DPA : Attaques et Contre-mesures

Shivam BHASIN, Taoufik CHOUTA, Guillaume DUC, Jean-Luc DANGER,
Aziz EL AABID, Florent FLAMENT, Philippe HOOGVORST,
Tarik GRABA, Sylvain GUILLEY, Houssem MAGHR'EBI,
Olivier MEYNARD, Maxime NASSAR, Renaud PACALET,
Laurent SAUVAGE, Nidhal SELMANE and Youssef SOUISSI.

Institut TELECOM / TELECOM-ParisTech
CNRS – LTCI (UMR 5141)

GDR SoC-SiP 14:00 – 14:45
AMPHI SAPHIR, *TELECOM ParisTech*, *PARIS*.

Presentation Outline

Presentation Outline

Adversary's goal

- Secrets extraction.

Protection

- Conceal the secrets in a device (ASIC) ...
- ... or in the bitstream of an FPGA.

Representativity of the study

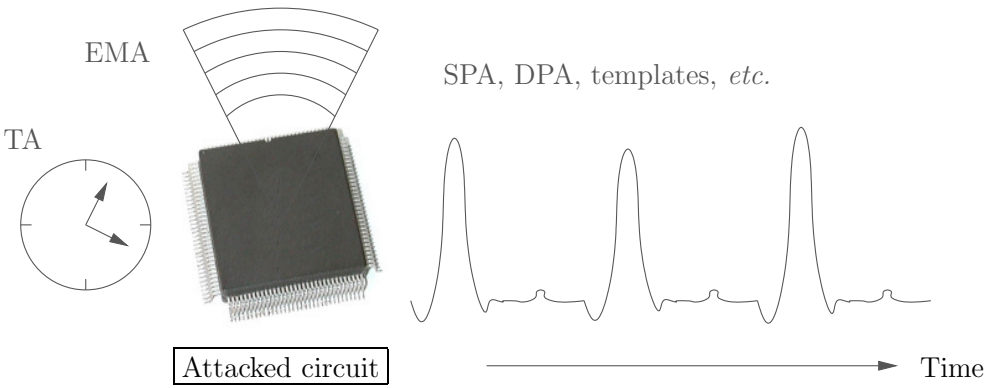
- Most problems come down to this...
- Example:
  - Fetching a data in an encrypted memory
  - $\Rightarrow$ decrypt the memory,
  - $\Rightarrow$ attack the CPU,
  - $\Rightarrow$ use side-channel attacks = SCA (for instance).

There are other applications of SCA

- SCARE: secret cryptography.
- Test (virtual oscilloscope).
- Subliminal channel for IPs watermarking.

Presentation Outline

Typical side-channels



- Timing Attacks [5].
- Power Analysis Attacks [6].
- Electro-magnetic Attacks [1].

Are SCAs intrusive?

Side-Channel Attacks (SCA) *versus* Fault Injection Attacks (FIA)

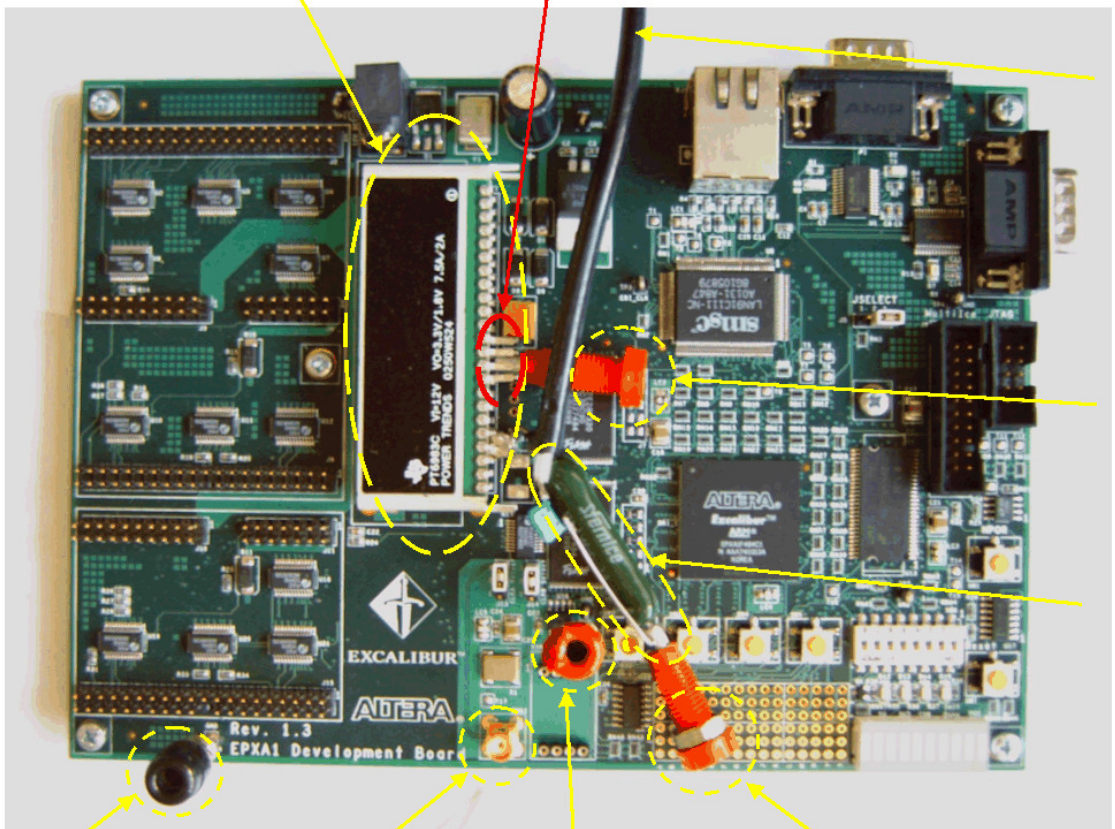
- SCA: passive
- FIA: active

But what about the experimental setup?

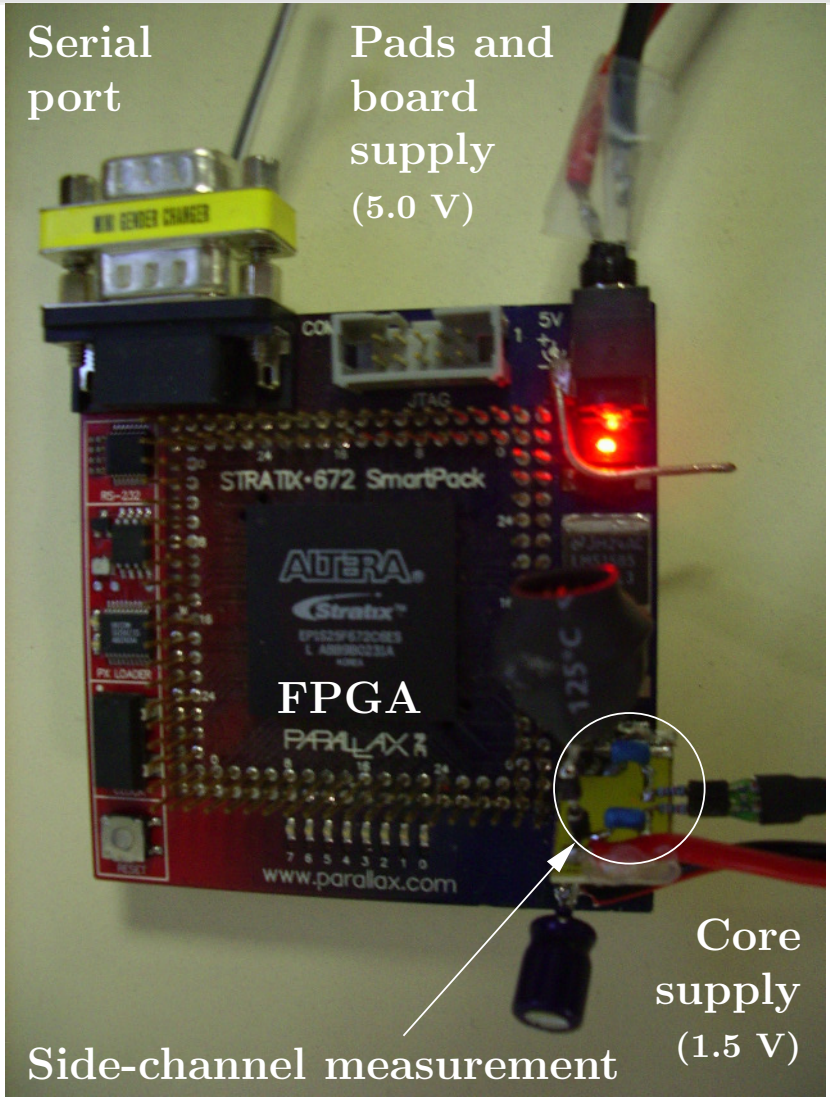
	Non-intrusive	**Intrusive**
Deportable IC (smartcard)	Timing, power, EM	—
Soldered IC or BGA (FPGA)	Timing, EM	power

The know-how in measurements is capital.
→ The 3rd version (2010–2011) of the DPA contest (http://www.dpacontest.org/) will have an acquisition competition, based on SASEBO GII.

ALTERA Excalibur evaluation board "customized for DPA"

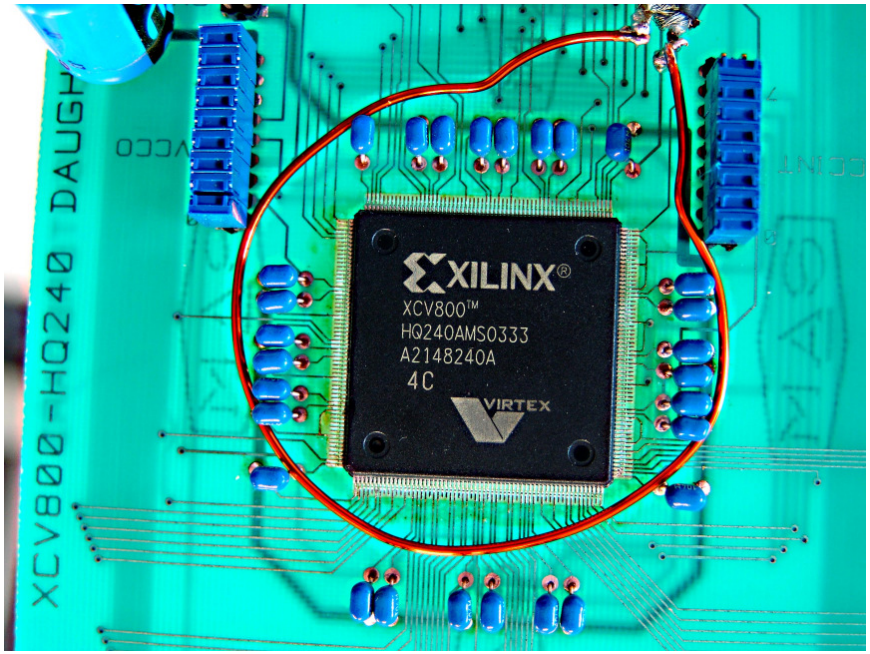


Parallax ALTERA Stratix board "customized for DPA" [3]

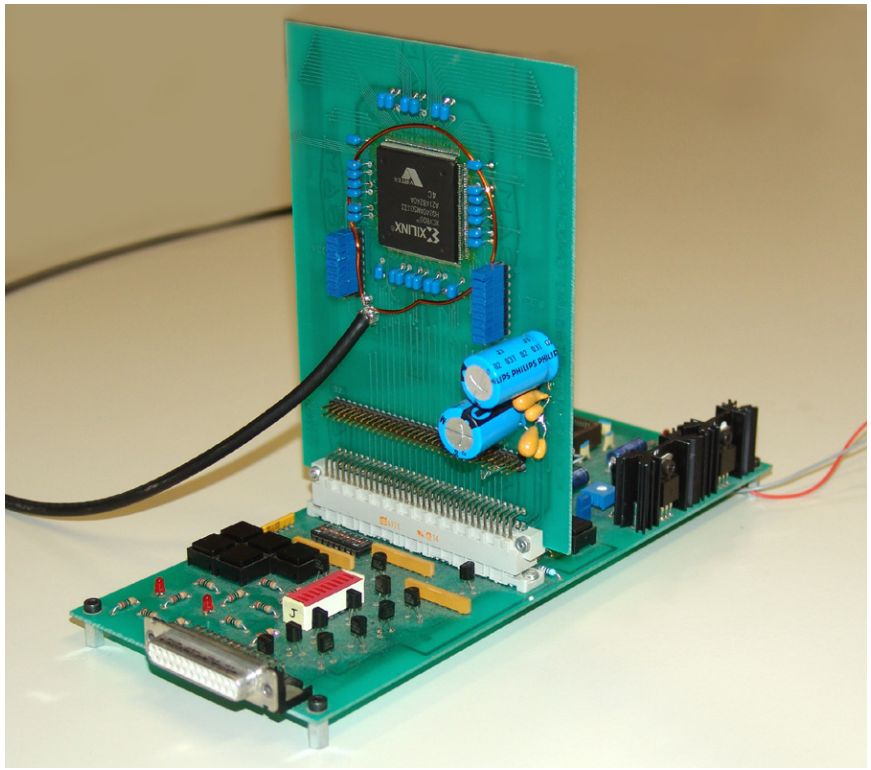


XCV800 home-made board suitable for **global** EMA

Antenna

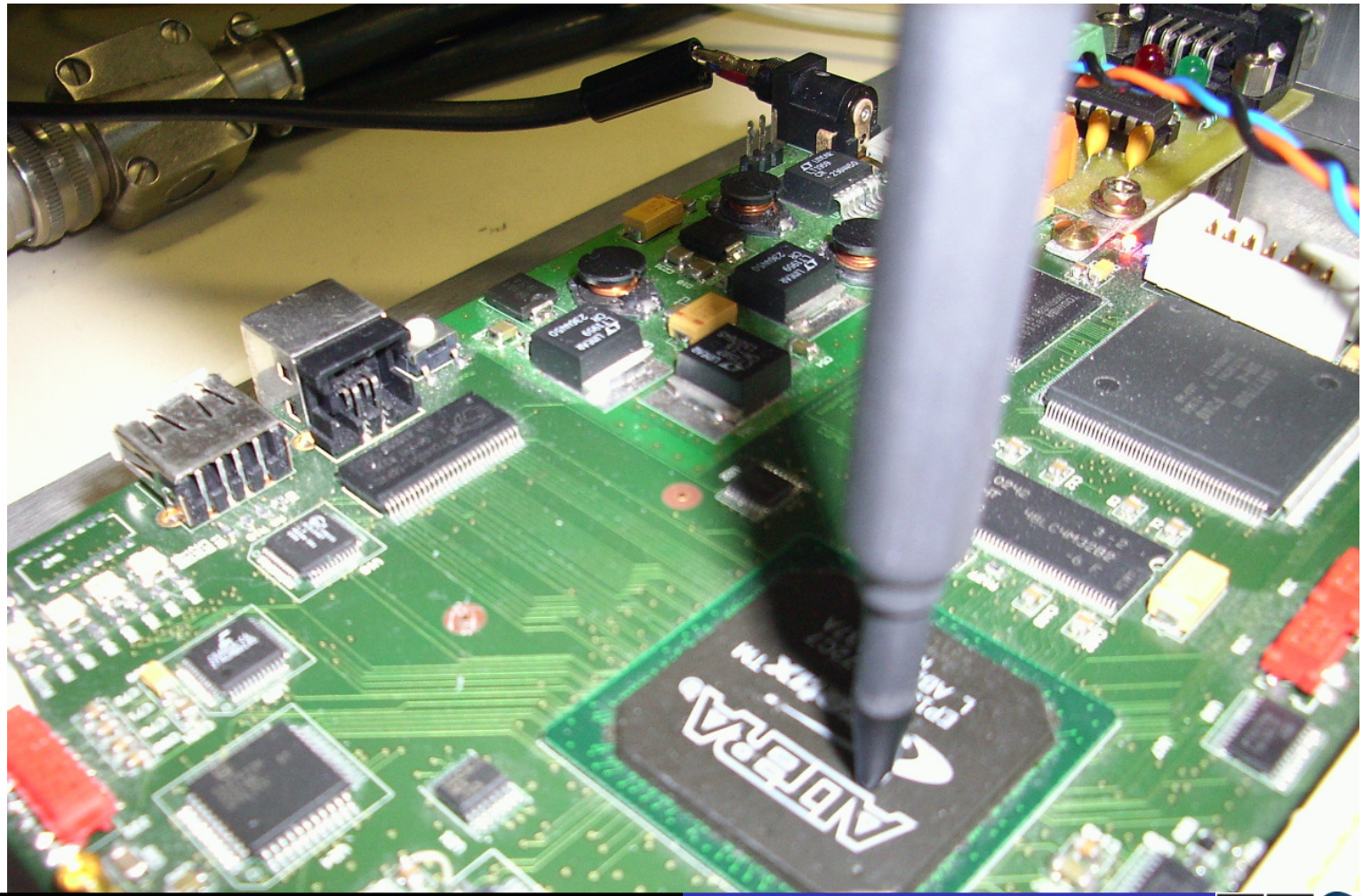


Acquisition setup

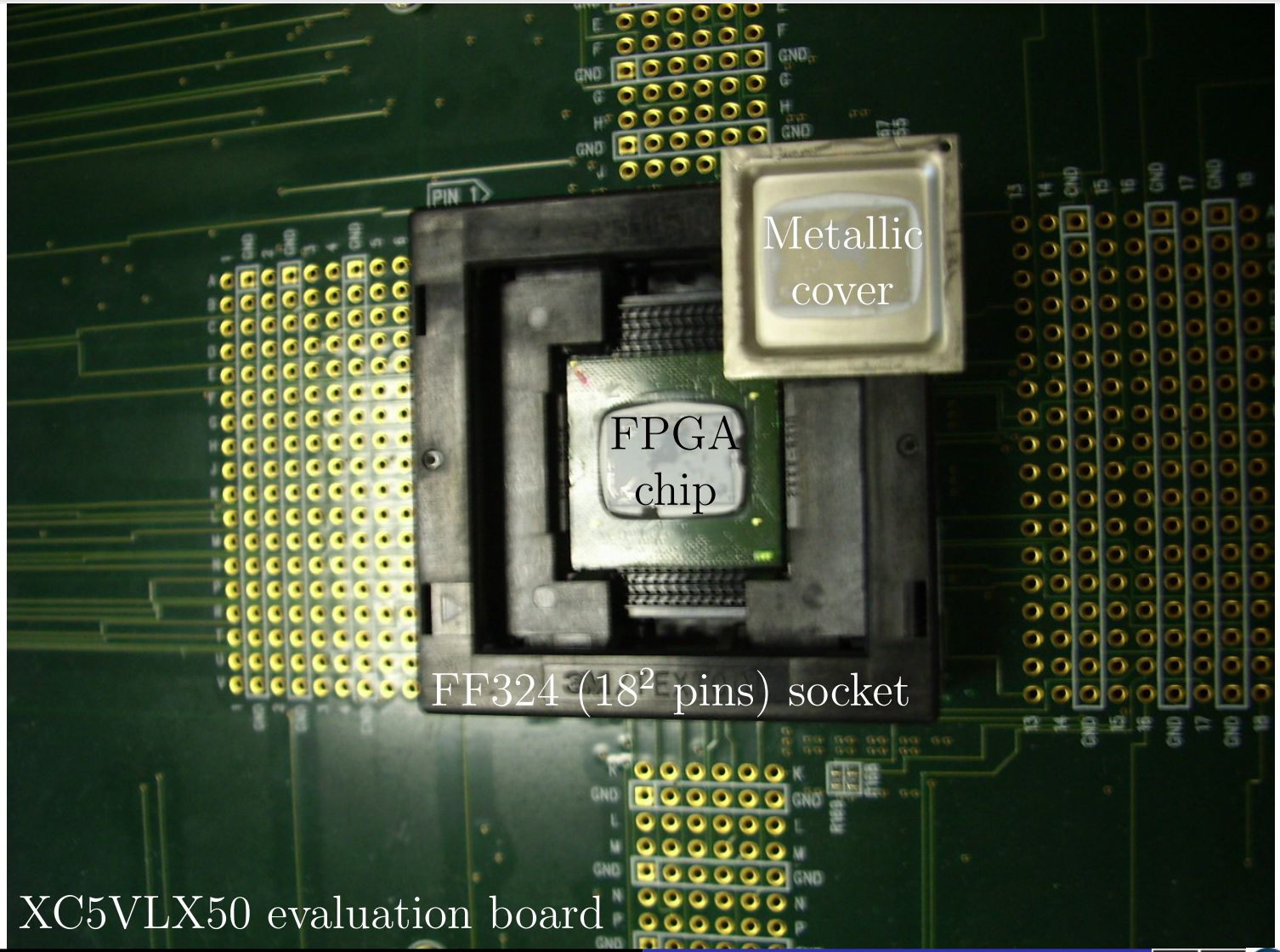


Pictures are courtesy of ESAT, Katholieke Universiteit Leuven, Belgium, (Elke De Mulder [7]).

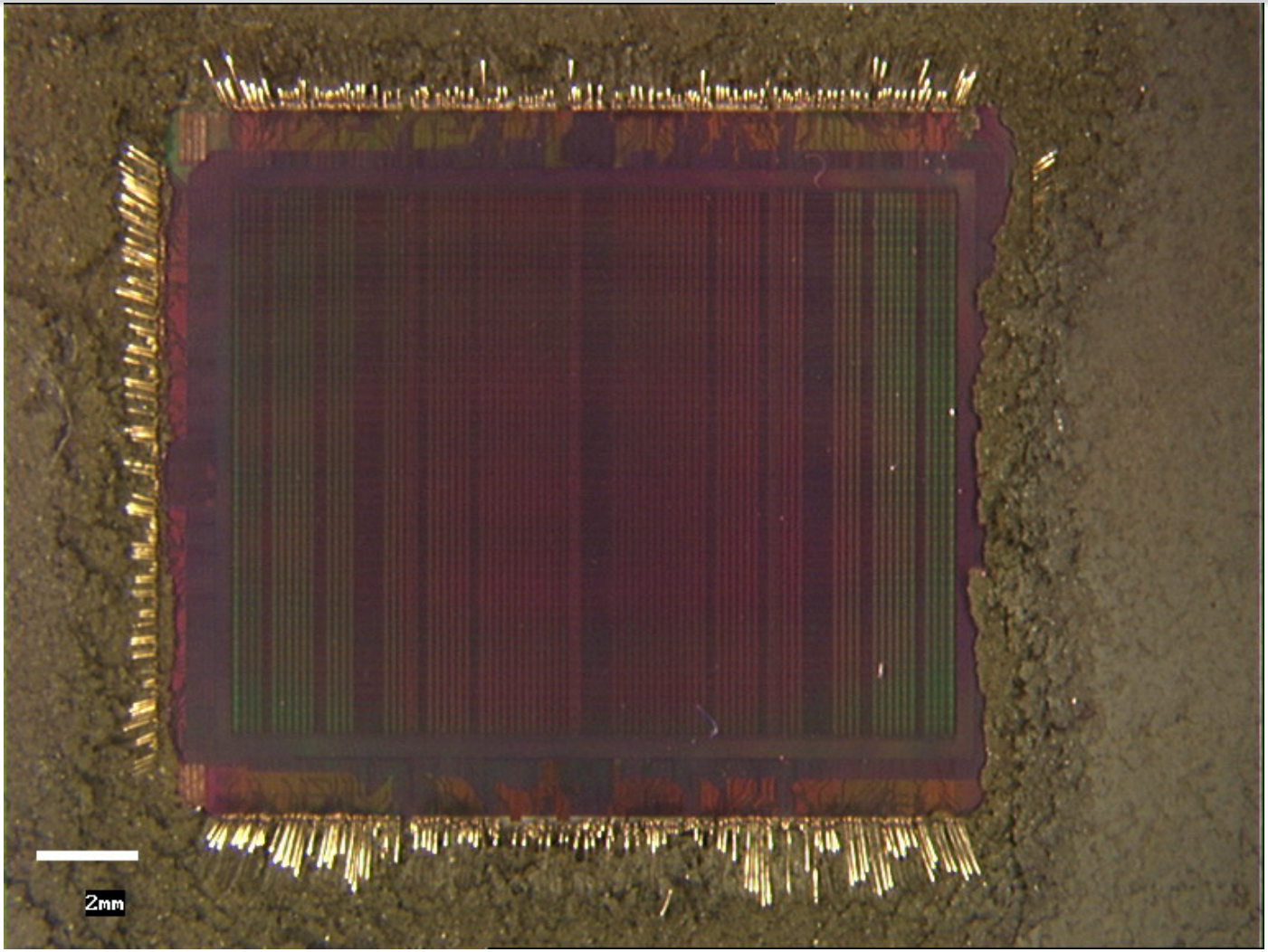
In-house ALTERA Stratix "as is" suitable for **local** EMA [9, 8]



XILINX Virtex-5 evaluation board "customized for EMA"



ALTERA Stratix with chemical preparation for EMA



Modus operandi

Information known/unknown by the attacker

- Known: Observations O;
- Known: (usually) either the plaintext or the ciphertext.
- Unknown: the encryption key (case of symmetric encryption).

Strategy: divide-and-conquer

- **Partition** observations according to a **sensitive** variable S:
  - depends on the secret K,
  - not too many bits of K, since attack = exhaustive search,
  - is computable from the plaintext / ciphertext.
- Therefore:
  - attacks target the first or the last round (in general),
  - `MixColumns` in AES hard to invert $\Rightarrow$ attack the last round.

Use the traces O to distinguishing between the **correct** partitioning from **wrong** ones

Distinguishers use a model

- $M(S)$ is the **physical syndrome** related to the **manipulation** of the secret S. It is called the **leakage model**.

Examples of distinguishers

- $|\mathbb{E}(O|M(S)=0) - \mathbb{E}(O|M(S)=1)|$: ..... DoM
- $\mathbb{E}_S\left((O|M(S) - \mathbb{E}O|M(S))(M(S) - \mathbb{E}M(S))\right)$: ... Covariance
- $\rho_s\left(O|S=s; M(s)\right)$: ..... CPA
- $\mathbb{E}_s \mathrm{H}\left(O|M(S)=M(s)\right)$ or $\mathrm{I}(O; M(S))$: ..... MIA

Models $M(S)$ (classification by [10])

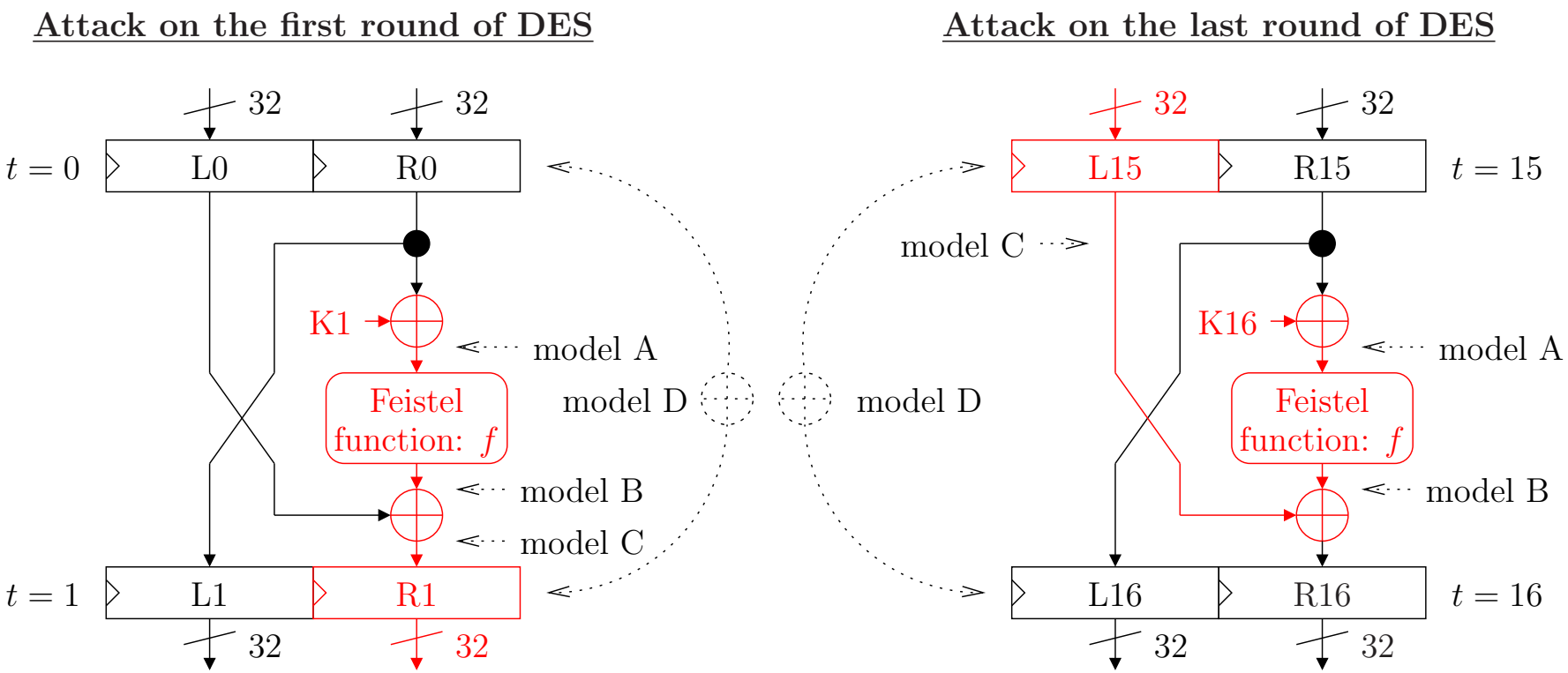
Partition-based:

- If unprotected:
  - $M(s) = |s|$; Hamming weight; Bus cleared in SW
  - $M(s) = |s \oplus R|$; Hamming weight; Bus precharged in SW
  - $M(s) = |s \oplus s_{-1}|$; Hamming distance; typical of HW
  - $M(s) = |\overline{s} \cdot s_{-1}| + (1-\delta)|s \cdot \overline{s_{-1}}|$; Idem, but in near-field EMA
- If protected:
  - $M(s) = s$. WARNING: 2^n values!
  - Difficult to be more inventive if the countermeasure is sound... but we'll see ☺

Comparison-based: (profiled attacks)

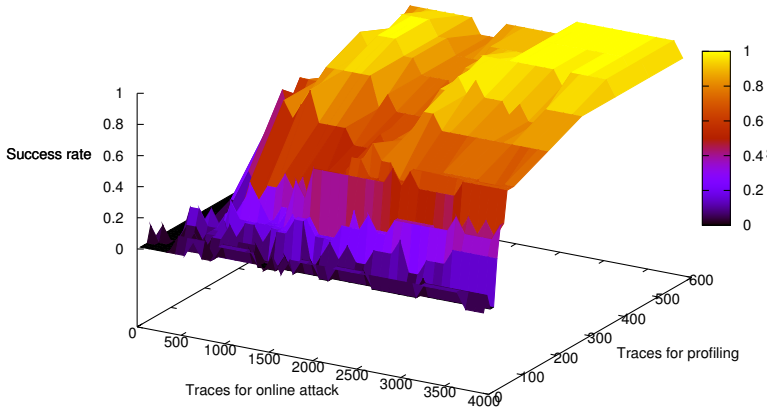
- $M(S) = \mathbb{E}(O|S)$; templates

Various leakage models for DES (iterative architecture)

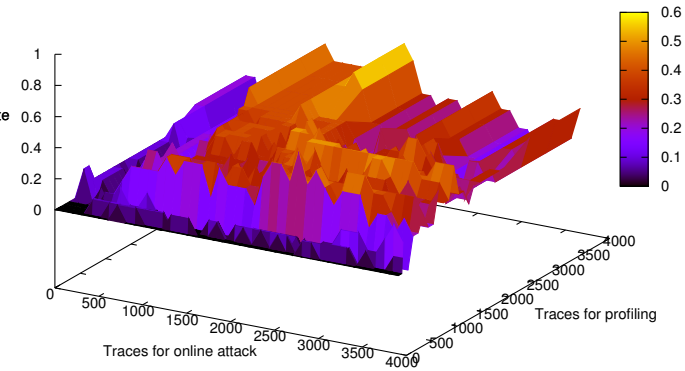


Caption: black = known values; red = unknown sensitive values

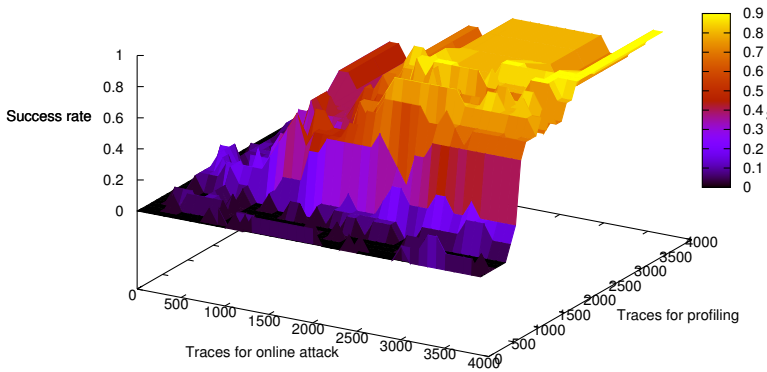
Finding the best leakage models is not obvious



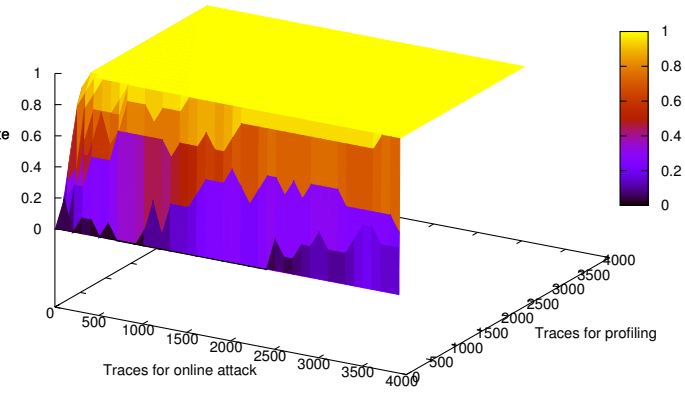
Success rate for model A.



Success rate for model B.

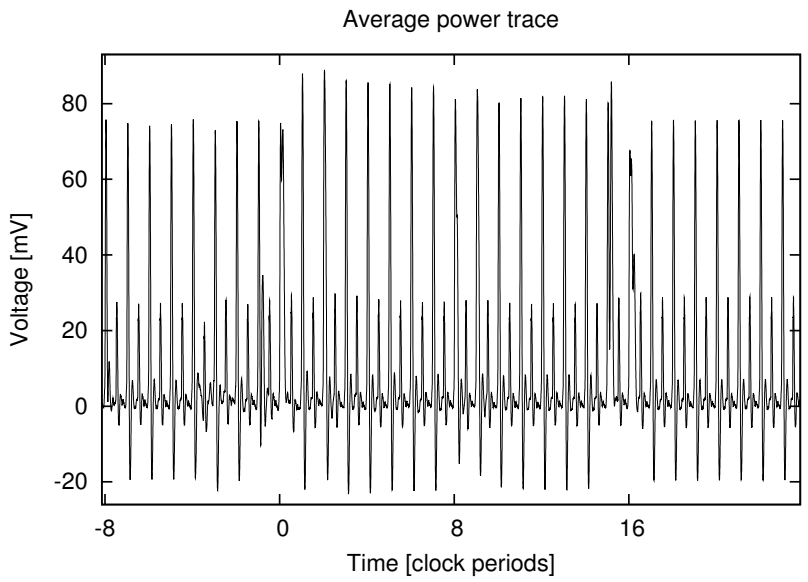


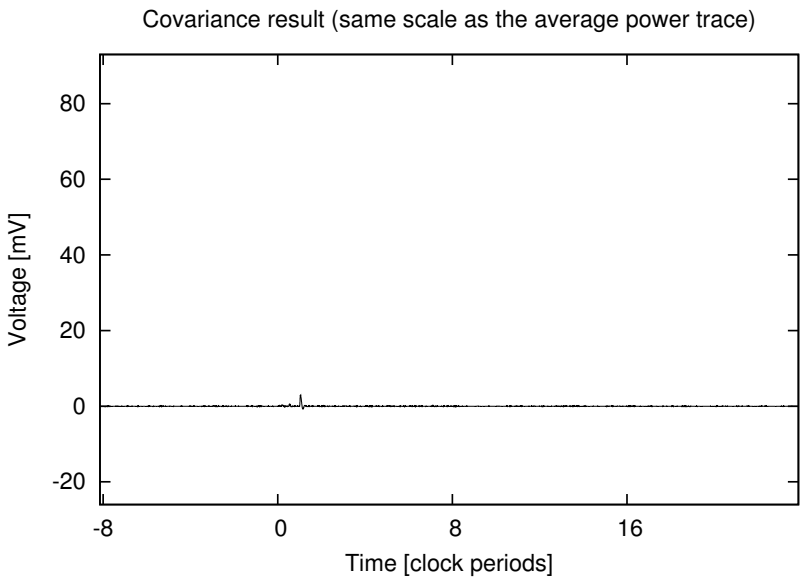
Success rate for model C.



Success rate for model D.

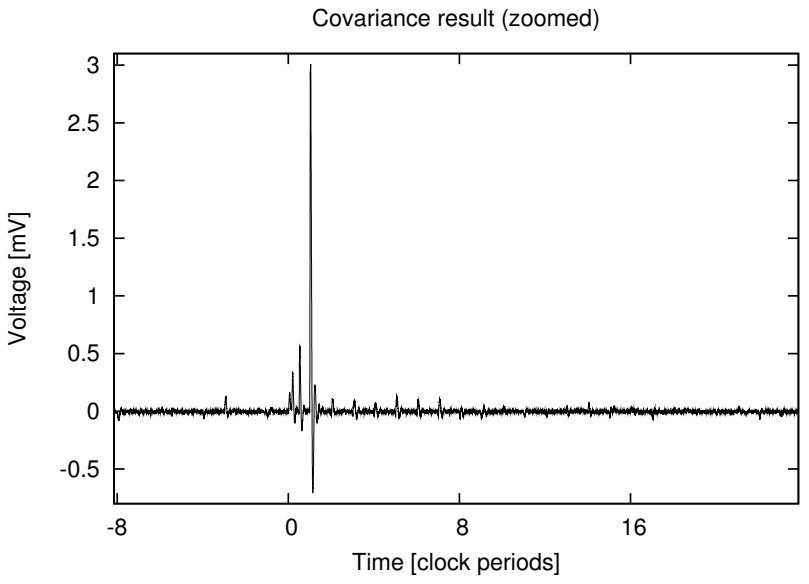
So, shall we conclude the Hamming distance (HD) — model D — is the ultimate model for HW?





SecMat v1[ASIC]:

- Typical trace: 92 mV
- Typical DPA: 3.0 mV
- $\Rightarrow$ Side-channel leakage: 3.3 %
- See [4]



Combined attacks!

1. Various distinguishers for a same partitioning;
2. One distinguisher can be evaluated on various partitionings;
3. The diversity can also come from the multiplicity of timing samples usually garnered during an acquisition campaign;
4. It can also arise from multi-modal acquisitions;
5. There can be situations where the most suitable partitioning can evolve from sample to sample in a side-channel capture.

Presentation Outline

Targeted strategies

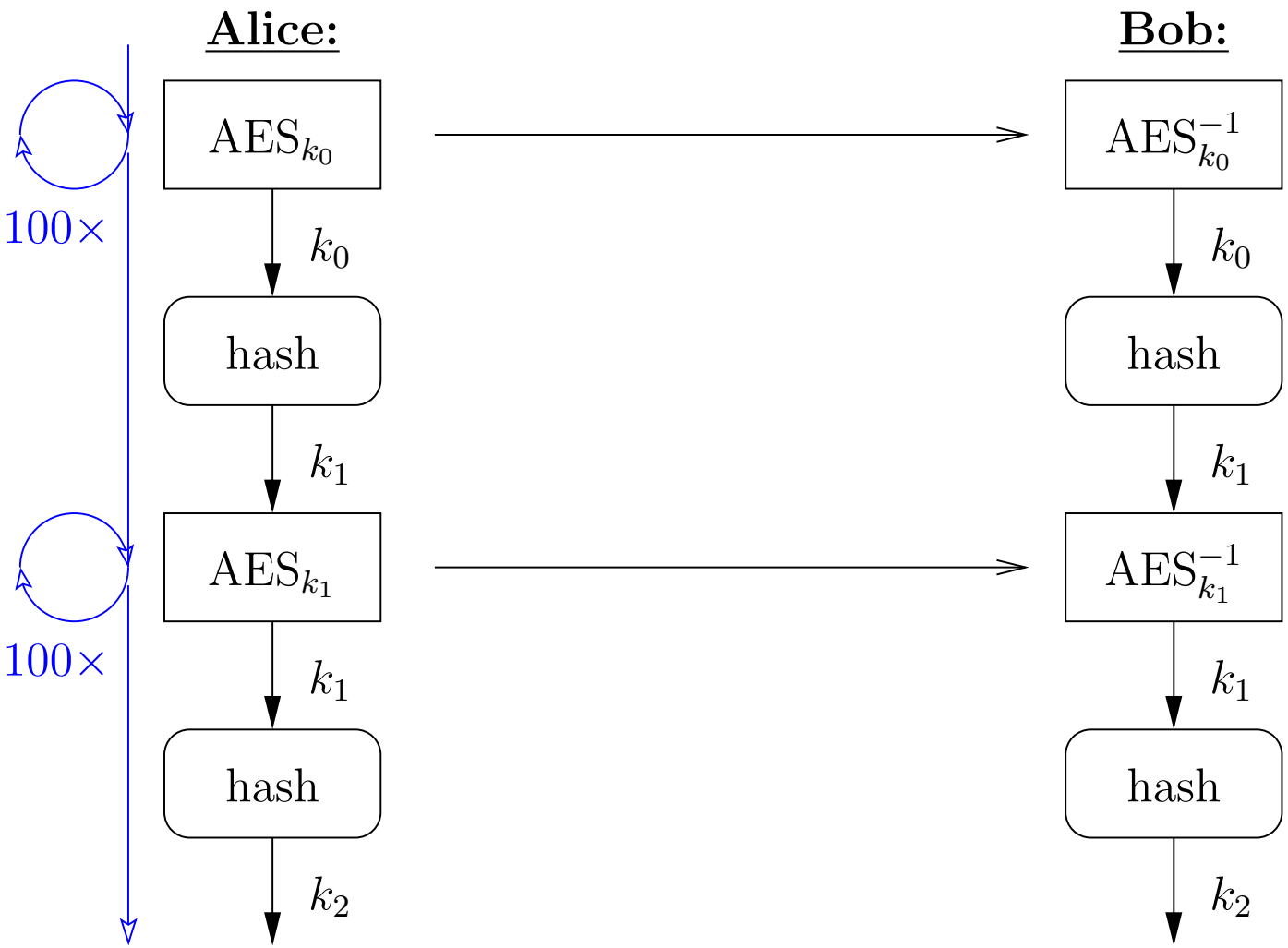
- Protocol-level:
  - Most wanted since provable
- Register-Transfer Level:
  - Masking. Easiest to implement; Boolean or algorithmic.
  - Encrypted leakage
  - Glitch-full circuits
- Netlist or implementation level:
  - Hiding (= DPL, Dual-rail with Precharge Logic)

Degenerated counter-measures / "Make difficult" strategies

- DPL w/o precharge
- Noise generator, Dummy instructions, Varying clock, *etc.*

$\Rightarrow$ And as for attacks, countermeasures can be combined.

Protocol level: if ≈ 1 bit is leaked per 100 encryptions...



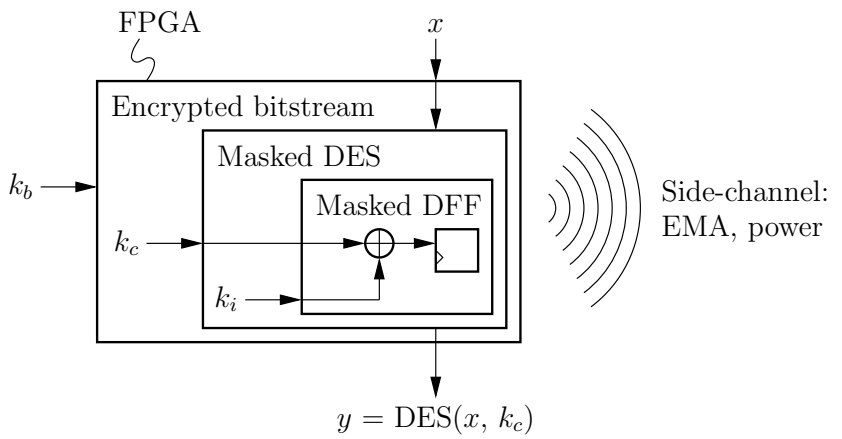
Masking

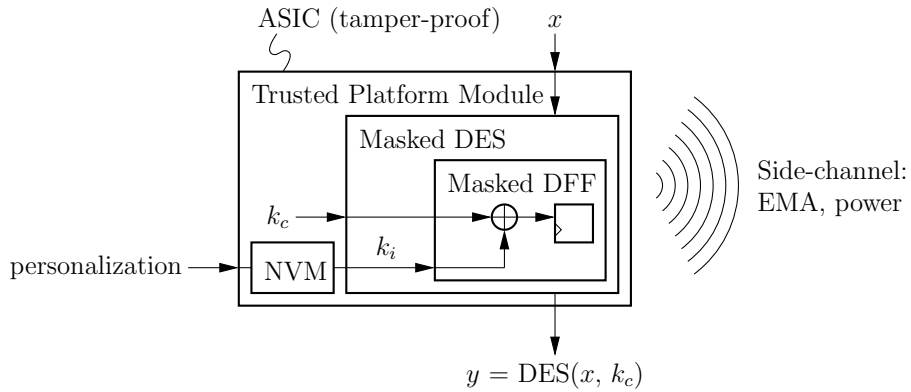
Principle

- Every variable s, potentially sensible, is represented as a share $\{s_0, s_1, \cdots, s_{n-1}\}$
- To reconstruct s, all the s_i are required.
- Example: $n = 2$, $s \doteq s_0 \oplus s_1$.

- Leakage resistant since variables are never used plain;
- Attractive but works only fine for registers.
- Efforts done to protect also the combinational logic.

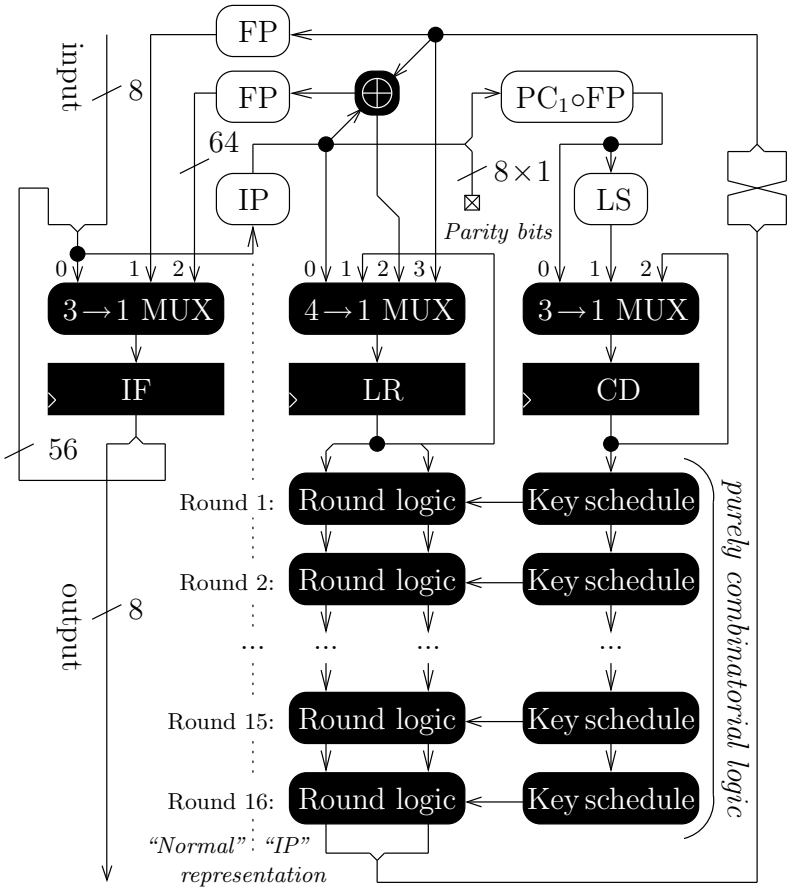
Encrypted Leakage



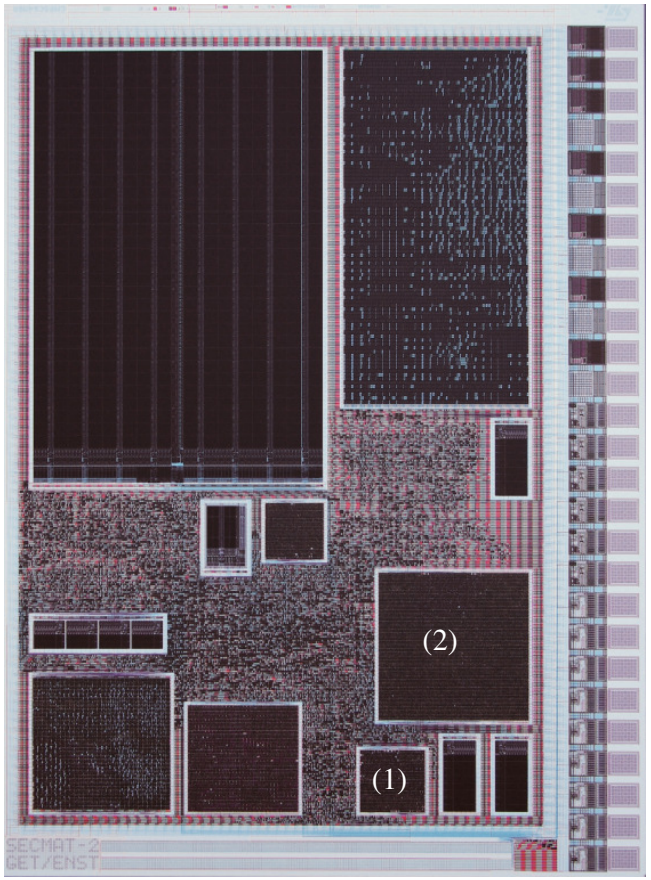


Glitch-full circuits

(a)

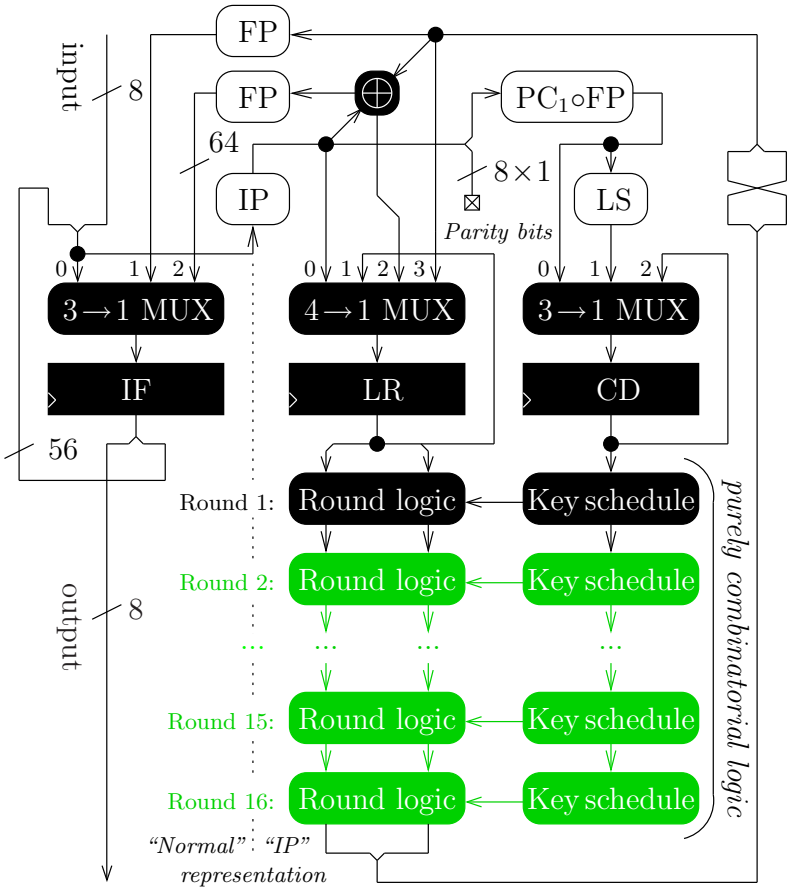


(b)

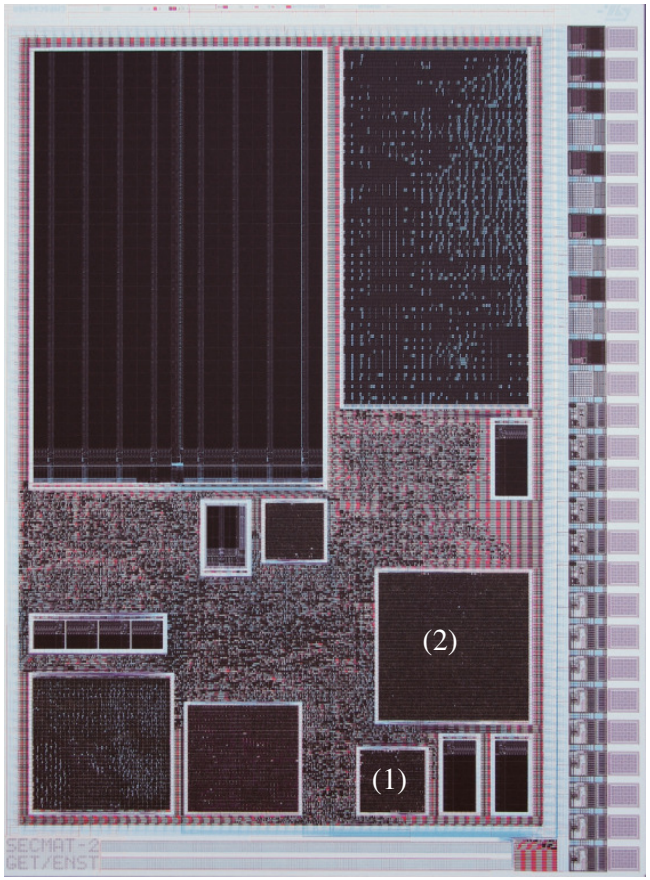


Glitch-full circuits

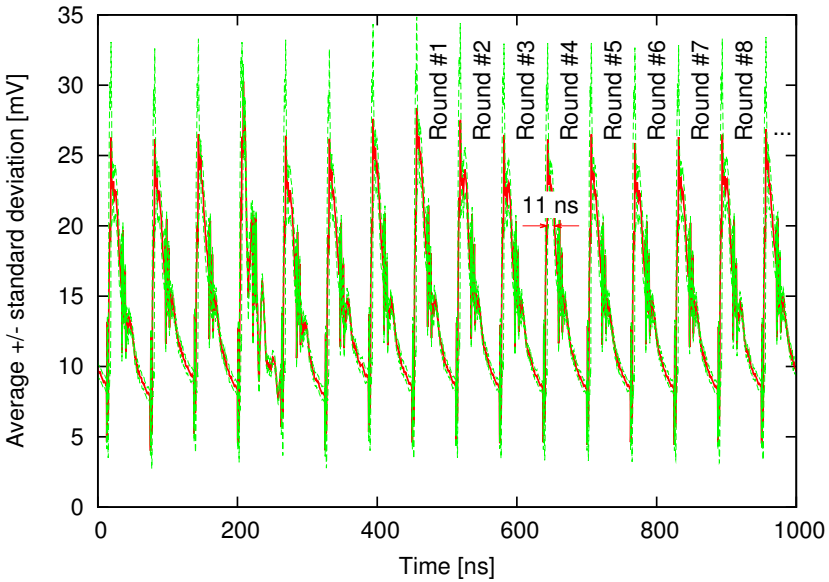
(a)



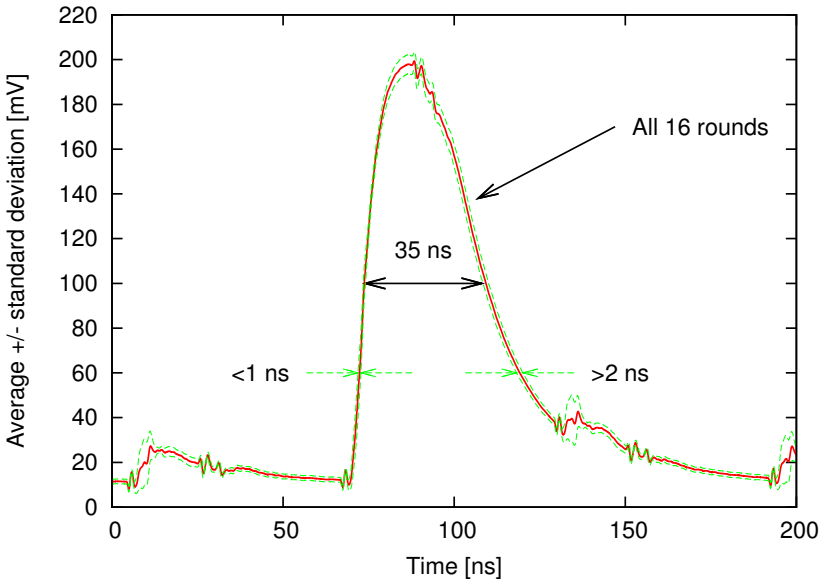
(b)



(a)



(b)

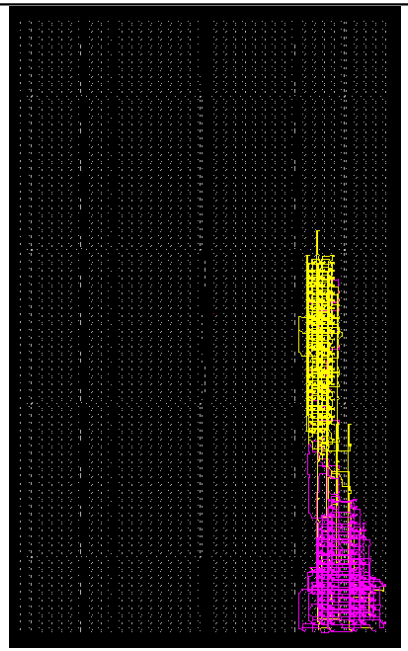
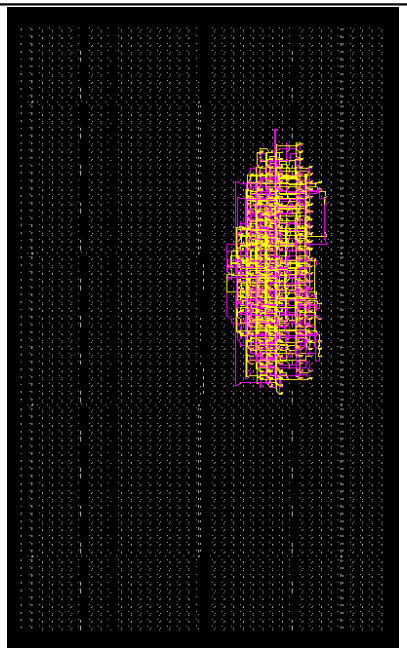


(a) Sequential iterative DES encryption signature, with the average variation margin, for statistics collected on 10k measurements.

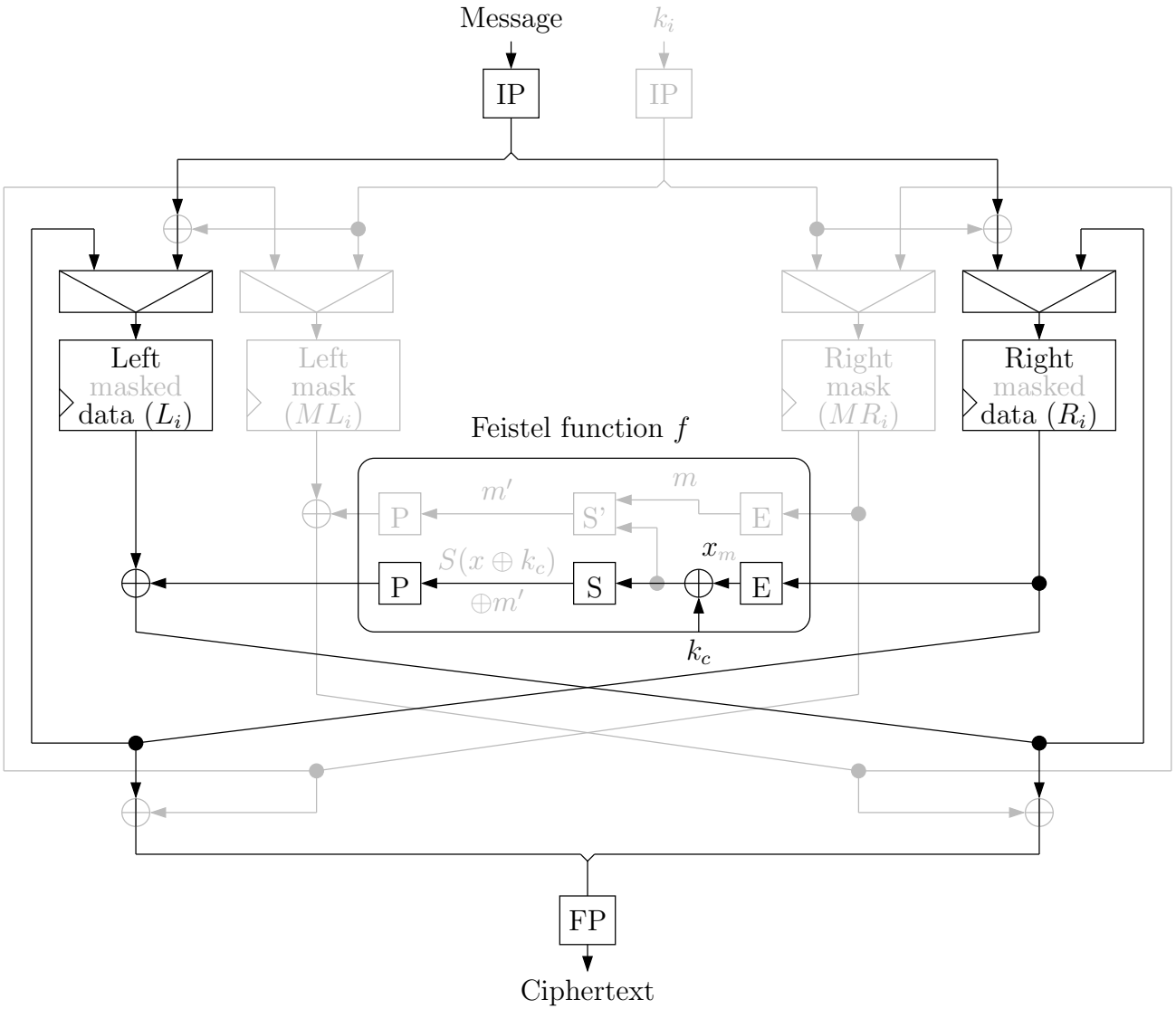
(b) Average combinatorial DES encryption signature, with the average variation margin, for statistics collected on 100k measurements.

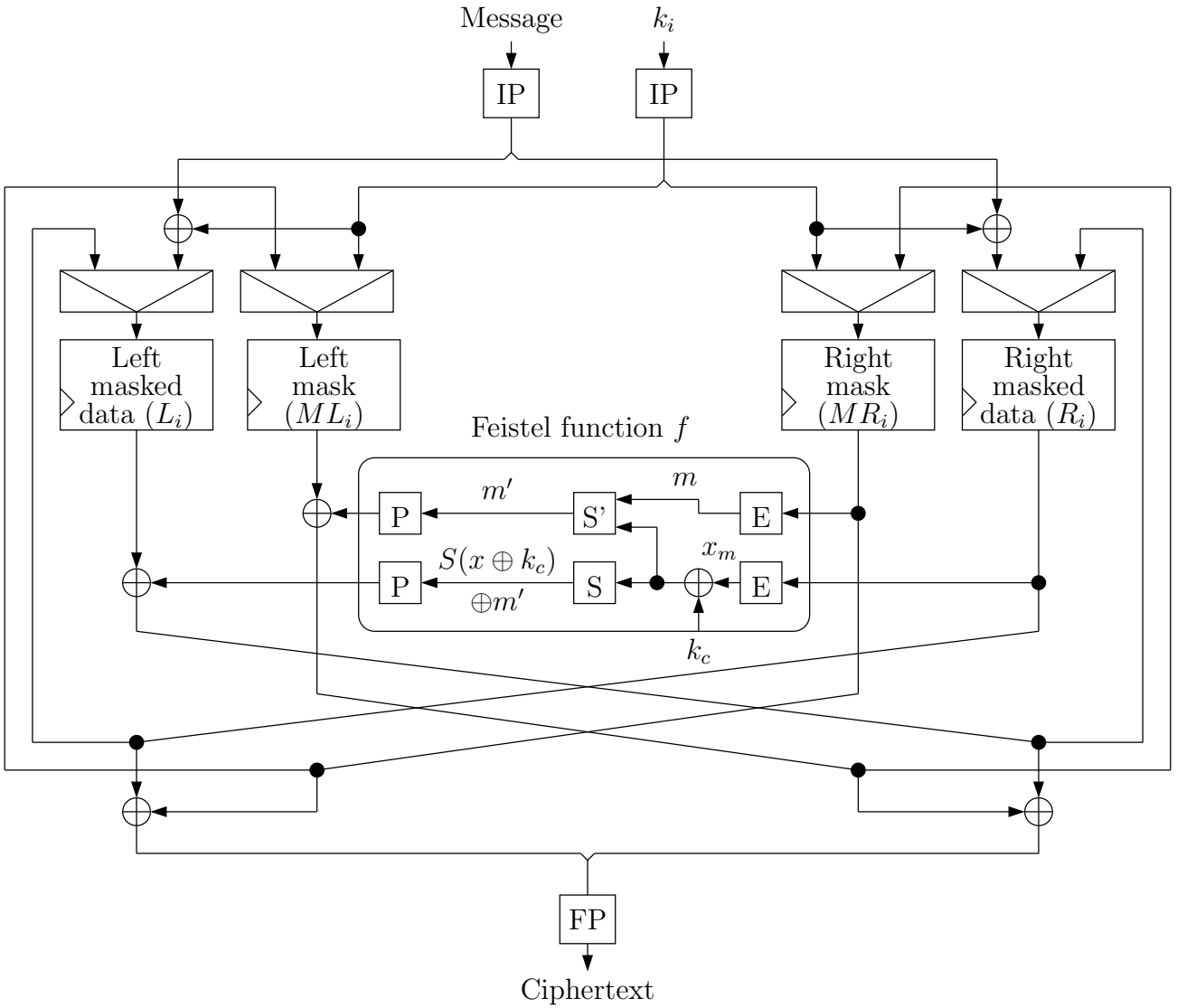
Hiding: Placement and Routing of Xilinx WDDL+ Netlists.

- P&R tools "naturally" separate true and false paths
- Example with AES substitution box SUBBYTES with and without placement constraints (2×2 LuT4 per slice)

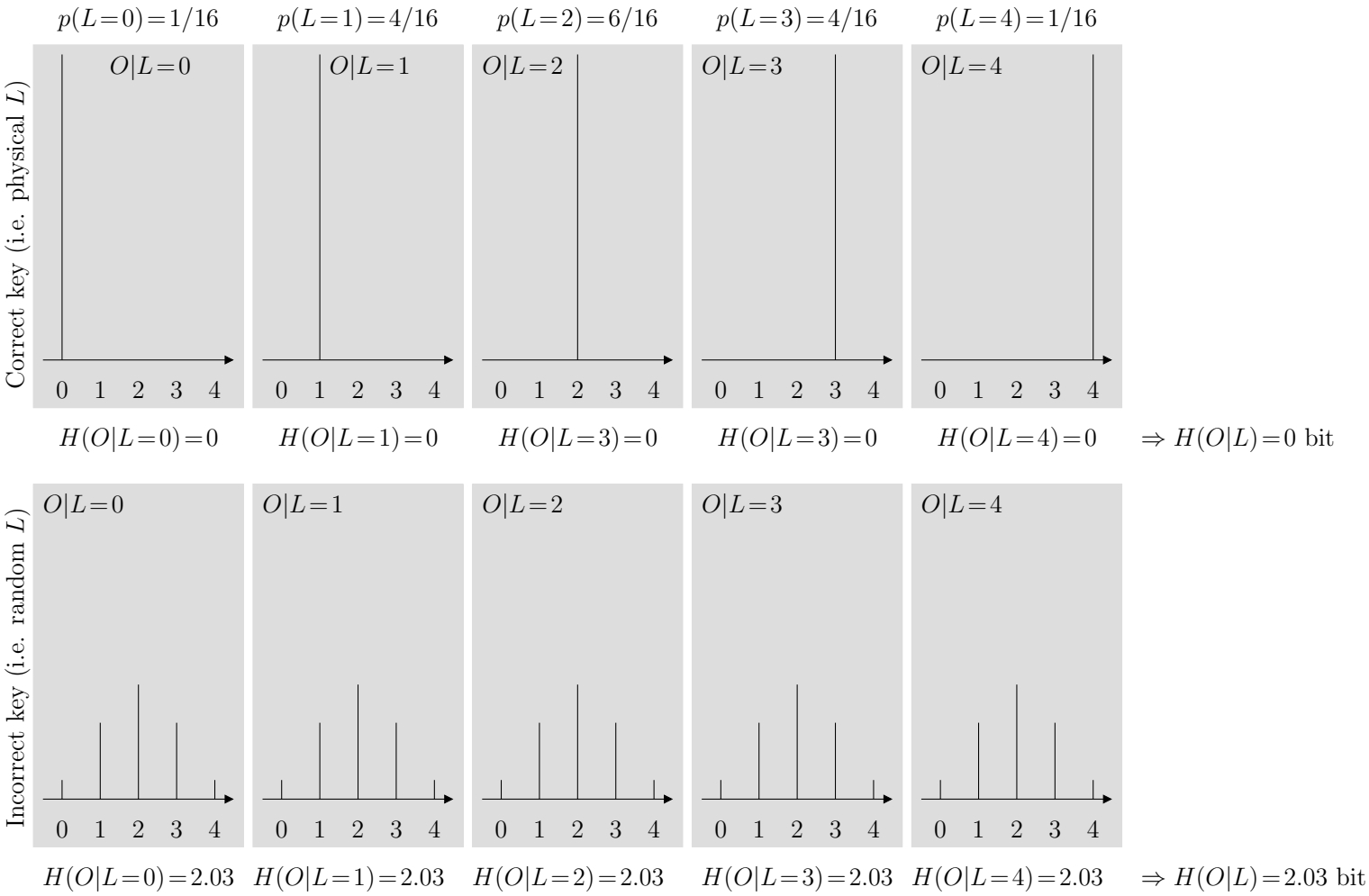
Unconstrained placement	**Constrained placement**
	

Presentation Outline

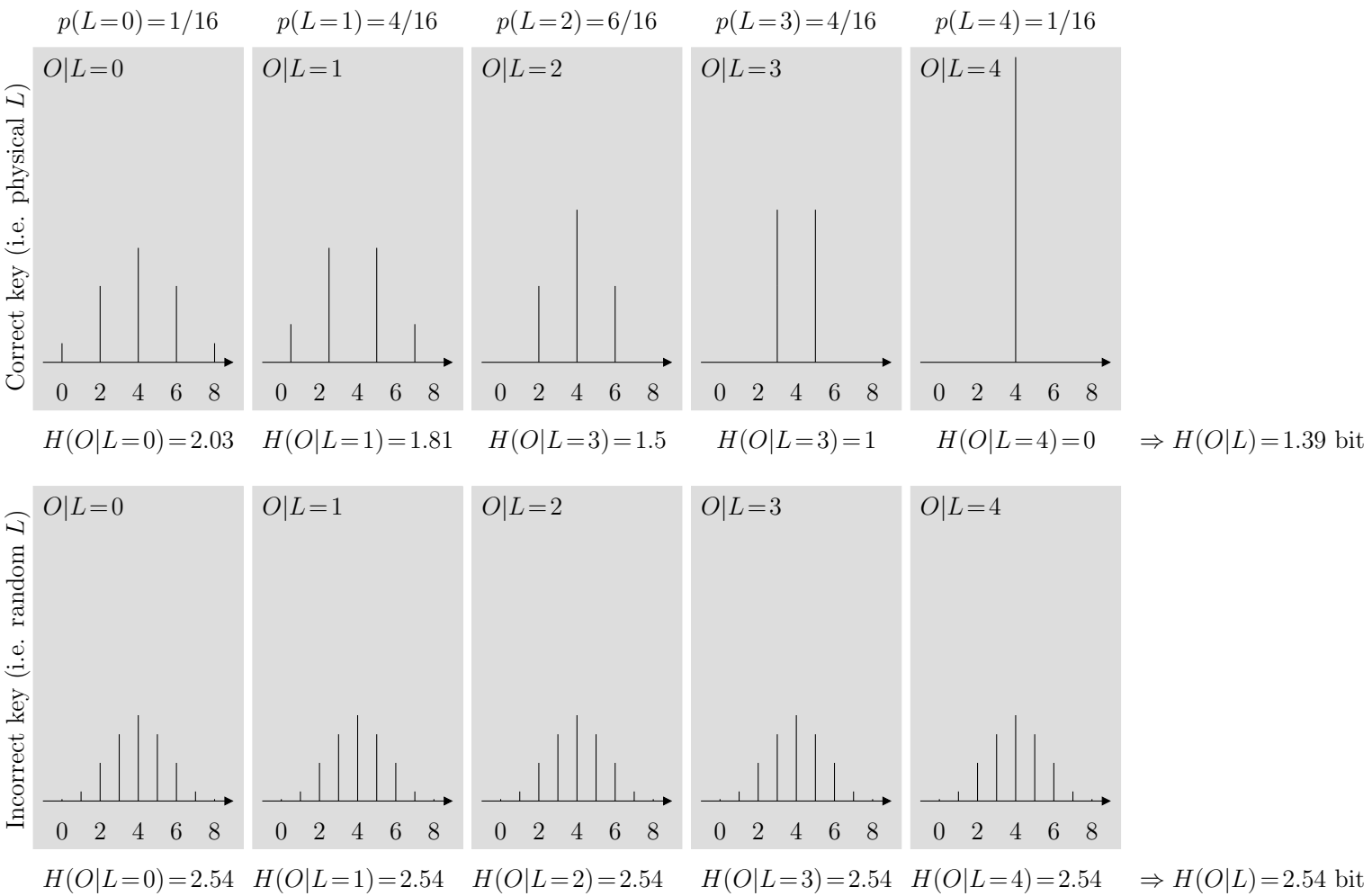

Message
k_i
IP
IP
Left masked data (L_i)
Left mask (ML_i)
Right mask (MR_i)
Right masked data (R_i)
Feistel function f
P
m'
S'
m
E
$S(x \oplus k_c)$
$\oplus m'$
P
S
x_m
E
k_c
FP
Ciphertext


Message
k_i
IP
IP
Left masked data (L_i)
Left mask (ML_i)
Right mask (MR_i)
Right masked data (R_i)
Feistel function f
P
m'
S'
m
E
P
$S(x \oplus k_c)$
$\oplus m'$
S
x_m
E
k_c
FP
Ciphertext

Attacks on masking (1/2)



Attacks on masking (2/2)



Models $M(S)$ (classification by [10])

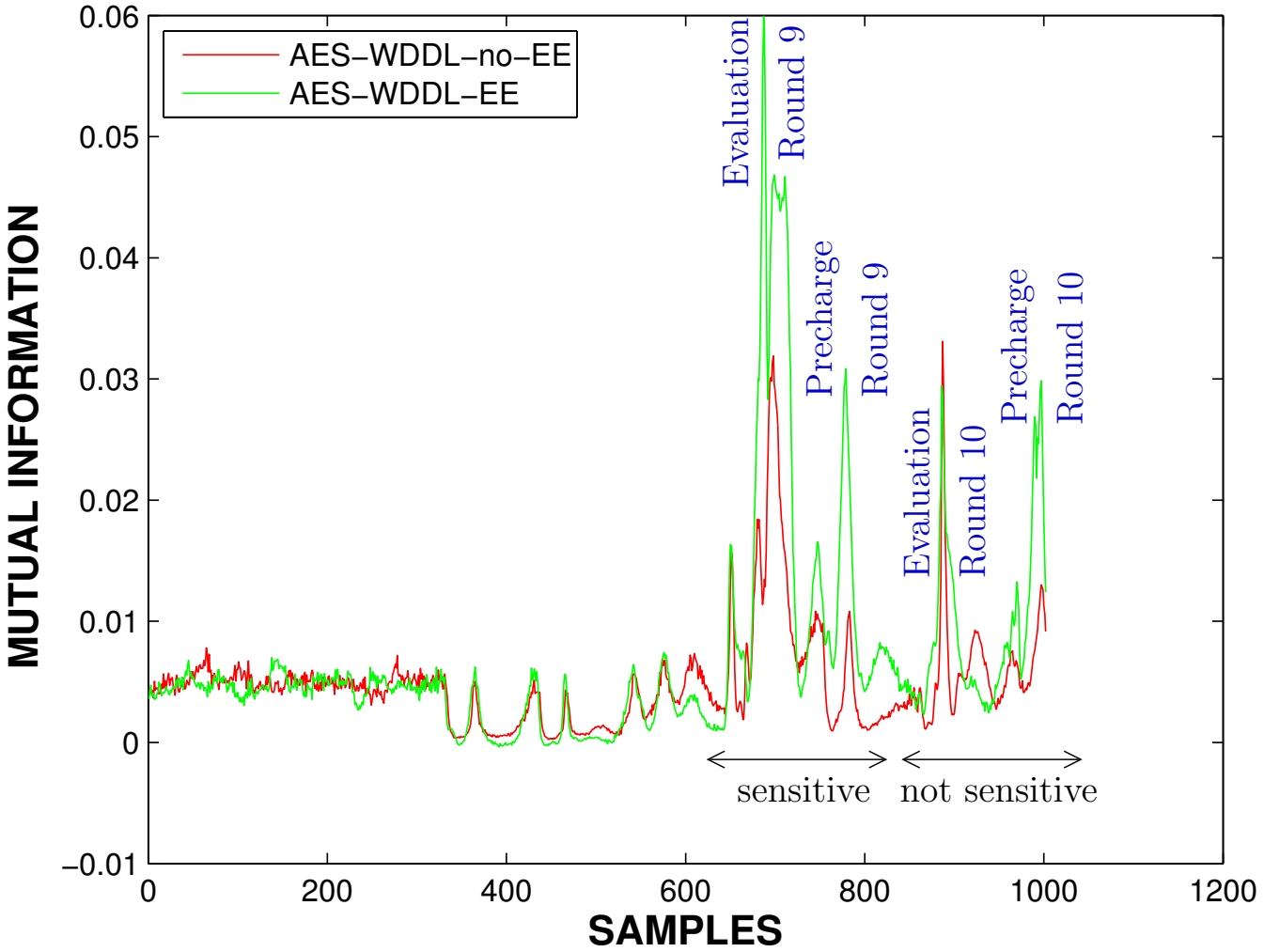
Partition-based:

- If unprotected:
  - $M(s) = |s|$; Hamming weight; Bus cleared in SW
  - $M(s) = |s \oplus R|$; Hamming weight; Bus precharged in SW
  - $M(s) = |s \oplus s_{-1}|$; Hamming distance; typical of HW
  - $M(s) = \sum_i \overline{s} \cdot s_{-1} + (1-\delta) s \cdot \overline{s_{-1}}$; Idem, but in near-field EMA
- If protected:
  - $M(s) = s$. WARNING: 2^n values!
  - Difficult to be more inventive if the countermeasure is sound...
  - $M(S) = S_1 + S_2$; Zero-offset
  - $M(S) = (S_1, S_2)$; Multi-variate MIA (MMIA [2])

Comparison-based: (profiled attacks)

- $M(S) = \mathbb{E}(O|S)$; templates

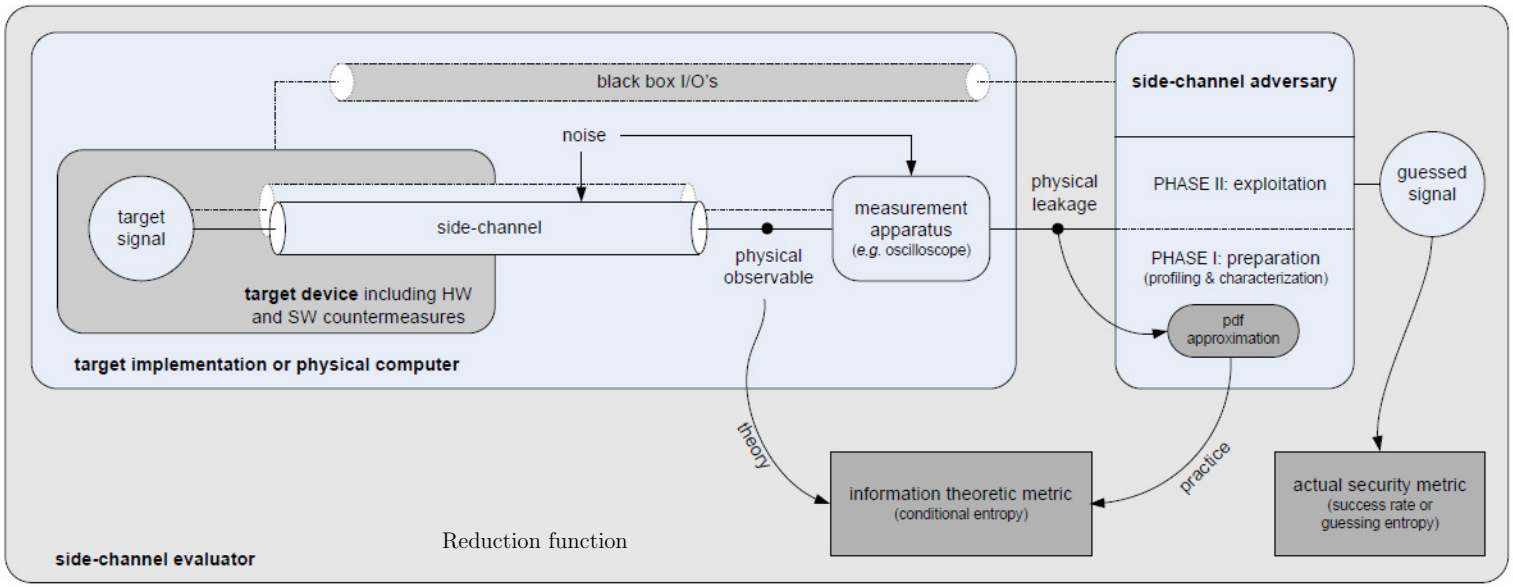
Attacks on DPL



Presentation Outline

Formal practice-oriented framework [11]

- Attacks metric
- Leakage metric



Counter-Measures are still *ad hoc*

1. Multiplicative masking of AES (M.-L. Akkar and Ch. Giraud, CHES 2001)
   - Zero Attack (Jovan Dj. Golic, Christophe Tymen, CHES 2002)
2. Provable secure S-Box implementation based on FFT (E. Prouff et al, CHES 2006)
   - Bias of the mask attack (S. Coron, CHES 2008)
3. MDPL (Th. Popp and S. Mangard, CHES 2005)
   - Folding attack (P. Schaumont and K. Tiri, CHES 2007), Subset attack (E. de Mulder et al, WIFS 2009)
4. DRSL (Z. Chen and Y. Zhou, CHES 2006)
   - Glitch on precharge (M. Nassar, DATE 2009)

Call for Further Researches ⇒ Open Issues

Need for formal proofs of security

- Can be at protocol level (*work in progress*).
- Could also be at implementation level (*new research area*).

Devise countermeasures globally ...

... taking into account all possible weaknesses:

- Observation.
- Perturbation.
- Manipulation.

[1] Karine Gandolfi, Christophe Mourtel, and Francis Olivier.
Electromagnetic Analysis: Concrete Results.
In *CHES*, volume 2162 of *LNCS*, pages 251–261. Springer, May 14-16 2001.
Paris, France.

[2] Benedikt Gierlichs, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede.
Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis.
In *CT-RSA*, volume 5985 of *LNCS*, pages 221–234. Springer, March 1-5 2010.
San Francisco, CA, USA.

[3] Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Tarik Graba, and Yves Mathieu.
Evaluation of Power-Constant Dual-Rail Logic as a Protection of Cryptographic Applications in FPGAs.
In *SSIRI*, pages 16–23, Yokohama, Japan, jul 2008. IEEE Computer Society.
DOI: 10.1109/SSIRI.2008.31, http://hal.archives-ouvertes.fr/hal-00259153/en/.

[4] Sylvain Guilley, Laurent Sauvage, Jean-Luc Danger, Nidhal Selmane, and Renaud Pacalet.
Silicon-level solutions to counteract passive and active attacks.
In *FDTC, 5th Workshop on Fault Detection and Tolerance in Cryptography, IEEE-CS*, pages 3–17, Washington DC, USA, aug 2008.
(Up-to-date version on http://hal.archives-ouvertes.fr/HAL: http://hal.archives-ouvertes.fr/hal-00311431/en/).

[5] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun.
Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems.
In *Proceedings of CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer-Verlag, 1996.
(http://www.cryptography.com/timingattack/paper.htmlPDF).

[6] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun.
Differential Power Analysis.
In *Proceedings of CRYPTO'99*, volume 1666 of *LNCS*, pages 388–397. Springer-Verlag, 1999.
(PDF).

[7] Elke De Mulder, Pieter Buysschaert, Sıddıka Berna Örs, Peter Delmotte, Bart Preneel, Guy Vandenbosch, and Ingrid Verbauwhede.
Electromagnetic Analysis Attack on an FPGA Implementation of an Elliptic Curve Cryptosystem.
In *IEEE International Conference on Computer as a tool (http://www.eurocon2005.org.yu/EUROCON)*, pages 1879–1882, November 2005.
Belgrade, Serbia & Montenegro.

[8] Laurent Sauvage, Sylvain Guilley, Jean-Luc Danger, Yves Mathieu, and Maxime Nassar.
Successful Attack on an FPGA-based Automatically Placed and Routed WDDL+ Crypto Processor.
In *DATE, track A4 (Secure embedded implementations)*, April 20–24 2009.
Nice, France. Electronic version: http://hal.archives-ouvertes.fr/hal-00325417/en/.

[9] Laurent Sauvage, Sylvain Guilley, and Yves Mathieu.
ElectroMagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack of a Cryptographic Module.
ACM Trans. Reconfigurable Technol. Syst., 2(1):1–24, March 2009.
Full text in http://hal.archives-ouvertes.fr/hal-00319164/en/.

[10] François-Xavier Standaert, Benedikt Gierlichs, and Ingrid Verbauwhede.
Partition vs. Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices.
In *ICISC*, volume 5461 of *LNCS*, pages 253–267. Springer, December 3-5 2008.
Seoul, Korea.

[11] François-Xavier Standaert, Tal Malkin, and Moti Yung.
A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks.
In *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 443–461. Springer, April 26-30 2009.
Cologne, Germany.