FROM RESEARCH TO INDUSTRY

cea tech

leti

# Feature Extraction for Side-Channel Attacks

Eleonora Cagli

05/12/2018, Paris

*PhD Supervisor :* Emmanuel Prouff
(Safran Identity & Security)
*CEA Supervisor :* Cécile Dumas
(CEA-Leti Grenoble)

## Contents

## Secure Component and Embedded Cryptography

**A piece of hardware with security properties.**
**It usually embeds cryptography to provide security services (authentication, signature, secure messaging with terminals...)**

- Sensitive applications: ID cards, credit cards, transport cards, health cards, SIM
- Pervasive aspect: several billion smartcards sold par year
- Hard to update
- Hostile environment

## Secure Component and Embedded Cryptography

**A piece of hardware with security properties.**
**It usually embeds cryptography to provide security services (authentication, signature, secure messaging with terminals...)**


- Sensitive applications: ID cards, credit cards, transport cards, health cards, SIM
- Pervasive aspect: several billion smartcards sold par year
- Hard to update
- Hostile environment

## Secure Component and Embedded Cryptography

**A piece of hardware with security properties.**
**It usually embeds cryptography to provide security services (authentication, signature, secure messaging with terminals...)**

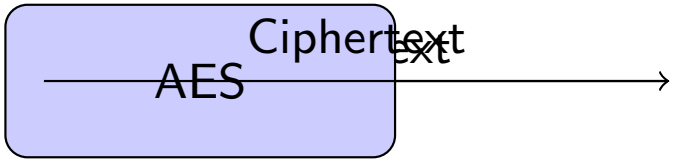

- Sensitive applications: ID cards, credit cards, transport cards, health cards, SIM
- Pervasive aspect: several billion smartcards sold par year
- Hard to update
- Hostile environment

$\Rightarrow$ Requires protection against very high-level attacker

# Security Certification


- Standardized Evaluation (*e.g.* ISO/IEC 15408 - Common Criteria)
- Assigns an Evaluation Assurance Level (EAL)
- The evaluator checks the Security Assurance Requirements (SAR), *e.g.* ADV, ALC, AVA, ...
- AVA: vulnerability assessment (penetration testing $\rightarrow$ attack potential rating)

# Side-Channel Attacks on Embedded Cryptography




**Classical Cryptanalysis**

- Black box (input, output)
- Formal attacker model (oracle, knowledge, ...)
- Computational complexity to perform the attack (*e.g.* $2^{126.1}$ operations to break AES-128 [**bogdanov**])

**Side-Channel Cryptanalysis**

- White box (input, output, side-channel observations of intermediate computations)
- Attacker with a certain equipment, expertise, knowledge of the embedded device, ...
- In Common Criteria: the cotation table of the attack

## Machine Learning

## Contents

# Notations

# Template Attack

## Contributions

### Objective

# References I