



ORTAK KRİTERLER VE BİLGİ GÜVENLİĞİ

Halil Tosunođlu

tosunoglu@uekae.tubitak.gov.tr

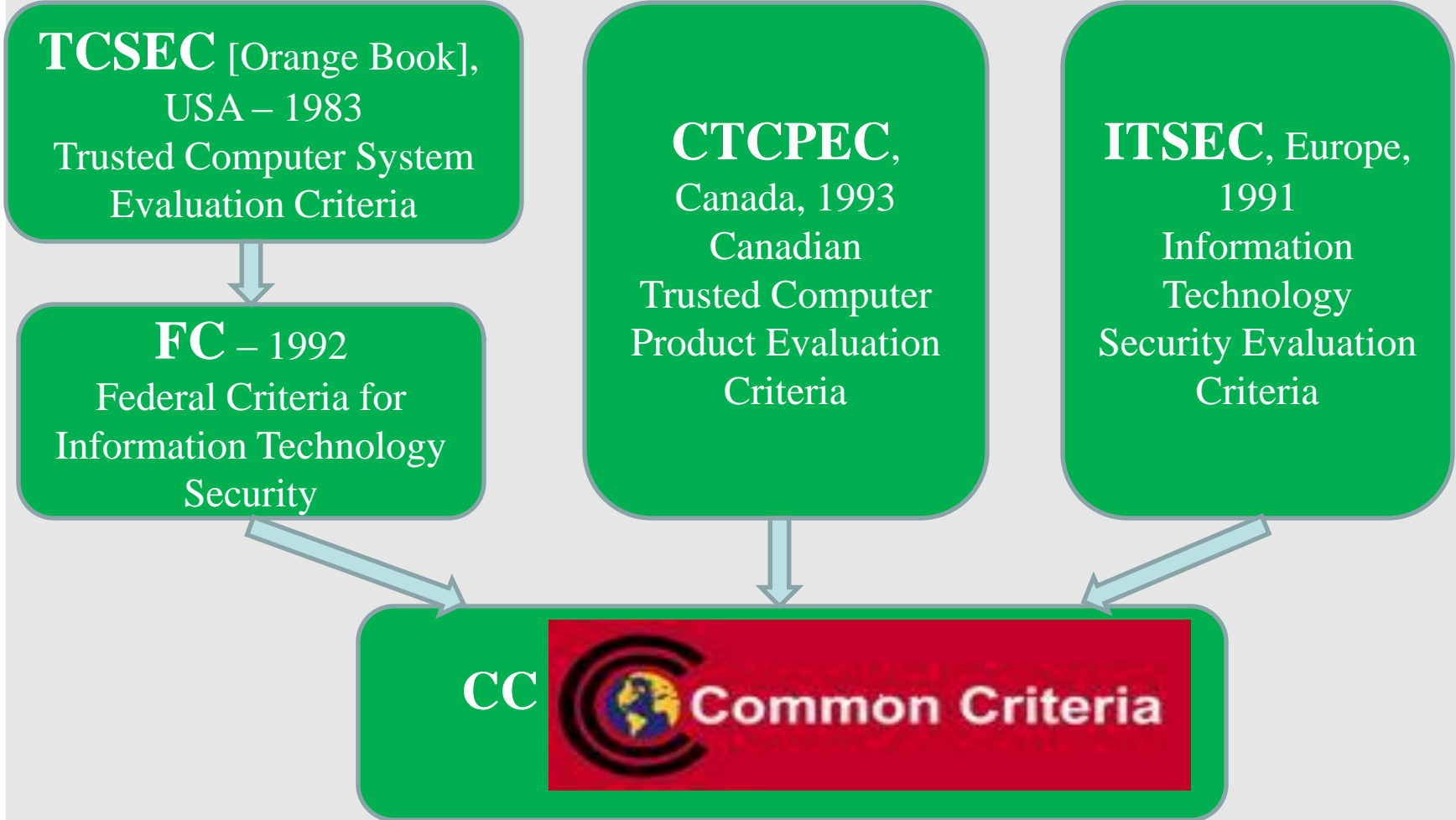
TÜBİTAK - BİLGEM - UEKAE

24 Haziran 2011, ANKARA

- **Ortak Kriterler Güvenlik Standardı**
 - Tanımı
 - Türkiye'de ve Dünya'da Gelişimi
 - Önemi

- **Ortak Kriterler Akıllı Kart Açıklık Analizi Değerlendirmeleri**
 - İnvazif Saldırıları
 - İnvazif Olmayan Saldırıları

Uluslararası IT Ürünü/Sistemi Güvenlik Standardıdır



- IT ürününün
 - Tehditlerini ve karşı önlemlerini,
 - Varsayımlarını,
 - Uyguladığı Politikalarını,
 - Geliştirme Metodolojisini,
 - Geliştirme Ortamını,
 - Teslim Prosedürlerini,
 - Müşteriye sağladığı desteği,güvenlik açısından değerlendirir.
- IT ürününe sızma testleri uygulayarak güvenlik seviyesini test eder.

Ürün geliştiricisi;

1. Tehditleri,
Ortam için varsayımları,
Kurumsal politikaları, belirler

1. Güvenlik Seviyesi İddiasında bulunur



1. Değerlendirme ve test için gereken doküman
ve ürünü sağlar

Değerlendirici:

- 1) - Tehditlerini ve onları önleme yöntemini,
- Varsayımlarını,
- Uyguladığı Politikalarını,
- Geliştirme Methodolojisini,
- Geliştirme Ortamını,
- Teslim prosedürlerini,
- Müşteriye sağladığı desteği,

güvenlik açısından değerlendirir.

2) Cihaza Sızma Testi Uygular:

- **Tehditlere**
- **Güvenlik seviyesine ve**
- **Sağlanan veri miktarına göre**
kapsam belirlenir

- 2000 : TSK OKTEM' i kurar,
- 2003 : Türkiye (TSE) Sertifika Müşterisi
- 2005 : OKTEM, 17025 Akreditasyonu
- 2007 : OKTEM, TSE'nin Lisanslı Lab1
- 2010 : Türkiye Sertifika Üretici Ülke !!!

Sertifika Üretici Ülkeler



1. Türkiye
2. Almanya
3. Amerika
4. Fransa
5. İngiltere
6. Kanada
7. Japonya
8. Avustralya
9. Yeni Zelanda
10. Norveç
11. Güney Kore
12. İtalya
- Hollanda
- İspanya
- İsveç

Sertifika müşterileri

1. Avusturya
2. Çek Cumhuriyeti
3. Danimarka
4. Finlandiya
5. Yunanistan
6. Macaristan
7. Hindistan
8. İsrail
9. Singapur
10. Pakistan
11. Malezya



- ❖ IT Ürünlerine güvenlik standardı getirir.
- ❖ Tüketicilerin, “Protection Profile” kullanmasını sağlayarak, istedikleri ürünü tam olarak belirtmelerini sağlamaktadır.
- ❖ Şartnamelere eklenen EAL seviyesi, ürün için güvenlik seviyesi belirlemektedir.

- **Ortak Kriterler Güvenlik Standardı**
 - Tanımı
 - Ulusal / Uluslararası Yeri
 - Önemi

- **Ortak Kriterler Akıllı Kart Açıklık Analizi Değerlendirmeleri**
 - İnvazif Saldırıları
 - İnvazif Olmayan Saldırıları

➤ İNVAZİF OLMAYAN SALDIRILAR

Saldırı ürün yapısını bozmaz, saldırı yapıldığı anlaşılmaz.

- Pasif güç saldırıları.
- Elektromanyetik yayılım saldırıları.
- Zamanlama saldırıları.
- Voltaj-Frekansa çentik ile hata saldırıları.

➤ İNVAZİF SALDIRILAR

Saldırı, ürün yapısı önemli derecede bozar.

- FIB ve tersine mühendislik saldırıları.
- Lazer ile hata yaptırma saldırıları.

- ✓ Güç ve Elektromanyetik Yayınım Saldırıları,
- ✓ Zamanlama Saldırıları,
- ✓ Çentik (Glitch) Saldırıları

Kripto modülünün, kripto işlemleri sırasında çektiği güç ya da yaydığı EM alan yaptığı kriptografik işlem hakkında bilgi verir.

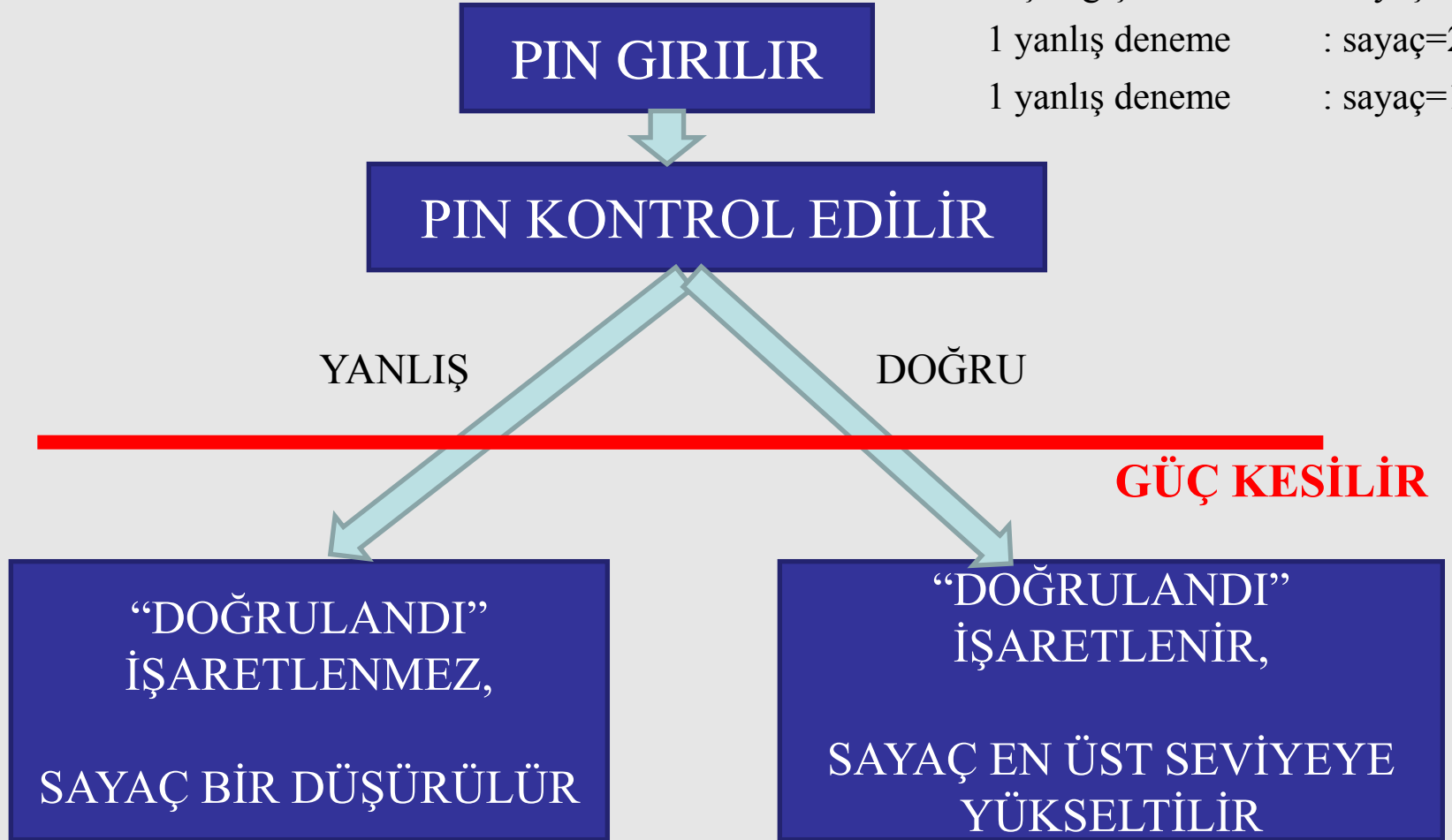
SPA → İşleme ait Anahtar tek güç/EM ölçümü ile bulunur.

DPA → İşleme ait Anahtar tek seferde bulunmaz, bilgisayara aktarılan çok sayıda güç/EM bilgisi işlenerek Anahtara ulaşılır.

- Gizli bilginin işlendiği donanımın, işletim sisteminin veya kriptomodülünün yaptığı işlem sırasında dışarı bilgi sızdırmasından faydalanılır.
- Yeterli önlem alınmadıysa, yapılan işlemde cevap dönme süresi veya çekilen güç/zaman işareti kullanılarak gizli veriye ulaşılır.

İNVAZİF OLMAYAN SALDIRILAR: KİMLİK DOĞRULAMA İÇİN ZAMANLAMA SALDIRISI ÖRNEĞİ

başlangıç : sayaç=3
1 yanlış deneme : sayaç=2
1 yanlış deneme : sayaç=1



- Voltaj ya da frekansta ani deęişiklik yapılarak:
 - Donanıma, işletim sistemine veya kriptomodüle hata yaptırılır.
 - Lazer saldırıları ile aynı neticeler elde edilebilir.
 - Hata elde etmek daha zordur.
 - Yaptırılan hatalar daha az kontrollüdür.

Tersine Mühendislik Saldırıları:

- Cihaz yapısının, işlevinin veya çalışmasının, çıkarımcı bir akıl yürütme analiziyle ortaya çıkarılmasıdır.
- Yazılım, Mekanik, Çip;
Askeri, Ticari alanlarda uygulamaları vardır.
- Ticari bir amaç için yapılırsa hukuki sonuçlar doğurur.

İNVAZİF SALDIRILAR : ASKERİ TERSİNE MÜHENDİSLİK ÖRNEKLERİ



**F/A-18 üzerinde
AIM-9**

Ruslar, K-13 füzelerini ele geçirdikleri bir AIM-9 üzerinde tersine mühendislik ile üretmiştir. NATO ele geçirdiği bir K-13'ün alt modüllerinin AIM-9 alt modülleri ile çapraz çalışabilecek kadar uyumlu olduğunu fark etmiştir.



**MiG-23 üzerinde
K-13**



B-29 Superfortress

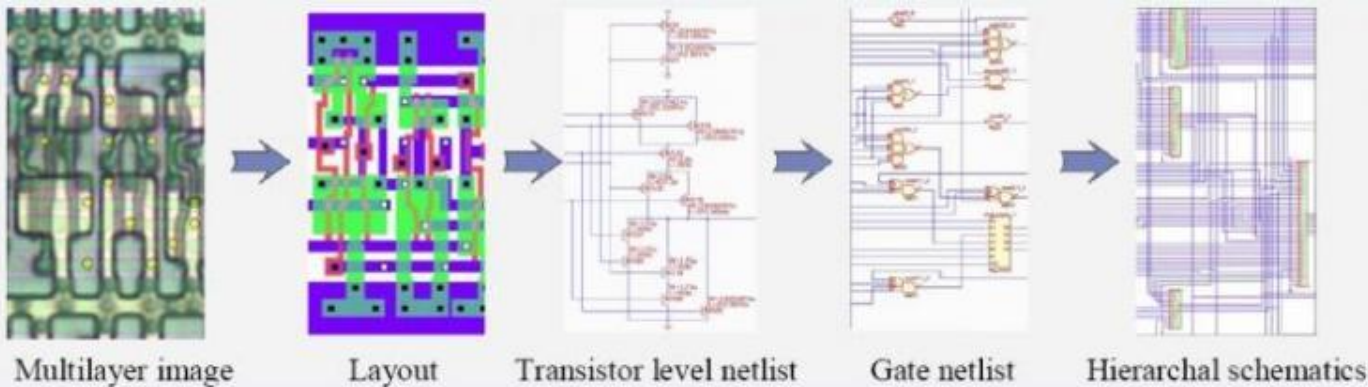
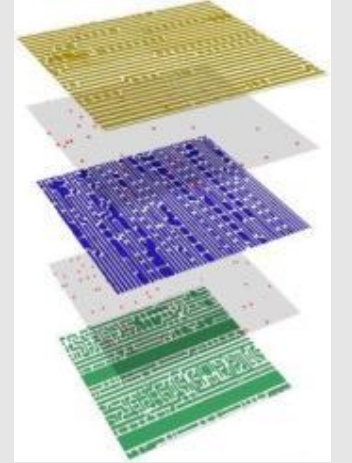
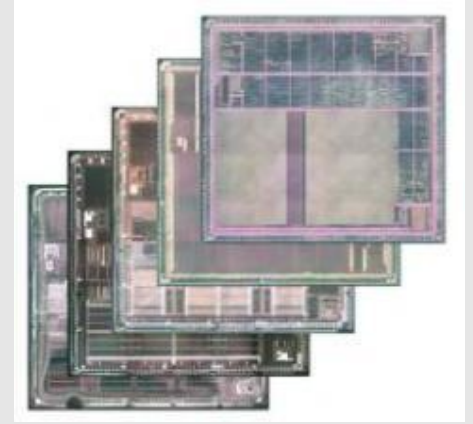
Ruslar, ele geçirdikleri bir B-29 bombardıman uçağından tersine mühendislikle Tu-4 bombardıman uçaklarını üretmişlerdir.



Tupolev Tu-4

İNVAZİF SALDIRILAR : ÇİPLERDE TERSİNE MÜHENDİSLİK

1. Çip üzerindeki kılıf soyulur
2. Metal ve yalıtkan katmanlar kimyasal veya plazma aşındırma ile sırayla kaldırılır
3. Her katman yüksek çözünürlükte fotoğraflanır



Çiplerde katman kaldırma yöntemleri



Kimyasal aşındırma



Plazma aşındırma

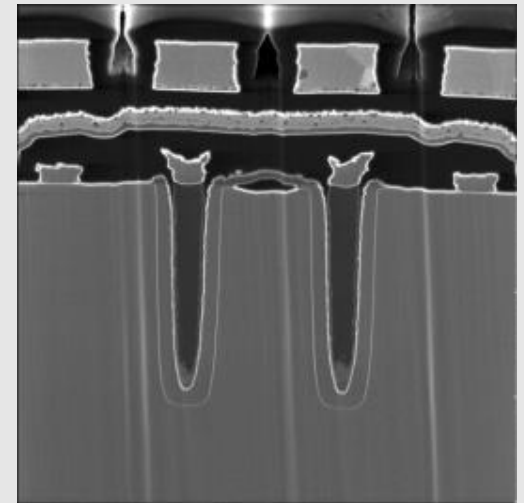
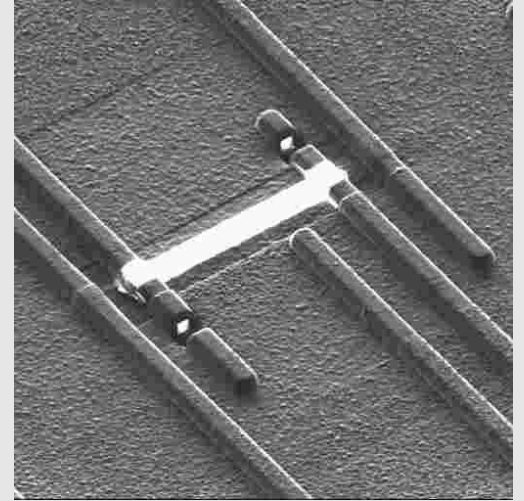
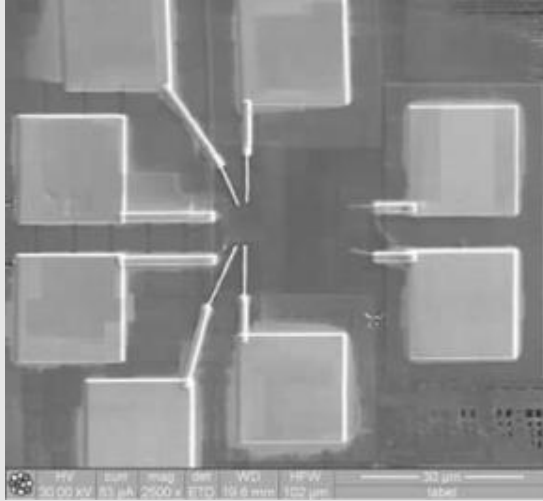
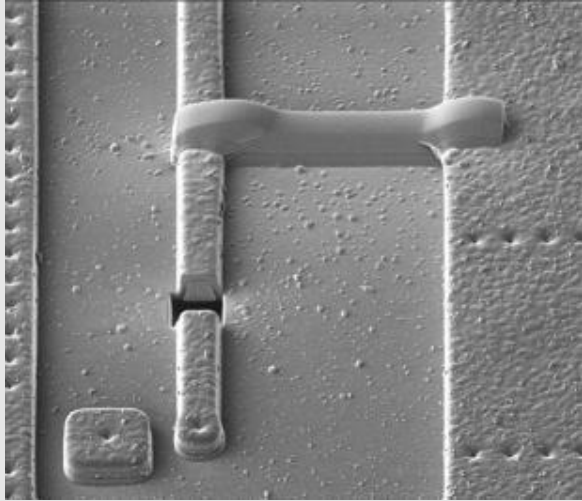
İNVAZİF SALDIRILAR : FIB (FOCUSED ION BEAM) SALDIRILARI

- FIB: Bir detektör (iyon ve elektron) ve kontrol edilebilen bir iyon (Ga) kaynağı
- İçine yerleştirilen örneklerde mikrometreler düzeyinde görüntüleme ve değişiklik.

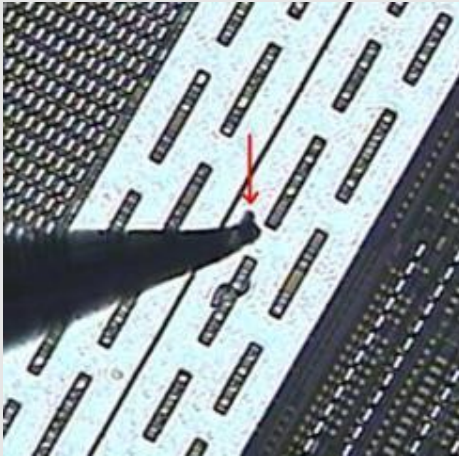
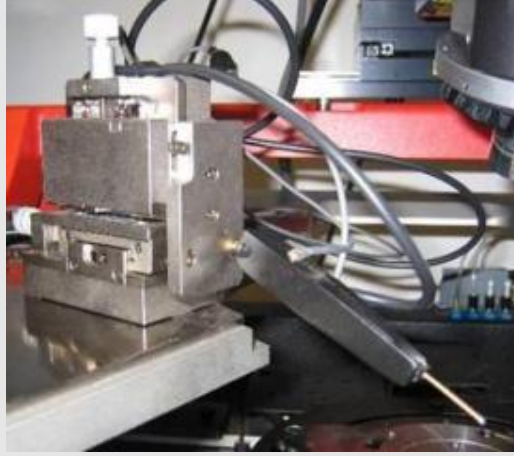


- 10^{-6} mbar vakum düzeyinde operasyon.
- Örnekler temiz ve kuru (özellikle el temasıyla yağ bulaşmamış) olmalıdır.

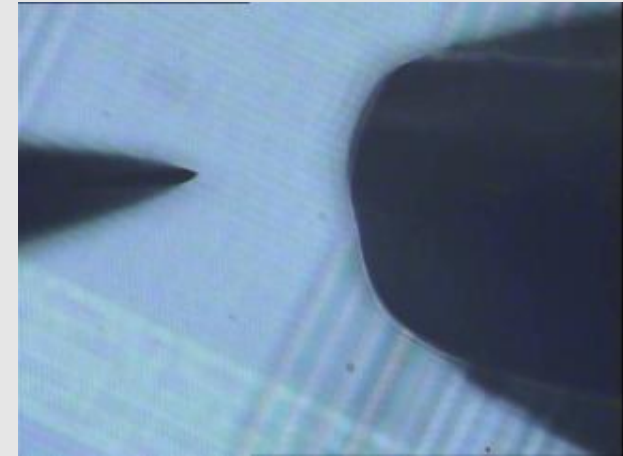
FIB ile Aşındırma, Kaplama ve Kesit Alma Örnekleri



FIB Sonrası Mikro Probing



FIB'de hazırlanmış çip üzerinde, mikro probing cihazı kullanılarak, ölçme ya da içeri sinyal gönderme işlemleri gerçekleştirilir.



Çiplerin kılıfları açılır



Yarı iletkenin yüzeyinde
mikrometre büyüklüğünde
bir alana lazer enjekte edilir



Devre hata yapar ancak hata
yaptığını fark etmez



Hata kullanılarak gizli bilgi
elde edilir



HATA ENJEKTE EDİLEN YER

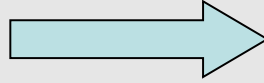
ELDE EDİLEN SONUÇ

Program sayacı
kütüğü



İşlem Atlama

Sonuç gösterici
kütük



Kapalı Yerine Açık Verinin
dışarı verilmesi

Kriptografik
işlemlerin
ara sonuçlarının
yazılı olduğu kütük



Çıkan sonuçtan
matematiksel işlemlerle
anahtarın bulunması

- Ortak Kriter Değerlendirme ve Belgelendirmesi konusunda Türkiye dünyanın sayılı ülkeleri arasında yer almaktadır.
- Ortak Kriter Test Merkezinde akıllı kart açıklık analizi konusunda en üst derecede bilgi birikimi mevcuttur.

Sorularınız?

Halil Tosunođlu

tosunoglu@uekae.tubitak.gov.tr

TÜBİTAK - BİLGEM – UEKAE