Introdution to Physical Cryptanalysis

ASK 2014

Victor LOMNE

ANSSI (French Network and Information Security Agency)

Saturday, December 20^{th}, 2014

Agenda

Agenda

Context

- Since the 90's, increasing use of secure embedded devices
  - 8G smartcard ICs sold in 2012 (SIM cards, credit cards ...)

- Strong cryptography from a mathematical point of view used to manage sensitive data
  - AES, RSA, ECC, SHA-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 $\Rightarrow$ reduce the Attack Surface

Examples of Secure Embedded Devices

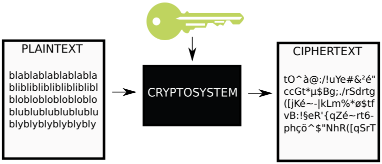
- Smartcards (credit cards, USIM, e-passports ...)
- Trusted Platform Modules (TPM)
- Smartphone secure elements
- Hard disk drives with HW encryption
- Set-Top Boxes
- Hardware Security Modules (HSM)
- Wireless sensors network
- ...

Agenda

Classical Cryptography

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

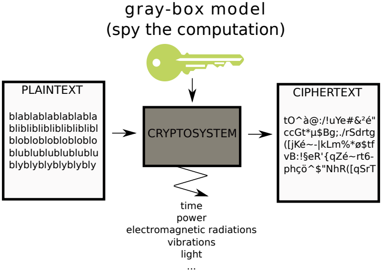
black-box model



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

Secure Cipher - Unsecure Implementation (1/2)

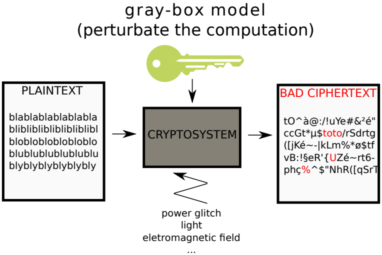
- [Kocher] (1996) ⇒ exploitation of physical leakages
  - cryptosystems integrated in CMOS technology
  - physical leakages correlated with computed data



- 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

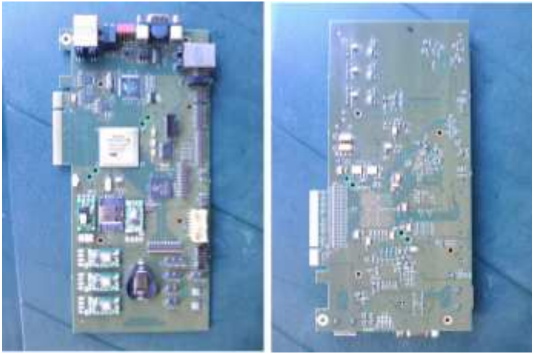
- **Light Emission Analysis** (CHES 10) - [Di Battista et al.]
  exploit the light emission of the IC

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

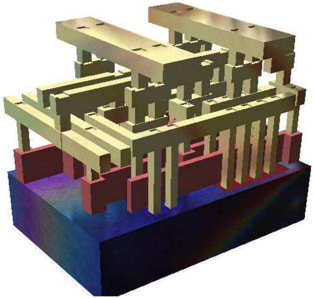
Measuring the Power Consumption of an IC (2/2)

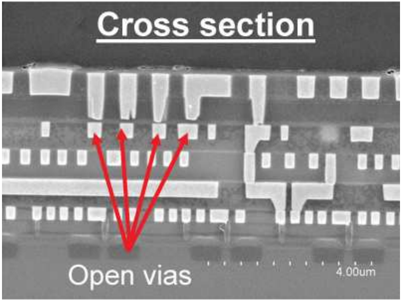
- The IC can filter the current switching
- The IC can be mounted on complex boards !!!
  - Where is the power supply pin ?
  - There is sometimes several power supply pins ...



Measuring the EM Radiations of an IC (1/3)

- 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





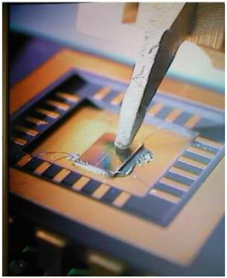
Measuring the EM Radiations of an IC (2/3)

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

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

- Examples of hand-made / commercial EM sensors:





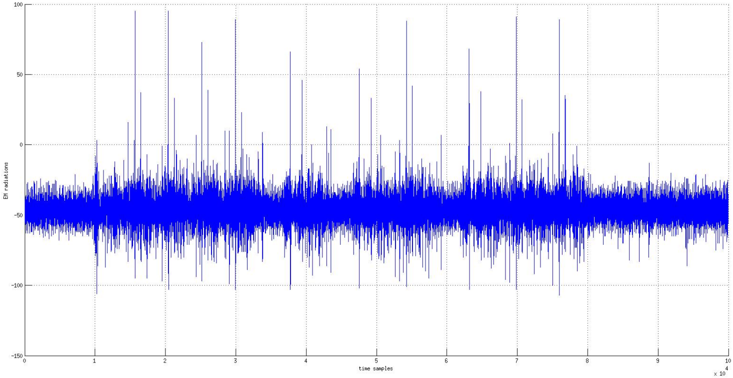
Digitizing the Side Channel Signal

- Oscilloscope:
  - frequency bandwidth
  - sampling rate
  - vertical sensibility
  - precision of digitizing
  - number & memory of channels
- Cost: medium / high

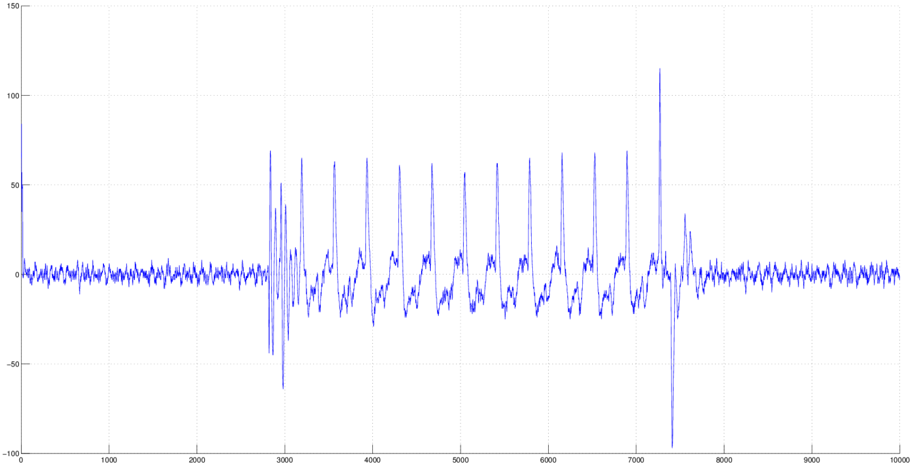
Triggering the Record

- 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

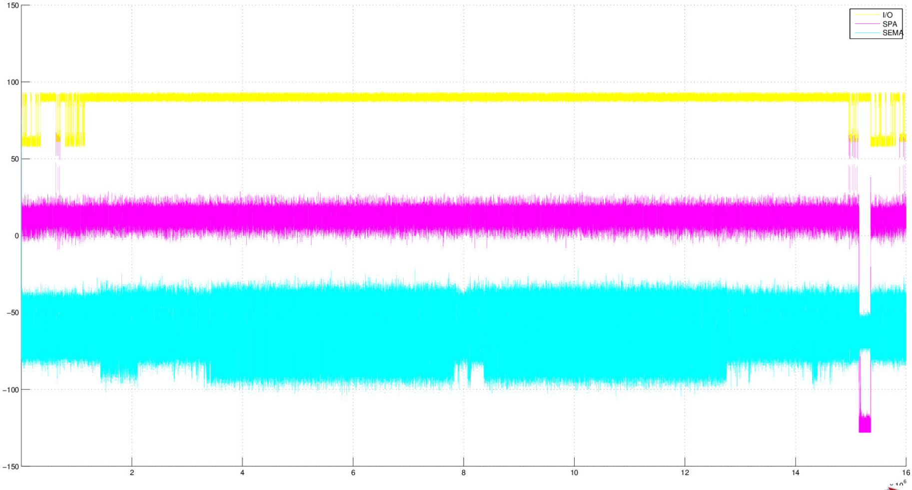
Example 1 - AES encryption on a smartcard chip



Example 2 - AES encryption on a FPGA



Example 3 - Internal Authenticate on a smartcard



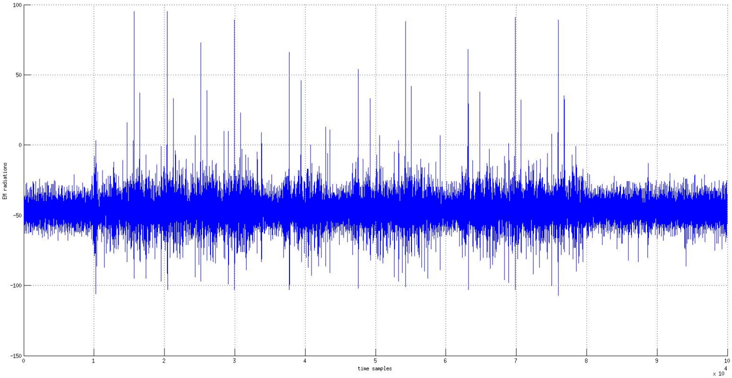
Agenda

Some Pre-Processing Techniques

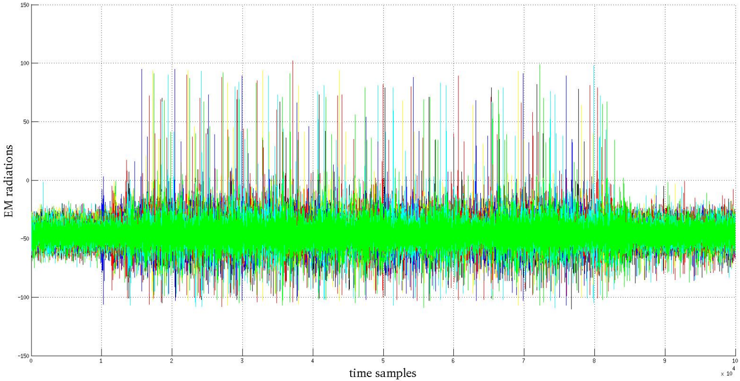
- Signal Processing Techniques
  - (smart) filtering
  - Resynchronization

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

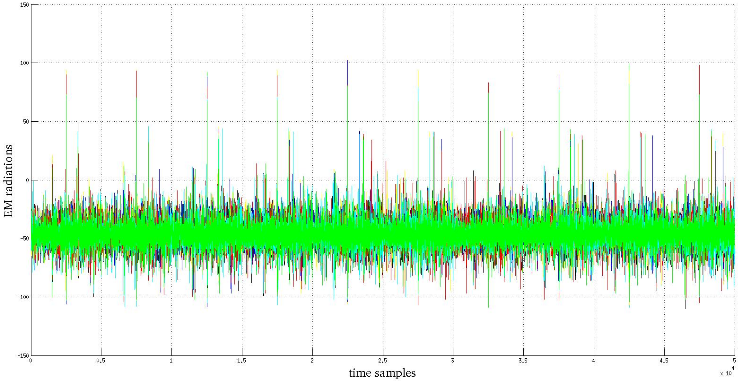
Resynchronization - Example (1/3)



Resynchronization - Example (2/3)



Resynchronization - Example (3/3)



Generic SCA Flow

1. Collect N side channel traces w. known inputs
   $t_1 \rightarrow Enc(p_1, k), \ldots, t_N \rightarrow Enc(p_N, k)$
2. Choose sensitive variable depend. on input & secret
   e.g. AES Sbox output $\rightarrow v_i^{\hat{k}} = S(p_i \oplus \hat{k})$
3. Choose a Leakage Model
   e.g. Hamming Weight (H)
4. Compute predictions for each key hypothesis
   $\hat{k} = 0 \quad \rightarrow H(v_1^{\hat{k}=0}), \ldots, H(v_N^{\hat{k}=0})$
   ...
   $\hat{k} = 255 \rightarrow H(v_1^{\hat{k}=255}), \ldots, H(v_N^{\hat{k}=255})$
5. Use a distinguisher to discriminate the correct key by comparing the N traces and the predictions

SCA flow and Leakage Model: 3 cases

1. Select a priori a Leakage Model
   - Hamming Weight, Hamming Distance
   - Used in classical SCA (DPA, CPA, MIA, ...)
2. Select a priori a space of Leakage Models
   - Attack will *guess* the correct model in selected space
   - Used in Linear Regression Attack (LRA)
3. Infer a Leakage Model through profiling before attack
   - A preliminary step is performed on an open copy of the device to build a leakage model for each key value
   - Used in Template Attack (TA)

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

Some Side Channel Distinguishers

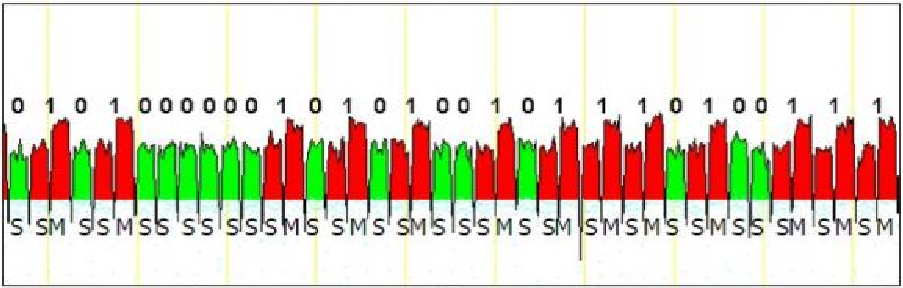
- Difference of Means (CRYPTO 99) - [Kocher et al.]
- Maximum Likelihood (CHES 02) - [Chari et al.]
- Pearson Correlation (CHES 04) - [Brier et al.]
- Mutual Information (CHES 07) - [Gierlichs et al.]
- Student T-Test (ICISC 08) - [Standaert et al.]
- Magnitude Squared Coherence (ePrint 11) - [Dehbaoui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

Some Post-Processing Techniques

- 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 keys from this information
  - KEA = smart brute-force attack

Example: SPA on RSA



Agenda

SCA on Commercial Products (1/4)

- KEELOQ (MICROCHIP)
  - On the Power of Power Analysis in the Real World: A Complete Break of the KEELOQ Code Hopping Scheme (CRYPTO 08) [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 (2/4)

- MIFARE DESFire (NXP)
  - Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World
    (CHES 11) [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

SCA on Commercial Products (3/4)

- Virtex II PRO (XILINX)
  - On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks: Extracting Keys from Xilinx Virtex-II FPGAs
    (CCS 11) [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 (4/4)

- ProASIC3 (ACTEL/MICROSEMI)
  - In the Blink of an Eye: There Goes your AES key (ePrint 12) [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

Agenda

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 (IV)
  - the effect of the injection on the IV

- The attacker can then apply algorithmic methods to extract the secret from the obtained results (correct and/or faulty)

Agenda

Fault Injection Means

- Different means to inject a fault inside an IC:
  - Inject a power glitch on the VCC of the IC
  - Tamper the clock signal of the IC
  - Inject a light beam inside the IC
  - Inject an EM field inside the IC

Fault Injection Effects

- Different effects when injecting a fault inside an IC:
  - Set/reset/flip a bit stored inside a register or a memory
  - Modify a value transiting on a bus
  - Modify the current executed opcode
  - Modify a current operand

Power glitch

- Principle: under/over supply a device during a very short time
- Low-cost attack
- Well known technique at the golden age of pay-TV smartcard hackers
- Modern secure devices (e.g. smartcards) are protected against this attack path
  power pins filter the current to prevent under/over-powering

Tamper the clock

- Principle: reduce the clock period at the clock cycle you want to disturb the device
- Low-cost attack
- Modern secure devices (e.g. smartcards) are protected against this attack path
  they generate their own clock internally

ElectroMagnetic Injection (EMI)

- Principle: inject an electromagnetic field inside the device to disturb it
- EMI sensor is made of several coils of wire
  similar to SCA EM sensors
- A high power pulse generator is necessary to generate the power spike injected in the sensor

Light Injection

- Principle: inject a light beam inside the device to disturb it
- Modern methods are based on laser
- It requires to open the device
  remove the package of the chip
- Laser attacks very powerful and difficult to thwart
- Countermeasures: light sensors

Agenda

Fault Attack Techniques

- **Differential Fault Analysis (DFA)** (CRYPTO 97) - [Shamir et al.]
  - require to encrypt/sign two times the same message
  - require to have one or several pairs of correct/wrong ciphertext/signature corresponding to the same message
- **Safe Error Attack (SEA)**
  - require to encrypt/sign two times the same message
  - similar to Template Attacks, they require an copy of the target device that the adversary can fully controls
- **Statistical Fault Attack** (FDTC 13) - [Fuhr et al.]
  - work even with a set of faulty ciphertexts corresponding to different unknown plaintexts
  - require a Fixed Fault Logical Effect

Classification of Fault Models

- One can define a Fault Model as a function f such that:

$$f : x \to x \star e \tag{1}$$

x target variable, e fault logical effect and $\star$ a logical operation

- Any Fault-based Cryptanalysis requires an Invariant
$\Rightarrow$ new classification of FA based on the Invariant:
    - FA based on a Fixed Fault Diffusion Pattern
      DFA - e.g. [Piret+ 2003], [Mukhopadhyay+ 2009] ...
    - FA based on a Fixed Fault Logical Effect
      Safe Error Attacks, Statistical Fault Attacks

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 $gcd(S - \tilde{S}, N) = q$

Agenda

Bug Attack

- Pentium FDIV bug was a bug in the Intel $P5$ Pentium floating point unit (FPU)
- Because of the bug, the processor would return incorrect results for many calculations
- Nevertheless, bug is hard to detect
  1 in 9 billion floating point divides with random parameters would produce inaccurate results
- Shamir proposed a modified version of the Bellcore attack which exploits this bug to retrieve a RSA private key
- More dangerous than a classical fault attack because can be perfomed remotely

PS3 Hack

- George Hotz (a.k.a. Geohot) published in 2009 a hack of the Sony PS3
- The otherOS functionnality of the PS3 allows to boot a Linux OS
- A bus glitch allows him to gain control of the hypervisor
  $\Rightarrow$ ring 0 access
  $\Rightarrow$ full memory access
- In consequence Sony took George Hotz to court
- Sony and Hotz had settled the lawsuit out of court, on the condition that Hotz would never again resume any hacking work on Sony products

Outline

Combined Attacks: Use Case

- Consider a cryptographic implementation secured by:
  - a masking scheme such that SCA are unpracticable
  - a duplication countermeasure to avoid FA
- Is such an implementation really secure ?
  - If one takes each attack path alone yes !
  - But if one mixes both attack paths . . .

Outline

Combined Attacks: Principle

- Combined Attacks exploit the side-channel leakage of a faulty encryption to bypass both SCA and FA CM

- Examples:
  - Combined Attack of [Clavier+ 2010]
    targets 1^{st} order masked AES implementation
  - Combined Attack of [Roche+ 2011]
    targets any masked AES implementation
  - Combined Attack of [Giraud+ 2013]
    targets a protected RSA implementation

- Interestingly enough, up to now only FA based on a Fixed Fault Logical Effect have been extended to CA

Example: Combined Attack of [Roche+ 2011]

- Encrypt N plaintexts $P_1 \ldots P_N$ and keep the N ciphertexts $C_1 \ldots C_N$
- Encrypt the N plaintexts once again by injecting a fault during the penultimate round of the Key-Schedule and record the leakage traces $\Omega_1 \ldots \Omega_N$
- Exploit the side-channel leakage of the faulty ciphertext:
  $k = argmax(\rho(HW(SB(SB^{-1}(C_j^i \oplus \hat{k}) \oplus \hat{e}_9) \oplus \hat{k} \oplus \hat{e}_{10}), \Omega_i))$
- The attack will work if the fault has the effect of a XOR with a non negligible rate

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
  - ...

Outline

Hardware level

- Analog level
  - jittered clock
  - glitch detector
  - light detector
  - ...
- Digital level
  - Redundant Logic
  - Store a value and its complementary
  - Error Detecting Codes
  - ...

Algorithmic Level

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

Outline

Certification Schemes

- Procedure to evaluate the security level of a product
- Three actors:
  the developper / the security lab / the scheme
- Some certification schemes:
  - Common Critera
  - EMVCo
  - CSPN
  - ...

Questions ?

- contact: victor.lomne@ssi.gouv.fr