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

KISALTMALAR

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

TABLO LİSTESİ

ŞEKİL LİSTESİ

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 tanıtacak bir alıcı (OKUYUCU) arasında kurulan bir tanımlama teknolojisidir. Günümüzde RFID teknolojisi; kullanım alanının geniş olması ve popülaritesi sonucu bu teknolojide 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 gerçeklenmesi 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 gerçeklenmesi 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'ler arası kablo ile haberleşme ve protokolün gerçeklenmesinin sağlanabileceğinden bahsedilmiştir.

Sonuç olarak, RFID doğrulama protokolünün donanımsal olarak güvenlikli bir şekilde gerçeklenmesi 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.