Extraction de clés secrètes enterrées : à qui la faute ?

Jean-Jacques Quisquater

Working with
Chong Hee Kim and F.-X. Standaert

UCL Crypto Group,
Université catholique de Louvain.

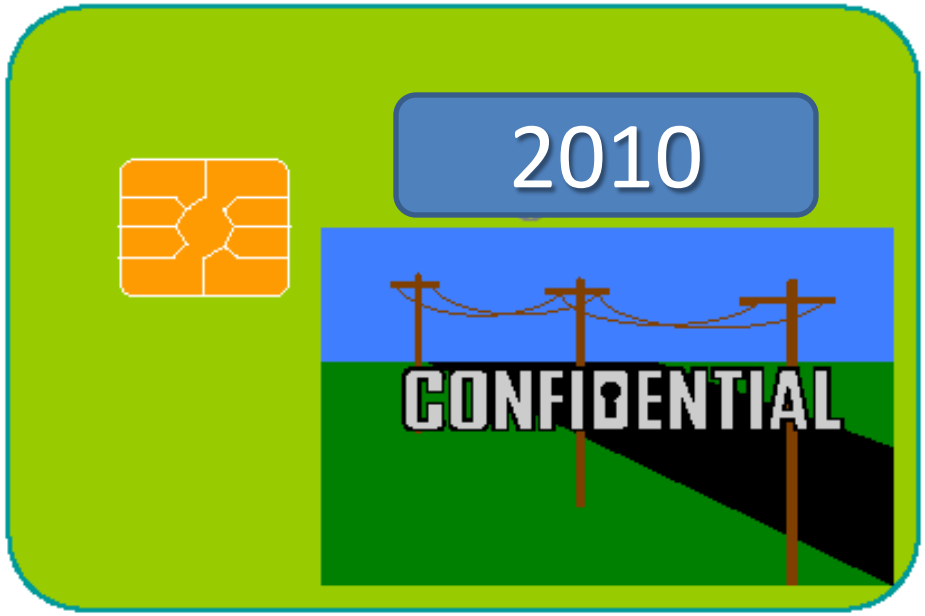
jjq@uclouvain.be
Paris, 31 mars 2010

Physical cryptography

- Introduction
- Hardware
- Random generation
- Quantum cryptography
- PUF (clone- resistance)
- New problems to be solved
- New countermeasures
- Interfaces, standards, complete security

My talk

- Describing magic tricks to recover secret keys
- Nothing really new
- Engineers are working about that for a long time …
- What is new (10 years): relation with cryptographic algorithms, hardware, use of statistics, new tools (scopes), models …


2010
CONFIDENTIAL

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

Magic Hat

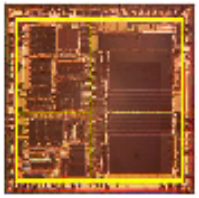
Cryptographic devices everywhere

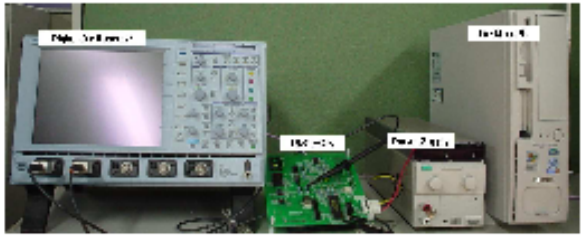


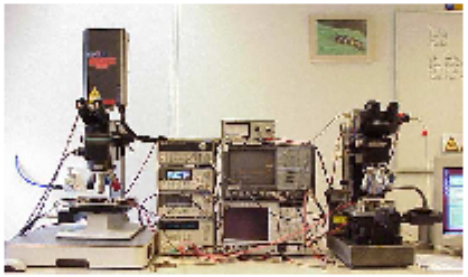


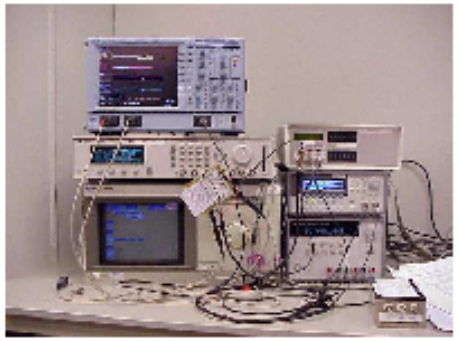


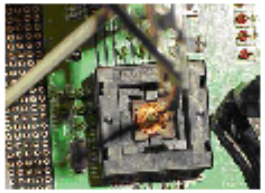

Physical attacks: cryptography *vs.* security



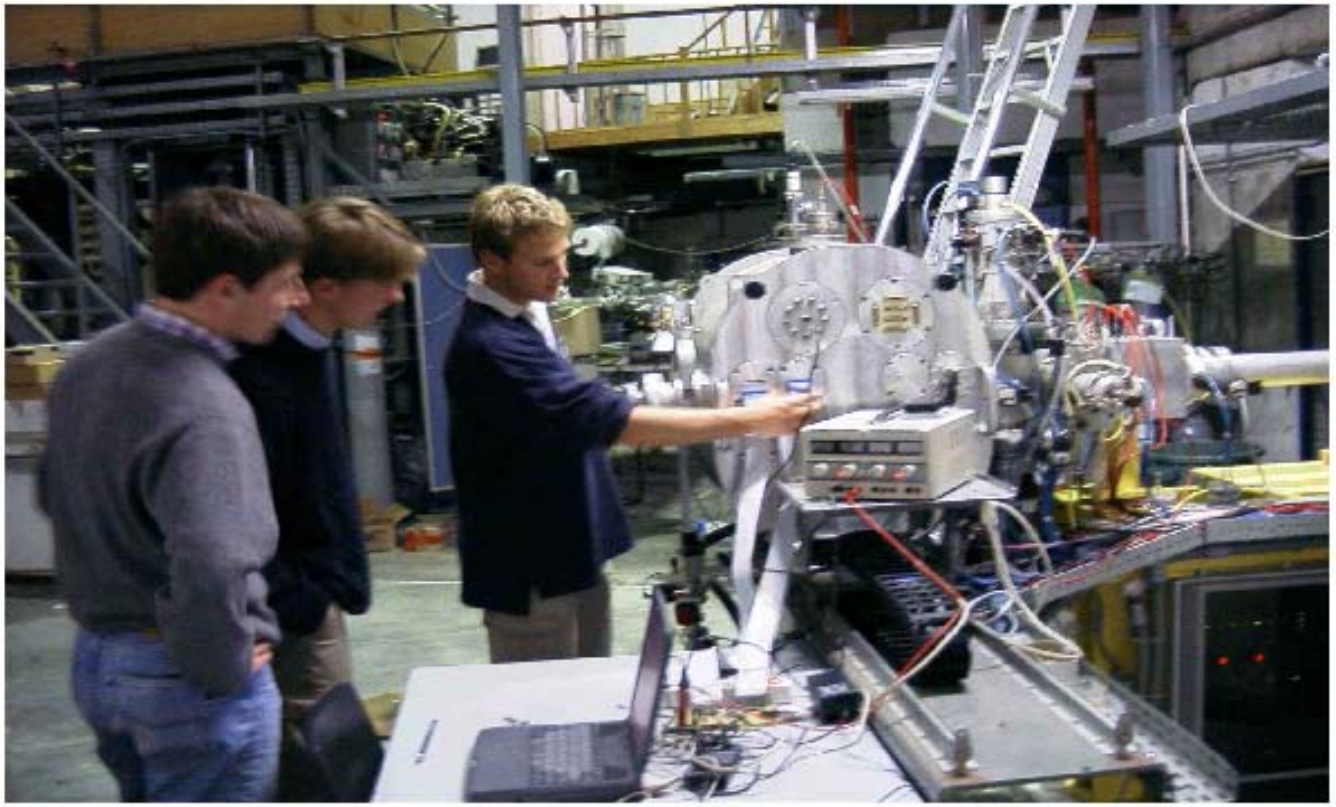




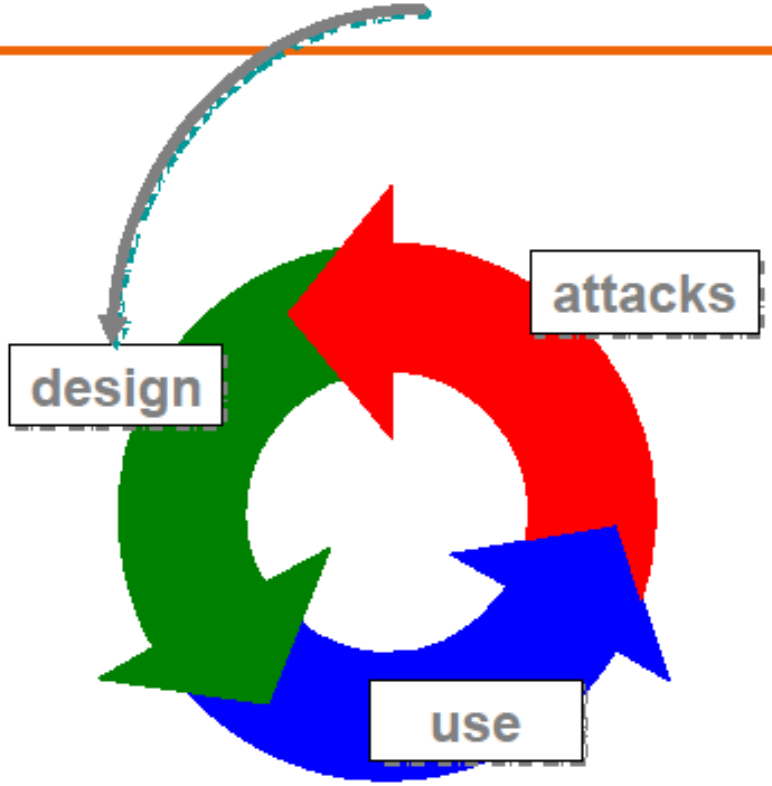


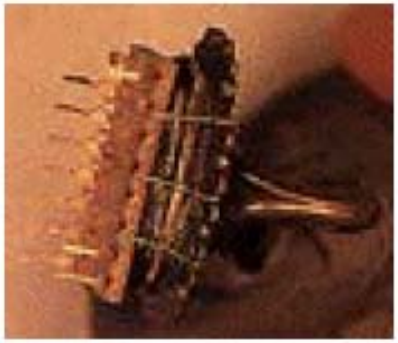


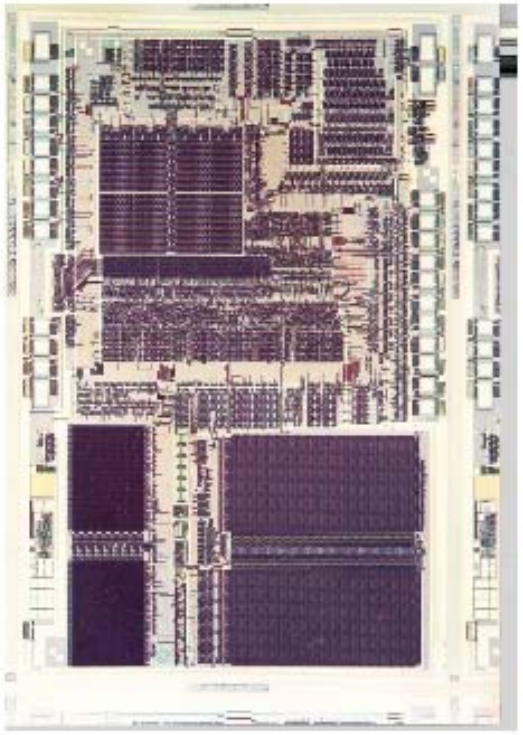
Security? Free slot at a cyclotron

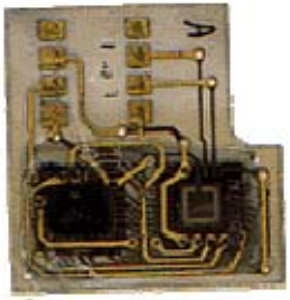


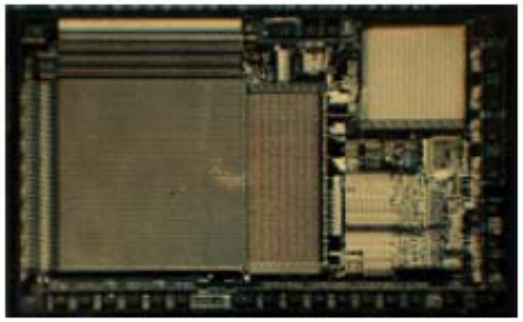
Hidden security or obscurity?

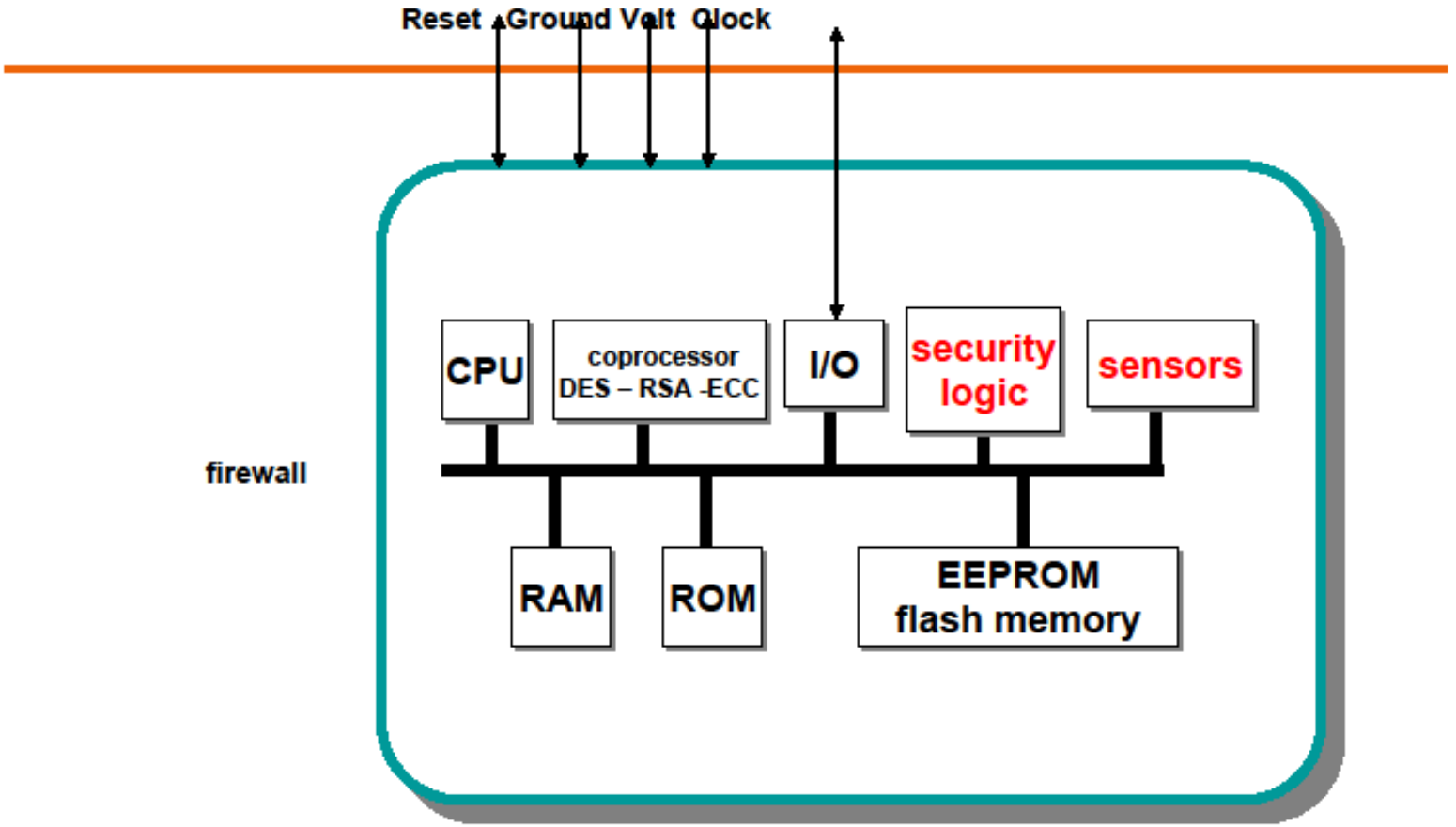











Reset
Ground
Volt
Clock
firewall
CPU
coprocessor
DES – RSA -ECC
I/O
security
logic
sensors
RAM
ROM
EEPROM
flash memory

Security design, logic and sensors 80-95 (I)

- voltage (low, high)
  - *to avoid side effects*
- frequency (low, high)
  - *RAM is mainly static*
- light (cell for detecting)
  - *to detect if somebody is removing the protective layers*
- resistivity (measure of)
  - *same reason*
- specific actions after reset
  - *init, increment EEPROM counter, ..*
- random values
  - *for blinding some effect*
- firewall (*Philips FAME-XA*)
  - *to avoid intrusive code (downloading, Java Card, ...)*

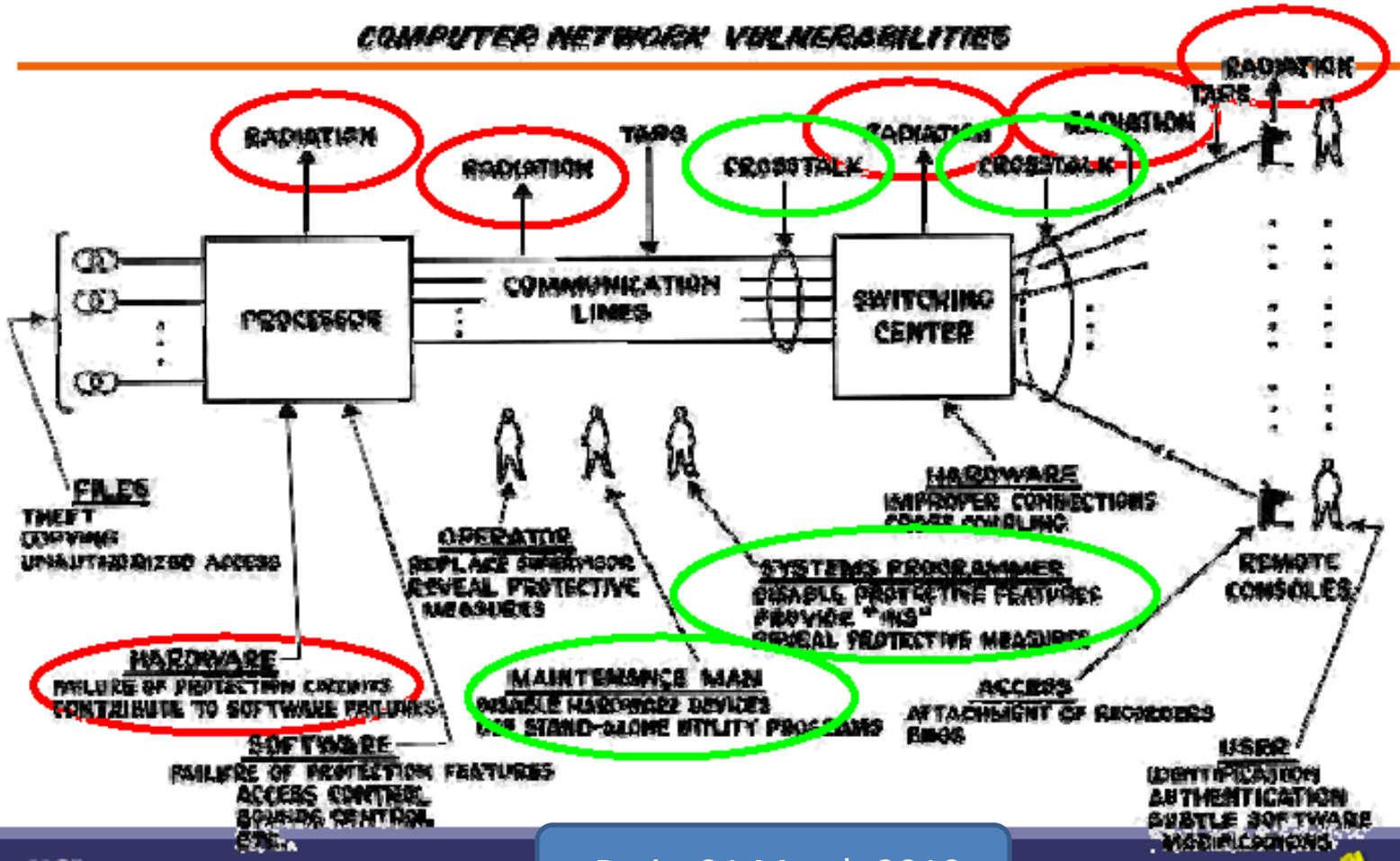
Security design, logic and sensors 80-95 (II)

- specific design rules (EEPROM, ...) and dummy gates and circuits
  - *to avoid reverse engineering*
- specific address decoders
  - *values logically adjacent are not physically adjacent*
- specific secret cells in memory (EEPROM)
  - *to detect manipulation (by radiation, ...)*
- embedded bus and ROM cells
  - *more resistant to probing*
- error-correcting codes for memory (hard and soft)
  - *same goal*
- ...
- *CLASSIFIED!*

But not enough research …

- And what about other old attacks
- Radiation?
- Faults?
- …

Baran: 1963


COMPUTER NETWORK VULNERABILITIES
RADIATION
RADIATION
TAPS
CROSSTALK
CROSSTALK
RADIATION
RADIATION
TAPS
PROCESSOR
COMMUNICATION LINES
SWITCHING CENTER
FILES
THEFT
UNAUTHORIZED ACCESS
OPERATING
REVEAL PROTECTIVE MEASURES
HARDWARE
IMPROPER CONNECTIONS
SYSTEMS PROGRAMMER
REVEAL PROTECTIVE MEASURES
REMOTE CONSOLES
HARDWARE
FAILURE OF PROTECTION CIRCUITS
CONTRIBUTE TO SOFTWARE FAILURES
MAINTENANCE MAN
ACCESS
ATTACHMENT OF RECORDERS
SOFTWARE
FAILURE OF PROTECTION FEATURES
ACCESS CONTROL
USER
IDENTIFICATION
AUTHENTICATION
SUBTLE SOFTWARE

Taxonomy of Attackers (from IBM)

- Class I – Clever outsiders - Insufficient knowledge of system, not highly sophisticated equipment, look for existing weaknesses.
- Class II – Knowledgeable Insiders - Have potential access to most parts of systems, and highly sophisticated tools.
- Class III – Funded Organizations – Governments, terrorists, Mafia have teams of experts, big budgets, most advanced tools.

Old timing attacks

- Vernam
- PIN code (remotely)
- Somebody (1986) wanted to set a challenge: distribution of a lot of smart cards during a large event (3 days): finding a PIN code of 4 digits
- I explained the problem but …
- Setup of a remote attack between Brussels and Rennes …

Old SPA

- End ‘80, beg ’90 several labs did but there were strong pressures to not publish it …

Old fault attacks

- Well known in the context of nuclear and space applications

Your electronic wallet in the Van Allen radiation belt,

- **Radiation and crypto (comp.risks)**
- *Jean-Jacques Quisquater <jjq@dice.ucl.ac.be> Mon, 02 Dec 96 09:23:18 GMT*
- November 30, 1996 From end September until now many announcements were issued about the so-called Bellcore attack against tamper-resistant chips (example: smartcard or chipcard for electronic commerce). The attack is based on the (theoretical) possibility of flipping some bits (at some random position) of the secret key, stored in RAM or E2PROM, before or during the computations done by the chip. Another attack is to induce some decoding error during the execution of one instruction (Anderson and Kuhn). One crucial question is the effectiveness of such attacks by malicious hackers. In fact, this problem was very well studied in the contexts of nuclear physics and of space applications (what about the behavior of semiconductors in such hard environments?). In that area, there is the concept of SEE (Single Event Effect) and it is what we are trying to study! A SEE is an event induced by radiation, temperature, microwave, ..., having some effect one time on a device. There are many studies about that. What we need to know are the SEEs --- relatively well focused (one or few bits are flipped), --- and/or at a given moment, --- and/or for a very short time.

References

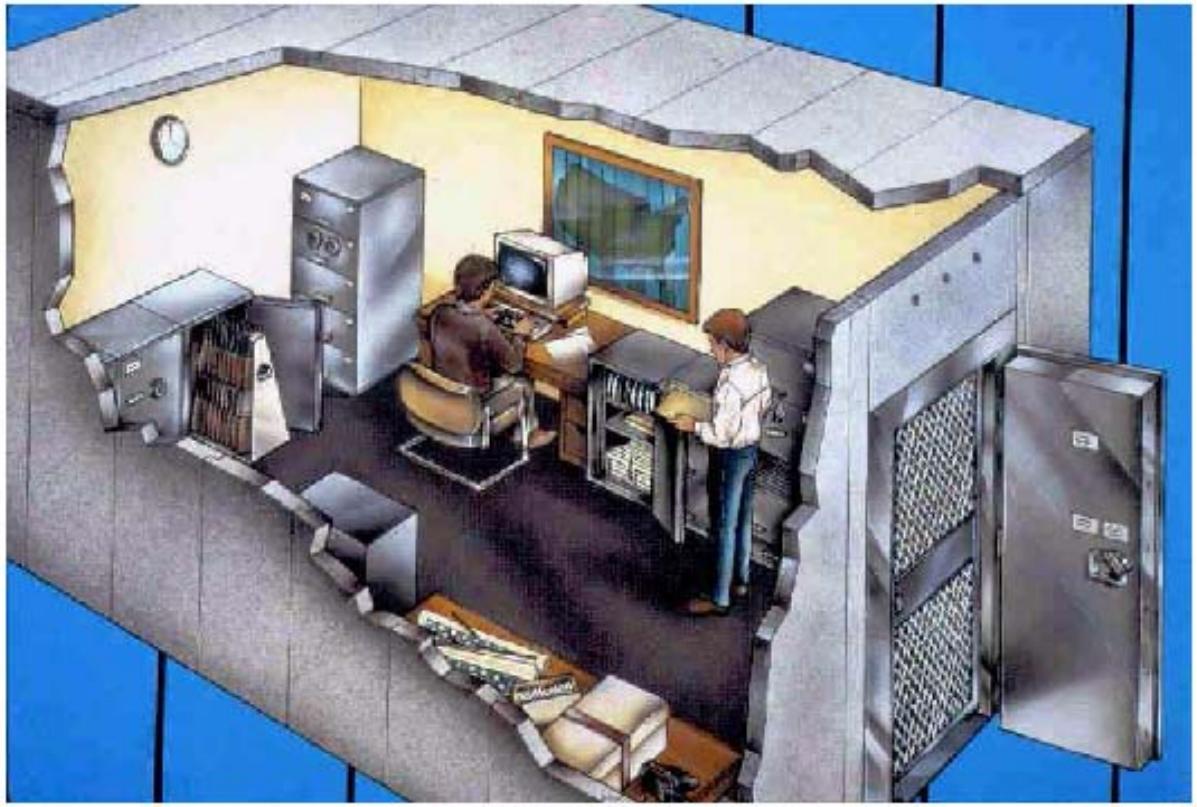
- The NASA ASIC guide, published by JPL and NASA, Chapter 4, Design for radiation tolerance, 1993.
- - Hardening integrated circuits against radiation effects, J.-P. Colinge and P. Francis, November 1996, Notes (66 pp.), Microelectronics Lab, UCL, Louvain-la-Neuve, Belgium.
- - Single-Event-Effect mitigation from a system perspective, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 654-660.
- Laboratory tests for Single-Event Effects, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 678-686.
- Microbeam studies of Single-Event Effects, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 687-695.
- Soft errors susceptibility ands immune structures in dynamic random access memories (DRAM's) investigated by nuclear microprobes, IEEE Trans. on Nuclear Science, vol. 43, April 1996, pp. 696-704.
- 32-bit processing unit for embedded space flight applications, IEEE Trans. on nuclear science, vol. 43, June 1996, pp. 873-878.
- - Single Event Effect testing of the Intel 80386 family and the 80486 microprocessor, IEEE Trans. on Nuclear Science, vol. 43, June 1996, pp. 879-885.
- - Analysis of local and global transient effects in a CMOS SRAM, IEEE Trans. on Nuclear Science, vol. 43, June 1996, pp. 899-906.

Old EMA (« tempest »)

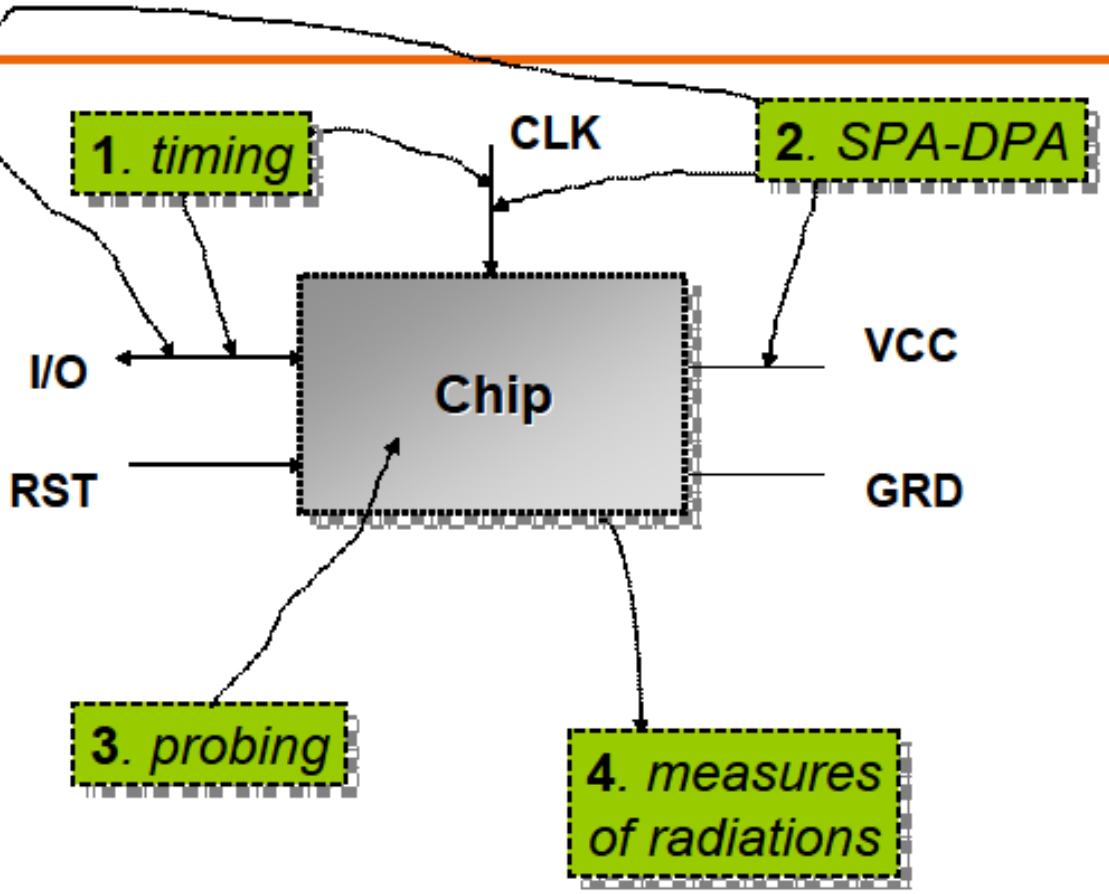
- Other experiments
- Wifi spectrum

Early EMA

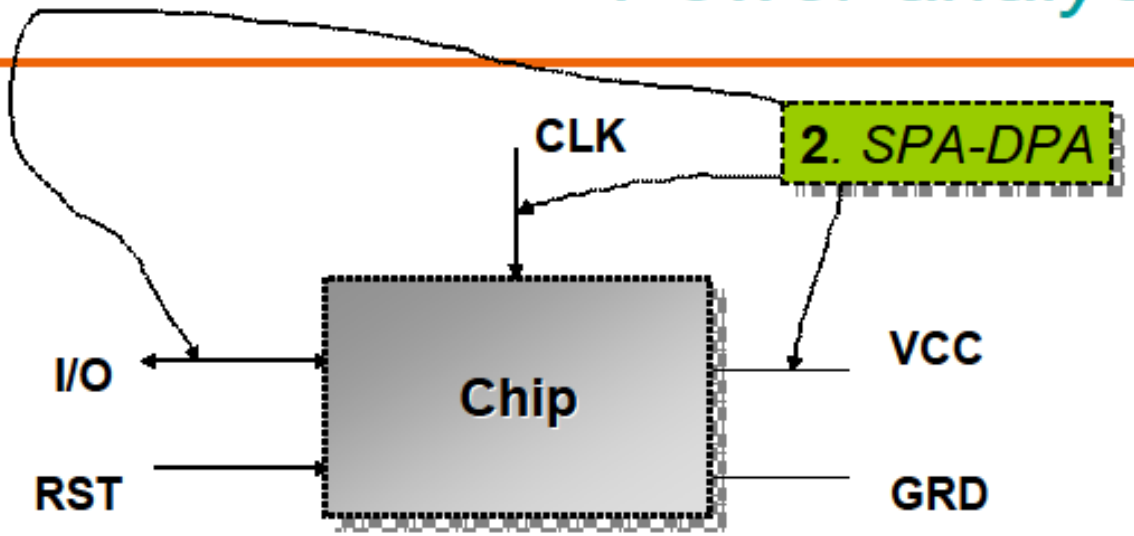
- **Late-1800s** Crosstalk is frequent problem in infantile telephone system.
- **1914-1915** Field telephone crosstalk in World War I exploited and jamming attempted, leading to lower signal British Fuller phone.
- **1918** Herbert Yardley and the Black Chamber discover radio transmitter emanations: *Yardley and his people found that various electronic devices used to handle classified information emanated information, and that these emanations could be exploited to reconstruct the classified materials.*
- **1940s** Receivers shielded for local oscillator radiation to prevent becoming beacons for enemy submarines in World War II.



Generic model of card for passive attacks



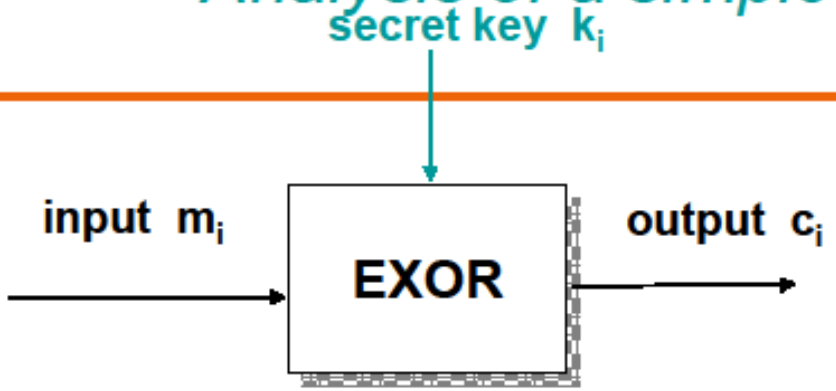
Power analysis



- ***SPA*** (simple power analysis): reverse engineering of the cryptographic algorithms and the secret used data (keys):

- ***DPA*** (differential power analysis): elimination of the "noise": this attack is not really related to the algorithm or its implementation but it is more intrinsic

Analysis of a simple model (Vernam)



mi	ki	ci
0	0	0
0	1	1
1	0	1
1	1	0

mi	ki	ci
0	0	***0***
0	1	1
1	0	1
1	1	0

if for some reason the two zeroes are not the same (SPA ...)
this perfect system is completely broken.

Classification

1. According to the type of attack:

	Active	*vs.*	**Passive**
Ex:	fault insertion		timing attack
	Invasive	*vs.*	**Non invasive**
Ex:	probing	… EMA …	power analysis

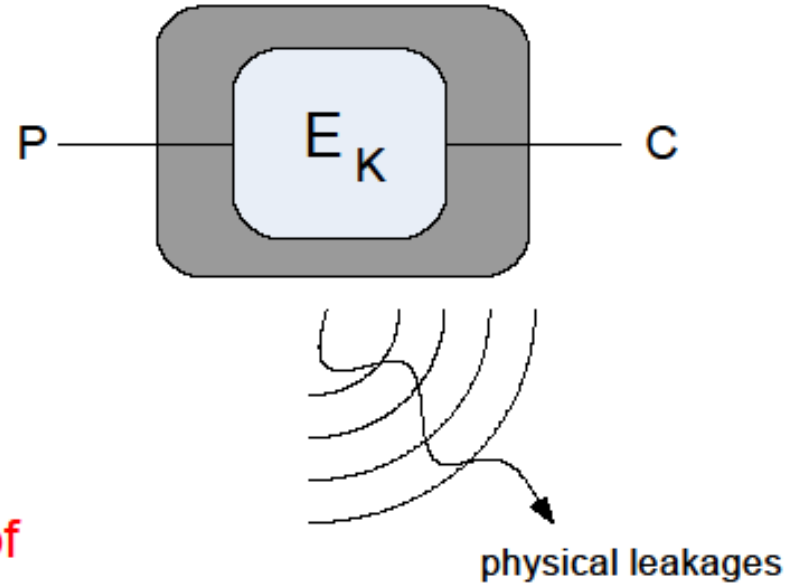
Side-channel attacks

2. According to the strength of the adversary:
   common criteria, FIPS 140-2, IBM taxonomy, …

General context

Black box cryptanalysis…

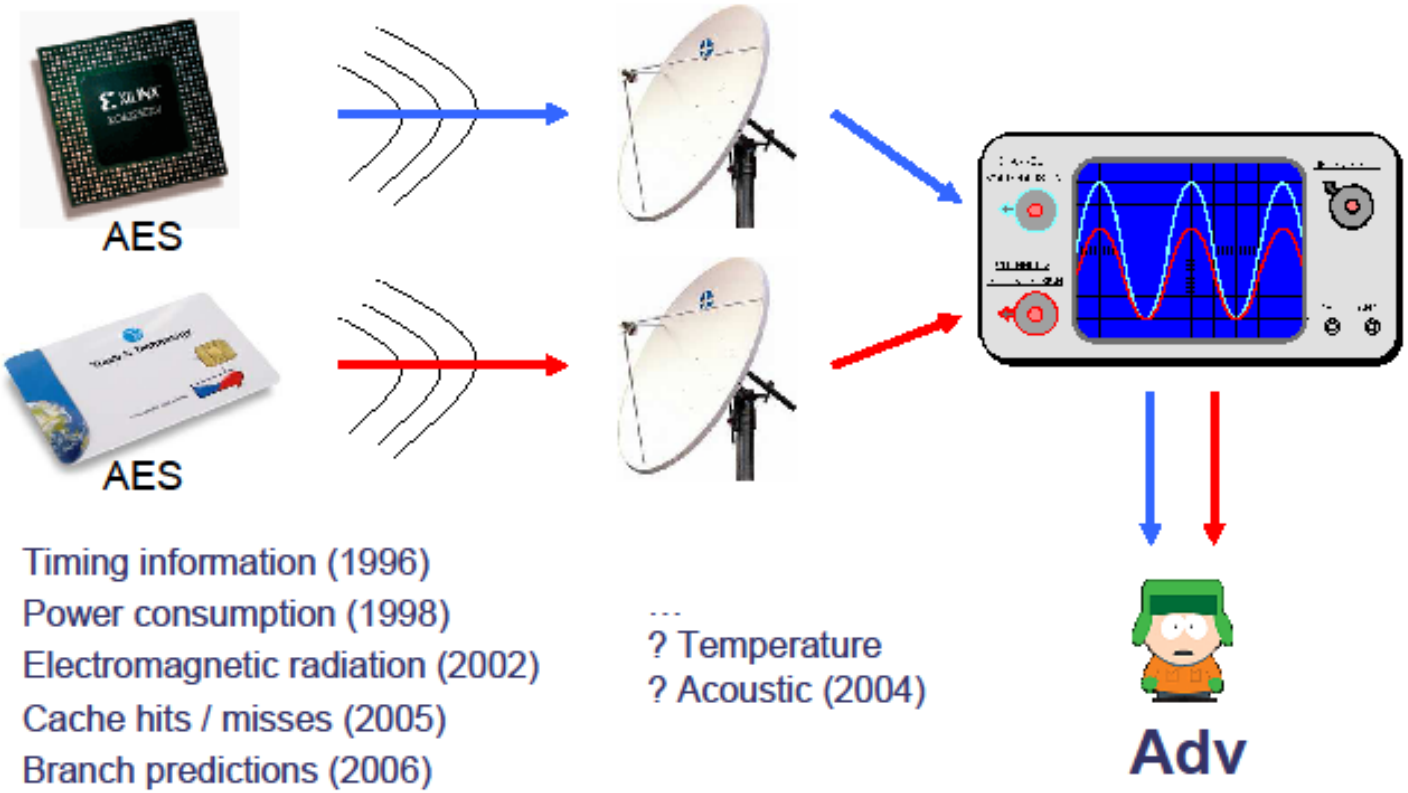
only uses the primitive's inputs and outputs, *e.g*, the plaintexts, ciphertexts for block ciphers



Side-channel attacks…

additionally takes advantage of physical leakages, *e.g.* power consumption, timing information, electromagnetic radiation

Side-channel attacks



- Timing information (1996)
- Power consumption (1998)
- Electromagnetic radiation (2002)
- Cache hits / misses (2005)
- Branch predictions (2006)

…
? Temperature
? Acoustic (2004)

An old story from 1956 ("Spycatchers", by Peter Wright):

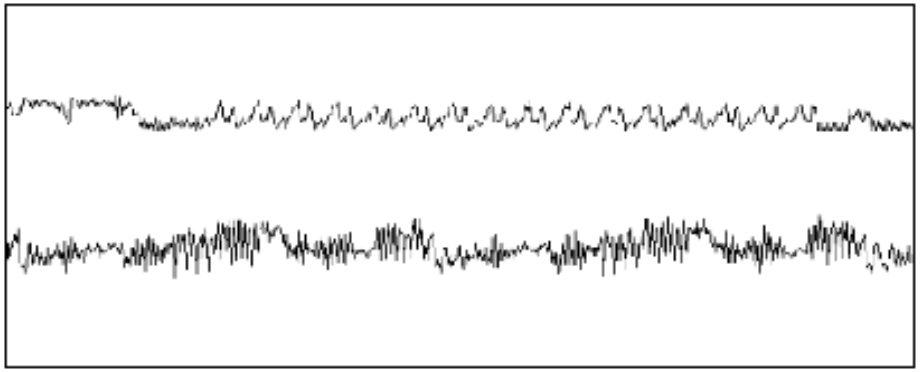
- British intelligence wanted to read Egyptian diplomatic traffic encrypted by Hagelin machine from their embassy in London to the foreign office in Cairo
- The secret key was set each morning by moving the rotors to a new initial setting.
- The British MI5 made sure that a nearby basement telephone was always connected
- All they had to do each morning was to count the number of clicks heard over the phone during the key setup on the adjacent Hagelin machine.

Acoustic triangulation attack (Fiona, 2006)

- http://personal.ie.cuhk.edu.hk/~kwwei/FYP/keyboard_acoustic_attack/Fiona--ERG4920CM.pdf
- Use 2 microphons …
- And triangulation
- Not only based on the sound of the keyboard but on the position

Simple Power Analysis

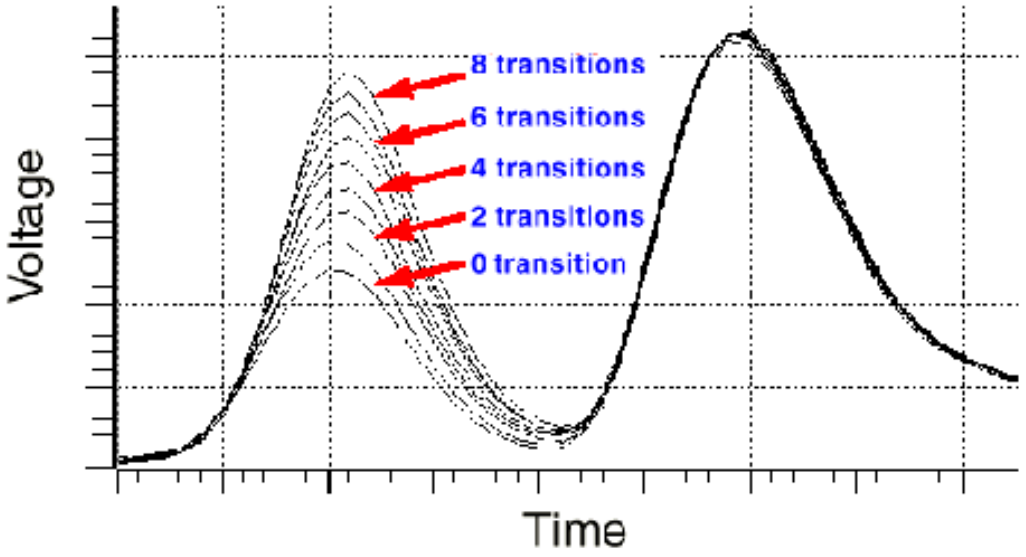
- Operation-dependent leakage variations:



e.g. DES: initial permutation, 16 rounds, final permutation

Differential Power Analysis

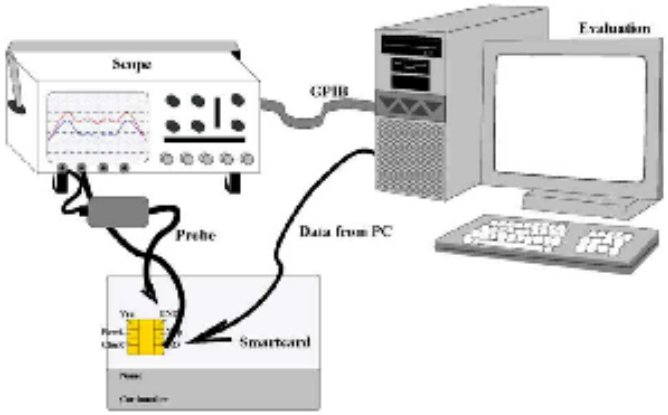
- Data-dependent leakage variations



e.g. CMOS => Power consumptions dependent on the number of bit switches

Measurements setups

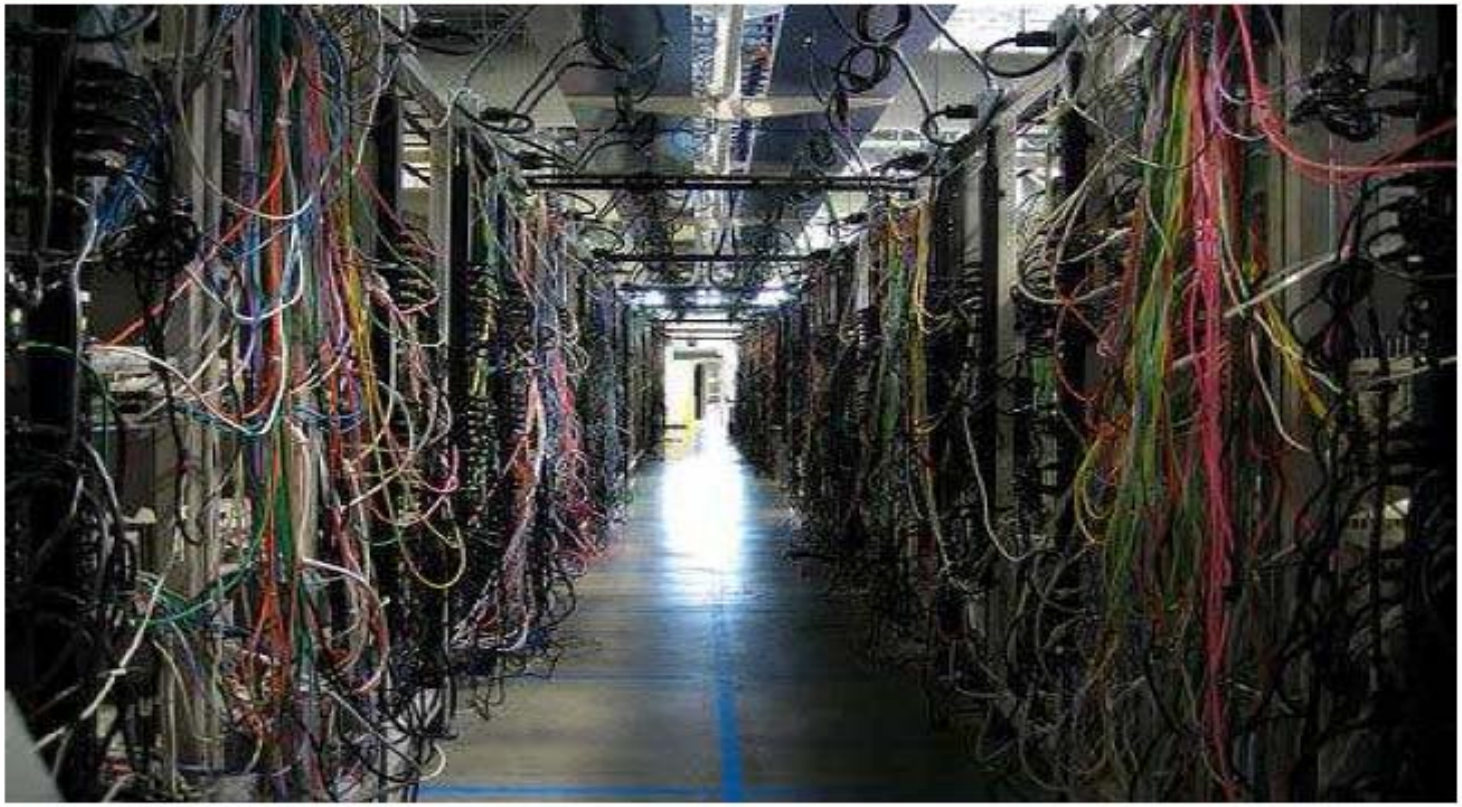
- Target cryptographic device: smart cards, FPGAs, …
- Measurement circuit: small resistor inserted between ground pin and actual ground, small antenna, …
- Acquisition device: 1 Gsample/sec oscilloscope



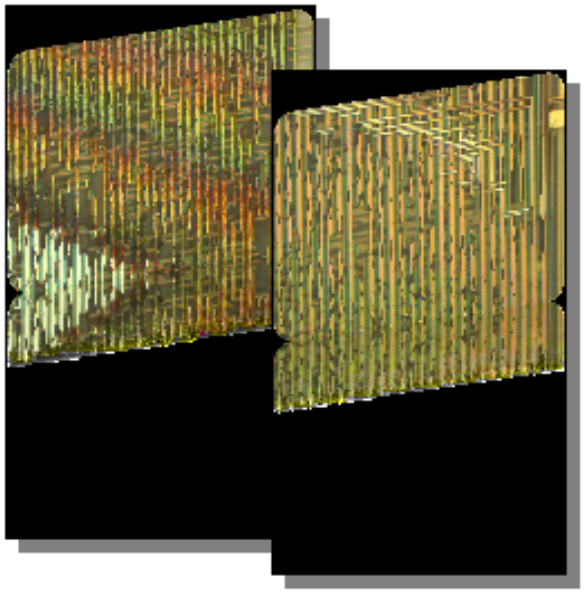
New countermeasures

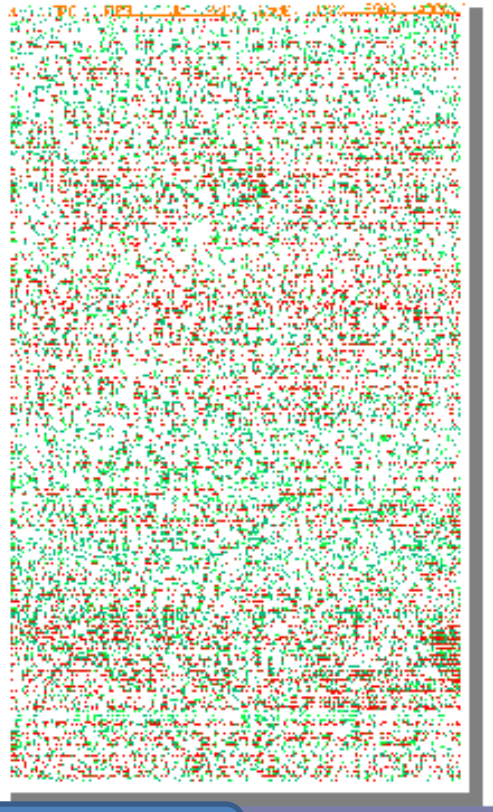
- New rules for design
- Spaghetti circuits

Spaghetti for digital circuits …



Spaghetti circuits





Side-channel attacks (SCA)

- Powerful but specific (usually target a particular implementation rather than an abstract algorithm)
- Still generic (most devices can be targeted)

- Hard to evaluate
- Hard to prevent

- Only a part of the physical reality (faults, probing, …)
  - Resisting one attack may induce weaknesses with respect to another one…

SCA & Fault attacks

- *Side channel Analysis* by Kocher, 1996
- Many variants
  - Using timing, power consumption, EM, etc
- *Fault attacks* by Boneh et al., 1997

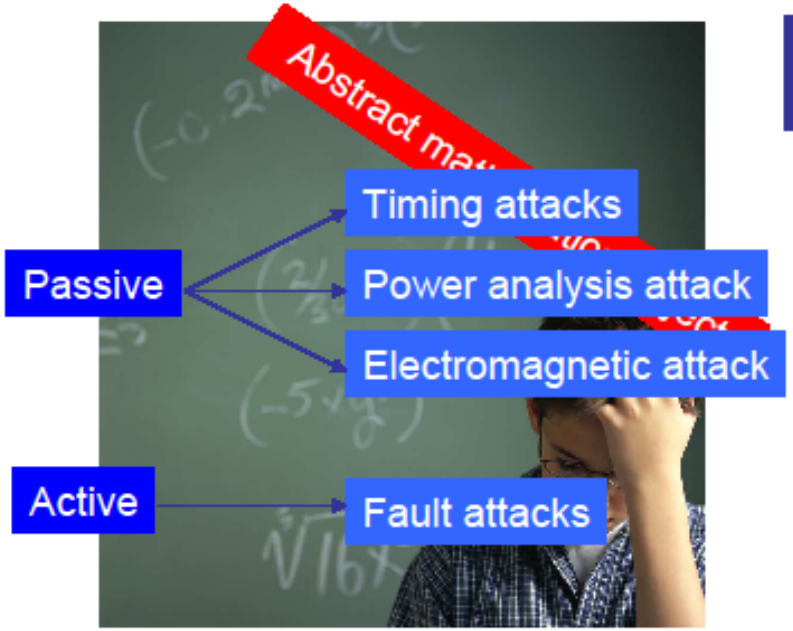
Side channel Analysis	Fault attacks
Passive	Semi-invasive
Measure timing, power consumption, EM radiation,...	Invoke faults and use the faulty outputs

Improved attacks

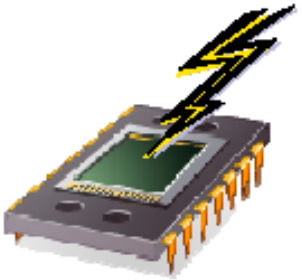
- Use of several leakages samples
  - Multivariate statistics
- Profiling and characterization of the device
  - Or assume knowledge of critical information
- Signal processing of the leakage traces
  - Filtering, averaging, …
- Various statistical tests
  - Difference of mean test
  - Correlation
  - Bayesian

Fault attack

- Cryptanalysis?



In practice, algorithms have to be implemented on real physical devices



Improved attacks

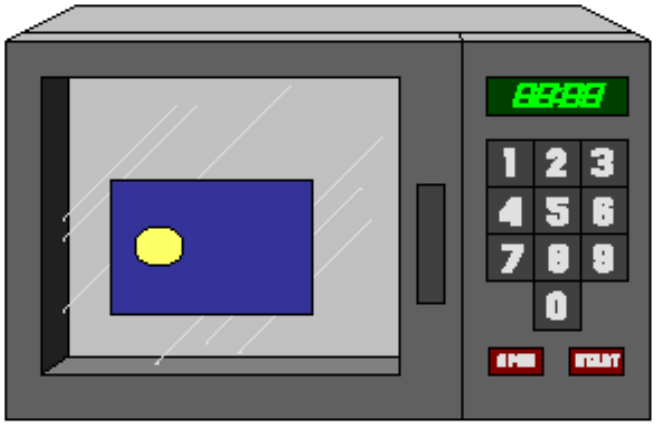
- Use of several leakages samples
  - Multivariate statistics
- Profiling and characterization of the device
  - Or assume knowledge of critical information
- Signal processing of the leakage traces
  - Filtering, averaging, …
- Various statistical tests
  - Difference of mean test
  - Correlation
  - Bayesian

Fault attack

- Method of fault injection
  - Glitch on the supply voltage or external clock
  - White light, laser
  - Electromagnetic wave, X-ray, ion beams
  - Temperature variation

- To be successful,
  - Generate the *right* fault at the right time and place
  - The generated fault must be exploitable
  - Depend on th

Magic Hat




ENIGMA

Bellcore attack (1996)

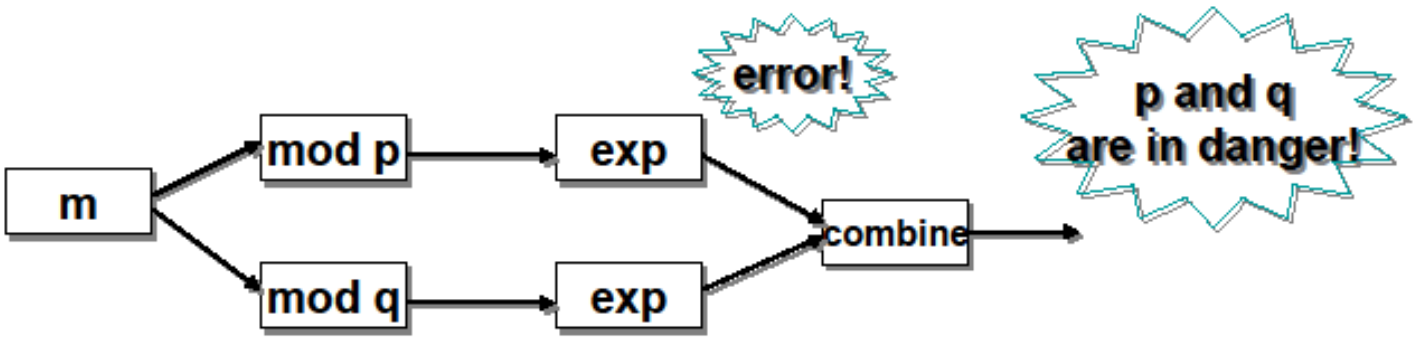
- Boneh, de Millo, Lipton: 2 signatures, one fault, break a RSA key, knowing the public key
- Lenstra: 1 signature, breaks a RSA key, knowing the public key
- Joye, Lenstra, Q.: 2 signatures, break a RSA key, NOT knowing the public key …

Implementation problems (Joye, Lenstra, Q.)

- optimisation: minimisation of the number of multiplications and square

- Error or attack? Bug Pentium … (Shamir)

- Chinese Remainder Theorem



RSA-CRT

- RSA-CRT (Chinese Remainder Theorem)
  - $N=p \cdot q$: RSA modulus, p and q: large primes
  - $e \cdot d = 1 \bmod (p-1)(q-1)$
  - $d_p = d \bmod (p-1)$ and $d_q = d \bmod (q-1)$
  - I_q: inverse of q modulo p
  - Signature S of a message m
    1. $S_p = m^{dp} \bmod p$
       $S_q = m^{dq} \bmod q$
    2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Fault attack on RSA-CRT

- Signature S of message m
  1. $S_p = m^{dp} \bmod p$

     $S_q = m^{dq} \bmod q$
  2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Fault attack on RSA-CRT

- Signature S of message m
  1. $\underline{S_p} = m^{dp} \bmod p$ ⟵ Fault attack
     $S_q = m^{dq} \bmod q$
  2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Fault attack on RSA-CRT

- Signature S of message m
  1. $S_p = m^{dp} \bmod p$

     $S_q = m^{dq} \bmod q$
  2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Fault attack on RSA-CRT

- Signature S of message m
  1. $S_p = m^{dp} \bmod p$

     $\underline{S_q} = m^{dq} \bmod q$ ⟵ Fault attack
  2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Fault attack on RSA-CRT

- Signature S of message m
  1. $S_p = m^{dp} \bmod p$

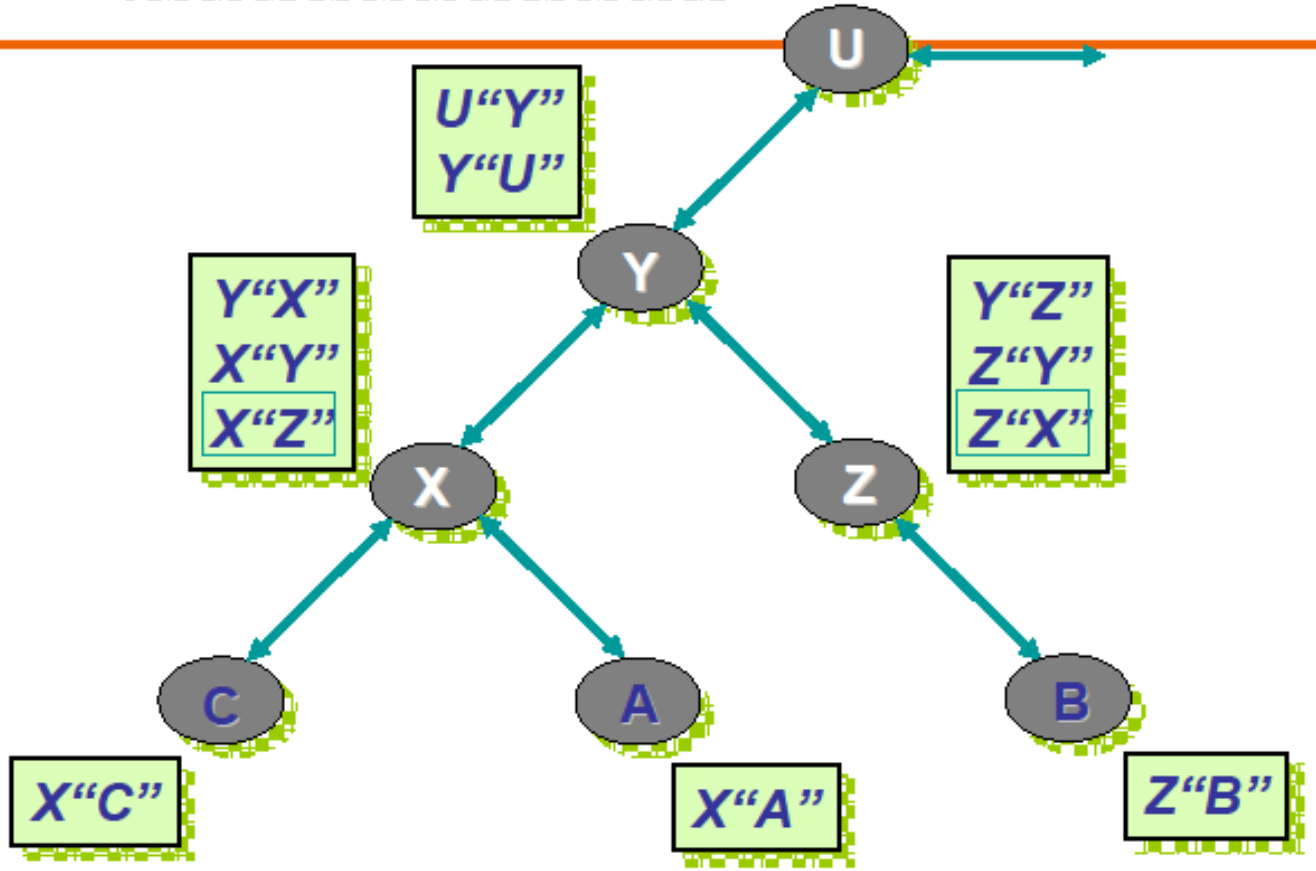
     $S_q = m^{dq} \bmod q$
  2. $S = \mathrm{CRT}(S_p, S_q) = S_q + q \cdot \{(S_p - S_q) \cdot I_q \bmod p\}$

Be careful about your PKI

- With added problems thanks to hash functions

certification path A to B:
X"Z" - Z"B"

certificate (X.509)



OK CRT-RSA but secret keys?

Fault attack

	Model	Location	# of faulty results
DES	Byte	Anywhere among last 6 rounds	2
AES: State	Byte	Anywhere between MixCol of 7th and 8th	2
AES: Key Schedule	Byte	9th round key scheduling	~~7~~ → 4
RSA-CRT	Size of modulus	Anywhere during one of CRT components	1
RSA-SFM	Bit	Anywhere among 128 bytes	1024
DSA	Bit	Anywhere among 20 bytes	160
ECDSA	Bit	Anywhere among 20 bytes	160

Differential Fault Attack on AES

- DFA on AES State
  - G. Piret and J.-J. Q's attack in 2003
    - 2 faulty ciphertexts
- DFA on AES Key Schedule
  - Giraud, 2003
  - Chen & Yen, 2003
  - Peacham & Thomas, 2006
  - Takahashi et al., 2007

Proposed DFA on AES Key Schedule

- Our fault model
- Basic attack
  - Retrieve 32 bits with 2 pairs
- Improved attack
  - Retrieve 96 bits with 2 pairs
  - Retrieve 128 bits with 4 pairs

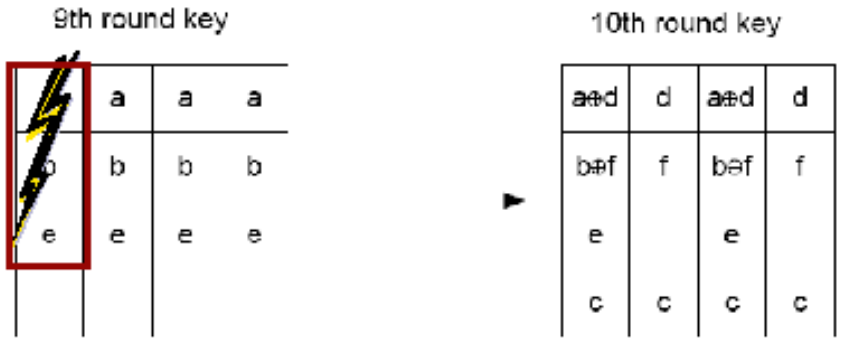
Fault Model

- We assume
  - Random fault is injected in 9th round AES Key Scheduling process
  - Some bytes of the first column of 9th round key are corrupted

Basic Attack

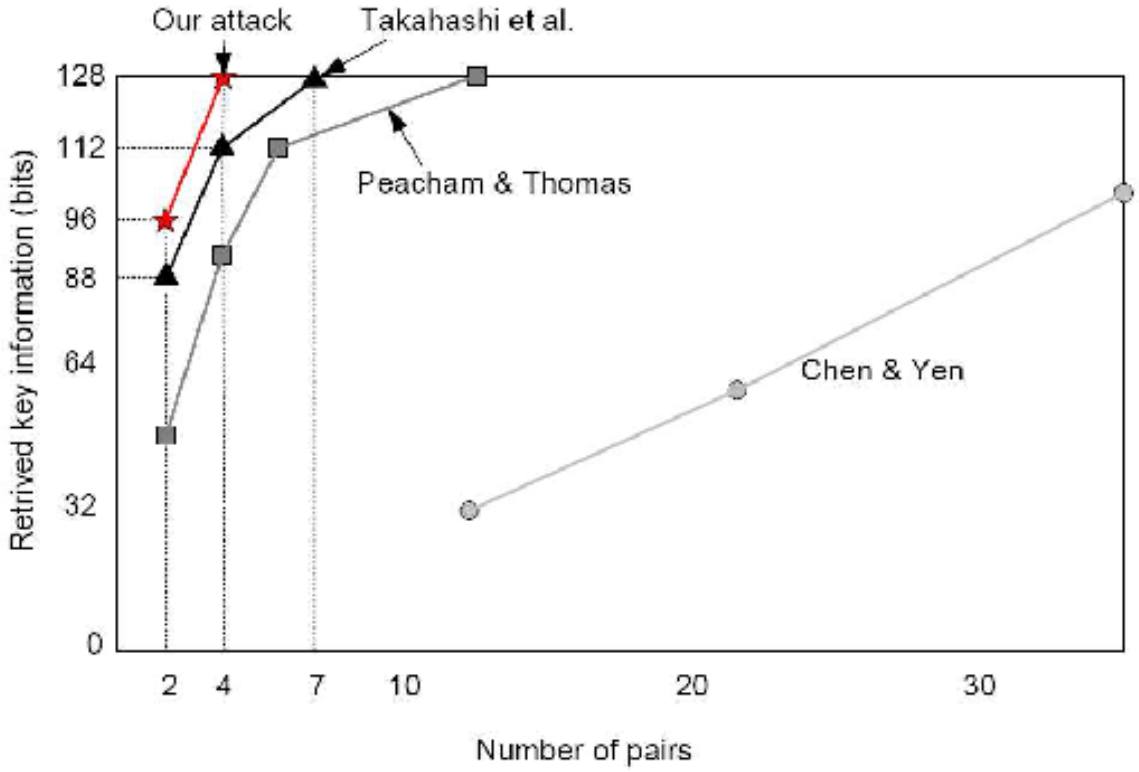
- Finally we have
  - One correct key for $(K^{10}_{0,0}, K^{10}_{0,1}, K^{10}_{0,2}, K^{10}_{0,3})$
  - Faulty values (a_1, a_2)
  - Simulation results
    - Less than 0.5 second on 3.2GHz Pentium 4 PC
- With 8 pairs
  - We can find 128 bits

Improved Attack

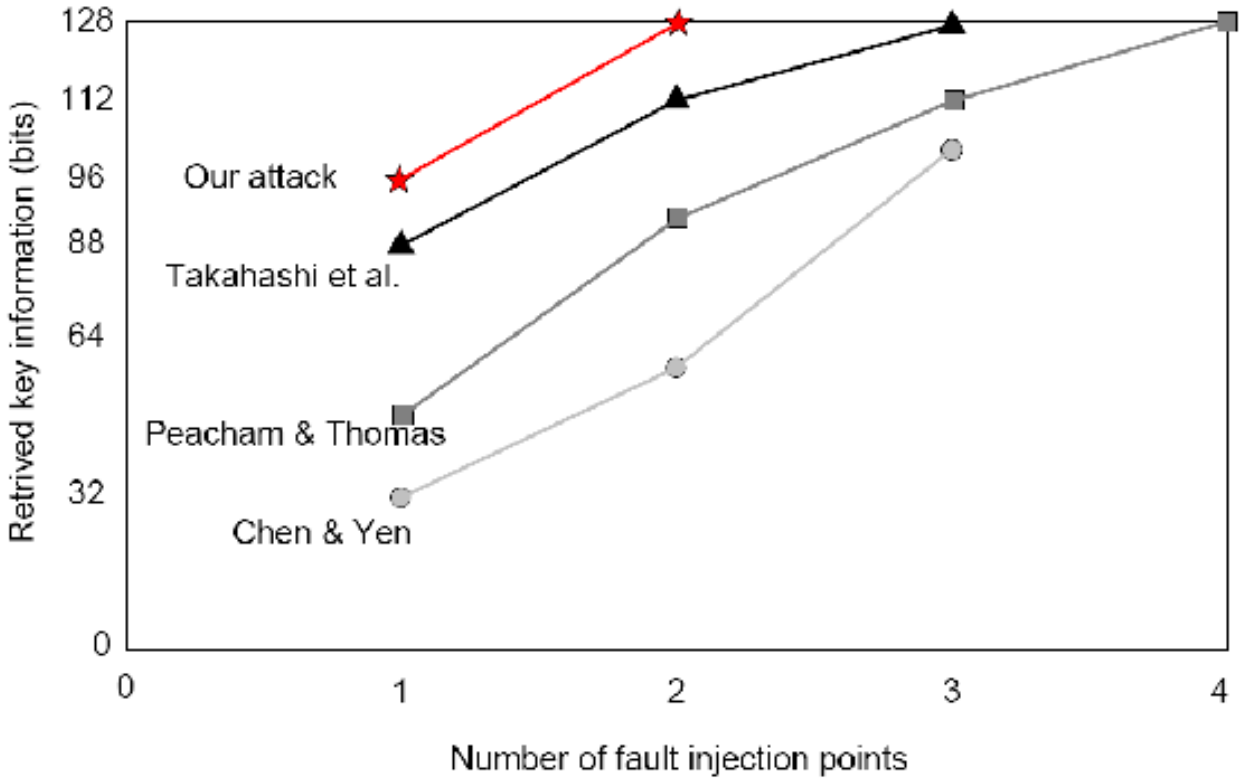


- We can find 96 bits with 2 pairs
- Last 32 bits
  - Another faults on $K^9_{3,0}$ with 2 pairs
- Total 4 pairs for 128 bits
  - 2.3 seconds by simulation

Comparison with previous attacks



Comparison with previous attacks



For AES

- DFA on AES State
  - 2 pairs by Piret & Q.
- DFA on AES Key schedule
  - Still many pairs until now
- We proposed a new DFA on AES Key Schedule
  - 2 pairs for 96 bits with exhaustive key search of 2^{32}
  - 4 pairs for 128 bits
- AES Key schedule should be protected against FA properly also.
- Submitted.

Magic Hat

Questions?

Magic Hat

Thanks for your attention

Questions?

Magic Hat

Thanks for your attention

Questions?

CHES 2010