# Blind Side Channel Analysis using joint distributions

Christophe Clavier, Léo Reynaud, Antoine Wurcker

Université de Limoges - XLIM
Eshard

# Table of contents

# Cryptology

### Cryptography

- Private communication
- Authentication
- Integrity
- Non repudiation

### Cryptanalysis

Tires to break cryptography

### Cryptology

Both cryptography and cryptanalysis

# Cryptanalysis

## Mathematical

- Targets algorithm itself
- Exploits mathematical properties between inputs/outputs

## Physical attacks

- Targets physical implementation
- Three kinds :
  - Invasives
  - Semi-invasives
  - Non-invasives / Passives

# Side Channel attacks

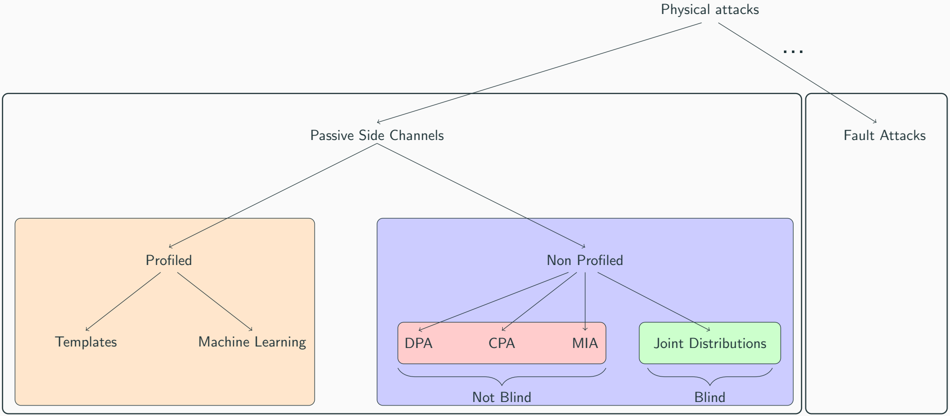



**Figure 1:** Non exaustive side channels attacks

# Side Channel attacks

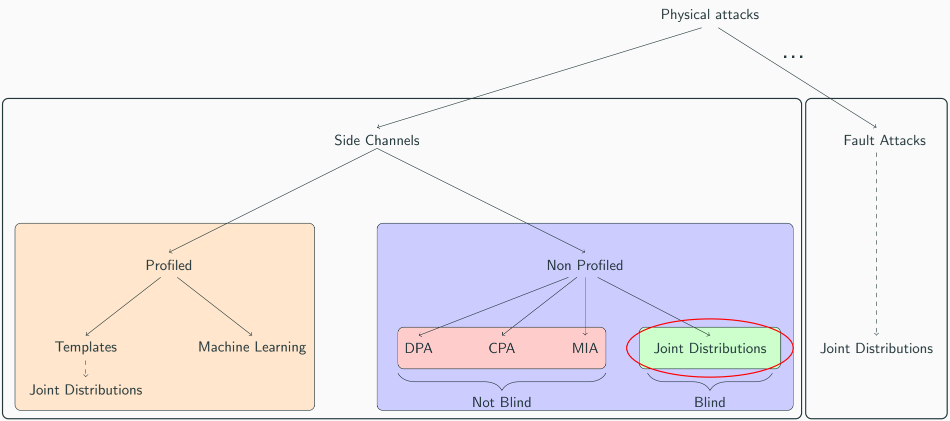



**Figure 1:** Non exaustive side channels attacks

# Side Channel attacks

## Common non profiled side channel attacks

- DPA [KJJ99]
- CPA [BCO04]
- MIA [GBTP08]

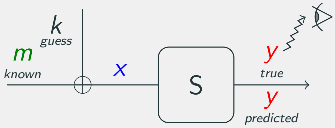



**Figure 2:** Internal states variables

## Needs

- Leakage on some internal state
- Knowledge and variability of plain/ciphertext

# Side Channel attacks : CPA

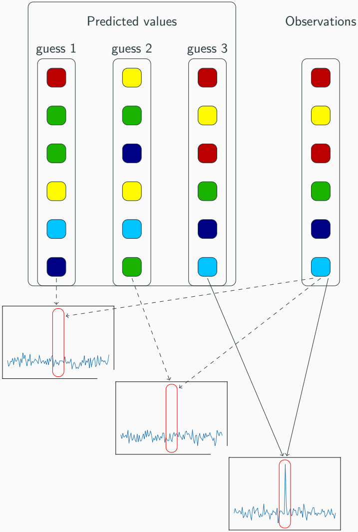



**Figure 3:** CPA principle

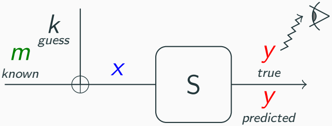



**Figure 2:** Internal states variables

# The need of blind attacks

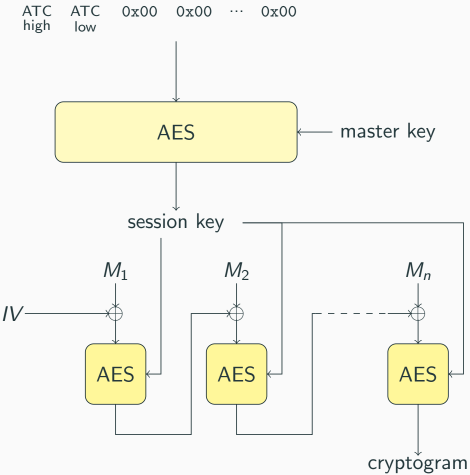



**Figure 4:** EMV session key derivation

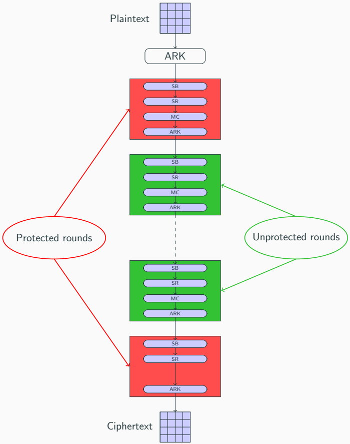



**Figure 5:** Aes early/final rounds protected

# The need of blind attacks

- *m* is unknown
  (does not vary much)
- *y* is unpredictable

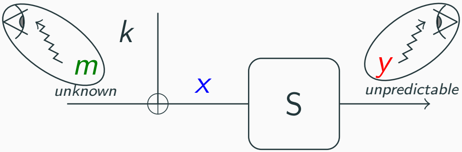



**Figure 6:** Passive Joint Distribution attack principle

$\rightarrow$ Let's observe both

# Joint Distributions

- $m$, $x$, $k \in GF(2)$
- $x = m \oplus k$

$k = 0$

| HW($x$) / HW($m$) | 0 | 1 |
|---|---|---|
| 0 | 1/2 | |
| 1 | | 1/2 |

**Figure 7:** Joint distribution $k = 0$

$k = 1$

| HW($x$) / HW($m$) | 0 | 1 |
|---|---|---|
| 0 | | 1/2 |
| 1 | 1/2 | |

**Figure 8:** Joint distribution $k = 1$

$\rightarrow$ Distribution related to $k$

# HWs Joint Distributions [LDL13]

- $m$, $y$, $k \in GF(2^8)$
- $y = S(m \oplus k)$
- HWs joint distributions of $m$ $y$ :

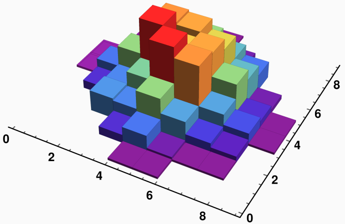



**Figure 9:** Joint distribution $k = 39$

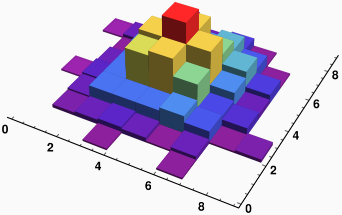


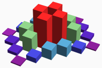

**Figure 10:** Joint distribution $k = 126$

# HWs Joint Distributions

**(a)** $\mathrm{HW}(k) = 0$

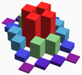
**(b)** $\mathrm{HW}(k) = 1$

**(c)** $\mathrm{HW}(k) = 2$



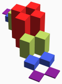
**(d)** $\mathrm{HW}(k) = 3$

**(e)** $\mathrm{HW}(k) = 4$



**(f)** $\mathrm{HW}(k) = 5$

**(g)** $\mathrm{HW}(k) = 6$



**(h)** $\mathrm{HW}(k) = 7$

**(i)** $\mathrm{HW}(k) = 8$

**Figure 11:** HWs joint distributions of $m$ and $x$

## The attack : Pros/Cons

**Cons**

- Needs to know the points of interest (PoI)
- Works on HWs not consumptions

**Pros**

- Works without plain/ciphertext
- Works with little variability of inputs
- Any round can be attacked

# The attack : Steps

- **Step 1 : Processing of the traces**
  Locate the PoIs where the considered variables leak
- **Step 2 : Reverse the consumption model**
  Infer HWs from the observed leakages at the PoI
- **Step 3 : Joint distributions**
  Build the joint distribution for each key (can be preprocessed)
- **Step 4 : Distinguisher**
  Select the key whose distribution best fits the observations

# Step 1 : Test Vector Leakage Assessment [GJJR11]

- Uses Welch's t-test
- Finds differences between distributions of samples
- Fixed vs Random : Non specific

$$t = \frac{\bar{x} - \bar{y}}{\sqrt{\frac{s_x^2}{N_x} + \frac{s_y^2}{N_y}}}$$

$\bar{x}$ : mean of $x$

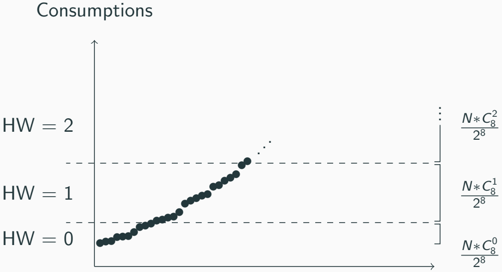
$s_x^2$ : variance of $x$

$N_x$ : sample size $x$

# Step 2 : Slices

**Consumption model**

$\ell = \alpha\,\mathrm{HW}(v) + \beta + \omega$




- Sort $N$ consumptions
- $\frac{N*\binom{0}{8}}{2^8}$ first $\rightarrow$ HW $= 0$
- $\frac{N*\binom{1}{8}}{2^8}$ next $\rightarrow$ HW $= 1$

**Figure 12:** Slice method to infer HWs

# Step 1/2 : Variance [CR17]

Goal : infer HW of a variable $v$

$\rightarrow$ Infer parameters $\alpha$, $\beta$ of consumption model

$$\begin{aligned}\mathrm{Var}(\ell) &= \mathrm{Var}(\alpha\,\mathrm{HW}(v) + \beta) + \mathrm{Var}(\omega)\\ &= \alpha^2\,\mathrm{Var}(\mathrm{HW}(v)) + \mathrm{Var}(\omega)\\ &= 2\alpha^2 + \mathrm{Var}(\omega)\end{aligned}$$

$$\alpha = \pm\sqrt{\frac{\mathrm{Var}(\ell)-\mathrm{Var}(\omega)}{2}}$$
$$\beta = \mathrm{E}(\ell) - \alpha\,\mathrm{E}(\mathrm{HW}(v))$$

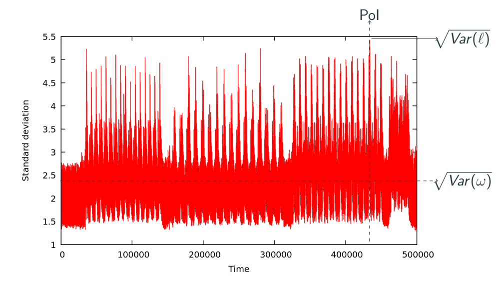



**Figure 13:** Standard deviation trace

$$\mathrm{HW}(v) = \frac{\ell-\beta}{\alpha}$$

# Step 4 : Distances [LDL13]

- Observe HWs
- Build histograms
- Apply distances between experimental and theoretical :
  - Inner product
  - $\chi^2$
  - ...
- Select $k$ such that distance is minimum

# Step 4 : Maximum likelihood [LB14]

## Observations

$h_m^*, h_y^*$: correct HWs (integers)

$\omega_m, \omega_y$: noise

$$h_m = h_m^* + \omega_m \qquad h_y = h_y^* + \omega_y$$

## Bayes

$$\Pr(k|(h_m, h_y)) = \frac{\Pr((h_m,h_y)|k)\cdot\Pr(k)}{\Pr((h_m,h_y))} \sim \Pr((h_m, h_y)|k) \cdot \Pr(k)$$

## Law of total probability

$$\Pr((h_m, h_y)|k) = \sum_{h_m^*, h_y^*} \Pr((h_m, h_y)|(h_m^*, h_y^*)) \cdot \Pr((h_m^*, h_y^*)|k)$$

## Noise probability

$$\Pr((h_m, h_y)|(h_m^*, h_y^*)) = \Pr(\omega_m = h_m - h_m^*) \cdot \Pr(\omega_y = h_y - h_y^*)$$

# Fault/Templates

- Fault attacks [Kor16]
- Templates [HTM09]

$\rightarrow$ Faults and templates in step 2

# Improvements : More PoIs [CR17]

| $x$ | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
|---|---|---|---|---|---|---|---|---|
| $S(x)$ | 010 | 110 | 011 | 101 | 001 | 111 | 100 | 000 |

k = 011

| $m$ | $x$ | $y$ |
|---|---|---|
| 000 | 011 | 101 |
| 001 | 010 | 011 |
| 010 | 001 | 110 |
| 011 | 000 | 010 |
| 100 | 111 | 000 |
| 101 | 110 | 100 |
| 110 | 101 | 111 |
| 111 | 100 | 001 |

| HW($m$) | HW($x$) | HW($y$) |
|---|---|---|
| 0 | 2 | 2 |
| 1 | 1 | 2 |
| 1 | 1 | 2 |
| 2 | 0 | 1 |
| 1 | 3 | 0 |
| 2 | 2 | 1 |
| 2 | 2 | 3 |
| 3 | 1 | 1 |

**Figure 14:** Three PoIs

- More $\neq$ between distributions
  $\rightarrow$ More efficient
- **Wrong PoI is catastrophic**

## Generalization

A secret $k$ is vulnerable if :

- We can observe at least 2 variables $a$ and $b$ such as $b = \varphi_k(a)$
- The joint distribution of the HWs of $a$ and $b$ is not identical for all $k$

## Generalization : First order masking

A secret $k$ is vulnerable in the case of boolean masking if :

- We can observe at least 2 variables $a$ and $b$ such as $b = \varphi_k(a)$
- The joint distribution of the HWs of $a$ and $b$ is not identical for all $k$
- $a$ and $b$ are masked with the same mask :
  - $a' = a \oplus r$
  - $b' = b \oplus r = \varphi_k(a) \oplus r$

$\rightarrow$ Distributions take into account all couples $(a' = a \oplus r, b' = b \oplus r)$

# HWs Joint Distributions first order masking

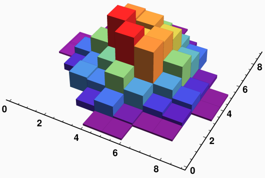



**Figure 15:** First order

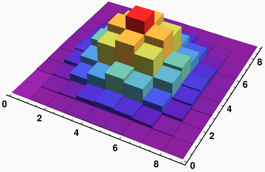



**Figure 16:** Second order

# HWs Joint Distributions first order masking

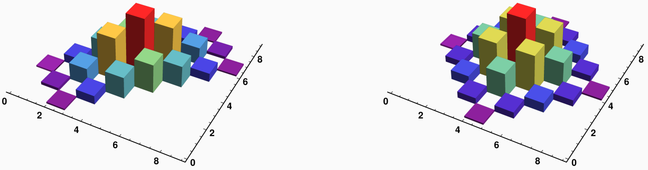



**Figure 17:** First order

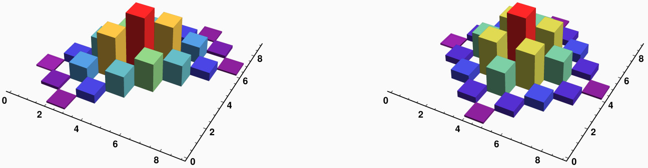
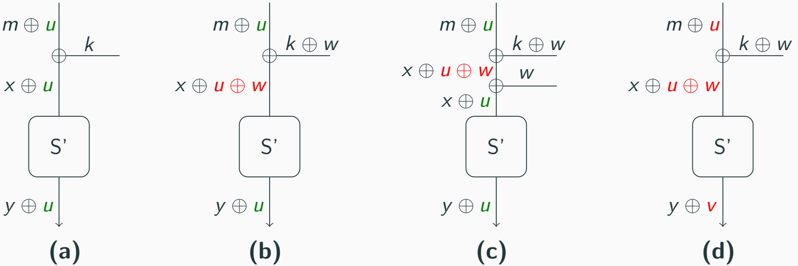



**Figure 18:** Second order

# Masked schemes




| | (a) | (b) | (c) | (d) |
|---|---|---|---|---|
| $m$ $y$ | ✓ | ✓ | ✓ | X |
| $m$ $x$ | ✓ | X | ✓ | X |
| $m$ $x$ $y$ | ✓ | X | ✓ | X |

**Figure 19:** Examples of Boolean masking

# Quadrivariate joint distributions [CRW18]

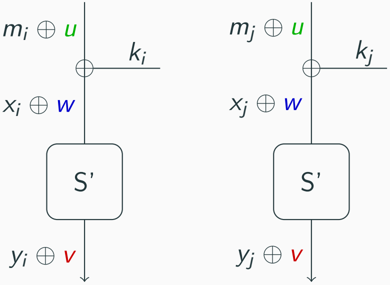



**Figure 20:** Two consecutives masked bytes

Three masks vertically
$\rightarrow$ Unable to attack

**But usually**

Same masks horizontally

# Quadrivariate joint distributions [CRW18]

HWs joint distributions of $m'_i$ $m'_j$ $y'_i$ $y'_j$

$m'_i = m_i \oplus u$
$m'_j = m_j \oplus u$
$y'_i = y_i \oplus v$
$y'_j = y_j \oplus v$

$\rightarrow$ Related to $k_i \oplus k_j$

HWs joint distributions of $m'_i$ $m'_j$ $x'_i$ $x'_j$

$m'_i = m_i \oplus u$
$m'_j = m_j \oplus u$
$x'_i = x_i \oplus v$
$x'_j = x_j \oplus v$

$\rightarrow$ Related to $HW(k_i \oplus k_j)$

# Quadrivariate joint distribution [CRW18]

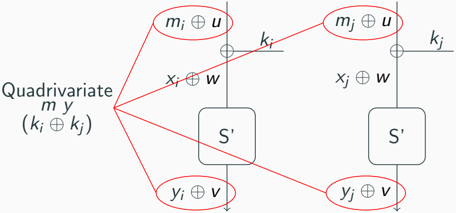



**Figure 21:** Quadrivariate *m y*

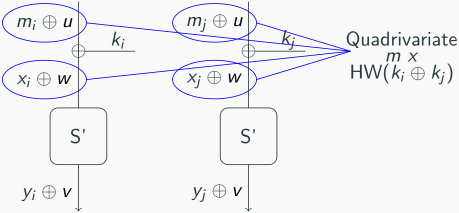



**Figure 22:** Quadrivariate *m x*

# Quadrivariate joint distribution : Recap

**Cons**

- Same issues as bivariate:
  - Need to locate the PoIs
  - Infer HW from leakages
  - $m$ $y$ not very efficient when masked
- Less efficient than classical joint distribution

**New possibilities**

A lot more masked schemes vulnerable :

$\rightarrow$ Any two bytes sharing the same couple of masks

# Quadrivariate $m$ $x$ : Key recovery on AES

Quadrivariate $m$ $x$ retrieves $\mathrm{HW}(k_i \oplus k_j)$

**Configurations considered**

We will consider three configurations :

- Cfg1 : All bytes are masked the same way (1 set of masks)
- Cfg2 : Only bytes of a round are masked the same way (11 sets)
- Cfg3 : Only bytes of a same position in the state are masked the same way (16 sets)

# Quadrivariate $m\ x$ : Key recovery on AES

A guess-compute-backtrack approach between key bytes can be used

- Guess one or several extended key byte
- Compute some other related key bytes (key expansion)
- Backtrack in case of inconsistency

# Full information

**Number of key candidates**

- Cfg1: Distances between all extended key bytes
- Cfg2: Distances between all bytes of a same round at every round
- Cfg3: Distances between all bytes of a same position for every position

$\rightarrow$ Only 1 candidate

# Local information

## Number of key candidates

- Cfg1/Cfg2 : Distances between all key bytes of a single round

  → Few millions

- Cfg 3 : Distances between all key bytes of a single position

  → Millions (66 key bytes involved)

→ Adding another round/position ends up with one/few candidates


**Figure 23:** Propagation 1 subgroup cfg3

Thank you

I will be pleased to answer your questions

(Bibliography is next)

# Bibliography i

Eric Brier, Christophe Clavier, and Francis Olivier.
**Correlation power analysis with a leakage model.**
In Marc Joye and Jean-Jacques Quisquater, editors, *Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings*, volume 3156 of *Lecture Notes in Computer Science*, pages 16–29. Springer, 2004.

# Bibliography ii

Christophe Clavier and Léo Reynaud.
**Improved blind side-channel analysis by exploitation of joint distributions of leakages.**
In Wieland Fischer and Naofumi Homma, editors, *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, volume 10529 of *Lecture Notes in Computer Science*, pages 24–44. Springer, 2017.

# Bibliography iii

Christophe Clavier, Léo Reynaud, and Antoine Wurcker.
**Quadrivariate improved blind side-channel analysis on boolean masked AES.**
In Junfeng Fan and Benedikt Gierlichs, editors, *Constructive Side-Channel Analysis and Secure Design - 9th International Workshop, COSADE 2018, Singapore, April 23-24, 2018, Proceedings*, volume 10815 of *Lecture Notes in Computer Science*, pages 153–167. Springer, 2018.

# Bibliography iv


Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel.
**Mutual information analysis.**
In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems - CHES 2008, 10th International Workshop, Washington, D.C., USA, August 10-13, 2008. Proceedings*, volume 5154 of *Lecture Notes in Computer Science*, pages 426–442. Springer, 2008.

Gilbert Goodwill, Benjamin Jun, J. Jaffe, and Pankaj Rohatgi.
**A testing methodology for side channel resistance.**
2011.

## Bibliography v

Neil Hanley, Michael Tunstall, and William P. Marnane.
**Unknown plaintext template attacks.**
In Heung Youl Youm and Moti Yung, editors, *Information Security Applications, 10th International Workshop, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers*, volume 5932 of *Lecture Notes in Computer Science*, pages 148–162. Springer, 2009.

Paul C. Kocher, Joshua Jaffe, and Benjamin Jun.
**Differential power analysis.**
In Michael J. Wiener, editor, *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

# Bibliography vi

Roman Korkikian.
**Side-channel and fault analysis in the presence of countermeasures : tools, theory, and practice.**
Theses, PSL Research University, October 2016.

Hélène Le Bouder.
**A FORMALISM FOR PHYSICAL ATTACKS ON CRYPTOGRAPHIC DEVICES AND ITS EXPLOITATION TO COMPARE AND RESEARCH NEWS ATTACKS.**
Theses, Ecole Nationale Supérieure des Mines de Saint-Etienne, October 2014.

# Bibliography vii

Yanis Linge, Cécile Dumas, and Sophie Lambert-Lacroix.
**Using the joint distributions of a cryptographic function in side channel analysis.**
*IACR Cryptology ePrint Archive*, 2013:859, 2013.