Exotic Leakage Models

Moulay Abdelaziz EL AABID[1,2], Sylvain GUILLEY[1,3],
Shivam BHASIN[1] and Jean-Luc DANGER[1,3].

[1] Institut TELECOM / TELECOM-ParisTech, CNRS LTCI (UMR 5141);
[2] Université Paris 8;
[3] Secure-IC S.A.S.

CryptArchi (Bochum, Germany),
June 15-18th 2011.

Presentation Outline

Presentation Outline

Leakage Models

Notions of Side-Channel Analysis (SCA)

- The leakage of a cryptographic function, as measured by an adversary, is a **probability law** of the inputs / the outputs;
- Interesting leakage depends on **manageable parts** of the secret key;
- It involves a so-called **sensitive variable**;
- Once a leakage function is known, it is straightforward to devise a **distinguisher**;
- It will hopefully **exploit** the leakage ...
- ... for a successful **key retrieval**.

Iterative Hardwired DES Example (1/2)

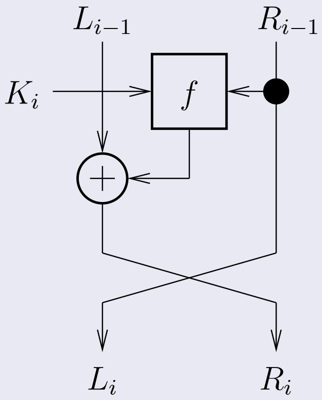
The Exact Leakage Model

- At date $i = 1$, $\mathcal{L}(LR_0, LR_1) \sim \mathrm{HW}(LR_0 \oplus LR_1) + \mathcal{N}(0, \sigma^2)$;
- For the specific example of DES, $f(R_0, K_1) = \mathrm{P} \circ \mathrm{S}(\mathrm{E}(R_0) \oplus K_1)$;
- Hence: $\mathcal{L}(LR_0, LR_1) \sim \sum_{i=1}^{32} L_i \oplus R_i + \sum_{s=1}^{8} \mathrm{HW}\left(\mathrm{S}_s(\mathrm{E}(R_0) \oplus K_1)[\![6(s-1)+1, 6s]\!] \oplus \mathrm{P}^{-1}(L_0 \oplus R_0)[\![4(s-1)+1, 4s]\!]\right) + \mathcal{N}(0, \sigma^2)$.

Color code:

left (unsensitive), right (sensitive) and noise.

Feistel Block



Iterative Hardwired DES Example (2/2)

Attack of the sbox $s \in [\![1, 8]\!]$

$$\mathcal{L}(\text{Sbox } s) \sim \text{HW}\left(\begin{array}{l} S_s(E(R_0) \oplus K_1)[\![6(s-1)+1, 6s]\!] \\ \oplus P^{-1}(L_0 \oplus R_0)[\![4(s-1)+1, 4s]\!] \end{array} \right) + \mathcal{N}(60/2, 60/4 + \sigma^2),$$

since the expectation of a random bit B is $1/2$ and its variance $\sum_{b \in \{0,1\}} \text{P}[B = b] \times (b - 1/2)^2 = 1/2 \times (1/4 + 1/4) = 1/4$.
Regarding the noise:

- $(64 - 4)/4 = 60/4$: algorithmic noise (left + rest of right);
- σ^2: measurement noise.

In ASIC, $60/4 \gg \sigma^2$ whereas in FPGA, $60/4 \ll \sigma^2$ (*softwarity* versus *hardwarity*).

Leaking Variables and Leakage Models

- In the previous example, a leakage model uses $4 \times 2 + 6 = 14$ **variables** from the plain text (4 initial & 4+6 final):
  - $R_{\{32,1,2,3,4,5\}}$ on the one hand, and
  - $R_{\mathrm{P}^{-1}\{1,2,3,4\}}$ and $L_{\mathrm{P}^{-1}\{1,2,3,4\}}$ on the other hand. It is also equal to $R_{\{9,17,23,31\}}$ and $L_{\{9,17,23,31\}}$.
- Then, those variables leak through a Hamming distance **model**.
- All attacks need to know the leaking **variables**, to realize a partitioning (2^{14} of them):
  - Template attacks (TA)
  - Mutual information analysis (MIA)
- Model-based attacks need an approximation of leakage **model**:
  - TA and MIA (less partitions, hence better distribution estimation),
  - Stochastic attacks, CPA.

Universal Leakage Model Characterization

- Build the templates $\forall k, \mathcal{L}(\text{inputs}, K) \mid K = k$.
- Issue: for DES, the profiling takes $2^{64} \times 2^{56} \times 1,000$ encryptions...

Kocher's mono-bit selection function

- Pick a bit B: easy enough and no leakage model.
- But can fail, *e.g.* on HW:
  $\text{Cov}(B, B \oplus L + \mathcal{N}(\mu, \sigma^2)) = 0$ if B and L are decorrelated.
- Typically L is the value of the left register that is `XORed` at the end of the round with B.

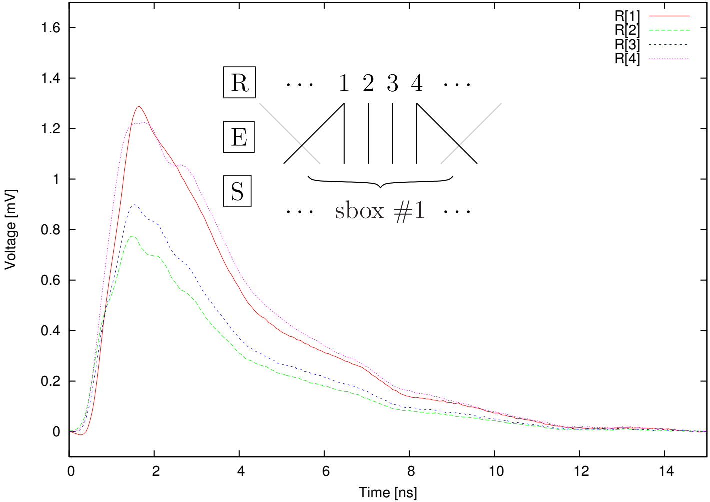
Examples

Some Empirical Approaches

- In [RRST02] (S&P'02), the authors use the memory bank where the data is written to;
- In [BCO04] (CHES'04), the authors use as initial state the memory bank where the data is written to;
- In [BP10] (CHES'10), the authors exhibit leakage functions for six SHA-3 candidates;
- In [GSM+10] (LatinCrypt'10), the authors find leakage models for stream ciphers.

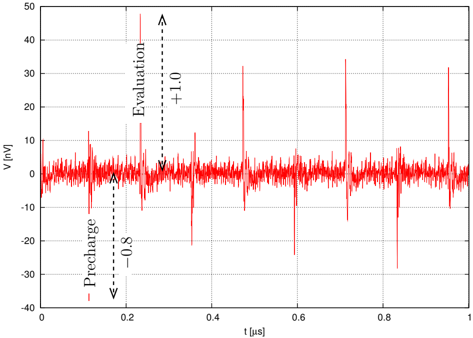
Presentation Outline

Hamming distance .... with nonequivalent bits



Hamming distance ....with nonequivalent transitions

EM field close to a Stratix FPGA implementing a DES in WDDL [SGD+09].

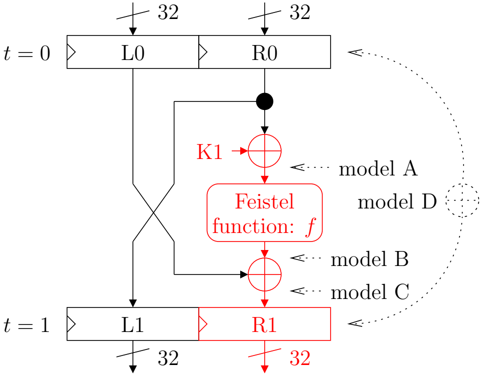


⇒ signed-distance leakage model [PSQ07]

$1 \cdot x_{\text{initial}} \wedge \overline{x_{\text{final}}} + (1-\delta) \cdot \overline{x_{\text{initial}}} \wedge x_{\text{final}}$, with $\delta \in \mathbb{R}$ (here $\delta \approx 1.8$).

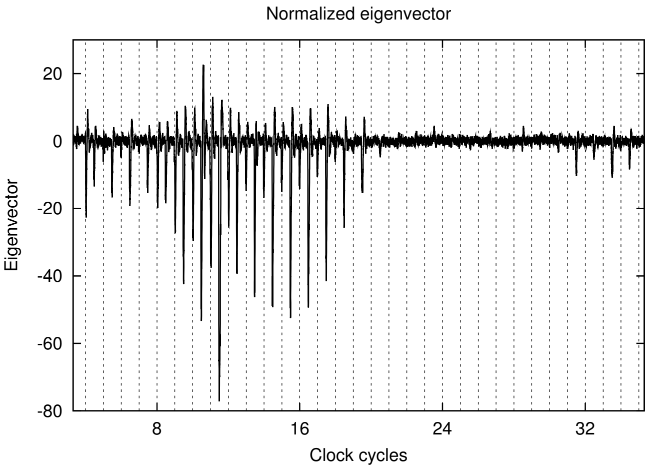
Various Leakage Models for DES [EG10]

Attack on the first round of DES

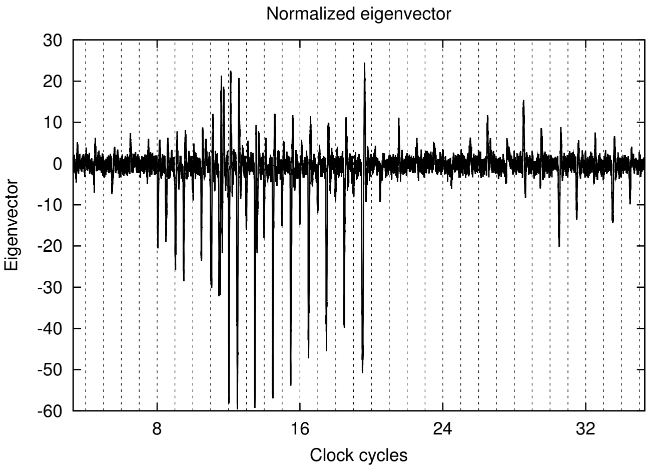


Caption: black = known values; red = unknown sensitive values

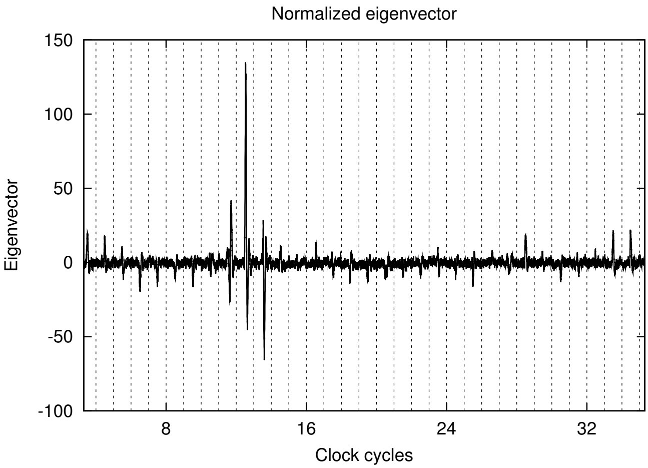
Eigenvector for model A



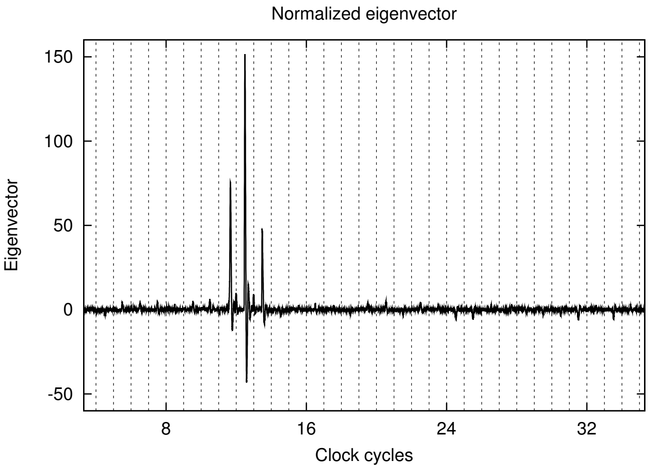
Eigenvector for model B



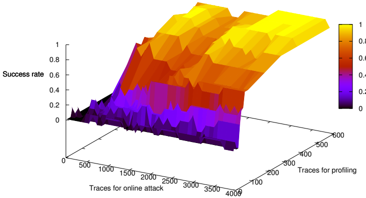
Eigenvector for model C



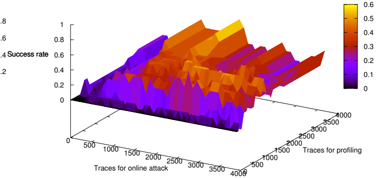
Eigenvector for model D



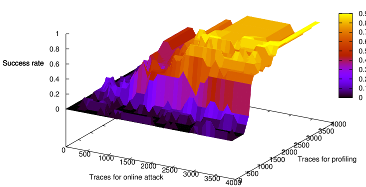
Finding the best leakage models is not obvious [EG10]



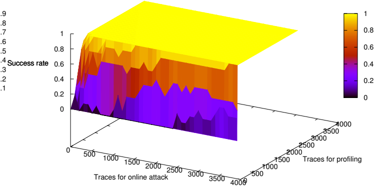
Success rate for model A.



Success rate for model B.

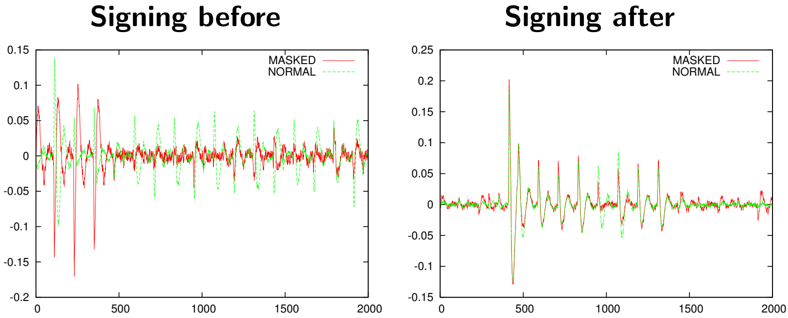


Success rate for model C.



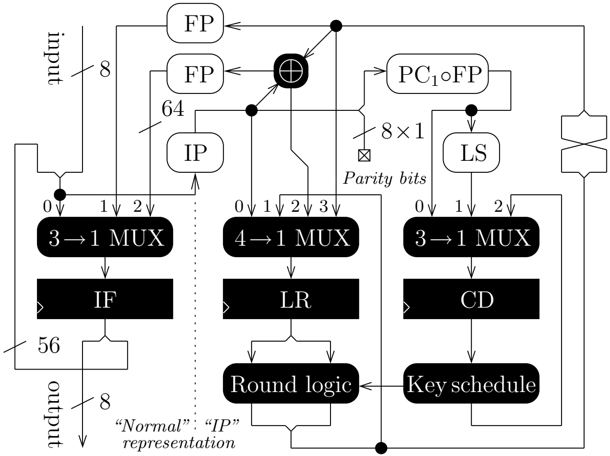
Success rate for model D.

Hamming Weight Model (A): Deeper Investigations



Memo: encryption starts around sample 400.

The DES Crypto-Processor has an 8-bit Interface



Leakage Explained: .... unsensitive

During the 8 cycles that precede the encryption:

```
M2 = L8    overwrites KEY58 => CD0[ 9] => CD1[ 8] => K[18]
M4 = L16   overwrites KEY60 => CD0[25] => CD1[24] => K[ 4]
M6 = L24   overwrites KEY62 => CD0[37] => CD1[36] => K[46]
M8 = L32   overwrites KEY64 => PARITY  =>
M1 = R8    overwrites KEY57 => CD0[57] => CD1[56] => K[40]
M3 = R16   overwrites KEY59 => CD0[17] => CD1[16] => K[18]
M5 = R24   overwrites KEY61 => CD0[45] => CD1[44] => K[18]
M7 = R32   overwrites KEY63 => CD0[29] => CD1[28] => K[ 8]
```

Then, during the 8 cycles that follow:

```
M58 = L1   is overwritten by a constant
M60 = L9   is overwritten by a constant
M62 = L17  is overwritten by a constant
M64 = L25  is overwritten by a constant
M57 = R1   is overwritten by a constant
M59 = R9   is overwritten by a constant
M61 = R17  is overwritten by a constant
M63 = R25  is overwritten by a constant
```

Presentation Outline

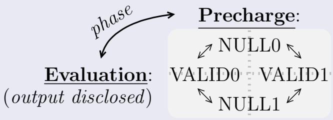
1. Introduction about Leakage Models
   - Definitions
   - Methodology to Characterize Leakage Models
2. Leakage Models in the Absence of Counter-Measures
3. Leakage Models for Hiding Logics
4. Leakage Models for Masked Logics
5. Conclusions and Perspectives

Hiding (Counter-Measure 1/2)

$a \leftrightarrow (a_f, a_t)$ DPL representation:

- a is **VALID** if $\boxed{a_f \oplus a_t = 1}$.
  VALID $\doteq$ {VALID0, VALID1} or VALID $\doteq \{(1,0),(0,1)\}$.
- a is **NULL** if $\boxed{a_f \oplus a_t = 0}$.
  NULL $\doteq$ {NULL0, NULL1} or NULL $\doteq \{(0,0),(1,1)\}$.

Protocol:



Flavors of Dual-rail with Precharge Logics (DPLs):

- **DPL w/ EPE**†: $\exists a$ VALID, $f(a, \text{NULL}) =$ VALID. Cheapest, but also less secure.
- **DPL w/o EPE**† [BDF+09]: $\forall a$ VALID, $f(a, \text{NULL}) =$ NULL. More expansive, but more secure.

†: EPE = Early Propagation Effect [SS06]

Leakage Simplification for DPL

- No history effect: **sensitive variables** leak plain.
- If DPL is perfectly implemented, there is no leakage (at least in theory).
- Thus DPL makes up a unique testbed to assess the amount of interaction between bits.

Stochastic Characterization [SLP05, Sch08]

Approximation of the leakage model at order $d \in \mathbb{N}^*$

$$\mathcal{L}(x) = \sum_{I \in \mathbb{F}_2^n | \mathrm{HW}(I) \leq d} \beta_I \cdot x^I \quad \text{where } x \in \mathbb{F}_2^n .$$

Notation: $x^I = \bigwedge_{i=1}^n x_i^{I[i]}$. Example: $x^{\{0,1,1,0,0,0,0,1\}} = x_6 \wedge x_5 \wedge x_0$.

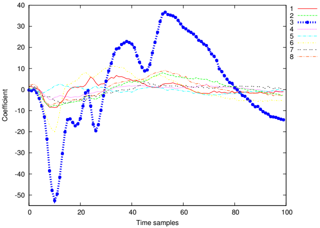
Coefficients $\beta_I \in \mathbb{R}$ (β_0 is non-informative)

- $n = 8$ of them for a linear model ($d = 1$),
- $+= \binom{8}{2} = 28$ of them for a quadratic model ($d = 2$),
- $\cdots$
- $+= \binom{8}{8}$ for a model at highest order ($d = 8$ or templates, with $2^n = \sum_{d=0}^n \binom{n}{d}$ coefficients).

Characterization results at order $d = 1$ (*traces:* [BGF+10])

Depending on the attack, leaking one bit might not be serious if the leakage function is bitwise:

- $\mathrm{I}(O; X \oplus k) = \mathrm{I}(O; X \oplus 0) = \mathrm{I}(O; X \oplus 1)$, or
- $\left|\rho(O; X \oplus \overline{k})\right| = \left|\rho(O; \overline{X \oplus k})\right| = \left|\rho(O; 1 - X \oplus k)\right| = \left|-\rho(O; X \oplus k)\right| = \left|\rho(O; X \oplus k)\right|, \quad \forall k.$



Harmful leakages are either non-injective or involve an extra random variable.

Basis vectors for quadratic leakage

$\mathrm{I}\left(X_i \wedge Y_j ; X_j\right) > 0$

$\mathrm{I}\left(X_i \wedge Y_j ; X_j\right) =$
$\mathrm{H}\left(X_i \wedge Y_j\right) - \mathrm{H}\left(X_i \wedge Y_j \mid X_j\right)$.

X_i	X_j	$Z = X_i \wedge X_j$
0	0	0
0	1	0
1	0	0
1	1	1

$\Rightarrow$ **inappropriate**

$\mathrm{I}\left(\left(X_i - \frac{1}{2}\right) \cdot \left(Y_j - \frac{1}{2}\right) ; \left(X_j - \frac{1}{2}\right)\right) = 0$

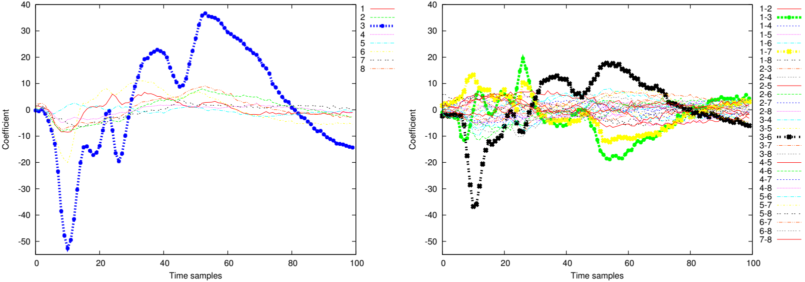
$\mathrm{I}\left(\left(X_i - \frac{1}{2}\right) \cdot \left(Y_j - \frac{1}{2}\right) ; \left(X_j - \frac{1}{2}\right)\right) =$
$\mathrm{H}\left(\left(X_i - \frac{1}{2}\right) \cdot \left(Y_j - \frac{1}{2}\right)\right) -$
$\mathrm{H}\left(\left(X_i - \frac{1}{2}\right) \cdot \left(Y_j - \frac{1}{2}\right) \mid \left(X_j - \frac{1}{2}\right)\right)$.

X_i	X_j	$\left(X_i - \frac{1}{2}\right) \cdot \left(Y_j - \frac{1}{2}\right)$
0	0	$+\frac{1}{4}$
0	1	$-\frac{1}{4}$
1	0	$-\frac{1}{4}$
1	1	$+\frac{1}{4}$

$\Rightarrow$ **appropriate**

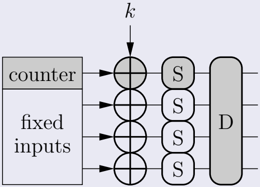
Characterization results at order $d = 2$ (*traces:* [BGF+10])

$$\mathcal{L}(x) = \sum_{i=1}^{n} \beta_i \cdot \left(x_i - \frac{1}{2}\right) + \sum_{i \neq j} \beta_{i,j} \cdot \left(x_i - \frac{1}{2}\right) \cdot \left(x_j - \frac{1}{2}\right) .$$

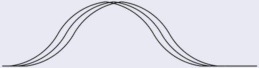


Estimating the leakage does not always translate into attacks

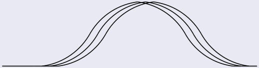
Ex. 1: Uncentered Templates



$\forall k[0]$, $k[1..3]$ fixed:



$\forall k[0]$, with different $k[1..3]$:



Ex. 2: Mutual information of bijective partitionings

$\mathsf{I}(O; \mathsf{S}^{-1}(X \oplus k) \oplus 0x00) = \mathsf{I}(O; X \oplus k)) = \mathsf{I}(O; X)$ if k is constant.

Presentation Outline

Principle

Principle (of masking at order d)

- Every variable $s \in \mathbb{F}_2^n$, potentially sensible, is represented as a set of shares $\{s_0, s_1, \cdots, s_d\} \in (\mathbb{F}_2^n)^{d+1}$.
- To reconstruct s, all the s_i are required.
- Example: $d = 1$, $\boxed{s \doteq s_0 \oplus s_1}$.

Leakage

- In masking schemes implemented in software, several leakage functions are considered (sum, absolute difference, centered product, *etc*).
- In [PR10, §4.3], the authors consider every share leaks independently.

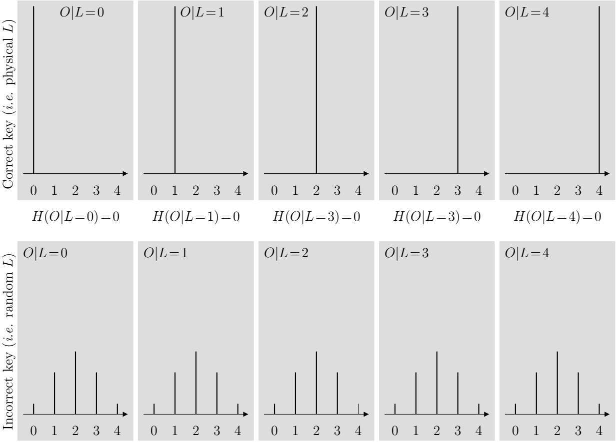
Pathological Leakage Models

- $\mathcal{L}(s_i) = \text{HW}\left(\oplus_{i=0}^{d} s_i\right)$: auto-demasking:
  - $m \oplus x \longrightarrow m$ leaks...
- $\mathcal{L}(s_i) = \delta\left(\oplus_{i=0}^{d} s_i = v\right)$: glitches [MS06].
  - When the shares take the value v (that can be independent of the masks), an highly-consuming glitch appears.
- $\mathcal{L}(x) = x[1] \oplus x[0]$:
  - is the optimal function of a masking that leaks $\text{HW}[X \oplus M]$ (see [PRB09]) if $n = 2$ and $M \sim \mathcal{U}\left(\{01, 10\} \subsetneq \mathbb{F}_2^n\right)$.
- $\mathcal{L}(x) = \text{HW}(x)$ ...
  - with a (first order) CPA on the *squared centered* traces. See next slides at Boolean 2O masking.

Attacks on masking (*w/o mask*) (1/3)

$\Rightarrow$ 1st-order dependence

$p(L=0)=1/16$ $p(L=1)=4/16$ $p(L=2)=6/16$ $p(L=3)=4/16$ $p(L=4)=1/16$

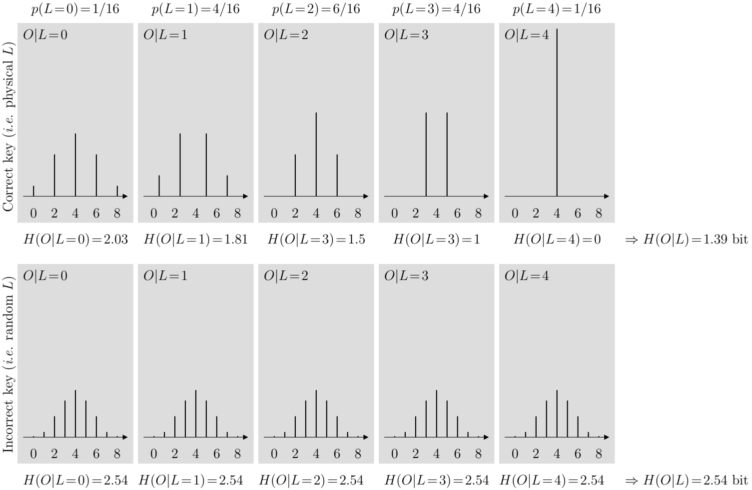


$H(O|L=0)=0$ $H(O|L=1)=0$ $H(O|L=3)=0$ $H(O|L=3)=0$ $H(O|L=4)=0$ $\Rightarrow H(O|L)=0$ bit

$H(O|L=0)=2.03$ $H(O|L=1)=2.03$ $H(O|L=2)=2.03$ $H(O|L=3)=2.03$ $H(O|L=4)=2.03$ $\Rightarrow H(O|L)=2.03$ bit

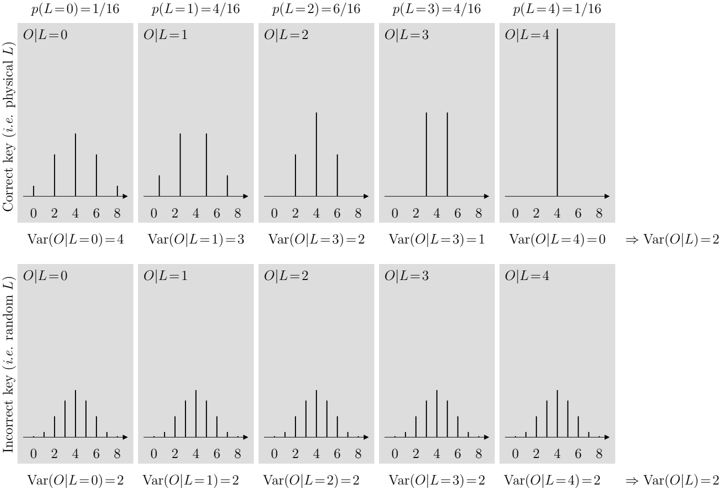
Attacks on masking (*w/ mask*) (2/3)

⇒ 2nd-order dependence



Attacks on masking (*w/ mask*) (3/3)

$\Rightarrow$ 2nd-order CPA



Presentation Outline

Conclusions

- Some partitioning can lead to differences, that are not sensitive!
  $\Rightarrow$ it is important to vary the key.
- Models can be more or less sophisticated

Perspectives

- A method to find the best partitioning, blindly.
- It is **the** side-channel (or SCARE) problem, to determine the hidden vulnerabilities.
- For DPL logics:
  - It is sufficient to test all the n nodes exhaustively on the t samples [BGF+10], hence a *constructive* proof-of-security ($\mathcal{O}(n \times t)$);
  - Harder for masking schemes! ($\mathcal{O}(n \times t^d)$ at order d).

References

[BCO04] Éric Brier, Christophe Clavier, and Francis Olivier.
Correlation Power Analysis with a Leakage Model.
In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004.
Cambridge, MA, USA.

[BDF+09] Shivam Bhasin, Jean-Luc Danger, Florent Flament, Tarik Graba, Sylvain Guilley, Yves Mathieu, Maxime Nassar, Laurent Sauvage, and Nidhal Selmane.
Combined SCA and DFA Countermeasures Integrable in a FPGA Design Flow.
In *ReConFig*, pages 213–218. IEEE Computer Society, December 9–11 2009.
Cancún, Quintana Roo, México, DOI: 10.1109/ReConFig.2009.50, http://hal.archives-ouvertes.fr/hal-00411843/en/.

[BGF+10] Shivam Bhasin, Sylvain Guilley, Florent Flament, Nidhal Selmane, and Jean-Luc Danger.
Countering Early Evaluation: An Approach Towards Robust Dual-Rail Precharge Logic.
In *WESS*, pages 6:1–6:8. ACM, October 24-28 2010.
Scottsdale, Arizona, USA. DOI: 10.1145/1873548.1873554.

[BP10] Olivier Benoît and Thomas Peyrin.
Side-Channel Analysis of Six SHA-3 Candidates.
In *CHES*, volume 6225 of *Lecture Notes in Computer Science*, pages 140–157. Springer, August 17-20 2010.
Santa Barbara, CA, USA.

[EG10] Moulay Abdelaziz Elaabid and Sylvain Guilley.
Practical Improvements of Profiled Side-Channel Attacks on a Hardware Crypto-Accelerator.
In *AFRICACRYPT*, volume 6055 of *LNCS*, pages 243–260. Springer, May 03-06 2010.
Stellenbosch, South Africa. DOI: 10.1007/978-3-642-12678-9_15.

[GSM+10] Sylvain Guilley, Laurent Sauvage, Julien Micolod, Denis Réal, and Frédéric Valette.
Defeating Any Secret Cryptography with SCARE Attacks.
In *LatinCrypt*, volume 6212 of *LNCS*, pages 273–293. Springer, August 8-11 2010.
Puebla, México, DOI: 10.1007/978-3-642-14712-8_17.

[MS06] Stefan Mangard and Kai Schramm.
Pinpointing the Side-Channel Leakage of Masked AES Hardware Implementations.
In *CHES*, volume 4249 of *LNCS*, pages 76–90. Springer, October 10-13 2006.
Yokohama, Japan.

[PR10] Emmanuel Prouff and Thomas Roche.
Attack on a Higher-Order Masking of the AES Based on Homographic Functions.
In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT*, volume 6498 of *Lecture Notes in Computer Science*, pages 262–281. Springer, 2010.

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan.
Statistical Analysis of Second Order Differential Power Analysis.
IEEE Trans. Computers, 58(6):799–811, 2009.

[PSQ07] Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater.
Power and electromagnetic analysis: Improved model, consequences and comparisons.
Integration, The VLSI Journal, special issue on "Embedded Cryptographic Hardware", 40:52–60, January 2007.
DOI: 10.1016/j.vlsi.2005.12.013.

[RRST02] Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, and Stephane Tinguely.
Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards.
In *IEEE Symposium on Security and Privacy (S&P)*, pages 31–41, 2002.
DOI: http://dx.doi.org/10.1109/SECPRI.2002.1004360.

[Sch08] Werner Schindler.
Advanced stochastic methods in side channel analysis on block ciphers in the presence of masking.
Journal of Mathematical Cryptology, 2(3):291–310, October 2008.
ISSN (Online) 1862-2984, ISSN (Print) 1862-2976, DOI: 10.1515/JMC.2008.013.

[SGD+09] Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Yves Mathieu, and Maxime Nassar.
Successful Attack on an FPGA-based WDDL DES Cryptoprocessor Without Place and Route Constraints.
In *DATE*, pages 640–645, Nice, France, apr 2009. IEEE Computer Society.

[SLP05] 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.

[SS06] Daisuke Suzuki and Minoru Saeki.
Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style.
In *CHES*, volume 4249 of *LNCS*, pages 255–269. Springer, October 10-13 2006.
Yokohama, Japan. http://dx.doi.org/10.1007/11894063_21.

Exotic Leakage Models

Moulay Abdelaziz EL AABID[1,2], Sylvain GUILLEY[1,3],
Shivam BHASIN[1] and Jean-Luc DANGER[1,3].

[1] Institut TELECOM / TELECOM-ParisTech, CNRS LTCI (UMR 5141);
[2] Université Paris 8;
[3] Secure-IC S.A.S.

CryptArchi (Bochum, Germany),
June 15-18th 2011.