



AKILLI KARTLAR GÜVENLİ Mİ?

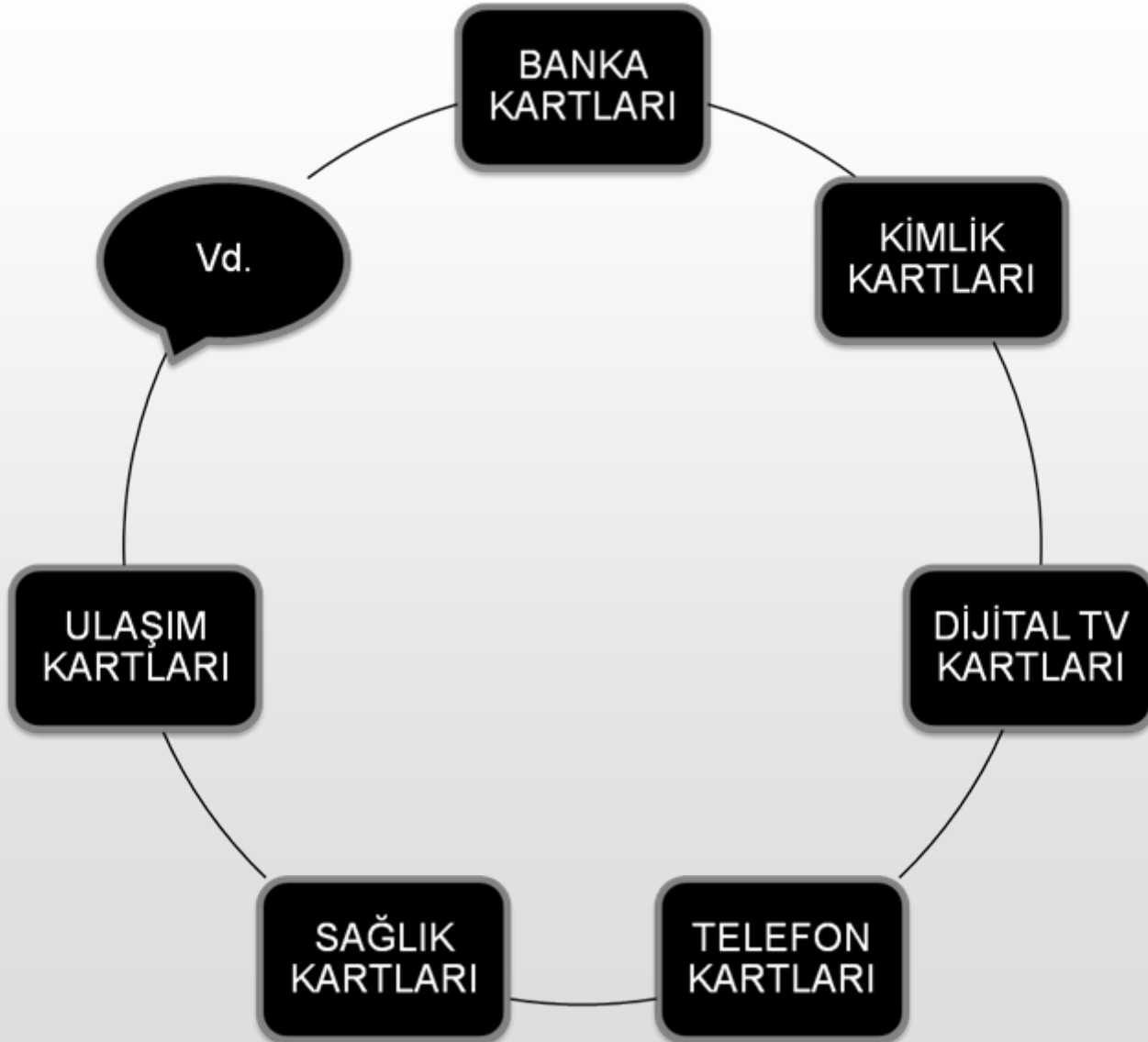
Erkut BEYDAĞLI

beydagli@uekae.tubitak.gov.tr

6 HAZİRAN 2008

- **Akıllı Kartlar ve Kullanım Alanları**
- **Ortak Kriterler (ISO 15408) Değerlendirme Standardı**
- **Akıllı Kart Atak Teknikleri**
- **Yan Kanal Analizi Atak Tekniği**
- **OKTEM Yan Kanal Analizi Faaliyetleri**

AKILLI KARTLAR & KULLANIM ALANLARI



GÜVENLİĞİN SAĞLANMASI KOLAY DEĞİLDİR !!!



TEST mi?

DEĞERLENDİRME mi?

DEĞERLENDİRME

ORTAK KRİTERLER

(ISO 15408)

www.commoncriteriaportal.org

- OKTEM Laboratuvarı



DEĞERLENDİRİLECEK AKILLI KARTLAR

- 4 Temmuz 2007 tarihli Resmi Gazete’de yayınlanan 2007/16 numaralı BAŞBAKANLIK GENELGESİ geređi,

SAĐLIK KARTLARI

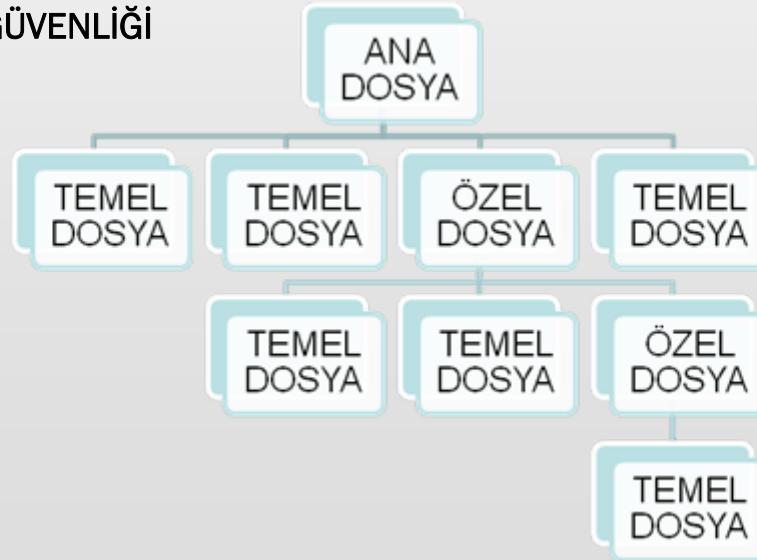
KİMLİK KARTLARI

tarafımızca deđerlendirilecektir.

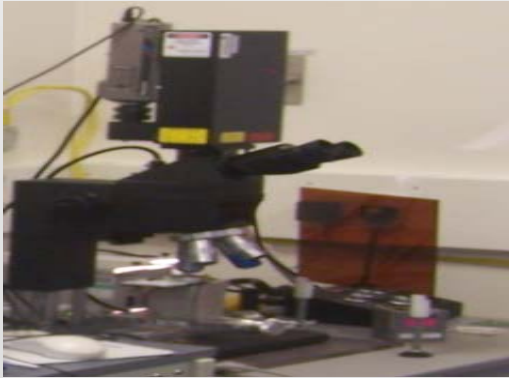
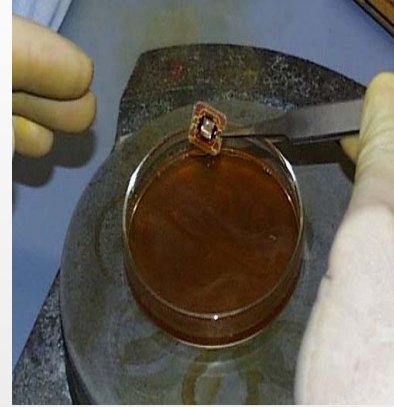
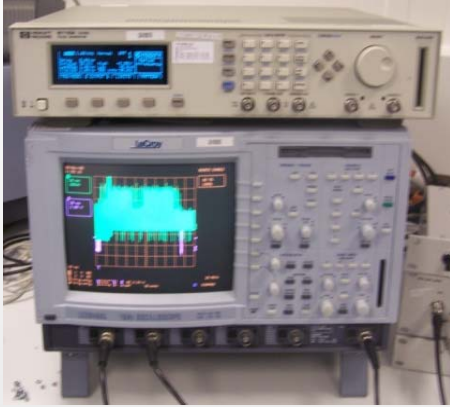
1. HABERLEŞME PROTOKOLÜ TEMELLİ ATA KLAR



2. İŞLETİM SİSTEMİ GÜVENLİĞİ



3. TERSİNE MÜHENDİSLİK & YAN KANAL ANALİZİ



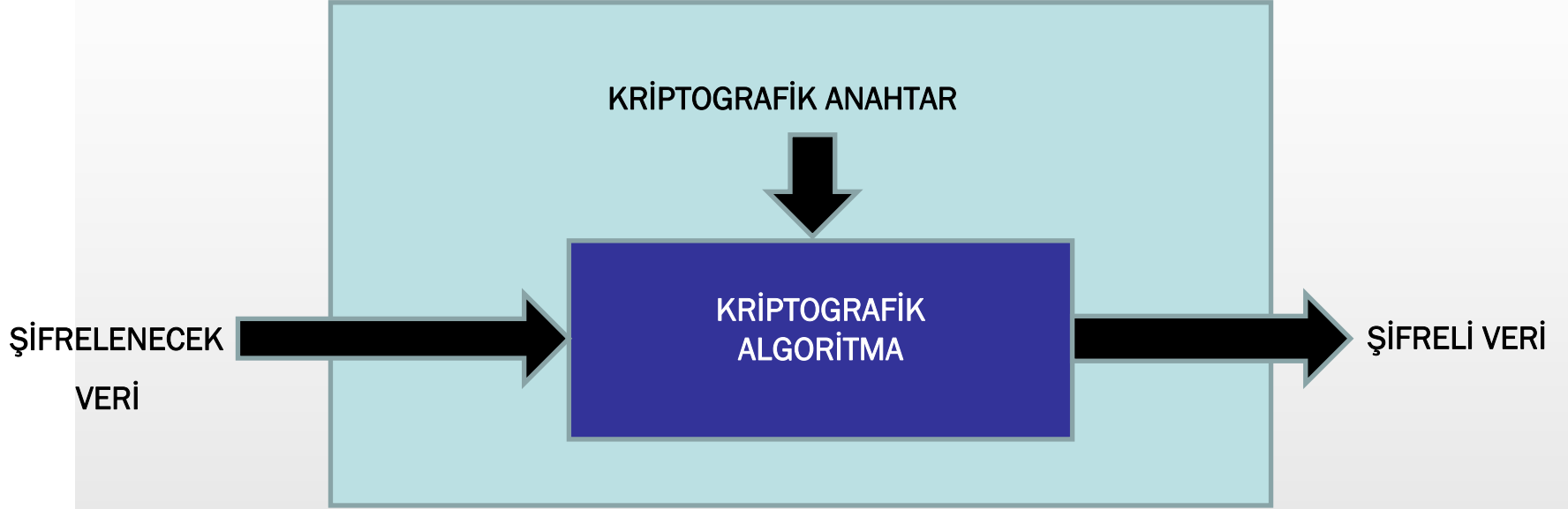
FOCUSED ION BEAM



PİNOKYO



AKILLI KART



YAN KANAL BİLGİSİ

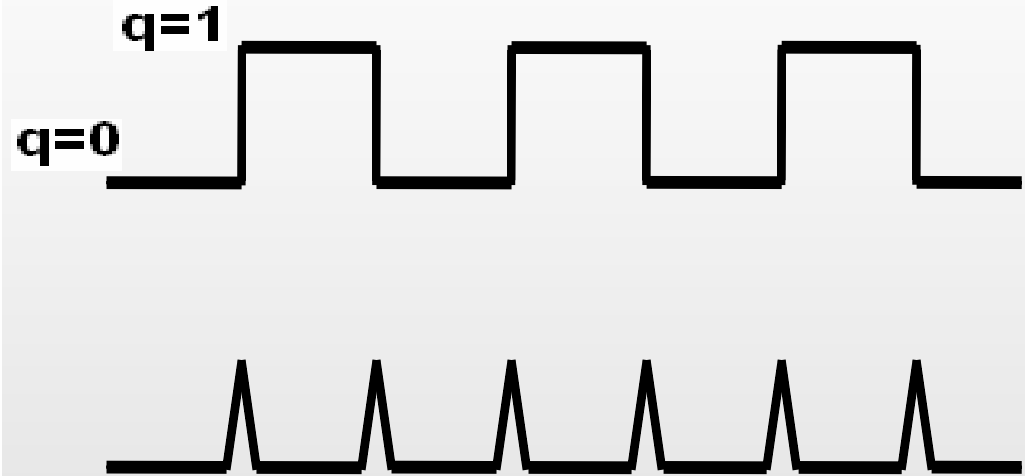
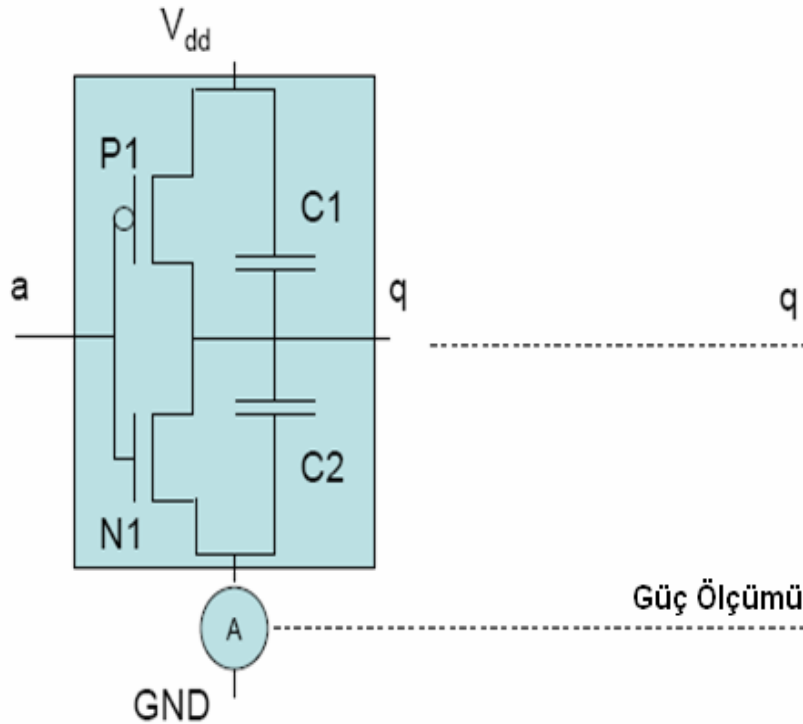
GÜÇ

ELEKTROMAGNETİK ALAN

ZAMAN

HATALI ŞİFRELİ VERİ

VERİ



CMOS transistörün çektiği güç işlediği veriye bağlıdır:

q: 0 -> 0 Güç çekimi yok, varsayılabılır.

q: 1 -> 1 Güç çekimi yok, varsayılabılır.

q: 0 ->1 Yüksek güç çekimi (C2 kondansatörü ile orantılı)

q: 1 ->0 Yüksek güç çekimi (C1 kondansatörü ile orantılı)

- 1995 yılı Paul KOCHER
- **Kriptografik protokollerde göz önüne alınmayan fakat saldırganlar tarafından elde edilebilecek bilgi nedir?**
- 500 \$ değerinde bir analog osiloskopa evde yaptığı bir çalışmada, RSA içeren bir akıllı karta saldırıyor.
- Güç eğrilerinden yola çıkarak bir gecede sonuca gidiyor.

- Tasarıma yönelik bir saldırı tekniğidir.
- Algoritmaların matematiksel güçlülüğü ile ilgilenmez.
- Saldırganın akıllı karta erişmesi atak için gereklidir.
- Akıllı kartın kurcalanmasını gerektirecek veya gerektirmeyecek atak senaryoları mevcuttur.

İşletim Sistemi ve Haberleşme Protokolü temelli atak tekniklerine ek olarak;

YAN KANAL ANALİZİ & TERSİNE MÜHENDİSLİK

atakları, akıllı kartlar için günümüzde çok ciddi birer atak tekniğidir.

Bu ataklar için; gerekli yazılımsal veya donanımsal karşı önlemlerin tasarım sırasında geliştirici tarafından düşünülmemesi, **saldırganlara açık kapı bırakacaktır.**

SECRET

**ISO 15408 (Ortak Kriterler)
DEĞERLENDİRMESİ**

TUBİTAK – UEKAE OKTEM Laboratuvarı olarak **YAN KANAL ANALİZİ** saldırıları kapsamında :

- **RSA Kripto Algoritması**
- **DES, 3-DES Kripto Algoritması**
- **AES Kripto Algoritması**
- **PIN uygulaması**

içeren akıllı kart uygulamalarına karşı yapılmış **BAŞARILI** saldırılarımız bulunmaktadır.

- Akıllı kart RSA kriptu işlemini yaparken şifrelenmek istenen veriyi gizli anahtarla modüler üs alma işlemine sokar.
- Böyle bir işlem tek bit mantığında gerçekleşiyorsa, özel anahtardaki değeri 1 olan bitler için **kare alma&çarpma**, 0 olan bitler için ise sadece **kare alma** işlemi gerçekleştirilir.
- **Eğer gerekli yan kanal önlemi alınmamışsa, kartın güç tüketim eğrisinden bu iki işlem kolaylıkla ayırt edilebilir ve ardışıl sırasına bakılarak gizli anahtar bitleri kolaylıkla elde edilir.**

.

..

...

....

$x := x.x$ (square – kare alma)

if $d=1$ (d gizli anahtardır)

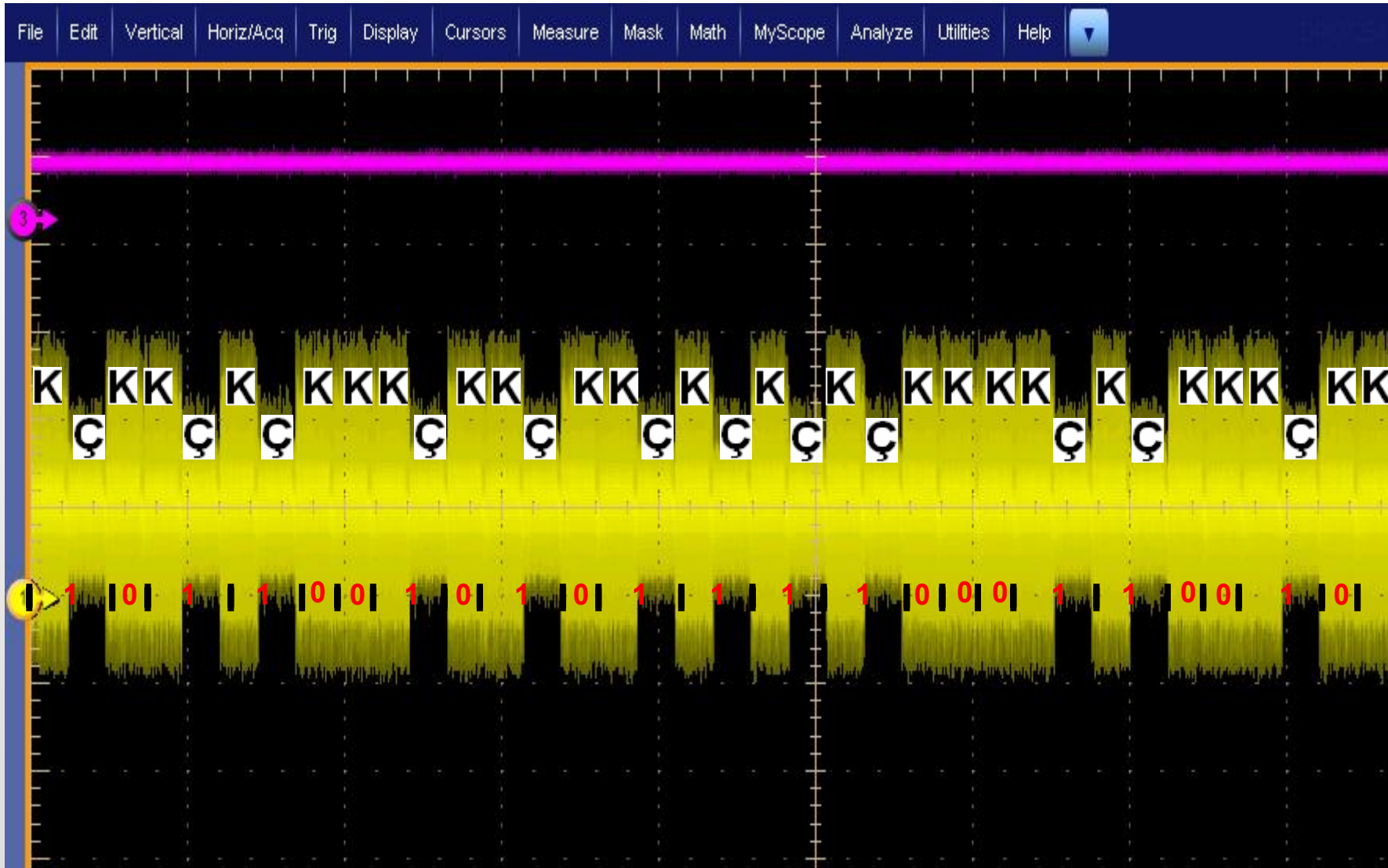
$x := m.x$ (multiply – çarpma)

.

..

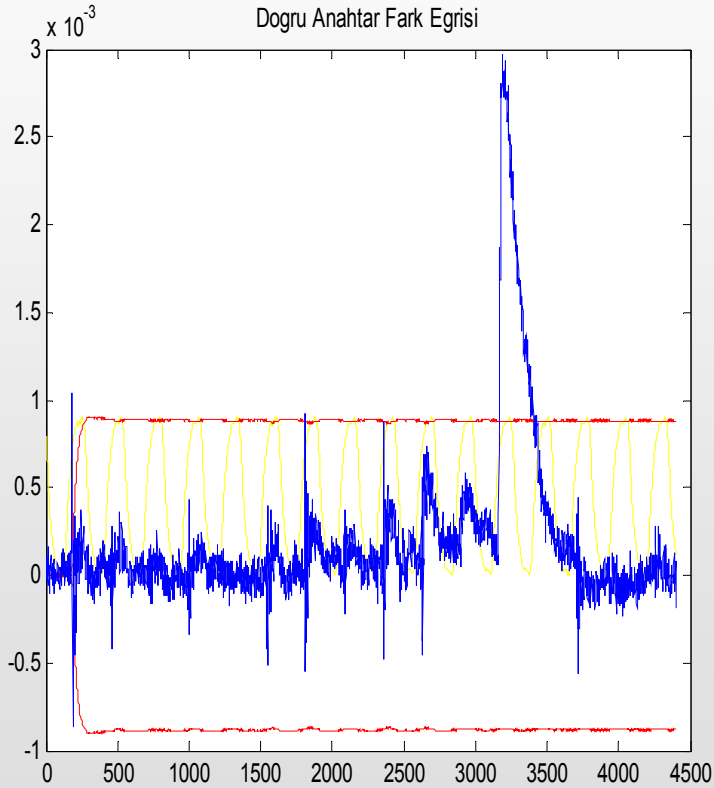
...

....

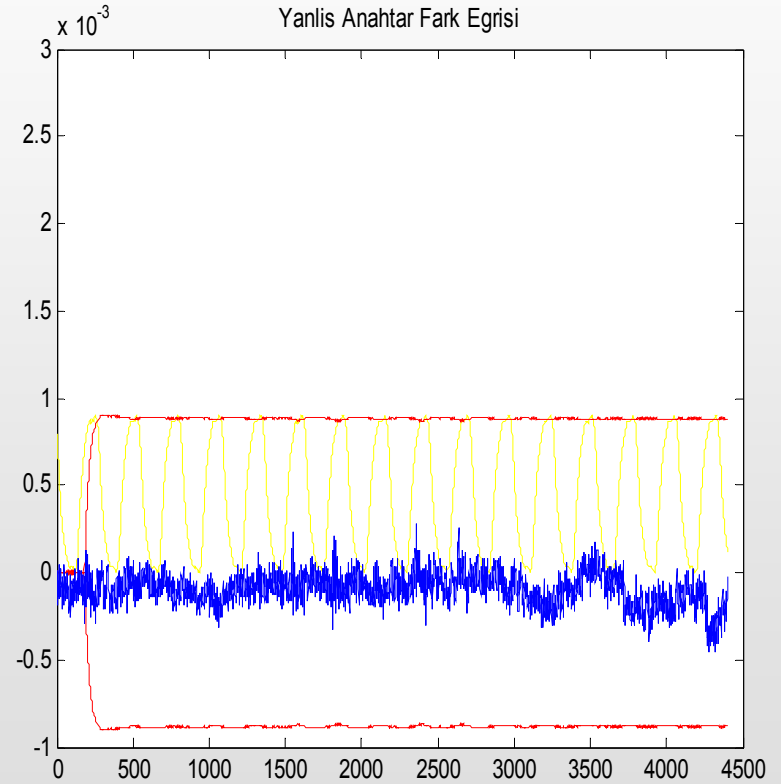


- Akıllı kartın güç tüketimi ile işlediği veri arasındaki ilişki kullanılır.
- Aynı AES anahtarı ile kapatılmak üzere yeterli sayıda (ör: 5000 adet) rasgele veri karta gönderilerek güç harcaması kaydedilir.
- Bu veri kullanılarak anahtar baytına ait tüm olasılıklar için bir güç modeli oluşturulur.
- Doğru anahtara ait model ile gerçek güç tüketimi arasında yüksek bir ilinti vardır ve doğru anahtar bu şekilde diğerlerinden ayırt edilir.

DOĞRU ANAHTAR

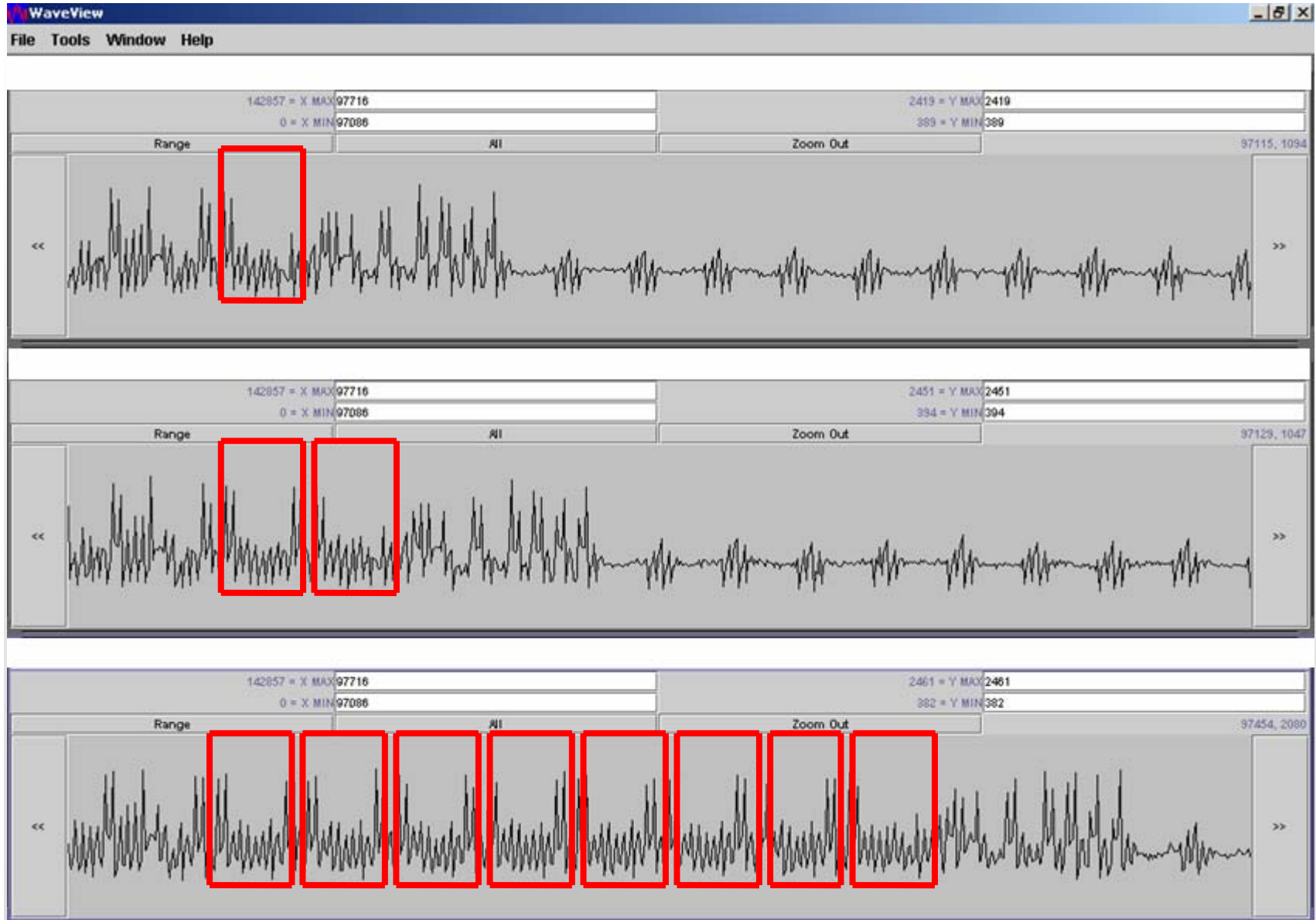


YANLIŞ ANAHTAR



- Pin doğrulama yapılırken kart, gördüğü ilk yanlış bitte, kullanıcıya yanlış yanıtını dönüyorsa,
- Denenmekte olan pin'in nereye kadar doğru olduğu anlaşılabilir demektir.
- Saldırganın n bitlik pin'e brute force (kaba güç) saldırısı yapmak için 2^n deneme yerine,
- Sadece $n+1$ deneme yapması yeterli olacaktır.

Zaman Analizi – PIN Uygulaması (2/2)



- Akıllı Kart uygulamalarında güvenliđi sađlamak için bu sunumda belirtilen dört temel atak tekniđine karşı gerekli önlemlerin geliştirici tarafından alınması gerekir.
- Aksi taktirde, akıllı kartın güvensiz olduđu kolayca söylenebilir.
- TÜBİTAK-UEKAE OKTEM Laboratuvarı tarafından gerçekleştirilen akıllı kart güvenlik deđerlendirmelerinde,
- Ortak Kriterler Standardı (ISO 15408) uygulanmakta ve bu dört temel atak tekniđine karşı analiz yapılmaktadır.



Teşekkürler Sorular

Erkut BEYDAĞLI

beydagli@uekae.tubitak.gov.tr

☎: (262) 648 1783