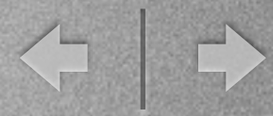



Side-Channel Attacks

Aggelos Kiayias

Side Channel Attack

- An attack against a cryptosystem using information from the implementation environment:
  - possible side channels: time, power consumption, electromagnetic emanation, sound etc.

Timing Attacks

P. Kocher, Crypto 1996

- Recall RSA Encryption / Decryption:

$$n = pq$$

$$f_{e,n}(x) = x^e \bmod n \qquad f^{-1}_{e,n}(c) = c^d \bmod n.$$

Public/Secret Key relation:

$$e \cdot d = 1 + k\phi(n)$$

Correctness based on:

$$x^{\phi(n)} = 1 \bmod n$$

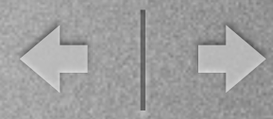
Typically public-exponent is small+fixed:
secret exponent is large

Modular Exponentiation

$$g^x = g^{x_0+2x_1+\ldots+2^{\nu-1}x_{\nu-1}}$$
$$= g^{x_0} \cdot (g^2)^{x_1} \cdot \ldots (g^{2^{\nu-1}})^{x_{\nu-1}}$$
$$= \prod_{\ell : x_\ell = 1} g^{2^\ell}$$

Required: ν modular squarings
$\#\{\ell : x_\ell = 1\}$ modular multiplications

ν = length of exponent

Implementation

```
input (g, x, n)
square = g;
result = 1;
for i = 1 to n
   if (x[i] == 1) then result = result * square mod n;
   square = square * square mod n;
end for
```

Think: you have a black-box access to this algorithm for fixed x and n (but you can specify g).

Basic Idea

Assume we know `x[0]=1`
state of algorithm is
`result = g`
`square = g^2`
To recover the `x[1]` bit : we have to distinguish between the sequence of operations
`square = (g^2 mod n) * (g^2 mod n) mod n`
takes place or whether
`result = g * (g^2 mod n)` `mod n`
`square = (g^2 mod n) * (g^2 mod n) mod n`

Focus on Modular Multiplication

- How is the operation *result* = *result* * *square* mod *n* implemented?
- Assume wlog $x_0 = 1$
- At the second step : either do a modular multiplication or not (depending on the hidden bit)
- Consider: what if we can find some *g* so that the operation "*g* g^2 mod *n*" is fast but also some other *g* so that the operation is slow?

Feasibility of Timing Attack

- Attacker is capable of timing the application of the secret-key in a number of scenarios:
  - submitting online queries since this is part of a key exchange handshake (e.g., SSL/TLS).
  - posing queries to a smartcard through a controlled smartcard reader.

Historical

- Proposed by P. Kocher in Crypto'95.
- subsequent work:
  - Against Smartcard Based RSA: J.-F. Dhem, F. Koeune, P.-A. Leroux, P. Mestré, J.-J. Quisquater, J.-L. Willems, CARDIS '98.
    - 350,000 observations for 512-bit RSA
  - Against OpenSSL: D. Boneh D. Brumley, Usenix '03. 1,433,600 observations for 1024-bit RSA

Protecting against Timing Attacks

For the specific attack against RSA:

- Prohibit clients from choosing the input to the modular exponentiation algorithm:

$$c^d \bmod n \quad \Big| \quad \begin{aligned} v &\leftarrow R^e \bmod n \\ c' &\leftarrow (v \cdot c)^d \bmod n \\ c &\leftarrow c' R^{-1} \bmod n \end{aligned}$$

Performance loss

Protecting against Timing Attacks, II

General

- Quantization of all cryptographic, key-dependent operations [they will all require the same amount of time]

Performance loss

Power Analysis

- Fundamental assumption: Attacker is able to measure power consumption information that is incurred due to a cryptographic operation.

- In CMOS logic, power is used when transistors are switching between states.

- consider: If a small resistor is inserted in series with power (or ground) the voltage difference (divided by resistance) will reveal the current.

Example

CMOS NAND gate

power supply

VCC

power supply

p-type transistors

P

P

Z

outputs

N

A

inputs

N

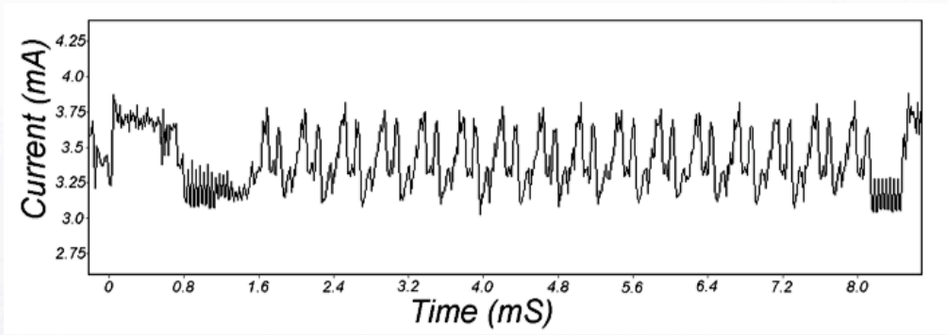
B

n-type transistors

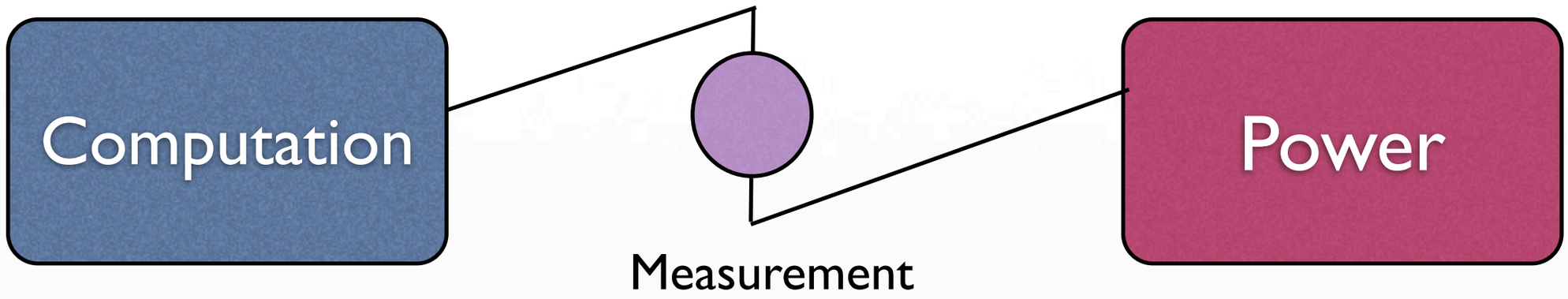
ground

GND

Oscilloscope



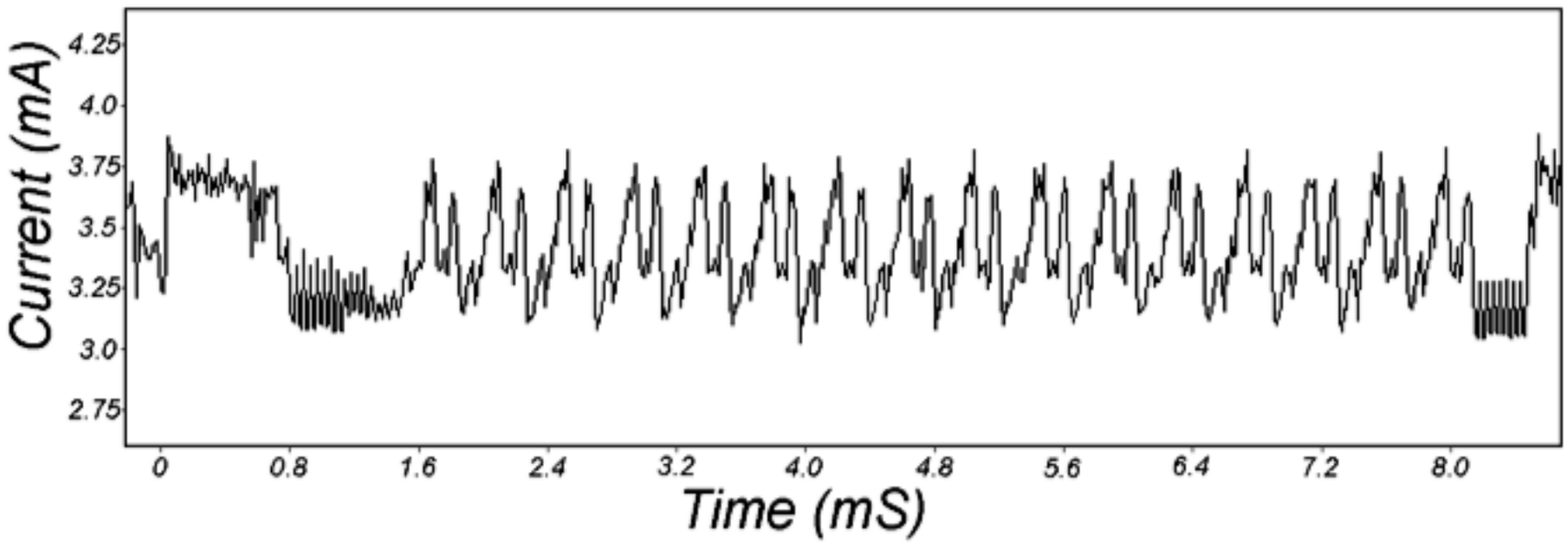
Setup



Simple Power Analysis: Power readings will be dependent on instructions performed, noise and data used.

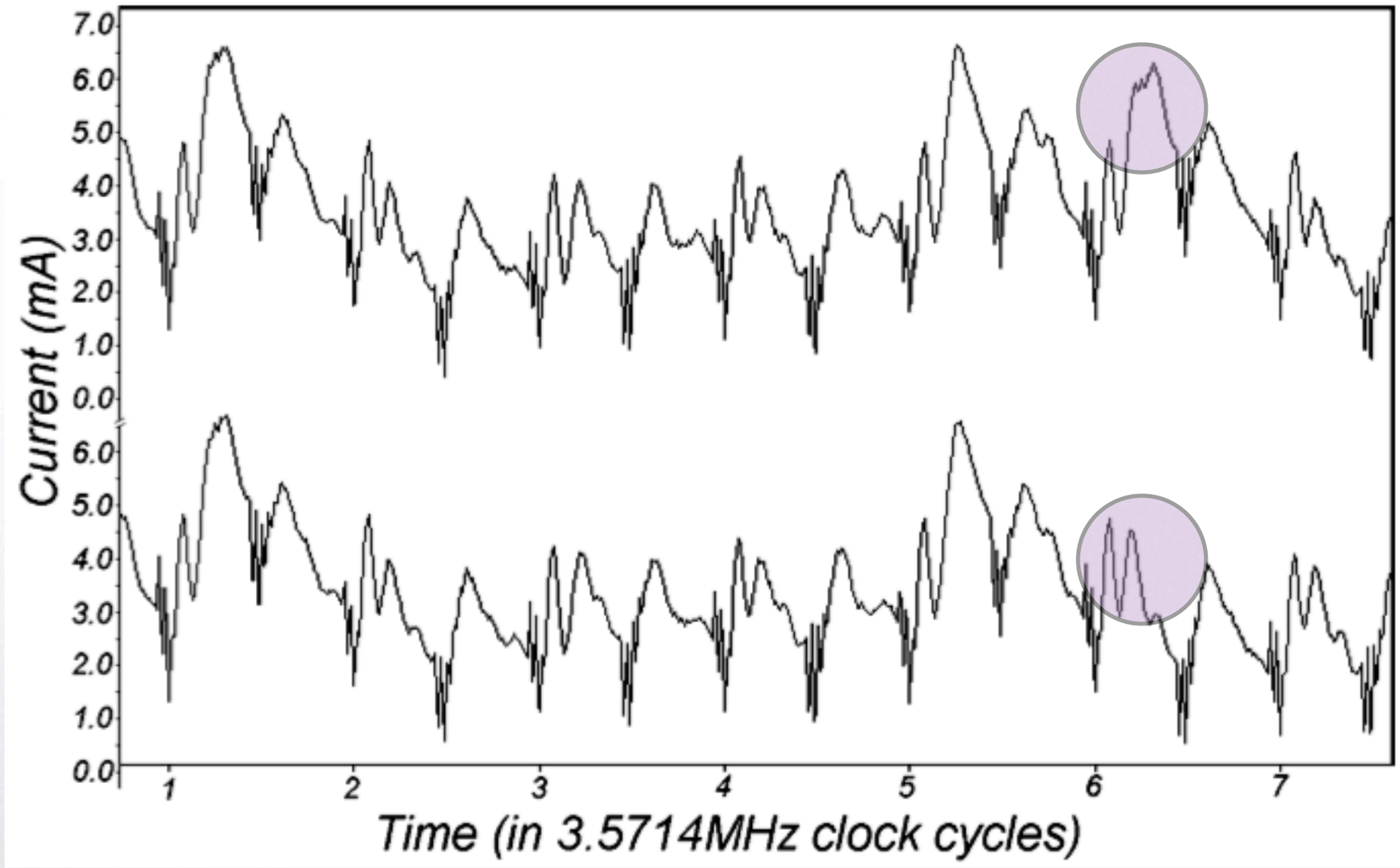
SPA & DES

P. Kocher, J. Jaffe, B. Jun, CRYPTO 99



The 16 rounds of DES are clearly visible in this SPA trace

A closer look



SPA differences like these in looping procedures reveal that different instructions were used across loops.

The specs are known => if different instructions are used conditioned on input bits -- this leaks information about the input.

Figure from P. Kocher, J. Jaffe, B. Jun, CRYPTO 99

Application to RSA

- Changes in power consumption in the modular exponentiation computation will affect the power trace.

Differential Power Analysis

- Different instruction sequences exhibit wide variability in power consumption. SPA can catch those.

- What about same instruction sequence on different data? Smaller variations can also be discernible (the difference between a "0" and "1") with massive sampling.

- *Use hypothesis testing to recover likely key bits.*

Differential Power Analysis, II

- Identify a target instruction sequence that affects a bit using a specific portion of the input you want to find (e.g., of the key).
- Measure power consumption (many samples)

power_sensitive_internal_binary_value = Bit(*public_information*, *part_of_secret_input*)

assumption: Bit(random_public_info, wrong_guess) ~ uniform over {0,1}

Differential Power Analysis, III

make m measurements

	0	1	1	1	0	0
measurements	M1	M2	M3	M4	M5	M6

Bit ← guess, public info

Compute the differential:

$$\frac{\sum_{i=1}^{m} \text{Bit}(\text{output}_i, \text{guess}) \cdot \mathbf{M}_i}{\sum_{i=1}^{m} \text{Bit}(\text{output}_i, \text{guess})} - \frac{\sum_{i=1}^{m} (1 - \text{Bit}(\text{output}_i, \text{guess})) \cdot \mathbf{M}_i}{\sum_{i=1}^{m} (1 - \text{Bit}(\text{output}_i, \text{guess}))}$$

guess is correct => differential spikes

guess is incorrect => differential zeroes

Differential Power Analysis, IV

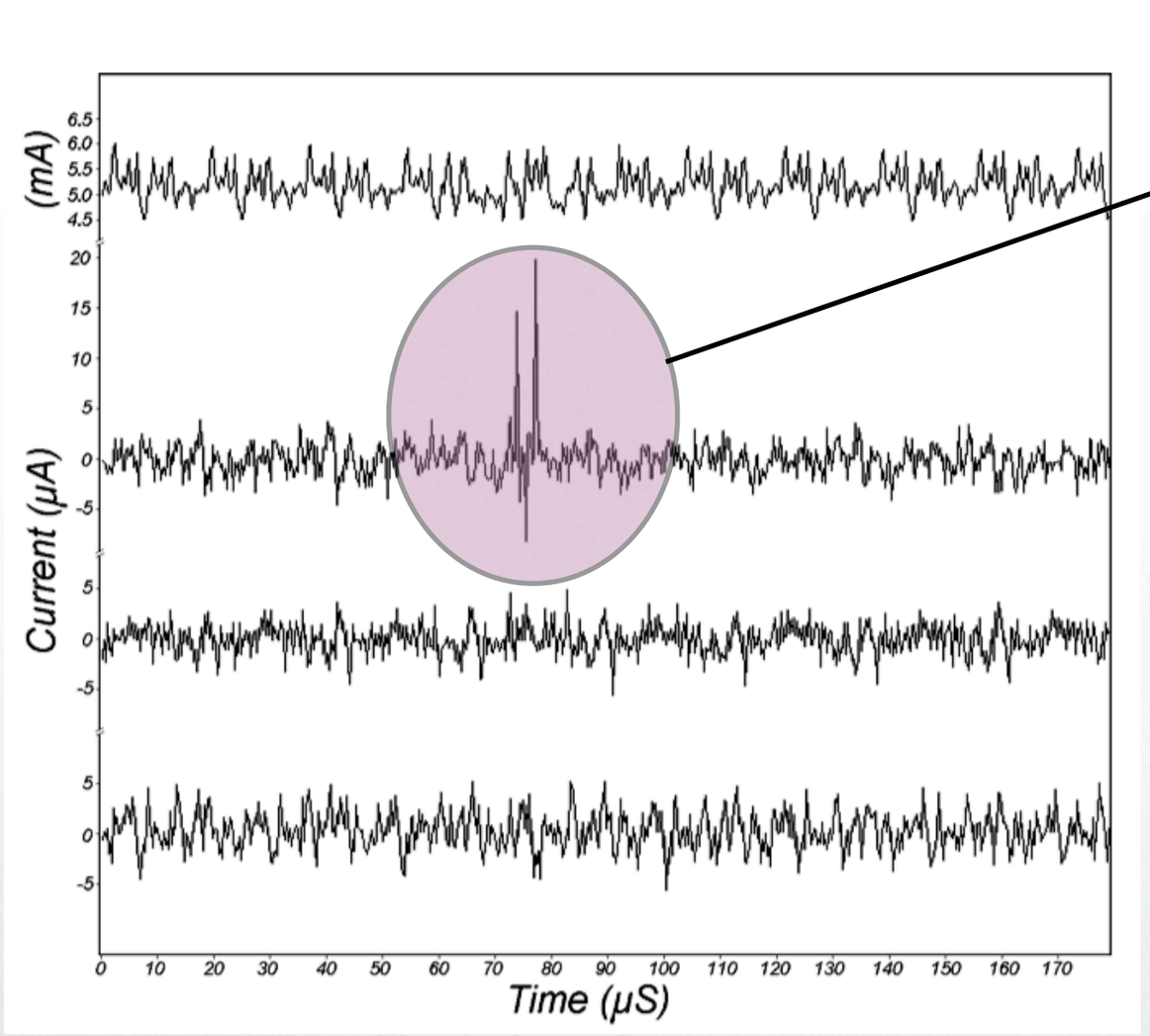
guess is correct => differential spikes

$$\frac{\sum_{\text{bit}=1} M_i^{(1)}}{\#\text{bit}=1} - \frac{\sum_{\text{bit}=0} M_i^{(0)}}{\#\text{bit}=0}$$

guess is incorrect => differential zeroes

$$\frac{\sum_{\text{bit}=1/\text{correct}} M_i^{(1)} + \sum_{\text{bit}=1/\text{false}} M_i^{(0)}}{\#\text{bit}=1} - \frac{\sum_{\text{bit}=0/\text{correct}} M_i^{(0)} + \sum_{\text{bit}=0/\text{false}} M_i^{(1)}}{\#\text{bit}=0}$$

DPA for DES

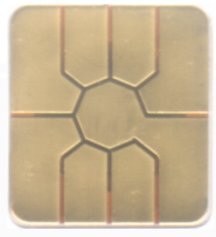


Correct Guess

Figure from P. Kocher, J. Jaffe, B. Jun, CRYPTO 99

Relevance of DPA attacks

- Need "hardware" access close to target.
- Vulnerable target : Smartcards



- integrated circuit in a card.
- power supplied by reader => opens the possibility for an attack by the reader.

Relevance of DPA attacks

- Trusted computing:
  - recall that a trusted computing system relies on the TPM for integrity security.
  - The TPM holds the keys internally but receives power from the "outside."

Protection

- Addition of power consumption noise at the hardware level.
- Addition of dispersed random instructions.

Capturing Video Signals

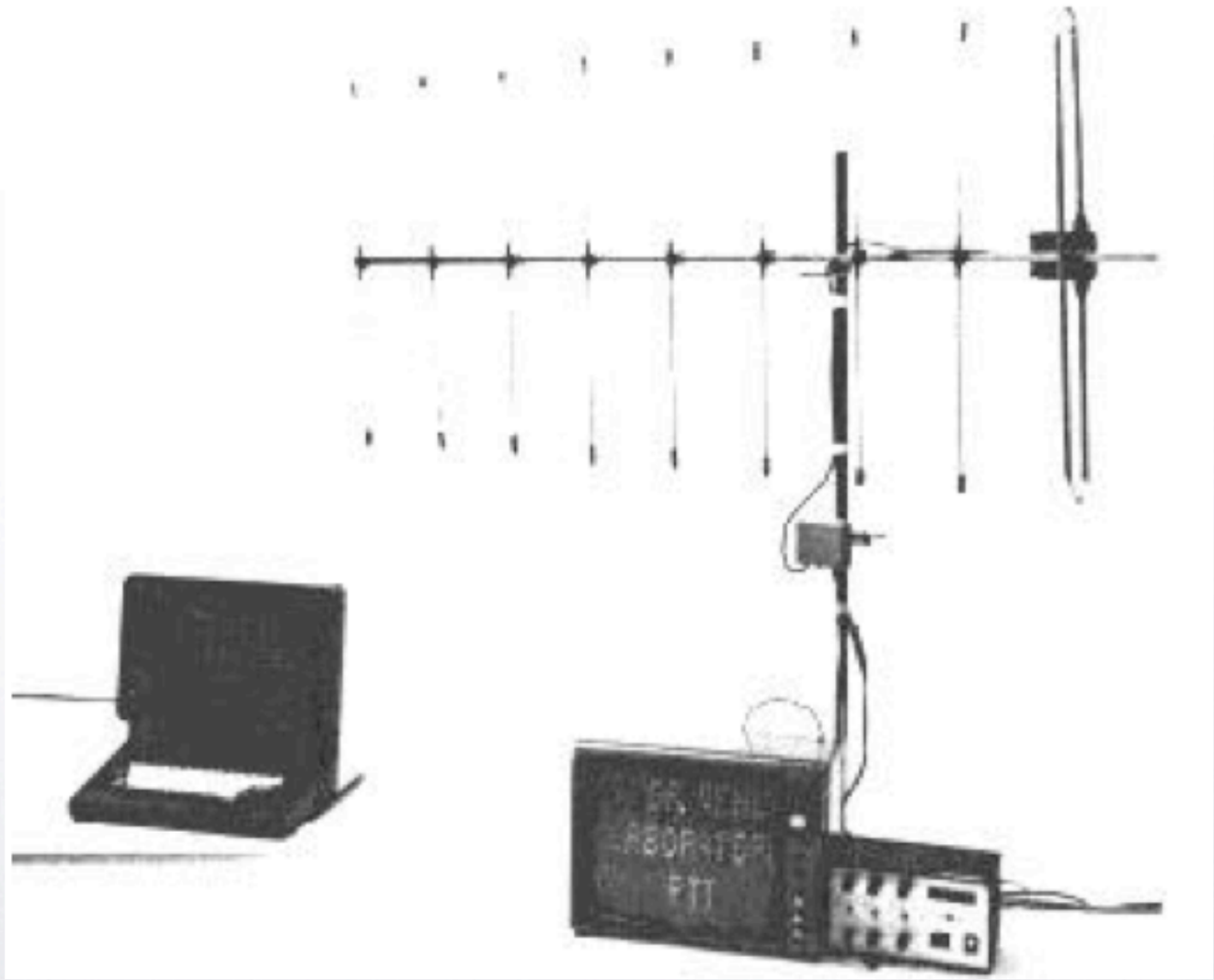
W. van Eck, 1985

"eavesdropping"
CRT Monitors

In cathode ray tube monitors the image is produced by the electron beam that bombards the screen with electrons.

This produces electromagnetic radiation in the RF range that may be captured.

possibility for 100 meters reception



TEMPEST

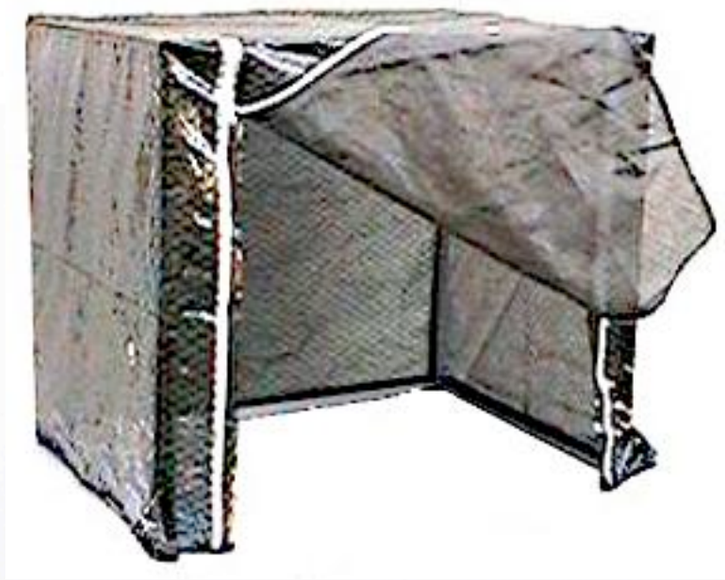
- Codename for US standard for limiting electric and electromagnetic radiation.
- used to be classified.
- involves metallic shielding of emanating equipment.

http://www.nsa.gov/ia/industry/tempest.cfm

Faraday Cages

M. Faraday 1836: the charge on a conductor will only reside on the outside

can be used for the effective isolation from external signals



picture from http://www.herzan.com/fc.html

Faraday Room

Entrance to a Faraday Room / Image from Wikipedia

Differential Fault Analysis

Shamir Biham Crypto 1997

- Assume asymmetry of bit flipping.
- Likely to switch from 1 to 0 but not the other way around.

Bits on EEPROM are stored as small charges on electrically isolated gates. Using radiation (UV light) the charges are more likely to leak out of the gates.

DFA

Given access to implementation of E_{K}(.)

- Repeat the following process:
  - supply m to obtain c.
  - After each trial apply physical stress and repeat till output stabilizes (K=0 at this stage).
  - Work backwards to recover the secret-key using an implementation of E_{.}

Other Side Channels

that were used for successful attacks

- Light
  - emitted from screens.
- Sound
  - produced by typing on keyboards.

