ELİPTİK EĞRİ TABANLI KRİPTOGRAFİK PROTOKOL ve AKILLI KART ÜZERİNDE BİR UYGULAMA

Y. Müh. Serap ATAY

Bilgisayar Mühendisliği Bölümü

Mühendislik Fakültesi
İzmir Yüksek Teknoloji Enstitüsü, 35430, Urla, İzmir
[1]e-posta: serapatay@iyte.edu.tr

Anahtar sözcükler:Elliptik Eğri Tabanlı Kriptosistem, Kimlik Denetimi, Sayısal İmza Araçları, Akıllı Kart Teknolojileri

ABSTRACT

This paper presents the smartcards and elliptic curve cryptography-ECC- as a cryptographic solution for access control and digital signature implementations. ECC is an element of asymmetrical cryptography and it provides the same level of security with less key length than RSA or DSA. In the mean time, the requirements of computational power, process time and bandwidth are less than the others. As a result the usability of ECC is higher than the other solutions of asymmetrical cryptography. Smartcards have minimal unit prices and they can be easily used as an electronic wallet, identity card or credit card etc. Therefore, if we can meet the ECC and smartcard advantages with an implementation such as digital signature or access control, we will have a powerful security solution. Starting from this point a new project has been realized and this paper discusses the details of the project.

1. GİRİŞ

Bilgi teknolojileri altyapısı büyük yeniliklerle hızlı bir gelişim sürecinde iken, temel sorulardan birisi, bu gelişimin toplumsal ve bireysel yaşantımıza nasıl yansıyacağı yönündedir. Bu kritik sorunun yanıtı, bugün sahip olduğumuz olanaklarla, bilimsel araştırmalardaki yatırımların ilgi alanları incelendiğinde görülebilir. Hedef; daha konforlu, rahat, hızlı, ekonomik ve güvenli bir uygulama ortamına ulaşmaktır. Özellikle e-devlet, e-pasaport, e-kimlik, e-cüzdan gibi uygulamalarla sanal dünya sayısal toplumun bir parçası durumuna gelecekse, güvenlik bileşenleri iyi tanımlanmalı, doğru ve etkin biçimde kullanılabilmelidir. Kullanılan güvenlik araçları, bireyle birlikte taşınabilirken, bireyin fiziksel etkinliklerini kısıtlayıcı özellikler içermemelidir. Bu bildiride, kimlik denetimi ve sayısal imza uygulamalarında yer alan asimetrik kriptografiyle, akıllı kartların olası en etkin birlikteliği ve bu birlikteliğe engel olan sorunların ortadan kaldırılması için gerekli olan bazı yöntemler ele alınacaktır.

Kriptografi; bir mesajın iki veya daha fazla nokta arasında, mesajın aktarıldığı ortamdan bağımsız olarak, güvenli paylaşımını sağlar. Kriptografinin uygulama alanları olarak;

- kablolu ve kablosuz ağlarda ses ve/veya veri aktarımının istenmeyen kişilerce izlenmesinin önlenmesi,
- bilgisayar sistemlerinde bulunan verilere yetkisiz erişimlerin engellenmesi ve,
- güvenli bir şekilde e-ticaret işlemlerinin yapılabilmesi

örneklenebilir.

Örnekleme alanlarının tümü için aşağıda sunulan güvenlik prensipleri kriptografinin kullanımıyla sağlanmalıdır. Bunlar;

- gizlilik,
- doğruluk, bütünlük, özgünlük ve,
- inkar edilemezliktir.

Akıllı kartlarsa, çok geniş uygulama alanına sahip başka bir teknolojik üründür. Finansal uygulamalarda kredi kartı ve elektronik cüzdan olarak, e-devlet uygulamalarında kimlik kartı, ehliyet ya da pasaport olarak dünyada gerçekleştirilmiş pek çok uygulaması bulunmaktadır. Uygulama alanlarına ait riskler dikkate alındığında, akıllı kartlarda hem sayısal imza hem de veri şifreleme özelliklerinin her ikisininde bulundurulması gerekmektedir. Ancak, akıllı kartlar için sahip olunan teknoloji, mimari ve çalışma şekilleri göz önüne alındığında bazı kısıtlamalar içerdiği görülür; örneğin:

- Bellek; 1KB – 32 KB arasında değişebilen kapasite,
- İşlemci; 8-16 bit'lik bir mikro işlemci,
- Güç; okuyucuyla RF üzerinden yapılan haberleşme sırasında oluşan manyetik alan,
- İşlem hızı ve zamanı; uygulamaya bağlı olarak çok sınırlı bir işlem zamanı ya da işlemlerde yüksek hız gereksinimi gibi.

Güncel çalışmalar kriptanalize karşı dayanıklı, güvenilir ve günlük yaşantı içinde kullanılabilecek pratik bir çözüm arayışı yönündedir. Bu amaçla, Avrupa Birliği 5. Çerçeve Programı kapsamında 183milyon€ bütçe ayrılarak, sadece akıllı kartların, finans ve e-devlet gibi sosyal uygulama alanlarında kullanımını sağlamaya yönelik, araştırma-geliştirme amaçlı 65 adet akıllıkart+güvenlik projesi başlatılmıştır [11]. Gelinen son nokta, kriptografik çözümlerin FPGA ya da ASIC gibi özel tasarımlarla akıllı kartların mimarisine aktarılması şeklinde olmuştur. Bu çözümlerde, tasarım ve ilk ürünün geliştirilmesinde maliyet yüksektir ve en önemli dezavantaj ASIC tasarımlarında güncelleme yapma olanağının bulunmamasıdır. FPGA lerde güncelleme olanağı bulunmakla beraber, ürünün çok sayıda üretilmesi, maliyet nedeniyle zordur. Biometrik çözümlerin akıllı kart üstünde uygulanmasıysa henüz başarılamamış, ancak araştırmaları sürdürülmektedir[4].

Bölüm 2'de tanımlanan asimetrik kriptografi ve çözüm seçeneklerinin tümü için ortak problem; bu çözümlerin yazılım olarak ele alındıklarında ortaya çıkan performans yetersizliğidir. Araştırmanın hedefinde, akıllı kartlarda kriptografik çözümün yazılım olarak uygulanması ve hızın arttırılması için gerekli araştırmaların yapılması bulunmaktadır. Sonuç alındığında, yazılım yoluyla üretilen çözümün üretim, güncelleme ve dağıtım gibi problemleri olmayacak ve yaygın bir kullanım alanına sunulabilecektir. Özellikle, yukarıda belirtildiği gibi, finans ve toplum yaşamında yaygın bir yer alacak e-devlet projelerinde düşük maliyetli ve güvenilir çözümlerin sağlanması hedeflenmiştir.

2. ASİMETRİK KRİPTOGRAFİ

Kriptografi, bilgi güvenliğiyle ilgili pek çok çözümün çekirdeğinde görülmektedir. Tarihsel olarak bakıldığında, bilgisayar ve ağ teknolojilerinin hızlı gelişimi ve getirdiği yeni tip riskler, kriptografik çözümlerin gelişmesini ve yeni yapıları zorunlu kılmıştır. Öte yandan; kriptografik çözümlerin tümünde güvenlik, kullanılan gizli anahtarın gizliliğiyle sağlanır. Algoritmalar, herkese açıktır. Ancak, bilgisayarların hızla artan işlem gücü gözönüne alındığında, gizli anahtarın deneme-yanılma ya da diğer saldırı yöntemleriyle kolayca tespit edilememesine dikkat edilmeli ve özellikle kullanılan anahtarın bit uzunluğu ve açık anahtar-gizli anahtar arasındaki matematiksel ilişkinin karmaşıklık derecesine dikkat edilmelidir.

Diffie ve Hellman 1976 yılında geliştirdikleri tek-yönlü-tuzak fonksiyonuyla (one way trap function), gerek anahtar paylaşımı ve gerekse kimlik denetimi için çözüm olacak "Asimetrik Kriptografi"nin doğmasını sağlamışlardır [1]. Asimetrik kriptografinin güncelde sunduğu çözüm setinde;

- Faktörizasyon problemini kullanan; RSA.
- Ayrık logaritma problemini kullanan, Diffie-Hellman Anahtar Değişim Protokolu, Sayısal İmza algoritması (DSA) ve
- Eliptik eğri ayrık logaritma problemini kullanan, Eliptik Eğri Kriptosistemi (EEK), Eliptik Eğri Sayısal İmza Algoritması (ECDSA) yer alır [2].

Asimetrik kriptografinin uygulama platformlarından birisi olan akıllı kartlar üzerinde yapılan çalışmalar, kullanılan anahtar uzunluğu, gereksinim duyulan işlem gücü ve bant genişliği gibi değerler için EEK'nın en uygun kriptografik çözümlerden birisi olabileceğini ortaya koymuştur [3].

3. ELİPTİK EĞRİ TABANLI KRİPTOGRAFİ - EEK

Eliptik eğrilerin matematiksel niteliklerinden yararlanan ve eliptik eğri tabanlı kriptosistem – EEK adı verilen kriptosistem, Koblitz ve Miller tarafından ortaya konmuştur. EEK'da güvenlik; bir eliptik eğride tanımlı noktalar üstüne kurulu ayrık logaritma problemine dayandırılmıştır [2].

Bir eliptik eğri, kendisini tanımlayan polinomdaki denkliği sağlayan (x,y) noktalarından oluşur. Polinom için bir örnek olarak;

$y^2 = x^3 + ax + b \pmod{p}$ verilebilir.

Eğer (x,y) yukarıdaki eşitliği sağlıyorsa P(x,y), eliptik eğri üstünde bir noktadır denir. Eliptik eğriler, gerçek, tamsayı ya da kompleks cisimlerden herhangi birisi üstünde tanımlanabilir. Ancak bir kriptosistem için kullanılacaklarsa, tamsayı ve asal bir mod değerine göre işlemlerin yapıldığı sonlu cisimler tercih edilir. Bu noktada dikkat edilmesi gereken özellik, kullanılan asal sayının büyüklüğü ve eliptik eğriyi tanımlayan polinomla, bu cisim üstünde sağlanan noktaların sayısının ne denli çok olduğudur. Bir sonlu cisim, toplama ve çarpma gibi aritmetik işlemlerde sonlu sayıda eleman içerir ve bilgisayar ortamlarında işlemlerin kolaylaştırılması ve hızlandırılması amacıyla, ikili sonlu cisimler (F_2m) kriptografik uygulamalarda özellikle tercih edilir. Eliptik eğri üstünde tanımlanan P ve Q gibi iki noktadan geçirilen bir doğru, eliptik eğriyi üçüncü bir noktada keser. Bu durum, iki noktanın

toplanması (P+Q) olarak ifade edilir ve üçüncü bir nokta elde edilir. Bu şekilde eliptik eğrinin üstündeki bir noktadan başlayarak, noktaların toplanmasıyla yeni noktalar elde edilerek sonlu sayıda elemanı olan bir cisim elde edilir. Kriptografide bu cisimin sahip olduğu eleman sayısının olası olan en büyük değer olması beklenir. Bu nedenle, seçilecek olan eliptik eğrinin, seçilen sonlu cismin ve başlama noktasının, oluşturulacak uygulamanın güvenlik seviyesinde büyük önemi vardır. EEK aslında, bir tek yönlü kapan fonksiyonudur. Burada; P başlangıç noktası, E eliptik eğriyi tanımlayan polinom, F(q) kullanılan sonlu cisim ve noktaları toplama aritmetiği gibi bilgiler herkese açıktır. Kullanıcının, Q noktasını üretmek için seçtiği x tamsayı değeri gizli anahtarı oluştururken, elde edilen Q noktasıysa açık anahtarı verir [2].

4. AKILLI KARTLAR

Akıllı kartlar, özelliklerine göre üç ana grupta toplanır.

1. Mikroişlemcili Kartlar
   - Mikroişlemci bulundurur,
   - Kendi bellek alanında veriyi işler.
   - 8, 16 ve 32 bit işlemci mimarisi kullanılır.
   - Veri saklama kapasiteleri 300byte'dan 32KB'a kadar genişletilebilir.
   - "Chip Cards" olarak da isimlendirilir.

Kriptografik işlemler, dinamik bellek yönetimi, çok fonksiyonlu programlanabilme gibi kullanım alanları vardır. Üst düzey güvenlik mekanizmalarını barındırma, yerel veri işleme, karmaşık hesaplamaları yapabilecek bir işlemci gücü ve etkileşimli süreçleri gerektiren uygulamalara uygun bir çözüm aracıdır. Aktif olarak; kart üstünde parasal değerin tutulması, para karşılığı değer tutulması, ağa güvenli erişim ve cep telefonlarında kişisel güvenlik numarasıyla güvenliğin sağlanması işlemlerinde kullanılır[5].

2. Bellek Kartları
   - Sadece bilgiyi tutar, işlem yapma yeteneği yoktur.
   - IC bellek kartları 1-4KB veri saklayabilir.
   - Mikroişlemcili kartlara göre daha ucuzdur.
   - Güvenlik, kart okuyucuya bağımlıdır.

Ön ödemeli telefon kartları olarak yaygın bir kullanım alanına sahiptir [5].

3. Optik Bellek Kartları
   - 4MB veriyi saklayabilir.
   - Yazılan veri değiştirilemez ve silinemez.

Bu özellikleriyle, sağlık, ehliyet, seyahat ve pasaport gibi bilgilerin saklanması için uygundur[5].

Akıllı kartlar, işlemler için gereksinim duyduğu enerjiyi kartın dışından elde eder ve iletişim için bir ara birime gereksinim duyar. Bu nedenle akıllı kartlar;

- İletişimini, bir okuyucuya fiziksel temasla sağlıyorsa: Temaslı kart (banka POS terminalleri, cep telefonları GSM, SIM kartları gibi),
- RF teknolojilerini kullanıp, kendi üstünde bulundurduğu anten yardımıyla iletişimi sağlıyorsa: Temassız kart (otomatik geçiş ve bilet sistemleri gibi) olarak sınıflandırılır[5].

5. UYGULAMA BİLEŞENLERİ

Kimlik denetimi ve sayısal imza gibi güvenlik bileşenleri için, akıllı kartlarla EEK'nın bir arada kullanımı, halen İzmir Yüksek Teknoloji Enstitüsü'nde geliştirilmekte olan bir projede ele alınmıştır. Tasarımı yapılan projede; kimlik denetimi, açık anahtar altyapısı gerektiren akıllı kartların kullanımı hedeflenmiştir.

5.1 Kriptografi Bileşeni

Yukarıda bölüm 2 ve 3 de açıklandığı gibi, EEK asimetrik kriptografinin yeni bir elemanıdır. Alternatiflerine göre, daha kısa anahtar boyları ve daha az işlemci ve güç gereksinimiyle kısıtlı kaynaklarla çalışıldığında üstünlüklere sahiptir. Tablo-1, aynı güvenlik seviyesini ya da olası kriptanalitik saldırılara dirençli olma oranı olarak bakıldığında çözümlerin gereksinim duyduğu anahtar boylarını göstermektedir[6]. Tablo-2, yine çözüm seçeneklerini sayısal imza oluşturma ve imzanın doğrulanması süreçlerinde gereksinim duyulan aritmetik işlem miktarlarıyla karşılaştırmaktadır[6].

Tablo-1. Asimetrik kriptografi çözüm elemanları için aynı güvenlik seviyesini oluşturan anahtar uzunlukları.

Simetrik Şifreleme	80 bit
Asimetrik Şifreleme-Çarpanlarını bulma (RSA)	1024 bit
Asimetrik Şifreleme-Ayrık Logaritma (Diffie-Hellman)	1024 bit
Asimetrik Şifreleme-Eliptik Eğri Ayrık Logaritma (EC Diffie-Hellman)	160 bit

Tablo-2 Asimetrik Kriptografi Algoritmalarında Aritmetik İşlem Gereksinimleri

Algoritma	Çarmada Operand Uzunluğu	Çarma sayısı/ Grup Operasyon sayısı	Grup Operasyon Sayısı/ Kripto Fonksiyonu
RSA	1024 bit	1	17 doğrulama 1300 imza
Ayrık logaritma	1024 bit	1	yaklaşık 200 imza
Eliptik Eğri	160 bit	yaklaşık 10	yaklaşık 200 imza

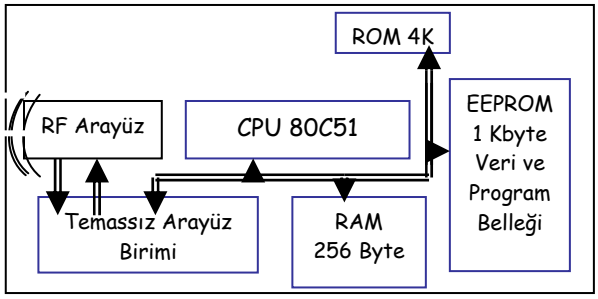
EEK'ler, bant genişliği, kısa anahtar boyları ve çarpma ya da üst alma işlemleri yerine nokta toplama işlemi kullanımı (skalar çarpma) gibi özellikleriyle tercih edilmekte ancak, istenilen hızda işlemlerin yapılması şu anda sadece algoritmaların donanıma gömülmesiyle sağlanmaktadır. Bu üstünlükler, hız problemiyle beraber bir araştırma alanı sunmaktadır. Bu nedenle projede, EEK'nın yazılımla uygulanması ve hız değerlerinin iyileştirilmesi için çalışmaların yapılması hedeflenmiştir. Tablo-3 de, farklı donanımlar üstünde 160bit anahtar boyu için EEK'de sadece skalar çarpma için işlem süreleri görülmektedir[6].

Tablo-3 EEK'de yazılımla skalar çarpma süreleri.

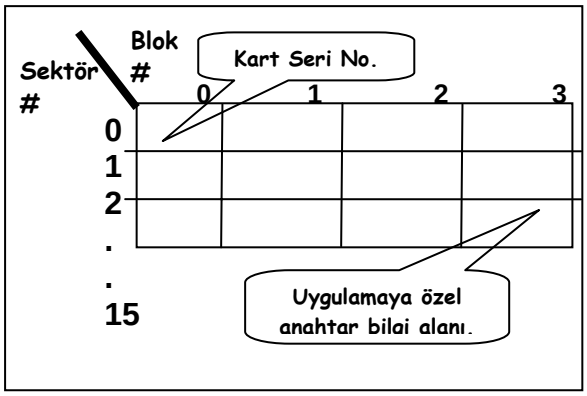
Grup	Donanım	Skalar Çarpma
2^{160}	ARM-50MHz	496.96ms
	ColdFire-90MHz	152.1 ms
	Pentium-1.8GHz	2.6 ms

5.2 Akıllı Kart Bileşeni

Projede temassız Akıllı Kart olarak Philips'in MiFare serisi IC S50 model kartlar kullanılmaktadır. Şekil 1'de kullanılan akıllı kartın mimarisi yer almaktadır[7]. Söz konusu akıllı kart, Mifare uygulama rehberi (MAD-Mifare Application Directory) adı verilen yapının kullanımıyla 15 ayrı uygulamayı üzerinde bulundurmaya olanak tanır. Şekil 2 uygulama rehberini göstermektedir [7].



Şekil 1 Philips MiFare Akıllı Kart Mimarisi.



Şekil 2 Philips MiFare Uygulama Rehberi.

5.3 Yazılım Geliştirme Bileşeni, Protokoller ve Standartlar

Kimlik denetimi ve sayısal imza uygulamalarının her ikisinde de eliptik eğri tabanlı kriptografik protokollerin kullanılması öngörülmüş olup, uygulamada ANSI C ve MIRACLE kütüphanesindeki hazır fonksiyonlar kullanılmaktadır.

Kullanılması planlanan algoritma ve protokoller [2];

- Anahtar oluşturma, sayısal imza ve doğrulama: Eliptik Eğri Sayısal İmza Algoritması - ECDSA
- Şifreleme Deşifreleme: Eliptik Eğri Şifreleme Şeması - ECES
- Anahtar değişim ve mesaj transfer protokolu : ECDH

Uyulması gereken standartlar;

- Finans sektörü için; ANSI X9.62 ve ANSI X9.63, ikili cisim (F_2m) üstünde polinom ve alan parametrelerini önerir [8, 9].
- "National Institue of Standart and Technology"-NIST'nin FIPS 186-2 içinde 15 adet elliptik eğrinin Amerika'da kullanımını önerir [10].

6. AKILLI KARTLAR VE EEK İLE KİMLİK DENETİMİ

Bir bilgisayar ağı ve/veya bir sunucuya yapılacak erişim denetiminde kimlik kontrolu esastır. Öngörülen projedeki sistemin genel olarak işleyişi tanımlanırsa; sunucunun kendisine ait bir anahtar çiftine sahip olması beklenir ve kimlik denetimini başlatmadan önce, erişime yetkili kullanıcıları için birer kimlik numarası (ID) oluşturması ve bu bilgiyi, kullanıcının akıllı kartına kendi gizli anahtarıyla şifreleyerek kaydetmesi gerekir. Bu şekilde, sunucu tarafından tanımlanan kimlik numaraları, sadece ilgili sunucu tarafından okunabilir ve veri tabanında kullanıcı kimliği için tanımlı yetkiler aktif edilebilir.

Çözümün bileşenleri ve işleyiş adımları:

1. Sunucu için anahtar çiftinin oluşturulması.
   - Uygun cisim ve eliptik eğrinin seçimi yapılır.
   - EEK anahtar çifti sunucu için oluşturulur.

2. Kullanıcının tanımlanması.
   - Sunucu bir kimlik bilgisi (ID) verir.
   - ID, açık anahtar kullanılarak EEK ile şifrelenir, akıllı karta yazılır.
   - Kullanıcı ID bilgisi, parmak izi bilgisi, yetkileri vb. bilgileri sunucu veritabanında saklanır. Bu şekilde akıllı kartın sahibi dışında bir kişi tarafından kullanımı engellenmeye çalışılır.

3. Kullanıcının tanınması ve geçiş kontrolunda sunucu.
   - Karttan ID bilgisi okunur.
   - Kullanıcının parmak izi bilgisi alınır.
   - ID bilgisi, sunucunun gizli anahtarıyla deşifrelenir ve veritabanında ID tanımlıysa, kullanıcı sunucu tarafından tanınır.
   - Parmak izi bilgileri, sunucu veritabanındaki desenle karşılaştırılır, eşleştirme başarılıysa, kartı kullanan kişinin, kartın sahibi olduğu belirlenir.
   - Denetimler başarıyla geçilirse, kullanıcının sistem erişimine izin verilir ve yetkileri aktif edilir.

7. AKILLI KARTLAR VE EEK İLE SAYISAL İMZA UYGULAMASI

Geliştirilmekte olan projede öngörülmüş olan sayısal imza uygulama adımları aşağıdaki gibidir:

- Amaç, anahtar çiftinin akıllı kart üstünde oluşturulması ve gizli anahtarın sadece akıllı kart üstünde tutulmasıdır.
- Akıllı kart üstünde oluşturulan EEK yazılımıyla anahtar çifti oluşturulur ve sertifika kurumuna sadece açık anahtar bilgilerinin gönderimi sağlanır.
- Sertifika kurumu, anahtar çiftini üreten kişi için gerekli kimlik bilgilerini alıp, tespit işlemlerini tamamladığında, açık anahtarın bu kişiye ait olduğunu gösteren bir sertifika oluşturur. Bu sertifika bilgisi, kurumun sunucusunda bulunduğu gibi, akıllı kart üstünde de saklanır.
- Akıllı kart üstünde, gizli anahtar ve sertifika bilgisi şifrelenmiş olarak kayıtlıdır.
- Sayısal imza oluşturmada, akıllı kart bir kart okuyucu üzerinden sistemle iletişime geçer. Kullanıcı parmak izi ve/veya şifreyle tanındıktan sonra, akıllı kart üstündeki gizli anahtar kullanılarak, ilgili sayısal belge imzalanabilir.
- Yukarıdaki işlemlerin tamamı MiFare SDK yazılımı kullanılarak, akıllı kart üzerinde gerçekleştirilir.

8. SONUÇ VE GELECEK

Bu çalışmayla, akıllı kart ve EEK bileşenlerinin teknolojinin günlük yaşantımıza aktarılmasında kritik öneme sahip olan güvenlik prensiplerini nasıl ve ne oranda sağlayabileceği incelenmiş, bu amaçla halen yürütülmekte olan bir projenin tanıtımı yapılmıştır. Proje bünyesinde hedeflenen; uygulamayla beraber EEK da kullanılan nokta sayma ve skalar çarpma algoritmaların iyileştirilmesi yoluyla, performans sorununa çözüm aranmasıdır. Çözüm, yazılım mühendisliği ve/veya matematik temelli olarak ortaya konabilir.

KAYNAKLAR

[1] Diffie, W., Hellmann, M., "New Directions in Cryptography", IEEE Trans. on Information Theory, 22:644-654, 1976

[2] Hankerson, D., Menezes, A., Vanstone, S. "Guide to Elliptic Curve Cryptography", Springer, 2004.

[3] "Current Public-Key Cryptographic Systems", Paper of Certicom, dd. April 1997 Updated July 2000.

[4] Card Technology Magazine, Jan. 2005, p. 12.

[5] http://www.ewh.ieee.org/r10/bombay/news5/SmartCards.htm

[6] Jan Pelzl, "Arithmetic on Elliptic Curves over GF(2n)", ECC Summer School, Ruhr-University of Bochum, Sept. 13-17, 2004.

[7] http://www.philips.semiconductors.com/

[8] ANSI X9.62 Public Key Cryptography for the Financial Services Industry: The ECDSA. American National Standarts Institute, 1999.

[9] ANSI X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography – PKC 2003

[10] FIPS 186-2 Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-2, National Standards and Technology, 2000.

[11] http://www.cordis.lu/fp5/5yr_reports.htm