Security evaluation → Common Criteria /design

Attacks on SmartCards — 2 ways: Perturbation / Observation
- Fully invasive attacks ← Reverse engineering
- Perturbation attacks → power glitch / microprobe tip / Electromagnetic pulse / light, laser pulse / T°... Bellcore attack.
- Observation - Side channel
- Embedded Software attacks

DFA = differential fault analysis ← side channal analysis and a fault is provoqued
SFA = statistical fault attacks ←
PFA = Persistent fault attacks
Elliptic curve
IFA = Ineffective Fault Attacks

Side channel attack = SCA ← exploit leak informations
SPA = Simple Power analysis ← exploit the power consumption ↗ operation ≠ → conso ≠ une multiplication consomme + qu'une addition par ex.
DPA = differential power analysis ←
CPA = Correlation Power Analysis ← best side channel attack
use statistical method to find a correlation between leakages and hypothesis
→ Data Masking
Deep Learning for SCA

cost = 36 tries at worst instead of the 10^4 theoritical ones

→ Side Channel Analysis
TA = timing attack ← ex for PIN when time is shorter = good figure ⇒ continue with others
chiffre
SPA / DPA / CPA = Power attacks
EMA = Electromagnetic Attack
Branch prediction
cache memories

Randomized Window Method
→ Dummy Point ~~Operation~~ Additions

Rotating masking

RTL : Register Transfert Level
Dual Rail Logic

→ Test Structures
Scan chain

test mode protection → Secured Test Controller → Reset Verification
System mode protection → scrambling method / scan enable tree protection / Spy Flip-Flops

BIST: Build in Self Test → se tester de manière autonome / ← pour améliorer la fiabilité

SIB = Segment Insertion Bit → partionner les tests → ne pas laisser l'accès libre de partout mais contrôler les entrées

→ Fault Attack
DFA on AES — Multi level countermeasure — Gate / RSR / RTL / Algo / Archi / System
• Hardware Redundancy
Basic redundancy / Partial redundancy

- information Redundancy
  EDC = Error detecting Code
  Nonlinear Codes
  Logic Conc
  RTL = Register Transfer Level

  Complementary parity : best trade off ?

- Timing Redundancy
  inverse computation
  involution ciphers
  pipeline redundancy
  Sliced
  → DDR = Data Double Rate
  FPGA = Field Programmable Gate Array
  Synchronous Logic ← use the clock
  Asynchronous Logic ← don't use it

ECC = Error correcting Code

TRNG = True Random Number Generator
PUF = Physical unclonable Function

Physical Security

Embedded Part:

What are side channel with an example: Side channels are indirect pathway through which attacker can gain information about a system by exploiting unintentionnal information leakage rather than direct access to the system's data. Problem → they bypass traditional security mecanisms.
ex: DPA : differential power analysis ← by measuring the card's consumption during the execution of a cryptographic algorithm, an attacker can identify patterns → secret about key.

Describe a counter measure against side channel at architectural level
→ bus scrambling → why: can reveal information by electromagnetic leaks
→ how: send data but not in a good order to avoid leaks.

Describe a counter measure against side channel at RTL level: ← Masking
→ Constant Ramming weight encoding → why: can reveal information if too much differencies between communications
→ how: Have the same Ramming weight for every message and avoid leakages

Why fault attacks are dangerous for secure implementations
Fault attack pose a significant threat to secure implementations as they manipulate a device's normal operation to induce errors → potentially revealing sensitive information
couple of example: glitch attacks - / overvolting
Techniques that can be used for fault attacks: - voltage glitching: temporarily reducing or spiking voltage to induce faults
- laser injection: using precise laser to cause fault in circuit
- Pulse EM injection: Applying EM pulse to alter chip behavior

Compare four of them with designer and attacker point of view:
designer: these attack require protection like error detecting code or hardware redundancy.
attacker: Each technique offers a level of precision and stealth

Describe advantages to use error detecting code:
Usefull against fault based attack and timing attack: give one other layer to detect errors.
Main application scenario: add redundancy information to the original data in order to detect errors
disadvantages: not enough to detect DFA and EMA ← sophisticate

Why internal test structures are used in digital design
High fault coverage, low area, short test time. ex scan chain → exposed state of a circuit
normal ↔ scan ← 2 modes ↔
How to exploit them: attacker can scan and obtain informations on the internal state on current encryption ← leaks on the key
How to protect system: Reconfigurable Scan Networks: allow secure access control, ensuring that test structures are only accessible under authorized conditions.
SIB = Segment insertion Bit.

In microelectronics which are the main counterfeiting type and how are they defined?
Which are main action for each for prevention?
- Recycling: refurbishing and selling used parts as new
- Remarking: relabeling lower grade unauthorized parts to appear as high grade
- Overproduction: Unauthorized production by the legitimate manufacturer beyond agreed quantities
- Cloning: Creating copies of authentics parts, often evolving reverse engineering

Define payload and trigger for Hardware trojan.
payload = malicious effect or action the trojan execute when activated
trigger: specific sequence of input or environmental condition allowing it to remain hidden until activated.

What are 2 main classes of PUFs (Physical unclonable function) : strong PUF and weak PUF
What is their purpose and how they are used.

Strong PUF = big number = weak ← at least 80 elements → 2^{80} possibilities
Weak PUF = low number = strong ← use for key storage → 2^{24} possibilities
Generate unique response based on inherent physical variation in each device, serving as a "fingerprint" for identification or cryptographic key generation

How ring oscillators can be used to design a PUF
→ by using difference between frequences of Ring oscillator → generate a PUF

TRNG = True Random Number generator
Use randomness in Radioxare like noise

For PUF → uniformity ⬭ ≈ 50%. 0 or 1
bit aliasing 0 ≈ 50% 0 or 1

Fault on round 8 of AES → 98%. to find the correct key
↳ the fault is propagated through the all AES ciphertext

With DFA on AES → 4 bytes can be retrieving with this method.

Elliptic curve & cryptography : smaller keys but slower computation on smartcards for same key size.

CPA principle : Leakage is usually correlated with Hamming weight.

SCA counter measure → Dummy operations / Random delays / Noise addition / Data masking

Level	Counter-measures against SCA (examples)
Gate (transistor level structure)	Power constant Logic // dual rail with precharge
P & R	Differential pairs routing
RTL	Constant Hamming weight encoding → DRL
Algorithm	Dynamic masking
Architecture	S-RNG, bus scrambling
System	Secret sharing

Level	Counter-measures against FA (examples)
Gate	Various sensors, robust structures against SEUs
P&R	Coupling reduction
RTL	Error detecting codes: limitations, timing redundancy
Algorithm	Precautions e.g. CRT use for RSA
Architecture	Function fusions to mask intermediate results
System	Depends on security policy: memory erasing, process or OS-level error recovery

cours3 Raingault = faults
cours4 " = side channel attaque
cours2 " = invasive attacks ← reverse engineering.

DFA:

	Conditions	Number / type of faults	Countermeasures
DFA: Differential Fault Attacks	Chosen plaintext Twice the same message	Low 1 on AES-128 with reduced entropy to 2^{40}. Low constraints on fault models	Redundancy, change messages (nonce), fault counter.

SFA:

	Conditions	Number / type of faults	Countermeasures
SFA: Statistical Fault attacks	Known ciphertexts	Many (in theory 10s, in practice 100s) Medium constraint on fault model ⇒ induce a bias in a random distrib°	Redundancy, fault detection
PFA: Persistent Fault attacks	Ciphertexts only	1 fault Many ciphertext (1000)	Self tests Breaks redundancy
IFA: Ineffective Fault attacks	Ciphertexts only Oracle needed	Many	Infection