TÜBİTAK UEKAE
ULUSAL ELEKTRONİK ve KRİPTOLOJİ ARAŞTIRMA ENSTİTÜSÜ

Chip Kart Kopyalanabilir mi ?
Chip Kartlara Yönelik Saldırılar

Dr. Y. Müh.
A. Murat APOHAN

Tel: 0 262 648 1767
e-posta: murat@uekae.tubitak.gov.tr
MAYIS 2006

Akıllı Kartlar

©Goverment smart card handbook

Akıllı Kartlar

- Mikrodenetleyici birimi
- RAM
  - Geçici değişkenler.
  - Oturum anahtarları.
- ROM
  - İşletim sistemi.
- EEPROM
  - Kalıcı anahtarlar, PIN,
- Kripto makinası (Crypto Engine),
- Dış çevre ile iletişim birimi (kontaklı veya telsiz).
- .....

Akıllı Kartlar

- İşletim Sistemi : Java kartlar, Multos, Cardos, Mpcos
  - Kart yönetimi
  - Güvenlik
  - Uygulamalar için platform

Akıllı Kartlar

- Government Smart Card Interoperability Specification
- ISO/IEC
- ANSI
- Biometric Standards.
- Federal Information Processing Standards (FIPS).
- EMV 2000 Specifications.
- Global System for Mobile Communication (GSM) Standards.
- .....

Akıllı Kartlar

- Gizli kripto anahtarları ve parametreleri,
- PIN,
- Karttaki e-para,
- Kimlik bilgileri,
- .....

Akıllı Kartlar

+ Standart manyetik kartlardan daha güvenli.
+ Standart manyetik kartlardan daha yetenekli.
– Kısıtlı RAM, ROM, EEPROM.
– Kısıtlı hesaplama gücü.

Kriptografik Yapılar

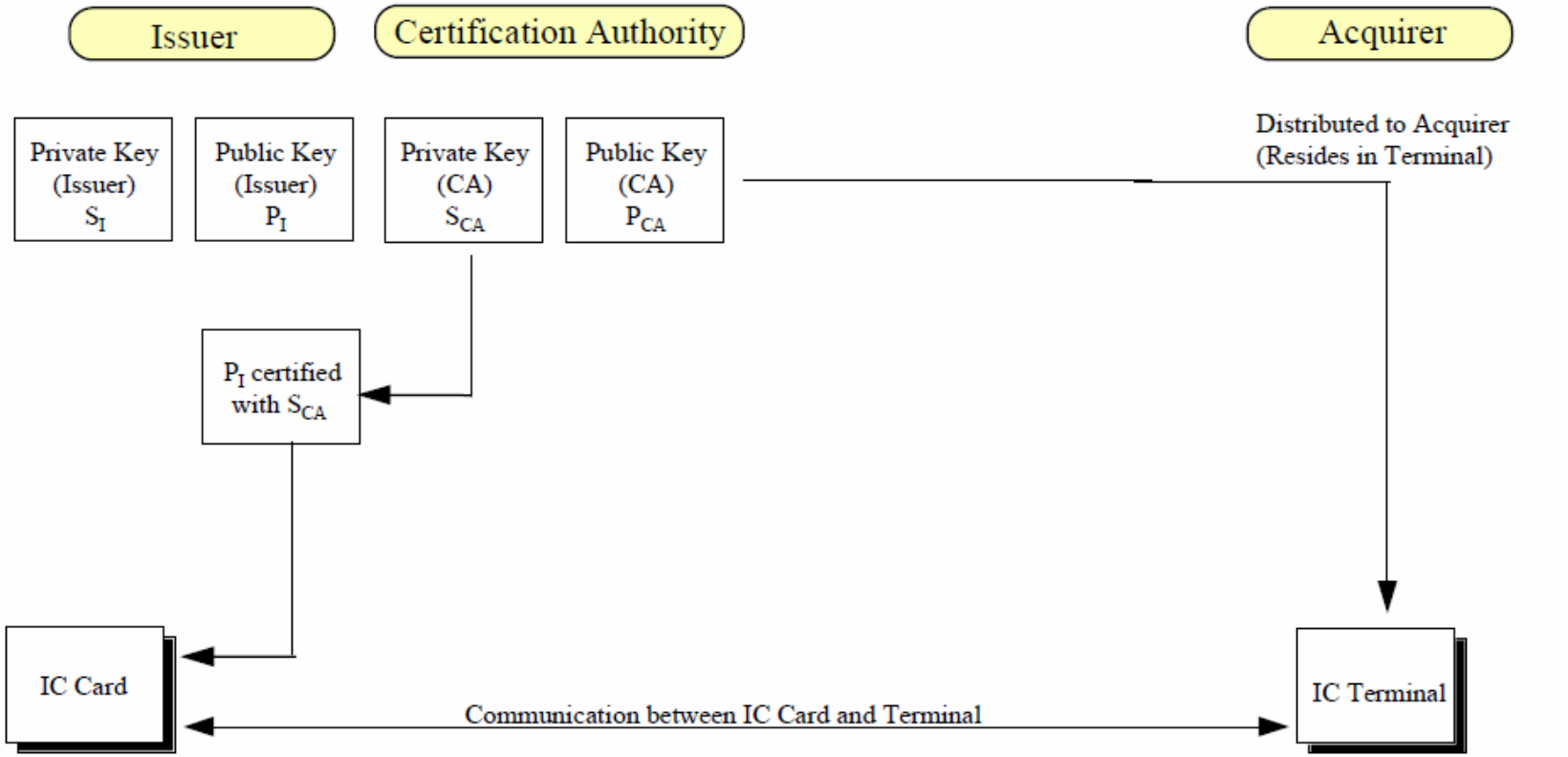
- Simetrik Algoritmalar (3DES, AES, ...)
  + Temel kriptografik servisler.
  + Düşük kaynak ihtiyacı (zaman, bellek).

  Kullanım yerleri : Gizlilik, veri bütünlüğü, ...

- Asimetrik Algoritmalar (RSA, Elliptic Curves, ...)
  + Gelişmiş kriptografik servisler.
  – Yüksek kaynak ihtiyacı (zaman, bellek).

  Kullanım yerleri : Sayısal imza, anahtar yönetimi, ...

Chip Kart Kullanım Örneği



©EMV2000 Integrated Circuit Card Specification for Payment Systems, Book 2 - Security and Key Management

Tehdit & Kaynaklar

Kabul:

- Chip karttaki gizli veriler kopyalanamaz.

Amaç:

- Karttaki gizli parametreleri ele geçirmek.

Kullanılabilecek kaynaklar:

- Kartta kullanılan algoritmalar ve protokollerin tanımları (FIPS, EMV, ...),
- Akıllı kartın kontrol komutları (ISO 7816),
- Hedef veya benzeri akıllı kartlar.

Atakların Sınıflandırılması

- Tahripli
- Tahripsiz
  - Kripto Analiz
  - Yazılıma ve donanımın açıklıkları
  - Yan kanal analizleri

Analizlerin Sınıflaması

Tahripli

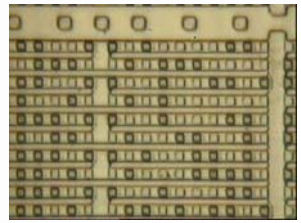
- Yüksek maliyetli araçlar (elektron mikroskobu, submikron problar, vs).
- Donanımın bazında koruma (kaplamalar).

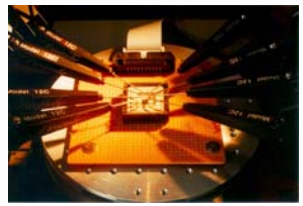
Tahripsiz

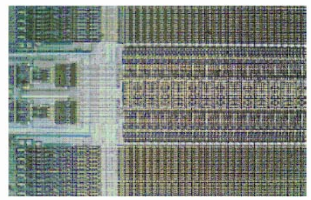
- Düşük maliyetli araçlar (osiloskop, PC, vs).
- Hasarlı analizden daha karmaşık.
- Yazılım donanım bazında koruma.

Tahripli Analizler

- Uzun analiz süresi,
- Kartta tahribat,
- İleri düzeyde uzmanlık,
- Özel laboratuar ve pahallı ekipman.







Yan Kanal Analizleri (SCA)

$\sum$

Kripto analiz
Yazılım analizi
Donanım analizi
Elektromanyetik
Optik
....

→ ***SCA***

SCA

- Kartta iz bırakmaz,
- Karta belli bir süre erişim yeterli,
- Otomatik ekipmanla sırdan biri gerçekleyebilir,
- Tahripli analizlere göre çok ucuz ekipman.

Yan Kanal Analizleri (SCA)

- Hata analizi
- Zamanlama analizi
- Güç analizi
- Elektromanyetik analiz.

Hata Tabanlı Analiz

- Kriptografik işlem sırasında sistemin hata yapmasının sağlanmasına dayanır.
- Asimetrik algoritmalar - Boneh, DeMillo, Lipton (1997).
- Simetrik algoritmalar - Biham, Shamir (1997).

Hata Tabanlı Analiz

RSA işlemi:

$$c = m^d \bmod n$$

$$n = p \times q, \qquad d = e^{-1} \bmod \mathrm{lcm}(p-1, q-1)$$

Hızlı hesaplama için:

$$c_1 = m^d \bmod p$$

$$c_2 = m^d \bmod q$$

$$c = c_1 + (((c_2 - c_1) (p^{-1} \bmod q)) \bmod q) p$$

Hata Tabanlı Analiz

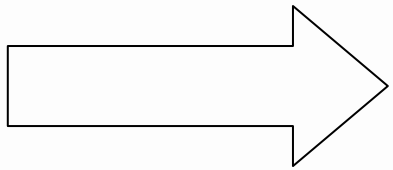
İşlem sırasında hata:

$c_1 \rightarrow c_1' \Rightarrow c \rightarrow c'$

Algoritmanın kırılması:

$\gcd(c-c', n) = q$

$\gcd(m-(c')^e, n) = q$



n çarpanlarına ayrılmış ve algoritma kırılmış olur.

Hata Tabanlı Analize Karşı Önlemler

- Bir çok kez hesaplatma.
- Gerekli yerlere kontrol mekanizmaları yerleştirme.
- Hata tespit kodları.
- .....

Zamanlama Analizi

- Bazı kripto algoritmalarının işlem yapma süresi anahtara bağlı - Kocher (1996).

- Asimetrik algoritmalar ciddi tehdit altında.

  Moduler aritmetik → Hız için optimizasyon

Zamanlama Analizine Karşı Önlemler

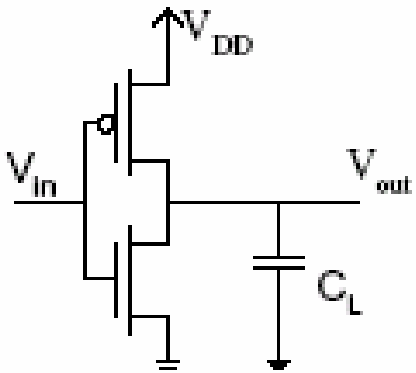
- Anahtara bağlı işlemleri sabit zamanlı işlemlere dönüştürmek.
  - Güç analizine açık hale gelebilir.
  - Çalışma hızı kaybı.
- Rasgele gecikmeler yerleştirmek.
- Hesaplamaya girdileri maskelemek.

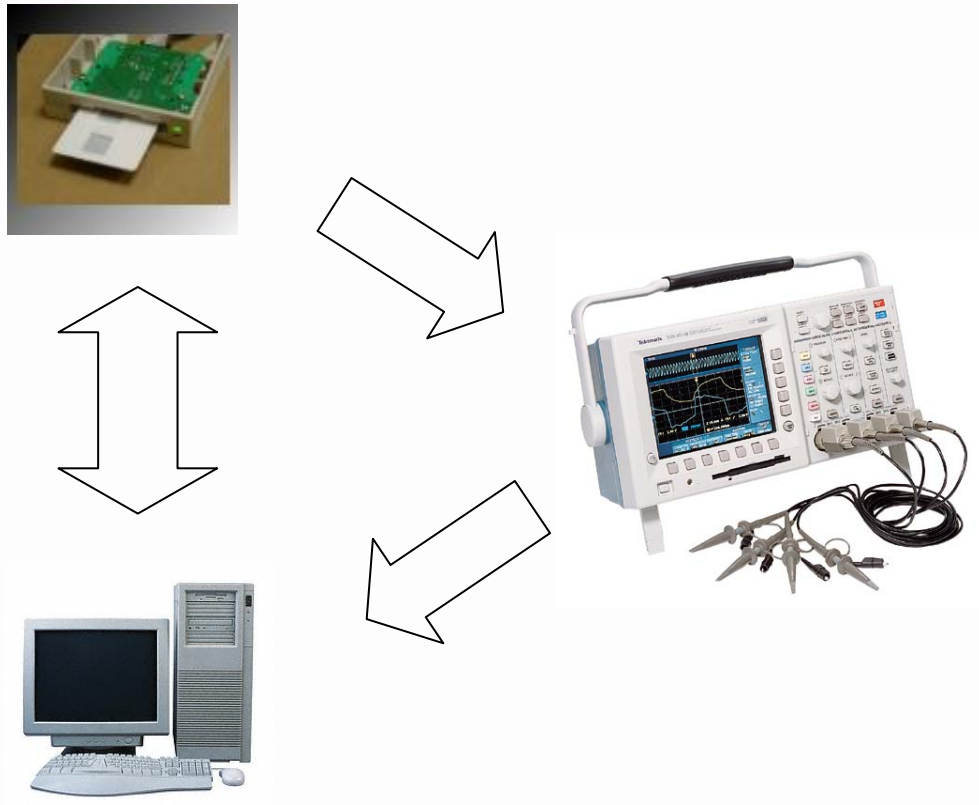
Güç Analizi

- Kocher, Jaffe, Jun (1999)
- Kriptografik işlem sırasında harcanan güç temel saldırı noktası.
- Saldırı için basit donanım ihtiyacı.

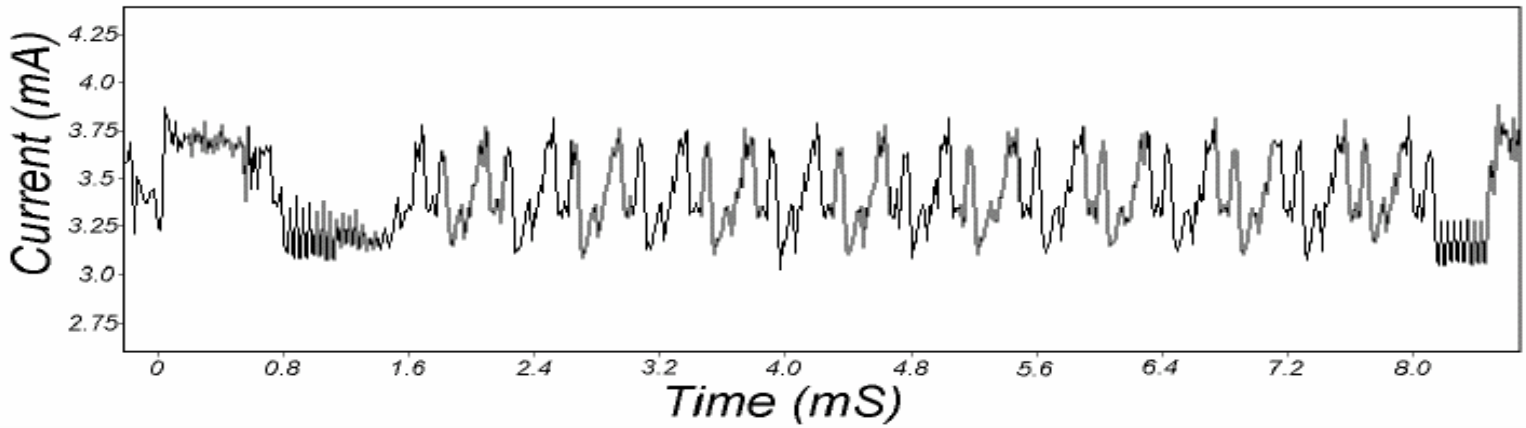
  - ❖ SPA
  - ❖ DPA

Güç Analizi - SPA

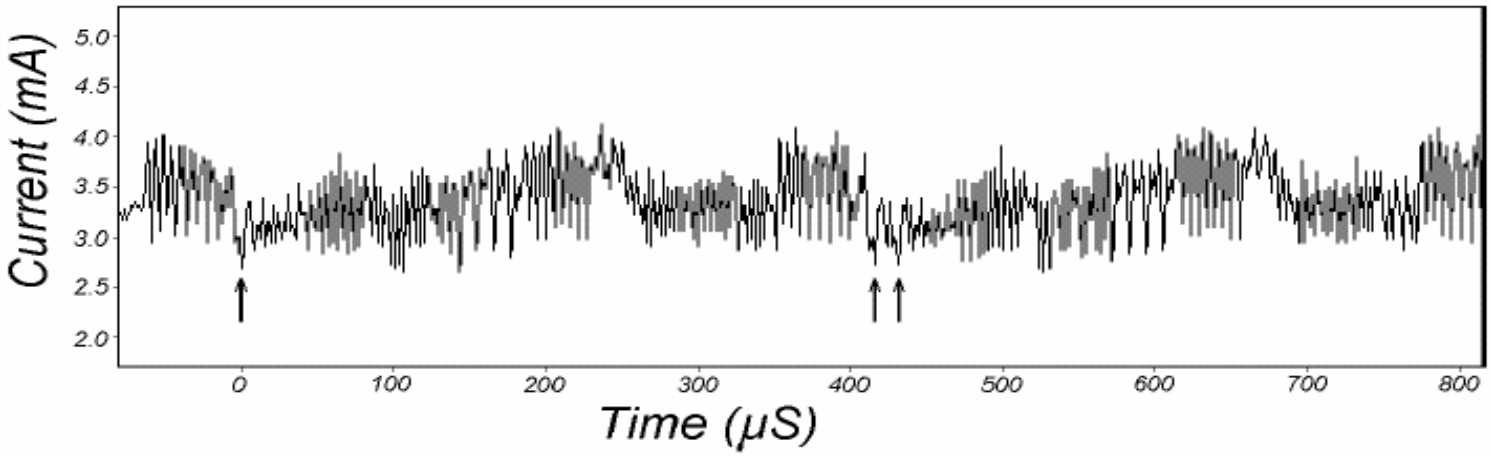




Güç Analizi - SPA



Paul Kocher, Joshua Jaffe, and Benjamin Jun *CRYPTO 1999.*



Güç Analizi - DPA

- İstatistiksel analiz teknikleri.
- Pek çok güç ölçümü.
- SPA'dan çok daha karmaşık.

Güç Analizi - DPA

"DPA Maliyet bir kaç bin dolar, kartın içerdiği güvenlik tedbirlerine bağlı olarak DPA bir kaç saniye ile saat arasında zaman alır."

Cryptograhy Research, Inc.

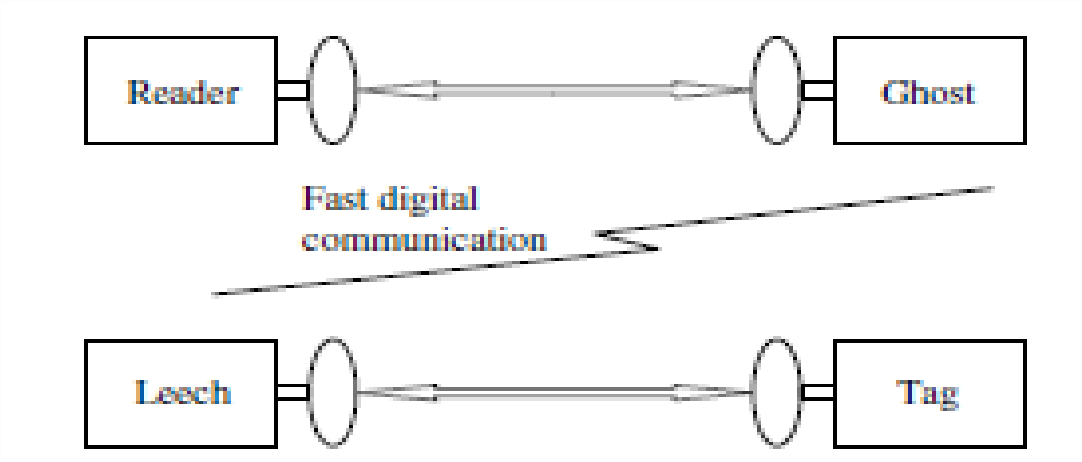
Güç Analizine Karşı Önlemler

- Donanımda alınabilecek önlemler
  - Bütün devre elemanlarının güç tüketimini veri bağımsız yapmak.
    - Yüksek güç tüketimi (mobil cihazlar),
    - Daha büyük chip alanı,
    - ...
- Yazılımda alınabilecek önlemler
  - Randomization – Maskeleme
    - Dahili gürültü üreteci.

Temassız Kartlar & Relay Analizi

"In case the card doesn't use reasonable authentication mechanisms, the card's data can be easily copied into the attacker's NFC device and used by the attacker."

Kfir and Wool (2005)



Güvenlik Açıklarının Sebepleri

- Akıllı kartların kısıtlı kaynakları,
- Tehdit değerlendirme hataları,
- Yeni analiz teknikleri,
- Gerekli bilgiye kolayca erişilebilmesi,
- Tasarım ve uygulama hataları,
- ....

Sonuç

- Korumanın & Korunanın maliyeti.
- Saldırılar henüz manyetik şeritli kartlarda olduğu gibi pratik değil.
- Analizler akademik, ancak geliştirilmeye devam ediyor.

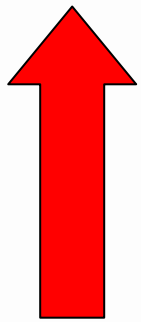
  DPA/DEMA (Agrawal, Josyula R. Rao, and Pankaj Rohatgi, 2003 CHES)

Sonuç - Sorular

- Chip kart her zaman kart sahibinin kontrolünde kullanılmalıdır.
- PIN zorunluluğu kartın yalnız bırakılma şansını azaltması nedeniyle saldırılara karşı korunmada olumlu etkisi vardır.

Sonuç - Sorular

GÜVENLİK ANALİZLERİ !!!!



Kart ve uygulama üreten firma sorumluluklar