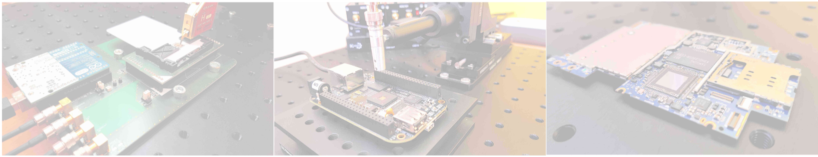
Introduction to Hardware Security

Victor LOMNE

NinjaLab

Master Informatique, University of Montpellier

Thursday January 31st 2019, Montpellier, France



Outline

Agenda

Context

- Since the 90's, increasing use of secure embedded devices
  - 9G smartcard ICs sold in 2016 (SIM cards, credit cards . . .)



- Strong cryptography from a mathematical point of view used to manage sensitive data
  - AES, RSA, ECC, SHA-2-3 . . .

Secure Embedded devices

- Functionalities :
  - secure boot
  - secure storage & execution of code
    in confidentiality & integrity
  - secure storage of sensitive data
    in confidentiality & integrity
  - secure implementation of crypto operations
- Small set of commands ⇒ reduce the Attack Surface

Examples of Secure Embedded Devices

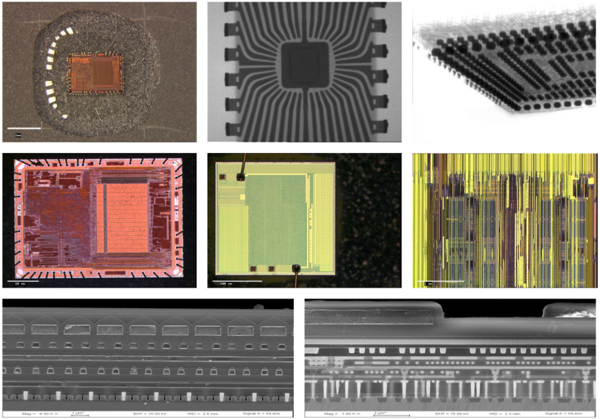
- Smartcard (credit cards, USIM, e-passports ...)
- Trusted Platform Module (TPM)
- Set-Top Box
- Hard disk drive with HW encryption
- Smartphone secure element
- Smartphone secure enclave
  security co-processor inside Application Processor
- Internet of Things ?
- ...

Adversary Model

- In this talk, we consider the following hypotheses :
  - The adversary can steal the device and get full control of it
  - The device has few communication interfaces
  - Each communication interface exposes few commands
  - There is no software vulnerability due to previous points

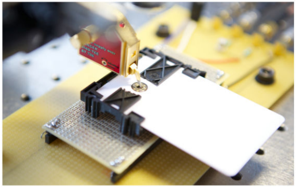
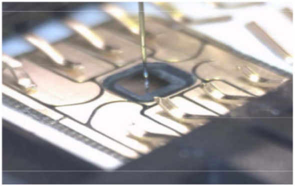
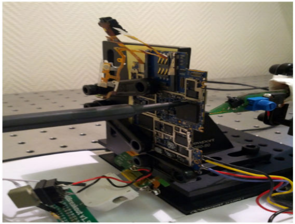
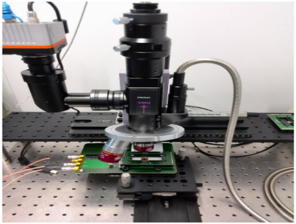
Root of Trust

- Root of trust : Cryptographic Integrated Circuit (IC)
  Microcontroller, SoC, FPGA, ASIC



Hardware Security

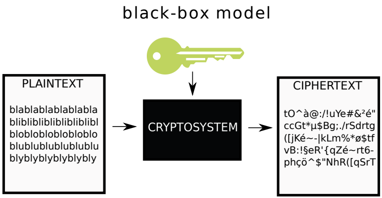
- Observe / Disturb the physical behaviour of crypto. IC
  - Observe : Side-Channel Attacks (SCA)
  - Disturb : Fault Attack (FA)
  - And more : Invasive Attacks

Agenda

Classical Cryptography

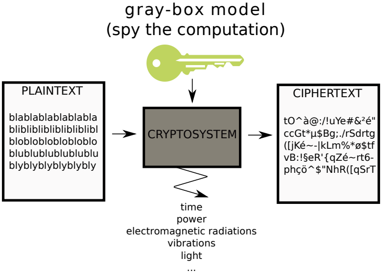
- Black-Box Model assumed in classical cryptography :
  - key(s) stored in the device
  - cryptographic operations computed inside the device



- The attacker has only access to pairs of plaintexts / ciphertexts.

Secure Cipher - Unsecure Implementation (1/2)

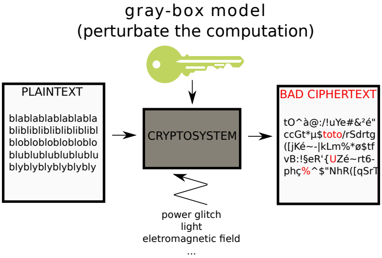
- [Kocher] (1996) ⇒ exploitation of physical leakages
  - cryptosystems integrated in CMOS technology
  - physical leakages correlated with computed data



- The attacker has also access to physical leakages
- New class of attacks ⇒ Side-Channel Attacks (SCA)

Secure Cipher - Unsecure Implementation (2/2)

- [Boneh et al.] (1997) ⇒ exploitation of faulty encryptions
  - the attacker can generate faulty encryptions



- the attacker has access to correct & faulty ciphertexts
- New class of attacks ⇒ Fault Attacks (FA)

Agenda

Side Channel Cryptanalysis

- SCA consist in measuring a physical leakage of a device when it handles sensitive information
  - e.g. cryptographic keys
- Handled info. are correlated with the physical leakage
  - e.g. a register leaking as the Hamming Weight of its value
- The attacker can then apply statistical methods to extract the secret from the measurements
  - Simple Side-Channel Attacks (SSCA)
  - Differential Side-Channel Attacks (DSCA)
  - Template Attacks (TA)
  - Collision-based Side-Channel Attacks
  - ...

Agenda

Physical Leakages exploited by SCA

- **Timing Attacks** (CRYPTO 96) - (Kocher)
  exploit the computational time of cryptographic operations

- **Power Analysis** (CRYPTO 99) - (Kocher et al.)
  exploit the power consumption of the IC

- **ElectroMagnetic Analysis** (CHES 01) - (Gandolfi et al.)
  exploit the electro-magnetic radiations of the IC

- **Acoustic Cryptanalysis** (2004) - (Shamir)
  exploit the sound emitted by the IC

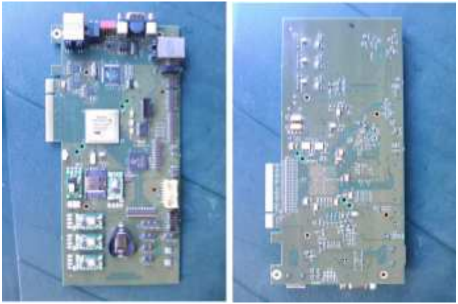
- **Light Emission Analysis** (CHES 10) - (Di Battista et al.)
  exploit the light emission of the IC

Measuring the Power Consumption of an IC (1/2)

- Different means :
  - shunt resistor
  - current probe
  - differential probe
- Optional : Low Noise Amplifier $\rightarrow$ amplify the signal
- Cost : low

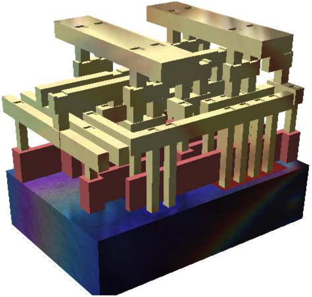
Measuring the Power Consumption of an IC (2/2)

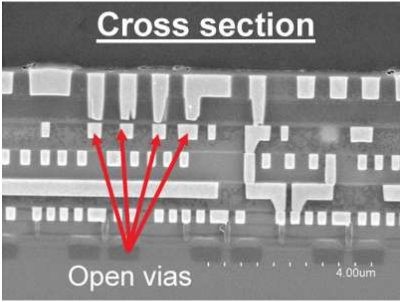
- The IC can filter the current switching.
- The IC can be mounted on complex boards !!!
  - Where is the power supply pin ?
  - There is sometimes several power supply pins . . .



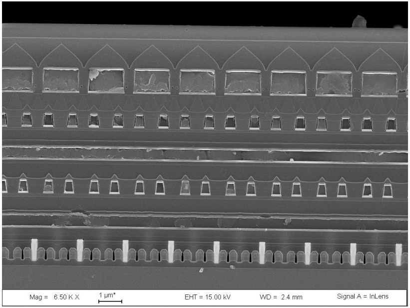
Measuring the EM Radiations of an IC (1/4)

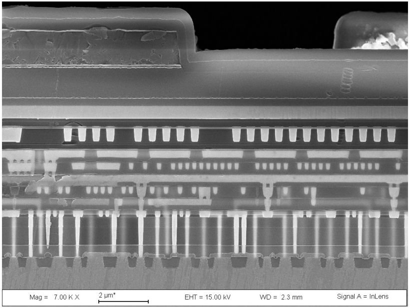
- When an IC is computing, current flows through the different metal layers to supply the gates.
- Maxwell equations $\Rightarrow$ current flowing through each metal rails creates an ElectroMagnetic field





Measuring the EM Radiations of an IC (2/4)





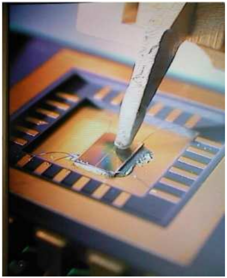
Measuring the EM Radiations of an IC (3/4)

- Electromagnetic sensor :
  - made of several coils of copper
  - diameter of coils $\rightarrow$ spatial precision
  - number of coils $\rightarrow$ increase the gain
- Mandatory : Low Noise Amplifier $\rightarrow$ amplify the signal
- Cost : medium

Measuring the EM Radiations of an IC (4/4)

- Examples of EM sensors :





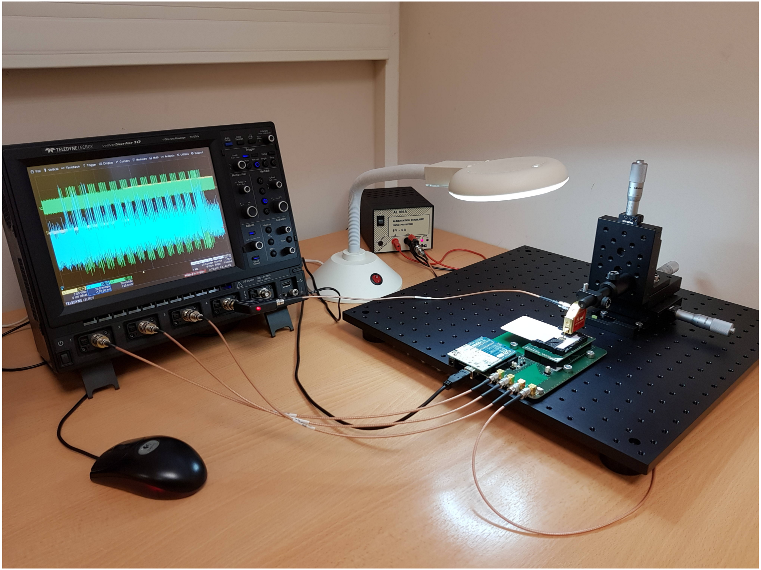
Digitizing the Side Channel Signal

- Oscilloscope :
  - frequency bandwidth
    in hertz (Hz)
  - sampling rate
    in samples/second (Sa/s)
  - vertical sensibility
    in volts (V)
  - precision of digitizing
    in bits (b)
  - number & memory of channels
    memory in bytes (B)
- Cost : high

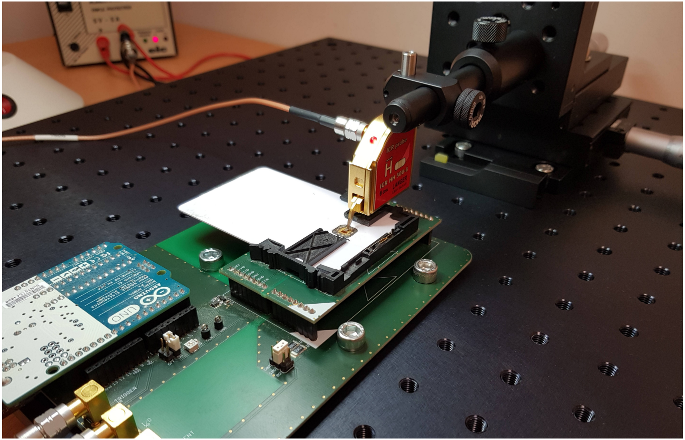
Triggering the Record

- Mechanism allowing to trig the record of the signal just before the beginning of the targeted operation
  - could be based on the sending of the command
  - could be generated by a test code running on the IC
- Most oscilloscopes have triggering capabilities
- Custom readers / electronic boards allow to communicate with the device & provide trigger capabilities

Example of a Side Channel Attack Setup (1/2)



Example of a Side Channel Attack Setup (2/2)



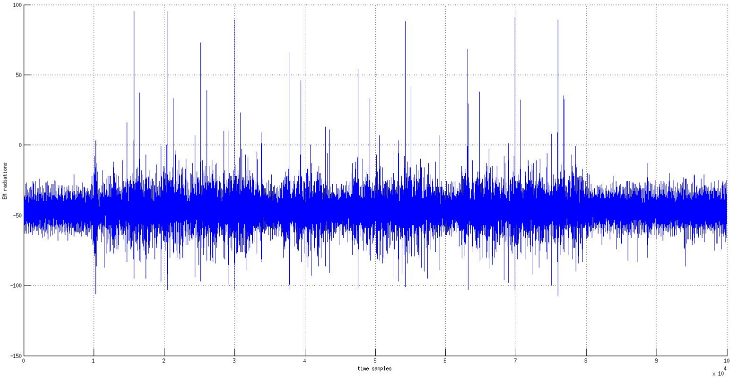
Example 1 (1/3)


Acquisition is stopped.
10.0 GSa/s 50.0 Mpts
1 On 5.00 V/
2 On 50.0 mV/
3 On
4 On 20.0 mV/
H 500 µs/
0.0 s
T 100 mV
Status Scales
Acquisition:
Sampling Mode Real Time
Capture Time 5.00 ms
Effective Res 100 ps/pt
Bits Of Res 8 bits
Trigger:
Mode Edge then Edge
InfiniiScan NA

Example 1 (2/3)

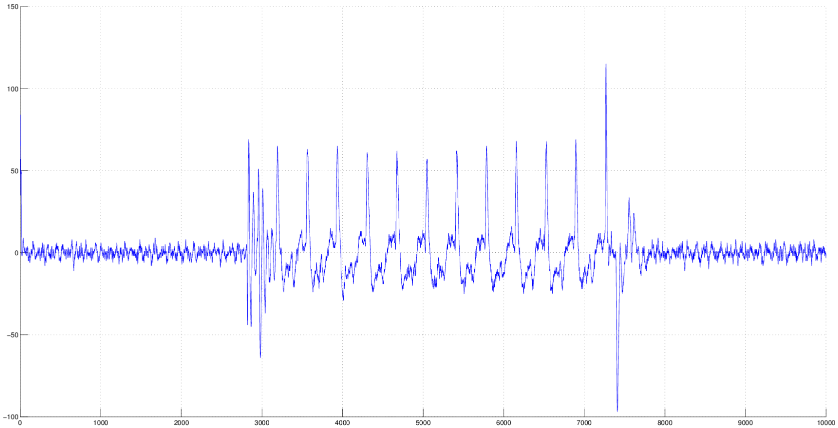
Acquisition is stopped.
10.0 GSa/s 50.0 Mpts
1 On
2 On 50.0 mV/
3 On
4 On 10.0 mV/
H 10.0 µs/
40.1335333 µs
T 100 mV
Status Scales
Acquisition:
Sampling Mode Real Time
Capture Time 5.00 ms
Effective Res 100 ps/pt
Bits Of Res 8 bits
Trigger:
Mode Edge then Edge
InfiniiScan NA

Example 1 (3/3)



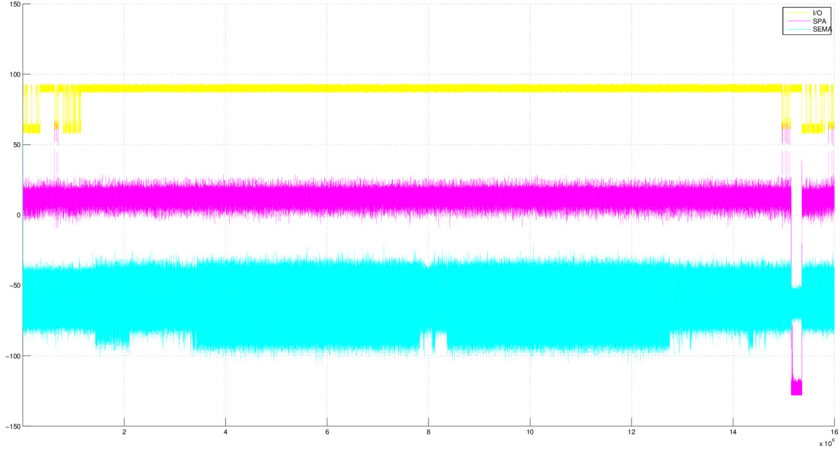
100
50
0
-50
-100
-150
EM radiations
0
1
2
3
4
5
6
7
8
9
10
time samples
x 10^4

Example 2



150
100
50
0
−50
−100
0
1000
2000
3000
4000
5000
6000
7000
8000
9000
10000

Example 3

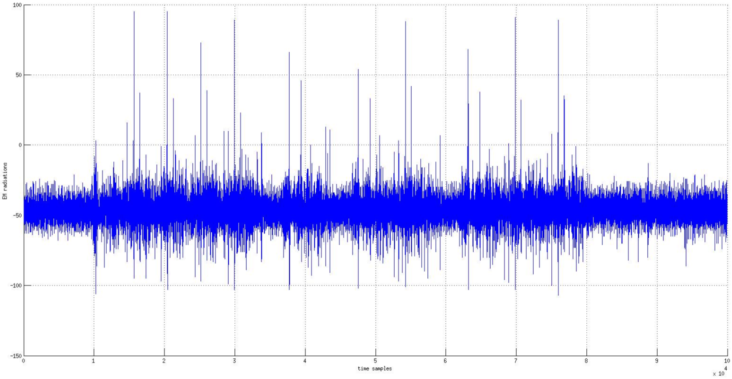


Agenda

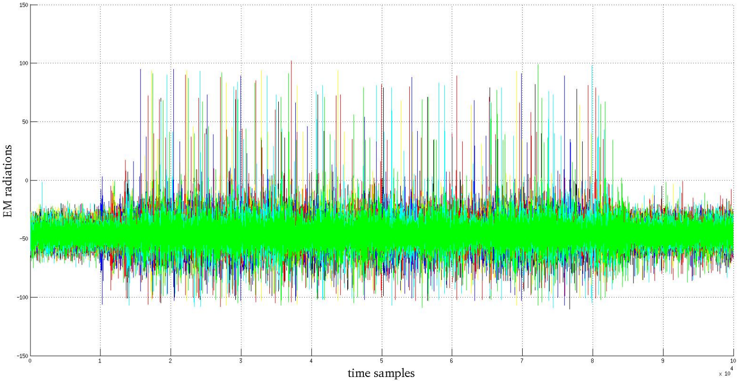
Some Pre-Processing Techniques

- Signal Processing Techniques
  - (smart) filtering
  - Resynchronization
- Dimension Reduction Techniques
  research of Points Of Interest (POI)
  - Signal-to-Noise-Ratio (SNR)
  - Variance
  - Principal Component Analysis (PCA)

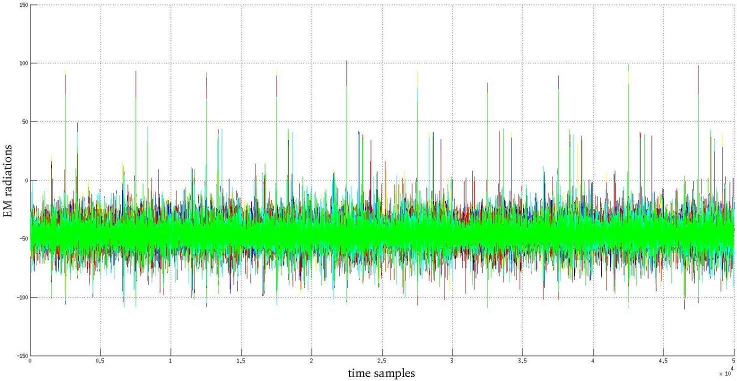
Resynchronization - Example (1/3)



Resynchronization - Example (2/3)



Resynchronization - Example (3/3)



Some Side Channel Attack Techniques (1/2)

- Simple Power Analysis (SPA) (CRYPTO 99) - (Kocher et al.)
  exploit one power trace to retrieve the key
- Differential Power Analysis (DPA) (CRYPTO 99) - (Kocher et al.)
  exploit several power traces to retrieve the key
- Big Mac Attack (CHES 01) - (Walter)
  extract private key from single exponentiation trace
- Template Attack (TA) (CHES 02) - (Chari et al.)
  build a dictionnary for all key values and use it to guess unknown key
- Collision based SCA (FSE 03) - (Schramm et al.)
  exploit a collision between two leakages

Some Side Channel Attack Techniques (2/2)

- **Correlation Power Analysis (CPA)** (CHES 04) - (Brier et al.)
  similar to DPA with Pearson correlation
- **Stochastic Attacks** (CHES 05) - (Schindler et al.)
  retrieve the key and the leakage model through profiling
- **Horizontal Correlation Analysis** (ICICS 10) - (Clavier et al.)
  perform CPA on a single RSA exponentiation
- **Collision-Correlation based SCA** (CHES 10) - (Moradi et al.)
  compute a correlation between collisions
- **Linear Regression Analysis (LRA)** (JCEN 12) - (Doget et al.)
  similar to stochastic attack without profiling
- **Deep Learning based SCA** (SPACE 16) - (Maghrebi et al.)
  similar to template attacks with deep learning

Some Side Channel Distinguishers

- Difference of Means (CRYPTO 99) - (Kocher et al.)
- Maximum Likelihood (CHES 02) - (Chari et al.)
- Pearson Correlation (CHES 04) - (Brier et al.)
- Mutual Information (CHES 07) - (Gierlichs et al.)
- Student T-Test (ICISC 08) - (Standaert et al.)
- Magnitude Squared Coherence (ePrint 11) - (Dehbaoui et al.)
- Kolmogorov-Smirnov Test (CARDIS 11) - (Whitnall et al.)

Some Post-Processing Techniques

- SCA attacks use Divide-and-Conquer strategy to guess cryptographic keys chunk by chunk
  e.g. AES128 master key guessed byte per byte
- Partial Brute-Force Attack
  - Require one pair of plaintext/ciphertext
- Key Enumeration Algorithms (KEA)
  - Require one pair of plaintext/ciphertext
  - SCA rank subkey values from the most likely to the less
  - KEA enumerates full keys from the most likely to the less thanks to subkeys SCA ranks
  - KEA = smart brute-force attack

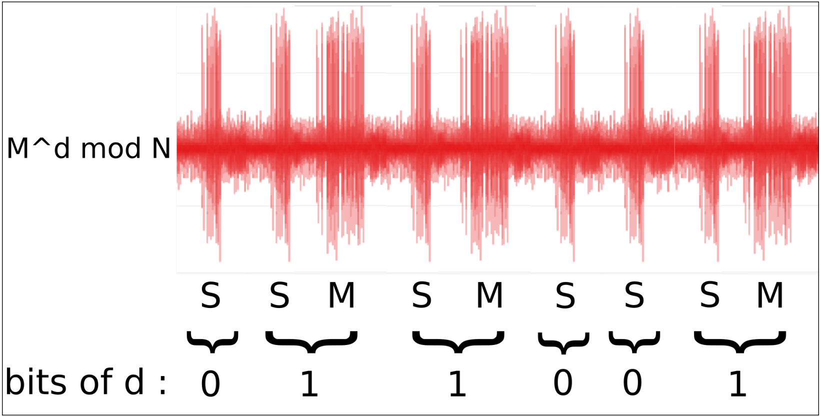
Example : SPA on RSA (1/2)

Data: d secret exponent
M message to sign
N modulo
Result: $R = M^d \; mod(N)$
Initialization : $R = 1$

for i : $size(d)$ $downto$ 0 **do**
  $R = R^2$
  if $d[i] = 1$ **then**
    $R = R \times M$
  end
end

Algorithm 1: Square-and-Multiply algorithm

Example : SPA on RSA (2/2)



Outline

Hardware level

- Add noise
  - jittered clock
  - noise generator
  - ...
- Balance/Randomize leakage
  - Balanced Dual Rail Logic
  - Masked/Random Dual Rail Logic
  - Asynchronous Logic

Algorithmic Level

- Random delay insertion
- Dummy instruction/operation insertion
- Schuffling operations
- Masking techniques
  - boolean masking
  - arithmetic masking
  - exponent blinding
  - ...

Agenda

SCA on Commercial Products (1/5)

- KEELOQ (MICROCHIP)
  - On the Power of Power Analysis in the Real World : A Complete Break of the KEELOQ Code Hopping Scheme
    CRYPTO 2008 - Eisenbarth et al.
  - Proprietary NLFSR-based block cipher implemented in
    - HCSXXX memory modules (HW implem.)
    - PIC microcontrollers (SW implem.)
  - Used in remote keyless entry systems
    (garage door openers, car anti-theft systems)
  - Successfull CPA attack in 10 traces
  - Extraction of the manufacturer key

SCA on Commercial Products (2/5)

- MIFARE DESFire MF3ICD40 (NXP)
  - Breaking Mifare DESFire MF3ICD40 : Power Analysis and Templates in the Real World

    CHES 2011 - Oswald et al.
  - Contactless smartcard with HW 3DES co-processor
  - Used for access control or public transport
  - Successfull CPA attack in 250k traces
  - Allow to clone the card
  - NXP has discontinuited the product

    new products : NXP MIFARE DESFire EV1 & EV2

SCA on Commercial Products (3/5)

- Virtex II PRO (XILINX)
  - On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks : Extracting Keys from Xilinx Virtex-II FPGAs
    ACM CCS 2011 - Moradi et al.
  - FPGA (SRAM) with HW 3DES co-processor
  - Used for bitstream encryption
  - Successfull CPA attack in 25k traces
  - Allow to clone/modify the bitstream

SCA on Commercial Products (4/5)

- ProASIC3 (ACTEL/MICROSEMI)
  - In the Blink of an Eye : There Goes your AES key
    IACR ePrint 2012 - Skorobogatov et al.
  - FPGA (FLASH) with HW AES co-processor
  - Used for bitstream encryption
  - Use of a custom acquisition setup
  - Successfull Pipeline Emission Analysis (PEA) in 0.01s
  - Allow to clone/modify the bitstream

SCA on Commercial Products (5/5)

- Superscalar Processors (INTEL, AMD, ARM, APPLE)
  - SPECTRE and MELTDOWN

    2018 - a lot of authors
  - Special feature of Intel processors : Speculative Execution
  - Can be exploited to manipulate sensitive data of other processus
  - Cache Timing Attacks can be used to guess this sensitive data
  - Devastating attack
  - Patch slows significantly CPU preformance

Agenda

Fault Zoology (1/2)

- Different ways to generate a fault :
  - Under / over-powering the IC
  - Tamper with the IC clock
  - Light injection
  - ElectroMagnetic (EM) field injection
  - Physical modification of the IC
    e.g. laser cutter, FIB
  - Software induced fault
    e.g. overclocking, register / memory modification

Fault Zoology (2/2)

- The duration of the fault can be :
  - Transient
  - Permanent
- Different effects :
  - Modification of operation flow
  - Modification of operands
- Different goals :
  - Bypassing a security mechanism
    PIN verification, file access right control, secure bootchain, . . .
  - Generating faulty encryptions/signatures
    $\Rightarrow$ *fault-based cryptanalysis*
  - Combined Attacks
    JavaCard based, FA + SCA

Fault based Cryptanalysis

- FA consist in perturbing the execution of the cryptographic operation in order to get faulty results
- Hypotheses are made on :
  - the targeted intermediate value
  - the effect of the injection on the intermediate value
- The attacker can then apply algorithmic methods to extract the secret from the obtained (correct and/or faulty) results
- Fault based Cryptanalysis use Divide-and-Conquer strategy to guess cryptographic keys chunk by chunk

  e.g. AES128 master key guessed byte per byte

Agenda

Under / Over-powering the IC (1/3)

- Under/over-power an IC during a very short time

- Over-powering cause unexpected electrical phenomenoms inside the IC
  e.g. local shortcuts

- Under-powering slows down the processing of the IC
  e.g. bad memory read/write, bad coprocessor execution

- Low / medium-cost attack
  e.g. power supply, pulse generator, custom electronic board

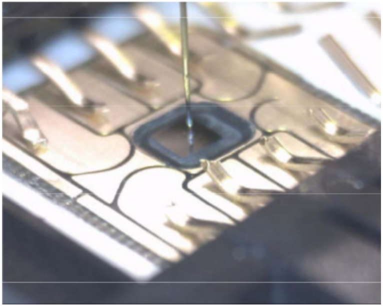
Under / Over-powering the IC (2/3)

- Adversary can control :
  - Amplitude of the glitch
  - Duration of the glitch
  - Shape of the glitch
- Generally no control of the fault precision :
  - On a microcontroller running code, modification of the current executed opcode and/or operand(s)
  - On a hardware coprocessor, modification of (some of) the current processed word(s) (e.g. registers)

Under / Over-powering the IC (3/3)

- Recent variant (Tobich+ 2012) :
  BBI : Body Bias Injection

- Consist in putting a needle in contact with the IC silicon through its backside



Tamper with the clock (1/2)

- Reduce one or several clock period(s) feeding the IC
- Accelerates the processing of the IC
  e.g. DFF sampling before correct computation of current instruction / combinational logic
- Low / medium-cost attack
  e.g. signal generator, custom electronic board

Tamper with the clock (2/2)

- Adversary can control :
  - Duration of the reduced clock period
  - Number of reduced clock period(s)
- Generally no control of the fault precision :
  - On a microcontroller running code, modification of the current executed opcode and/or operand(s)
  - On a hardware coprocessor, modification of (some of) the current processed word(s) (e.g. registers)

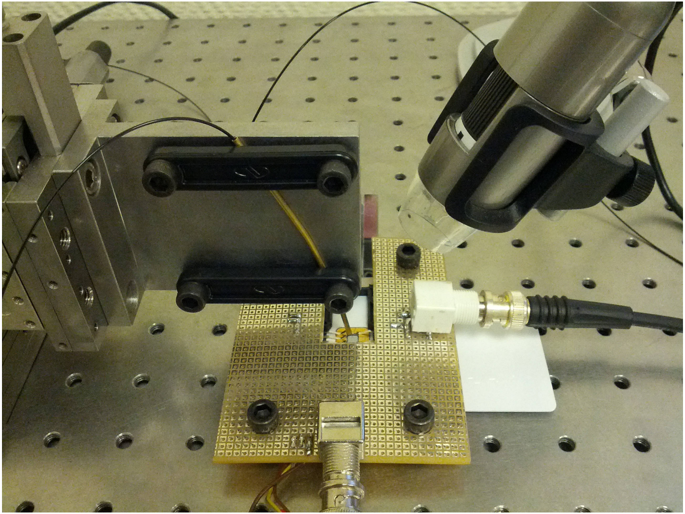
Light based Fault Injection (1/2)

- Inject a light beam into the IC
- A photoelectric phenomenom transforms light energy into electrical energy, provoking unexpected behaviour of transistors
- Old school setups were using flash lamp
- Modern setups are based on laser modules
- Medium / high-cost attack
  e.g. pulse generator, laser diode module, motorized X-Y-Z stage, optical microscope

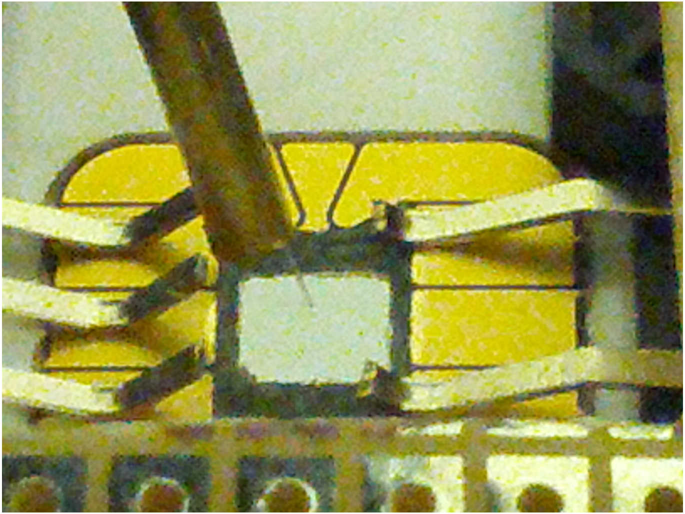
Light based Fault Injection (2/2)

- Requires to open the package of the IC in order the light beam can be injected into the frontside or the backside of the die
- On complex ICs with many metal layers, or on *secure* ICs with anti-probing shield, it can be difficult to inject light on the frontside of the IC
- As silicon is transparent to infrared light, backside light injection uses infrared light

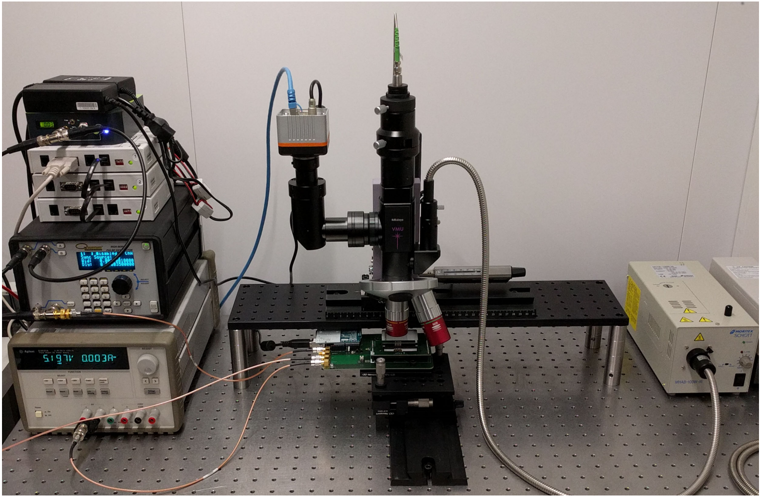
Laser Setup example 1 (1/2)



Laser Setup example 1 (2/2)



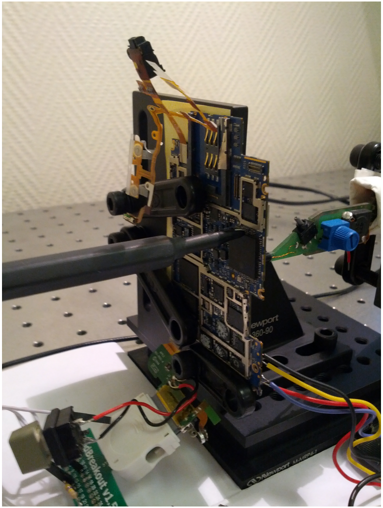
Laser Setup example 2



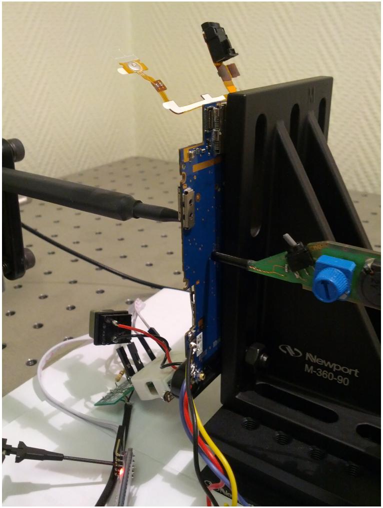
ElectroMagnetic Fault Injection (EMFI)

- Inject an electromagnetic field inside the IC
- Can be done without removing the package of the IC
- In practice, a glitch of high power is injected into an EM probe positionned above the IC
- Medium / high-cost attack
  e.g. high power pulse generator, EMFI probe, motorized X-Y-Z stage

ElectroMagnetic Injection Setup example (1/2)



ElectroMagnetic Injection Setup example (2/2)



Synchronization Mean

- In many cases, need of a synchronization mean to trig the fault at the right instant
- Classical method : monitoring power consumption / EM activity of the IC to find the side-channel signature of the event one wants disturb
- Several solutions :
  - Triggering capabilities of oscilloscopes
  - Real-time waveform-matching based triggering system
    Beckers+ 2016

Agenda

Introduction
- Embedded Systems
- Security Models

Side Channel Attacks (SCA)
- Side Channels
- Cryptanalysis Techniques
- SCA Protections
- SCA on Commercial Products

Fault Attacks (FA)
- Fault Zoology
- Fault Injection Means
- Cryptanalysis Techniques
- FA Protections

Invasive Attacks
- Attacks
- Countermeasures

Conclusion

Some Fault Attack Techniques

- Differential Fault Analysis (DFA) (CRYPTO 97) - (Shamir et al.)
  exploit pairs of correct/faulty ciphertexts to retrieve the key

- Safe Error Attack (SEA)
  similar to Template Attacks with faults

- Statistical Fault Attack (FDTC 13) - (Fuhr et al.)
  exploit only correct/faulty ciphertexts to retrieve the key

Example : FA on RSA CRT

- Consider a RSA CRT implementation, with
  - $N = p.q$ the public modulous
  - e and d the public and private exponents s.t. $e.d = 1 \; mod(\phi(N))$
- The adversary generates two RSA signatures S and $\tilde{S}$
  - $S = M^d \; mod \; N$, a correct signature
  - $\tilde{S} = M^d \; mod \; N$, a faulted signature
- The adversary can then factorize N to get p and q with $gcd(S - \tilde{S}, N) = q$

Outline

Hardware level

- Add noise
  - jittered clock
  - noise generator
  - ...
- Use robust gates
  - Redundant Logic
  - Store a value and its complementary
  - Asynchronous Logic

Algorithmic Level

- Random delay insertion
- Dummy instruction/operation insertion
- Schuffling operations
- Redundancy techniques
- Infection techniques

Outline

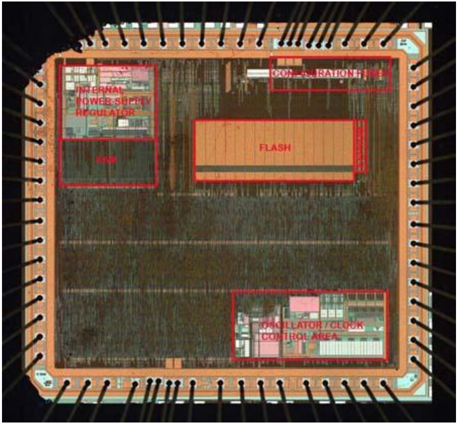
Invasive Attacks : different goals

- Get a secret key
- Disable hardware security mechanisms
- Dump the code of the device
- Reverse-engineer hardware blocks of the device
- ...

Example : heart of a micro-controller (1/2)

www.flylogic.net/blog

Example : heart of a micro-controller (2/2)



www.flylogic.net/blog

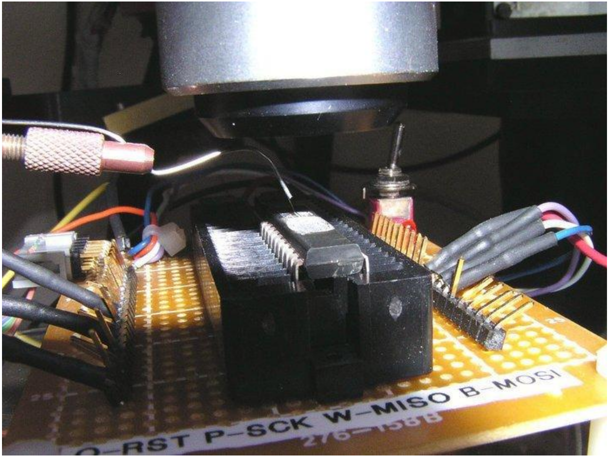
Microprobing (1/3)

- What happens inside the IC when a crypto operation begins ?
  - The key is read from the non-volatile memory
    EEPROM, Flash . . .
  - The key goes through the data bus
  - The key is loaded into the key register / RAM
  - The crypto operation can begin !

Microprobing (2/3)

- Imagine that you are able to spy data flowing between elements inside the IC!!!
  - You can spy the outputs of non-volatile memory
    EEPROM, Flash ...
  - You can spy the data bus
  - You can spy inside the glue logic of the CPU / crypto-coprocessor

Microprobing (3/3)



www.flylogic.net/blog

Disable Hardware Security Mechanisms

- Some devices contain fuses to lock a state
  e.g. one can lock the reconfiguration features of a micro-controller by irremediably disabling a fuse

- An attacker could reactivate the fuse to go back in the reconfiguration state.
  e.g. UV light, FIB

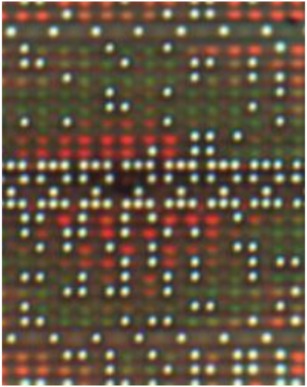
- Inversely, he could cut a wire to disable a security mechanism.
  e.g. laser cutter, FIB

ROM Reading Attack

- In most devices, bootloader is stored in ROM (Read Only Memory)
- Data stored in ROM cannot be modified, because implemented in logic gates.
- It is possible to read the bits of the ROM to reconstruct the binary code.
  e.g. via optical or electronic microscopy

Example : ARM micro-controller (Atmel AT91) (5/5)

- some bits of the ROM



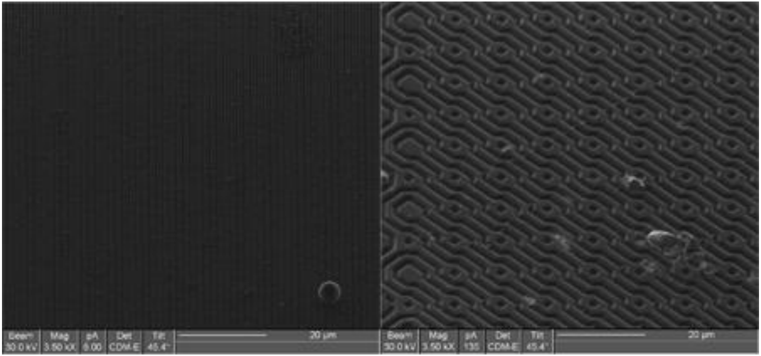
www.flylogic.net/blog

Outline

Invasive Attacks : Countermeasures

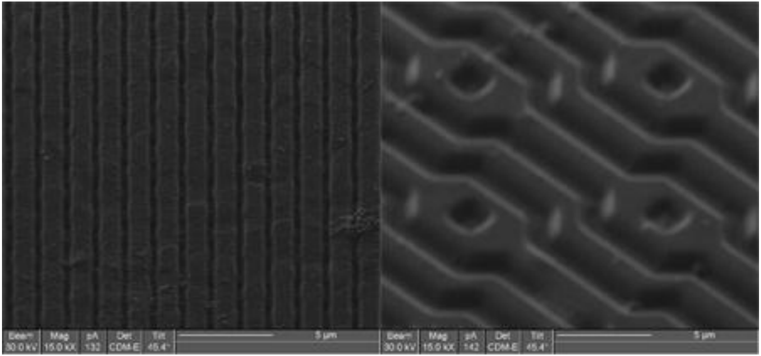
- Non-volatile memory encryption
- Bus encryption
- Active shield inserted above the top metal layer
  - current goes through the active shield.
  - if a rail of the active shield is disconnected, termination of the IC ! ! !

Invasive Attacks : Some Examples of Active Shields (1/3)



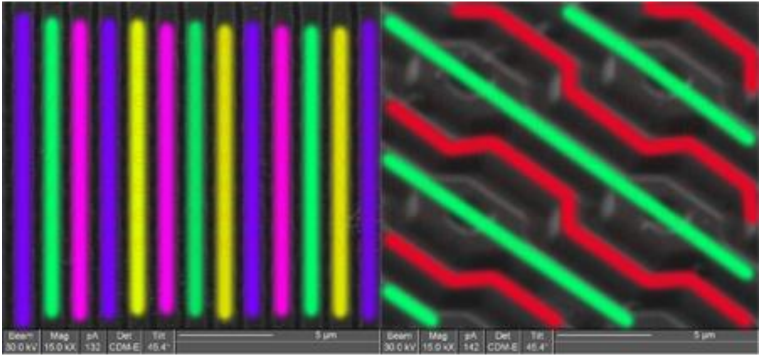
www.flylogic.net/blog

Invasive Attacks : Some Examples of Active Shields (2/3)



www.flylogic.net/blog

Invasive Attacks : Some Examples of Active Shields (3/3)



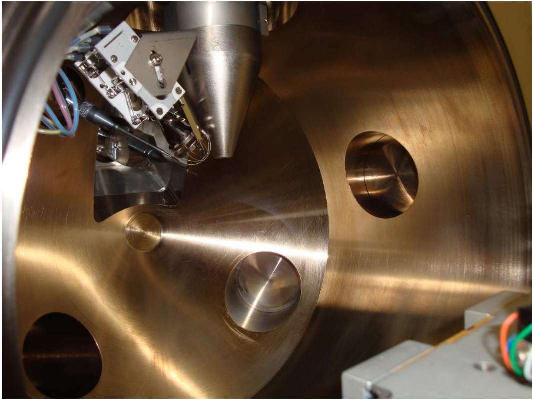
www.flylogic.net/blog

Focus Ion Beam : the ultimate tool ! ! !

- A Focus Ion Beam (FIB) is a Failure Analysis tool
- It is used to cut or etch wires at a very high precision
- It can be used for Hardware Attacks purpose :
  - reconnect a fuse
  - cut and re-rout a wire from the active shield

FIB (1/2)

FIB (2/2)



www.flylogic.net/blog

Hardware Reverse-Engineering

- Use chemical methods to delayer the chip.
- Make precise pictures of each metal layer.
- Recognize forms corresponding to logic gates.
- Reconstruct the netlist of the chip.

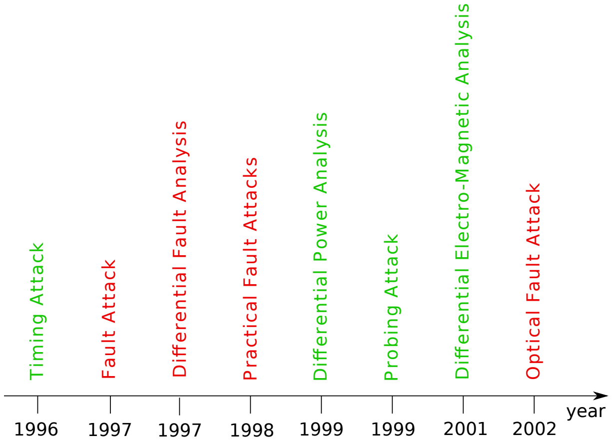
Hardware Reverse-Engineering

- HW RE can be used to reverse a secret cryptographic algorithm.
  e.g. NXP Mifare Classic & K. Nohl story

- HW RE can be used to find Hardware Trojans.
  Syrian radar story

Outline

Evolution of Non/Semi-Invasive Attacks



Certification Schemes

- Procedure to evaluate the security level of a product
- Three actors :
  - The Developer
  - The Security Lab
  - The Certification Body
- Some certification schemes :
  - Common Critera
  - EMVCo
  - Global Platform
  - CSPN

Thank you !

- Any question ?
- Contact : victor@ninjalab.io