontroller development kit. After integrating that control unit and NFC subsystem card, this system is tested and verified by a trusted NFC reader module. Then, NFC peer to peer mode protocol layers are implemented on Microblaze soft core processor on a Field Programmable Gate Array (FPGA) development kit. By integrating that control unit and NFC subsystem card, this system is communicated with a NFC enabled smartphone and executed an image transfer. At the final phase of this part, two NFC subsystem cards and two control units designed on FPGA development kits are communicated each other with NFC peer to peer mode and executed an image transfer.

For the secure communication channel, a mutual authentication protocol is implemented on FPGA by using hardware/software codesign methode and integrated with NFC data transfer flow.

Hash based Radio Frequency Identification (RFID) mutual authentication protocol, which is proposed by Dehkordi, and Farzaneh is preferred for mentioned authentication process. This protocol is an improved version of Cho et al.'s protocol and has similar properties. It consist of eight phases and operates between three units, which are back-end server, reader and tag. These three units can be called RFID system members also. In order to implement this protocol on the NFC devices, which communicate each other with peer-to-peer mode, protocol is slightly modified. This modification is made by combining the phases, which are performed by back-end server and reader on NFC initiator device. The phases of tag are performed on NFC target device without modification.

Implementation of the authentication protocol includes cryptographic algorithms. These algorithms consist of hash function generation, encryption and random number generation. These algorithms are implemented on hardware side of the design.

Hash function generation is implemented by using the algorithm, which is called The Davies-Meyer hash function. This function is a construction for a hash function based on a block cipher, where the length in bits of the hash result is equal to the block length of the block cipher.

Tiny Encryption Algorithm (TEA) is used for implementing the block cipher. This algorithm is a Fiestel type cipher that uses operations from mixed algebraic groups with 64 rounds. TEA has two inputs, which are 64 bit data and 128 bit key. Implementation of this block cipher includes adder, substracter, logical shift and exclusive or submodules.

The phases of authentication protocol where hash function is used, hash function input length is defined 192 bit. Because of that reason, Davies-Meyer hash function operates two rounds. At each round of hash function, block cipher TEA operates 64 rounds. The output of hash function is 64 bit length. For being compatible with Microblaze, input and output values of hash function are divided to 32 bit length parts.

Tiny Encryption Algorithm is not only used for hash function generation. This algoritihm is used for enrcrpyting the data, which is send at NFC data transfer stage. Moreover, TEA decrypting module is implemented similarly to encryption module for decrypting the message which is formatted by NFC Data Exchange Format (NDEF).

Linear feedback shift registers are used for implementing random number generator. 96 bit random number generator is implemented which is defined at authentication protocol phases. This module generates a new 96-bit random number at each clock cycle by using a seed value and processing shift and exclusive or operations. Also this module's output is divided to 32 bit length parts in order to be compatible with Microblaze.

By accessing the hardware modules, which are hash function generation, encryption and random number generation modules, authentication protocol phases are implemented on Microblaze soft core processor.

After the stage of implementing authentication protocol, this protocol is integrated with NFC data transfer flow. Integration is made by operating mutual authentication protocol before NFC data transfer flow. With that design, primarily units mutually authenticate. After the success of this operation NFC data transfer flow processes execute, otherwise communication is terminated. Before the NFC data transfer stage, message is encrypted with TEA by using the secret values, which are generated at authentication stage as key. Similarly, message is decrypted with the same key value by the receiver unit which is uniquely generated for only the current session.

In this thesis, additionally to the implementations, the topics of NFC technology's technical properties, application areas, possible attack types to communication channel, technical requirements of communication channel implementation are detaily researched.

Implementation environment infrastructure's application and protocol layers are designed with a modifiable point of view. Thus, this infrastructure can be easily used for different application and protocol implementations.

1. GİRİŞ

Gelişen teknoloji ve değişen yaşam koşulları ile beraber, kişisel cüzdanlarda taşımak durumunda kalınan elektronik kartların sayısı gün geçtikçe artış göstermektedir [1]. Söz konusu kartlardan birçoğu yalnızca bir amaç doğrultusunda kullanım gösterebilmektedir. Güncel şartlar altında kullanılan bu kartlara örnek vermek gerekirse, toplu taşıma, kartlı geçiş sistemleri, öğrenci kimlikleri, ödeme işlemleri gibi uygulamaların her biri için farklı kartları aynı anda taşınması ve kullanılması bir zorunluluk haline gelmiştir.

Söz konusu elektronik kartlar ile yapılan işlem ve uygulamaların tek bir cihaz ile gerçekleştirilebilme düşüncesi Yakın Alan Haberleşmesi'nin (Near Field Communication – NFC) getirdiği önemli bir yeniliktir [2]. Bu yenilik ile NFC teknolojisi kullanılarak bahsedilen uygulamaların gündelik kullanımı oldukça yaygınlaşmış olan cep telefonları ile gerçekleştirilmesi mümkün kılınmıştır.

Yakın Alan Haberleşmesi bir kısa mesafeli kablosuz haberleşme protokolüdür [3, 4]. Bu teknoloji 13.56 MHz çalışma frekansında saniyede 424 kbps'e kadar veriyi aradaki mesafe en fazla 10 cm olacak şekilde cihazlar arasında aktarılmasını mümkün kılar [2, 5].

NFC teknolojisinin kullanım alanlarına örnekler aşağıda sıralanmıştır [6].

- Fransa; Ulaşım, ödeme, akıllı poster, öğrenci kimlikleri, müze ve sergilerde rehberlik uygulamaları
- İspanya; Ulaşım uygulamaları
- Hollanda; Stadyum ve sinemalarda bilet uygulamaları,
- Belçika; Ödeme uygulamaları
- Avusturya; Ulaşım ve ödeme uygulamaları
- Almanya; Ulaşım, müze ve sergilerde rehberlik uygulamaları

- İngiltere; Stadyumlarda biletleme, ulaşım, öğrenciler için servis kullanımı ve kişisel sağlık servisi uygulamaları
- Finlandiya; Ulaşım uygulamaları
- İtalya; Kayak merkezlerine giriş kontrolü uygulaması

NFC teknolojisinin 2016 sonuna kadar dünya çapında yaygınlaşarak 448 milyon kullanıcıya ulaşması ve 617 milyar dolarlık mobil ödeme işleminin bu cihazlarla gerçekleşmesi beklenmektedir [7]. Bununla beraber sektörde söz sahibi olan cep telefonu üreticilerinin üretilen cep telefonlarının içerisine NFC özelliğini destekleyecek donanım birimlerini koyarak bu teknoloji için gerekli alt yapıyı sağladıkları gözükmektedir.

Uygulama alanlarına bahsedildiği üzere ödeme uygulamalarında NFC teknolojisinin ne denli sık bir şekilde kullanıldığı ve kullanılması beklendiği gözükmektedir. Literatürde NFC özellikli cihaz yapılabilecek ataklara dair çalışmalar yapılmıştır [8, 9]. Bu kaynaklarda belirtilen NFC özellikli cihazlara yapılabilecek ataklar aşağıdaki gibi sıralanabilir.

- Hattın dinlenmesi
- Veri bozma
- Veri değiştirme
- Veri ekleme
- Ortadaki adam saldırısı

Bu tez çalışmasının ilk amacı; Yakın Alan Haberleşmesi için bir geliştirme ortamı tasarımı ve gerçeklemesi yapmak ve bu gerçekleme sonrasında söz konusu geliştirme ortamı üzerinde bir güvenlik protokolü gerçeklenerek dinlenme, veri değiştirme, veri ekleme ve ortadaki adam saldırısı gibi birçok atak yöntemlerine karşı NFC özellikli cihazlar arasında güvenli bir kablosuz hat kurulmasıdır.

Çalışmanın ikinci amacı ise, söz konusu gerçeklemeleri yeni bir tasarım yöntemi olan donanım/yazılım ortak tasarım ile tasarlamak ve karşılıklı haberleşen iki FPGA üzerinde gerçeklemektir. Söz konusu gerçekleme aşamasında gerçeklenen çözümün etiket gibi içerisinde kriptografi algoritmaları için sınırlı hafıza alanı ve işlem

kabiliyetinde olan cihazlar için de uygulanabilir bir seviyede olması bir diğer önemli hedeftir.

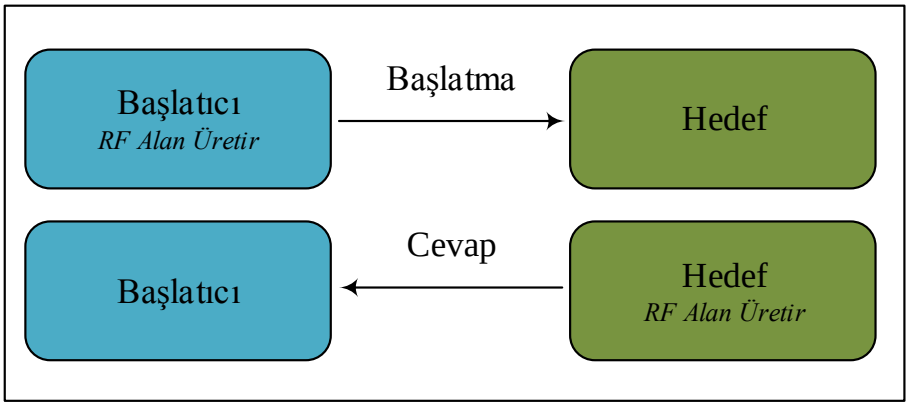
Bu tez çalışması kapsamında öncelikle NFC teknolojisi ile ilişkili uygulama alanlarına, haberleşme kanalına uygulanabilecek ataklara ve haberleşme kanalını gerçeklemek için kullanılacak teknik gereksinimlere dair temel bilgiler paylaşılacaktır. Sonrasında gerçeklenecek protokol, beraberinde kullanılacak şifreleme algoritması ve diğer alt bileşenler anlatılacaktır. Sonraki bölümlerde ise tasarlanan geliştirme altyapısı ve protokol gerçeklemesi anlatılacaktır.

2. YAKIN ALAN HABERLEŞMESİ

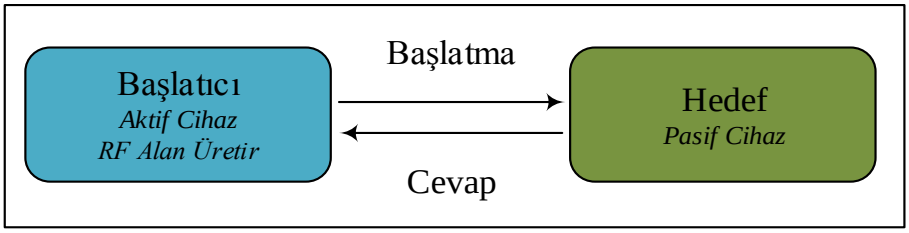
Yakın Alan Haberleşmesi bir kısa mesafeli kablosuz haberleşme protokolüdür [3, 4]. Philips ve Sony firmaları tarafından ortaklaşa geliştirilmiş olan bu teknoloji ile cihazlar arasında 13.56 Mhz radyo frekansı haberleşme bandında saniyede 424 kilobit'e kadar veriyi aradaki mesafe en fazla 10 cm olacak şekilde iletilebilmektedir [2, 5].

Söz konusu teknoloji Uluslararası Standartlar Teşkilatı/Uluslararası Elektroteknik Komisyonu tarafından ISO/IEC 18092 ve ISO/IEC 21481 kodlu standartlar ile standartlaştırılmıştır [3, 4]. NFC'nin standartlaşması sonrasında bu teknolojinin geliştirilmesi ve yaygınlaştırılması amacıyla Nokia, Sony ve NXP firmaları tarafından NFC Forum kurulmuştur [2].

NFC teknolojisinin çalışma prensibine değinmek gerekirse NFC özellikli cihazlar iki kategoride incelenebilir. Bunlardan ilki pasif NFC cihazı diğeri ise aktif NFC cihazıdır [3]. Pasif cihaz içerisinde herhangi bir güç kaynağı barındırmayan bir yapıya sahiptir. Haberleşeceği cihazın elektromanyetik alanına girdiği durumda anteni üzerinde indüklenen enerji ile beslenerek üzerinde bulunan elektronik birimleri çalıştırır ve haberleşmenin kurulmasını sağlar. Aktif cihaz ise yapısında kendi güç kaynağına sahip olan cihaz tipidir. Aktif cihazlar istenildiği durumda kendi elektromanyetik alanlarını oluşturarak pasif cihazlar ile ya da başka bir aktif cihazın elektromanyetik alanına girdiğinde aktif cihazlar ile haberleşme sağlayabilirler. İki pasif cihazın kendi aralarında haberleşme kurması mümkün değildir. Pasif cihaz için NFC etiketleri, aktif cihaz için ise NFC özellikli bir cep telefonu örnek olarak gösterilebilir. Aktif ve pasif cihazların birbirleri ile haberleşmesi Şekil 2.1 ile iki aktif cihazın birbiri ile haberleşmesi ise Şekil 2.2 ile gösterilmiştir.



Şekil 2.1 : İki aktif NFC cihazı arasında kurulan aktif haberleşme yapısı.



Şekil 2.2 : Aktif ve pasif cihazlar arasında kurulan pasif haberleşme yapısı.

NFC teknolojisi aşağıda sıralandığı gibi üç farklı çalışma modunda veri iletişimi gerçekleştirir [10].

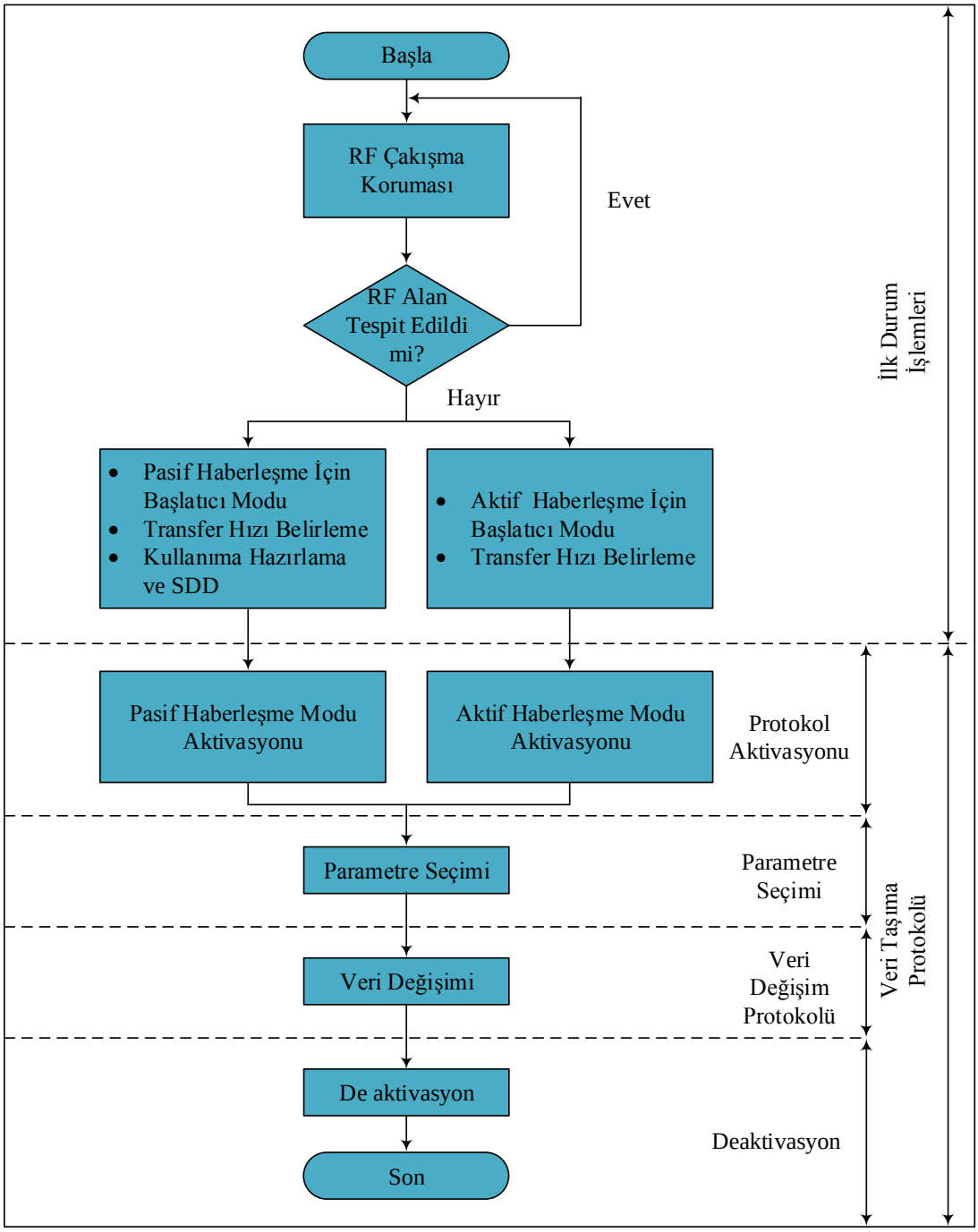
- Okuyucu/yazıcı modu (reader/writer mode)
- Kart emülasyon modu (card emulation mode)
- Eşten eşe bağlantı modu (peer to peer mode)

Okuyucu/yazıcı modunda NFC özellikli cihaz ISO14443 ile tanımlanmış standart ile uyumlu çalışarak pasif etiketler ile haberleşme gerçekleştirebilir [11-14]. Akıllı poster bu modun kullanımı ile alakalı örneklerdendir [15].

Kart emülasyon modunda NFC cihaz ISO14443 standardı ile tanımlanmış pasif bir akıllı kart davranışı sergiler. Bu çalışma modu kullanılarak NFC özellikli cihaz ile NFC okuyucu arasında bağlantı kurularak temassız ödeme ve elektronik biletleme uygulamaları gerçeklenebilir [16].

Eşten eşe bağlantı modunda ise ISO/IEC 18092 ile standartlaştırılmış yapı ile NFC özellikli aktif cihazlar arasında bağlantı kurularak iki yönlü veri aktarımı gerçekleştirilebilir [3]. Örnek olarak birbirlerine yaklaştırılan iki NFC özellikli cep telefonu arasında bu mod ile veri paylaşımı gerçekleştirilebilir.

Değinilen çalışma modlarına dair NFC özellikli cihazlar arasında haberleşme kurulması için haberleşme adımlarına dair ortak bir protokol akışı tanımlamıştır [3]. Söz konusu protokol akışı Şekil 2.3 ile verilmiştir.



Şekil 2.3 : NFC özellikli cihazlar için NFCIP-1 protokol akışı.

2.1 Yakın Alan Haberleşmesi Uygulamaları

NFC ile gerçeklenebilecek temel olarak dört mobil uygulama vardır. Bu uygulamaların bazılarında NFC cihazı okuyucu modunda, bazılarında kart emülasyon modunda çalışma gerçekleştirir [6].

2.1.1 Ödeme uygulamaları

NFC'nin en önemli uygulaması olan ödeme uygulaması mobil ödeme, elektronik cüzdan, mobil cüzdan gibi isimlerle de kullanılmaktadır. Temelde kredi kartı yerine bir cep telefonunun bir okuyucuya yaklaştırılarak ödeme yapılması esasına dayanır. Burada telefonun etiket olarak kullanılması durumu söz konusudur. Telefonda bankaya ait bir kart numarası bilgisi taşınır [6].

NFC ile mobil ödeme uygulamaları son kullanıcılara çok büyük avantajlar sağlar, yanlarında farklı bankaların kartlarını taşımak yerine zaten sürekli yanlarında olan cep telefonlarıyla alışverişlerini güvenli bir şekilde gerçekleştirebilirler.

2.1.2 Biletleme uygulamaları

NFC'nin en yaygın olarak kullanılan uygulaması olan bilet uygulaması günlük hayatta birçok kolaylık sağlamaktadır. Bu uygulama esasen telefonun içinde bir miktar para tutulmasına ve bu parayla ödeme yapılmasına dayanır. Burada da cep telefonu kart emülasyon modu ile etiket gibi kullanılır [6].

Özellikle Avrupa ülkelerinde ulaşımda oldukça fazla kullanılan bu uygulama sayesinde bilet kuyruklarında sıra beklemek veya sürekli ekstra bir ulaşım kartı taşımak gibi zorluklardan kurtulup sadece cep telefonuyla kolayca ödeme yapılabilir.

Bilet uygulamasının tek geçerli olduğu yer ulaşım alanı değildir. Spor müsabakalarının yaygın olduğu yerlerde stadyumlara veya kapalı spor salonlarına girişte de kullanılabilir. Bunun yanında bu uygulamaya geçen sinemalarda sinema biletleri de bu şekilde alınabilir. Ayrıca müze ve sergilere giriş için müze kart gibi kullanılabilir.

Bu teknolojinin yaygınlaşması durumunda kampüs kart taşımak yerine cep telefonlarıyla kampüsün her yerinde, bütün imkânlardan yararlanabilmek öğrencilere çok büyük kolaylık sağlayacaktır. Üniversite yemekhanesinde, kütüphanesinde, spor

tesislerinde, havuzunda ve cüzi miktarlarda para ödenen birçok yerde sadece cep telefonları kullanılarak hizmet alınabilecektir.

2.1.3 Servis sorgulama uygulamaları

Servis sorgulama, bir diğer adıyla akıllı poster uygulaması NFC teknolojisinin günlük hayata getireceği en büyük yeniliklerden biridir. Ödeme ve bilet uygulamalarından farklı olarak burada NFC özellikli cep telefonu kart emülasyon modu yerine NFC okuyucu/yazıcı modunda kullanılır [6].

Bu uygulamanın kullanıldığı en önemli alanlardan biri olan turizm alanında, müze ve sergilerde eserlerin yanında bir etiket bulunur. Telefonu bu etikete yaklaştırınca eser hakkında bilgi telefon ekranına düşer böylece eser hakkında rehberlik hizmeti alınmış olur.

2.1.4 Eşten eşe bağlantı uygulamaları

Bu uygulama biçiminde ise diğer uygulama biçiminde kullanılan çalışma modlarından farklı olarak NFC cihazlar eşten eşe bağlantı modunda çalıştırılırlar. Söz konusu uygulama biçimi ile aynı modda çalıştırılan iki NFC özellikli cep telefonu birbirlerine yaklaştırılarak herhangi bir formatta veri paylaşımı gerçekleştirilebilir.

2.2 Yakın Alan Haberleşmesi'ne Karşı Yapılabilecek Ataklar

NFC özellikli cihazlara yapılabilecek ataklar literatürde incelenmiştir [8, 9]. Bu bölümde NFC teknolojisine karşı gerçekleştirilebilecek atak çeşitleri sıralanacak ve açıklanacaktır.

2.2.1 Hattın dinlenmesi

Atak yapan kişi veya cihaz da bir anten kullanıp gönderilen işareti alabilir. Deney yaparak veya iyi bir literatür araştırması ile aldığı RF işaretinden gönderilen sayısal veriyi çıkarabilir. RF işaretini ölçmek ve RF işaretinden sayısal veriyi çıkarmak için gereken cihazlar pek çok laboratuvarda bulunabilen, çok da özel olmayan cihazlardır. Bu sebeple atak yapmak isteyen herkesin bu cihazlara sahip olabileceğini varsaymak gerekir.

Görüldüğü gibi hattın dinlenmesini önlemek mümkün değildir. Esas olan RF işaretinden çıkarılan sayısal veriden gizli verilerin elde edilememesini sağlamaktır. NFC ile haberleşen iki taraf arasında kurulacak güvenli kanal bu problem için görünen bir çözümdür.

2.2.2 Veri bozma

Atak yapan kişi sadece veriyi dinlemek yerine bozmayı hedefleyebilir. En basit durumda haberleşmeyi bozarak alıcının veriyi anlamamasını sağlayabilir. Veri bozma gönderici ile aynı anda frekansta rastgele işaret göndererek yapılabilir. Atak yapan kişi kullanılan modülasyon ve kodlama yöntemi konusunda bilgi sahibi ise doğru anı kolayca tespit edebilir.

Bu atak gönderilen verilerin değiştirilmesini sağlamaz. Bu sebeple kullanıcının bir kayba uğraması söz konusu değildir. Ancak servisi engelleme özelliği vardır.

2.2.3 Veri değiştirme

Bu atağın başarım oranı tamamen kullanılan genlik modülasyon yöntemine bağlıdır. Miller kodlama yönteminde bazı bitlerin değiştirilmesi mümkünken, Manchester kodlamada bitlerin tamam değiştirilebilir.

Verinin değiştirilmesini engellemenin veya değişimin fark edilmesinin yolu yine anahtar paylaşımı kullanılarak iki taraf arasında güvenli kanal oluşturmaktır.

2.2.4 Veri ekleme

Burada atak sahibinin amacı veriyi sadece rastgele değiştirmek değil, göndericinin hiç göndermediği bir veriyi alıcıya göndermektir. Bu atağın başarılı olması için atak yapanın veri göndermeye, göndericiden önce başlaması gerekir.

Veri eklenmesini engellemenin veya eklendiğinin fark edilmesinin yolu yine iki taraf arasında güvenli kanal oluşturmaktır.

2.2.5 Ortadaki adam saldırısı

Ortadaki adam saldırısı (Man in the Middle Attack - MITM) aktif hat dinlemeye bir örnektir. Bu atakta ortadaki kişi gönderici ve alıcı ile birbirinden bağımsız bağlantılar kurar ve tarafları birbirleriyle haberleştiklerine inandırır. Alıcı ve verici güvenli kanaldan doğrudan haberleştiklerini düşünürken, aslında bütün haberleşme ortadaki

atak yapan tarafından kontrol edilir. Şekil 2.4 ile ortadaki adam saldırısına örnek bir yapı gösterilmiştir [17].

Şekil 2.4 : Ortadaki adam saldırısı.

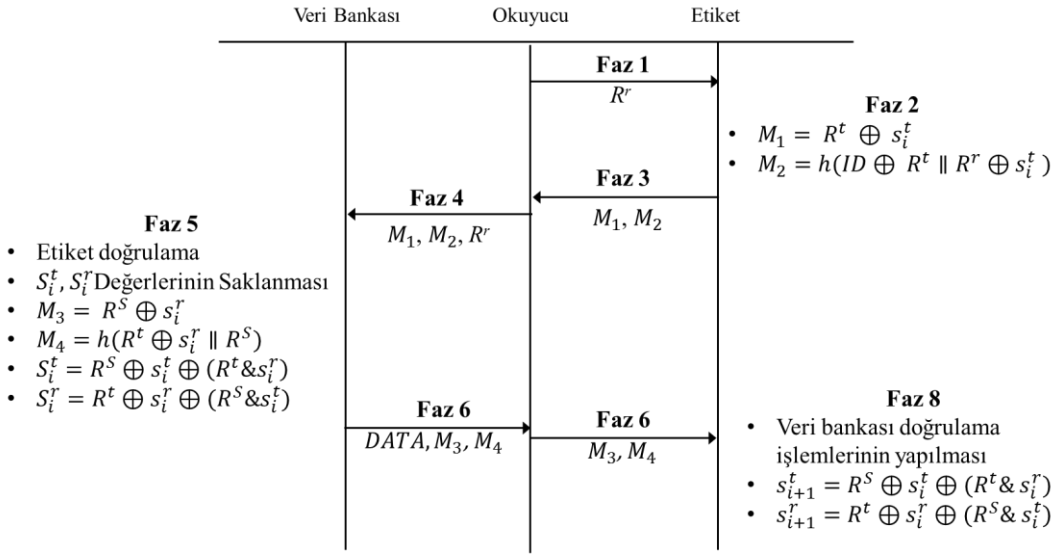
Ataklar konusundaki çalışmalarda bu atağın radyo frekansı ile haberleşen sistemler için geçerli olamayacağı, çünkü radyo dalgalarının sadece ortadaki adama değil aynı zamanda alıcıya da ulaşılacağı bildirilmiştir [8]. Ancak burada atağın sadece iki taraf arasındaki kablosuz kanala yapılabileceği varsayımı yapılmıştır.

Bu tez çalışmasında NFC ile haberleşebilen bir cep telefonunda güvenli NFC protokollerinin gerçeklenmesi hedeflenmektedir. Bu durumda cep telefonunun NFC katına işletim sistemi üzerinden ulaşılacaktır. Bu da kontrol altında olmayan işletim sisteminin ve uygulamaların ortadaki adam atağını yapabilmesi durumunu ortaya çıkarmaktadır.

3. MATEMATİKSEL ÖN BİLGİLER

3.1 Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü

Literatürde önerilen karşılıklı doğrulama protokolleri incelendiğinde protokoller arasında en güncel olanının Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü olduğu görülmüştür [18]. Okuyucu, etiket ve veri bankası arasında gerçekleşen söz konusu doğrulama protokol adımları Şekil 3.1 ile gösterilmiştir.



Şekil 3.1 : Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü.

Protokol adımları aşağıdaki gibi detaylandırılabilir;

- Okuyucu bir rastgele sayı üretir.
- Okuyucu ürettiği rastgele sayı R^r ile karşı tarafa istek mesajı gönderir.
- Etiket istek mesajını yakalar.
- Etiket bir rastgele sayı üretir.
- Etiket ürettiği rastgele sayı R^t ve kayıtlı tuttuğu gizli sayı s^t_i kullanılarak Denklem 2.1 ile M_1 değerini üretir.

$$M_1 = R^t \oplus s_i^t \qquad \textbf{(2.1)}$$

- Etiket kayıtlı tuttuğu kimlik verisi *ID*, gizli sayı s^t_i, üretilen rastgele sayı R^t ve karşı taraftan alınan rastgele sayı R^r'yi özet fonksiyonu *h( )* girişine uygulanarak Denklem 2.2 ile M_2 değerini üretir.

$$M_2 = h(ID \oplus R^t \parallel R^r \oplus s_i^t) \quad \textbf{(2.2)}$$

- Etiket M_1 ve M_2 değerlerini karşı tarafa gönderir.
- Okuyucu M_1 ve M_2 değerlerini yakalar.
- Okuyucu R^r, M_1 ve M_2 değerlerini veri bankasına iletir.
- Veri bankası sahip olduğu

$$R^{t\prime} = M_1 \oplus s_i^t \quad \textbf{(2.3)}$$

- Çizelge 3.1'de verilen biçimdeki etiket tablosundaki verilerden s^t_i gizli sayılarını kullanarak Denklem 2.3 uyarınca tabloda tanımlanmış her etiket için bir $R^{t'}$ değeri hesaplar.

$$R^{t\prime} = M_1 \oplus s_i^t \quad \textbf{(2.3)}$$

Çizelge 3.1 : Veri bankası etiket tablosu.

ID	s^t_i	s^r_i	s^t_{i-1}	s^r_{i-1}	*DATA*

- Veri bankası hesaplanan $R^{t'}$değeri, tabloda $R^{t'}$ değerinin hesaplanması sırasında kullanılan etikete karşılık düşen *ID*, s^t_i ve okuyucu tarafından üretilen R^r değerlerini özet fonksiyonunu kullanarak Denklem 2.4 uyarınca M_2'değerini üretir.

$$M_2' = h(ID \oplus R^{t\prime} \parallel R^r \oplus s_i^t) \quad \textbf{(2.4)}$$

- Veri bankası M_2 ve M_2' değerleri birbirlerine eşit olana dek yukarıdaki iki adımı tekrar eder, eşitlik sağlandığında etiket bulunmuş olur.
- Eğer veri bankası etiketi bulmuş ise aşağıdaki adımlar gerçeklenir;
    - Veri bankası bir rastgele sayı üretir; R^s
    - Veri bankası Denklem 2.5 uyarınca M_3 değerini üretir

$$M_3 = R^S \oplus s_i^r \quad \textbf{(2.5)}$$

- Veri bankası Denklem 2.6 uyarınca M_4 değerini üretir

$$M_4 = h(R^t \oplus s_i^r \parallel R^S) \quad \textbf{(2.6)}$$

- Veri bankası Denklem 2.7 ile gösterilen veriyi okuyucuya gönderir.

$$DATA \parallel M_3 \parallel M_4 \quad \textbf{(2.7)}$$

- Veri bankası etikete ait gizli değerleri S^t_{i-1} ve S^r_{i-1} değerlerine kaydeder.
- Veri bankası etikete ait gizli değerleri Denklem 2.8 ve Denklem 2.9 uyarınca günceller.

$$S_i^t = R^S \oplus s_i^t \oplus (R^t \& s_i^r) \quad \textbf{(2.8)}$$

$$S_i^r = R^t \oplus s_i^r \oplus (R^S \& s_i^t) \quad \textbf{(2.9)}$$

- Eğer veri bankası etiketi bulamamış ise etiket tablosunda bulunan S^t_{i-1} ve S^r_{i-1} değerler ile yukarıdaki işlemleri tekrar eder.
  - Bu durumda da etiket bulunamaz ise haberleşme bu aşamada sonlandırılır.
- Okuyucu Denklem 2.7 ile gösterilen veriyi alması durumunda haberleşmeyi sürdürür ve veri bankasından aldığı M_3 ve M_4 değerlerini etikete iletir.
- Etiket M_3 ve M_4 değerlerini yakalar.
- Etiket Denklem 2.10 ile R_s' değerini hesaplar.

$$R^{s\prime} = M_3 \oplus s_i^r \quad \textbf{(2.10)}$$

- Etiket hesaplanan R_s' değerini kullanarak Denklem 2.11 ile M_4' değerini hesaplar.

$$M_4' = h(R^t \oplus s_i^r \parallel R^{S'}) \quad \textbf{(2.11)}$$

- Etiket alınan M_4 ile hesaplanan M_4' değerlerini karşılaştırarak eşit olması durumunda okuyucuyu doğrular.

- Doğrulama işleminin başarısız olması durumunda haberleşme adımları bu aşamada sonlandırılır.

- Etiketin okuyucuyu doğrulaması sonrasında Denklem 2.12 ve Denklem 2.13 kullanılarak yeni gizli değerler hesaplanır.

$$s_{i+1}^{t} = R^{S} \oplus s_i^{t} \oplus (R^{t} \& s_i^{r}) \quad \textbf{(2.12)}$$

$$s_{i+1}^{r} = R^{t} \oplus s_i^{r} \oplus (R^{S} \& s_i^{t}) \quad \textbf{(2.13)}$$

Yukarıda sıralanan adımlar neticesinde hesaplanan yeni gizli değerlerin bu protokolü takip edecek bir şifreli mesajlaşma yapısında kullanımı uygundur.

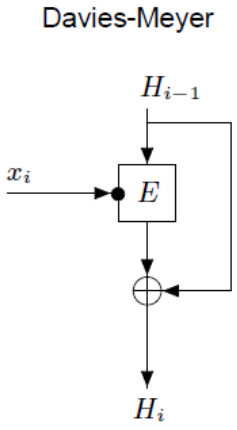
Söz konusu doğrulama protokolünün adımları sırasında işletilmesi gereken fonksiyonlar aşağıdaki gibi sıralanabilir.

- Rastgele sayı üreteci
- Özet fonksiyonu
- Özel veya fonksiyonu

Protokolün gerçeklenmesi aşamasında yukarıda listelenen fonksiyonlardan rastgele sayı üreteci için Bölüm 3.3'de anlatılan doğrusal geri beslemeli kaydırma yazmacı kullanılabilir.

3.1.1 Davies-Meyer özet fonksiyonu

Özet fonksiyonu için ise blok diyagramı Şekil 3.2'de verilen Davies-Meyer isimli blok şifreleme tipi özet fonksiyonu kullanılabilir [19].



Şekil 3.2 : Davies-Meyer özet fonksiyonu blok diyagramı.

Şekil 3.2'de verilen blok diyagramda görüldüğü üzere özet fonksiyonunun H_{i-1} ve x_i olmak üzere iki girişi vardır. H_{i-1} girişine özet fonksiyonunun birinci turunda başlangıç vektörü, diğer turlarında bir önceki turun çıkışı verilir. x_i girişine ise özet fonksiyonu çıkartılacak veri verilir. Söz konusu tur sayısı giriş verisinin uzunluğu kadardır. Blok diyagramda *E* ile gösterilen kutu bir şifreleme modülünü ifade eder. Bu şifreleme modülü için ilerleyen Bölüm 3.2'de anlatılacak Küçük Şifreleme Algoritması kullanılması uygundur [20].

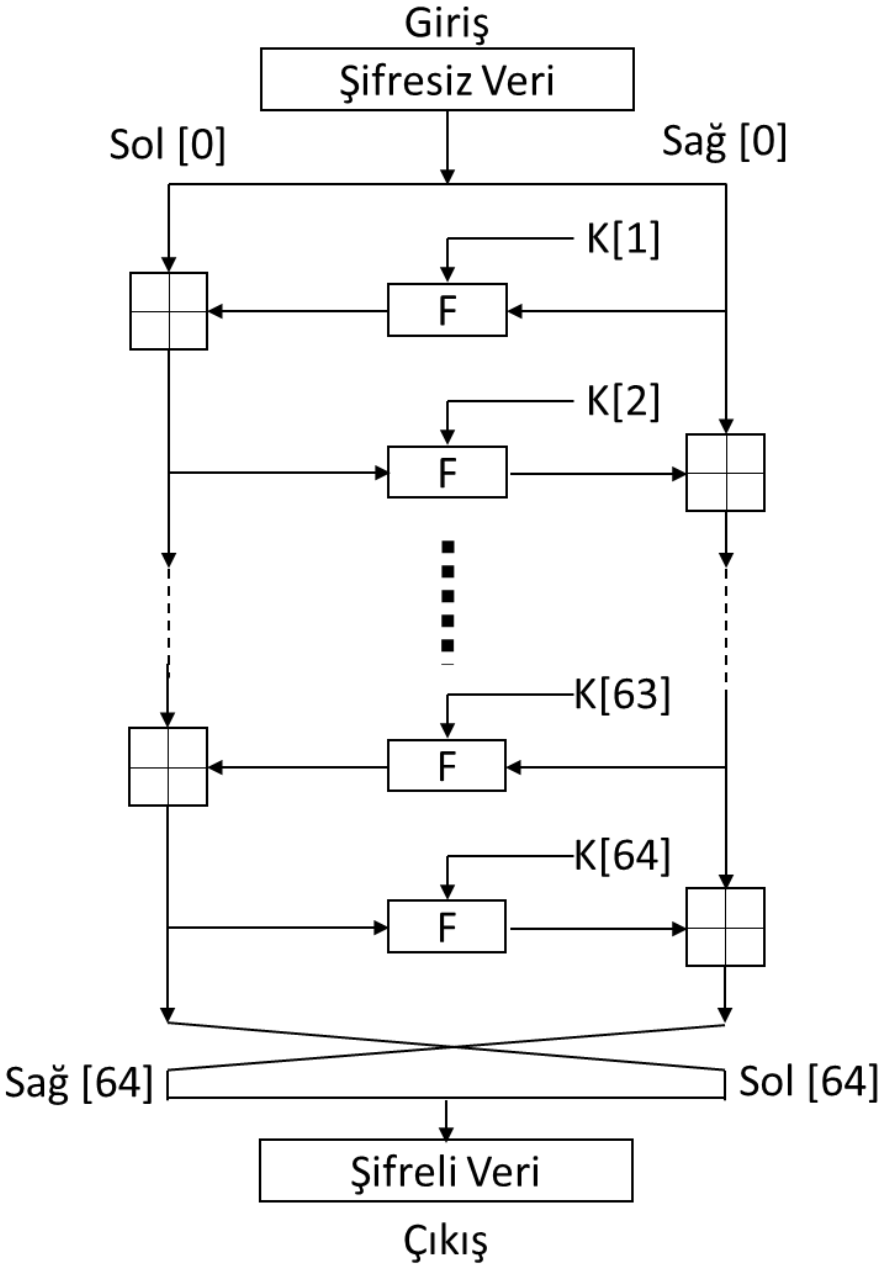
3.2 Küçük Şifreleme Algoritması

Küçük Şifreleme Algoritması (Tiny Encryption Algorithm - TEA), karışık cebirsel işlemleri kullanan, Feistel türü şifreleme yapan, minimum hafıza alanı ve maksimum hız hedeflenerek oluşturulmuş bir şifreleme algoritmasıdır [20]. Feistel türü şifreleme blok şeklinde şifreleme yapılmasını gerektirir ve sadece altı tur sonra tam yayınım sağlamaktadır. Böylece, şifrelenecek metinde 1 bit değiştirildiğinde çıkıştan alınan şifreli metine bu değişiklik 32 bit olarak yansıyacaktır. Zaman performansı ise bilgisayarlarda ve iş istasyonlarında oldukça etkileyicidir.

TEA algoritması blok şifreleme yapısında olması sebebiyle girişine uygulanan 64 bitlik metni bit bit olarak şifrelemek yerine 64 biti tek blok olarak alarak sanki tek bir bitmiş gibi şifrelemektedir [20]. TEA şifreleme yapısında 128 bit uzunluklu şifreleme anahtarı kullanılmaktadır. Bu 128 bit uzunluklu anahtar Şekil 3.4'de görünen *K[0], K[1], K[2] ve K[3]* şeklinde dört adet 32 bit uzunluklu anahtarlara bölünerek işlemlere sokulur.

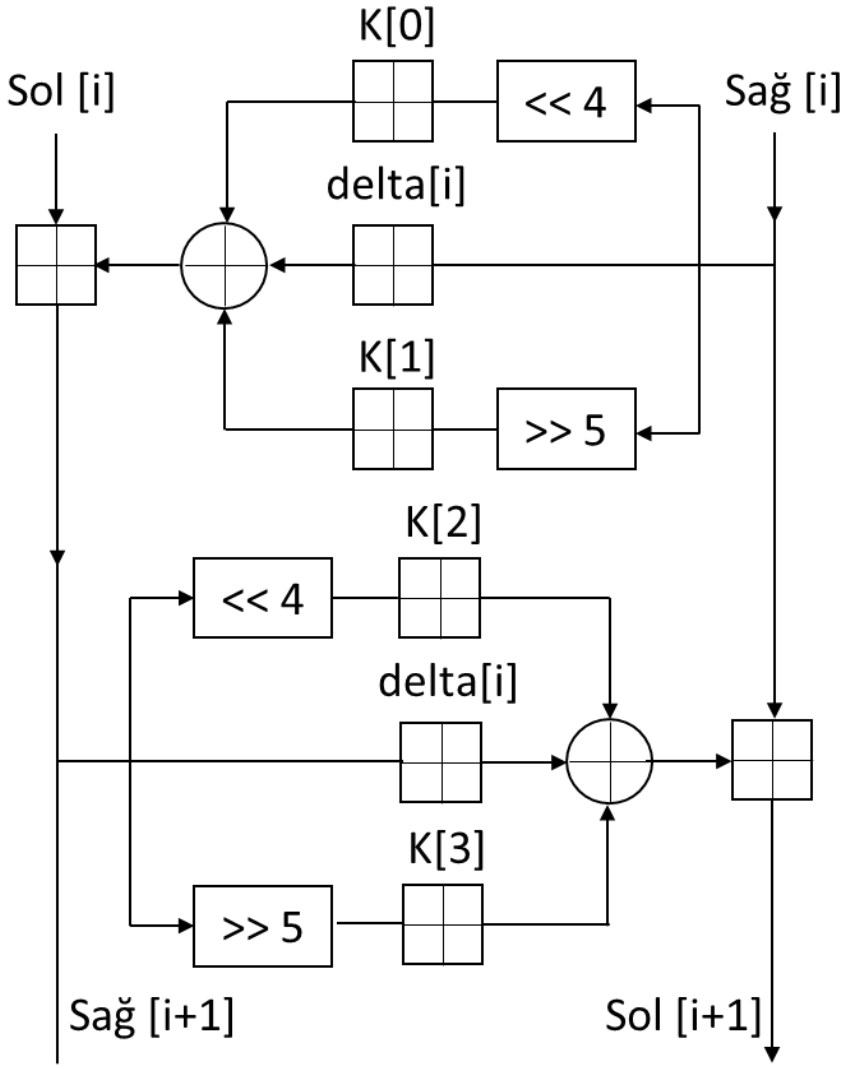
Şekil 3.3'de algoritmanın şifreleme yapan kısmının blok diyagram yapısı görülmektedir [20]. Şifreleme yapısı 64 adet Feistel döngüsünden meydana gelmektedir. Şifrelenmek istenen metin 32'şer bitlik *Sol[0]* ve *Sağ[0]* ile adlandırılmış iki kısma bölünerek şifrelenmek üzere döngüye sokulur. Her bir döngüde farklı anahtar kullanılmaktadır. Girişe uygulanan 32 bitlik iki giriş *K[0], K[1], ..., K[64]* anahtarları tarafından şifrelenerek bu 64 döngünün sonunda yine iki adet 32 bitlik şifrelenmiş metin halinde çıkmaktadırlar. Yapı, her bir döngünün girişi bir önceki döngünün çıkışına bağlanacak şekilde oluşturulmuştur. Her bir döngüye giren 64 farklı *K[i]* anahtarı, 128 bit şifreleme anahtarının "delta" isimli altın orandan üretilen bir sabitin işleme sokularak oluşturulmaktadır. Delta sabitinin ilk değeri Denklem 2.14'den hesaplanmaktadır.

$$Delta = \left(\sqrt{5} - 1\right) * 2^{31} = 9E3779B9h \quad \textbf{(2.14)}$$



Şekil 3.3 : TEA şifreleme rutini.

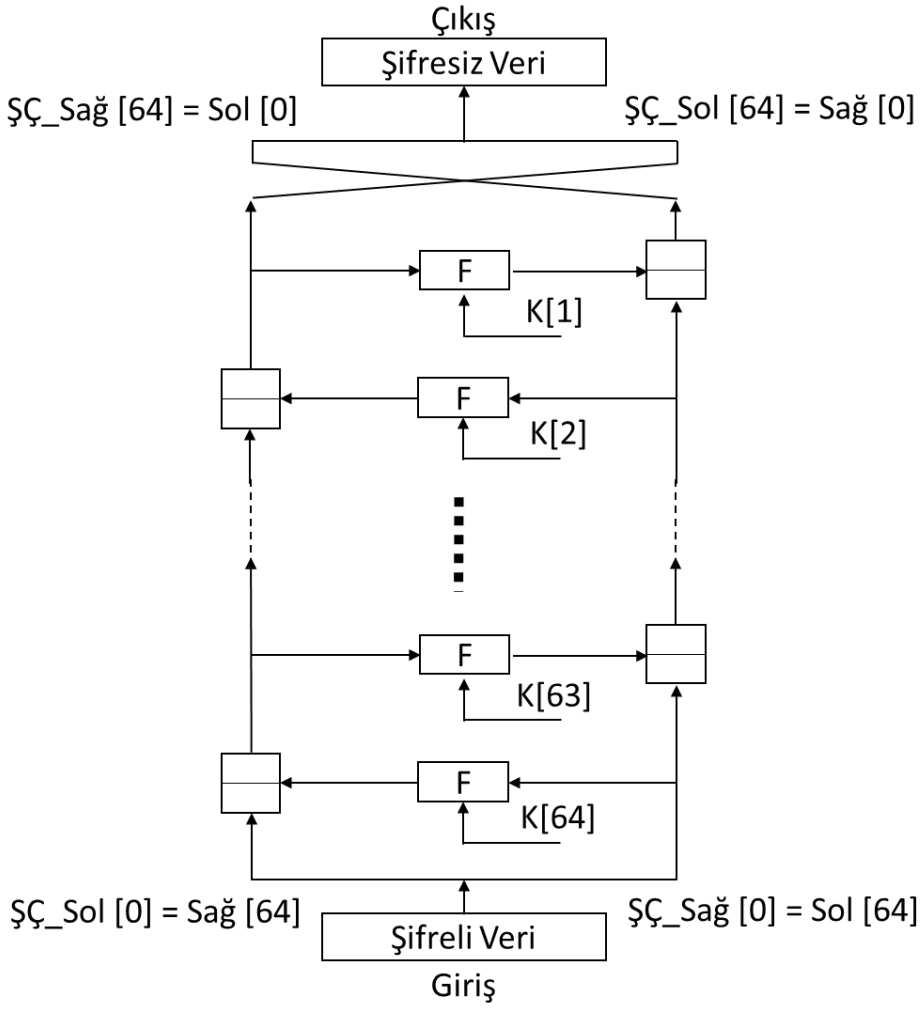
Şifreleme kısmının içyapısına değinilecek olunursa, 64 Feistel döngüsünde oluştuğu bilinen şifreleme yapısı Şekil 3.4 ile verilen yapının 32 döngüde kullanılmasıyla oluşur [20]. Yani Şekil 3.4 iki tane Feistel döngüsü içermektedir. Her bir döngüde döngüye giren metinler toplama, özel veya (exclusive or, XOR), mantıksal kaydırma işlemlerine tabii tutulmaktadır.



Şekil 3.4 : TEA i. Döngüsü.

Şekil 3.4'de de görüldüğü gibi bir döngüye sağ taraftan giren şifresiz metin öncelikle 4 bit sola kaydırılır ve daha sonra *K[0]* anahtarıyla toplama işlemine girer. Yine aynı bilgi 5 bit sağa kaydırılarak *K[1]* anahtarıyla toplama işlemine girmektedir. Ayrıca bilginin kendisi de direkt olarak *delta[i]* sabitiyle toplama işlemine girmektedir. Daha sonra işleme giren bu üç koldan gelen veriler XOR işlemine girerek sol tarafta metinle toplanmaktadır. Bu toplamın sonucu o döngünün sol taraftan verdiği çıkışı olarak bulunmaktadır. Sol taraftan çıkan bu bilgi bir Feistel turu önce sağdan girmiş olan metinle aynı işlemlere tabii tutularak bu döngünün sağ taraftan verdiği çıkış sonucu elde edilmektedir. Bu işleme bu şeklide 32 tur devam edilerek son turun çıkışında girişten verilen şifresiz metinlerin şifreli halleri elde edilmektedir.

TEA simetrik yapılı şifreleme algoritması olması sebebiyle şifre çözme yapısı da şifreleme yapısıyla benzer olmaktadır. TEA Şifre çözme yapısı Şekil 3.5'da verilmiştir [20].



Şekil 3.5 : TEA şifre çözme rutini.

Şekil 3.5'da görüldüğü üzere TEA şifre çözme rutini şifreli metinin çıkıştan girişe doğru işlenmesi şeklindedir. Şifre çözme yapısını şifreleme yapısından ayıran bir nokta olarak şifresi çözülecek metinin başlangıçta *K[64]* anahtarı kullanılarak işleme sokulmasıdır. Yani anahtarların sırası da tamamen yer değiştirmiştir. Bir diğer fark ise sağ ve solda görülmekte olan ana kollardaki toplama işlemlerin yerini çıkarma işlemleri alması şeklinde olmaktadır.

3.3 Doğrusal Geribeslemeli Kaydırma Yazmacı

Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolünün adımları arasında bahsedildiği üzere protokolün doğrulama mekanizmasının gerçekleştirilmesi aşamasında bir rastgele sayının üretilmesi gerekmektedir [18]. Sistemin daha güvenilir bir hale gelmesi açısından üretilen rastgele sayının tahmin edilemez olması önemlidir. Tamamen rastgele bir sayı üretmek ayrı bir tasarım yükü getireceğinden bu tez aşamasında ürettiği sayıların rastgele olduğu varsayılan doğrusal geri beslemeli kaydırma yazmacı (Linear Feedback Shift Register, LFSR) kullanılmıştır.

LFSR donanım gerçeklemeleri için uygun olması, büyük periyotlu dizi üretimi özelliği, iyi istatistiksel özellikli dizi üretimi özelliği ve yapısının cebirsel teknikleri kullanarak basit bir şekilde ifade edilebilmesinden ötürü sıklıkta tercih edilmektedir [21].

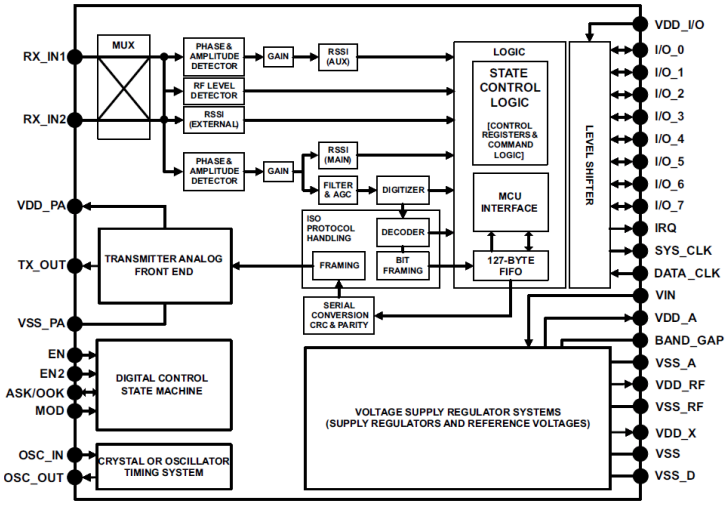
Sözde-rastgele sayı üreteci olan LFSR girişine tohum yani başlangıç değeri uygulanarak her saat darbesi geldiğinde farklı bir rastgele sayıyı çıkışından vermektedir. L bit uzunluklu bir LFSR'nin çalışma yapısı, ilk olarak aldığı L bit uzunluklu tohum değerini her saat işareti geldiğinde bir düşük anlamlı bitine kaydırır. Her bit bir anlamsız basamağa kaydığı zaman boşta kalan en anlamlı bit olan L-1 bitine diğer bitlerin bir kaçının XOR işlemine tabii tutulmasıyla elde edilen değer atanır. LFSR belirli bir periyodu tamamlandığında başlangıç değerine geri dönmektedir. Bu sebepten dolayı tasarlanan sistemlerin daha güvenli olabilmesi için bu periyodun mümkün olduğu kadar uzun tutulması gerekmektedir.

4. GELİŞTİRME ORTAMI BİRİMLERİ

4.1 TRF7970A Analog Uç Birimi

TRF7970A; NFC sistemleri için tasarlanmış bir analog uç birim entegre devresidir [22]. Bölüm 5.2'de anlatılacak NFC alt sistem tasarımında bu entegre devre kullanılmıştır. TRF7970A; NFCIP-1 (ISO/IEC 18092) ve NFCIP-2 (ISO/IEC 21481) standartlarına uyumlu, 106 kbps, 212 kbps, 424 kbps çalışma hızlarında NFC okuyucu, NFC Eşten Eşe Bağlantı (Peer to Peer – P2P) ve kart emülasyon modlarında çalışma gerçekleştirebilmektedir [3, 4].

RF alan detektörü, programlanabilir çıkış gücü, programlanabilir giriş çıkış gerilim seviyesi ve sistem saat işareti çıkışı bu ürünün özelliklerindendir. TRF7970A'nın bağlanacak kontrol birimi ile haberleşmesi paralel hat üzerinden ya da SPI protokolü ile gerçeklenmektedir. Şekil 4.1'de söz konusu ürünün blok diyagramı verilmiştir [22].



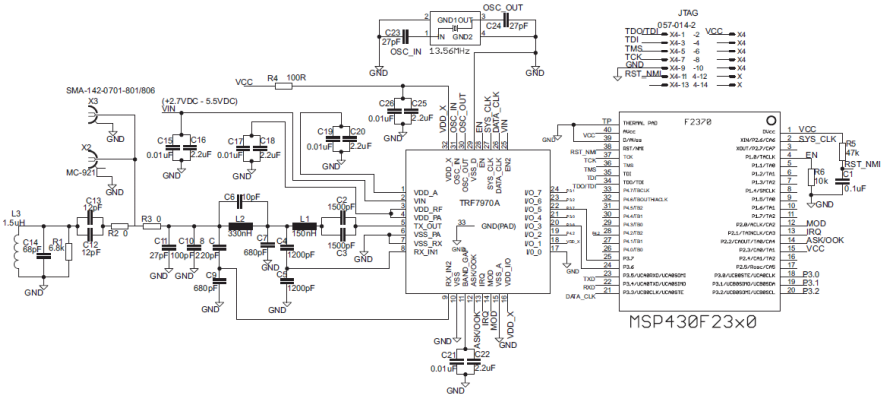
Şekil 4.1 : TRF7970A blok diyagramı.

TRF7970A analog uç birimi aşağıda sıralanan uygulama alanlarında kullanıma imkân sağlamaktadır;

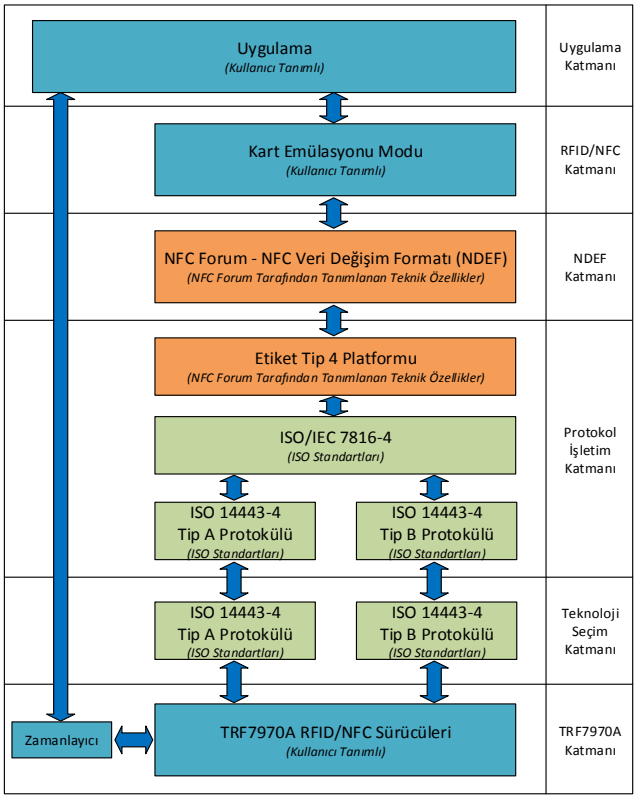
- Mobil cihazlar (tablet ve cep telefonu)

- Toplu taşıma ya da etkinlik biletlemesi
- Pasaport veya ödeme (POS) için okuyucu sistemleri
- Ürün kimliklendirme
- Geçiş kontrolü veya dijital kapı kilitleri

Söz konusu ürünün uygulama devresi Şekil 4.2'de, kart emülasyon modunda gerçekleme için üretici uygulama notlarında önerilen yığın mimarisi Şekil 4.3 ile verilmiştir [22, 23].

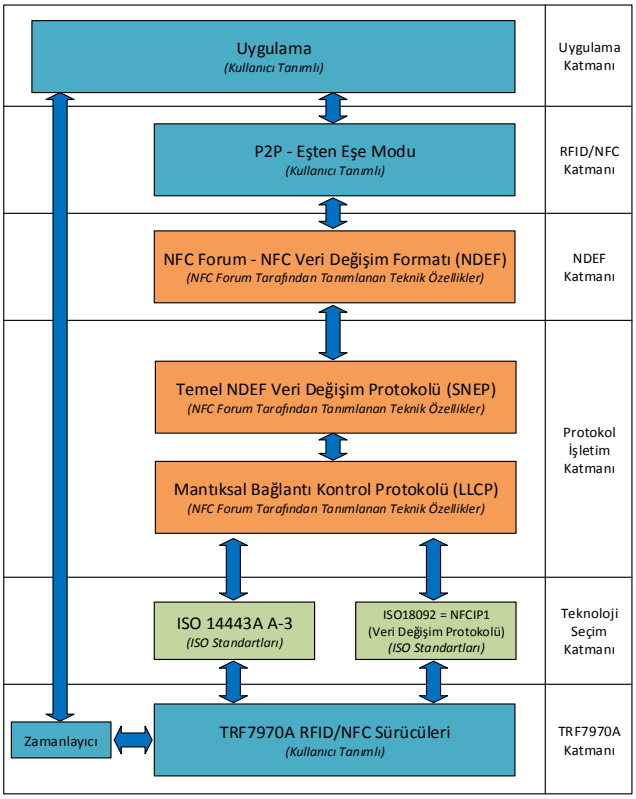


Şekil 4.2 : TRF7970A uygulama devresi.



Şekil 4.3 : Kart emülasyon modu için NFC yığın mimarisi.

Eşten eşe bağlantı modu için ise üretici tarafından önerilen yığın mimarisi ise Şekil 4.4 ile verildiği gibidir [24].



Şekil 4.4 : Eşten eşe bağlantı modu için NFC yığın mimarisi.

4.2 MSP430 Geliştirme Kiti

NFC alt sistem tasarımında kullanılması belirlenen analog uç birimi TRF7970A'ın dokümanlarında paylaşılan örnek tasarımlarda kontrol birimi olarak yine Texas Instruments firmasına ait MSP430 ailesinden bir mikrodenetleyici kullanılmış ve bu mikrodenetleyici ile beraber örnek yazılım tasarımları firma tarafından paylaşılmıştır [25]. Bölüm 5.2'de detaylandırılacak, tasarlanan NFC alt sistemin analog kısmının doğrulanması aşaması için kullanılan MSP430 geliştirme kiti ile alakalı bilgiler aşağıdaki gibidir.

MSP430 geliştirme kiti, MSP430g2xx serisi mikrodenetleyiciler için tasarlanmış olan temel bir geliştirme kitidir [26]. MSP430 LaunchPad kiti üzerinde, programlama ve hata ayıklama donanımını barındırmaktadır. Kit üzerinde genel amaçlı birçok giriş/çıkış pini, LED'ler, MSP430g2xx ailesi için bir dip soket ve 2 adet MSP430 mikrodenetleyici barındırmaktadır. Gerçeklenecek protokollerin hafıza

gereksinimlerinden ötürü kit ile beraber gelen MSP430G2553 kodlu mikrodenetleyici çalışma kapsamında tercih edilmiştir.

MSP430 mikrodenetleyicileri, Texas Instruments tarafından üretilen 16-bit, RISC tabanlı, ultra düşük güç tüketimli bir mikrodenetleyici ailesidir. Basit tasarımının yanı sıra, zengin çevreselleri, kullanım kolaylığı, düşük maliyeti ve çok düşük güç tüketimi ile MSP430 tasarımcılar tarafından sıklıkla tercih edilmektedir. MSP430, uyku modunda 0.1uA'den daha az akım tüketmektedir ve bu performansı ile düşük güçlü işlemci aileleri içinde önemli bir yer edinmiştir. MSP430 25MHz'e kadar kristal osilatör desteklemektedir. Ek olarak 128B ile 64 KB arasında RAM, 512B ile 521KB Flash bellek bulunduran modelleri mevcuttur. Bu anlamda bellek boyutları anlamında MSP430 ailesi çok geniş bir yelpazede seçenekler sunmaktadır. [27].

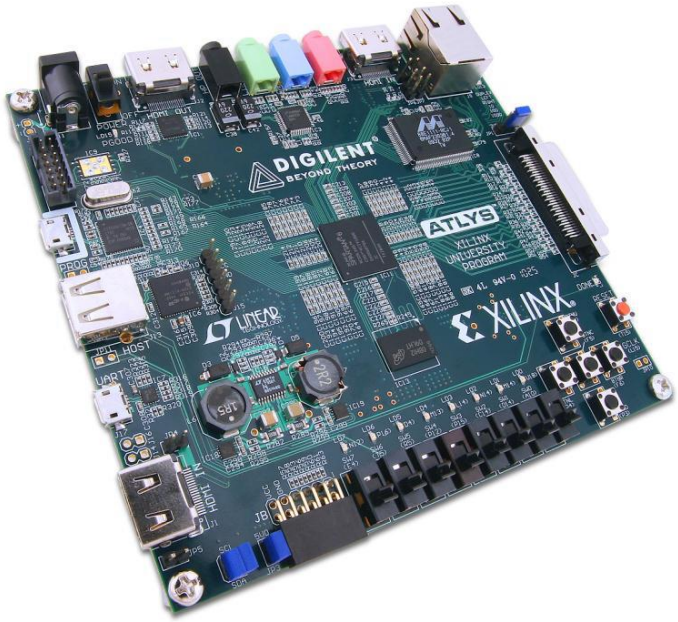
MSP40 için, Code Composer Studio ya da IAR Embedded Workbench ortamlarında yazılım geliştirmek mümkündür [28, 29]. Bu tez kapsamında yapılan çalışmalarda Code Composer Studio geliştirme ortamı kullanılmıştır. MSP430 kitleri, aynı zamanda JTAG programlama ünitesi de içerdiğinden, başka bir programlayıcı ya da hata ayıklama ünitesi gerektirmemektedir. Kullanılan geliştirme kartının resmi Şekil 4.5'de paylaşılmıştır [26].

Şekil 4.5 : MSP430 geliştirme kiti.

4.3 Digilent Atlys FPGA Geliştirme Kiti

Bu tez çalışmasında yazılım / donanım gerçekleme platformu olarak Xilinx firmasının Spartan-6 LX45 FPGA'sını üzerinde barındıran Digilent firmasının Atlys

Spartan-6 FPGA geliştirme kartı kullanılmıştır [30]. Geliştirme kartın görüntüsü Şekil 4.6'da verilmiştir.

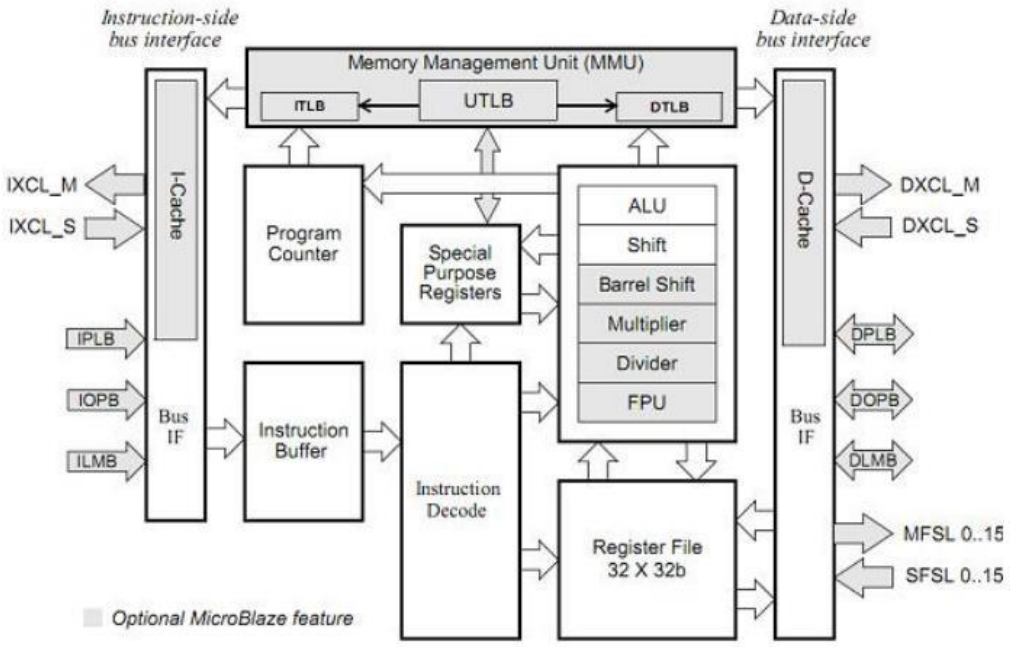


Şekil 4.6 : Atlys FPGA geliştirme kartı.

Söz konusu kartın özelliklerinden bahsetmek gerekirse Atlys kartı üzerinde bulunan FPGA, her biri 4 adet 6 girişli LUT ve 8 adet flip flop içeren 6822 dilim, 58 DSP dilimi içermektedir. Ayrıca 500 MHz'e kadar saat hızı sunmaktadır.

Söz konusu FPGA üzerinde yazılım tasarımının gerçeklenmesine olanak sağlayan Microblaze isimli sanal çekirdekli bir işlemci konumlandırılabilmektedir [31]. Mimari yapısı Şekil 4.7 ile gösterilen MicroBlaze mikroişlemcisi, FPGA üzerinde yazılım ile kontrol edilebilir gömülü sistemler tasarlamaya olanak sağlamak üzere donanım bloklarının uygun şekilde programlanması ile oluşturulur. MicroBlaze, tek FPGA üzerinde kullanılacak çevre birimleri, hafıza ve ara yüz özelliklerinin seçiminde esneklik sağlayarak kullanıcının isteğine tam olarak cevap veren gömülü sistemler tasarlamaya olanak sağlar. 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. 32 bitlik 32 adet genel amaçlı kaydedicileri 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

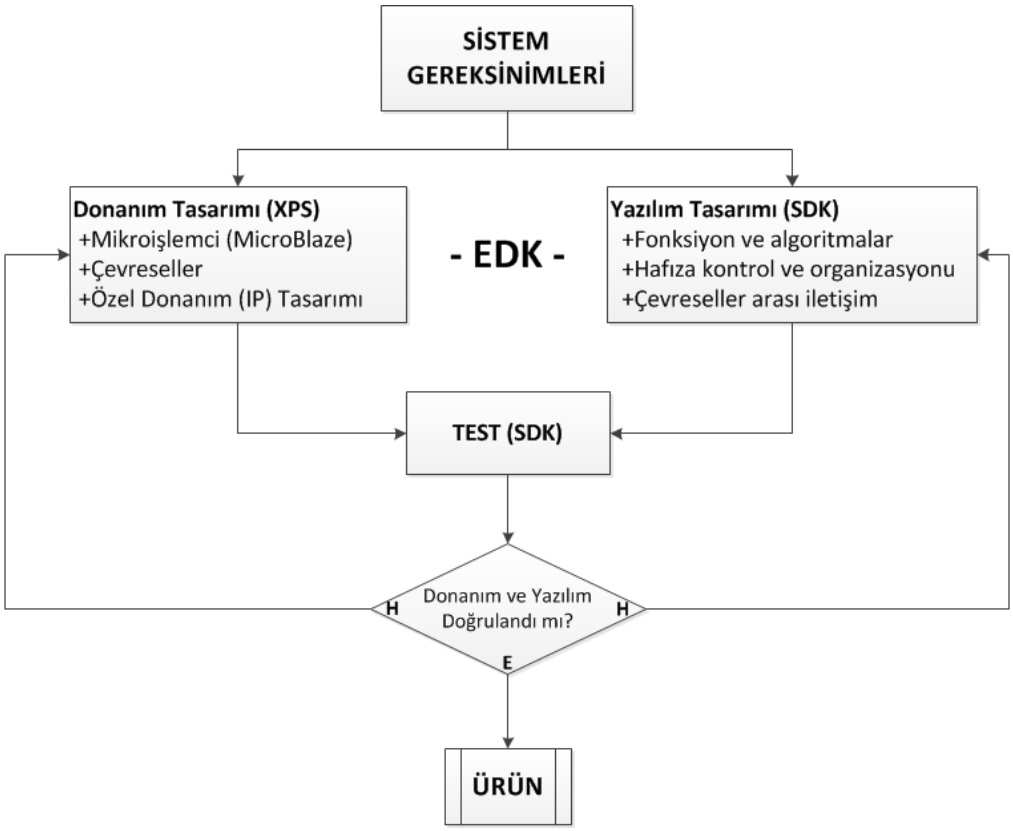
(Memory Management Unit – MMU) gibi özellikleri ile FPGA için optimize edilmiş bir mikroişlemcidir [31].



Şekil 4.7 : Microblaze mimarisi.

Microblaze mimarisinin geliştirme ortamı ise Xilinx firması tarafından Gömülü Sistem Geliştirme Aracı (Embedded Development Kit – EDK) olarak adlandırılmıştır [32]. Bu geliştirme ortamı gömülü sistem tasarımı için tümleştirilmiş bir bilgisayar programıdır. Bu program ile gömülü sistem tasarımında gerekli olan yazılım ve donanım tasarımları bir arada yapılabilmektedir.

Xilinx EDK, bir FPGA üzerinde hem donanım hem de yazılım geliştirilmesine olanak tanımaktadır. Xilinx tasarım araçları ile yapılan bir gömülü sistem tasarım akışı Şekil 4.8 ile verilmiştir.

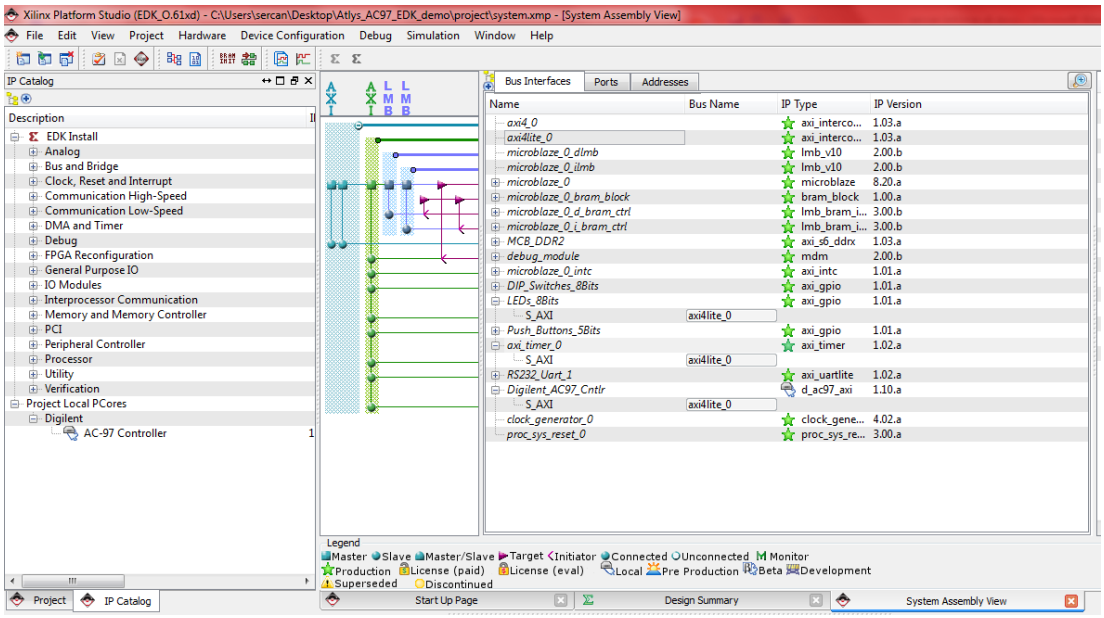


Şekil 4.8 : Xilinx araçlarının gömülü sistem tasarım aşamalarında kullanımı.

Şekil 4.8'de, gömülü sistem tasarımında kat edilen aşamalar ve bu noktalarda hangi araçların kullanılabileceği gösterilmiştir. Xilinx EDK'nın sağladığı bir başka fayda, test aşamasında donanımın yetersiz bulunması durumunda, esnek ve kolay biçimde donanım güncellemesine olanak sağlamasıdır. Standart bir tasarımda, test aşamasında donanım tarafında karşılaşılan kritik bir problemde, işlemci yetersiz bulunur ise, güncelleme yapmanın çok daha zor olacağı ortadadır. Hem yeni bir işlemci seçilmesi, hem de elektronik kartın yeniden çizilip bastırılması gerekli olacak, süreç oldukça uzayacaktır.

Bu yönüyle Xilinx EDK, prototip aşamasındaki projelerde, donanım ve yazılım ortak tasarımı sağlaması ve özellikle esnek biçimde donanımsal güncellemeye olanak tanıması sebebiyle tasarım ve test süreçleri için oldukça elverişli bir geliştirme ortamıdır.

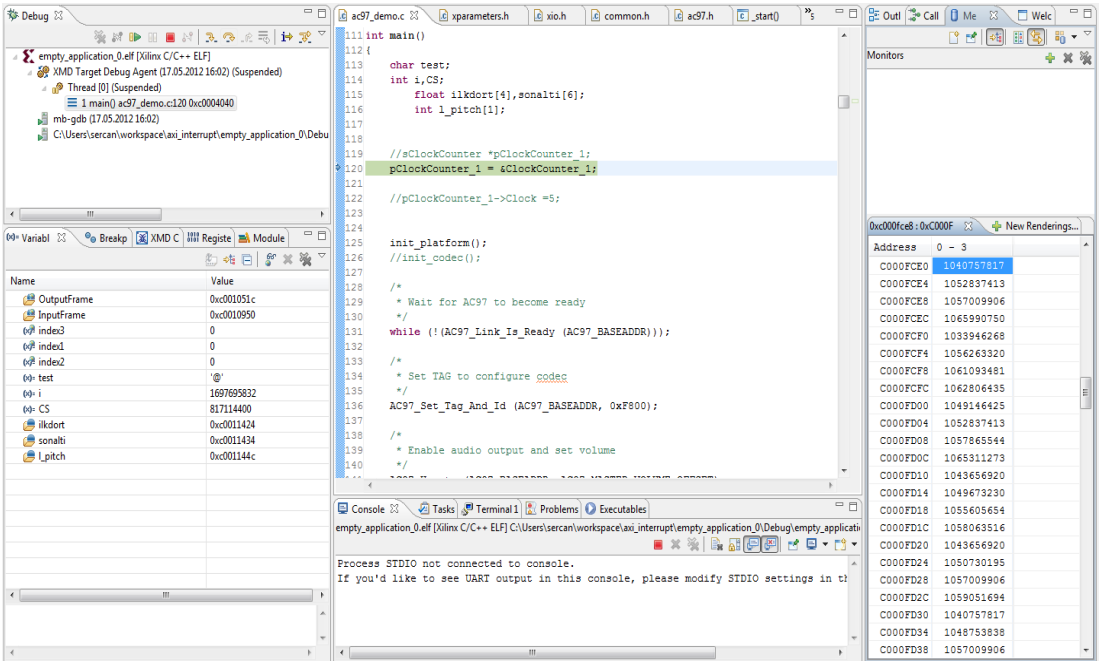
Xilinx Platform Studio (XPS) ise, mikroişlemci mimarisinin oluşturulduğu tasarım aracıdır [33]. Bu araç ile sistemin sahip olacağı çevreseller, işlemci ve özel tasarım donanımlar oluşturulur. Programın ekran görüntüsü Şekil 4.9 ile verilmiştir.



Şekil 4.9 : XPS ekran görüntüsü.

Programın sol tarafındaki bölüm Özel Tasarım Donanım (Intellectual Property-IP) kataloğunu göstermektedir ve bu bölümden işlemcide olması arzu edilen; zamanlayıcı (timer), seri haberleşme (UART, USB vb.) gibi temel çevreseller ve de kullanıcıya ait donanımlar bulunmaktadır. Tez kapsamında mimariye eklenen donanımlar ilerleyen bölümlerde açıklanacaktır.

Software Development Kit (SDK) programı ise, XPS ile tasarlanan donanım mimarisi üzerinde yazılım geliştirilmesine imkân tanımaktadır [34]. Geliştirme dili olarak C kullanılabilmektedir. SDK hem yazlım geliştirme hem de test ortamı olarak kullanılmıştır. Şekil 4.10 ile ekran görüntüsü verilen program vasıtasıyla, tasarlanan mimarideki donanımların yazılım tarafında kullanılabilmesi için otomatik olarak birçok kütüphane derlenmekte ve bu sayede donanımların kullanımı oldukça kolaylaşmaktadır. SDK ile ayrıca geliştirilen yazılımların çözümlemesi (Debug) de yapılabilmektedir.



Şekil 4.10 : SDK programına ait ekran görüntüsü.

5. YAKIN ALAN HABERLEŞMESİ GELİŞTİRME ORTAMI TASARIMI

Bu yüksek lisans çalışmasındaki temel amaç, Yakın Alan Haberleşmesi teknolojisini güvenli hale getirebilecek bir protokol ile sistem tasarımı ve gerçeklemesi yapmaktır. Tasarlanacak sistemin hali hazırda yaygınca kullanılan NFC etkin cihazlarca kullanımının desteklenebilmesi hedefiyle ISO/IEC 18092/ECMA-340 ve ISO/IEC 21481/ECMA-352 kodlu standartlara sadık kalmak önemli bir gereksinim olarak belirlenmiştir [35, 36]. Bu doğrultuda gerçeklenecek protokolün söz konusu standartlarca tanımlanmış haberleşme yapısını destekleyen bir geliştirme ortamı üzerine kurulması birincil tasarım hedefi olarak ortaya çıkmıştır. Bu tasarım hedefi bu çalışmanın ilk adımı olarak yalnızca söz konusu standartlara uygun haberleşmenin gerçekleştirilebildiği bir geliştirme ortamının hazırlanması şeklinde ifade edilebilir.

Çalışmanın ilerleyen adımlarında gerçeklenecek protokolün sisteme eklenebilir olması da başka bir gerekliliktir. Bu sebepten ötürü tasarlanacak sistemin mümkün olduğunca hazır alt birimlerden kaçınılarak entegre devre seviyesinde bir tasarım yapılması bir diğer tasarım hedefi olarak ortaya çıkmaktadır. Bu şartlar altında Bölüm 5.1'de detaylandırılacak, bir NFC etkin cihazın içerdiği NFC teknolojisi ile ilişkili alt birimlerin sırasıyla tasarlanması ve gerçeklenmesi gerektiği gözükmektedir.

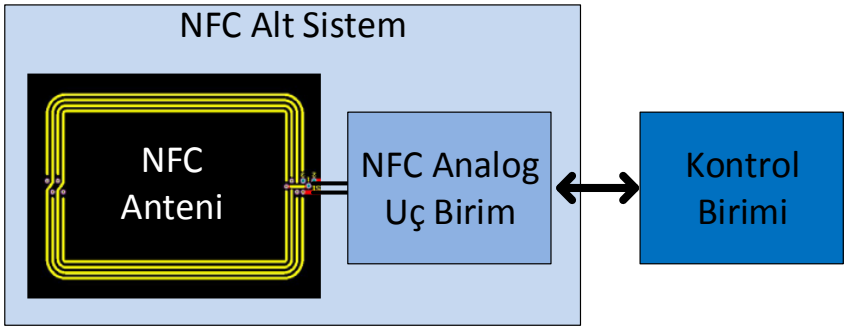
Bu bölümde yukarıda bahsedilen tasarım hedefleri ışığında öncelikle bir NFC etkin cihazın NFC teknolojisi ile ilişkili alt birimlerine değinilecektir. Sonrasında bu alt birimlerin gerçeklenmesi için kullanılması tercih edilen donanım birimlerine, kullanılacak geliştirme ortamlarına ve söz konusu birimlerin nasıl gerçeklendikleri anlatılacaktır.

5.1 Yakın Alan Haberleşmesi Etkin Cihaz Alt Birimleri

NFC etkin cihazların veya bir NFC etkin cihaz olarak nitelendirilebilecek NFC özellikli cep telefonlarının içeriğinde NFC teknolojisi ile ilişkili iki temel öğe bulunmaktadır [37]. Bunlar;

- Cihazlar arasında kablosuz haberleşmeyi sağlayacak çerçeve tipi anten,
- Anten ile NFC etkin cihazın kontrol birimi arasındaki uyumu sağlayacak NFC analog uç birimidir.

Bu iki birimin birleşimi NFC alt sistem olarak adlandırılabilir. NFC alt sistem kullanılan uygulamaya göre değişebilecek şekilde bir kontrol birimine bağlıdır [37]. Kontrol birimi bir cep telefonu için cihazın uygulama işlemcisidir. Örnek bir NFC alt sistemin yapısı ve kontrol birimi ile beraber Şekil 5.1'de verilmiştir.



Şekil 5.1 : NFC alt sistem ve kontrol birimi.

NFC etkin cihazlar ile haberleşebilmek için şekildeki yapının içinde olduğu bir gerçekleme ortamına ihtiyaç vardır. İlerleyen bölümlerde bu gerçekleme ortamı detaylıca anlatılacaktır.

5.2 NFC Alt Sistem Tasarımı ve Gerçeklenmesi

Şekil 5.1'de verildiği üzere bir NFC alt sistemin içeriğinde analog uç birim ve NFC anten olmak üzere iki temel birim vardır.

NFC analog uç birimi bir NFC etkin cihazın kontrol birimi ile NFC anteni arasındaki uyumu sağlayan entegre devresidir [22]. Bu entegre devreler kontrol birimi ile genellikle UART, SPI ya da paralel bir sayısal arayüzle haberleşirken çıkışına bağlanacak NFC anteni ile 13.56 Mhz'de kablosuz veri transferinin yapılmasını sağlarlar [22, 38-40]. Piyasada bu görev ile alakalı olarak NXP, Texas Instruments, ST Microelectronics gibi firmaların sunduğu çözümler mevcuttur. Çizelge 5.1'de örnek olarak nitelendirilebilecek ürünler listelenmiştir [22, 38-40].

Çizelge 5.1 : Örnek NFC analog uç birimleri.

Ürün İsmi	NXP CLRC66302HN	TI TRF7970A	TI TRF7960A	ST ST95HF
Desteklenen Standartlar	ISO/IEC 14443A	ISO 14443A	ISO 14443A	ISO/IEC 14443
	ISO/IEC 14443B	ISO 14443B	ISO 14443B	ISO/IEC 15693
	ISO/IEC 15693	ISO 15693	ISO 15693	ISO/IEC 18092
	ISO/IEC 18000-3	ISO 18000-3	ISO 18000-3	
	ISO/IEC 18092	ISO 18092		
FIFO (bytes)	512	128	12	528
Çıkış Gücü (mW)		100	100	
		200	200	
Tahmini Fiyat	10.35$	3.10$ | 1ku	2.80$ | 1ku	2.53$ | 1ku
Haberleşme Arayüzü	SPI, UART, I2C	SPI, Paralel	SPI, Paralel	SPI

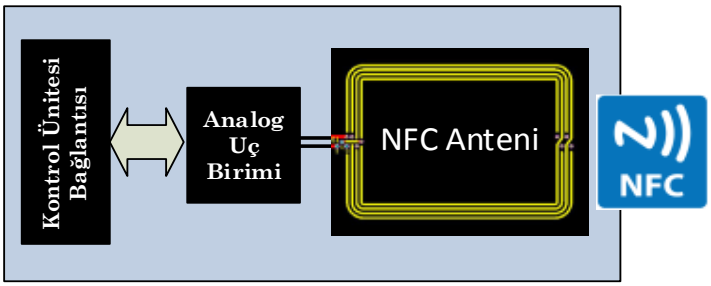
NFC standartlarına uygun haberleşme altyapısının kurulmasında NFC analog uç birimi en önemli tasarım alt birimidir. Bu entegre devresinin önemi tasarlanacak anten yapısını ve daha önemlisi kontrol birimi tarafındaki alt katman yazılım tasarımının bu birime göre yapılması gerektiğinden ileri gelmektedir. Gerçeklenecek güvenlik protokolü her ne olursa olsun karşı birime aktarılacak tüm veriler bu birim üzerinden aktarılacaktır.

Bu birimin seçiminde Çizelge 3.1 ile paylaşılmış olan entegre devreler detaylıca incelenmiştir. Yapılan incelemelerde temin kolaylığı, fiyat ve daha önemlisi örnek donanım ve yazılım tasarımlarına erişim imkânı ve gerçekleme kolaylığı göz önünde bulundurulmuştur. Bu değerlendirmeler neticesinde NFC standartlarını kapsamlıca destekleyen, donanım/yazılım tasarım örnekli yeteri seviyede paylaşılmış ve ücretsiz örnek ürün temini yapılmasına olanak sağlayan Texas Instruments firmasının TRF7970A kodlu entegre devresinin kullanılmasına karar verilmiştir [22]. TRF7970A entegre devresi ile ilişkili detaylı bilgi Bölüm 4.1'de verilmiştir.

Analog uç birimi için yapılan tercih yukarıda anlatıldığı üzere entegre devre seviyesindedir. Dolayısıyla bu entegre devrenin bir sistem dahilinde kullanılabilmesi analog uç birimi ve çevre elemanlarının beraber bir baskı devre kartı üzerinde kullanılmaları ile mümkün olabilir.

TRF7970A'nın tasarım dokümanlarında analog uç birimi ile NFC anteninin aynı kart üzerinde olduğu örnek tasarımlar mevcuttur [41]. Bu örnek tasarımlardan esinlenerek tez kapsamında yapılan çalışmada NFC alt sistem için benzer bir tasarım yapılmıştır. Üzerinde NFC alt sistem bileşenlerinden analog uç birimi, NFC anteni, anten uyumlaştırıcı yapısı ve kontrol birimi ile haberleşmenin sağlanacağı konnektörleri

bulunduran bu kart NFC Alt Sistem Kartı olarak adlandırılmıştır. Söz konusu kart üzerinde bulunan konnektörler ile ileriki bölümlerde değinilecek her iki kontrol ünitesi yani MSP430 geliştirme kartı ve Atlys Spartan-6 geliştirme kartı ile haberleşebilir ve yine üzerinde bulunan çerçeve tipi anten ile belirtilen standartlara uygun kablosuz haberleşme sağlayabilmektedir [42, 30]. Tasarlanan NFC Alt Sistem Kartının yapısı Şekil 5.2'de paylaşılmıştır.

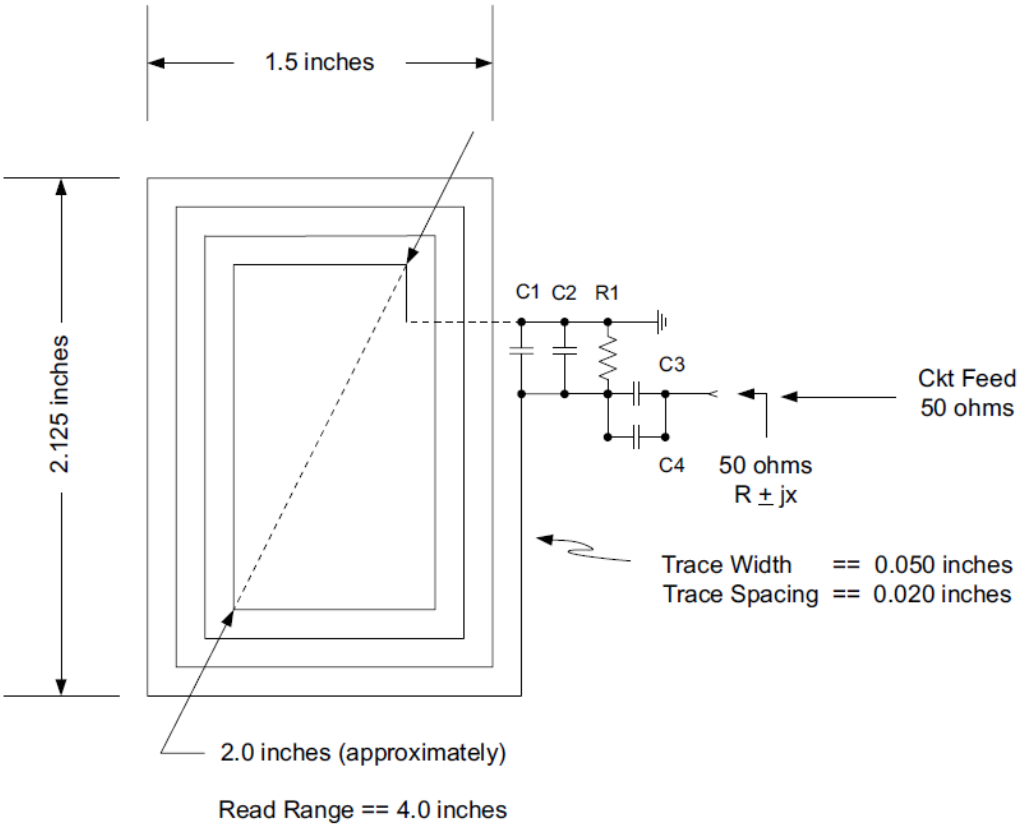


Şekil 5.2 : NFC Alt Sistem Kartı blok diyagramı.

NFC Alt Sistem Kartı Şekil 5.2'de Kontrol Ünitesi Bağlantısı ismiyle anılan konnektör üzerinden kontrol üniteleri ile SPI haberleşme protokolü ile haberleşecektir. Aynı zamanda kartın beslemesi de yine bu konnektör üzerinden kontrol ünitelerinden sağlanacaktır. NFC Alt Sistem Kartının şematik tasarımı Ek A'da verilmiştir.

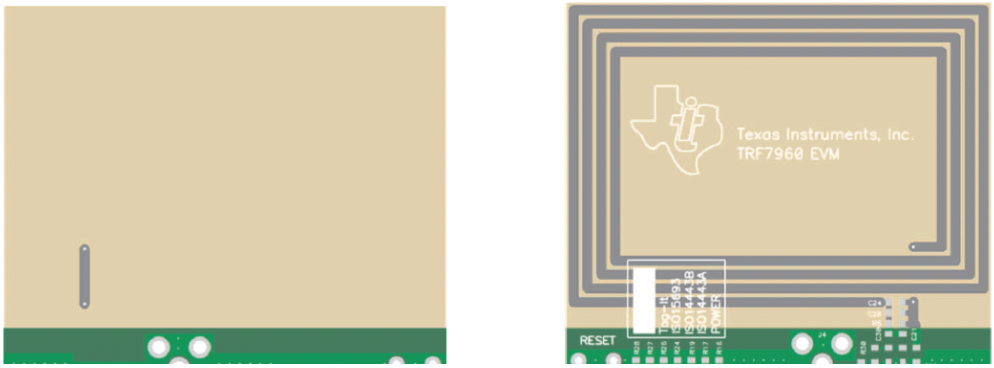
Kartın baskı devre tasarımı da yine üretici firmanın uygulama notlarında ve NFC Forum tarafından paylaşılan teknik dokümanlardaki bilgiler doğrultusunda gerçekleştirilmiştir [43, 44]. Bu aşama ile alakalı önemli hususlardan biri NFC anten tasarımıdır.

Yapılacak anten tasarımında göz önünde bulundurulacak parametreler empedans uyumu ve haberleşme menzili ile alakalı değişkenleri belirlemektedir [45]. NFC anteni 10 cm'lik yayınım mesafesini sağlamak amacı ile dış ölçüleri 5.63 cm x 3,81 cm olacak şekilde olmalıdır [46]. Uygulama notlarında önerilen "NFC Forum POLLER-3" tipi antenin yapısı Şekil 5.3'de verilmiştir [46]. Ayrıca tasarlanan empedans uyumlaştırıcı yapısı ile söz konusu anten 50 ohm'a uyumlu hale getirilmiştir.



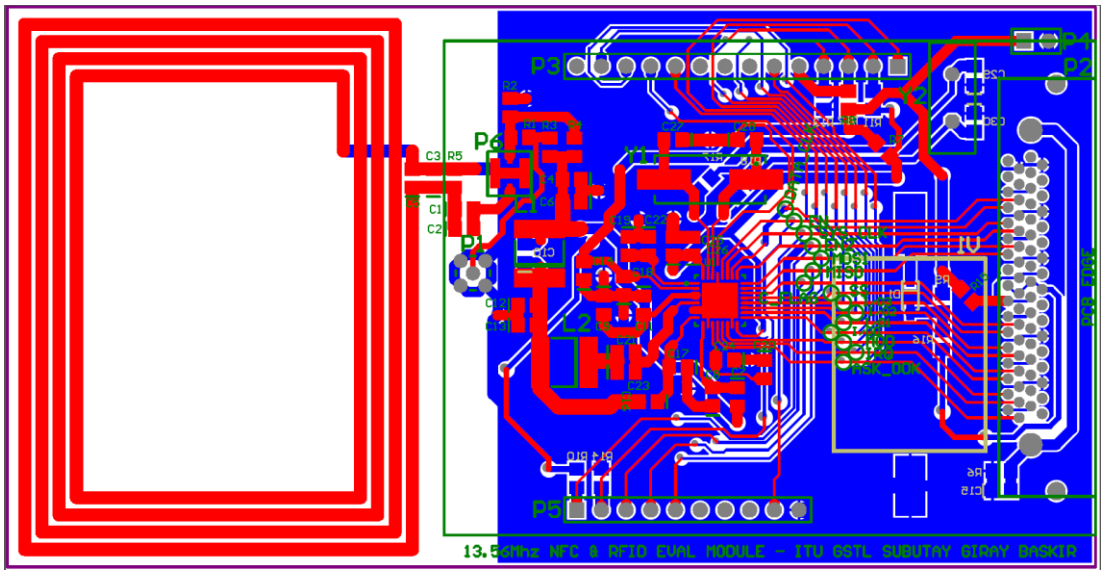
Şekil 5.3 : NFC anten yapısı.

Baskı devre üzerinde bakır yol ile gerçeklenecek çerçeve formundaki NFC anteni için ise bir örnek resim Şekil 5.4 ile verilmiştir [46]. Söz konusu antenin gerçeklenmesi için FR4 maddesi ile 1.6 mm toplam kalınlıkta, 2 oz bakır kalınlığı ve 2 katmanlı bir baskı devre tasarlanması uygulama notunda önerilmiştir.



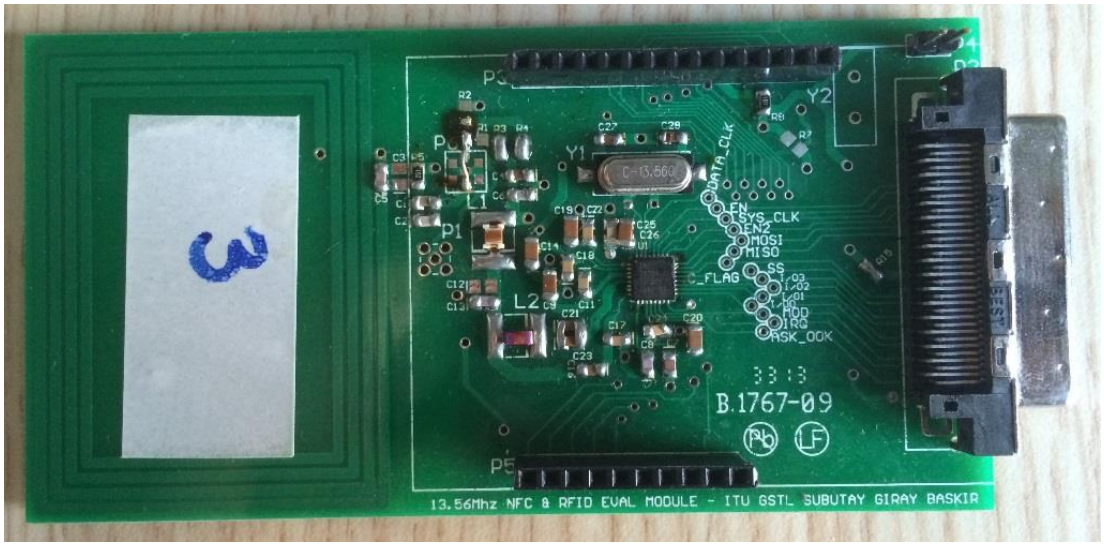
Şekil 5.4 : TI firması tarafından önerilmiş NFC anten yapısı.

Değinilen tasarım kısıtları doğrultusunda tasarlanan baskı devre kartı tasarım görüntüsü Şekil 5.5'de paylaşılmıştır.



Şekil 5.5 : NFC Alt Sistem Kartı tasarım görüntüsü.

NFC Alt Sistem Kartının tasarımı tamamlandıktan sonra sırasıyla baskı devre üretimi ve dizgi işlemleri gerçekleştirilmiştir. Nihai olarak Atlys Spartan-6 geliştirme kartı veya MSP430 geliştirme kartı ile beraber çalışmaya hazır kartın görüntüsü Şekil 5.6 ile verilmiştir.



Şekil 5.6 : Dizgi işlemi tamamlanmış NFC Alt Sistem Kartı.

5.3 Kontrol Birimi Gerçeklemesi

Kontrol birimi temel olarak analog uç birim ile haberleşerek kurulacak NFC bağlantısının yönetileceği birimdir [37]. Analog uç birimi gerçekleme ortamının en önemli birimi olarak gözükse de haberleşmenin nasıl gerçekleşeceği kontrol birimi

tarafından doğru zamanlama ile analog uç birime gönderilecek komutlar ile sağlanmaktadır. Bu doğrultuda NFC standartlarında tanımlanmış olan sayısal haberleşme protokolleri bu birimde gerçeklenmelidir [35, 36].

Gerçekleme aşamalarında donanım ve yazılım ortak tasarım yönteminin kullanılması tez çalışmasının önemli hedeflerinden biridir. İlerleyen bölümlerde değinilecek doğrulama protokolünün donanım kısmında FPGA ortamı kullanılarak kapı seviyesinde gerçeklenmesi NFC teknolojisinin zamanlama isterlerinin karşılanabilmesi açısından elzem bir durumdur [35, 36]. Çalışmanın yazılım kısmında ise donanım olarak gerçeklenen kriptografi algoritmalarının kontrolü yapılarak güvenli NFC protokolündeki akış sırası ve karşılıklı haberleşme gerçeklenecektir.

Bu doğrultuda kontrol birimi üzerinde gerçeklenmesi gereken görevler aşağıdaki gibi listelenebilir;

- NFC protokolleri yazılım kısmında
- Doğrulama protokolü alt modülleri donanım kısmında
- Doğrulama protokolü akış kontrolü yazılım kısmında gerçeklenecektir.

Yukarıda listelenen görevlerin gerçeklenebilmesi amacıyla kontrol birimi tasarımı için, üzerinde sanal çekirdekli bir işlemci olan Microblaze işlemcisinin gerçeklenebildiği Atlys Spartan-6 geliştirme kitinin kullanılması uygun görülmüştür [31, 30]. Söz konusu geliştirme kiti Bölüm 4.3'de anlatılmıştır.

Kontrol birimi gerçekleme aşaması öncesinde, önceki bölüde değinilen NFC Alt Sistem Kartı'nın belirtilen standartlarca çalışma gerçekleştirmesinin TRF7970A uygulama notlarında paylaşılan örnek tasarımlarla doğrulanması amacıyla örnek yazılım tasarımlarının uyumlu olduğu, üzerinde MSP430 ailesinden bir mikrodenetleyici bulunduran bir geliştirme kartı olan MSP340 geliştirme kiti ile kısıtlı kapsamlı bir kontrol birimi tasarımı yapılmıştır [25]. Söz konusu geliştirme kiti Bölüm 4.2'da anlatılmıştır.

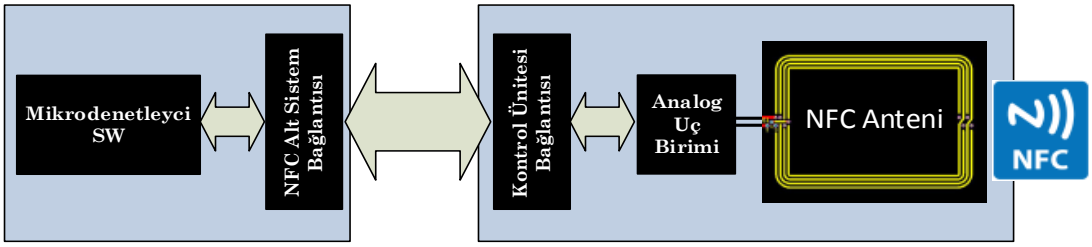
Kontrol birimi temel olarak kurulacak haberleşmenin önceki bölümlerde değinilen standartlara uygun olması için gereken sayısal gereksinimlerin gerçeklendiği birimdir. Bu tez çalışması kapsamında kontrol birimi öncelikle yalnızca kart

emülasyon modunda MSP430 geliştirme kiti üzerinde sonrasında eşten eşe bağlantı modunda Atlys Spartan-6 geliştirme kartı üzerinde gerçeklenmiştir.

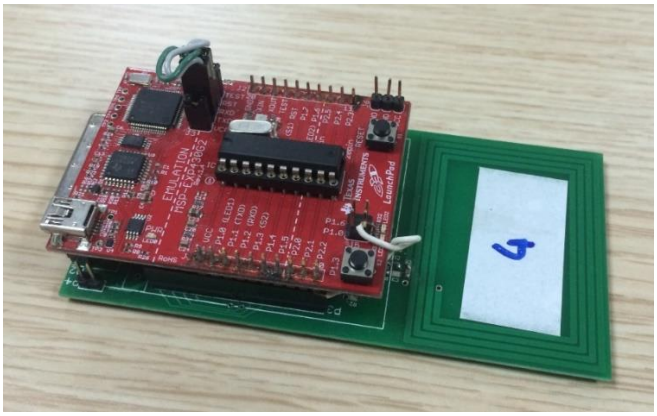
5.3.1 MSP430 geliştirme kiti kontrol birimi ile tasarım

Tez çalışması kapsamında gerçeklenen kontrol birimi / analog uç birim ikilisi ve analog uç birim / NFC anten ikilisi sırasıyla sistemin sayısal ve analog kısımları olarak adlandırılabilir. Sistemin analog kısmının gerçeklenmesi ve çalışır hale getirilmesi aşamasında güvenilir ve çalışmasından emin olunan bir sayısal kısım kullanılabilmesi amacı ile MSP430 geliştirme kiti isimli geliştirme kartında TRF7970A için paylaşılan örnek kodlar kullanılarak geçici bir kontrol birimi tasarımı yapılması hedeflemiştir [26].

MSP430 geliştirme kartı ile yapılan çalışmalardaki birincil hedef tasarlanan NFC Alt Sistem Kartının analog olarak çalışmasının doğrulamasının yapılmasıdır. Bu doğrulama için yazılım tarafında TRF7970A'ın uygulama notlarında yine MSP430 ailesinden ancak farklı bir mikrodenetleyici için kart emülasyon modu yazılmış olan kodlar MSP430 geliştirme kartı üzerinde bulunan MSP430G2553 işlemcisine uyarlanmıştır. Söz konusu bu aşamaya dair hazırlanan birimin blok diyagramı Şekil 5.7 ile birimin resmi ise Şekil 5.8 ile verilmiştir.

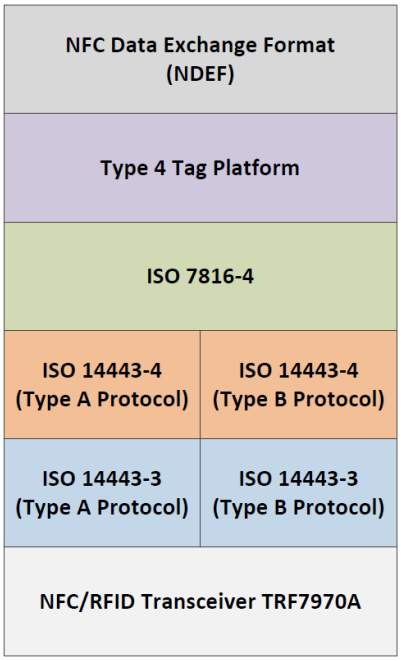


Şekil 5.7 : MSP430 geliştirme kartı ile gerçeklenen tasarım platformu blok diyagramı.

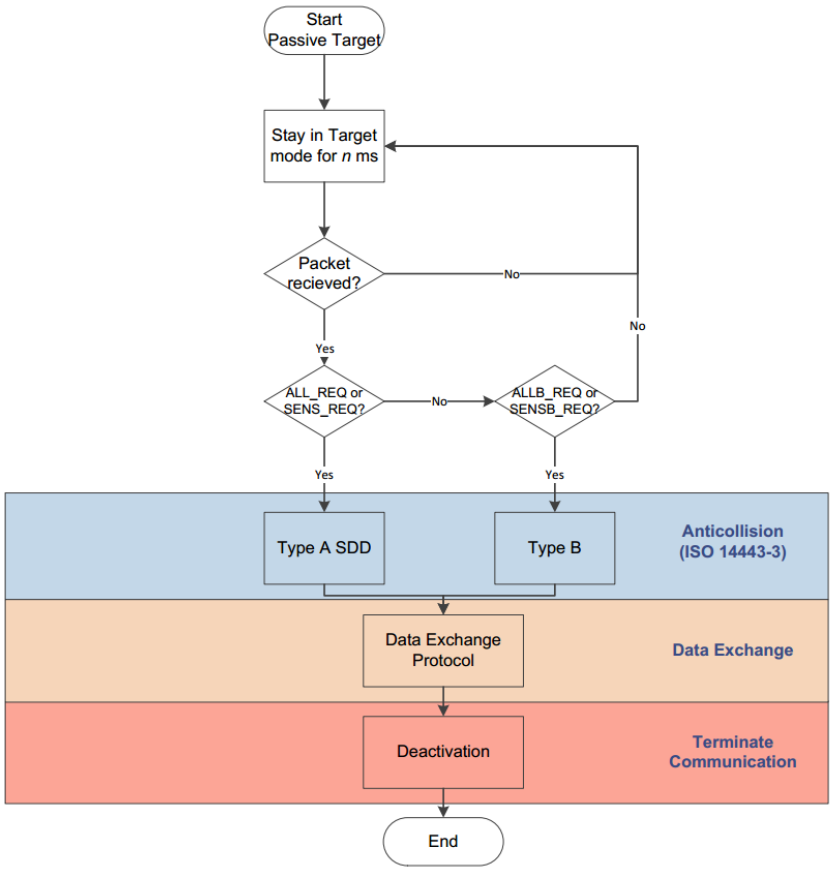


Şekil 5.8 : MSP430 geliştirme kartı ile gerçeklenen tasarım platformu.

Gerçeklenen kart emülasyon modu ile alakalı protokol katmanları Şekil 5.9 ile, protokol akışı Şekil 5.10 ile verilmiştir [23].

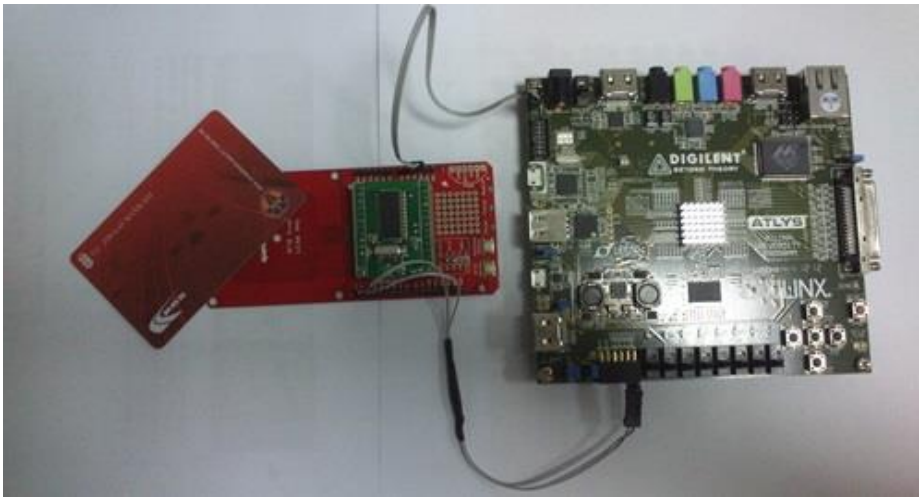


Şekil 5.9 : Kart emülasyon modu protokol katmanları.



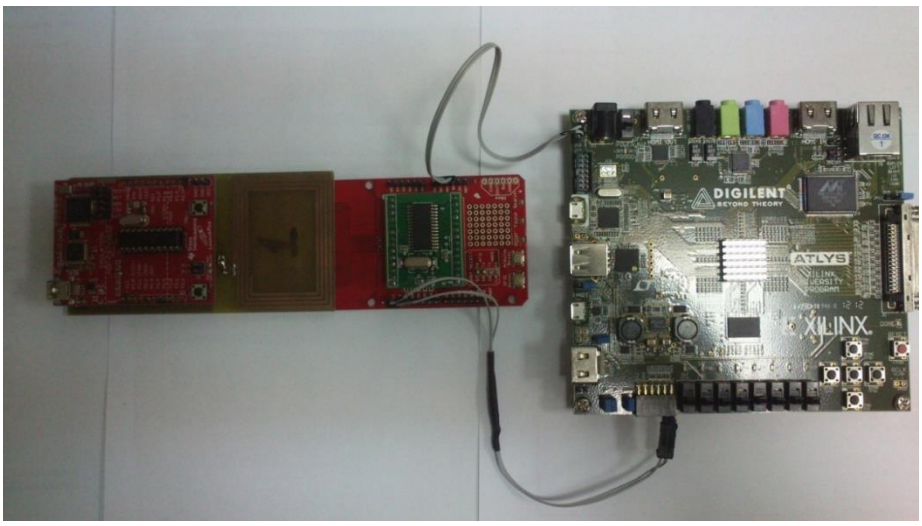
Şekil 5.10 : Kart emülasyon modu akış diyagramı.

MSP430 geliştirme kiti kontrol birimi ile tasarımı aşamasında öncelikle bir ISO/IEC 14443 kart okuyucu olan SM130 RFID Okuyucu Modülü Atyls Spartan-6 geliştirme kiti üzerinde Microblaze işlemcisi ile çalıştırılmış, UART protokolü ile söz konusu modül ve Microblaze işlemcisi arasında haberleşme kurulmuştur [47]. Sonrasında bir ISO/IEC 14443 kartı olan Karayolları Genel Müdürlüğü Kartlı Geçiş Sistemi Kartı (KGS) ile SM130 modülünün çalışması doğrulanmış ve söz konusu kartın kimlik bilgisi kayıt edilmiştir [48]. Söz konusu aşama ile alakalı bir görüntü Şekil 5.11 ile verilmiştir.



Şekil 5.11 : SM130 modülü ile KGS kartı kimlik bilgisi okunması.

Bundan sonraki aşamada kayıt edilen kimlik bilgisi MSP430 işlemcisinin içerisine gömülerek tasarımın kart emülasyon modunda çalıştırılması gerçeleştirilmiştir. Söz konusu aşama ile alakalı bir görüntü Şekil 5.12 ile verilmiştir.



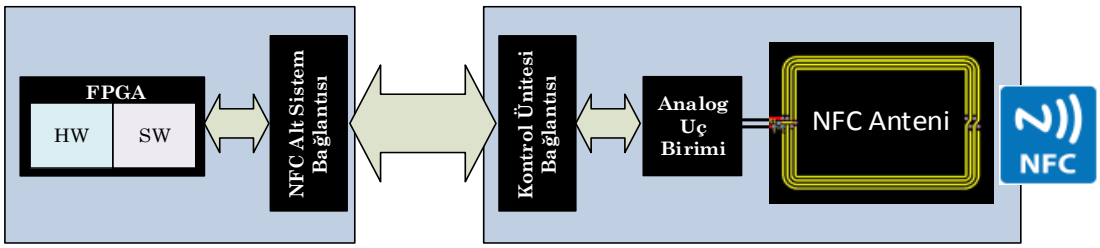
Şekil 5.12 : SM130 modülü, MSP430 geliştirme kiti kontrol birimi ve NFC Alt Sistem Kartı'nın birlikte çalıştırılması.

Gerçekleştirilen bu uygulama ile NFC alt sistem ile haberleşme kurulabildiği ve sonrasında Şekil 3.20'de verilen akışa uygun bir şekilde kart emülasyon modu ile çalışma gerçekleştirilmiştir. Bu doğrultuda NFC Alt Sistem kartının analog olarak belirtilen standartlara uygun çalışma sergilediği doğrulanmıştır.

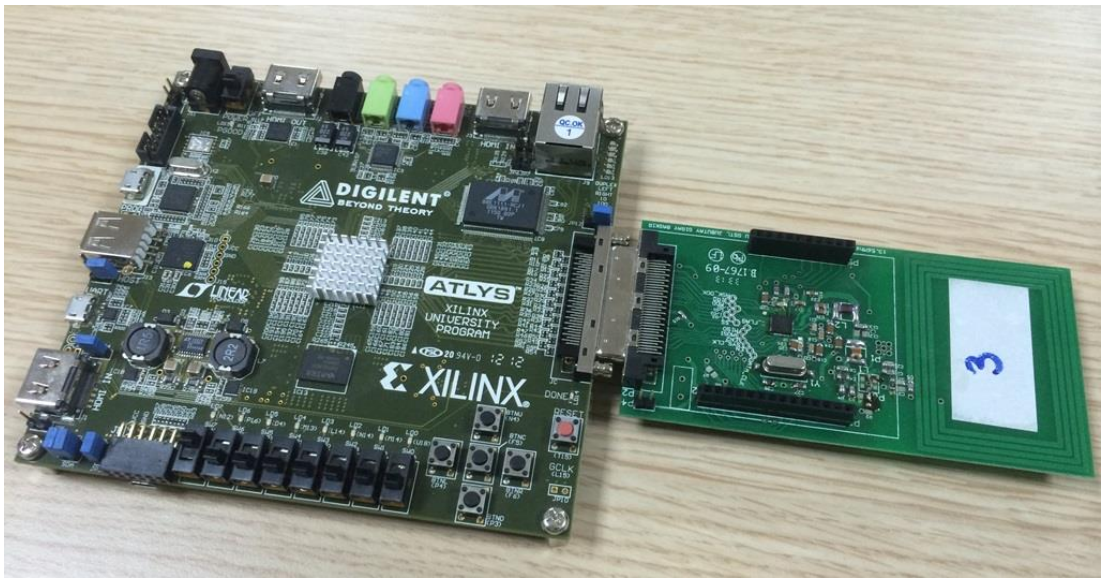
MSP430 geliştirme kiti ile yapılan çalışma sonrasında elde edilen bilgi NFC Alt Sistem Kartının hedeflenen amaçlar doğrultusunda çalışabildiğidir. Yani bu aşama sonrasında yapılacak çalışmada Atlys Spartan-6 kartı üzerinde gerçeklenecek kontrol birimi üzerinde yapılacak tasarımda yaşanacak hatalar NFC Alt Sistem'den bağımsız olacaktır.

5.3.2 Atlys Spartan-6 geliştirme kiti kontrol birimi ile tasarım

Bu aşamanın ilk hedefi eşten eşe bağlantı modu ile öncelikle Atlys Spartan-6 geliştirme kiti kontrol birimi ve NFC Alt Sistem Kartı ikilisini NFC özellikli bir cep telefonu ile haberleştirmektir. İkinci hedefi ise iki adet Atlys Spartan-6 geliştirme kiti kontrol birimi ve NFC Alt Sistem Kartı ikilisini birbirleri arasında haberleştirmektir. Atlys Spartan-6 kartı'nın kontrol birimi olarak kullanıldığı birim ile alakalı yapı Şekil 5.13 ile birimin resmi ise Şekil 5.14 ile verilmiştir.



Şekil 5.13 : NFC Alt Sistem Kartı ve Atlys Spartan-6 geliştirme kiti kontrol birimi yapısı.

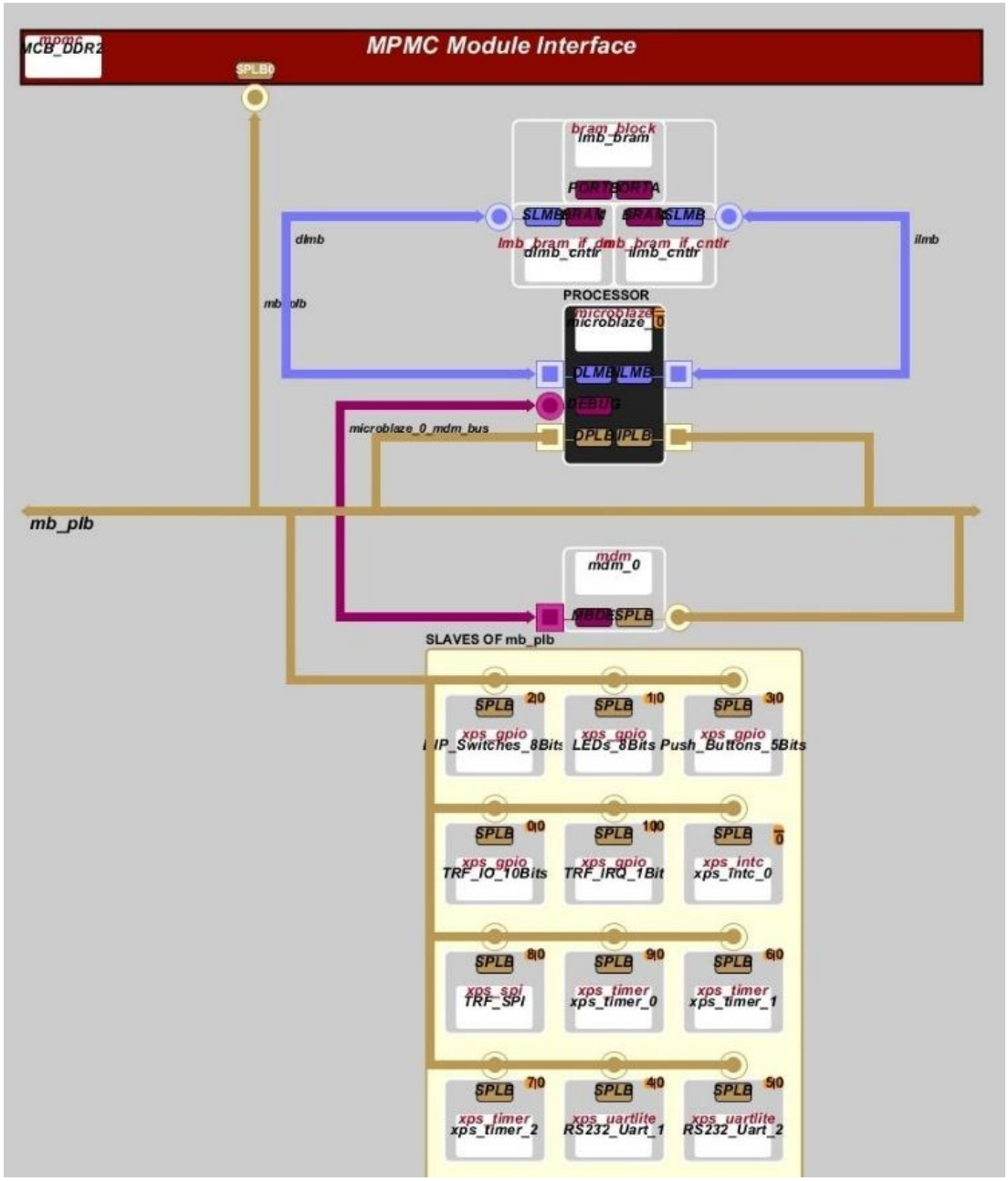


Şekil 5.14 : NFC Alt Sistem Kartı ve Atlys Spartan6 geliştirme kiti kontrol birimi.

Söz konusu aşamada öncelikle Microblaze işlemcisi gerekli çevresel birimler ile Xilinx XPS platformu kullanılarak konfigure edilmiştir [33]. Microblaze işlemcisi içerisinde kullanılan çevresel birimlerden birkaçı aşağıda sıralanmıştır.

- Microblaze işlemci çekirdeği
- DDR2 RAM
- XPS Kesme Kontrol Birimi
- DIP Switch 8 Bit
- LED 8 Bit
- TRF7970A Giriş Çıkış 10 Bit
- TRF7970A Kesme Girişi
- TRF7970A SPI
- Zamanlayıcı
- UART

Yapılan konfigürasyon sonrasında Microblaze işlemcisi çevreselleri ile beraber oluşturulmuş ve bu donanım tasarımı yazılım tasarımın yapılacağı Xilinx SDK platformuna taşınmıştır. Microblaze işlemcisi ve çevre birimlerine dair blok diyagram Şekil 5.15 ile verilmiştir.



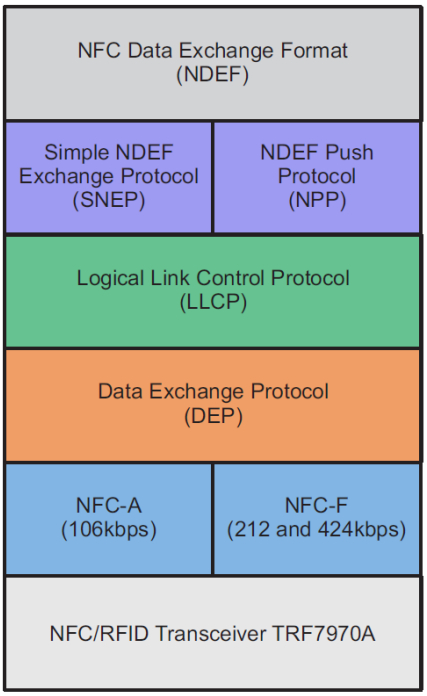
Şekil 5.15 : Eşten eşe modu için Microblaze işlemcisi ve çevre birimlerine dair blok diyagram.

SDK platformunda yapılan yazılım tasarımında ise öncelikle aşağıda sıralanan çevresellerin kullanıma hazırlanması amacıyla sürücü kodlar yazılmıştır.

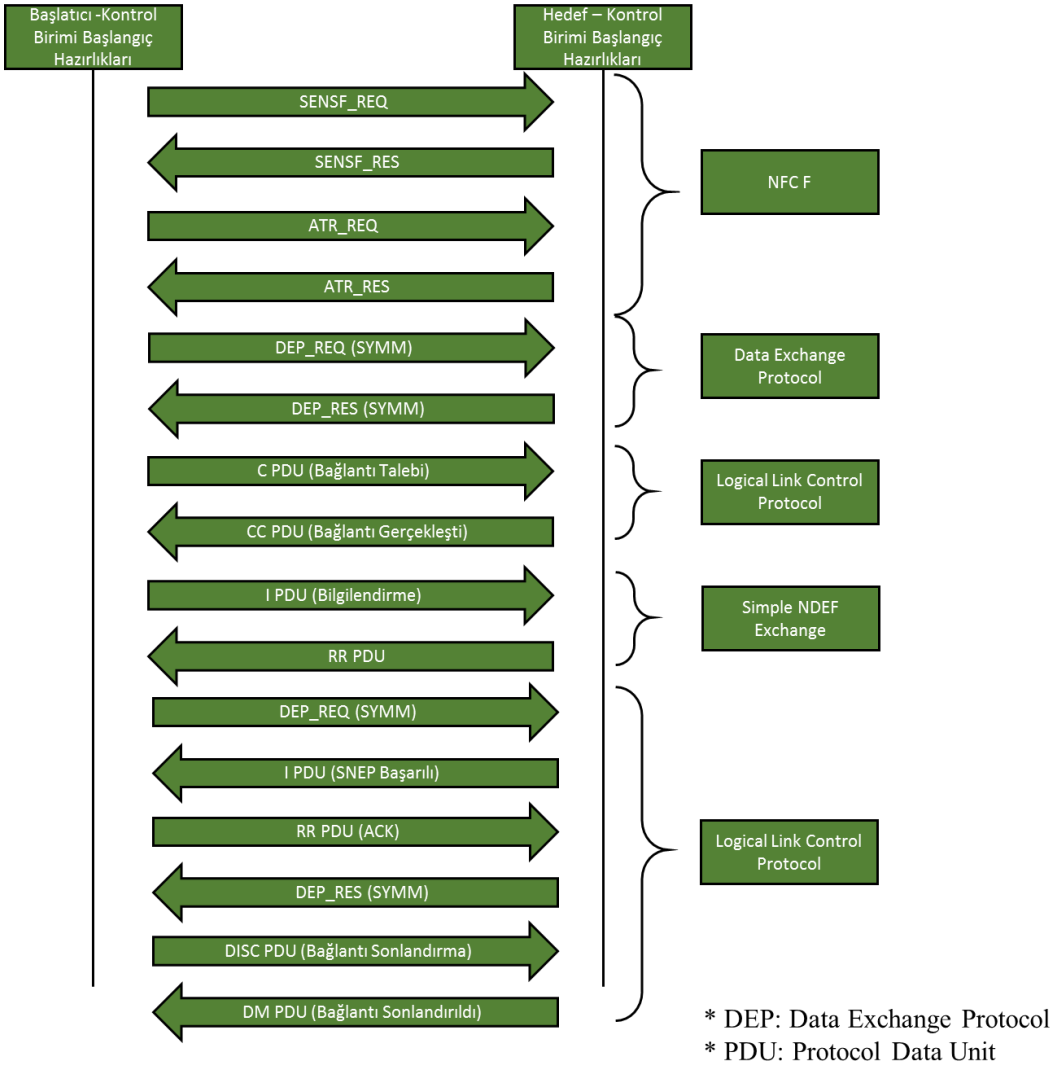
- Genel amaçlı giriş çıkışlar
- Kesmeler kontrol birimi
- SPI
- Zamanlayıcı

- UART

Bu aşamadan sonra Spartan-6 FPGA'sı kullanılarak hazırlanan kontrol birimi üzerinde NFC veri transfer yapısının kurulması için gerekli olan temel yapı hazır olarak nitelendirilebilecek durumdadır. Bu yapı üzerine Microblaze işlemcisi üzerinde gerçeklenen protokol katmanları Şekil 5.16'de, eşten eşe bağlantı modu ile alakalı akış Şekil 5.17 ile verilmiştir [24].



Şekil 5.16 : Eşten eşe bağlantı modu protokol katmanları.



Şekil 5.17 : Eşten eşe bağlantı modu akış diyagramı.

Gerçeklenen birinci aşamada kontrol birimi ve NFC alt sistem ikilisi aktif hedef modunda konfigure edilip eşten eşe bağlantı modu ile NFC etkin bir cep telefonuna 3.581 bayt boyutunda ve jpg formatında veri transferi gerçekleştirilmiştir. Aktarılan resim dosyası Şekil 5.18 ile verilmiştir. Kullanılan cihazlar ile alakalı görüntü ise Şekil 5.19 ile verilmiştir.

Şekil 5.18 : Eşten eşe bağlantı modu ile NFC özellikli cep telefonuna aktarılmış JPG formatlı resim dosyası.

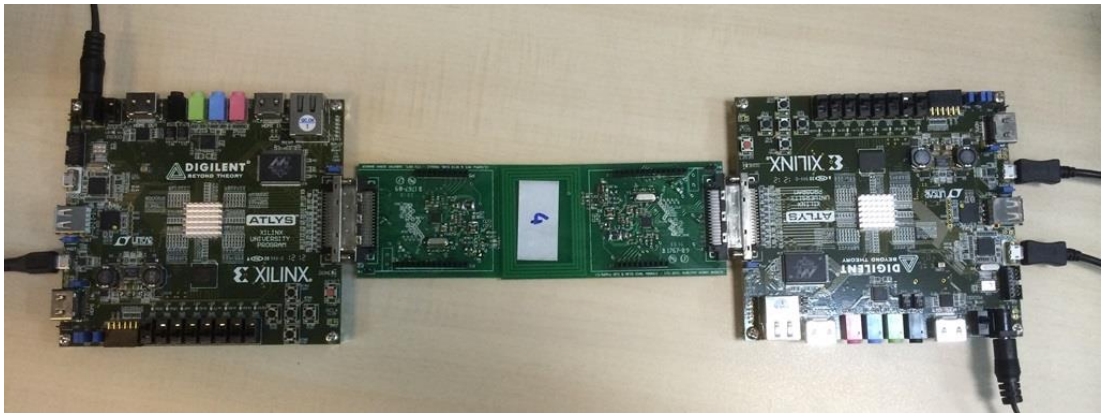
Şekil 5.19 : Eşten eşe bağlantı modu ile NFC etkin bir cep telefonuna resim dosyası aktarımı.

Yapılan çalışmada kontrol birimi içerisinde gerçeklenen adımlar aşağıdaki gibi sıralanabilir.

- Analog uç biriminin aktive edilmesi
- SPI çevreselinin konfigure edilmesi
- SPI arayüzü ile TRF7970A'ya mesaj gönderilmesi
- SPI arayüzü ile TRF7970A'dan mesaj okunması
- TRF7970A'nın konfigure edilmesi
    - 424kbps Aktif Hedef Modu konfigurasyonu
    - NFCID bilgisinin TRF7970A'ya yazılması
- NFC_F bağlantısının kurulması
- NFC DEP protokollerinin işletilmesi
- LLCP protokolünün işletilmesi
- SNEP protokolünün işletilmesi
- NDEF formatı ile veri gönderiminin gerçekleştirilmesi

Bu aşama sonrasında ise iki adet Atlys Spartan-6 geliştirme kiti kontrol birimi ile NFC alt sistem kartı ikilisi kullanılarak bir önceki aşamada olduğuna benzer bir

şekilde eşten eşe bağlantı modu ile veri aktarımı gerçekleştirilmiştir. Cihazlardan biri aktif başlatıcı, diğeri ise aktif hedef modunda konfigure edilerek cihazlar arasında hem resim dosyası hem de metin dosyası aktarımı gerçekleştirilmiştir. Aktarılan veriler her bir cihazın UART protokolü ile bağlı olduğu birer bilgisayar yardımıyla gözlemlenmiştir. Gerçekleştirilen bu aşama ile alakalı görüntü Şekil 5.20 ile paylaşılmıştır.



Şekil 5.20 : İki adet Atlys Spartan-6 geliştirme kiti kontrol birimi ile NFC alt sistem kartı ikilisi kullanılarak gerçekleştirilen eşten eşe bağlantı görüntüsü.

Gerçeklenen bu aşamalar sonrasında bölümün başında belirtilen NFC geliştirme ortamı üzerinde bir sonraki bölümde açıklanacak doğrulama protokolünün gerçeklenmesi için hazır hale gelmiştir.

6. DOĞRULAMA PROTOKOLÜNÜN GERÇEKLENMESİ

Bu bölümde Bölüm 3.1'de anlatılmış olan Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolünün eşten eşe modu ile birbiri ile NFC teknolojisi ile haberleşebilen ve yazılım / donanım ortak tasarımını destekleyen cihazlar üzerinde gerçeklenmesi anlatılacaktır [18]. Söz konusu protokol dâhilinde gerçeklenmesi gereken alt modüller özel tasarım donanımlar halinde FPGA üzerinde kapı seviyesinde tasarlanmıştır. Sonrasında bu alt modüller Xilinx Platform Studio ortamı kullanılarak Microblaze işlemcisi ile beraber FPGA içerisine gömülmüştür. Protokol adımları NFC veri transfer adımlarının gerçeklenmesinde olduğu gibi Microblaze işlemcisi içerisinde gerçeklenmiştir. NFC veri transfer adımlarının gerçeklenmesinden farklı olarak protokol için gerekli olan adımlara dair işlem veya fonksiyonlar tasarlanan özel tasarım donanımlara erişim sağlanarak gerçeklenmiştir.

Doğrulama protokolünün gerçeklenmesinden sonra söz konusu protokol NFC veri transfer akışı ile entegre edilmiştir. Bu işlem ile NFC veri transferi öncesinde anahtar paylaşımı sağlanmıştır. Sonrasında paylaşılan anahtarlar ile şifrelenmiş verinin NFC teknolojisi ile aktarılması, karşı taraf tarafından da şifrelenmiş verinin çözülmesi işlemleri ile NFC özellikli cihazlar arasında şifreli veri aktarımı gerçeklenmiştir.

6.1 Gerçeklenen Donanım Alt Modülleri

Bölüm 3.1'de anlatılmış olan doğrulama protokolünün adımları detaylı olarak incelendiğinde doğrulama protokolünün gerçeklenmesi için NFC teknolojisi ile haberleşecek karşılıklı birimlerde aşağıda sıralanan modüllerin tasarlanması gerekmektedir.

- TEA şifreleme modülü
- Özet fonksiyonu modülü
- Rastgele sayı üreteci modülü
- 96 bit özel veya modülü

Yukarıda sıralanan modüllere ek olarak NFC veri transfer akışında şifreli olarak aktarılacak verinin şifre çözme işlemine tabi tutulması aşamasında kullanılacak olan TEA şifre çözme modülü de bu bölümde anlatılmıştır.

6.1.1 Küçük şifreleme algoritması modülleri

6.1.1.1 Kullanılan alt bloklar

TEA şifreleme ve şifre çözme modülleri kendi içerisinde aşağıda sıralanan alt blokları barındırmaktadır [49].

- Toplama ve çıkarma blokları
- Mantıksal kaydırma bloğu
- Özel veya bloğu

Toplama bloğu şifreleme ve şifre çözme yapılarında 32 bit uzunluklu iki sayıyı toplamak amacıyla tasarlanmıştır. Sistemin daha hızlı hale getirmek amacıyla seri toplama yerine paralel toplama bloğunun tasarlanması tercih edilmiştir. Toplama bloğu şifre çözme ve şifreleme yapılarında çok sayıda kullanılacağı için tasarımda az yer kaplaması oldukça önem arz etmektedir. Söz konusu toplama bloğu iki adet 32 bit uzunluklu sayıyı girişlerinden alarak bu iki sayının toplamlarını çıkışından yine 32 bit uzunluklu olarak vermektedir. Toplama işleminin sonucu belirli değerler toplandığında 33 bit uzunluklu olduğunda ise en anlamlı biti yok sayarak diğer 32 biti çıkışa vermektedir.

Çıkarma bloğu ise şifre çözme modülü içerisinde kullanılmaktadır. Bu blok girişinden aldığı iki adet 32 bitlik sayının farkını alıp çıkışından yine 32 bit olarak vermektedir.

Mantıksal kaydırma bloğu yapısında her bir döngüde iki tane sola 4 bit kaydırma işlemi 2 tane de sağa 5 bit kaydırma işlemi bulunmaktadır. Bu sağa ve sola bit kaydırma işlemleri tek bir blok tasarlanarak gerçekleştirilmiştir. Sadece içerisindeki parametreler değiştirilerek bu blok istenilen uzunlukta istenilen tarafa doğru kaydırma işlemi yapabilmektedir. Blokta 5 bit uzunluklu *lenght*, 32 bit uzunluklu *value_in* ve 1 bit uzunluklu *direction* girişleri bulunmaktadır. Bloğun çıkışı ise 32 bit uzunluklu *result* değeridir. Blokta yön seçme girişi yüksek iken blok sol tarafa kaydırma işlemi yön seçme girişi düşük iken sağ tarafa doğru kaydırma işlemi

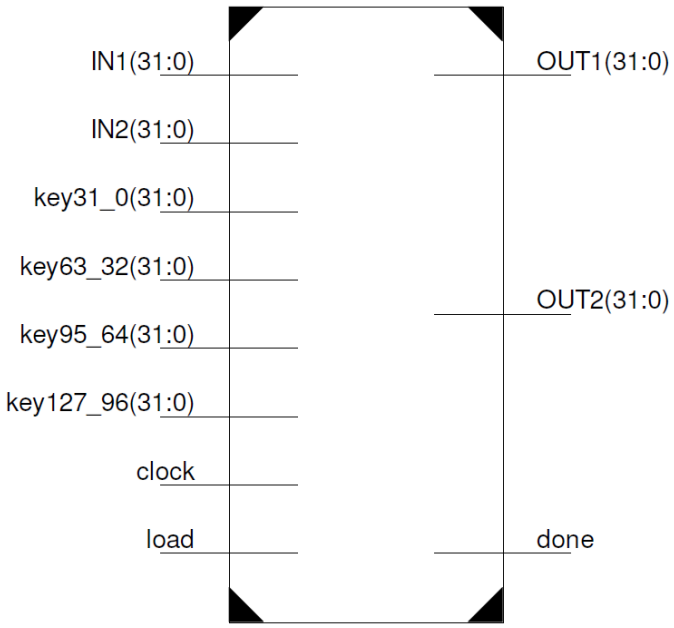
yapmaktadır. Bloğun ne kadar uzunlukta kaydırma yapacağı ise bloğun *lenght*, girişi değiştirilerek ayarlanmaktadır. Blok 4 bit sola kaydırma işlemi için kullanıldığında seçme girişi yüksek seçilip kaydırma uzunluğu girişi de 4 seçilerek kaydırılmak istenen 32 bit uzunluklu veri girilir. Blok 4 bit sola kaydırılmak istenen sayının her bir bitini 4 defa bir yüksek anlamlı bite taşır ve en sağda kalan 4 boş bitleri de sıfır değeri ile doldurur. Yine 5 bit sağa kaydırma işleminde ise seçme girişi düşük seçilip kaydırma uzunluğu 5 seçilerek kaydırılmak istenen 32 bit uzunluklu veri girişe uygulanır. Blok 5 bit sağa kaydırılmak istenen sayının her bir bitini 5 defa bir düşük anlamlı bite kaydırır. Bu işlem sonucunda en sağda kalan 5 bite sıfır değeri atanır.

Özel veya bloğu; şifreleme bloğunun içerisinde bir tur içinde iki adet ihtiyaç duyulan bir bloktur. Tasarım aşamasında kullanılacak özel veya bloğu 32 bit uzunluklu üç adet veri girişi barındırmalıdır. Bu blok girişine uygulanan üç verinin özel veya işlemine girmesiyle 32 bit uzunluklu çıkış verisi üretmektedir.

Yukarıda sıralanan şifreleme ve şifre çözme donanımlarının alt donanım bloklarının tasarımları tamamlandıktan sonra TEA şifreleme ve TEA şifre çözme üst blokları tasarlanmıştır. Şifreleme ve şifre çözme modüllerinin donanımda mümkün olduğunca az alan kaplaması ve az güç tüketmesi amacı doğrultusunda TEA şifreleme ve şifre çözme modüllerinin saat işareti ile eş zamanlı olarak çalıştırılması tercih edilmiştir. Tasarlanan saat işaretine sahip TEA şifreleme modülü FPGA üzerinde yalnızca 231 dilim, şifre çözme modülü ise 182 dilim kaplamaktadır.

6.1.1.2 Küçük şifreleme algoritmasi şifreleme modülü

TEA şifreleme modülünün genel yapısı Şekil 6.1'de görüldüğü gibidir. Şifreleme modülü donanımı 4 adet mantıksal kaydırma, 8 adet toplama ve 2 adet özel veya bloğu içermektedir. Verilog dili kullanılarak bu alt bloklar birbirlerine Şekil 3.4'de gösterilen yapı doğrultusunda bağlanmıştır. Bu bağlama işlemleri yapılırken her bir bağlantıya birer kablo ya da kaydediciler atanarak bu kablolar ve kaydediciler şifreleme yapısını sağlayacak şekilde alt donanımların giriş ve çıkışlarına atanmışlardır. Şifreleme kısmında her bir döngüde farklı olmak üzere kullanılacak delta değişken değerleri ise hesabı fazladan alan yükü getirmemesi amacıyla Denklem 2.1 kullanılarak Matlab programı yardımı kullanılarak hesaplanmış ve dizi halinde kodun içerisine yerleştirilmiştir.



Şekil 6.1 : Saat işaretli TEA şifreleme modülü.

Söz konusu modülün sekiz girişi ve üç çıkışı bulunmaktadır. Girişlerden ilk ikisi şifrelenecek verinin alınacağı iki adet 32 bit'lik kablolardır. Sonraki dört giriş ise şifrelemede kullanılacak 128 bitlik anahtara ait dört adet 32 bit'lik kablolardır. Diğer iki girişten ilki ise saat işaretinin uygulanacağı 1 bit'lik kablo, ikincisi ise giriş mesajı ve anahtarın modülün girişine yüklendiğinin ve şifreleme işleminin başlayabilir olduğunun anlaşılacağı 1 bitlik kablodur.

Söz konusu modülün Microblaze işlemcisi ile haberleştirilebilir olması için maksimum veri genişliği Microblaze veri genişliği kadar yani 32 bit olarak ayarlanmıştır.

Bloğun kullanımı için öncelikle şifrelenecek veri ve anahtarın bloğun girişine uygulanması gerekmektedir. Bu aşama sonrasında *load* girişi yüksek seviye çekilir. Böylece modüle şifreleme işleminde kullanılacak giriş verilerinin güncel olduğunun bilgisi verilir. Bu aşamada alınan sayılar donanım içerisinde iki tane 32 bit uzunluklu kaydediciye atılmaktadır. Bunun sebebi şifrelenecek sayıların saat ile eş zamanlı biçimde işlenmesi için değişken bir değere atama gerekliliğidir. Aynı zamanda daha önceden hesaplanan delta değişken değerleri de başlangıçta bir kaydediciye atılmıştır. Sonrasında ise *load* girişi düşük seviyeye çekilir ve şifreleme işlemi başlatılır. TEA'nın yapısından da görüldüğü üzere şifreleme mekanizması 32 döngü sonunda tamamlanmaktadır. Döngü sayısını kontrol etmek için bloğun içerisine bir sayıcı eklenmiştir. Sayıcıya başlangıçta 1 değeri atanmakta ve her saat darbesinde

sayıcı bir değer arttırılmaktadır. Sayıcı değişkeni 32 değerini aldığında şifreleme tamamlanmış olur ve söz konusu modül *done* isimli çıkışını yüksek seviyeye çeker. Şifreleme modülünün içinde kullanıldığı üst modül tarafından bu işaret takip edilerek *done* sinyalinin lojik 1 olduğu zaman şifrelenmiş verinin modülün çıkışlarından okunabilir durumda olduğu anlaşılır. Bu süreç boyunca saat işareti modül girişine sürekli uygulanmaktadır.

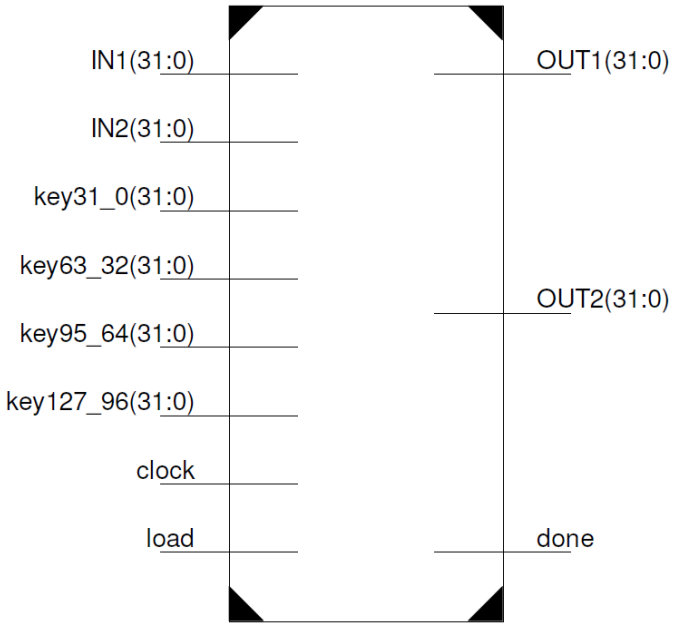
Tasarlanan modülün ISE ortamındaki benzetimi EK B'de verilmiştir. Benzetime dair giriş ve çıkışlar Çizelge 6.1'deki gibidir.

Çizelge 6.1 : TEA şifreleme modülüne dair giriş ve çıkış değerleri.

Girişler	Değerler	Çıkışlar	Değerler
IN1	32'h20FF9b64	OUT1	32'h24be9182
IN2	32'h37FF4e28	OUT2	32'hd7c5d5b9
key31_0	32'hAAFF4e28		
key63_32	32'hBBFF4e28		
key95_64	32'hCCFF4e28		
key127_96	32'hDDFF4e28		

6.1.1.3 Küçük şifreleme algoritmasi şifre çözme modülü

TEA şifre çözme modülünün genel yapısı ise şifreleme modülüne benzer şekilde Şekil 6.2'de görüldüğü gibidir.



Şekil 6.2 : Saat işaretli TEA şifre çözme modülü.

Şifre çözme bloğu Şekil 3.5'da görülen akış doğrultusunda tasarlanmıştır. Bu modülde de şifreleme modülüne benzer bir şekilde Şekil 3.4 verilen turun 32 defa tekrarlanması ile tamamlanmaktadır. Şifreleme modülünden farkı işlemler sırasında anahtarların ters dönmesi ve ana kollardaki toplama bloklarının yerlerini çıkarma bloklarının almasıdır. Şifre çözme modülü donanımı 4 adet mantıksal kaydırma, 2 adet çıkarma 8 adet toplama ve 2 adet özel veya bloğu içermektedir. Delta değişken değerleri şifreleme modülünde olduğu gibi yine kodun içerisine yerleştirilmiştir.

Söz konusu modülün giriş ve çıkışları yine şifrelemede olduğuna benzer bir şekilde sekiz giriş ve üç çıkıştır. Girişlerden ilk ikisi şifrelenmiş verinin alınacağı iki adet 32 bit'lik kablolardır. Sonraki dört giriş ise şifre çözmede kullanılacak 128 bitlik anahtara ait dört adet 32 bit'lik kablolardır. Diğer iki girişten ilki ise saat işaretinin uygulanacağı 1 bit'lik kablo, ikincisi ise giriş mesajı ve anahtarın modülün girişine yüklendiğinin ve şifre çözme işleminin başlayabilir olduğunun anlaşılacağı 1 bitlik kablodur.

Söz konusu modülün Microblaze işlemcisi ile haberleştirilebilir olması için maksimum veri genişliği Microblaze veri genişliği kadar yani 32 bit olarak ayarlanmıştır.

Bloğun kullanımı şu şekildedir; öncelikle şifrelenmiş veri ve anahtarın bloğun girişine uygulanmalıdır. Bu aşama sonrasında *load* girişi yüksek seviye çekilir. Böylece modüle şifre çözme işleminde kullanılacak giriş verilerinin güncel olduğunun bilgisi verilir. Bu aşamada alınan sayılar donanım içerisinde iki tane 32 bit uzunluklu kaydediciye atılmaktadır. Aynı zamanda kodun içerisine yerleştirilmiş olan delta değişken değerleri de başlangıçta bir kaydediciye atılmıştır. Sonrasında ise *load* girişi düşük seviyeye çekilir ve şifre çözme işlemi başlatılır. TEA'nın yapısından da görüldüğü üzere şifre çözme mekanizması 32 döngü sonunda tamamlanmaktadır. Döngü sayısını kontrol etmek için bloğun içerisine bir sayıcı eklenmiştir. Sayıcıya başlangıçta 0 değeri atanmakta ve her saat darbesinde sayıcı bir değer arttırılmaktadır. Sayıcı değişkeni 31 değerini aldığında şifre çözme işlemi tamamlanmış olur ve söz konusu modül *done* isimli çıkışını yüksek seviyeye çeker. Şifre çözme modülünün içinde kullanıldığı üst modül tarafından bu işaret takip edilerek *done* sinyalinin lojik 1 olduğu zaman çözülmüş verinin modülün çıkışlarından okunabilir durumda olduğu anlaşılır. Bu süreç boyunca saat işareti modül girişine sürekli uygulanmaktadır.

Tasarlanan modülün ISE ortamındaki benzetimi EK C'de verilmiştir. Benzetime dair giriş ve çıkışlar aşağıdaki gibidir.

Çizelge 6.2 : TEA şifre çözme modülüne dair giriş ve çıkış değerleri.

Girişler	Değerler	Çıkışlar	Değerler
IN1	32'h24be9182	OUT1	32'h20FF9b64
IN2	32'hd7c5d5b9	OUT2	32'h37FF4e28
key31_0	32'hAAFF4e28		
key63_32	32'hBBFF4e28		
key95_64	32'hCCFF4e28		
key127_96	32'hDDFF4e28		

Çizelge 6.1 ve Çizelge 6.2'de görüldüğü üzere TEA şifreleme ve şifre çözme modüllerine aynı anahtar kullanılarak şifrelenmiş veri şifre çözücü modül tarafından çözüldüğünde şifreleme modülünün girişindeki değerler ile şifre çözme modülünün çıkışındaki değerlerin aynı olduğu görülmüştür.

6.1.2 Özet fonksiyonu modülü

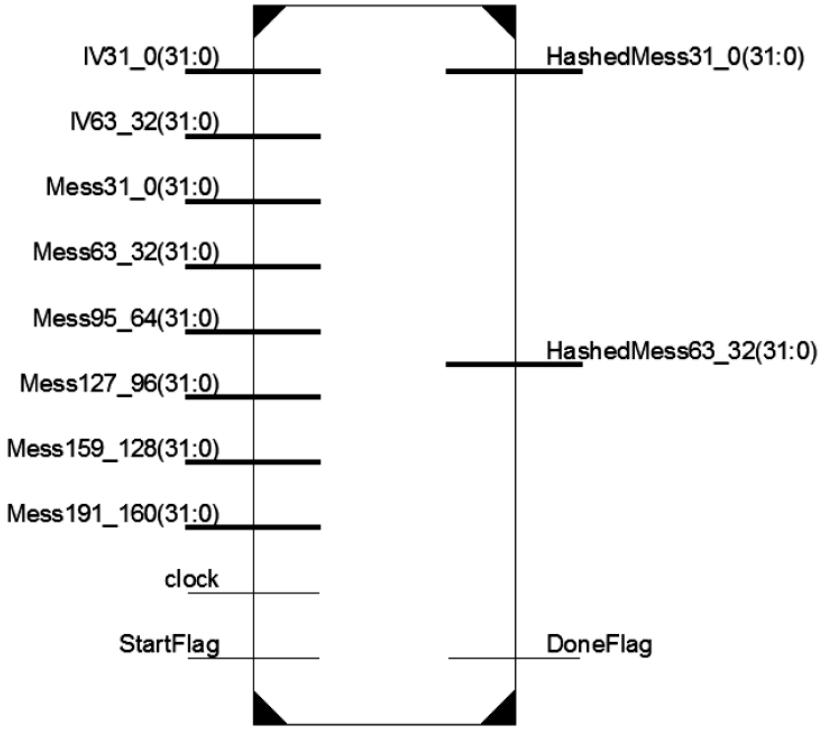
Bölüm 3.1'de anlatıldığı üzere protokol adımlarının gerçeklenmesi için bir özet fonksiyonunun kullanılması gerekmektedir. Söz konusu özet fonksiyonu için Şekil 3.2'da blok diyagramı verilen Davies-Meyer özet fonksiyonu tez çalışması kapsamında gerçeklenmiştir [19].

Şekil 3.2'da verilen blok diyagramda görüldüğü üzere özet fonksiyonunun H_{i-1} ve x_i olmak üzere iki girişi vardır. H_{i-1} girişine özet fonksiyonunun birinci turunda başlangıç vektörü, diğer turlarında bir önceki turun çıkışı verilir. x_i girişine ise özet fonksiyonu çıkartılacak veri girilir. Blok diyagramda *E* ile gösterilen kutu bir şifreleme modülünü ifade eder. Bu şifreleme modülü için Bölüm 6.1.1.2'de gerçeklenmesi anlatılan Küçük Şifreleme Algoritması Şifreleme Modülü kullanılmıştır [20].

Özet fonksiyonu modülü donanımı bir adet TEA şifreleme modülü kullanılarak gerçeklenmiştir. Ardışıl olarak tasarlanan bu modülde her tur için aynı TEA modülü kullanılarak düşük alanda modülün gerçeklemesi yapılmıştır.

Davies-Meyer özet fonksiyonunun gerçeklenmesi sırasında *E* modülüne giren H_{i-1} girişi TEA şifreleme modülünün şifrelenecek veri girişine (*IN1, IN2*) x_i girişi ise TEA şifreleme modülünün anahtar girişine bağlanmalıdır.

Gerçeklenecek protokol gereği 192 bit'lik verinin özet fonksiyonunun çıkarılmasının hedeflendiğinden ötürü, verinin TEA şifreleme modülünün 128 bit'lik anahtar girişine uygulanacağı düşünüldüğünde bu özet fonksiyonunun iki turda gerçeklenecek olduğu ortaya çıkmaktadır. İkinci turda x_i girişine uygulanabilecek 64 bit'lik veri kalacağı için ikinci turda giren veriye 64 bit'lik sabit bir sayı eklenerek veri 128 bit'e tamamlanmalıdır [18]. Modülün çıkışı ise TEA şifreleme modülünün çıkışının genişliğinde yani 64 bit'tir. Tasarlanan modül ile alakalı yapı Şekil 6.3 ile verilmiştir.



Şekil 6.3 : Özet fonksiyonu modülü

Söz konusu modülün 10 girişi 3 çıkışı bulunmaktadır. Girişlerden ilk ikisi başlangıç vektörünün uygulanacağını giriştir. Bunları takip eden 6 giriş ise özet fonksiyonu çıkartılacak verinin yükleneceği girişlerdir. Söz konusu modülün Microblaze işlemcisi ile haberleştirilebilir olması için maksimum veri genişliği Microblaze veri genişliği kadar yani 32 bit olarak ayarlanmıştır.

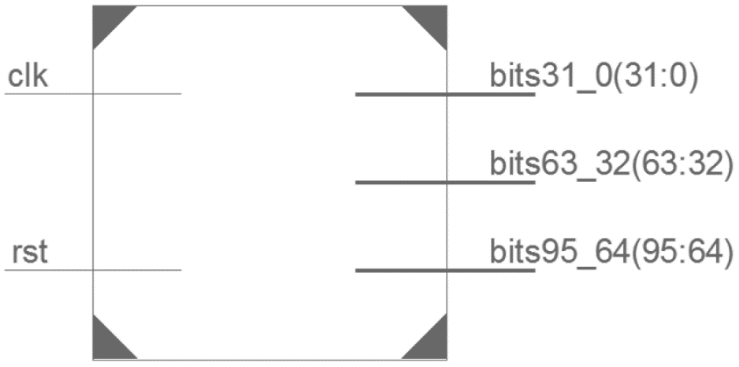
Bloğun kullanımı için öncelikle özet fonksiyonu alınacak veri ve başlangıç vektörü modülün girişlerine uygulanır. Bu aşama sonrasında *StartFlag* girişi yüksek seviyeye çekilir. Bu aşama sonrasında girişe uygulanan değerler modülün içindeki kaydedicilere aktarılır. Sonrasında *StartFlag* girişi düşük seviyeye getirilerek özet fonksiyonu üretme işlemi başlatılır. Özet fonksiyonu modülü iki turu tamamladığı

zaman *done* işaretini yüksek seviyeye çeker. Modülün içinde kullanıldığı üst modül tarafından söz konusu bu *done* işareti takip edilerek *done* işaretini yüksek seviyeye çekildiği zaman özet fonksiyonu modülünün çıkışları okunabilir duruma gelmiş olur. Bu süreç boyunca saat işareti modül girişine sürekli uygulanmaktadır. Modül içerisinde TEA şifreleme modülü iki kere kullanıldığı için özet fonksiyonu alma işlemi 64 saat darbesinde tamamlanır. Tasarlanan modülün ISE ortamındaki benzetimi EK D'de verilmiştir.

6.1.3 Doğrusal geribeslemeli kaydırma yazmacı modülü

Bölüm 3.1'de belirtildiği üzere Özet Fonksiyonu tabanlı RFID Karşılıklı Doğurulama Protokolü adımlarında doğrusal geri beslemeli kaydırma yazmacının kullanılması gerekmektedir. Şifreleme bloğunda oluğu gibi bu modül de bir özel donanım modülü olacak şekilde tasarlanmıştır.

Tasarımın genel yapısı Şekil 6.4 görülmektedir. Rastgele sayı üretimi için kullanılan bu bloğun çalışmasına değinilmesi gerekirse, modülün içerisine gömülmüş 96 bit'lik tohum verisi ilk saat darbesinde ilk çıkış değeri olarak atanmaktadır [50]. Takip eden her saat darbesinde farklı bir rastgele sayı modülün çıkışından vermektedir.



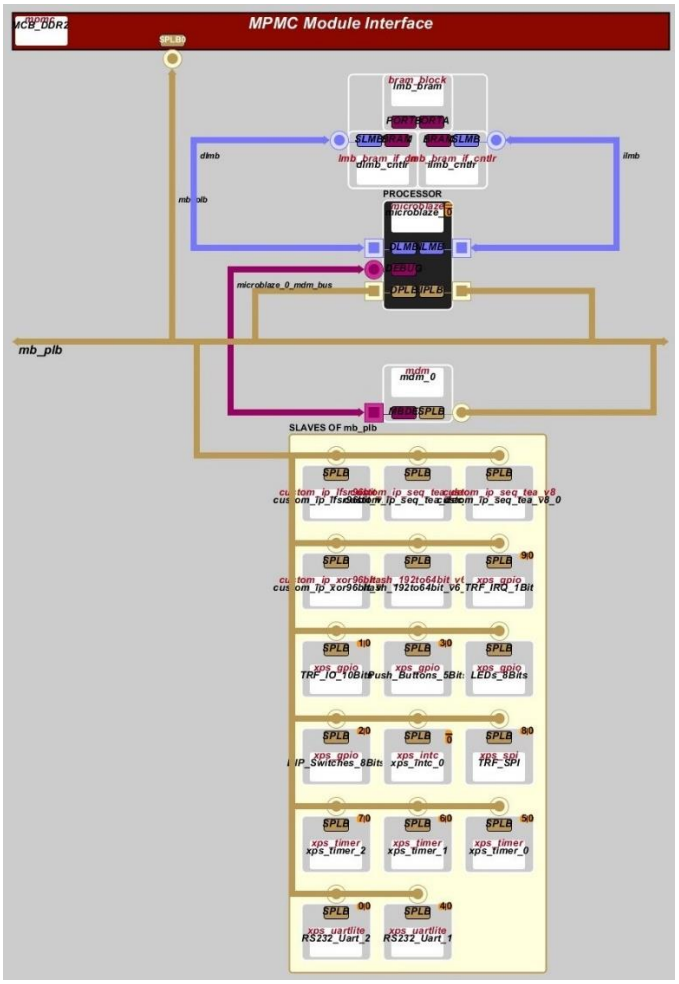
Şekil 6.4 : Doğrusal geri beslemeli kaydırma yazmacı bloğu.

96 bit uzunluklu bir LFSR'nin iç yapısı ise şu şekildedir. Modül ilk olarak içerisine gömülmüş olan 96 bit uzunluklu tohum değerini her saat işareti geldiğinde bir yüksek anlamlı bitine kaydırır. Her bit bir yüksek anlamlı basamağa kaydığı zaman boşta kalan en düşük anlamlı bit olan 0. bitine 95. 89. 86. ve 85. bitlerin özel veya değil işlemine tabii tutulmasıyla elde edilen değer atanır. Tüm bu işlemler sonucunda rastgele sayı üreteci bloğu her saat darbesinde 96 bitlik rastgele bir sayı üretmiş olur. Söz konusu modülün Microblaze işlemcisi ile haberleştirilebilir olması için maksimum veri genişliği Microblaze veri genişliği kadar yani 32 bit olarak

ayarlanmıştır. Bu doğrultuda 96 bitlik rastgele sayı üç adet 32 bit halinde çıkışa verilir.

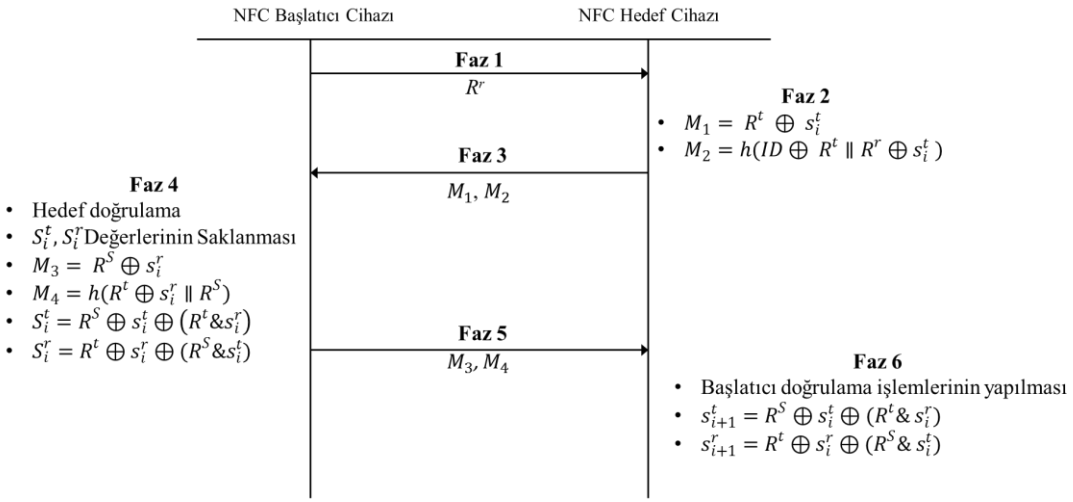
6.2 Doğrulama Protokol Gerçeklemesi

Bu aşamanın hedefi Bölüm 3.1'de anlatılan doğrulama protokolünün gerçeklenmesidir. Protokol adımları Microblaze işlemcisi içerisinde gerçeklenmiştir. Adımlar içerisinde kullanılması gereken fonksiyonlar ise Microblaze işlemcisinin Bölüm 6.1'de anlatılan donanım alt modüllerine erişmesi ile çalıştırılmıştır. Yapılan çalışmada tasarlanan alt modüller Bölüm 5.3.2 'de tasarlanan eşten eşe bağlantı modu için hazırlanmış Microblaze işlemcisi ve çevre birimleri yapısına eklenmiş ve doğrulama protokolünün NFC veri transfer akışı ile entegrasyonu aşaması için bir altyapı hazırlanmıştır. Söz konusu yapı ile ilişkili Microblaze işlemcisi ve çevre birimlerine dair blok diyagram Şekil 6.5 ile verilmiştir.



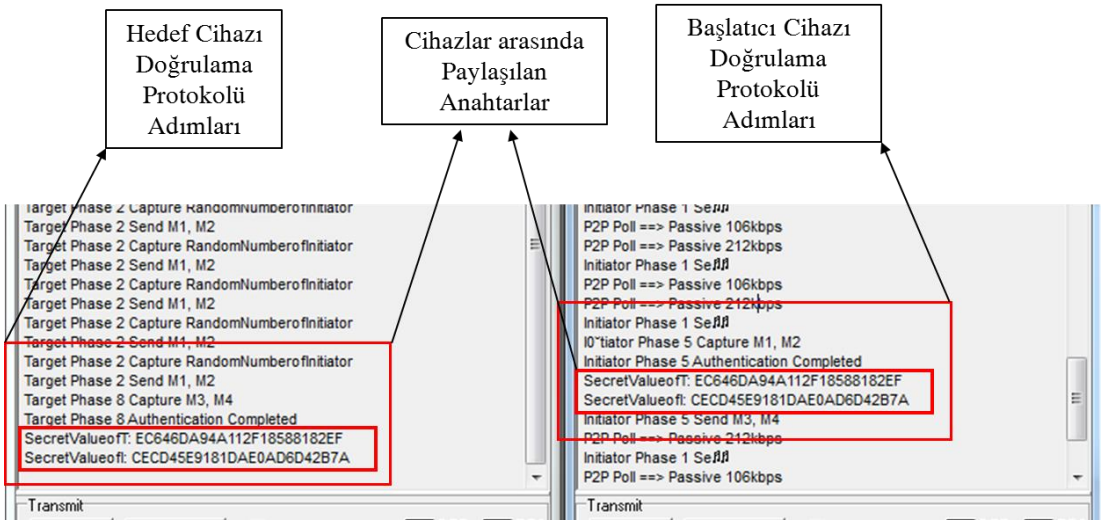
Şekil 6.5 : Doğrulama protokolü gerçeklemesi için Microblaze işlemcisi ve çevre birimlerine dair blok diyagram.

Bu aşama sonrasında Microblaze işlemcisi içerisinde söz konusu protokol adımlarına dair yazılım tasarımı gerçeklenmiştir. Bölüm 3.1'de anlatılan yapıda okuyucu, etiket ve veri bankası olarak adlandırılan birimler bulunmaktadır. Gerçeklemenin tez çalışması kapsamında NFC özellikli cihazlar için tasarlanacak olması ve bu doğrultuda NFC özellikli cihazların veri depolama kapasitelerinin RFID etiketleri ile karşılaştırılması veri bankası biriminin de NFC özellikli cihazlar üzerinde gerçeklenebilir olduğunu göstermektedir. NFC eşten eşe modu için bu yapının gerçeklenmesi düşünüldüğünde veri bankası ve okuyucu birimlerinde gerçekleştirilen adımlar NFC başlatıcı biriminde, etiket biriminde gerçekleştirilen adımlar ise NFC hedef modunda çalışan birim üzerinde gerçeklenebilir. Bu bakış açısıyla tez çalışması kapsamında düzenlenen doğrulama protokolü akışı Şekil 6.6 ile verilmiştir.



Şekil 6.6 : NFC eşten eşe modu için düzenlenen doğrulama protokolü adımları.

Şekil 6.6 ile verilen akışın Microblaze işlemcisi üzerinde gerçeklenmesi sonrasında iki adet Atlys Spartan-6 geliştirme kiti ile NFC Alt Sistem kartı ikilisi kullanılarak. NFC veri transfer akışından bağımsız bir şekilde kartlar çalıştırılıp anahtar paylaşımı işlemi gerçekleştirilmiştir. Söz konusu çalışma ile her bir birimin protokol adımlarını tamamlamasından sonra ürettiği anahtarlar UART üzerinden dışarıya gönderilerek bilgisayar ekranında görüntülenmiştir. Söz konusu ekran görüntüsü Şekil 6.7 ile verilmiştir.



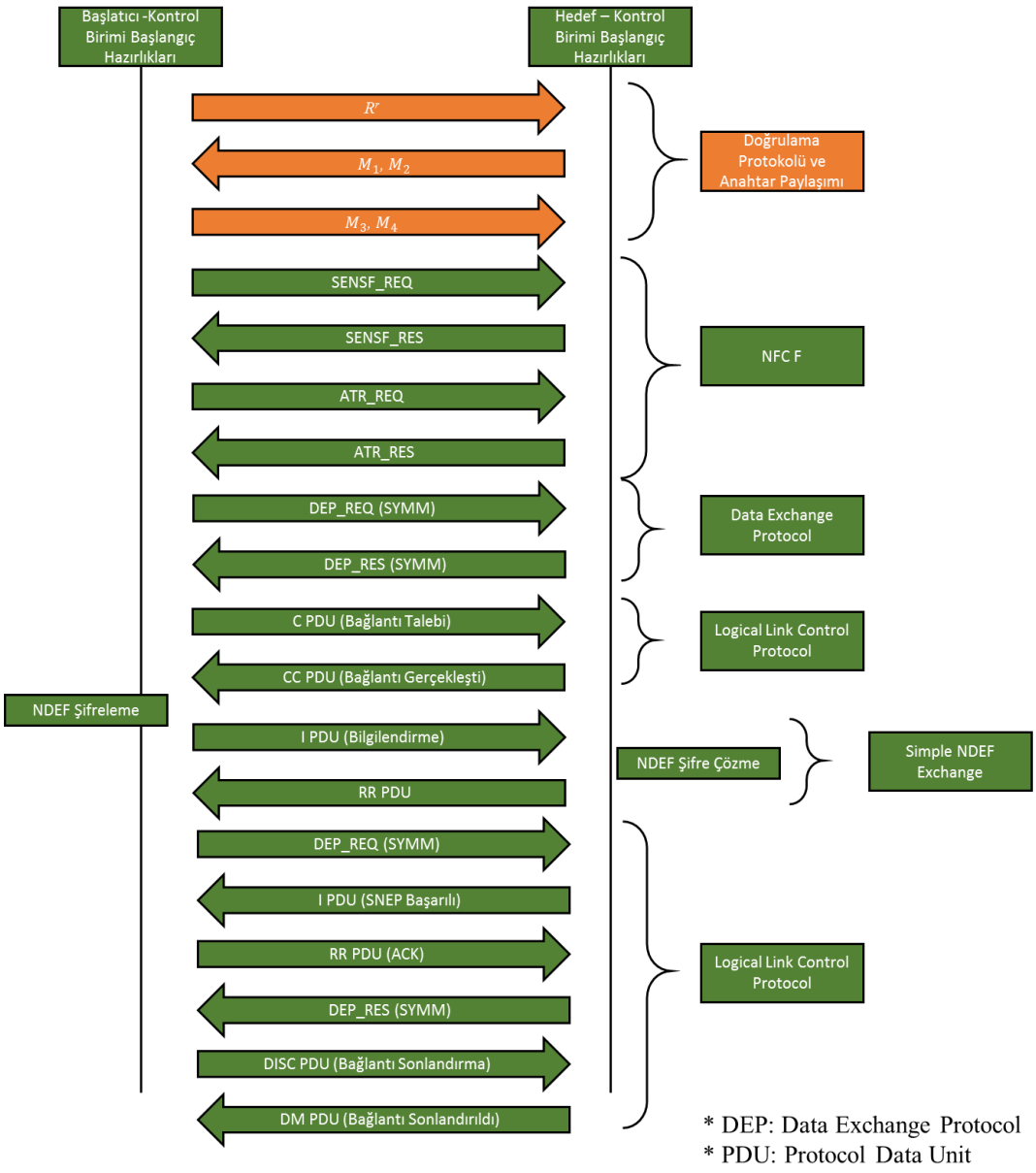
Şekil 6.7 : Cihazlar arası anahtar paylaşımına dair ekran görüntüsü.

6.3 Doğrulama Protokolünün NFC Veri Trasfer Akışı ile Entegrasyonu

Bu aşamada Bölüm 5.3.2 ’de anlatılan ve Şekil 5.17’de akışı verilen eşten eşe bağlantı modunda haberleşme akışı ile Bölüm 6.2’de anlatılan ve Şekil 6.6’de verilen doğrulama protokolü akışı birleştirilmiştir. Yenilenen protokol akışı Şekil 6.8 ile verilmiştir.

Şekil 6.8’de gösterilen birinci adımda R_r mesajının gönderimi başlatıcı birim tarafından belirli bir periyot ile karşı birim tarafından M_1 ve M_2 değerlerinin yakandığı duruma kadar sürekli olarak gerçekleştirilir. M_1 ve M_2 değerlerinin yakalanması durumunda Şekil 6.8’de verilen diğer adımlar sırasıyla işletilmektedir. Doğrulama protokolü ile ilişkili olan ilk üç adımın işletilmesi sonucunda Bölüm 6.2’de anlatıldığı gibi karşılıklı birimler arasında doğrulama ve anahtar paylaşımı işlemi tamamlanmış olur.

Doğrulama işleminin karşılıklı olarak tamamlanmasından sonra başlatıcı cihaz NFC veri transfer akışının ilk mesajı olan *SENSF_REQ* mesajını göndererek NFC veri transfer akışını başlatır. Bu aşama sonrasında sırasıyla NFC-F bağlantısı, Veri Paylaşım Protokolü, Mantıksal Bağlantı Protokolü, Temel NDEF Değişimi ve tekrar Mantıksal Bağlantı Protokolü işletilerek NFC veri transfer akışı tamamlanır.

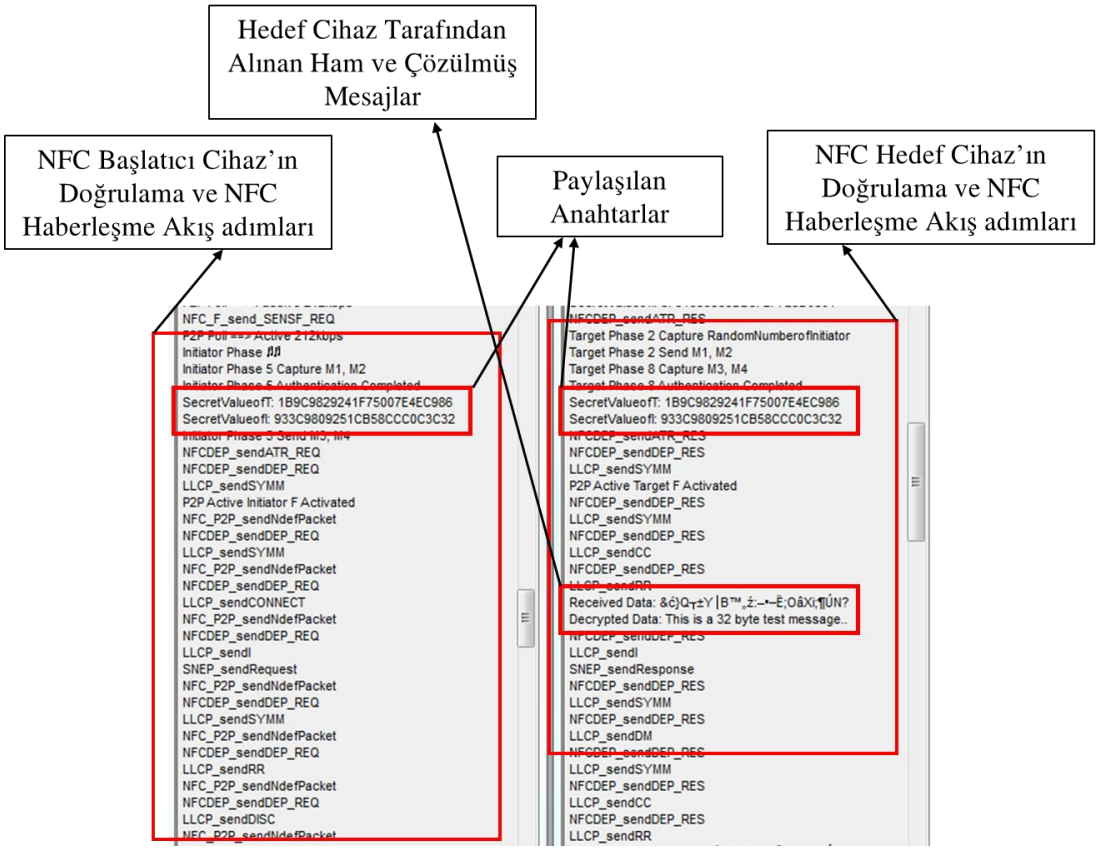


Şekil 6.8 : NFC ile güvenli haberleşme kanalı üzerinden veri aktarımına dair protokol akışı.

Temel NDEF Değişimi adımı NFC özellikli birimler arasında paylaşılacak verinin aktarıldığı adımdır. Başlatıcı birim tarafından paylaşılacak verinin akış içerisinde belirtilen *I_PDU* mesajının içerisine yerleştirilmesi aşaması öncesinde söz konusu veri bütünü Microblaze işlemcisinin donanım alt modüllere erişmesi ile TEA şifreleme modülü kullanılarak şifrelenir. Mesajın şifrelenmesinde doğrulama protokolü sonunda paylaşılan anahtar kullanılır. Bu adım sonrasında hedef cihaz tarafından yakalanan mesaj yine doğrulama protokolü sonunda elde edilmiş anahtar kullanılarak ve şifre çözme modülüne erişim sağlanarak şifre çözme işlemine tabi

tutulur. Nihayetinde şifrelenmemiş veri hedef birim tarafından elde edilir. Akışda belirtilen diğer adımlar haberleşmenin sonlandırılması ile ilişkilidir.

Yukarıda açıklanan adımlar ile NFC eşten eşe haberleşme modunda başlatıcı ve hedef cihazlar arasında güvenli bir kanal üzerinden veri paylaşımı gerçekleştirilmiştir. Söz konusu gerçekleme aşmasına dair mesaj akışı ile alakalı ekran görüntüsü Şekil 6.9'de verilmiştir.



Şekil 6.9 : Doğrulama protokolü sonrasında NFC eşten eşe haberleşmesine dair mesaj akışı.

Gerçeklenen NFC veri transfer akışı adımları içeriside NFC özellikli cihazlara dair kimlik bilgisi ilişkili standartlar gereği birimler arasında paylaşılmaktadır. Cihazların izlenebilirliğinin engellenemesi amacı ile söz konusu kimlik bilgisi değerlerine test edilen tüm cihazlarda aynı değerler verilmiştir. Bu yol ile olası bir ortadaki adam saldırısına maruz kalınması durumunda birimler arasında NFC veri transfer akışı adımlarında şifrelenmemiş halde aktarılan bu kimlik bilgilerinin elde edilmesi saldırıyı geçekleştiren birim tarafından anlamlandırılamayacaktır. Benzer bir bakış açısı ile söz konusu akış içerisinde aktarılan mesajların uzunlukları da sabit tutulmuştur.

7. SONUÇ VE ÖNERİLER

Bu yüksek lisans tez çalışmasında NFC ile güvenli uygulamalar için donanım/yazılım ortak sistem tasarımı ve gerçeklenmesi yapılmıştır. Çalışmanın ilk aşamasında NFC ile haberleşebilmek için TRF7970A analog uç birimi entegreleri kullanılarak NFC özellikli cihazların içerisinde bulunan NFC alt sistem yapısına karşılık düşecek iki adet haberleşme kartı tasarlanmış ve gerçeklenmiştir. Bu kartlar ile birlikte NFC kontrol birimi için iki adet FPGA geliştirme kiti üzerinde Microblaze işlemcisi kullanılmış ve birimler arasında kablosuz NFC veri transfer hattı kurulmuştur. Sonrasında söz konusu haberleşme hattının güvenlik uygulamalarında kullanılabilmesi için standartlarca tanımlanmış ve tez kapsamında yazılım ile gerçeklenmiş NFC protokollerine donanım/yazılım parçaları ile eklentiler yapılarak birimler arasında güvenli haberleşme kanalı kurulmuş ve bu kanal üzerinden şifreli veri aktarımı gerçekleştirilmiştir.

Bu tez çalışmasında NFC ile ilişkili aşağıdaki alanlarda literatür taraması yapılmıştır.

- NFC teknolojisine dair teknik özellikler
- Uygulama alanları
- Haberleşme kanalına uygulanabilecek ataklar
- Haberleşme kanalını gerçeklemek için kullanılacak teknik gerekler

Bu yol ile hem NFC teknolojisi hakkında detaylı bilgi edinilmiş hem de bu teknolojinin güvenlik açıkları incelenmiştir. Bu güvenlik açıklarının kapatılması ile ilişkili Bölüm 3.1 de anlatılan Özet Fonksiyonu Tabanlı RFID Karşılıklı Doğrulama Protokolü'nün kullanılması uygun bulunarak gerçeklenmiş ve NFC birimleri arasında güvenli haberleşme kanalı kurulması amacıyla kullanılmıştır. Gerçekleme ortamının uygulama ve protokol katmanları değiştirilebilir bir yapıda tasarlanmıştır. Bu bakış açısıyla geliştirilen deney düzeneği farklı uygulama ve protokol gerçeklemelerinde kullanılabilir.

Yapılan literatür araştırmalarında benzer bir uygulamaya rastlanmadığından ötürü yapılan tasarımın diğer çalışmalar ile karşılaştırılması mümkün olmamıştır.

KAYNAKLAR

[1] **Svítok, M.** (2014). Implementation of payment protocol on NFC-enabled mobile phone (yüksek lisans tezi), Masarykova Unıverzıta, Czech Republic.

[2] **NFC Forum**, http://www.nfc-forum.org, Alındığı tarih: 19.04.2014.

[3] **International Organization for Standardization/International Electrotechnical Commission**, (2004). ISO/IEC 18092 Information technology / Telecommunications and information exchange between systems / Near Field Communication / Interface and Protocol (NFCIP-1), ISO/IEC 18092:2004(E).

[4] **International Organization for Standardization/International Electrotechnical Commission**, (2012). ISO/IEC 21481 Information technology / Telecommunications and information exchange between systems / Near Field Communication / Interface and Protocol - 2 (NFCIP-2), ISO/IEC 21481:2012.

[5] **Want, R.** (2011). Near Field communication, IEEE Pervasive Computing.

[6] **Destot, M**. (2009). Several NFC initiatives in Europe, Forum des services mobiles sans contact-Mobile Contactless Services.

[7] **Shen**, **S.** (2012). Forecast: Mobile payment, Worldwide, 2009-2016, Gartner, Inc.

[8] **Haselsteiner, E., Breitfuß K.** (2013). Security in Near Field Communication (NFC) Strengths and Weaknesses.

[9] **Mulliner**, **C.** (2009). Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones, pages 695-700, ARES 2009, IEEE.

[10] **Madlmayr, G., Dillinger, O., Langer, J., Schaffer, C., Kantner, C. and Scharinger**, **J.** (2007). The benefit of using sim application toolkit in the context of near field communication applications for mobile applications, ICMB 2007, vol. 06, p. 7.

[11] **ISO/IEC 14443-1**. (2008). Identification cards - Contactless integrated circuit(s) cards - Proximity cards:Part 1: Physical characteristics. 2nd edition. Geneva, Switzerland: ECMA International.

[12] **ISO/IEC 14443-2**. (2001). Identification cards - Contactless integrated circuit(s) cards - Proximity cards:Part 2: Radio frequency power and signal interface. 1st edition. Geneva, Switzerland: ISO.

[13] **ISO/IEC 14443-3**. (2001). Identification cards - Contactless integrated circuit(s) cards Proximity cards:Part 3: Initialization and anticollision. 1st edition. Geneva, Switzerland: ISO.

[14] **ISO/IEC 14443-4**. (2008). Identification cards - Contactless integrated circuit(s) cards - Proximity cards:Part 4: Transmission protocol. 2nd edition. Geneva, Switzerland: ISO.

[15] **Ruiz, I. L., Gomez-Nieto**, **M. A.** (2008). University Smart Poster: Study of NFC Technology Applications for University Ambient, Proc. 3rd Symposium of Ubiquitous Computing and Ambient Intelligence, Salamanca, İspanya, Springer, 112-116.

[16] **Ghiron, S. L., Sposato S., Medaglia, C. M. et al.** (2009). NFC Ticketing: A Prototype and Usability Test of an NFC-Based Virtual Ticketing Application, Proc. 1st International Workshop on Near Field Communication, Hagenberg, Avusturya, IEEE, 2009, 45-50.

[17] **The Open Web Application security project (OWASP)**, "Man-in-the-middle attack", https://www.owasp.org/index.php/Man-in-the-middle_attack, Alındığı tarih: 11.04.2012.

[18] **Dehkordi, M.H., ve Farzaneh, Y.** (2014). Improvement of the Hash-Based RFID MutualAuthentication Protocol. *Wireless Pers Commun*, 75:219–232.

[19] **Menezes, A., Oorschot, P.V., Vanstone, S.** (1996). *Handbook of Applied Cryptography.* CRC Press.

[20] **Andem, V.R.** (2003). A Cryptanalysis of the Tiny Encryption Algorithm (yüksek lisans tezi),The University of Alabama, Alabama.

[21] **Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A.,** (1997). Handbook of Applied Cryptography, pp. 195-198, CRC Press.

[22] **Texas Instruments**, Multi-Protocol Fully Integrated 13.56-MHz RFID Writer/Reader IC, http://www.ti.com/lit/ds/symlink/trf7970a.pdf, Alındığı tarih: 19.04.2014.

[23] **Texas Instruments**, NFC Card Emulation Using the TRF7970A, http://www.ti.com/lit/an/sloa208/sloa208.pdf, Alındığı tarih: 13.08 2014.

[24] **Texas Instruments**, NFC Active and Passive Peer-to-Peer Communication Using the TRF7970A Application Report, http://www.ti.com/lit/ds/symlink/msp430g2213.pdf, Alındığı tarih: 19.04.2014.

[25] **Texas Instruments**, TRF7970A Multiprotocol Fully Integrated 13.56-MHz RFID and Near Field Communication (NFC) Transceiver IC, http://www.ti.com/lit/ds/symlink/trf7970a.pdf, Alındığı tarih: 19.04.2014.

[26] **Texas Instruments**, MSP430 LaunchPad Value Line Development kit, http://www.ti.com/tool/msp-exp430g2, Alındığı tarih: 13.08 2014.

[27] **Texas Instruments**, Mixed Signal Microcontroller veri sayfası, http://www.ti.com/lit/ds/symlink/msp430g2213.pdf, Alındığı tarih: 19.04.2014.

[28] **Texas Instruments**, Code Composer Studio (CCS) Integrated Development Environment (IDE), http://www.ti.com/tool/CCSTUDIO, Alındığı tarih: 13.08 2014.

[29] **IAR Systems**, IAR Embedded Workbench for Atmel AVR, http://www.iar.com/Products/IAR-Embedded-Workbench/AVR/, Alındığı tarih: 13.08 2014.

[30] **Atlys™ Spartan-6 FPGA Development Board**, http://www.digilentinc.com, Alındığı tarih: 10.12.2013.

[31] **Xilinx**, (2007). MicroBlaze Processor Reference Guide.

[32] **Xilinx**, Platform Studio and the Embedded Development Kit, http://www.xilinx.com/tools/platform.htm, Alındığı tarih: 13.08 2014.

[33] **Xilinx**, Xilinx Platform Studio, http://www.xilinx.com/tools/xps.htm, Alındığı tarih: 13.08.2014.

[34] **Xilinx**, Xilinx Software Development Kit, http://www.xilinx.com/tools/sdk.htm, Alındığı tarih: 13.08 2014.

[35] **ECMA International**. (2003). ECMA-352, Near Field Communication Interface and Protocol (NFCIP-2).

[36] **ECMA International**. (2004). ECMA-340, Near Field Communication Interface and Protocol (NFCIP-1).

[37] **GSMA Association**. Official Document TS.26 – NFC Handset Requirements, Version 6.0, Alındığı tarih: 21.07.2014.

[38] **NXP Semiconductors**. (2014). *CLRC663*, Revision 3.8.

[39] **Texas Instruments**, Multi-Protocol Fully Integrated 13.56-MHz RFID Writer/Reader IC, http://www.ti.com/lit/ds/symlink/trf7960a.pdf, Alındığı tarih: 19.04.2014.

[40] **ST Microelectronics**. (2014). *ST95HF*, Rev 3.

[41] **Texas Instruments**. (2011). *TRF7970A Evaluation Module (EVM).*

[42] **Texas Instruments**, MSP430 LaunchPad Value Line Development kit, http://www.ti.com/tool/msp-exp430g2, Alındığı tarih: 13.08 2014.

[43] **Texas Instruments**, TF796x HF-RFID Reader Layout Design Guide, http://www.ti.com/lit/an/sloa139/sloa139.pdf, Alındığı tarih: 13.08 2014.

[44] **NFC ForumTM,** (2012). NFC Analogue Specification – Technical Specification, Analog1.0, NFC Forum-TS-Analog-v1.0.

[45] **FINKENZELLER, K**. (2010). RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication. 3rd ed., Wiley.

[46] **Texas Instruments**, Antenna Matching for the TRF7960 RFID Reader, http://www.ti.com/lit/an/sloa135a/sloa135a.pdf, Alındığı tarih: 19.04.2014.

[47] **SONMICRO**. (2008). *SM130*, Revision A.8, https://www.sparkfun.com/datasheets/Sensors/ID/SM130.pdf, Alındığı tarih: 13.08.2014.

[48] **Kara Yolları Genel Müdürlüğü**, KGS, http://www.kgm.gov.tr/Sayfalar/KGM/SiteTr/Otoyollar/KGS.aspx, Alındığı tarih: 13.08.2014.

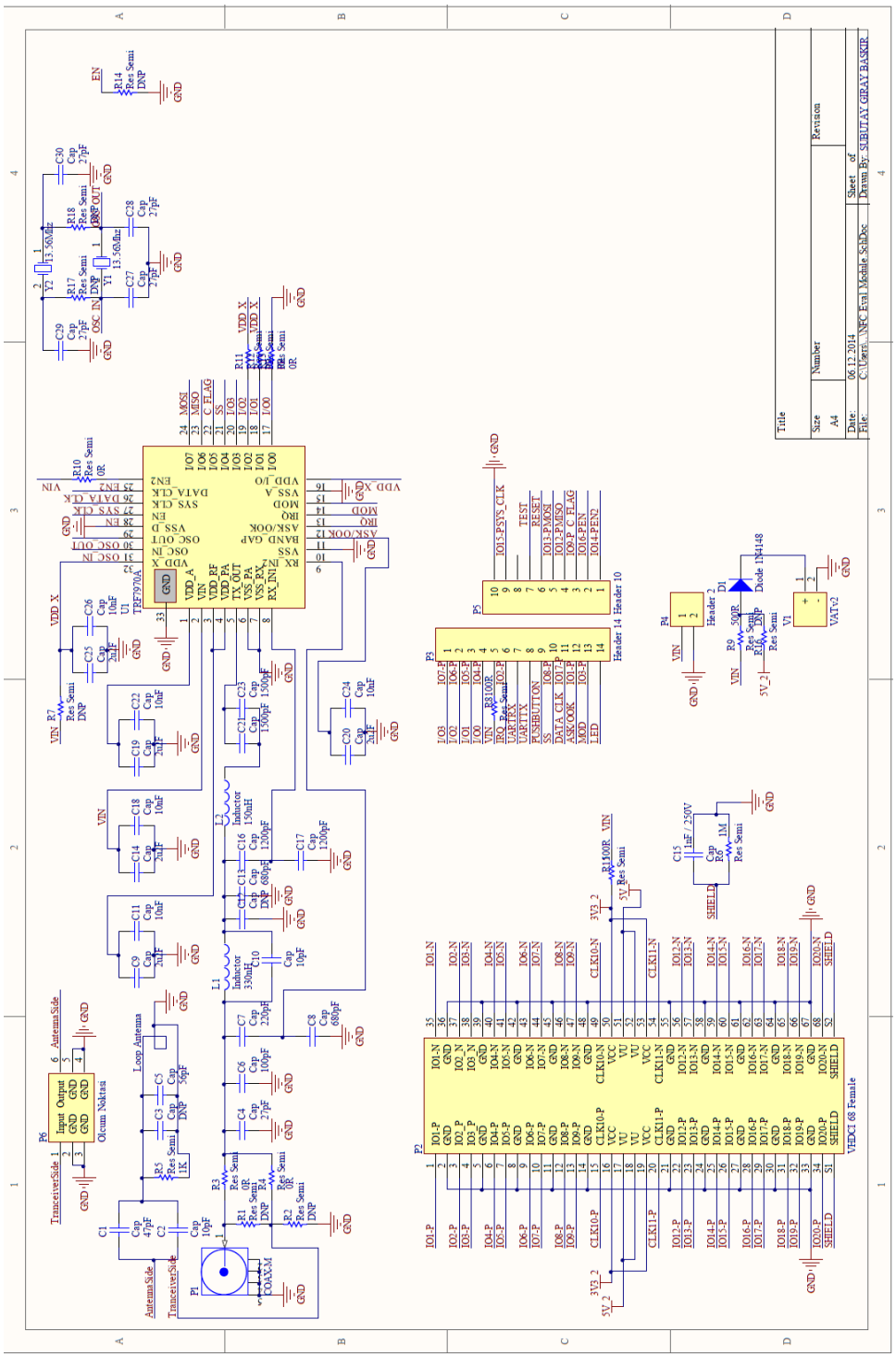
[49] **Alparslan, S.** (2012) Güvenli RFID Sistemleri İçin Bir Kimlik Doğrulama Protokolünün Gerçeklenmesi (lisans tezi), İstanbul Teknik Üniversitesi, İstanbul

[50] **Ward, R., Molteno T.** Table of Linear Feedback Shift Registers, http://courses.cse.tamu.edu/csce680/walker/lfsr_table.pdf, Alındığı tarih: 13.11.2014.

EKLER

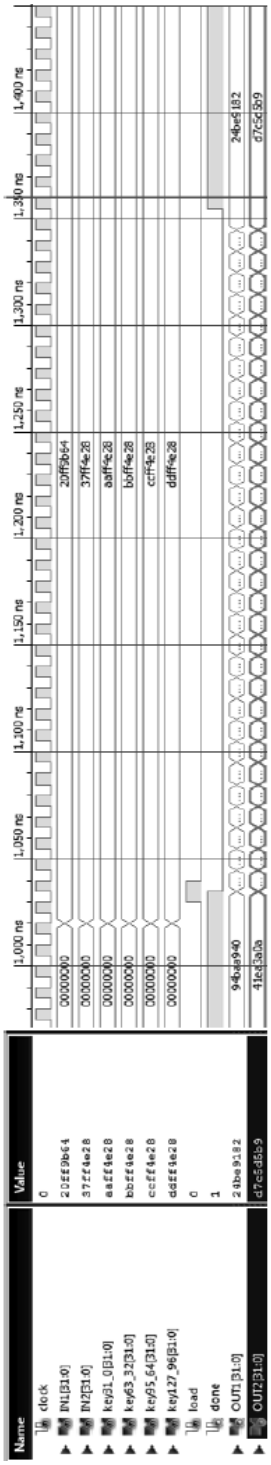
EK A: NFC Alt Sistem Kartı Şematik Tasarımı
EK B: Saat İşaretli TEA Şifreleme Modülü Simülasyon Sonuçları
EK C: Saat İşaretli TEA Şifre Çözme Modülü Simülasyon Sonuçları
EK D: Özet Fonksiyonu Modülü Simülasyon Sonuçları

EK A



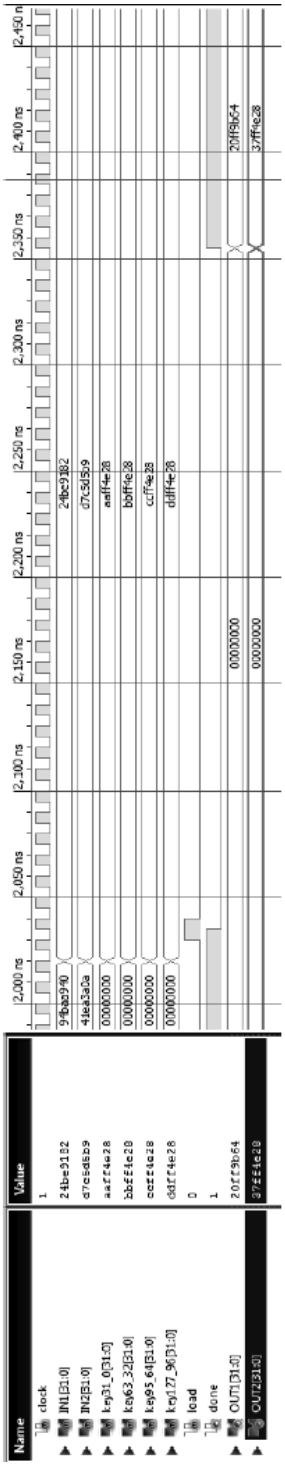
Şekil A.1 : NFC Alt Sistem Kartı şematik tasarımı.

EK B



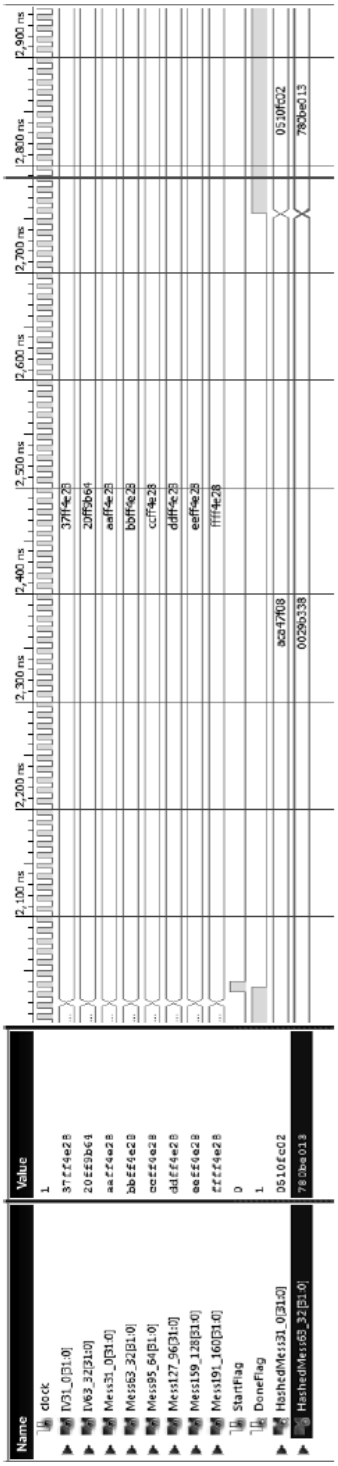
Şekil B.1 : Saat işaretli TEA şifreleme modülü simülasyon sonuçları.

EK C



Şekil C.1 : Saat işaretli TEA şifre çözme modülü simülasyon sonuçları.

EK D



Şekil D.1 : Özet fonksiyonu modülü simülasyon sonuçları.

ÖZGEÇMİŞ

Ad-Soyad **:** Subutay Giray Başkır

Doğum Tarihi ve Yeri **:** 1989, Üsküdar

E-posta **:** sgbaskir@gmail.com

Lisans **:** İstanbul Teknik Üniversitesi Elektronik Mühendisliği

TEZDEN TÜRETİLEN YAYINLAR/SUNUMLAR

- Baskir, S.G.; Ors, B., "Implementation of a secure RFID protocol," Signal Processing and Communications Applications Conference (SIU), 2013 21st , vol., no., pp.1,4, 24-26 April 2013