

**İSTANBUL TEKNİK ÜNİVERSİTESİ**  
**ELEKTRİK-ELEKTRONİK FAKÜLTESİ**

**ÖZET FONKSİYON TABANLI GÜVENLİ BİR RFID PROTOKOLÜNÜN  
FPGA ÜZERİNDE GERÇEKLENMESİ**

**BİTİRME ÖDEVİ**

**YUSUF GÖRÜM**

**040080379**

**Bölümü: Elektronik ve Haberleşme Mühendisliği Bölümü**

**Programı: Elektronik Mühendisliği**

**Danışmanı: Doç. Dr. Sıddıka Berna ÖRS YALÇIN**

**AĞUSTOS 2013**

## ÖNSÖZ

Mensubu olmaktan onur duyduğum İstanbul Teknik Üniversitesi'ndeki tez çalışmam süresince bana değerli vaktini ayırıp sınırsız anlayışıyla yardımlarını esirgemeyen danışman hocam Sayın Doç. Dr. Sıddıka Berna ÖRS YALÇIN' a teşekkürlerimi sunmayı bir borç bilirim.

Ayrıca öğrenim hayatım boyunca maddi ve manevi desteklerini hissettiğim aileme, beni yalnız bırakmayan arkadaşlarıma sonsuz saygı ve teşekkürlerimi sunarım.

AĞUSTOS 2013

Yusuf GÖRÜM

# İÇİNDEKİLER

	<u>Sayfa</u>
<b>ÖNSÖZ</b>	ii
<b>İÇİNDEKİLER</b>	iii
<b>KISALTMALAR</b>	iv
<b>TABLO LİSTESİ</b>	v
<b>ŞEKİL LİSTESİ</b>	vi
<b>ÖZET</b>	vii
<b>SUMMARY</b>	viii
<b>1. GİRİŞ</b>	<b>1</b>
<b>2. KULLANILAN DONANIM VE YAZILIMLAR</b>	<b>2</b>
2.1. Kullanılan Donanımlar	2
2.2. Kullanılan Yazılımlar	2
<b>3. KECCAK</b>	<b>3</b>
3.1. Keccak Özet Fonksiyonu	3
3.1.1. Keccak Sponge Yapısı	3
3.2. Keccak Özet Fonksiyonlarının İncelenmesi	4
3.2.1. Round Fonksiyonunun İncelenmesi	4
3.2.2. Keccak Fonksiyonunun İncelenmesi	11
<b>4. RFID SİSTEMLER</b>	<b>13</b>
4.1. RFID Sistem Elemanları	13
4.1.1. Etiket	13
4.1.2. Okuyucu	14
4.2. RFID Güvenlik Protokolleri	14
<b>5. KONUM GİZLİLİĞİ PROTOKOLÜ</b>	<b>15</b>
<b>6. KECCAK GERÇEKLEME VE BENZETİM SONUÇLARI</b>	<b>18</b>
6.1. Keccak'ın VHDL ile Gerçeklenmesi	18
6.2. Keccak'ın MATLAB ile Gerçeklenmesi	21
<b>7. SONUÇLAR VE TARTIŞMA</b>	<b>23</b>
<b>KAYNAKLAR</b>	<b>24</b>
<b>EKLER</b>	<b>25</b>
<b>ÖZGEÇMİŞ</b>	<b>26</b>

## **KISALTMALAR**

<b>FPGA</b>	: Field Programmable Gate Array
<b>RFID</b>	: Radio Frequency Identification
<b>HDL</b>	: Hardware Description Language
<b>ISIM</b>	: Xilinx ISE Simulator
<b>RF</b>	: Radio Frequency
<b>SHA</b>	: Secure Hash Algorithm
<b>XOR</b>	: Exclusive OR
<b>VHDL</b>	: Very-High-Speed Integrated Circuits HDL
<b>NIST</b>	: National Institute of Standards and Technology

## TABLO LİSTESİ

	<u>Sayfa</u>
<b>Tablo 4.1:</b> Rho fonksiyonu Matlab çıktısı	6
<b>Tablo 4.2:</b> Round sayılarına karşılık round sabitleri	8

## ŞEKİL LİSTESİ

	<b><u>Sayfa</u></b>
Şekil 2.1: Spartan 3E Geliştirme Kiti [1]	2
Şekil 3.1: Sponge Yapı Bloğu	3
Şekil 3.2: Keccak – $f$ durumu ve kısımları	4
Şekil 3.3: Round Fonksiyonu Matematiksel İfadeleri	5
Şekil 3.4: Pi fonksiyonunun incelenmesi	7
Şekil 3.5: Round Bloğunun incelenmesi	10
Şekil 3.6: Keccak Özet Fonksiyonunun Blok Diyagramı	11
Şekil 4.1: RFID Teknolojisi Oluşum Elamanları	13
Şekil 5.1: Veritabanı Gösterim Bloğu[6]	15
Şekil 5.2: Konum Gizliliği Protokolünün Haberleşme Bloğu[6]	16
Şekil 6.1: Design Summary Sonucu	18
Şekil 6.2: Keccak Fonksiyonunun Hiyerarşi Görüntüsü	18
Şekil 6.3: Keccak RTL Şematik Görüntüsü	19
Şekil 6.4: Keccak Benzetim Sonucu 1	20
Şekil 6.5: Keccak Benzetim Sonucu 2	20
Şekil 6.6: Keccak'ın MATLAB ile gerçekleştirilmesi	21
Şekil 6.7: MATLAB Workspace	21
Şekil 6.8: Keccak Sonuçlarının Karşılaştırılması	22

# ÖZET FONKSİYON TABANLI GÜVENLİ BİR RFID PROTOKOLÜNÜN FPGA ÜZERİNDE GERÇEKLENMESİ

## ÖZET

Radyo Frekans ile Tanımlama (RFID - Radio Frequency Identification) basit anlamda; herhangi bir nesnenin üzerinde bulunan ve o nesneye ait bilgiyi içeren elektronik bir etiket (TAG) ile radyo frekansı üzerinden kendisini tanıttak bir alıcı (OKUYUCU) arasında kurulan bir tanımlama teknolojisidir. Günümüzde RFID teknolojisi; kullanım alanının geniş olması ve popüleritesi sonucu bu teknolojiye meydana gelebilecek güvenlik açıklıklarının giderilmesi konusundaki öneminin hızla artmasına neden olmuştur. Bu yüzden RFID uygulamalarında şifreleme algoritmaları kullanılmaktadır.

Tez içeriğinde; hash (özet) fonksiyon temelli güvenli bir RFID algoritmasının FPGA üzerinde gerçekleştirilmesi açıklanacaktır. Öncelikle RFID sistemleri ile ilgili genel bilgi verilmiş, daha sonra ise kullanılan özet fonksiyonu –Keccak (SHA-3)– ayrıntılı olarak tanıtılmış ve bu özet fonksiyonunun VHDL (Very-High-Speed Integrated Circuits HDL) ile yazılımı sağlanmıştır. En son aşamada ise özet fonksiyon temelli güvenli bir RFID protokolü ile ilgili ayrıntılı bilgi verilerek MATLAB ile Keccak doğrulanmıştır.

Keccak algoritmasının kod geliştirilerek gerçekleştirilmesi aşamasında; uygun teste tabi tutulup doğruluğu kontrol edilmiş ve etiket ile okuyucu benzetimi için iki ayrı donanımsal modülü tasarlanmıştır. Daha sonra tasarlanan bu modüller tek bir modül altında birleştirilip, doğruluğu sınanmıştır. Tasarlanan bu iki modülün iki ayrı FPGA'ya yüklenip, FPGA'lar arası kablo ile haberleşme ve protokolün gerçekleştirilmesinin sağlanabileceğinden bahsedilmiştir.

Sonuç olarak, RFID doğrulama protokolünün donanımsal olarak güvenli bir şekilde gerçekleştirilmesi için; uygun FPGA deneme kitleri seçilmelidir. Aksi takdirde, istenmeyen zamanlama problemlerine ve test aşamasında zorluklara neden olabilir. Bu kitler; özet fonksiyona, kullanılan değişkenlere, verilerin büyüklüklerine ve kodun yapısına bağlı olarak değişebilir.

# **IMPLEMENTATION OF A HASH BASED RFID AUTHENTICATION PROTOCOL**

## **SUMMARY**

In simple terms, Radio Frequency Identification (RFID) technology is an identification technology, established between a tag, taking part in any objects, has information which is belong to that object and a receiver (READER) which introduces itself over the radio frequency. Spreading the use of this technology and popularity of RFID has resulted the increase in the given importance because of the security problems that may occur. Therefore, the encryption algorithms are used in RFID applications.

In the content of the B.Sc. thesis project, implementation of a hash based RFID authentication protocol on FPGAs will be explained. Firstly, general information about the RFID systems were given, then the hash function – Keccak (SHA-3) – was introduced in detail and the software of the hash function was provided with VHDL (Very-High-Speed Integrated Circuits HDL). In the final stage, it has mentioned about the hash function based secure RFID authentication protocol which can be implemented. Also Keccak has verified with the MATLAB codes.

In the stage of Keccak Algorithm's implementation with improved code, the accuracy of this was controlled with applying appropriate test and the tag with reader was designed to simulate two separate hardware modules. These modules were combined under a single module and it was tested. These modules could be initialized into two separate FPGAs and the communication via the cable between FPGAs with the implementation of the RFID protocol could be provided.

As a result, to implement a secure RFID authentication protocol in hardware, suitable FPGA test kits should be selected. Otherwise, undesired timing problems and difficulties during the test may occur. These kits can change with the effect of hash function, the variables used, the size of the data and the structure of the code.