İSTANBUL TEKNİK ÜNİVERSİTESİ

ELEKTRİK - ELEKTRONİK FAKÜLTESİ

GÜVENLİ AKILLI KART TASARIMI

BİTİRME ÖDEVİ

CEM SÜMENGEN

040060305

Bölümü: Elektronik ve Haberleşme Mühendisliği Bölümü

Programı: Elektronik Mühendisliği

Danışmanı: Yrd. Doc. Dr. Sıddıka Berna ÖRS YALÇIN

MAYIS 2010

ÖNSÖZ

Tez çalışmam boyunca bana yol gösteren, yardımlarını esirgemeyen danışman hocam Yrd. Doç. Dr. Sıddıka Berna ÖRS YALÇIN'a teşekkürü bir borç bilirim.

Ayrıca üniversite öğrenim hayatım boyunca beni yalnız bırakmayan arkadaşlarıma teşekkür ederim.

Son olarak bütün çalışmalarımda yanımda olan, manevi desteğini eksik etmeyen aileme teşekkürlerimi sunarım.

MAYIS 2010 Cem SÜMENGEN

İÇİNDEKİLER

	Sayfa
KISALTMALAR	**iv**
TABLO LİSTESİ	**v**
ŞEKİL LİSTESİ	**vi**
ÖZET	**vii**
SUMMARY	**viii**
1. GİRİŞ	**1**
1.1. Giriş	1
1.2. Tezin kapsamı	1
2. AKILLI KARTLAR	**3**
2.1. Akıllı Kartların Fiziksel Özellikleri	3
2.2. Akıllı Kartların Çeşitleri	4
2.3. Akıllı Kart Donanımı	5
2.4. Kullanım Amaçları	6
2.5. İletişim Standartları	7
2.6. Saldırılar	11
3. SAYISAL İMZA	**13**
3.1. Giriş	13
3.2. Güvenlik	15
3.3. Sayısal Zarf	16
3.4. Kullanım Alanları	18
4. KULLANILAN DONANIM	**19**
4.1. Silicon Laboratories C8051060 Geliştirme Kiti	19
4.1.1. Kit içeriği	19
4.1.2. Geliştirme kartı	19
4.1.3. C8051F060 Mikro-denetleyici ünitesi	20
4.2. XILINX Spartan 3E Starter Kit	22
4.2.1. Kit içeriği	22
4.2.2. Geliştirme kartı	22
5. AKILLI KART TASARIMI	**24**
5.1. Uygulama Protokolü	24
5.2. Kullanılan Algoritmalar	26
5.2.1. RSA	26
5.2.2. AES	27
5.3. Devre Bağlantıları	29
5.4. Kart Okuyucu	30
5.5. MCU Uygulaması	30
5.6. Yardımcı İşlemci Gerçeklemesi	30
6. SONUÇLAR VE TARTIŞMA	**32**
KAYNAKLAR	**33**
ÖZGEÇMİŞ	**34**

KISALTMALAR

RSA	: Rivest-Shamir-Adleman
MCU	: Micro-Controller Unit
FPGA	: Field Programmable Gate Array
PIN	: Personal Idendification Number
RAM	: Random-Access Memory
ROM	: Read-Only Memory
EEPROM	: Electrically Erasable Programmable Read-Only Memory
CPU	: Central Processing Unit
UART	: Universal Asynchronous Receiver/Transmitter
MMU	: Memory Management Unit
APDU	: Application Protocol Data Units
CAPDU	: Command APDU
RAPDU	: Response APDU
ATR	: Answer to Reset
DES	: Data Encryption Standard
MD-5	: Sessage Digest 5
SHA	: Secure Hash Algorithm
AES	: Advanced Encryption Standard
ASIC	: Application Specific Integrated Circuit

TABLO LİSTESİ

Sayfa

Tablo 2.1 : Akıllı Kart Temas Noktaları 4

ŞEKİL LİSTESİ

	Sayfa
Şekil 2.1 : Akıllı Kartın Fiziksel Özellikleri	3
Şekil 2.2 : Akıllı kart mikrobilgisayar mimarisi	5
Şekil 2.3 : “T=0” protokolü komut veri yapısı	9
Şekil 2.4 : “T=0” protokolü yanıt veri yapısı	10
Şekil 3.1 : Sayısal imza üretimi	15
Şekil 3.2 : Sayısal imza doğrulama işlemi	15
Şekil 3.3 : İmzalanmış mesaj içeren sayısal zarf yaratma işlemi	17
Şekil 3.4 : İmzalanmış mesaj içeren sayısal zarfın açılması	17
Şekil 4.1 : C8051F050 Geliştirme kartı	20
Şekil 4.2 : C8051F060 Mikro-denetleyicisi	21
Şekil 4.3 : SPARTAN-3E Starter Kit	23
Şekil 5.1 : Uygulama protokolü	25
Şekil 5.2 : Akıllı kart veri iletişimi	26
Şekil 5.3 : AES blok diyagramı	29

GÜVENLİ AKILLI KART TASARIMI

ÖZET

Bilgi güvenliği gün geçtikçe artan bir öneme sahiptir. Önceleri yalnızca askeri uygulamalar için kullanılan kriptografik işlemler günlük yaşamımızda sıklıkla kullanılır hale gelmiştir. Her türlü resmi, ticari ve özel işlemde elektronik doküman paylaşımının vazgeçilmez bir hal almasıyla güvenli iletişim için önlemler alma gereği ortaya çıkmıştır.

Bu çalışmada Intel 8051 tabanlı bir mikro-denetleyici üzerinde bir akıllı kart tasarımı yapılacaktır. Akıllı kart sayısal imzalama ve simetrik şifreleme işlemlerini gerçekleştirecektir. Bu kriptografik işlemlerin tasarlanan akıllı kartta efektif bir şekilde yürütülebilmesi için bir kriptografik yardımcı işlemci tasarımı FPGA üzerinde gerçeklenecektir.

Bu amaçla birinci kısımda çalışmanın önemi anlatılmış, ikinci kısımda akıllı kartlar hakkında, üçüncü kısımda sayısal imza konusunda bilgi verilmiş, dördüncü kısımda kullanılan donanım araçları tanıtılmış, beşinci kısımda tasarlanan akıllı kart tanıtılmış, altıncı ve son kısımda çalışmadan elde edilen sonuçlara değinilmiştir.

DESIGN OF A SECURE SMART CARD

SUMMARY

Information security has an increasing significance day after day. Cryptographic processes which are only used for military applications in the past has become very common in daily life. Because sharing electronic documents become widespread in formal, commercial, and private applications, the neccessarity of taking special precautions becomes mandatory.

In this study smart card is designed on a Intel 8051 based micro-controller. This smart card is designed to perform digital signature and symmetric encryption operations. In order to implement these cryptographic operations effectively on the smart card, an co-processor is designed and realized on FPGA.

For this purpose in the first chapter of the thesis the importance of this study is explained, in the second chapter smart cards and in the third chapter digital signatures are described, in the fourth chapter the dedicated hardware is presented, in the fifth chapter the design of the smart card is introduced and in the last chapter the results are discussed.

1. GİRİŞ

1.1. Giriş

İçinde bulunduğumuz bilgi çağının gereklerinden dolayı çevrimiçi işlemlerin yoğunluğu oldukça artmıştır. Bu durum çok fazla önemli bilginin genel kullanıma açık paylaşılan ağlarda tutulmasını beraberinde getirmiştir. Bu nedenle önemli elektronik dokümanların kötü niyetli üçüncü şahıslardan korunması gereği ortaya çıkmıştır [1].

Elektronik ortamda paylaşılan önemli bilgilerin gizliliği kritik öneme sahip bir konu haline gelmiştir. Bu nedenle önceleri yalnızca askeri uygulamalar için kullanılan kriptografi teknikleri günlük yaşamda sıklıkla kullanılır hale gelmiştir. Bu şekilde yapılan bilgi transferinde bilginin kim tarafından gönderildiği ve değişikliğe uğrayıp uğramadığı da büyük önem teşkil etmektedir. 1976'da Whitfield Diffie ve Martin Hellman ilk kez sayısal imza kavramını ortaya koymuştur. Bundan kısa bir süre sonra Ronald Rivest, Adi Shamir ve Len Adleman sayısal imzalama için kullanılabilecek RSA algoritmasını geliştirdiler. Günümüzde sayısal imzanın geliştirilerek kullanılmasıyla mesajın değiştirilmediğinin kanıtlanması ve göndericinin kimliğinin kanıtlanması hususlarında güvenilirlik sağlanmıştır [2].

Bu amaçlarla kullanıcıların kişisel bilgilerinin kartın dışına hiçbir zaman çıkmadığı kriptografik işlemleri dahili olarak yürütebilen akıllı kartların kullanımı büyük önem kazanmıştır. Özellikle e-devlet uygulamalarında, resmi işlemlerde, ticari uygulamalarda gizliliğin korunması amacıyla akıllı kartların kullanımı yaygınlaşmıştır [3].

1.2. Tezin Kapsamı

Bitirme çalışmasında kullanıcılar arasında güvenli veri iletişimi için bir akıllı kart tasarımı yapılmıştır. İletilmek istenen mesaja güvenli iletişim için bir takım kriptografik işlemler uygulanmaktadır. Kişisel bilgisayardan tasarlanan akıllı karta aktarılan mesaja öncelikle sayısal imzalama yapılmaktadır. Böylece bilginin

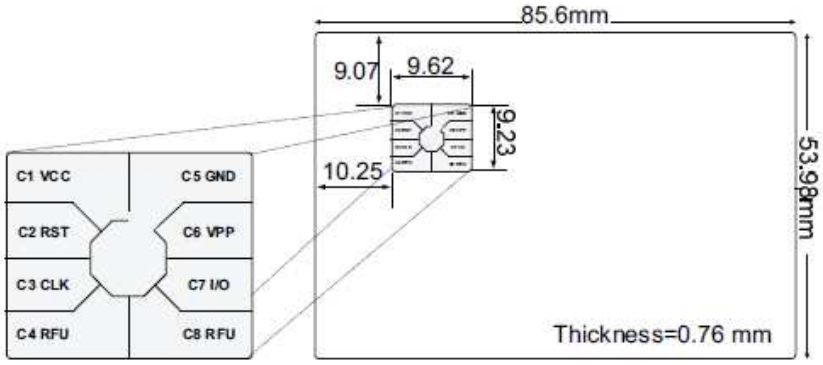
değiştirilmeden gönderildiği ve kim tarafından gönderildiği kesin olarak ispatlanabilecektir. Ardından iletişimin gizliliği için mesaj şifrelenmektedir. Böylece mahremiyetin korunması amaçlanmaktadır.

Akıllı kart tasarımı için mikro-denetleyici (micro-controller unit – MCU) üzerinde uygulama geliştirilmiştir. Ayrıca akıllı karta kriptografik işlemleri efektif bir şekilde gerçekleştirebilmek üzere bir kriptografik yardımcı işlemci eklenmiştir. Yardımcı işlemcinin uygulaması için yapılan tasarım sahada programlanabilir kapı dizisi (field programmable gate array – FPGA) üzerinde gerçeklenmiştir.

2. AKILLI KARTLAR

2.1. Akıllı Kartların Fiziksel Özellikleri

Akıllı kart, gömülü bir mikroçip içeren kredi kartı boyutlarında, insan-makine ara yüzü barındırmayan plastik bir karttır. Benzer kullanım alanına sahip manyetik şeritli kartlara göre çok daha güvenli ve yüksek kapasitelidir. Akıllı kartların fiziksel büyüklükleri ISO 7810 standardında belirlenmiştir. Buna göre akıllı kartların eni ve boyu 85,6 x 53,98 mm, köşelerinin çapı 3,18 mm ve kalınlığı 0,76 mm olmalıdır (bkz. Şekil 2.1).



Şekil 2.1. Akıllı Kartın Fiziksel Özellikleri [4]

Akıllı kartlar dış dünya ile iletişim kurma biçimlerine göre kontaksız ve kontaklı olmak üzere ikiye ayrılırlar. Kontaksız kartlar fiziksel temas olmadan elektromanyetik bir ara yüz kullanarak; kontaklı kartlar ise kart okuyucuya doğrudan fiziksel temas ile iletişim sağlarlar.

Kontaklı kartlar 1 cm çapında, altın kaplama, 8 temas noktası barındıran bir temas yüzeyine sahiptirler. Bu temas noktaları temas yüzeyinin altındaki mikroçipe bağlanmıştır. Bu temas noktaları sol üstten sağ alta doğru C1'den C8'e kadar isimlendirilmiştir. Temas noktalarının yerleşimi Sekil 2.1'de ve açıklamaları Tablo 2.1'de gösterilmiştir.

Tablo 2.1. Akıllı Kart Temas Noktaları [4]

Pozisyon	**Teknik Kısaltma**	**Tanım**
C1	VCC	Besleme gerilimi
C2	RST	Sıfırlama, reset
C3	CLK	Saat işareti
C4,C8	RFU	Geleceğe yönelik kullanım için rezerve edilmiş
C5	GND	Referans gerilimi
C6	VPP	Harici programlama gerilimi
C7	I/O	Seri giriş/çıkış

Kontaksız akıllı kartlar, kontaksız kartlardan farklı olarak minyatür bir radyo alıcı-vericisine ve antene sahiptirler. Bu tip kartları kart okuyucusuna yerleştirmektense, basitçe okuyucuya yaklaştırmak yeterlidir. Bu tip kartlar güç kaynağına ihtiyaç duymamakta; güç gereksinimi, kartta bulunan anteninin sabit bir cihazdan sağlanan manyetik alan içinde hareketi sonucunda oluşan indüksiyon ile karşılanmaktadır [4].

2.2. Akıllı Kartların Çeşitleri

Akıllı kartlar işlem yeteneklerine göre 3 gruba ayrılabilirler:

1. Bellek kartları
2. Mikroişlemcili kartlar
3. Kriptografik kartlar

Bellek kartları, akıllı kartların en basit formudur. Yaptıkları iş, kartın üzerinde veri saklamaktan ibarettir. Bu tip kartlarda güvenlik karta özgü herhangi bir işlemle değil, kartta saklanacak verinin şifrelenmiş olması ile sağlanır.

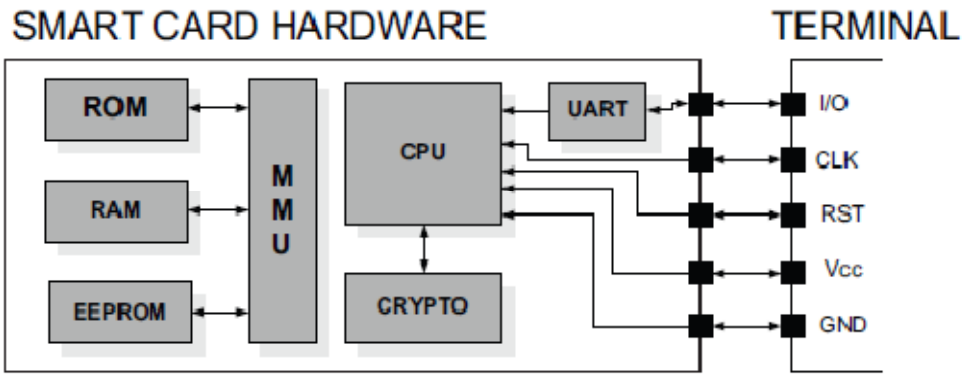
Mikroişlemcili akıllı kartlarda kartın belleğine erişim tamamen mikroişlemci üzerinden yapılır. Bununla birlikte mikroişlemci kişisel kimlik numarası (personal idendification number – PIN) koruması ve bazı diğer güvenlik özellikleri içerebilir.

Mikroişlemcili kartlar bir mini bilgisayar gibidir. İçlerinde rastgele erişimli bellek (random-access memory - RAM), salt okunur bellek (read-only memory - ROM) ve elektriksel olarak silinebilir ve programlanabilir bellek (electrically erasable programmable read-only memory - EEPROM) barındırırlar.

Akıllı kartların en gelişmiş tipi kriptografik kartlardır. Bunlar kriptografik işlem desteği içeren gelişmiş mikroişlemcili akıllı kartlardır. Kriptografik akıllı kartlar, kriptografik fonksiyonları dahili olarak yürütürler ve kullanıcıların özel anahtarları için güvenli depolama olanağı sağlarlar. Bu kartlarda EEPROM müdahaleye karşı dayanıklı (*tamper-resistant*) tasarlandığından izinsiz kullanıcılar kartın sırlarını ele geçiremezler. Bu kartlarda karmaşık kriptografik fonksiyonları makul hızlarda gerçekleştirebilmek için donanımsal önlemlere ihtiyaç duyulmaktadır. [1].

2.3. Akıllı Kart Donanımı

Akıllı kartın kalbi merkezi işlem birimidir (central processing unit – CPU) ve ROM, EEPROM, RAM ile giriş/çıkış portu (UART) olmak üzere dört fonksiyonel blok ile çevrelenmiştir. Bunların yanında özel olarak güvenlik için kripto veya bellek yönetimi yapıları bulunabilir (bkz. Şekil 2.2)[4].



Şekil 2.2. Akıllı kart mikrobilgisayar mimarisi [4]

CPU (Merkezi İşlem Birimi) kendisine elektriksel olarak bağlı çevre birimleri ile birlikte akıllı karta "akıllı" denmesine neden olan yazılımı ileten birimdir. Yazılım komutlarını ROM veya EEPROM bellekten okur ve işler. Elde ettiği sonucu yine çevre birimleri aracılıyla ya saklar ya da kullanıcının programı doğrultusunda dış dünyayla paylaşır. Akıllı kartlarda kullanılan CPU, önceleri 8 bit olarak tasarlanmış, daha sonra 16 bite ve giderek 32 bite çıkarılarak işlemcinin gücü artırılmıştır [5].

ROM üretim aşamasında programlanmış işletim sistemini içerir. ROM kapladığı alan ve güç harcaması bakımından oldukça verimlidir. Aynı zamanda sabit verilerin, standart rutinlerin ve başvuru tablolarının saklanması için kullanılır. ROM içeriği çip ömrü boyunca sabittir.

RAM mikroişlemcinin çalışma belleğidir. Program çalıştırılırken geçici depolama için kullanılan kısa süreli bellektir. RAM, sınırlı alanı bakımından akıllı kart yazılım geliştiricileri için en değerli kaynaktır.

EEPROM uçucu olmayan, yüksek maliyetli bir elemandır. Çipin fiziksel boyutunun %50'si kadar büyüklükte olabilir [4]. Akıllı kartın bilgi saklama belleğidir ve kart sahibinin açık veya gizli bilgileri burada saklanır. Akıllı kart, güç kaynağına bağlı değilken de bu bellekteki bilgiler kalıcı olarak tutulur. EEPROM bellek boyu ilk aşamalarda 4K, sonraları gereksinimler doğrultusunda 8K, 16K, 32K, 64K, 128K, … olarak artırılmıştır [5].

Merkezi işlem biriminden belleğe erişim isteklerinden bellek yönetim birimi(memory management unit - MMU) denilen bir donanımsal yapı sorumludur.

Evrensel asenkron giriş/çıkış (universal asynchronous receiver/transmitter - UART) modülü terminalden gelen komutların ve terminale gönderilen cevapların seri iletişimini sağlar [4].

Bazı üreticiler çipe donanımsal olarak ilave fonksiyonlar eklemektedir. Bunların en sık kullanılanları rassal sayı üreteci ve kriptografik yardımcı işlemcilerdir. Güvenlik işlemleri için kullanılan akıllı kartlarda çok basamaklı aritmetik işlemler için özelleşmiş yardımcı işlemciler bulunabilmektedir. Bazı durumlarda ise yardımcı işlemciler yaygın kriptografik fonksiyonları doğrudan uygulayabilecek kapasitededir [6].

Kripto işlemci ünitesi yalnızca sınırlı bir takım kriptografik işlemleri yerine getirmek için tahsis edilmiş bir donanımsal yapıdır. Karmaşık kriptografik işlemleri çok yüksek işlem performansı ve etkin enerji kullanımıyla yerine getirebilir [4].

2.4. Kullanım Amaçları

Akıllı kartlar kriptografik işlemleri dahili olarak gerçekleştirebildiklerinden, ataları olan manyetik şeritli kartlara göre büyük avantaja sahiptirler. Akıllı kartlar

kullanıcının PIN ve anahtar gibi kişisel bilgilerinin hiçbir zaman karttaki çipin dışına çıkmaması ile güvenliğin üst düzeye çıkarılmasını sağlamaktadır [3].

Akıllı kartlar çok çeşitli bilişim uygulamalarında hızla artan kullanım alanına sahiptir. Akıllı kartların kullanım alanları en genel olarak üç başlık altında incelenebilir:

Kimlik kanıtlama: Akıllı kartlar bir bireyin, gerçekten iddia ettiği kişi olduğunu, hususi bir cihaza sahip olma ve/veya bilgiye dayanan yöntemlerle kanıtlayıcı özelliktedirler. Bir unsura sahip olmaya dayalı sistemlerde kullanıcının kendine özgü akıllı karta sahip olup olmadığı denetlenirken, bilgiye dayanan sistemlerde PIN gibi yalnızca bireyin sahip olduğu bir bilgi denetlenir.

Kimlik tanımlama: Kamusal ve özel organizasyonların hizmet sunmak için elektronik ortama ağırlık vermeleri güvenli elektronik kimlik tanımlamanın önem kazanmasını sağlamıştır. Her organizasyon (üniversite, şirket, kütüphane vs.) akıllı kartları kimlik tanımlama için kullanma potansiyeline sahiptir.

İşlem yapma: Teknolojinin mal ve hizmet ticaretinde kullanımında akıllı kartların kullanım alanı çok geniştir. Akıllı kartlar bankamatiklerde nakite dönüştürülebilir veya kredi kartı olarak kullanılabilir [4].

2.5. İletişim Standartları

Akıllı kartlar dış dünya ile iletişimlerini olarak adlandırılan uygulama protokol veri paketleri(application protocol data units - APDU) aracılığıyla yaparlar [7]. APDU, ISO 7816-4 standardında tanımlanmış, uygulama seviyesi bir protokoldür. Uygulama katmanında, kart ve okuyucu arasındaki tüm iletişim APDU aracılığıyla gerçekleşir. Uygulamalar bunlarla, alttaki protokolden bağımsız olarak kartla iletişim kurabilir. İki çeşit APDU tanımlanmıştır: Komut APDU (CAPDU – Command APDU) ve Cevap APDU (RAPDU - Response APDU). CAPDU kartı okuyucudan akıllı karta veri yollamakla sorumluyken; RAPDU’nun görevi akıllı karttan, kart okuyucuya cevap olarak veri yollamaktır. [4, 8].

Kartı işletmek için okuyucunun aşağıdaki fonksiyonları yerine getirmesi gerekmektedir:

- Karta besleme gerilimi vermek/kesmek

- Kartı sıfırlamak(resetlemek)
- Karttan veri okumak (Komut almak)
- Karta veri göndermek (Komut vermek) [3]

Akıllı kartın veri iletişiminde öncelikli olarak kart okuyucu ile el sıkışması gerekir. İletişime başlamak için bu anlaşma şarttır. El sıkışma işleminin ilk adımı yongada bulunan RST (reset) ucu ile sağlanır. Akıllı kart okuyucu yuvasına takıldığında kartı okuyucu ilk olarak VCC ucundan yongaya enerji verirken, yonganın RST ucunu belirli bir süre 0V potansiyelinde tutar; sonra RST ucunu yeniden 5V gerilim düzeyine yükseltir. Bu işlem yongadaki işlemcinin durum makinesini sıfırlar ve işlemcinin koşturduğu işletim sisteminin ilk duruma gelmesini sağlar. El sıkışma işleminin ikinci adımı yonga ve işletim sisteminin doğru koşullandırıp, kart okuyucu ile ilk mantıksal iletişimin gerçekleştirilmesidir Yukarıda açıklanan donanımsal işlemden sonra işletim sistemi, yonganın doğru başlatıldığı bilgisini ve beraberinde, kendi çalışma koşullarını da içeren bilgileri, ATR (Answer to Reset) verileri olarak kart okuyucuya gönderir.

ATR bilgisi akıllı kartlar için temel bir işlemdir ve olmazsa olmaz bir bilgidir. ATR verileri beş ayrı gruba ayrılmıştır:

- Başlangıç Karakteri(TS),
- Format Karakteri (T0),
- Arayüz Karakterleri(TA, TB, TC, TD, vb.),
- Tarihsel Karakterler (T1… TK),
- Kontrol Karakteri (TCK)

Yukarıdaki verilen TS, T0 ve TCK zorunlu bilgiler, diğerleri seçimlik bilgilerdir. Arayüz karakterleri ve tarihsel karakterler akıllı kartın çalışma hızını, parametre değiştirme olanağını, üretici ile ilgili bilgileri ve iletişim sorunlarını çözmeye yönelik bilgileri içeriri. ATR içerisindeki TS, başlangıç ve kodlama yöntemini, T0 karakteri ise iletişim formatını belirler. TS karakteri birçok işletim sisteminde 0x3B olarak tanımlanmıştır. T0, iletişim formatını belirlediğinden, bu baytta bulunan en anlamlı dört bit (b8, b7, b6, b4) ATR’de TA(1), TB(1), TC(1) ve TD(1) baytlarının olup

olmadığı, geri kalan dört bir ise tarihsel verilerin sayısını belirtir. Böylece, tarihsel karakterlerin en fazla 15 tane sekizliden oluşacağı ortaya çıkmış olur.

Bu aşamadan sonra yonga ile kart okuyucu aralarında, bir iletişim protokolüne göre bilgi alışverişinde bulunmaya başlar. Bu iletişim protokolü ATR'de bulunan bilgi doğrultusunda "T=0" ya da "T=1" protokolüdür [5].

Temaslı kartlarda bilgi transferi için genellikle seri giriş/çıkış ara yüzü bulunur [6]. Bu kartlarda iletişim ISO 7816-3 standardında tanımlanmıştır. Bu standart bayt tabanlı (T=0) ve blok tabanlı (T=1) iki farklı protokolü tanımlamaktadır. Ancak 14 protokole kadar rezerve edilmiştir [3]. Akıllı kartların büyük çoğunluğu bayt tabanlı asenkron ("T=0") protokolü kullanırlar. [6].

Temassız kartlarda ise, veri iletişimi için, ISO 14443'te "Tip A" veya "Tip B" olarak adlandırılan protokoller kullanılır.

Kullanılacak iletişim protokolü, iletişim hızı, gönderilecek mesajın olabilecek en büyük uzunluğu gibi bilgiler ATR içinde belirtilir. ATR içindeki bu bilgiler doğrultusunda komut iletimi başlar [2].

Akıllı kartlarda "T=0" iletişim protokolü seri, asenkron, yarı çift yönlü karakter iletişim protokolüdür. 'Reset' ve ATR işleminin başarılı bir şekilde gerçekleşmesinden sonra, ilk işlem olarak, gönderilecek sekizlilerin sekteye uğramasının veya veri gecikmesinin algılanması için, ATR'de tanımlı özel bir sekizli olan TC(2) arayüz sekizlisi içerisinde belirtilen karakter bekleme süresi parametresi ile protokolde bekleme süresi hesaplanır. Sonra, arayüz birimi komut göndererek işletişimi başlatır. Akıllı kart ise, gelen komuta, istenen verileri ve bu veriler ile birlikte standartlarda tanımlı sonuç durum bilgisini geri döndürerek yanıt verir. "T=0" protokolünde komut yapısı Şekil 2.3'te gösterildiği gibi, komut başlığı ve komut verisinden oluşur.

Şekil 2.3. "T=0" protokolü komut veri yapısı

“T=0” protokolünde komut başlığı; ilk sekizli CLS (class) olarak adlandırılan sınıf sekizlisi, daha sonra gelen INS(instruction) olarak adlandırılan komut sekizlisi ve bunlardan sora gelen P1 ve P2 olarak adlandırılan iki tane parametre sekizlileri ve son olarak P3 veya komut veri boyu olarak adlandırılan Lc sekizlisinden oluşur. Eğer Lc=0 ise, arayüz birimi tarafından gönderilecek bir verinin olmadığı anlaşılır. Buna karşılık Lc≠0 ise, boy kadar bilgi akıllı kart yongasına iletilir.

Akıllı kart yongası komutu aldıktan sonra, yanıt olarak, eğer geri döndüreceği bir veri varsa, bu veri ve bununla birlikte en son iki sekizliden oluşan durum bilgisini de arayüz birimine iletir (bkz. Şekil 2.4).

Şekil 2.4. “T=0” protokolü yanıt veri yapısı

SW1 ve SW2 durum sekizlileri, yordam (prosedür) sekizlisi olarak 3 tiptir:

1. NULL sekizlisi: 0x60 değerini alır.
2. ACK sekizlileri: Bular veri aktarımını denetlemekte ve VPP durumunu hakkında bilgi vermekte kullanılır.
3. Durum sekizlileri: Bunlardan SW1, 0x60 dışında, 0x6X ve 0x9X değerlerini alır (X, 16 tabanında herhangi bir rakamdır.). SW2 üzerinde herhangi bir kısıt yoktur.

Akıllı kartlarda “T=1” iletişim protokolü, asenkron, yarı çift yönlü blok iletişim protokolüdür. Bu protokolde karta özel denetimler ile birlikte veri aktarım akış denetimi, zincir blok mesaj aktarımı ve hata denetimi tanımlanmaktadır. Protokol ATR işleminden sonra veya başarılı bir protokol parametre seçimi işleminden sonra parametre seçme süresi başlar. Protokolün temel karakteristiği şöyledir:

- Protokol, arayüz cihazının gönderdiği ilk blok ile başlar, blok gönderme hakkını değiştirerek devam eder.
- Bir blok, aktarılan en küçük veri birimidir; protokolden bağımsız uygulama verisini veya aktarım hatalarını kotaran aktarım denetim verilerini içerir.

- Blok yapısı, taşınan verinin işlenmesinden önce alınan bloğun denetlenmesini sağlar [5].

2.6. Saldırılar

Akıllı kartların manyetik kart ya da disket gibi diğer veri saklama araçlarına olan üstünlüğü veriyi güvenli olarak saklayabilmeleridir.

Akıllı kartlarda güvenlik dört bileşen ile sağlanmaktadır. İlki fiziksel olarak kartın kendisidir. Diğer bileşenler yonga, işletim sistemi ve kart üzerindeki uygulamalardır. Bir akıllı kartın güvenli olduğunu söyleyebilmek için kartın tüm bu bileşenlerinin saldırılara karşı savunma mekanizmaları olmalıdır. Bu bileşenlerden herhangi biri güvenlik gereksinimlerini karşılamıyorsa o akıllı kartın güvenliğinden bahsedilemez.

Akıllı kartların kullanımı yaygınlaştıkça kartlara olan saldırılar da çoğalmaktadır. Aşağıda akıllı kartlara uygulanan genel saldırı yöntemleri anlatılmaktadır.

- **Veri iletişiminin dinlenmesi:** Kart okuyucu ve kart arasındaki hattın dinlenerek gelen/giden verinin ele geçirilmesi.
- **Veri iletişiminin manipülasyonu:** Yonga modülünün temas noktalarına tel iliştirilerek okuyucu ve kart arasındaki veri istenilen şekilde değiştirilebilir.
- **UV ışığı kullanarak EEPROM'un silinmesi:** UV ışığıyla EEPROM silinerek kartın güvenli durumu bozulabilir.
- **Gücün kesilmesi:** PIN kontrolü sırasında güç kesilerek hata sayacının sıfırlanması önlenebilir.
- **Saat işaretinin kesilmesi:** Saat işareti kesilip elektron ışın test edici ile RAM içeriği gözlenebilir.
- **Mikroişlemcinin lazerle kesilmesi:** Mikroişlemcinin üst tabakaları lazerle kesilerek içyapısı bozulabilir.
- **Zamanlama saldırısı:** Kriptografik algoritmalarda anahtara bağlı olarak işlem süresi değişebilmektedir. Bu değişimden yararlanarak anahtarlar ortaya çıkabilir.
- **DES anahtarı analizi:** Süper bilgisayarlar kullanılarak deneme yanılma yöntemiyle DES (data encryption standard) anahtarları ele geçirilebilir.

- **Yan kanal analizleri**: Kart çalışırken karttan sızan bilgileri inceleyerek yapılan işlemleri ve gizli verileri açığa çıkarmaya yönelik bir saldırıdır. Yan kanal analizlerinin zamanlama analizi, güç analizi, elektromanyetik analiz gibi türleri vardır.
- **Hata enjeksiyonu:** Belli mekanizmalar kullanarak kart işlemcisine hata yaptırmayı amaçlar. Gerilimdeki değişimler işlemcinin komutları atlamasına ya da yanlış yorumlamasına sebep olabilir. Saat işaretindeki değişimler verinin yanlış okunmasına sebep olabilir. Sıcaklıktaki değişimler işlemcide tutarsız davranışlara yol açabilir. İşlemciye yöneltilen lazer ışığı ya da beyaz ışık devrelerde hataya sebep olabilir. Elektromanyetik değişimler RAM'deki verilerin değişmesine sebep olabilir [7].

3. SAYISAL İMZA

3.1. Giriş

Bankacılık, hisse senedi alım satım, ticaret gibi uygulamaların operasyonel maliyetlerini azaltmak ve hizmet kalitesini arttırmak amacıyla elektronik işlemlere olan ilgi artmaktadır. Bu durum bilgisayarlarda yaratılan, işlenen, saklanan ve ağ üzerinden iletilen elektronik dokümanların miktarında büyük artışa yol açmıştır. Bu uygulamalarda kullanılan değerli ve hassas elektronik dokümanların kötü niyetli üçüncü şahıslardan korunması gereği ortaya çıkmıştır.

Geleneksel olarak kağıt üzerindeki dokümanlar ıslak imza ile doğrulanmaktadır. Bu yöntem sahicilikte oldukça iyi çalışmaktadır. Elektronik dokümanlar için de benzer bir mekanizma gereklidir. Sayısal imzalama algoritmalarıyla oluşturulan, sayısal bir veri dizisinden oluşan sayısal imzalar elektronik dokümanların doğrulanması ve kimlik denetimine hizmet etmektedir. Doğrulama dokümanın içeriğinin onaylanması, kimlik denetimi ise dokümanın göndericisinin onaylanması işlerini belirtmektedir [9].

Sayısal imza, yalnızca imzalayanın bildiği bir takım bilgilere ve imzalanan mesajın içeriğine dayanan sayısal bir veridir. Sayısal imza doğrulanabilir olmalıdır. İmzalanan doküman üzerinde tartışmalı bir durumun varlığında, tartışma tarafsız kişilerce adil bir biçimde imzalayanın gizli bilgilerine erişime gerek duyulmadan çözülebilmelidir.

Sayısal imzanın bilgi güvenliği, kimlik doğrulama, veri bütünlüğü ve inkar edilemezlik konularında bir çok uygulaması vardır [10].

Sayısal imzanın, geleneksel imzanın bütün özelliklerine sahip olması gerekmektedir. Bunlara ek olarak imza verisi, imzalanan dokümanın içeriğine bağlı olmalıdır. Böylece aynı kişi tarafından imzalanan dokümanlarda imza verisi farklı olacaktır. İmzalama işleminde sahteciliği ve inkar edilebilirliği engellemek için imzalayan

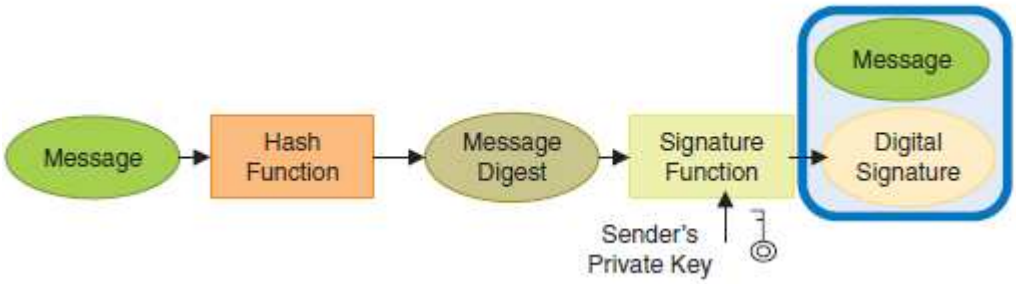
kişiye özgü bir bilgi kullanılmalıdır. İmzanın üretilmesi ve doğrulanması kolay olmalı, sahte imza üretmek mümkün olmamalıdır

Sayısal imza verisi, imzalanacak olan dokümana(mesaj/bilgi) ve yalnızca göndericinin sahip olduğu özel bir bilgiye dayanılarak üretilir. Pratikte mesajın tamamını kullanmak yerine, bir özetleme algoritması mesaja uygulanarak mesaj özeti elde edilir. Özetleme fonksiyonu herhangi bir uzunluktaki mesaj girişine karşılık sabit uzunluklu bir özet çıkışı üretmektedir. En çok kullanılan özetleme fonksiyonları arasında MD-5(mesaj özeti algoritması 5 - message digest 5) ve SHA (güvenli özetleme algoritması - secure hash algorithm) gösterilebilir. Bu algoritmalar çok karmaşıktır ve iki farklı mesajın aynı özet değerine sahip olması oldukça imkansızdır [9]. Dolayısıyla özet değerinin, özetlediği veriyi temsil ettiği varsayılabilir. Bu nedenle literatürde elektronik verinin özet değerine, genellikle “parmak izi” denir.

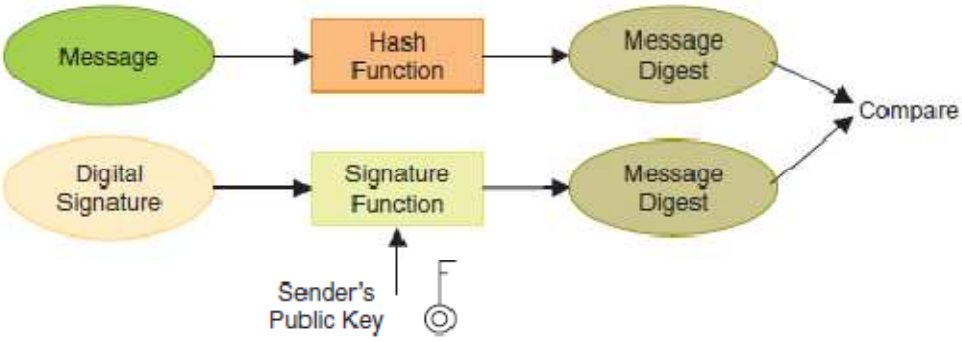
Sayısal imza teknolojisinin temeli olan ilk açık anahtar kripto algoritması Diffie ve Hellman tarafından, yaklaşık 30 yıl önce ortaya konmuştur. Ticari sayısal imza hizmetlerinin başlamasından bu yana ise 13 yıl geçmiştir. Geçen bu zaman dilimi içerisinde e-imza ve onun temeli olan açık anahtar altyapılı sistemleri ve standartları çok büyük gelişmeler göstermiş, yapılan birçok eleştiriye ve olumsuz tepkilere karşın yaygınlaşmasını sürdürmüştür [2].

Sayısal imza kavramı ve yararlılığı, pratik bir uygulaması gerçekleştirilmeden birkaç yıl önce ortaya konmuştur. Sayısal imza şeması(mekanizması) bir imza oluşturma algoritması ve buna bağlı bir imza doğrulama algoritmansın bütünüdür. İlk ortaya konan yöntem günümüzde hala en pratik ve çok yönlü yöntemlerden biri olan RSA imzalama şemasıdır [10].

İmza oluşturmak ve onaylamak için basit ve genel bir şema şekil 3.1 ve şekil 3.2’de gösterilmiştir. Sabit genişlikli mesaj özeti üreten bir özet algoritması mesaja uygulanmıştır. İmzalama fonksiyonu, sayısal imzayı üretmek için mesaj özetini ve göndericinin özel anahtarını kullanmaktadır. Bu işlemin ardından mesaj ve imza alıcıya gönderilebilir. Alıcı ters imza fonksiyonunu imza verisine uygular. Alınan mesajın özeti, aynı özet fonksiyonu ile elde edilir. Elde edilen özet verisi, imzadan elde edilen ile karşılaştırılır. İkisinin örtüşmesi durumunda mesajın gerçekten iddia edilen kişi tarafından gönderildiği ve değiştirilmediği kesinlik kazanır [9].



Şekil 3.1. Sayısal imza üretimi [9]



Şekil 3.2. Sayısal imza doğrulama işlemi [9]

3.2. Güvenlik

Sayısal imzanın güvenilir olarak kullanılabilmesi için taklit edilemez ve tamamen imza sahibinin denetiminde olan bir yöntemle oluşturulması gerekir. Günümüz teknolojisi bu şekilde oluşturulabilecek ve elle atılan imzadan çok daha güvenli sayısal imza yöntemleri sunmaktadır. Güvenli sayısal imza yöntemleri imza taklidini ve sahtekarlıklarını engellemekte çok başarılıdırlar ve genellikle karmaşık matematik temellere dayanmaktadırlar.

Güvenli elektronik imzanın temelini oluşturan açık anahtar altyapısı çeşitli veri standartları ve kripto algoritmalarının beraber kullanılmasıyla oluşturulmuştur. Bu sistemde asimetrik bir kripto algoritması (RSA, DSA, ECDSA vb.) ve her kullanıcının iki anahtarı vardır.

Özel anahtar: İmza oluşturma verisi olarak da adlandırılır. Sahibi tarafından kimseye verilmemek üzere güvenli bir şekilde saklanır ve kullanılır (örneğin, akıllı kart üzerinde.). Özel anahtar, imzalanacak veri üzerinde bir dizi matematik işlemi gerçekleştirerek, veriye bağımlı olan sayısal imzayı ortaya çıkarmaya yarar.

Açık anahtar: İmza doğrulama verisi olarak da adlandırılır. Bu anahtar imza doğrulaması yapması gereken kişilere verilir ve genellikle sayısal imza sahibinin kimlik bilgilerini de taşıyan elektronik sertifikanın içerisinde yer alır. Açık anahtar, imza üzerinde bir dizi matematik işlemi gerçekleştirerek, sayısal imzayı doğrulamaya yarar.

Özel anahtar - açık anahtar çifti aynı anda üretilir ve aralarında matematiksel bir bağıntı vardır; ancak, sadece açık anahtarı bilen bir kişinin özel anahtarı tahmin yoluyla veya başka bir şekilde bulması, bilinen teknolojilerle olanaksızdır. (Kullanılan asimetrik algoritmalarda, tahmin veya diğer yöntemlere karşı dirençli anahtar çiftlerini üretmek için, anahtar uzunluklarının ve diğer parametrelerin uzmanlarca seçilmesi gereklidir.)

Sayısal imza, imzanın atıldığı belgenin içeriği de kullanılarak oluşturulur. Bu nedenle, her dokümanın altındaki sayısal imza birbirinden farklıdır. Böylece sayısal imza veri bütünlüğünü de sağlamış olur. Belge içeriği değiştirildiğinde imza artık geçersiz olacaktır. Halbuki elle alınan ıslak imza tüm belgelere aynı şekilde atılır ve fiziksel olarak taklidi kolaydır. Dolayısıyla ıslak imza atılmış bir belge değiştirilse bile imza geçerliliğini korumaktadır.

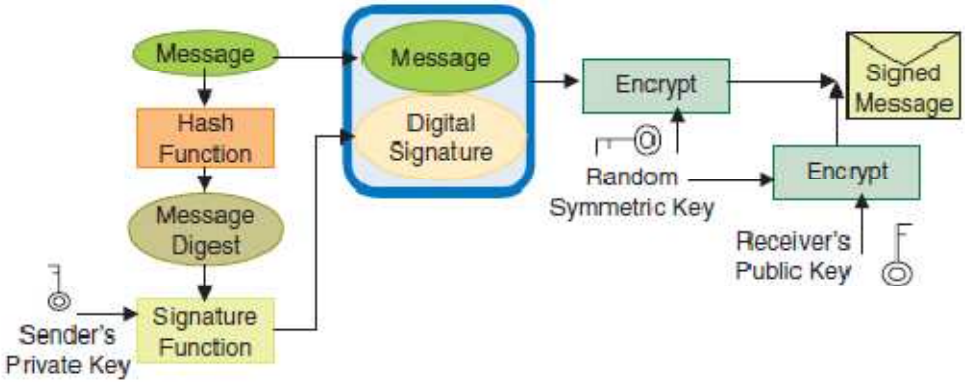
Sayısal imza, imza sahibinin kimliğini imzalanan veriyle ilişkilendirir ve imzalanan verinin değiştirilmediğini kanıtlar. Bu kanıtlama, kullanılan açık anahtarın hangi kişiye ait olduğunun kesinlikle bilinmesini gerektirir. Hangi açık anahtarın hangi kişiye ait olduğunu belirlemek için elektronik sertifika adı verilen veri yapıları kullanılır. Elektronik sertifikaların üretimini “sertifika hizmet sağlayıcısı” denilen güvenilir kurumlar yapar. Çoğu zaman kişiler anahtar çiftlerini ve bu kurumlar tarafından üretilen elektronik sertifikalarını akıllı kartlar içinde saklarlar. Böylece akıllı kartların sağladığı güvenlikten yararlanırlar [2].

3.3. Sayısal Zarf

Sayısal zarf, imzalanmamış bir mektup içeren mühürlenmiş bir zarf gibidir. Mesaj, gönderici tarafından rastgele üretilen bir simetrik anahtar ile şifrelenir. Simetrik anahtar da alıcının açık anahtarı ile şifrelenir. Şifrelenmiş mesaj ve şifrelenmiş simetrik anahtar çifti sayısal zarfı meydana getirir.

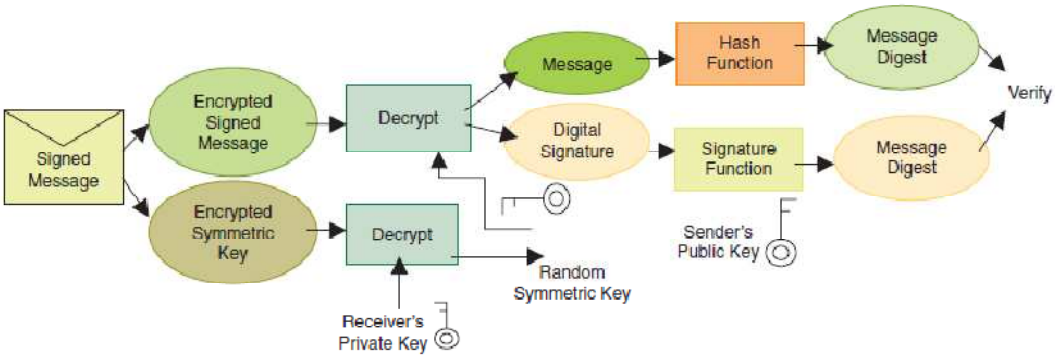
Sayısal zarfı açma ve içeriğini geri elde etme işleminde öncelikle şifrelenmiş simetrik anahtar alıcının özel anahtarı kullanılarak elde edilir. Ardından simetrik anahtar kullanılarak mesajın şifresi çözülür.

İmzalanmış mesaj içeren sayısal zarf yaratma işlemi Şekil 3.3'te gösterilmiştir. Sayısal imza verisi mesaj özeti ve göndericinin özel anahtarı kullanılarak imza fonksiyonundan elde edilir. Orijinal mesaj ve imza verisi gönderici tarafından rastsal olarak üretilmiş bir anahtarla simetrik bir şifreleme tekniği ile şifrelenir. Simetrik anahtar da alıcının açık anahtarı ile şifrelenir. Şifrelenmiş mesaj ile imza verisi ve şifrelenmiş simetrik anahtar birlikte imzalanmış mesaj içeren sayısal zarfı oluşturur.



Şekil 3.3. İmzalanmış mesaj içeren sayısal zarf yaratma işlemi [9]

Şekil 3.4 imzalanmış mesaj içeren sayısal zarfı açma, mesajı geri elde etme ve imzayı doğrulama işlemini göstermektedir. Öncelikle simetrik anahtar alıcının özel anahtarı ile elde edilir. Elde edilen anahtar şifrelenmiş mesaj ve imzayı elde etmek için kullanılır. Son olarak daha önce bahsedildiği gibi sayısal imza doğrulaması yapılır [9].



Şekil 3.4. İmzalanmış mesaj içeren sayısal zarfın açılması [9]

3.4. Kullanım Alanları

Sayısal imza elektronik veriler için bilgi bütünlüğü, kimlik doğrulama ve inkar edilemezlik hizmetlerini sunar. Bu hizmetler elektronik ortamda çok çeşitli uygulamalarda kullanılabilmektedir. Bunlardan en yaygını belge-evrak yönetim sistemleridir. Kağıt evraktan elektronik evraka geçişte elektronik evrakın yönetimi ciddi bir zorluk olarak ortaya çıkmaktadır. Özellikle bu evrakın resmi değer taşıması için sayısal imza ile imzalanması gerekmektedir. Bu nedenle evrak yönetim sistemi, belge akış sistemi vb. adlarla kullanıma sunulan birçok sistemde sayısal imza desteği bulunmaktadır.

Sayısal imzanın diğer bir kullanım alanı e-posta olarak ortaya çıkmaktadır. E-posta iletilerinin de birer elektronik belge olmasından dolayı imzalı e-posta mesajları gittikçe yaygınlaşmaktadır. E-posta sistemlerinde sayısal imza kullanımı kimlik doğrulama ve bilgi bütünlüğünün ispatı açısından gaydalı olmaktadır. Son dönemlerde Avrupa'da taahhütlü e-posta uygulamaları da başlamıştır. Böylece inkar edilemezlik hizmetini e-posta ile alma olanağı müşterilere sunulmaktadır.

Sayısal imzanın diğer bir uygulama alanı da zaman damgasıdır. Zaman damgası bir verinin özet değerinin belirli bir tarih ve saat bilgisi ile birleştirilerek imzalanmasıdır. Zaman damgası hizmetini güvenilir bir zaman kaynağı kullanan sunucular üretir. Böylece bir verinin belirli bir tarihten önce var olduğu kanıtlanabilir.

Sayısal imza günlük yaşamda e-fatura, e-sözleşme, e-dilekçe vb. birçok alanda yarar saplamasının yanı sıra, birçok iletişim protokolünün içinde de bilgi güvenliği aracı olarak kullanılmaktadır [2].

4. KULLANILAN DONANIM

4.1. SILICON LABORATORIES C8051F060 Development Kit

4.1.1. Kit içeriği

Silicon Laboratories C8051F060 Geliştirme Kiti, C8051F060 mikro-denetleyici ünitesi (MCU – Microcontroller Unit) ile uygulama geliştirmek için gerekli araçları içermektedir.

Geliştirme kiti içeriğinde:

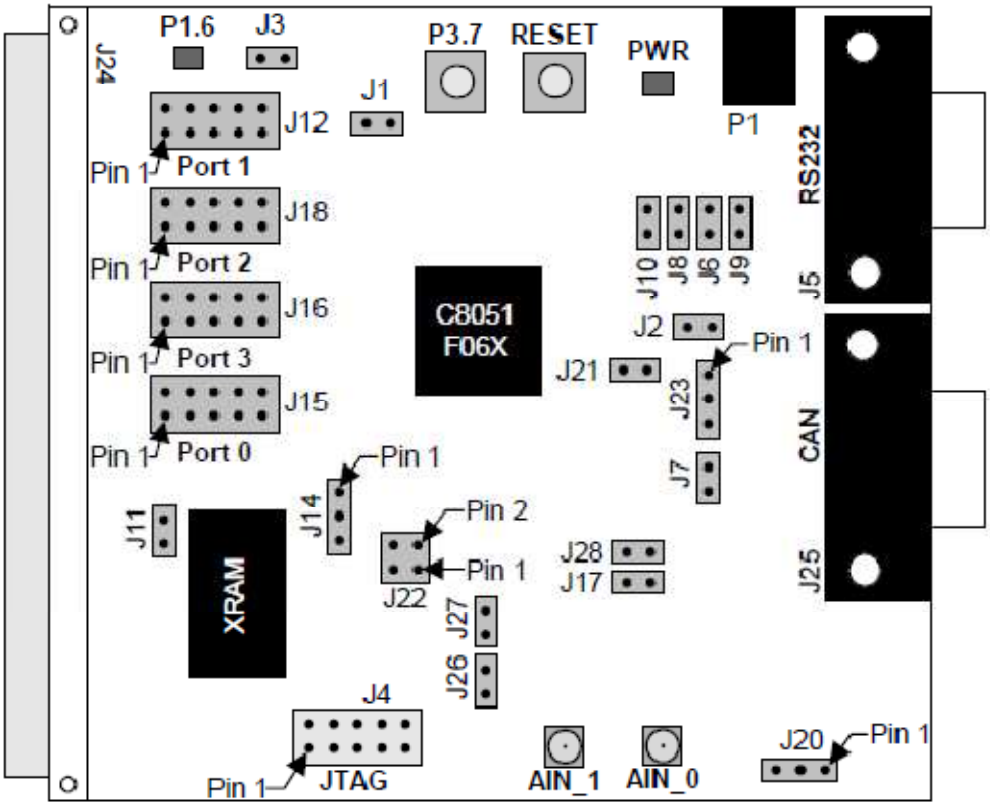
- C8051F060 geliştirme kartı,
- Hızlı başlangıç rehberi,
- Silicon Laboratories IDE(Integrated Development Enviroment – Bütünleşik Geliştirme Ortamı) ve ürün bilgisi CD-ROM'u,
- AC/DC güç adaptörü,
- USB Debug adaptörü(USB-Debug Arayüzü),
- USB kablosu

bulunmaktadır.

Geliştirme kitini yazılım geliştirmeye hazır hale getirmek için geliştirme kartının PC arayüz ve güç bağlantılarının yapılması ve bilgisayara gerekli sürücüler ile Silicon Laboratories IDE'nin kurulması gerekmektedir.

4.1.2. Geliştirme kartı

C8051F060 geliştirme kartı C8051F060 mikro-denetleyicisi, çevre birimleri ve birçok giriş/çıkış modülü içermektedir (bkz. Şekil 4.1).



Şekil 4.1. C8051F050 Geliştirme kartı [11]

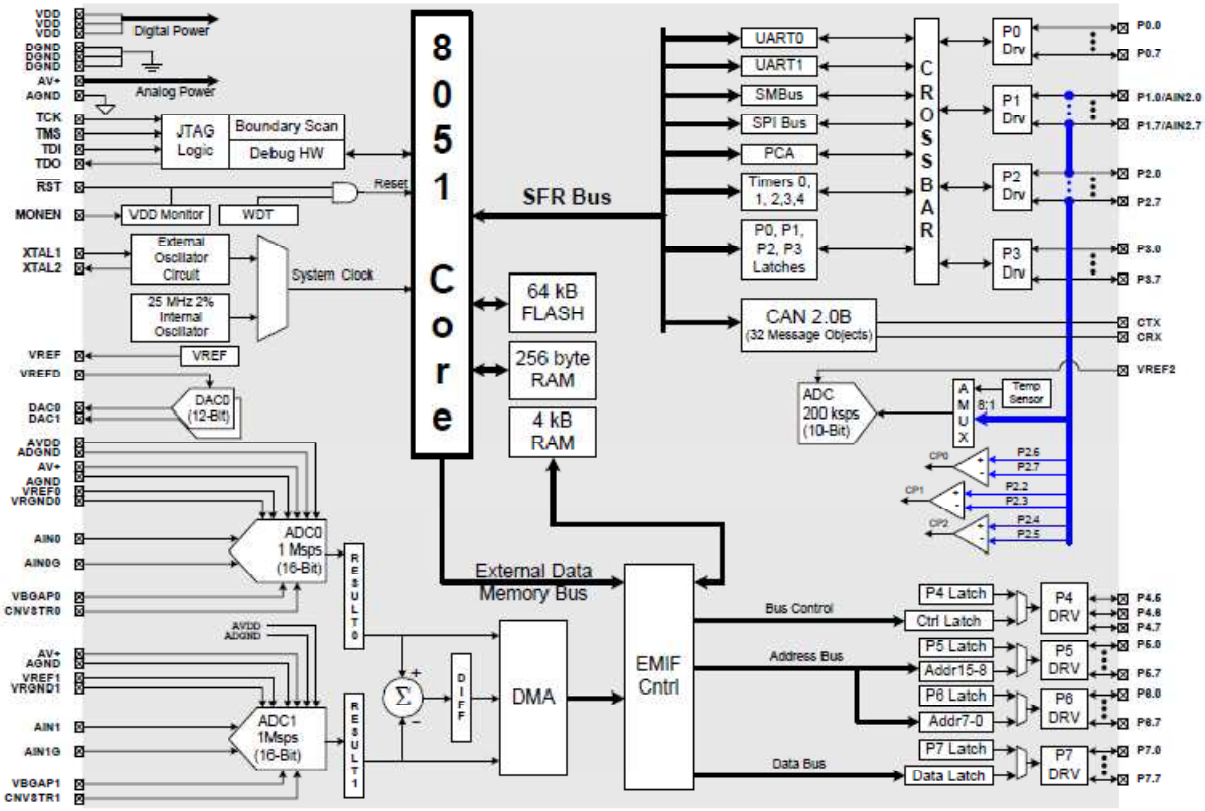
Geliştirme kartının üzerinde C8051F060 mikro-denetleyicisi ünitesi, 22,1184MHz harici kristal, anahtarlar ve LED'ler, JTAG arayüzü, RS232 alıcı-verici devresi ve DB-9 konektörü, CAN (Controller Area Network) arayüzü ve DB-9 konektörü, 128kB SRAM ve harici bellek arayüzü, analog girişler, port giriş/çıkış konektörleri ve 96 pin genişleme konektörü bulunmaktadır [11].

4.1.3. C8051F060 Mikro-denetleyici ünitesi

Geliştirme kartının üzerinde Intel 8051 çekirdeğine sahip bir mikro-denetleyici olan C8051F060 devresi bulunmaktadır (bkz. Şekil 4.2). Çipin teknik özellikleri aşağıda maddelenmiştir:

- 100 pin TQFP (Thin Quad Flat Pack) kılıf
- 25MHZ sistem saatiyle 25MIPS'e kadar çıkabilen, pipeline komut mimarisine sahip yüksek hızlı 8051 çekirdek
- 4352 bayt veri hafızası (RAM)
- 64kB Flash bellek

- Harici paralel veri belleği arayüzü
- CAN BUS 2.0B
- 59 port giriş/çıkış
- I2C, SPI ve iki adet UART arayüzü
- 5 adet 16-bit zamanlayıcı
- Dahili programlanabilir 24,5MHz osilatör
- İki adet 16-bit ADC
- 10-bit ADC
- İki adet 12-bit DAC
- Üç adet karşılaştırıcı [12]



Şekil 4.2. C8051F060 Mikro-denetleyicisi [12]

4.2. SPARTAN-3E Starter Kit

4.2.1. Kit içeriği

Spartan-3E Starter Kit tasarımcıların Spartan-3E FPGA ailesinin yeteneklerine hızlı bir başlangıç yapmaları için hazırlanmış bir geliştirme kartı çözümüdür. Kitin içeriğinde:

- Geliştirme kartı,
- Üniversal güç kaynağı (100-240V 50-60Hz),
- Değerlendirme yazılımı CD'si (Xilinx ISE® yazılımı ve EDK),
- El kitabı,
- Başlangıç kiti kaynak CD'si,
- USB kablosu

bulunmaktadır.

4.2.2. Geliştirme kartı

Geliştirme kartı(bkz. Şekil 4.3) üzerinde bulunan donanımlar:

Xilinx araçları:

- Spartan-3E FPGA (XC3S500E-4FG320C)
- CoolRunner™-II CPLD (XC2C64A-5VQ44C)
- Platform Flash (XCF04S-VO20C)

Saat işareti kaynağı:

- 50MHz kristal saat osilatörü

Bellek:

- 128 Mbit Paralel Flash
- 16 Mbit SPI Flash
- 64 MByte DDR SDRAM

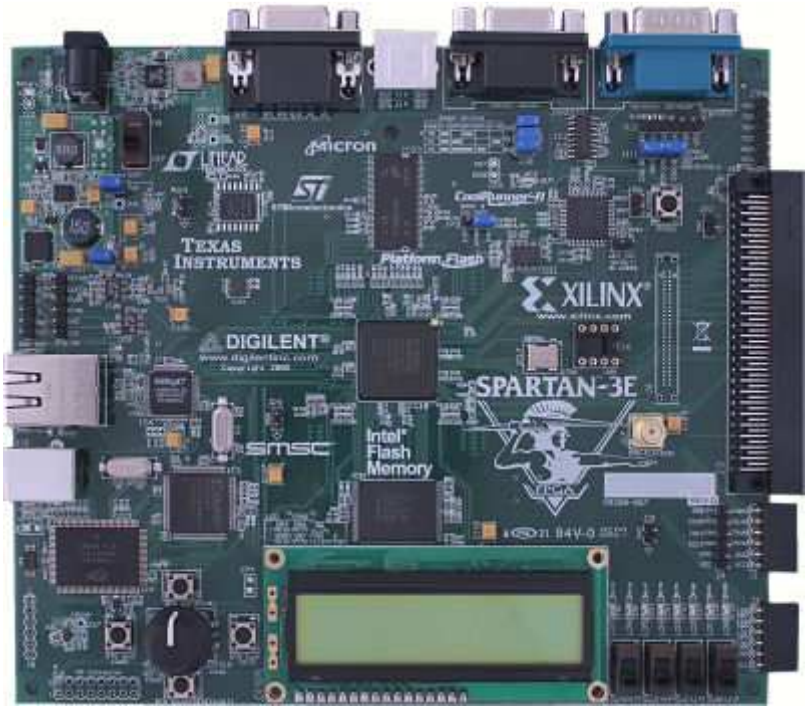
Konektör ve Arayüzler

- Ethernet 10/100

- JTAG USB arayüzü
- İki adet 9-pin RS-232 seri port
- PS/2 fare/klavye portu
- 4 adet kayan anahtar
- 8 adet LED çıkışı
- 4 adet anlık temaslı buton
- 100-Pin genişleme bağlantı portu
- 3 adet 6-pin genişleme konektörü

Ekran

- 16 Karakter – 2 satır LCD [13]



Şekil 4.3. SPARTAN-3E Starter Kit [13]

5. AKILLI KART TASARIMI

5.1. Uygulama Protokolü

Sayısal imzalar için çeşitli modeller önerilmiştir. Bunlar basit olarak “direkt” ve “hakemli” olarak ikiye ayrılabilir.

Direkt sayısal imza yalnızca haberleşen tarafları yani gönderici ve alıcıyı içerir. Bu, sayısal imzanın en basit şeklidir. Burada alıcının, göndericinin açık anahtarını bildiği kabul edilir. Basit bir şemada, sayısal imza mesajın tümünden veya mesaj özetinden göndericinin özel anahtarı ile elde edilebilir. Tüm mesajın ve imzanın, alıcının açık anahtarıyla veya paylaşılan bir simetrik anahtarla şifrelenmesiyle gizlilik sağlanabilir.

Hakemli imzalama şemasında gönderici ve alıcı tarafların dışında hakem diye tabir edilen güvenilir bir üçüncü kişi vardır. Gönderilen her imzalı mesajın içeriği ve kaynağı hakem tarafından test edilir [9].

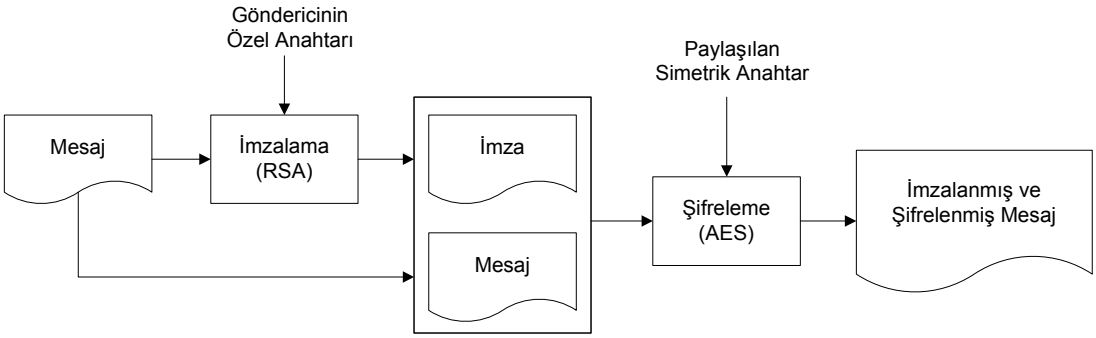
Bitirme projesinde taraflar arasında güvenli bir biçimde mesaj iletiminin sağlanması için sayısal imzalama ve simetrik şifreleme işlemlerini yapan bir akıllı kart tasarlanmıştır.

Göndericinin kimlik kanıtlaması ve mesajın değiştirilmeden alıcıya ulaştığının kanıtlanması için uygulanan sayısal imzalama işlemi için yaygın olarak kullanılan RSA imzalama yöntemi seçilmiştir. Uygulamada direkt sayısal imzalama modeli kullanılmıştır. Göndericinin özel anahtarı akıllı kart üzerinde saklanmaktadır, açık anahtarının ise herkes tarafından bilindiği varsayılmıştır. Herhangi bir açık anahtar sertifika standardı temel alınmamıştır. İmzalama işlemi doğrudan gönderilecek mesaja uygulanmaktadır.

Gönderilen mesajın gizliliğinin sağlanması için uygulanan simetrik şifreleme işlemi için gelişmiş şifreleme standardı (advanced encryption standard – AES) algoritması

seçilmiştir. Simetrik şifrelemede kullanılan anahtarın gönderici ve alıcı taraflar arasında paylaşıldığı varsayılmıştır.

Proje uygulamasında kişisel bilgisayardan akıllı karta gönderilen mesaj verisi imzalanmakta, ardından mesaj ve imza verileri birlikte simetrik şifreleme algoritması ile şifrelenmekte ve şifrelenmiş veri bilgisayara geri gönderilmektedir (bkz. Şekil 5.1).



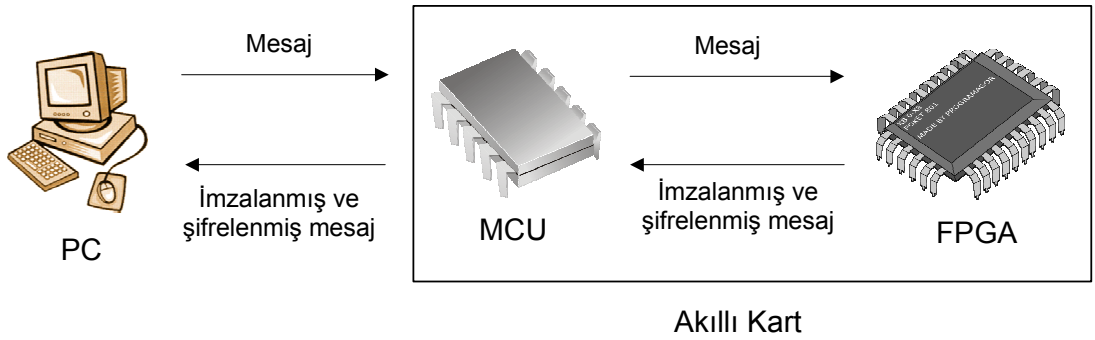
Şekil 5.1. Uygulama protokolü

Halen akıllı kartlarda işlemci olarak yaygın biçimde Motorola 68HC05 ve INTEL 80C51 çekirdekli 8-bit mikro-denetleyiciler kullanılmaktadır. Ancak gelişen teknoloji ve artan işlem yükü nedeniyle akıllı kartlarda 32-bit işlemcilerin kullanımı yaygınlaşmaktadır [3, 8].

Bitirme çalışmasında akıllı kart gerçeklemesinde Intel 8051 tabanlı bir mikro-denetleyici olan C8051F060 kullanılmıştır. Bu mikro-denetleyicide yazılım geliştirme için kullanılan geliştirme kiti 4. bölümde tanıtılmıştır. Uygulamada tasarlanan akıllı kartta kriptografik işlemlerin gerçekleştirilmesi için yardımcı işlemci tasarlanmıştır. Yardımcı işlemci tasarımı için XILINX Spartan 3-E FPGA kullanılmıştır. Yine yardımcı işlemci tasarımında kullanılan FPGA geliştirme kiti de 4. bölümde tanıtılmıştır.

Esneklik ve yüksek hız kapasiteleri FPGA'leri kriptografik uygulamalar için oldukça elverişli kılmaktadır. Yapılarından dolayı, genel amaçlı mikroişlemciler için uygun olmayan karmaşık aritmetik işlemler çok daha verimli gerçekleştirilebilmektedir. Ayrıca geleneksel ASIC (application specific integrated circuit - uygulamaya özel tümleşik devre) donanımlarından daha efektif maliyetli çözümler sunmaktadırlar. FPGA tasarımının prototip geliştirme süresinin kısa olması, değişikliklerin kolaylıkla uygulanmasını sağlamaktadır [14].

Uygulamada kullanılan mikro-denetleyici, kişisel bilgisayar ile akıllı kart arasındaki veri iletişimini sağlamakta ve yardımcı işlemciye gerekli verileri göndererek kriptografik işlemlerin yerine getirilmesini sağlamaktadır. İmzalama ve simetrik şifreleme işlemleri ise yardımcı işlemci olarak kullanılan FPGA üzerinde gerçekleştirilmektedir (bkz. Şekil 5.2).



Şekil 5.2. Akıllı kart veri iletişimi

5.2. Kullanılan algoritmalar

5.2.1. RSA

RSA şifreleme tekniği en çok kullanılan açık anahtar altyapılı kripto sistemidir. Güvenliği çarpanlara ayırma probleminin zorluğuna dayanan RSA, sayısal imza için veya gizlilik için kullanılabilmektedir. RSA şifreleme algoritması aşağıdaki gibidir:

RSA açık anahtar şifreleme metodu için anahtar üretimi:

1. Yaklaşık aynı boyutlarda, farklı iki büyük asal sayı p ve q üretilir.
2. $n=pq$ ve $\varphi=(p-1)(q-1)$ hesaplanır.
3. $1<e<\varphi$ aralığında, obeb$(e,\varphi)=1$ olacak şekilde rastgele bir e tamsayısı seçilir.
4. $1<d<\varphi$ aralığındaki $ed\equiv1 \pmod{\varphi}$ olan tek d tamsayısı hesaplanır.
5. Burada açık anahtar (n,e); özel anahtar d olur.

Şifreleme:

Gönderici m mesajını alıcıya göndermek için şifrelemektedir.

- Gönderici, alıcının açık anahtarını(n,e) elde eder.
- Mesaj, $[0, n-1]$ aralığında bir tamsayı m ile ifade edilir.

- $c = m^e$ mod n hesaplanır.
- Şifrelenmiş mesaj c alıcıya gönderilir.

Şifre Çözme:

Alıcı orijinal mesaj m'yi, şifrelenmiş metin c'den elde etmektedir.

- $m=c^d$ mod n hesaplanarak mesaj elde edilir.

RSA açık anahtar şifreleme şemasında, mesaj uzayı ile şifre uzayı birebir-örten olduğundan, şifreleme ve şifre çözme işlemlerinin rolleri değiştirilerek sayısal imza üretilebilir. RSA imzalama şeması nedenseldir ve mesajın geri elde edilmesine olanak tanır [10].

RSA sayısal imzalama işleminde sıklıkla kullanılan bir şemadır. Genel olarak imzalanacak mesaj bir özetleme algoritmasından geçirilerek sabit uzunluklu özet verisi elde edilir. Ardından bu özet, göndericinin özel anahtarı ile şifrelenerek imza elde edilir. Son olarak imza ve mesaj birleştirilerek iletilebilir.

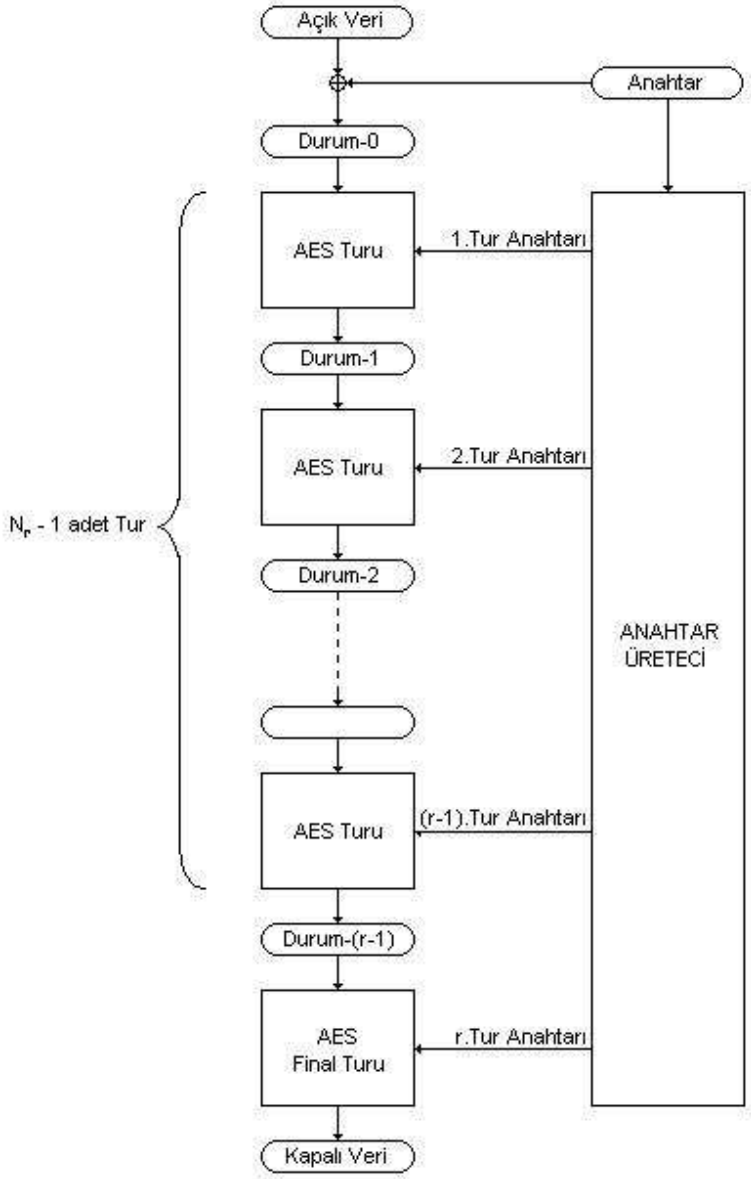
İmza doğrulama işlemi için alıcı aynı özetleme fonksiyonunu kullanarak mesajdan özet verisini üretir. Alıcı aynı zamanda göndericinin açık anahtarını kullanarak imzaya şifre çözme işlemini uygular. Elde edilen özet verisi, şifre çözme işlemi uygulanmış imza ile eşleşirse imza geçerli sayılır. Özel anahtarı yalnızca gönderici bilmelidir ve böylece gönderici geçerli bir imza üretebilir [9].

5.2.2. AES

AES algoritması 128 bit veriyi şifrelemek ve çözmek için oluşturulmuş simetrik veri kodlama standardıdır. 128 bit veriyi şifrelemek/çözmek için 128 bit, 192 bit ve yahut 256 bit anahtar uzunlukları kullanılabilmektedir. Bu kullanılan anahtarın uzunluğuna göre tur sayısı değişiklik göstermektedir. 128 bit anahtar uzunluğu için 10 tur, 192 bit anahtar uzunluğu için 12 tur ve 256 bit anahtar uzunluğu için 14 tur işlem yapılmaktadır.

AES algoritması 2 temel yapıdan oluşmaktadır. Bunlar şifreleme/çözme ve anahtar üreteci yapılarıdır. 128 bitlik anahtar uzunluğu için şifreleme/çözme işlemlerinde 10 tur işlem yapılıyor iken aynı zamanda her tur için farklı bir anahtar, anahtar üreteci yapısı sayesinde ana şifre kullanılarak üretilmektedir. Şifreleme/çözme işlemi ise

sırası ile ilk anahtar toplanması, tur sayısının 1 eksiği kadar tur işlemleri ve son olarak da final tur işleminden oluşmaktadır (bkz. Şekil 5.3).



Şekil 5.3. AES blok diyagramı

AES algoritmasının kodlama yapılırken gerçekleştirdiği tur işlemlerinin içerisindeki yapıların her birisi birer adım olarak adlandırılır. Durum tanımlama işlemi gerçekleştikten sonra final tur hariç olmak üzere turlar aşağıdaki 4 adımı gerçekleştirirler. Final turunda ise sütunları karıştırma işlemi hariç olmak üzere diğer 3 adım gerçekleştirilir.

1. Bayt yer değiştirme
2. Satırları kaydırma

3. Sütunları karıştırma
4. Tur anahtarının toplanması

Bu adımlar sırası ile gerçekleştirilince 1 tur tamamlanmış olur. 1 tur tamamlandıktan sonra bu turun çıkışları bir sonraki tur için girişi oluşturur ve tur dönüşüm işlemleri aynı sıra ile devam ettirilir. Final turuna gelindiğinde ise bahsedildiği gibi sütunları karıştırma işlemi atlanarak tur anahtarı işlemi gerçekleştirilir. Bu işlem gerçekleştirildikten sonra ise kodlanmış veri elde edilmiş olur [15].

5.3. Devre Bağlantıları

Mikro-denetleyici ve FPGA geliştirme kartlarının aralarında veri transferi yapılacağından referans gerilimlerini aynı düzeye getirmek gerekmektedir. Bunun için iki geliştirme kartı üzerinde bulunan GND uçları kablo ile bağlanmıştır.

Uygulamada kullanılan C8051F060 mikro-denetleyicisi 2 adet UART modülü içermektedir (UART0, UART1).

UART0 modülü akıllı kart ile PC'nin seri haberleşmesinde kullanılmıştır. UART0 modülünün PC ile bağlantısı, geliştirme kartı üzerinde bulunan RS-232 arayüzü üzerinden yapılmıştır. Geliştirme kartında bulunan DB9 konektörü ile PC'nin seri portu, standart seri kablo ile bağlanmıştır.

Mikro-denetleyici ile FPGA arasındaki seri haberleşme UART1 modülü kullanılarak gerçekleştirilmiştir. UART1 modülünün gönderme ucu(TX1) mikro-denetleyicinin P0.2 pinine, alıcı ucu(RX1) ise P0.3 pinine atanmıştır.

FPGA'de sentezlenen UART bloğunun gönderme ucu ise FPGA'in IO_L18P_0 isimli C7 numaralı pinine atanmıştır. Bu pin geliştirme kartı üzerinde 6-pin J4 eklenti başlığında bulunan FX2_IO10 pinine bağlıdır. Alıcı uç ise FPGA'in IO_L18N_0 isimli D7 numaralı pinine atanmıştır. Bu pin geliştirme kartı üzerinde 6-pin J4 eklenti başlığında bulunan FX2_IO9 pinine bağlıdır.

Mikro-denetleyicide bulunan ve FPGA'de sentezlenen UART bloklarının alıcı ve verici uçları arasında çapraz şekilde kablo ile bağlantı kurulmuştur.

5.4. Kart Okuyucu

PC'den akıllı karta veri göndermek ve akıllı kartta işlenip hazır hale gelen verileri PC'ye alıp görüntüleyebilmek için MATLAB uygulaması geliştirilmiştir.

MATLAB uygulamasında öncelikle seri port konfigürasyonu yapılmakta, veri alış verişine hazır hale gelen seri port açılmaktadır.

Uygulama öncelikle akıllı kart ile 2. bölümde anlatılan şekilde el sıkışmakta ve ardından PIN girişi yapmaktadır. PIN girişi kart tarafından onaylandıktan sonra karta "T=0" protokolüne uygun biçimde komut ve işlenecek veriyi asenkron modda göndermektedir. Uygulama ardından verilen komutun kartta gerçekleştirilmesini ve karttan gelecek cevabı beklemekte ve son olarak karttan alınan veriyi ekrana yazdırmaktadır.

5.5. MCU Uygulaması

Akıllı kart için mikro-denetleyici üzerinde C dilinde yazılım geliştirilmiştir.

Öncelikle mikro-denetleyici ve çeşitli birimlerinin konfigürasyonu yapılmaktadır. UART birimleri, giriş/çıkış portları, osilatör frekansı ve diğer yapıların konfigürasyonları yapılmaktadır.

Yazılım öncelikle PC ile el sıkışma işlemini yapmak için beklemekte, ardından PIN kontrolü yapmaktadır. Olumlu sonuç alınması durumunda kullanılan protokole uygun formattaki komutları beklemekte ve gelen komutları gerçekleştirmektedir. İmzalama ve şifreleme için belirtilen komut geldiğinde PC'den alınan mesajı FPGA'e göndermekte, FPGA'de işlenen mesajı geri aldıktan sonra PC'ye iletmekte ve yeni bir komut gelmesini beklemektedir.

5.5. Yardımcı İşlemci Gerçeklemesi

FPGA kullanılarak gerçeklenen yardımcı işlemci imzalama ve şifreleme işlemlerini yapmaktadır. FPGA'de sentezlenen yazılım UART, RSA, AES bloklarından ve bunları düzenleyen bir üst bloktan oluşmaktadır.

UART bloğu FPGA ile mikro-denetleyici arasındaki seri haberleşmeden sorumludur.

Mikro-denetleyiciden alınan emir doğrultusunda gelen veriler RSA bloğu ile imzalanmakta, ardından mesaj ve imza verisi AES bloğu kullanılarak şifrelenmektedir. Son olarak işlenmiş veri UART modülü aracılığıyla seri olarak mikro-denetleyiciye aktarılmaktadır.

Kullanılan UART, RSA ve AES bloklarında İTÜ Gömülü Sistem Tasarımı Laboratuvarı'nın kütüphanesinden faydalanılmıştır.

6. SONUÇLAR VE TARTIŞMA

Bu çalışmada bir akıllı kart tasarımı yapılmıştır. Bunun için C programlama dilinde yazılım geliştirilmiş ve bu yazılım Silicon Laboratories C8051F060 mikro-denetleyicisi üzerinde gerçeklenmiştir. Ayrıca yardımcı işlemci gerçeklemesi için VHDL dilinde yazılan kod FPGA üzerinde gerçeklenmiştir. Sonuçta mikro-denetleyici ünitesi ve FPGA bir arada çalışan bir sistem halinde akıllı kartı oluşturmuştur.

Çalışmada akıllı kartın PC ile seri haberleşmesi, mikro denetleyici ile FPGA'in seri haberleşmesi, FPGA'de sentezlenen kriptografik modüllerin sırayla alınan veriye uygulanması ve bütün sistemin koordineli biçimde çalışması sağlanmıştır.

KAYNAKLAR

[1] **RSA Security Inc.,** 2001. The cryptographic Smart Card: a Portable, Integrated Security Platform. *CSC WP 0301*

[2] **TÜBİTAK,** UEKAE Dergisi., Cilt 1, Sayı 1, Eylül-Aralık 2009

[3] **Naccache, D., M'Raihi, D.**, "Cryptographic smart cards," Micro, IEEE , vol.16, no.3, pp.14, 16-24, Jun 1996

[4] **Selimis, G., Fournaris, A., Kostopoulos, G., Koufopavlou, O.,** 2009. Software and Hardware Issues in Smart Card Technology, Communications Surveys & Tutorials, IEEE , vol.11, no.3, pp.143-152

[5] **TÜBİTAK,** UEKAE Dergisi., Cilt 2, Sayı 2, Ocak-Nisan 2010

[6] **Trichina, E., Bucci, M., De Seta, D., Luzzi, R.,** "Supplemental cryptographic hardware for smart cards," Micro, IEEE , vol.21, no.6, pp.26-35, Nov/Dec 2001

[7] **Başak, M., Bıyıklıoğlu, F.**, Bilgi Güvenliği ve Akıllı Kartlar, *Ağ ve Bilgi Güvenliği Sempozyumu*, ABG 2008, 16-18 Mayıs 2008, Girne, Kuzey Kıbrıs Türk Cumhuriyeti, pp.213-215

[8] **Rankl W. and Effing W.,** 2003. Smart Card Handbook. John Wiley & Sons

[9] **Subramanya, S.R., Yi, B.K.**, "Digital signatures," Potentials, IEEE , vol.25, no.2, pp. 5- 8, March-April 2006

[10] Menezes A.J., van Oorschot P.V., Vanstone S.C., 1996. CRC Press

[11] **Silicon Laboratories,** C8051F06X Development Kit User's Guide

[12] **Silicon Laboratories,** 2004: C8051F60/1/2/3/4/5/6/7 Mixed Signal ISP Flash MCU Family, Datasheet.

[13] **Xilinx.** Spartan-3E Starter Kit Board User Guide

[14] **Crowe, F.; Daly, A.; Kerins, T.; Marnane, W.;** , "Single-chip FPGA implementation of a cryptographic co-processor," Field-Programmable Technology, 2004. Proceedings. 2004 IEEE International Conference on , vol., no., pp. 279- 285, 6-8 Dec. 2004

[15] **Ahmed, Y. D.,** 2008. AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı, *Yüksek Lisans Tezi*, İTÜ Fen Bilimleri Enstitüsü, İstanbul.

ÖZGEÇMİŞ

Ad Soyad: Cem SÜMENGEN

Doğum Yeri ve Tarihi: İstanbul, 1988

Adres: Ataköy 7-8. Kısım Gazi Sitesi L8C Daire 32 Bakırköy/İstanbul-TÜRKİYE

Lisans: İstanbul Teknik Üniversitesi, Elektronik Mühendisliği - 2006

İstanbul Teknik Üniversitesi, Endüstri Mühendisliği - 2008 (Çift Anadal Programı)