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...)**

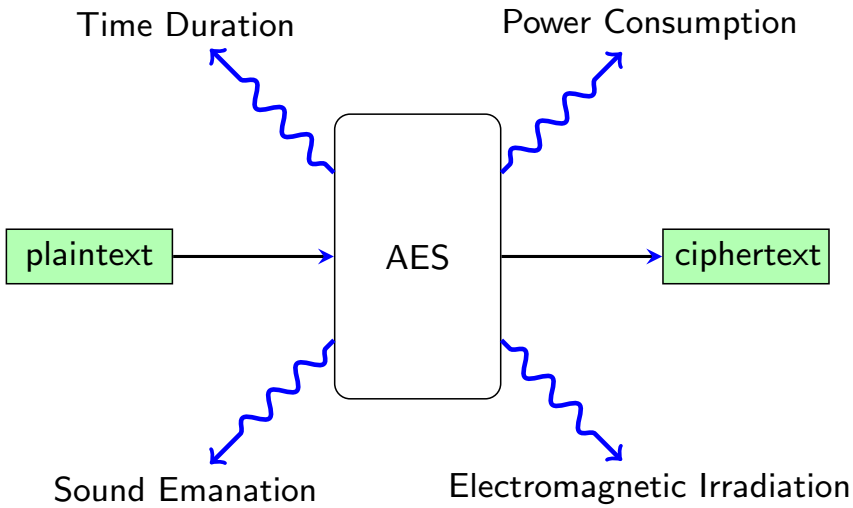

- Sensitive applications: ID cards, credit cards, transport cards, health cards, SIM
- Pervasive aspect: several billion smartcards sold par year
- Hard to update
- Hostile environment

$\Rightarrow$ 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 Vulnerability of Embedded Cryptography



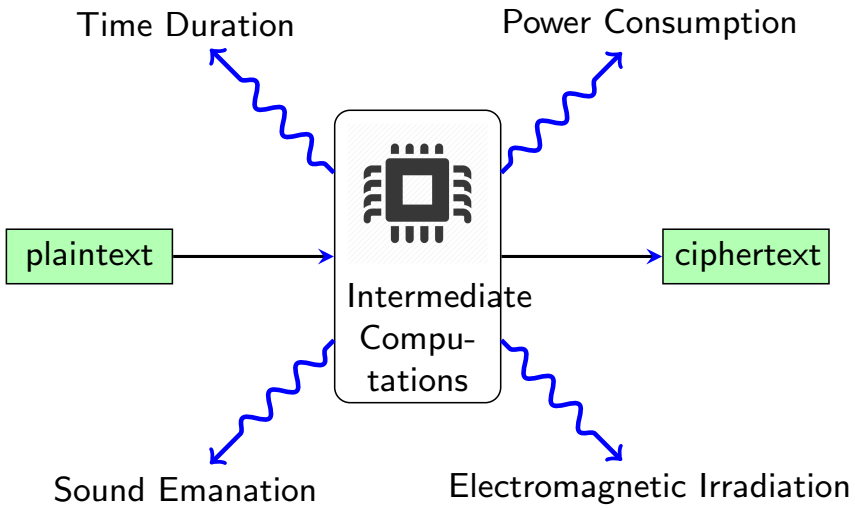

## Classical Cryptanalysis

- 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 [BKR11])

## Side-Channel Cryptanalysis

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

# Side-Channel Vulnerability of 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 [BKR11])

## Side-Channel Cryptanalysis

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

## Side-Channel Attacks

- **the physical nature of the exploited signals**: power consumption, electromagnetic irradiation, time, sound, temperature, ...
- **the chosen sensitive variable/s** $Z$:
  - $Z = K$ a secret key chunk
  - $Z = f(K, E)$ a variable depending on a secret key chunk and on a piece of public information
  - an operation (*e.g.* $Z \in \{square, multiply, \dots\}$)
  - a register
  - $Z' = \varphi(Z)$ a non-injective function of any sensitive variable (*e.g.* $f = \mathrm{HW}$ Hamming Weight)
- **the strategy family**: simple attacks, collision attacks, differential/advanced attacks
- **the shape of the attack**: horizontal attacks, vertical attacks
- **the attacker knowledge**: profiling, non-profiling attacks

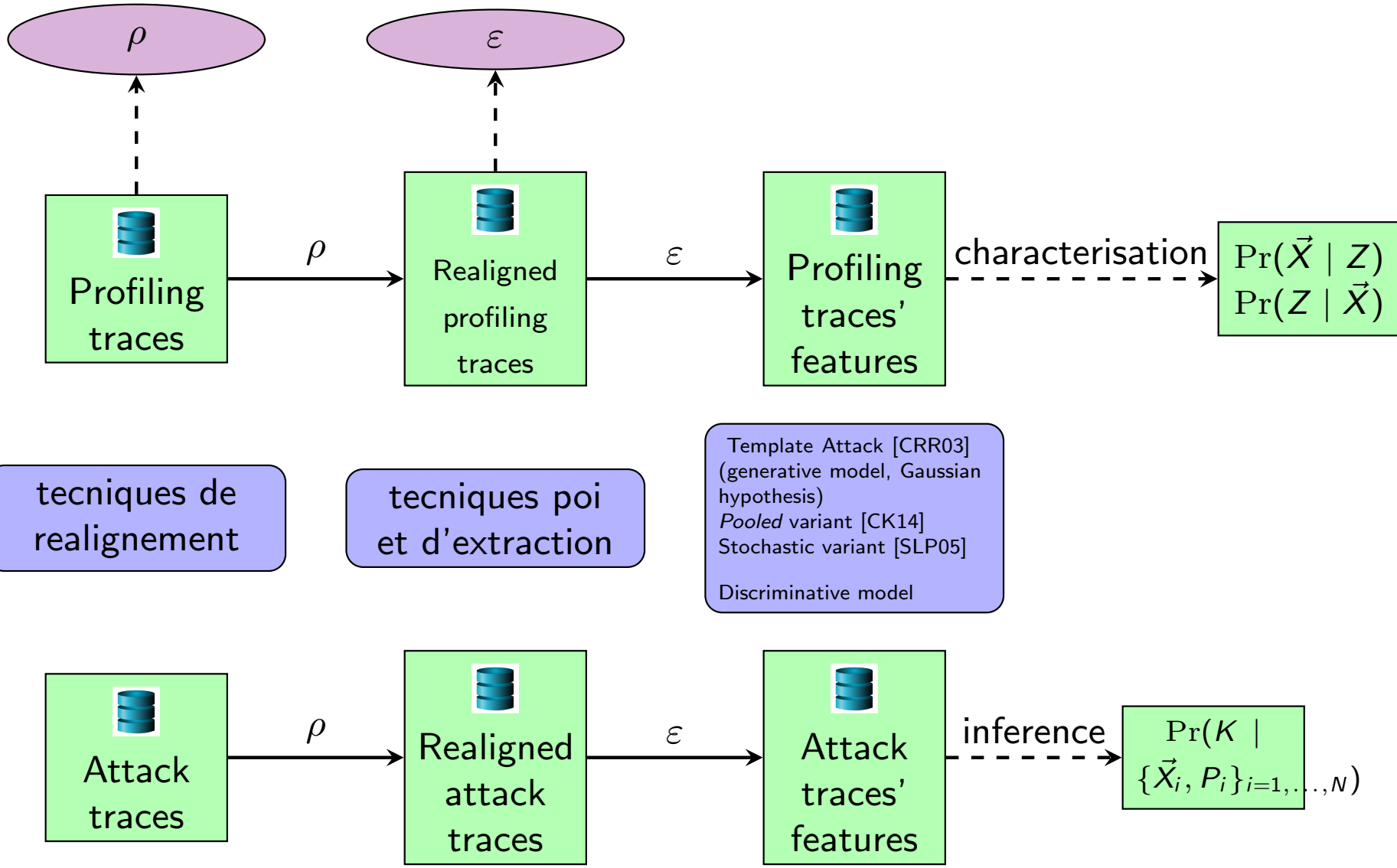
## Side-Channel Attacks

- **the physical nature of the exploited signals**: power consumption, electromagnetic irradiation, time, sound, temperature, ...
- **the chosen sensitive variable/s** $Z$:
  - $Z = K$ a secret key chunk
  - $Z = f(K, E)$ a variable depending on a secret key chunk and on a piece of public information
  - an operation (*e.g.* $Z \in \{square, multiply, \dots\}$)
  - a register
  - $Z' = \varphi(Z)$ a non-injective function of any sensitive variable (*e.g.* $f = \mathrm{HW}$ Hamming Weight)
- **the strategy family**: simple attacks, collision attacks, differential/advanced attacks
- **the shape of the attack**: horizontal attacks, vertical attacks
- **the attacker knowledge**: profiling, non-profiling attacks

## Contents

# Notations

# Template Attack



## Contributions

### Objective

# References I

[BKR11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. *Biclique Cryptanalysis of the Full AES*. Cryptology ePrint Archive, Report 2011/449. https://eprint.iacr.org/2011/449. 2011.

[CRR03] Suresh Chari, JosyulaR. Rao, and Pankaj Rohatgi. "Template Attacks". English. In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. Ed. by Burton S. Kaliski, Cetin K. Koc, and Christof Paar. Vol. 2523. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2003, pp. 13–28. ISBN: 978-3-540-00409-7. DOI: 10.1007/3-540-36400-5_3. URL: http://dx.doi.org/10.1007/3-540-36400-5_3.

[CK14] Omar Choudary and Markus G Kuhn. "Efficient template attacks". In: *Smart Card Research and Advanced Applications*. Springer, 2014, pp. 253–270.

# References II

[SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. "A stochastic model for differential side channel cryptanalysis". In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2005, pp. 30–46.