Leakage Squeezing — Defeating Instantaneous $(d+1)$th-order Correlation Power Analysis with Strictly Less Than d Masks

Sylvain Guilley, Claude Carlet, Houssem Maghrebi,
Jean-Luc Danger and Emmanuel Prouff

TELECOM ParisTech, Univ. Paris 8 & ANSSI

Wednesday June 20th 2012,
10th CryptArchi Workshop — Château de Goutelas, Marcoux

Presentation Outline

Presentation Outline

Context — Protection of Block Ciphers

Definition of a sensitive variable

Z: a sensitive variable, *i.e.* that depends

- on a unknown static key K and
- on a known dynamic plaintext/ciphertext X.

Side-Channel Analysis

Predict Z,

- despite countermeasures (*e.g.* masking with M),
- so as to distinguish the correct $K = k^\star$ from the incorrect key guesses.

Presentation Outline

Masking at Order d

Definition

Split a sensitive variable $Z \in \mathbb{F}_2^n$

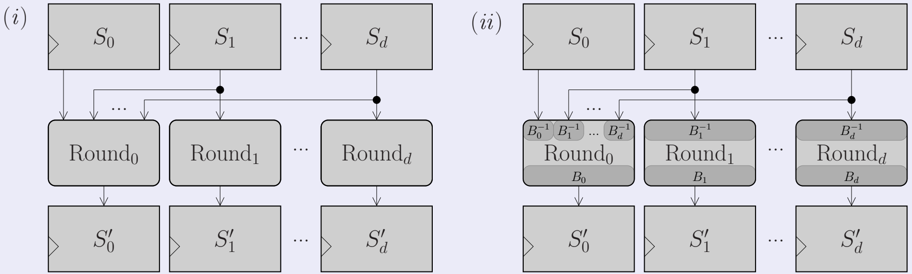
- into $d+1$ random shares, noted $\vec{S} = (S_i)_{i \in [\![0,d]\!]}$,
- in such a way that the relation $S_0 \perp \cdots \perp S_d = Z$ is satisfied, for group operation $\perp$ (*e.g.* the XOR operation in Boolean masking).

Soundness of the dth Order Masking Scheme

- Z can be deterministically reconstructed knowing the $d+1$ shares, while
- no information about Z can be extracted from strictly less than $d+1$ shares.

Example of Secure Computation

(i) Whitebox (ii) with squeezing.



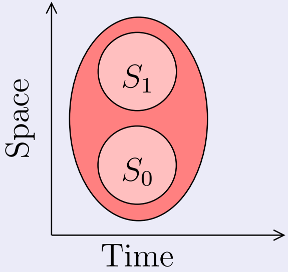
Other dth Order Sound Masking Schemes Exist...

"*Provably Secure Higher-Order Masking of AES*", [RP10].

Order of the Attack

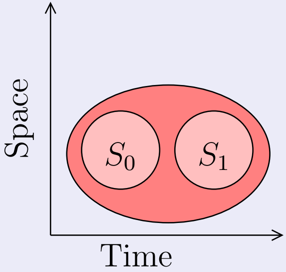
Depends on the Resolution of the Attacker

Hardware



High spatial resolution...

Software



High frequential resolution...

Leakage model: $\vec{L} = \ell_0(S_0) \overset{,}{\oplus} \ell_1(S_1)$

Independent Leaking of the Shares

Modelization

- The leakage passes through the noisy functions ℓ_i, where
- $\ell_i : X \mapsto f_i(X) + N_i$.
- Notation: $\vec{L} \doteq (L_0, \cdots, L_d) \doteq (\ell_0(S_0), \cdots, \ell_d(S_d))$.

Usual assumptions

1. Bits indiscernibility and independence: $f_i = w_H$.
   - *i.e.* f_i is a Hamming weight function.
2. Gaussian noise: $N_i \sim \mathcal{N}(0, \sigma_i^2)$.
   - For the sake of clarity, we can sometimes set: $\forall i \in [\![0, d]\!], \sigma_i = \sigma$.

How to Collect as Many Shares as Possible?

Initial Combination

- Nicknamed $\mathcal{C}_{\text{device}}$ (in reference to hardware; in software, it could also have been called $\mathcal{C}_{\text{measure}}$).
- Not chosen by the attacker.

Final Combination

- Nicknamed $\mathcal{C}_{\text{attacker}}$.
- Chosen by the attacker.

Total Combination

- Nicknamed $\mathcal{C}_{\text{total}} \doteq \mathcal{C}_{\text{attacker}} \circ \mathcal{C}_{\text{device}}$.

Notion of Attack Order

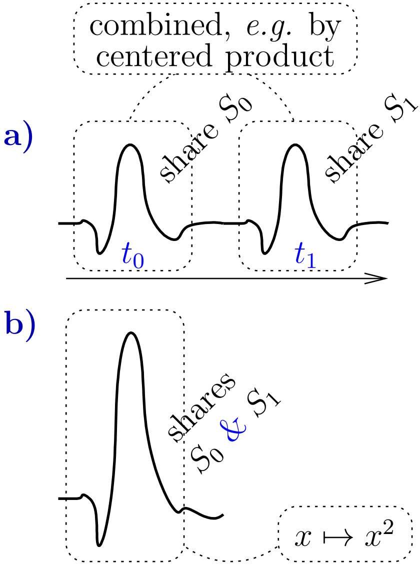
Depending the implementation is:

- **a)** Sequential, *i.e.* software, or
- **b)** Parallel, *i.e.* hardware,

exploitation of a first-order masking can be done either by:

- **a)** centered product (proved optimal in [PRB09], or
- **b)** squaring the leakage (called 2Z-DPA in [WW04]).

The common point is the *degree* 2 of the exploited leakage $\mathcal{C}_{\text{total}}(\vec{L})$. We base ourselves on this notion in the sequel.



Leakage Polynomial Decomposition

- $\mathcal{C}_{\text{total}}(\vec{L}) \doteq \sum_{\vec{\alpha}\in\mathbb{N}^{d+1}} a_{\vec{\alpha}} \cdot \vec{L}^{\vec{\alpha}}$, with $a_{\vec{\alpha}} \in \mathbb{R}$ (they can be null).

Polynomial Degree $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L}))$

- Usual definition for polynomials in $\mathbb{R}^{d+1}$ of variables $\vec{L} = (L_0, \cdots, L_d)$,
- $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L})) \doteq \max_{\vec{\alpha} \text{ s.t. } a_{\vec{\alpha}}\neq 0} ||\vec{\alpha}||_1 = \max_{\vec{\alpha} \text{ s.t. } a_{\vec{\alpha}}\neq 0} \sum_{i=0}^{d} \alpha_i$.

Algebraic Degree $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L}))$ (*aka* multivariate degree)

- Similar definition for polynomials in $\mathbb{R}[L_0, \cdots, L_d]/\left(\prod_{i=0}^{d} L_i^2 - L_i\right)$,
- α_i is counted as 1 if $\alpha_i > 0$, and as 0 otherwise.

Property

$$d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L})) \quad \geq \quad d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L})).$$

Attack Success Condition

- The attack succeeds **if and only if** the leakage meets the condition:
- $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L})) = d + 1$.

Attack Success Necessary Condition

- The attack can succeed **if** the leakage meets this condition:
- $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L})) = d + 1$.

Argument of the Talk

- This last relationship might not be a *necessary* condition.
- Indeed, we will argue it is possible to have
  $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L})) \quad > \quad d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L}))$ [*strict*].

Presentation Outline

HCI: High-Order CPA Immunity

Remark

- $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L})) \geq d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L}))$.
- But for the attack to succeed, the first condition is on $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L}))$:
  - $d_{\text{poly}}(L_0^3) = 3$, however, with a countermeasure ($d > 0$),
  - $d_{\text{alg}}(L_0^3) = 1 < d + 1 = 2$ [*i.e.* attack failure in 1st order masking].

HCI Definition

- $\text{HCI} \doteq \min \left\{ i \in \mathbb{N} \text{ such that } \exists z, \mu^i(\mathcal{C}_{\text{total}} | Z = z) \neq \mu^i(\mathcal{C}_{\text{total}}) \right\}$;
- Idem $\forall i < \text{HCI}, \forall z, \mu^i(\mathcal{C}_{\text{total}} | Z = z) = \mu^i(\mathcal{C}_{\text{total}})$ [*moments*].
- Idem $\forall i < \text{HCI}, \forall z, k^i(\mathcal{C}_{\text{total}} | Z = z) = k^i(\mathcal{C}_{\text{total}})$ [*cumulants*].
- *Because,* $\forall z, \mu^i(\mathcal{C}_{total} | Z = z)$ *are equal* $\implies \mu^i(\mathcal{C}_{total} | Z = z) = \mu^i(\mathcal{C}_{total})$ *(idem for the cumulants* k^i*).*

HCI $= d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L}))$ for common SW/HW leakages

Software leakage archetype [time extensive]

- **Identity leakage**: $\mathcal{C}_{\text{device}}(\vec{L}) = \vec{L}$,
  - Rigorously: $\mathcal{C}_{\text{device}}(\vec{L}) = \vec{L} - \mathbb{E}(\vec{L})$.
- Attack strategy: $\mathcal{C}_{\text{total}}(\vec{L}) = \mathcal{C}_{\text{device}}(\vec{L})^{\vec{i}}$, with $\vec{i} \in (\mathbb{N}^{\star})^{d+1}$;
  - $i = ||\vec{i}||_1 \geq d+1$ because $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L})) = \min\{i, d+1\}$,
  - and as small as possible since SNR $\leq \sigma^{-2i}$.

Hardware leakage archetype [time intensive]

- **Sum leakage**: $\mathcal{C}_{\text{device}}(\vec{L}) = \sum_{i=0}^{d} L_i$.
  - Rigorously: $\mathcal{C}_{\text{device}}(\vec{L}) = \sum_{i=0}^{d} L_i - \mathbb{E}(\sum_{i=0}^{d} L_i)$.
- Attack strategy: $\mathcal{C}_{\text{total}}(\vec{L}) = \mathcal{C}_{\text{device}}(\vec{L})^{i}$ with $i \in [\![d+1, +\infty [\![$;
  - $i \geq d+1$ because $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L})) = \min\{i, d+1\}$,
  - and as small as possible since SNR $\leq \sigma^{-2i}$.

HCI is an Attack Metric

HO-CPA: Value-based Attacks

- $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) = \frac{\text{Var}(\mathbb{E}(\mathcal{C}_{\text{total}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))} = \frac{\text{Var}(\mathbb{E}(\mathcal{C}^i_{\text{device}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))}$. [PRB09]
- By definition of HCI, the largest i such that $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) \neq 0$ is $i = \text{HCI}$.

MIA: Distribution-based Attacks

- There's no notion of order in MIA, but we have this theorem [LB10]:

$$\mathrm{I}(\mathcal{C}_{\text{total}}(\vec{L}); Z) = \sum_{i=0}^{+\infty} \frac{1}{2 \cdot i!} \sum_{z} \mathrm{P}[z] \frac{\left(k_i(\mathcal{C}_{\text{total}}(\vec{L}) \mid Z = z) - k_i(\mathcal{C}_{\text{total}}(\vec{L}))\right)^2}{\left(\sigma^2_{\text{tot}} + \sigma^2\right)^i} . \quad (1)$$

HCI is an Attack Metric

HO-CPA: Value-based Attacks

- $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) = \frac{\text{Var}(\mathbb{E}(\mathcal{C}_{\text{total}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))} = \frac{\text{Var}(\mu^i(\mathcal{C}_{\text{device}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))}$. [PRB09]
- By definition of HCI, the largest i such that $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) \neq 0$ is $i = \text{HCI}$.

MIA: Distribution-based Attacks

- There's no notion of order in MIA, but we have this theorem [LB10]:

$$\text{I}(\mathcal{C}_{\text{total}}(\vec{L}); Z) = \sum_{i=0}^{+\infty} \frac{1}{2 \cdot i!} \sum_z \text{P}[z] \frac{\left(k_i(\mathcal{C}_{\text{total}}(\vec{L}) \mid Z = z) - k_i(\mathcal{C}_{\text{total}}(\vec{L}))\right)^2}{\left(\sigma_{\text{tot}}^2 + \sigma^2\right)^i} . \quad (1)$$

HCI is an Attack Metric

HO-CPA: Value-based Attacks

- $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) = \frac{\text{Var}(\mathbb{E}(\mathcal{C}_{\text{total}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))} = \frac{\text{Var}(\mu^i(\mathcal{C}_{\text{device}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))}$. [PRB09]
- By definition of HCI, the largest i such that $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) \neq 0$ is $i = \text{HCI}$.

MIA: Distribution-based Attacks

- There's no notion of order in MIA, but we have this theorem [LB10]:

$$\text{I}(\mathcal{C}_{\text{total}}(\vec{L}); Z) = \sum_{i=\text{HCI}}^{+\infty} \frac{1}{2 \cdot i!} \sum_{z} \text{P}[z] \frac{\left(k_i(\mathcal{C}_{\text{total}}(\vec{L}) \mid Z=z) - k_i(\mathcal{C}_{\text{total}}(\vec{L}))\right)^2}{\left(\sigma_{\text{tot}}^2 + \sigma^2\right)^i} . \quad (1)$$

HCI is an Attack Metric

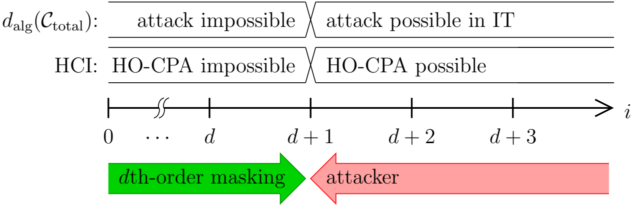
HO-CPA: Value-based Attacks

- $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) = \frac{\text{Var}(\mathbb{E}(\mathcal{C}_{\text{total}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))} = \frac{\text{Var}(\mu^i(\mathcal{C}_{\text{device}}(\vec{L})|Z))}{\text{Var}(\mathcal{C}_{\text{total}}(\vec{L}))}$. [PRB09]
- By definition of HCI, the largest i such that $\rho(\mathcal{C}_{\text{total}}(\vec{L}), Z) \neq 0$ is $i = \text{HCI}$.

MIA: Distribution-based Attacks

- There's no notion of order in MIA, but we have this theorem [LB10]:

$$\text{I}(\mathcal{C}_{\text{total}}(\vec{L}); Z) = \sum_{i=\text{HCI}}^{+\infty} \frac{1}{2 \cdot i!} \sum_{z} \text{P}[z] \frac{\left(k_i(\mathcal{C}_{\text{total}}(\vec{L}) \mid Z = z) - k_i(\mathcal{C}_{\text{total}}(\vec{L}))\right)^2}{\left(\sigma_{\text{tot}}^2 + \sigma^2\right)^i} = \mathcal{O}\left(\sigma^{-2\times\text{HCI}}\right) . \quad (1)$$



Defender

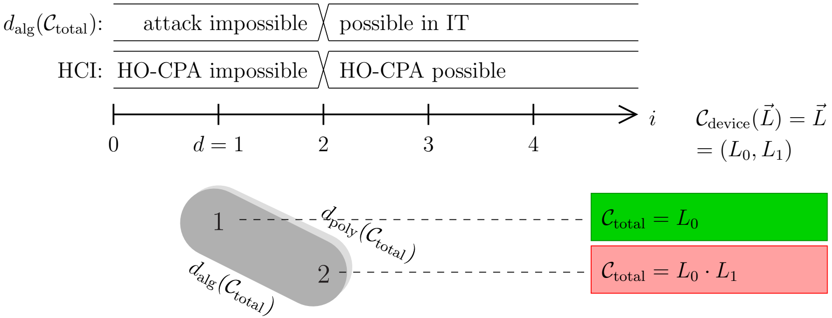
- Increase $d_{\text{alg}}(\mathcal{C}_{\text{total}}(\vec{L}))$,
- because from the information theory standpoint, no attack can succeed w/o combining all the $d+1$ shares.

Attacker

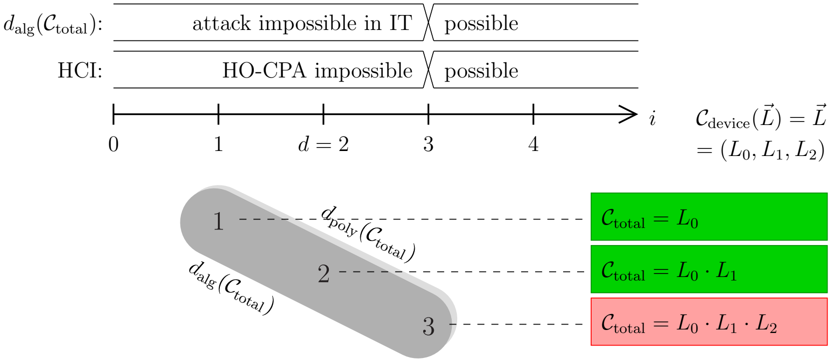
- Decrease $d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L}))$ (= HCI for power $\mathcal{C}_{\text{attacker}}$),
- because the SNR decreases exponentially:
  - $\text{Var}(\mathcal{C}_{\text{total}}(\vec{L})|\vec{S}) \geq \sigma^{2d_{\text{poly}}(\mathcal{C}_{\text{total}}(\vec{L}))}$.

Presentation Outline

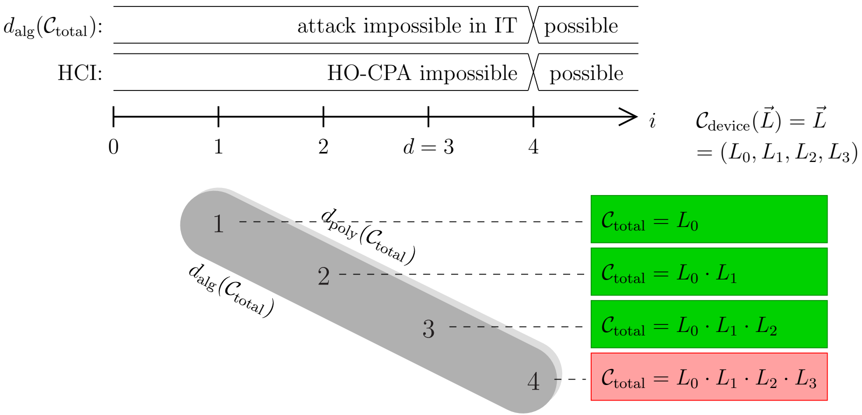
No Leakage Squeezing: $n = 4, d = 1, \mathrm{HCI} = 2$



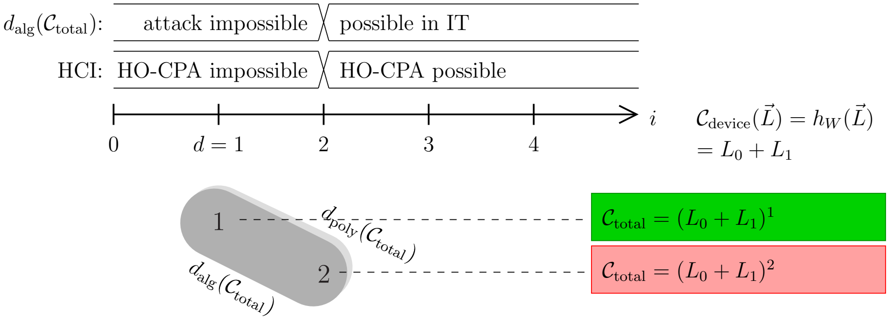
No Leakage Squeezing: $n = 4, d = 2, \text{HCI} = 3$



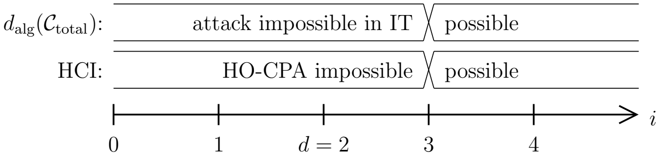
No Leakage Squeezing: $n = 4, d = 3, \mathrm{HCI} = 4$



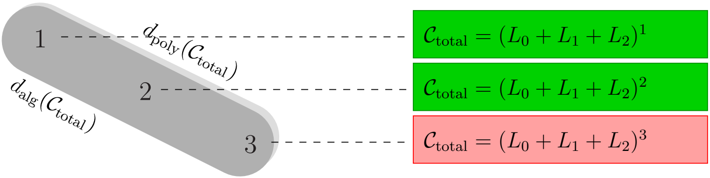
No Leakage Squeezing: $n = 4, d = 1, \mathrm{HCI} = 2$



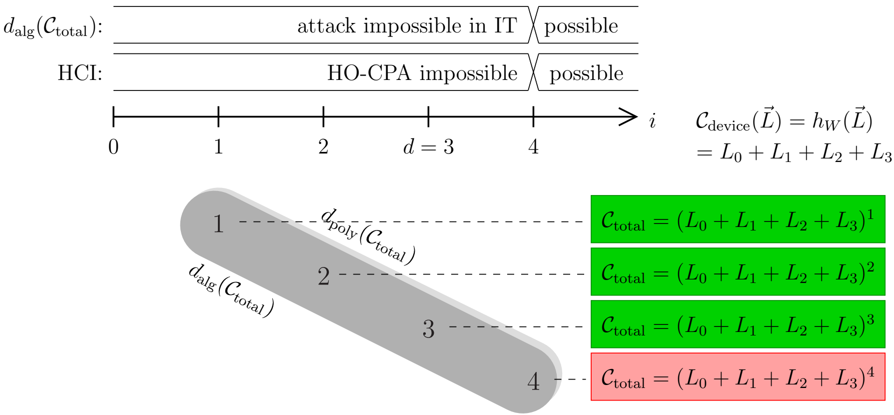
No Leakage Squeezing: $n = 4, d = 2, \mathrm{HCI} = 3$

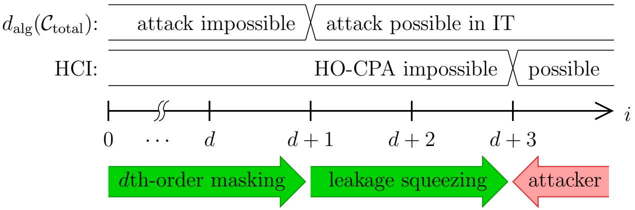


$$\mathcal{C}_{\mathrm{device}}(\vec{L}) = h_W(\vec{L}) = L_0 + L_1 + L_2$$



No Leakage Squeezing: $n = 4, d = 3, \mathrm{HCI} = 4$





Goal

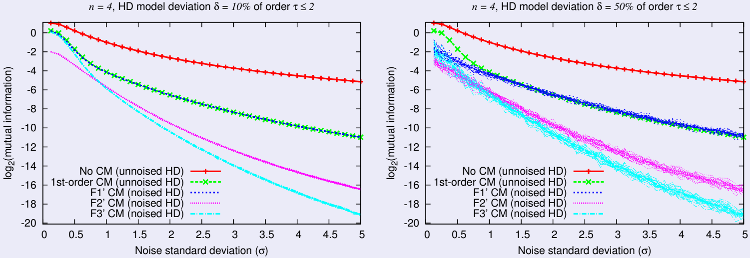
- Save masks and/or
- reduce the attacker's SNR.

Principle

- Replace S_i by $B_i(S_i)$,
- when B_i is linear, we note $B_i : X \mapsto M_i \times X$, with $M_i \in (\mathbb{F}_2^n)^2$.

Hamming Weight Leakage is Important

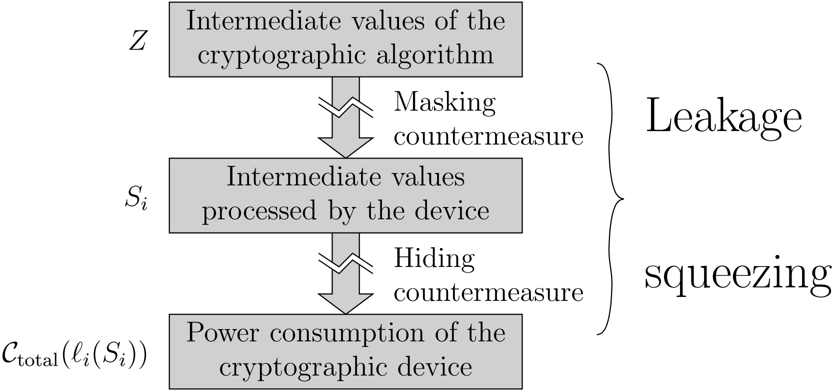
- The leakage squeezing works only because $f_i = w_H$
  - at least approximately;
- Prior characterization with stochastic model increases the confidence.



Because it adapts to both Hamming **weight** and **distance** [MM12]

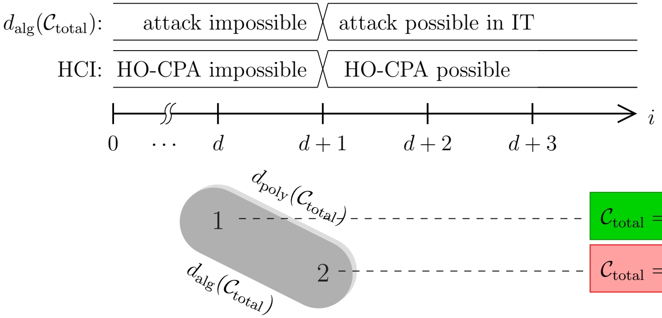
- Hamming weight: $f_i(X) = w_H(B(X))$.
- Hamming distance: $\tilde{f}_i(X, X') = w_H(B(X) \oplus B(X')) = w_H(B(X \oplus X')) = f_i(X \oplus X') = f_i(\Delta X)$.

The Big Picture



- **Shares** make up the **masking**, that is enhanced by
- **indiscernibility** of the bits (*i.e.* **hiding**).

No Leakage Squeezing: $n = 4, d = 1, \mathrm{HCI} = 2$

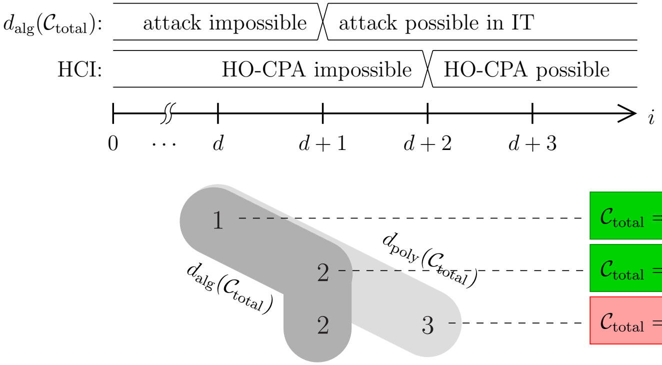


$$M_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{C}_{\mathrm{total}} = (\ell_0(S_0) + \ell_1(M_1 \times S_1))^1$$

$$\mathcal{C}_{\mathrm{total}} = (\ell_0(S_0) + \ell_1(M_1 \times S_1))^2$$

Leakage squeezing: $n = 4, d = 1, \mathrm{HCI} = 3$



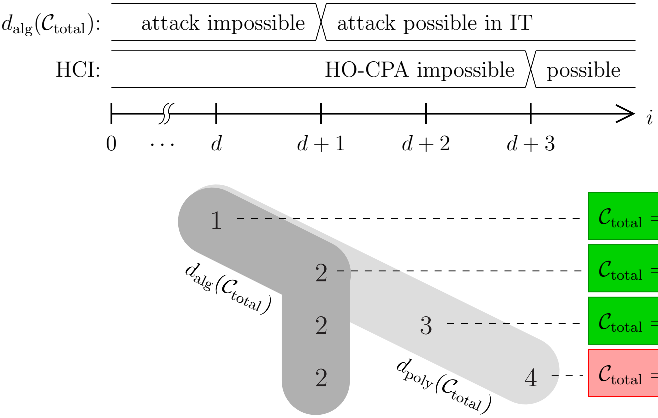
$$M_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

$$\mathcal{C}_{\mathrm{total}} = (\ell_0(S_0) + \ell_1(M_2 \times S_1))^1$$

$$\mathcal{C}_{\mathrm{total}} = (\ell_0(S_0) + \ell_1(M_2 \times S_1))^2$$

$$\mathcal{C}_{\mathrm{total}} = (\ell_0(S_0) + \ell_1(M_2 \times S_1))^3$$

Leakage squeezing: $n = 4, d = 1, \mathrm{HCI} = 4$



$$M_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$\mathcal{C}_{\text{total}} = (\ell_0(S_0) + \ell_1(M_3 \times S_1))^1$

$\mathcal{C}_{\text{total}} = (\ell_0(S_0) + \ell_1(M_3 \times S_1))^2$

$\mathcal{C}_{\text{total}} = (\ell_0(S_0) + \ell_1(M_3 \times S_1))^3$

$\mathcal{C}_{\text{total}} = (\ell_0(S_0) + \ell_1(M_3 \times S_1))^4$

Problem Statement for $d = 1$ Whatever n

Specification

- $\forall i <$ HCI, $\mu^i(\mathcal{C}_{\text{device}}(\vec{L})|Z = z)$ must not depend on z.

In Hardware $(S_0, S_1) = (Z \oplus M, M)$

- $(w_H(z \oplus M) + w_H \circ B(M))^i = \sum_{j=0}^{i} \binom{i}{j} w_H(z \oplus M)^i \cdot w_H \circ B(M)^{j-i}$.
- Idem: $\forall p, q$ such that $p + q <$ HCI, $\mathbb{E}(w_H(z \oplus M)^p \cdot w_H \circ B(M)^q)$ does not depend on z.

Theorem

- Idem: $\widehat{w_H^p}(a) \cdot \widehat{w_H \circ B^q}(a) = \text{cst} \times \delta(a)$.

Proof Fourier transform: $\widehat{f}(a) \doteq \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x \cdot a}$

- Fourier of a constant (resp. convolution) is a Dirac (resp. product).

Property

- $\widehat{w_H^p}(a) = 0 \iff w_H(a) > p$.

Problem Equivalent Formulation

- Find B such that $\forall a \neq 0, w_H(a) \leq p \Longrightarrow \widehat{w_H \circ B^q}(a) = 0$.

Some Linear Solutions

HCI = 2	HCI = 3	HCI = 4
$M_1 = \mathrm{Id}_4$	$M_2 = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$	$M_3 = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$
$M_1^{-1} = \mathrm{Id}_4$	$M_2^{-1} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$	$M_3^{-1} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$

Presentation Outline

Prior Belief

- If d masks are used, then:
  - combining $d+1$ samples (software) or
  - raising the traces at power $d+1$ (hardware)
- **suffice** to break the concealed keys.

Leakage Squeezing

- If d masks are used, then:
  - combining $\mathsf{HCI} > d+1$ samples (software) or
  - raising the traces at power $\mathsf{HCI} > d+1$ (hardware)
- **are necessary** to break the key via the traces.

Attack Performance is Reduced

- HO-CPA of order HCI are required,
- $\mathsf{MI} = \mathcal{O}(\sigma^{-2\cdot\mathsf{HCI}})$.

Perspectives

Non-linear bijections B:

- In distance: problem is solved [MGCD12]
- In values: **open issue**

- How to adapt the *leakage squeezing* to a leakage model different than $f_i = h_W$ (*i.e.* the Hamming weight),
- for instance characterized by a stochastic approach [SLP05]: $f_i(X) = \sum_{\vec{i} \in \mathbb{F}_2^n} \beta_{\vec{i}} X^{\vec{i}}$.

- HCI depends on n... Does focusing on smaller parts help?
- High-order leakage squeezing

Leakage Squeezing — Defeating Instantaneous $(d+1)$th-order Correlation Power Analysis with Strictly Less Than d Masks

Sylvain Guilley, Claude Carlet, Houssem Maghrebi,
Jean-Luc Danger and Emmanuel Prouff

TELECOM ParisTech, Univ. Paris 8 & ANSSI

Wednesday June 20th 2012,
10th CryptArchi Workshop — Château de Goutelas, Marcoux

References I

Thanh-Ha Le and Maël Berthier.
Mutual Information Analysis under the View of Higher-Order Statistics.
In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC*, volume 6434 of *LNCS*, pages 285–300. Springer, 2010.

Houssem Maghrebi, Sylvain Guilley, Claude Carlet, and Jean-Luc Danger.
Optimal First-Order Masking with Linear and Non-Linear Bijections.
In *AFRICACRYPT*, LNCS. Springer, July 10-12 2012.
Al Akhawayn University in Ifrane, Morocco.

Houssem Maghrebi, Sylvain Guilley, and Jean-Luc Danger.
Leakage Squeezing Countermeasure Against High-Order Attacks.
In *WISTP*, volume 6633 of *LNCS*, pages 208–223. Springer, June 1-3 2011.
Heraklion, Greece. DOI: 10.1007/978-3-642-21040-2_14.

Amir Moradi and Oliver Mischke.
How Far Should Theory be from Practice? Evaluation of a Countermeasure.
In *CHES*, September 9-12 2012.
Leuven, Belgium.

Emmanuel Prouff, Matthieu Rivain, and Régis Bevan.
Statistical Analysis of Second Order Differential Power Analysis.
IEEE Trans. Computers, 58(6):799–811, 2009.

Matthieu Rivain and Emmanuel Prouff.
Provably Secure Higher-Order Masking of AES.
In Stefan Mangard and François-Xavier Standaert, editors, *CHES*, volume 6225 of *LNCS*, pages 413–427. Springer, 2010.

References II

Werner Schindler, Kerstin Lemke, and Christof Paar.
A Stochastic Model for Differential Side Channel Cryptanalysis.
In LNCS, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005.
Edinburgh, Scotland, UK.

Jason Waddle and David Wagner.
Towards Efficient Second-Order Power Analysis.
In *CHES*, volume 3156 of *LNCS*, pages 1–15. Springer, 2004.
Cambridge, MA, USA.