Silicon-level Solutions against DPA & DFA

Sylvain GUILLEY Laurent SAUVAGE Jean-Luc DANGER
Nidhal SELMANE Renaud PACALET
< sylvain.guilley@TELECOM-ParisTech.fr >

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

FDTC'08, Sunday, August 10th, 2008, 08:30 – 09:10,
Mayflower Hotel, *Colonial Room*, Washington DC, USA.

Presentation Outline

Rationale for non-invasive attacks

- A thorough study of the **vulnerabilities** is required ...
- ... to come up with sound **protections**.

Methodology

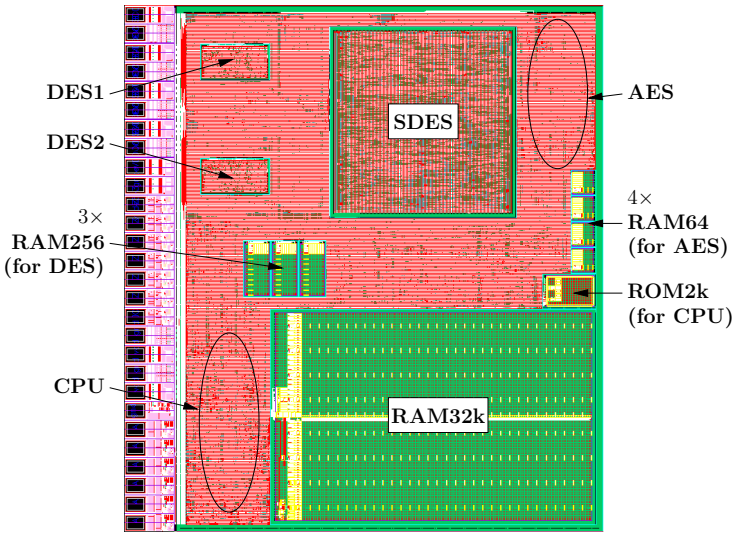
- Validation by the **experience** is absolutely mandatory
- Hence: **dedicated circuits**, namely the following ASICs:
  - SecMat v$\{1, 3/2, 2, 3\}$ academic smartcards.
- Fair knowledge of the **underlying physics**:
  - How does the circuit leak?
  - How do faults appear?
- Attacks **fine-tuning**:

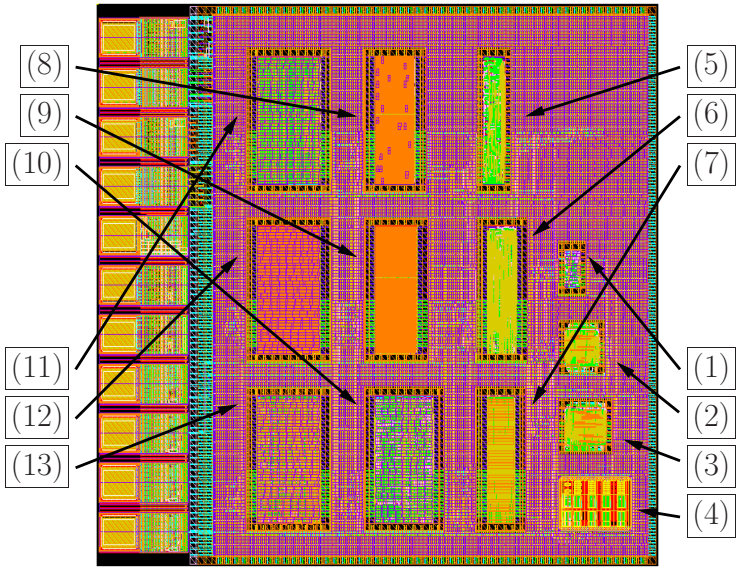
  $$\boxed{\text{DPA} < \text{CPA} < \text{enhanced-CPA} < \text{PPA} < \text{blind attacks}}.$$

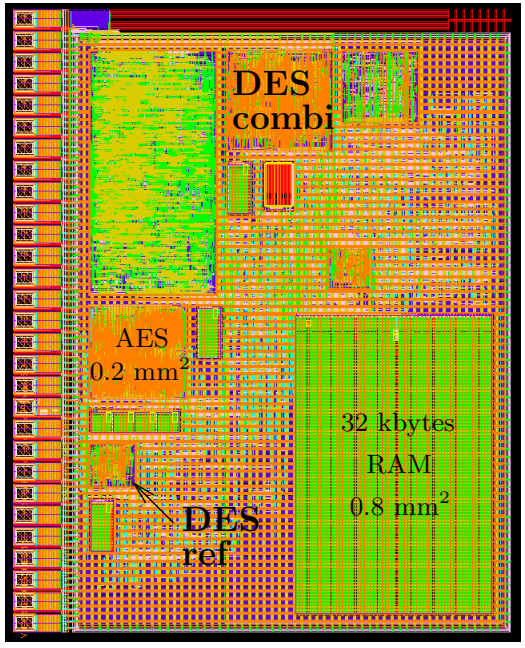
  What's next? $\Rightarrow$ http://www.dpacontest.org/.

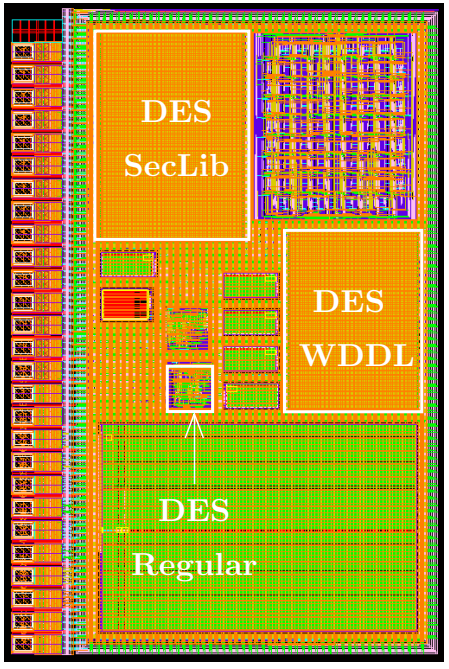
Presentation Outline

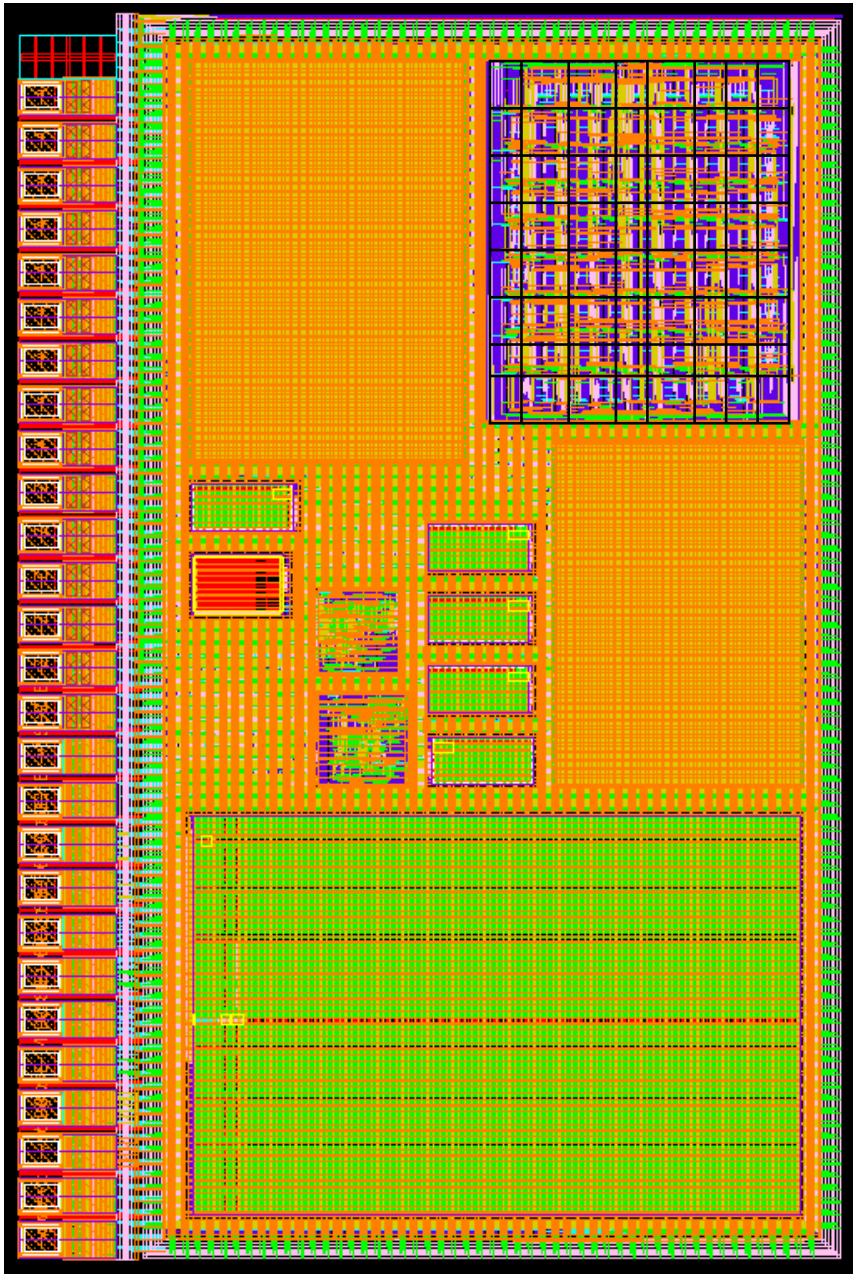
Circuits to Study DPA & DFA: SecMat v{1, 3/2, 2, 3}





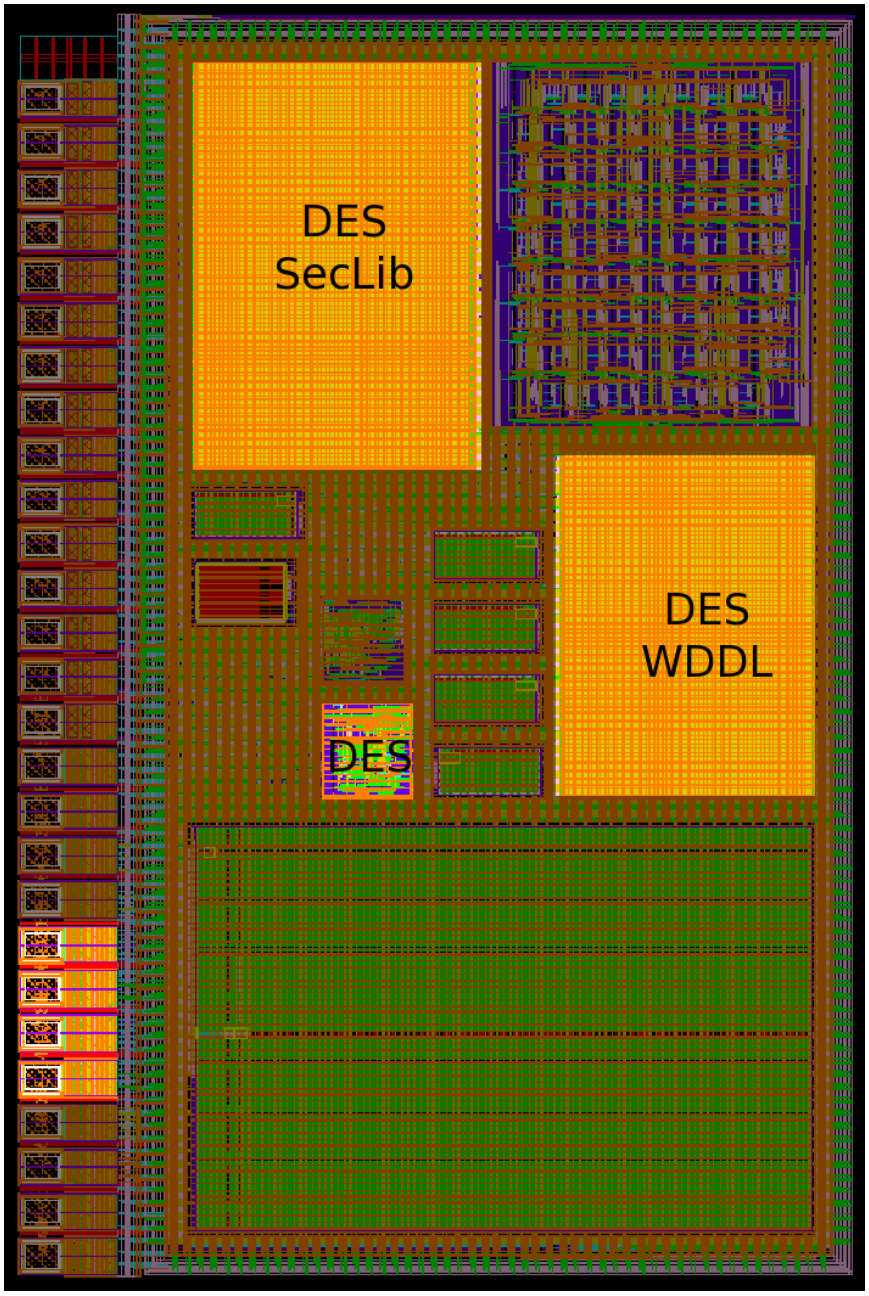






Features of the circuit

- Smartcard with encryption accelerators and an e-FPGA
- Programmation in ANSI C
- Hardware driver: ACME Fox running GNU / Linux 2.4.31
- 4.4 mm^2, 2.4×10^6 tr.
- HCMOS9GP 130 nm techno
- Manufacturing via CMP run S12C7_1 of 03/01/07
- 3 power domains
- Vertical insulation of P^- and N^- wells
- SW controllable clock-gating + scan-chain

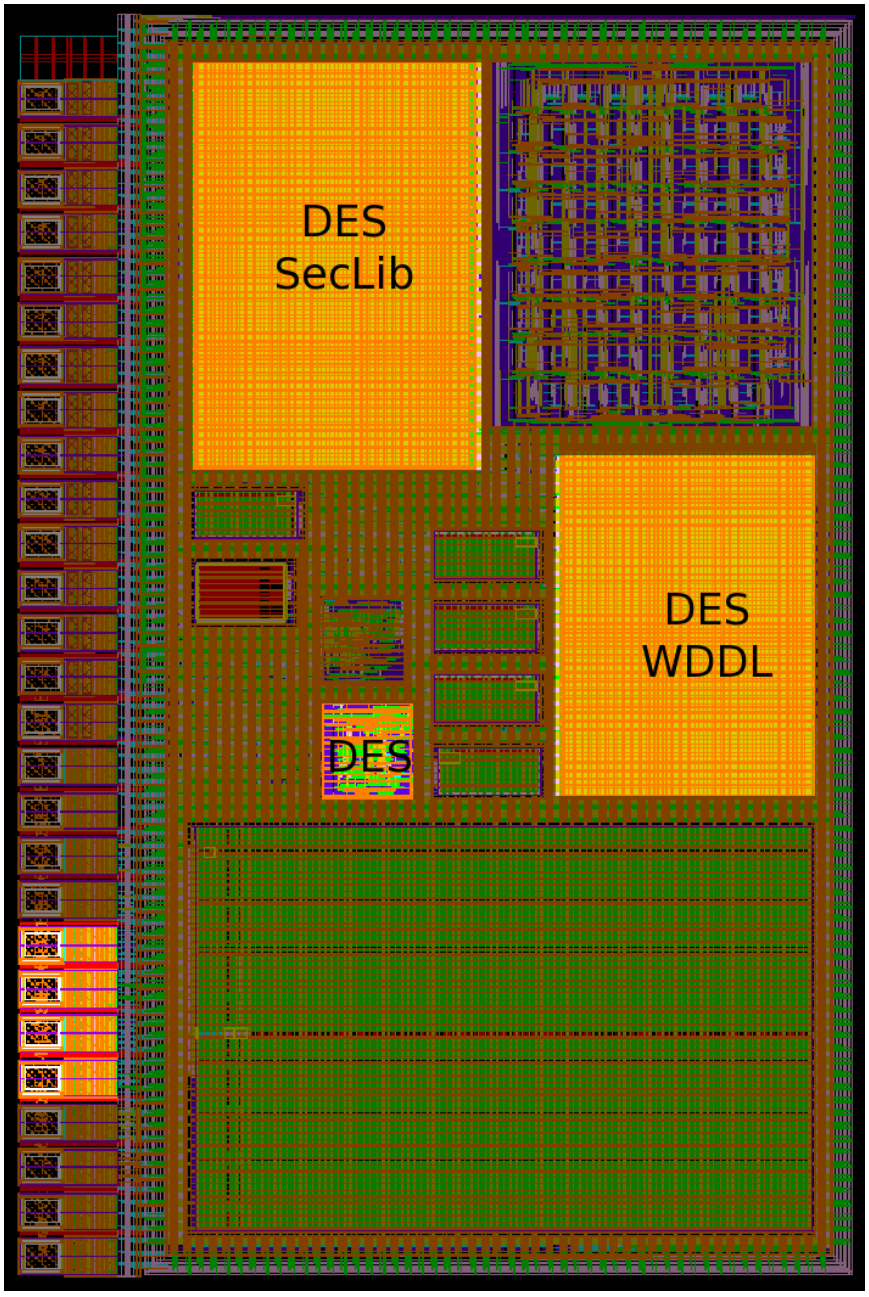


One Run-Time Reconfigurable embedded FPGA [4]

- Slave of the CPU (6502)
- 8×8 LuT4

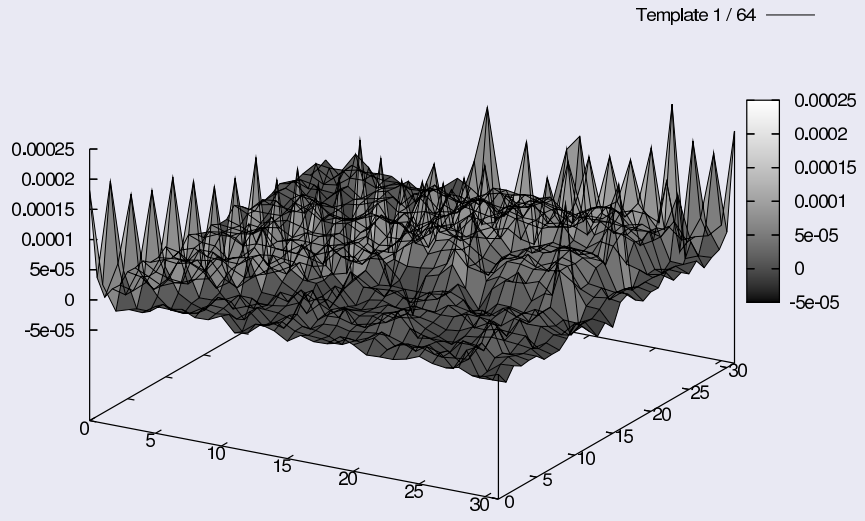
Three functionally identical DES modules

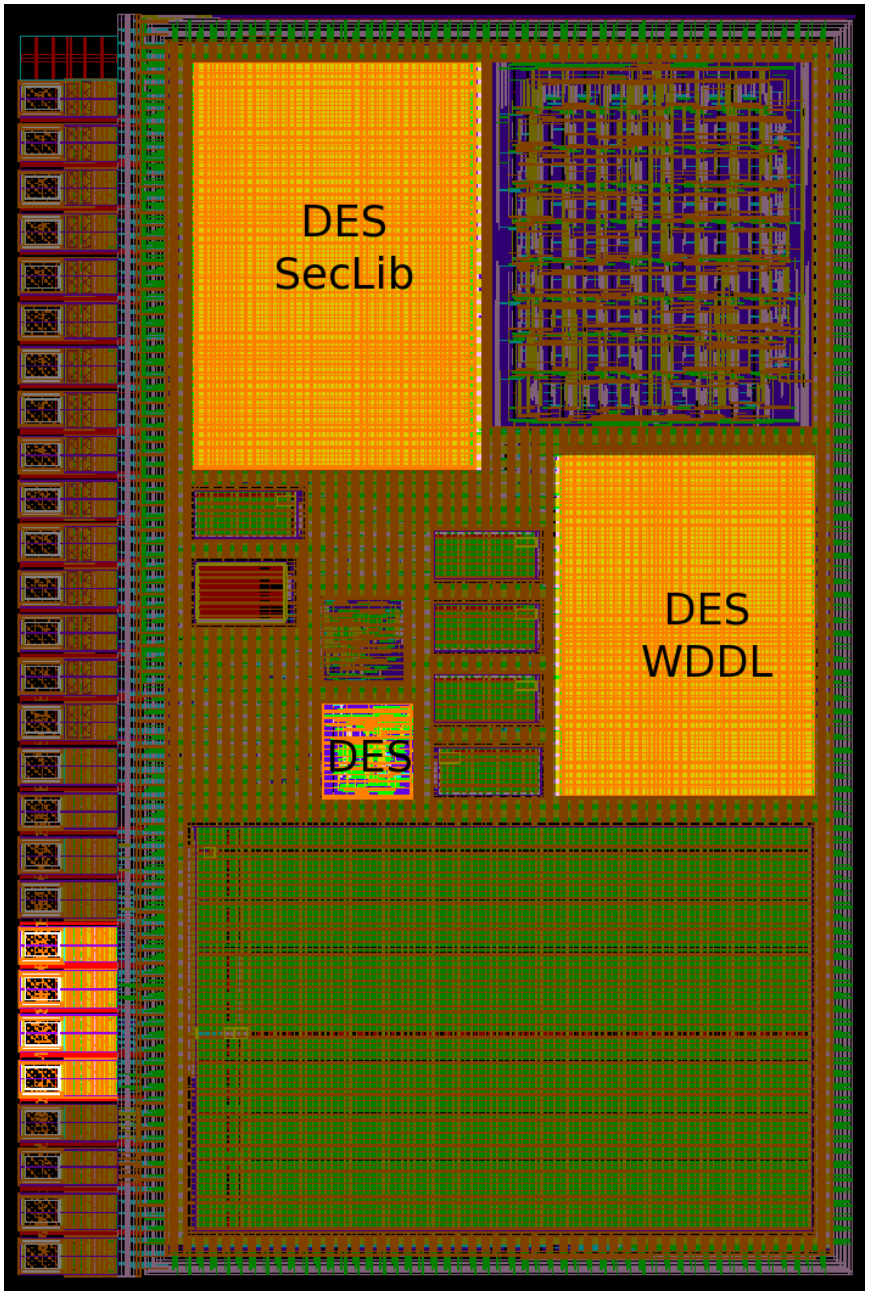
- From the same VHDL source code:
  1. **Unprotected**, and *reference* DES cipher
  2. **WDDL** DES
  3. **SecLib** DES
- **Protected instances** are **DPA-resistant** [5]



Template Attacks on DES [1]

- Using 32 points of interest for every SBOX
- Template = couple (average, standard deviation)
- Estimated for instance for every 8×2^6 sub-keys of DES



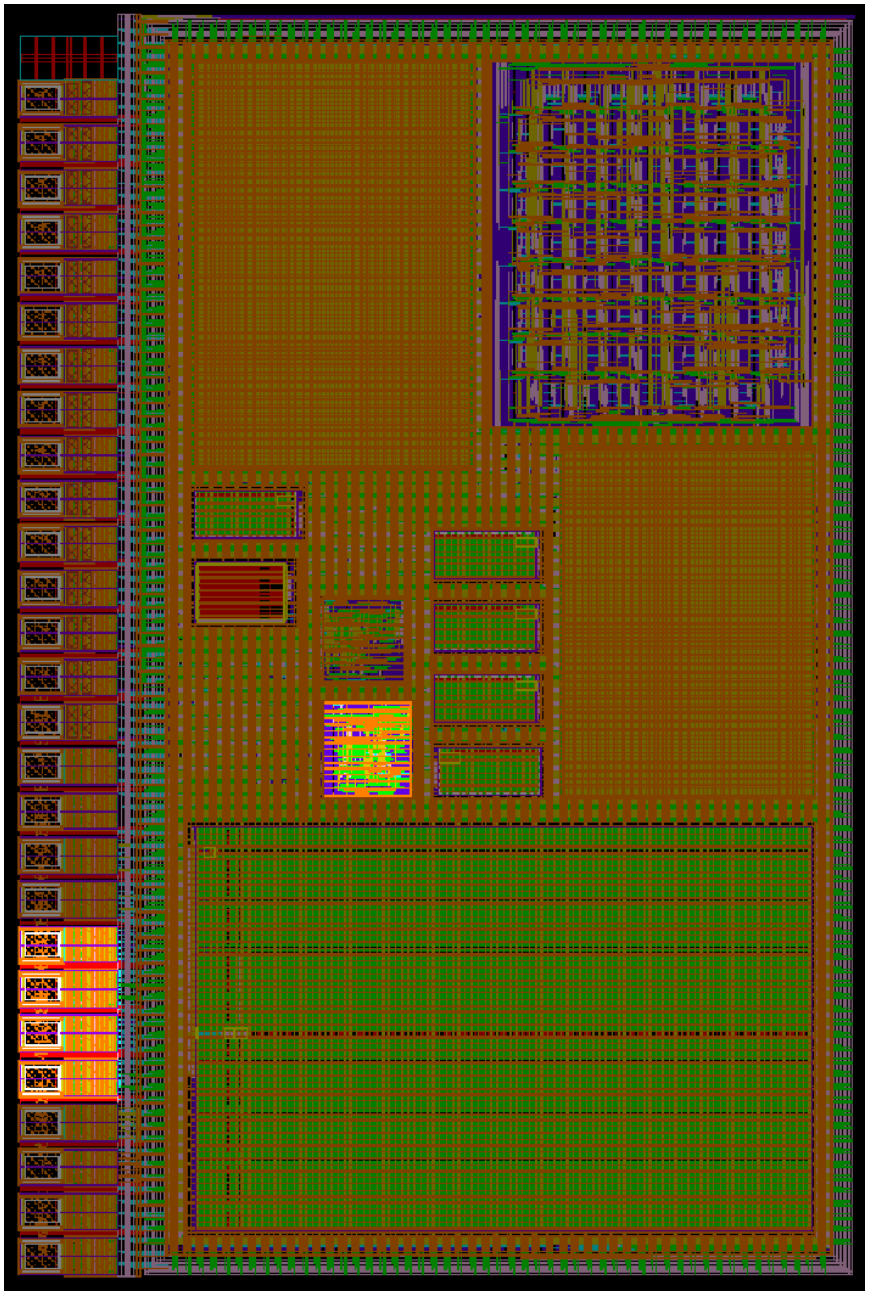


Successful attack

- Classification rate for one trace: 100 %
- Templates built from 20 000 power traces on DES
- 100 selected pts of interest
- Computation time: ~ 1 minute on `genie.enst.fr` (Intel Xeon @ 3 GHz)

Attack of protected DES: SecLib and WDDL

- So far: security gain > 350
- Result: WDDL $<$ SecLib security-wise

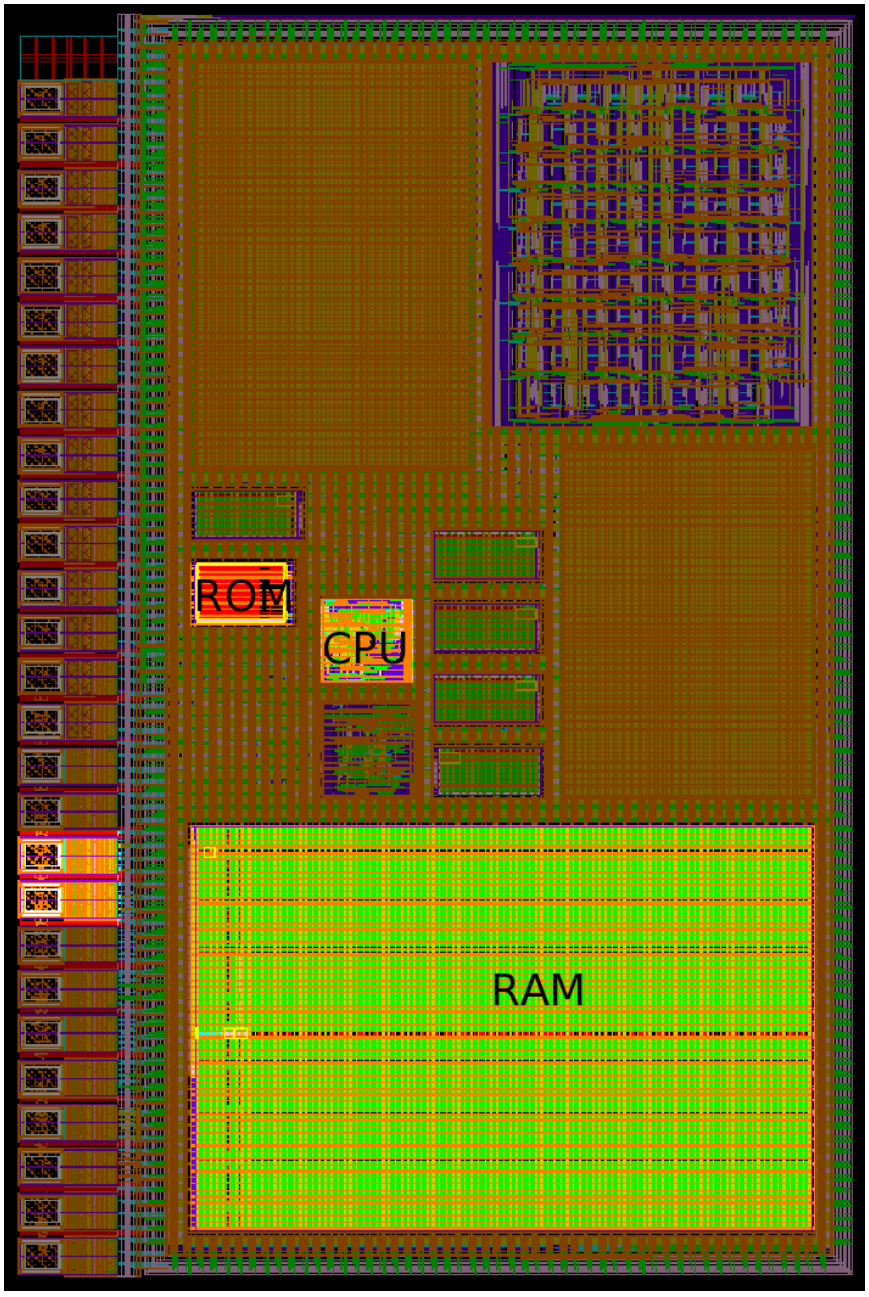


Either **under-powering** or **over-clocking** the crypto module

- Mimics a contact-less smartcard attack
- Practical attack on AES = G. Piret & J.-J. Quisquater

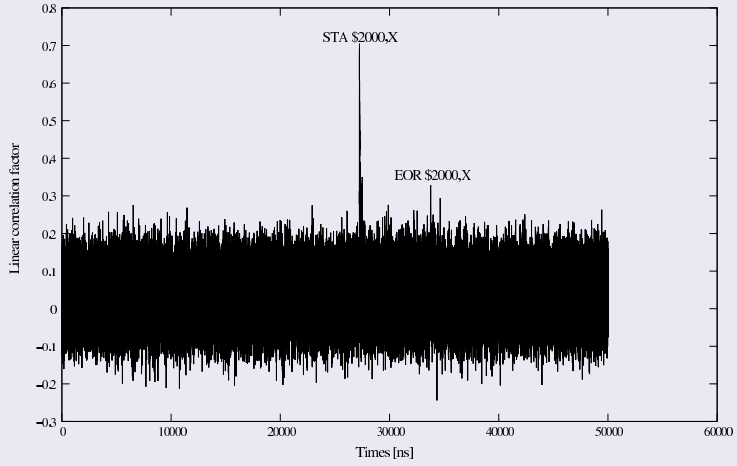
Status

- RTL simulation ..... ✔
- FPGA emulation ..... ✔
- Real-world ASIC ..... ✔
- Real-world FPGA ..... ✔
- Nidhal SELMANE's Master of Science + PhD work



SW Reverse-Engineering:

- $\hat{\rho}_{H,W} \doteq$ correlation between
  - H: power model
  - W: experimental waves



Our State-of-the-Art

- Reverse-engineering of:
  - Data ..... ✖
  - Code ..... ✔
  - Addresses ..... ✔

Presentation Outline

$\mathrm{DPA}_{\mathrm{diff}}$, $\mathrm{DPA}_{\mathrm{cov}}$ and CPA Oracles

Amongst the many oracles that have been proposed, we focus on three of them, noted:

1. $\mathrm{DPA}_{\mathrm{diff}}$: Differential Power Analysis (difference of means),
2. $\mathrm{DPA}_{\mathrm{cov}}$: Differential Power Analysis (covariance) and
3. CPA: Correlation Power Analysis,

defined in equations (1), (2) and (3).

The idea behind the $\mathrm{DPA}_{\mathrm{diff}}$ is to exhibit an asymptotic difference between the behaviors.
The "difference of means" criterion introduced by Paul Kocher is:

$$\mathrm{DPA}_{\mathrm{diff}} \doteq \frac{1}{m_0} \sum_{i/D_i=0} \mathbf{T}_i - \frac{1}{m_1} \sum_{i/D_i=1} \mathbf{T}_i \,, \tag{1}$$

where m_0 and m_1 denote the number of traces for each decision.
More specifically,

- $m_0 \doteq \#\{i \in [0, m[/ D_i = 0\}$ and, symmetrically,
- $m_1 \doteq \sum_{i=0}^{m-1} D_i$, with the following complementation property $m_0 + m_1 = m$.

$\mathrm{DPA}_{\mathrm{cov}}$

A seemingly different approach consists in computing a covariance between the m traces and their associated decision functions. The DPA covariance estimator is:

$$\mathrm{DPA}_{\mathrm{cov}} \doteq \frac{1}{m}\sum_i \mathbf{T}_i \times D_i - \frac{1}{m}\sum_i \mathbf{T}_i \times \frac{1}{m}\sum_i D_i \,. \qquad (2)$$

It **extracts** the contribution of D_i: only the net i is selected out of the whole netlist j [7].

$\mathrm{DPA}_{\mathrm{diff}}$ versus $\mathrm{DPA}_{\mathrm{cov}}$

The two definitions of the DPA actually coincide, as far as the decision function is balanced:

Proof.

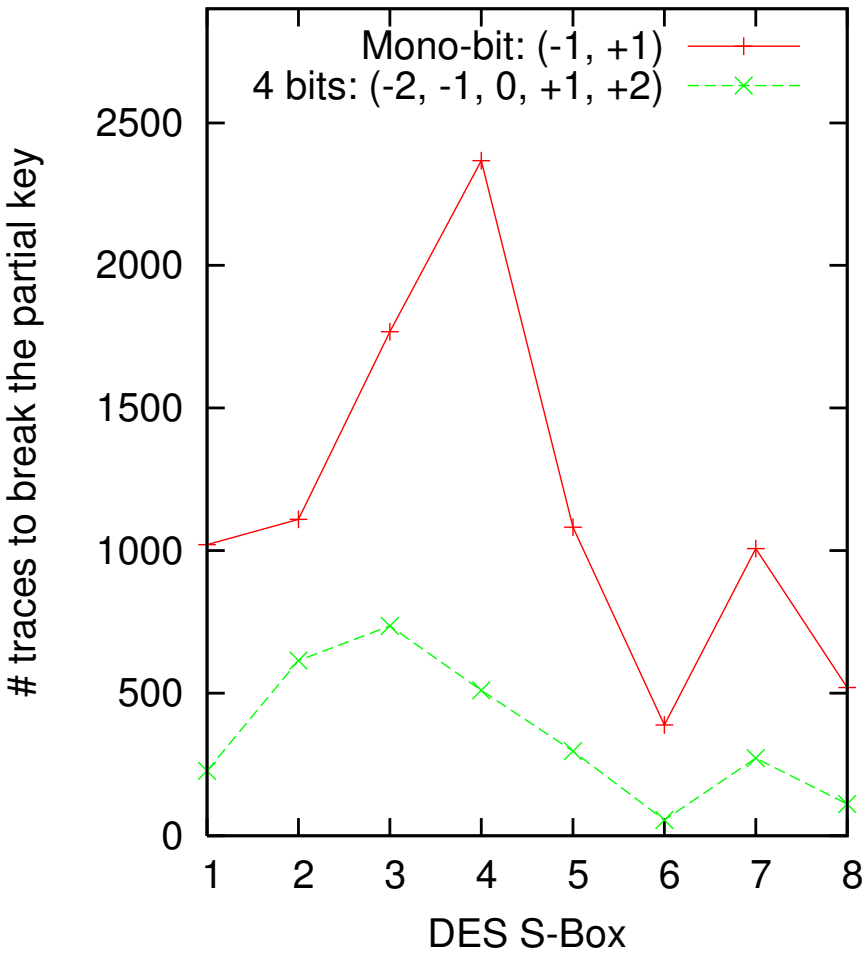
Assuming that $m_0 = m_1 = m/2$,

$$\begin{aligned}
\mathrm{DPA}_{\mathrm{cov}} &= \frac{1}{m}\sum_i \mathbf{T}_i \times \left(D_i - \frac{1}{2}\right) \\
&= \frac{1}{2m}\sum_i \mathbf{T}_i \times (-1)^{D_i} \quad \left\{ \begin{array}{l} \text{Covariance with} \\ \text{the character} \\ \text{function of } D. \end{array} \right. \\
&= \frac{1}{4}\,\mathrm{DPA}_{\mathrm{diff}}\,.
\end{aligned}$$

Mono-bit *versus* Multi-bit DPA

Vectorial Decision Function D

- $D \in \{0,1\}^n$
- Dominant practice: assume bits are indiscernible
- Hence partition traces according to $|D| \in [0, n]$
- Several philosophies:
  1. Thomas S. MESSERGES [11]: prune all but $|D| = 0$ or n, and continue à la mono-bit
  2. Éric BRIER [3]: weight the partitions with $|D|$
  3. Thanh-Ha LE [9, 8]: weight the partitions with $(-1, -2, 0, +2, +1)$



CPA

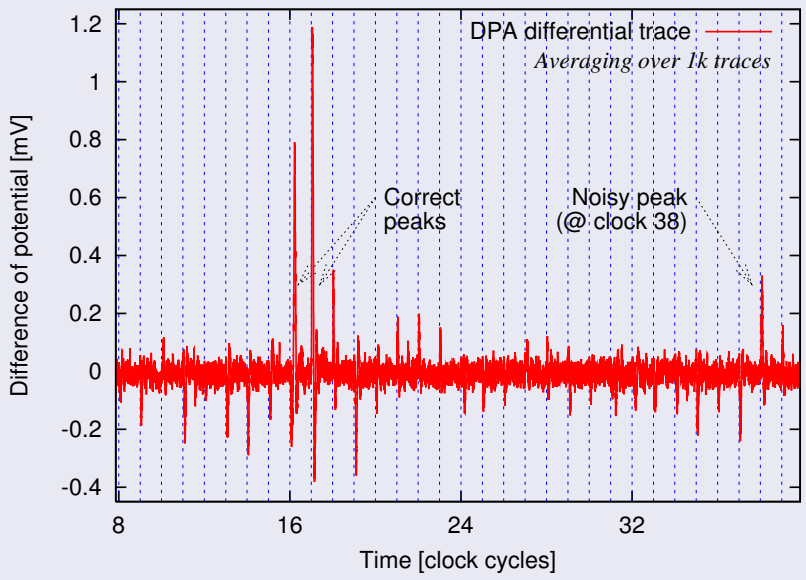
By definition [3], CPA is a normalization of the DPA. It is defined as a correlation coefficient, estimated by:

$$\mathrm{CPA} \doteq \frac{\mathrm{DPA}_{\mathrm{cov}}}{\sigma_{\mathbf{T}} \cdot \sigma_D} \in [-1, +1], \tag{3}$$

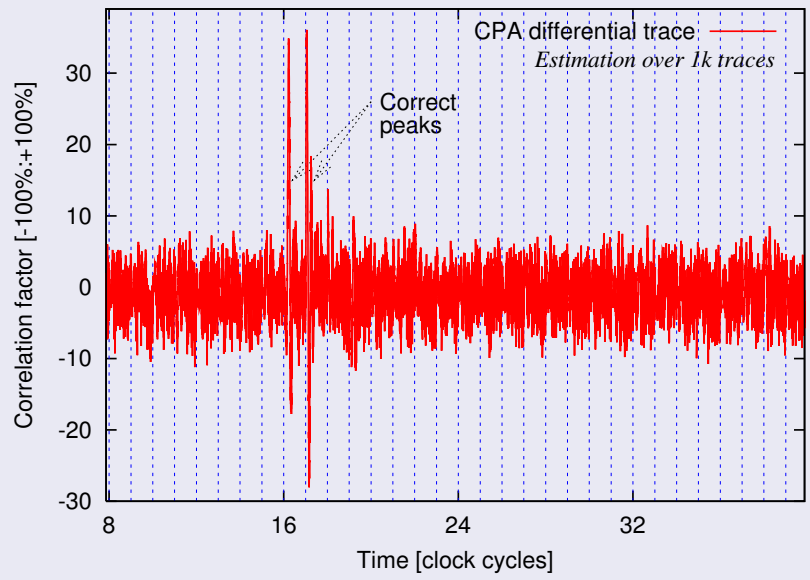
where σ_X is the standard deviation of the random variable X, for which an unbiased empirical estimator is $\sqrt{\frac{1}{m-1}\sum_{i=0}^{m-1}\left(X_i - \frac{1}{m}\sum_{j=0}^{m-1} X_j\right)^2}$.

DPA_{cov} versus CPA

DPA_{cov} after 1k traces

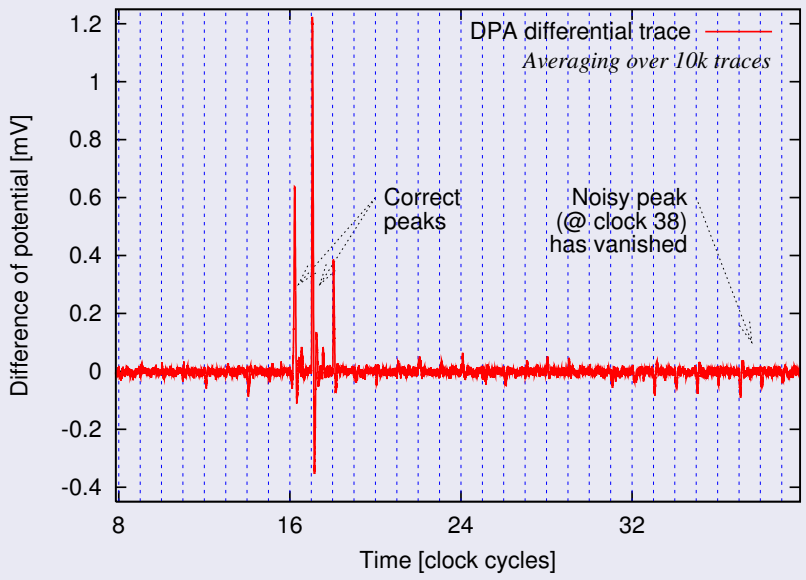


CPA after 1k traces

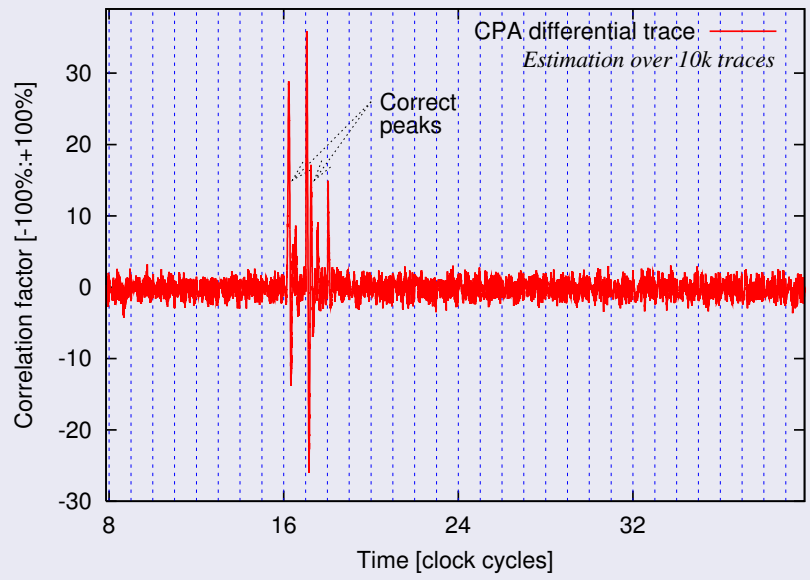


DPA_{cov} versus CPA

DPA_{cov} after 10k traces



CPA after 10k traces

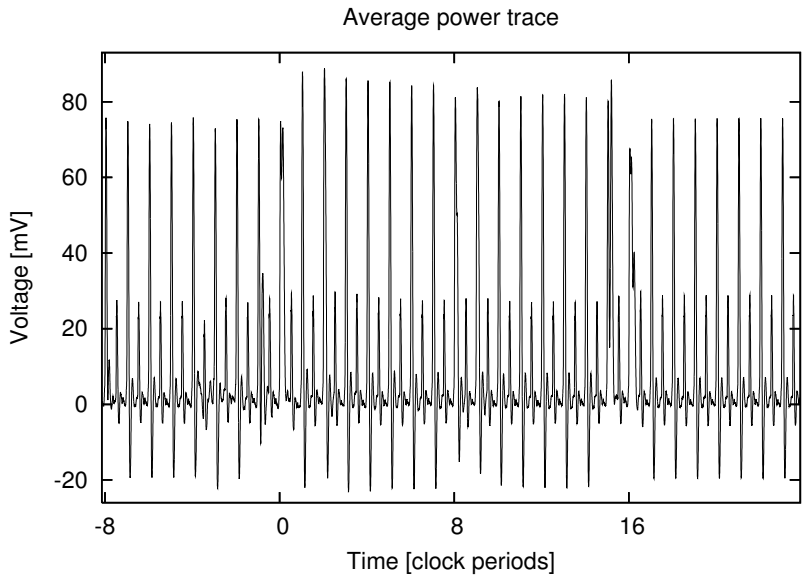


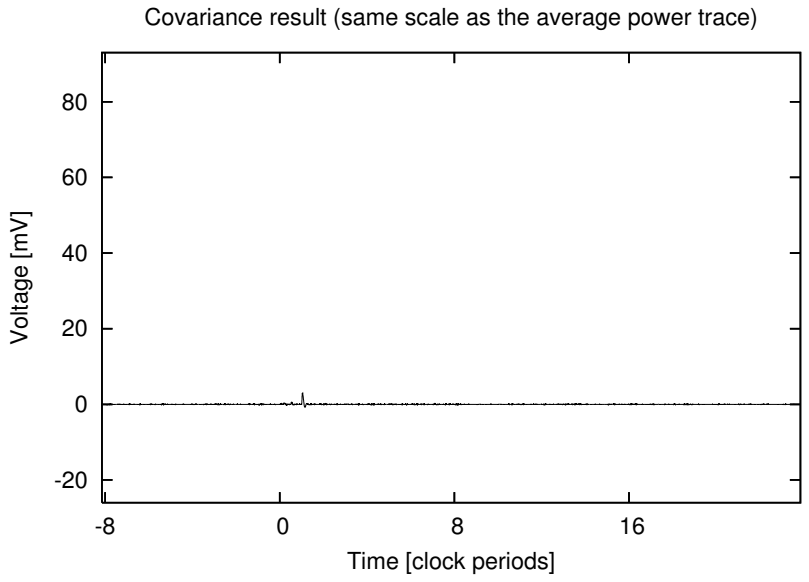
Comparison between SecMat v{1,3}[ASIC] & SecMat v3[FPGA] in terms of power leakage

- **SecMat v1[ASIC]:**
  - Dedicated power supply for the DES module
  - No clock tree (non-fatal bug)
- **SecMat v3[ASIC]:**
  - Shared power supply between all modules
  - Clock tree OK
- **SecMat v3[FPGA]:**
  - SecMat v3[ASIC] VHDL code synthesized in an Altera Stratix EPS1S25
  - Global power supply
  - 10,157 logic elements and 286,720 RAM bits for the whole SoC
  - DES alone is 1,125 logic elements (LuT4)

NEW! The power traces acquired from those three circuits are available for download from http://www.dpacontest.org/.

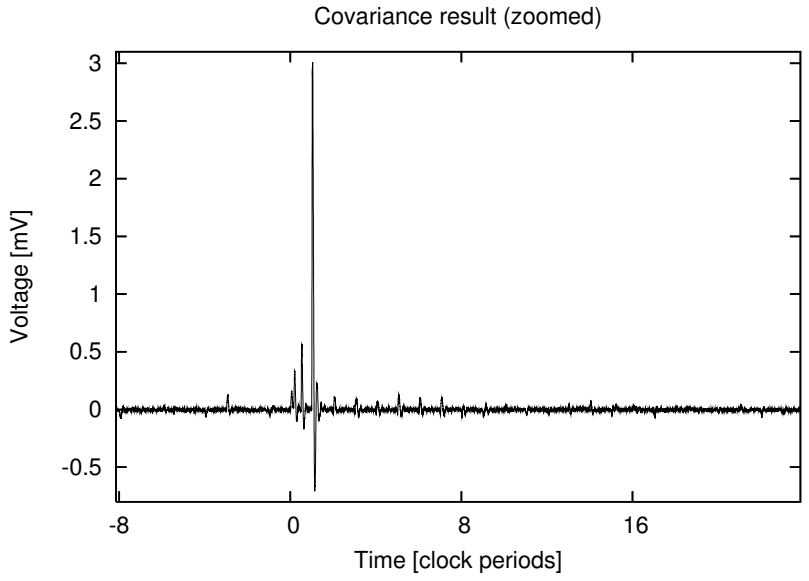
SecMat v1[ASIC] – covariance with $|LR[0] \oplus LR[1]|$



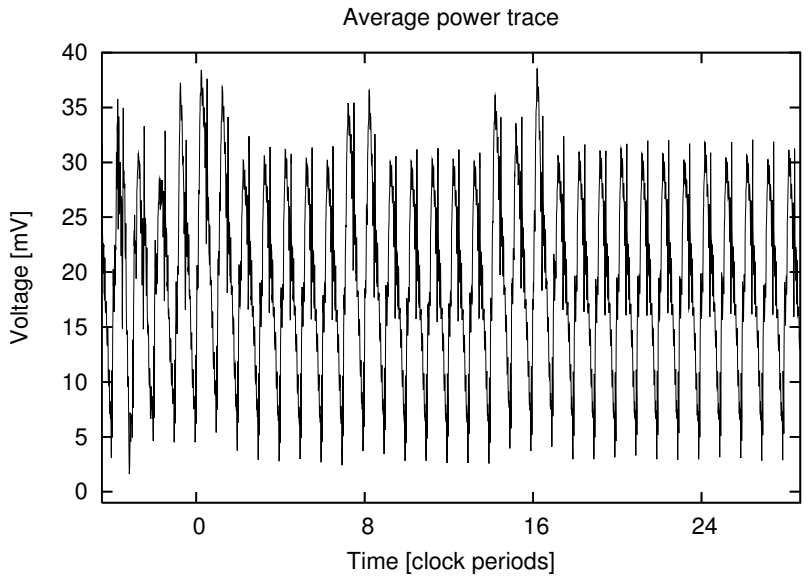


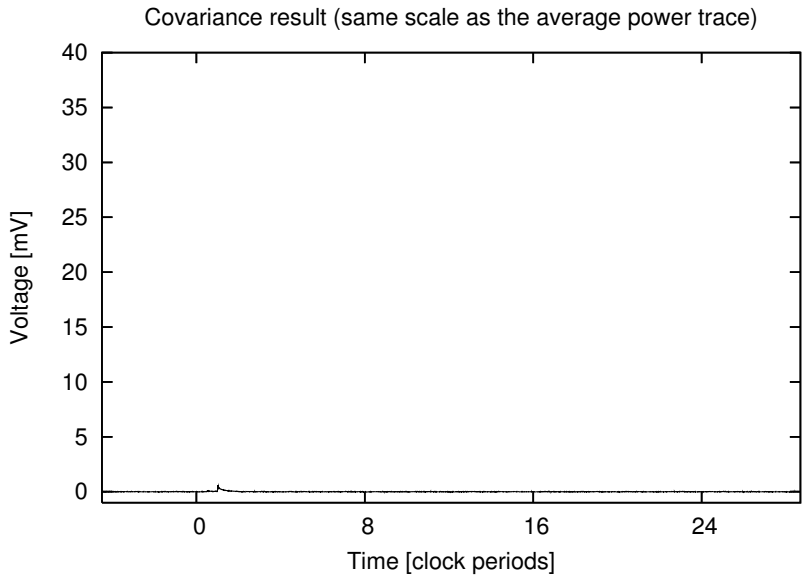
SecMat v1[ASIC]:

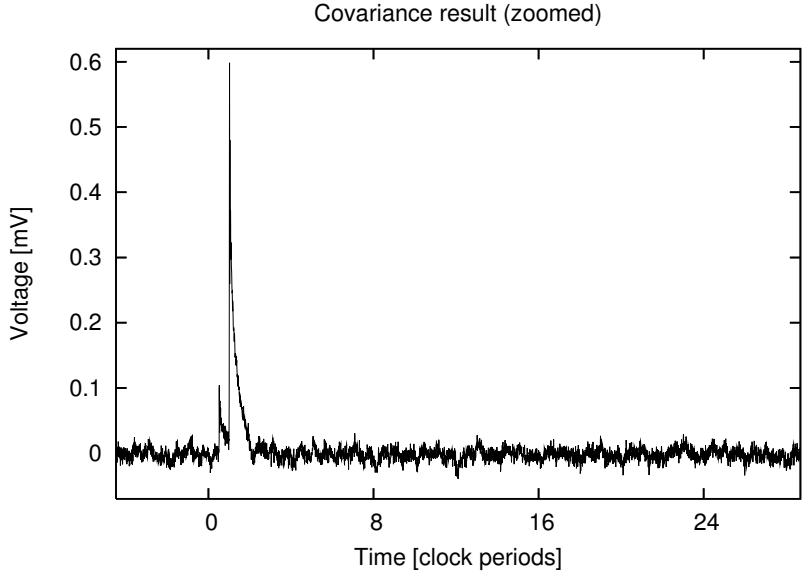
- Typical trace: 92 mV
- Typical DPA: 3.0 mV
- $\Rightarrow$ Side-channel leakage: 3.3 %



SecMat v3[ASIC] – covariance with $|LR[0] \oplus LR[1]|$



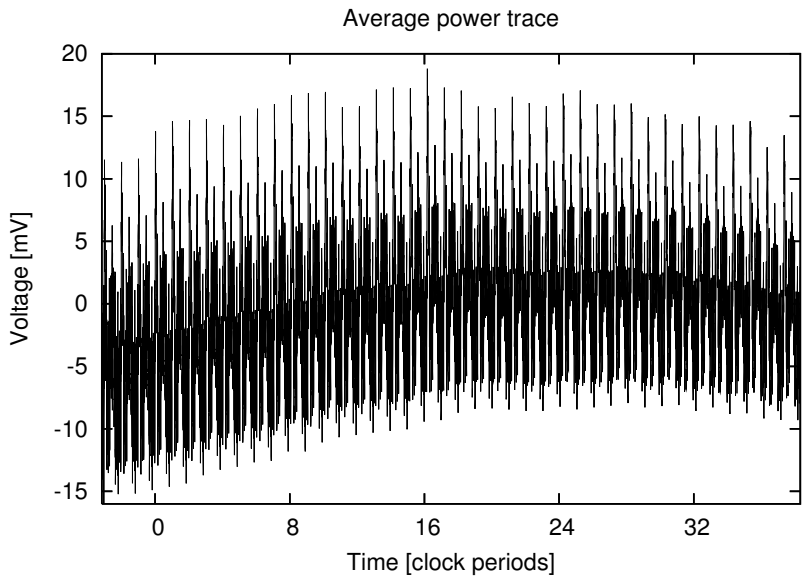


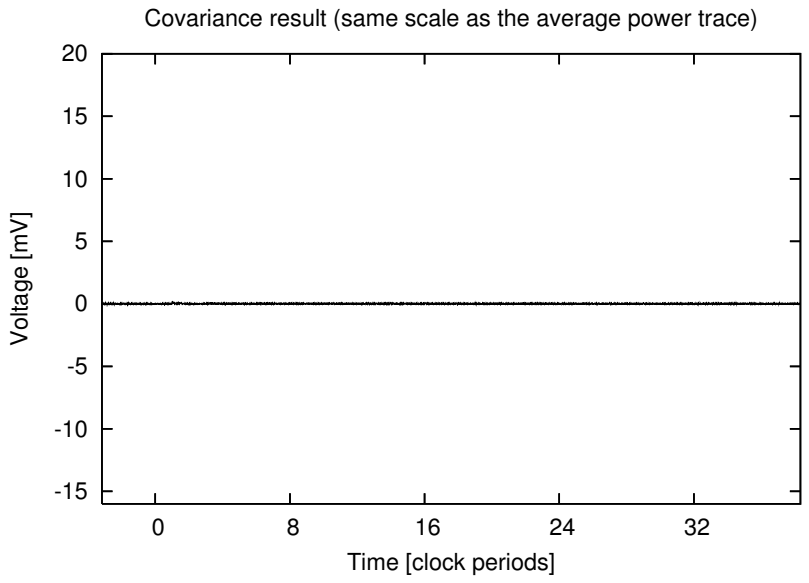


SecMat v3[ASIC]:

- Typical trace: 38 mV
- Typical DPA: 0.6 mV
- $\Rightarrow$ Side-channel leakage: 1.5 %

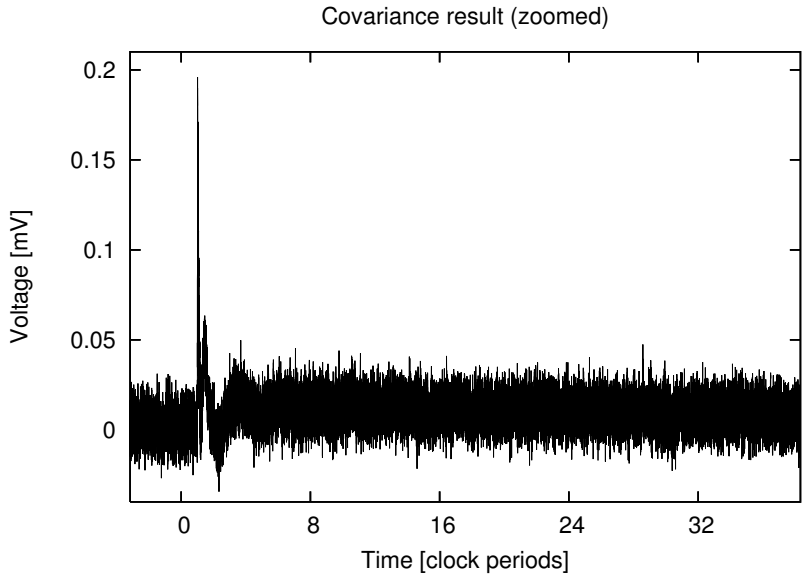
SecMat v3[FPGA] – covariance with $|LR[0] \oplus LR[1]|$





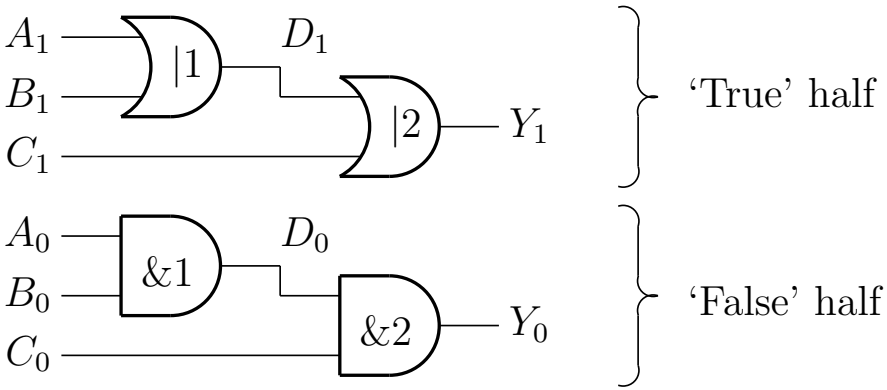
SecMat v3[FPGA]:

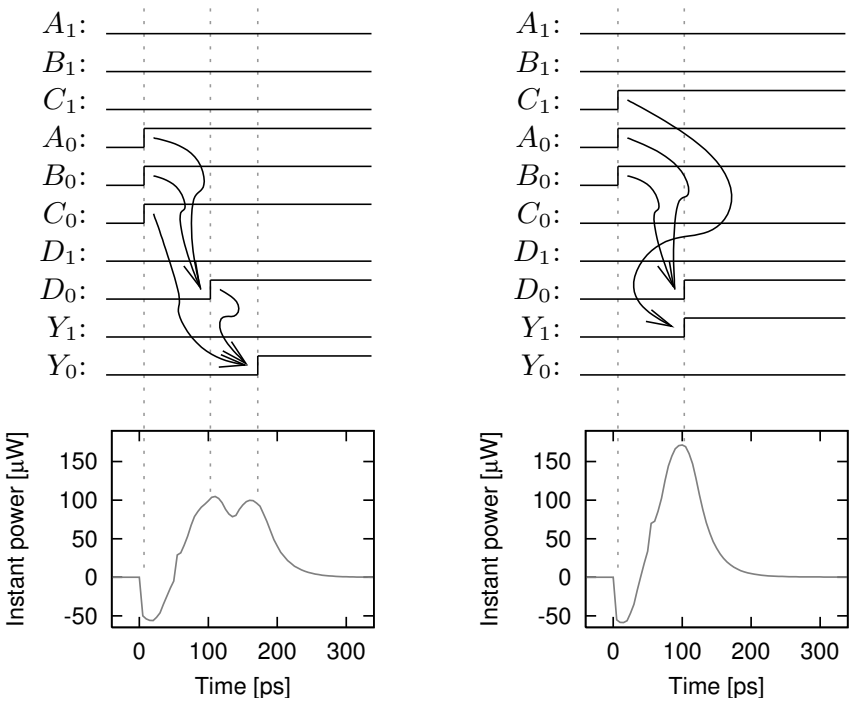
- Typical trace: 19 mV
- Typical DPA: 0.19 mV
- $\Rightarrow$ Side-channel leakage: 1.0 %
- $64/(2,125 \times 1 + (10,157 - 2,125) \times 0.5) \approx 1\ \% \Rightarrow$ **OK**



Early Evaluation in WDDL Illustrated

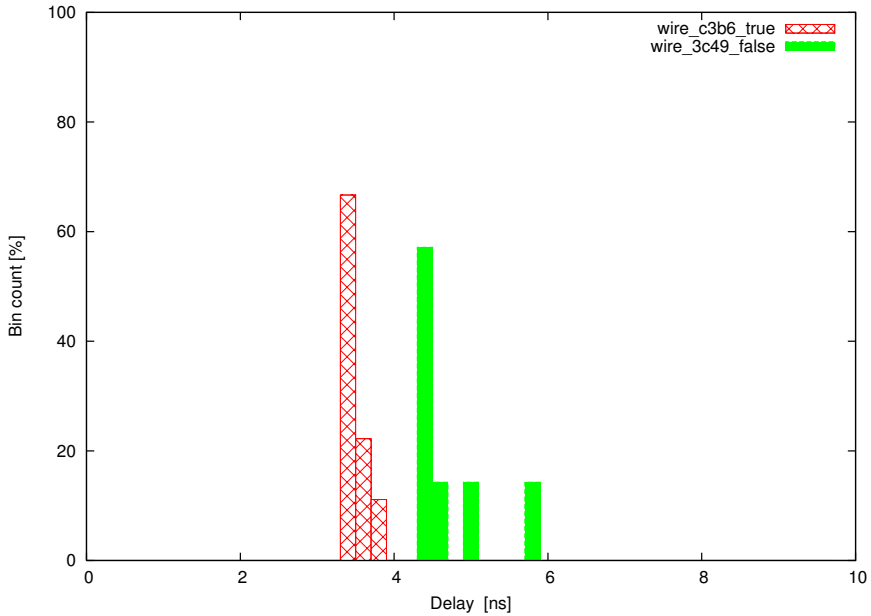
WDDL example and vulnerability:





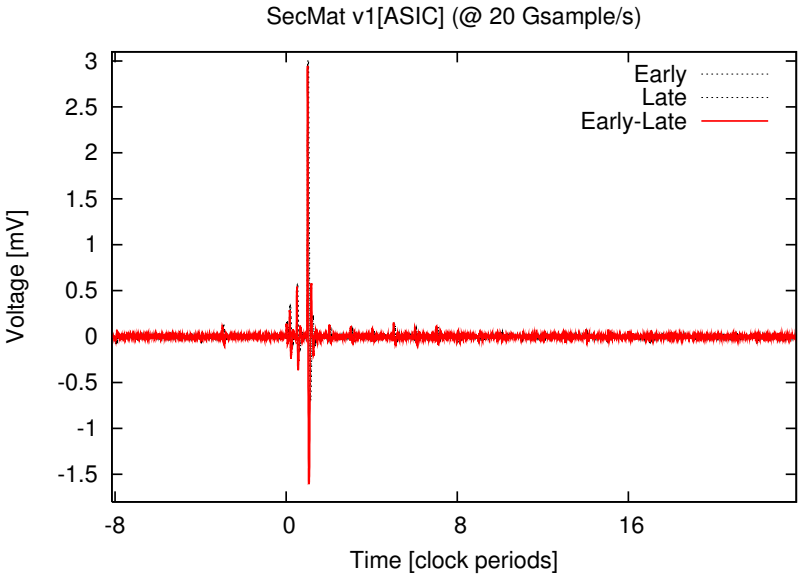
SDF Simulation on Altera [6]

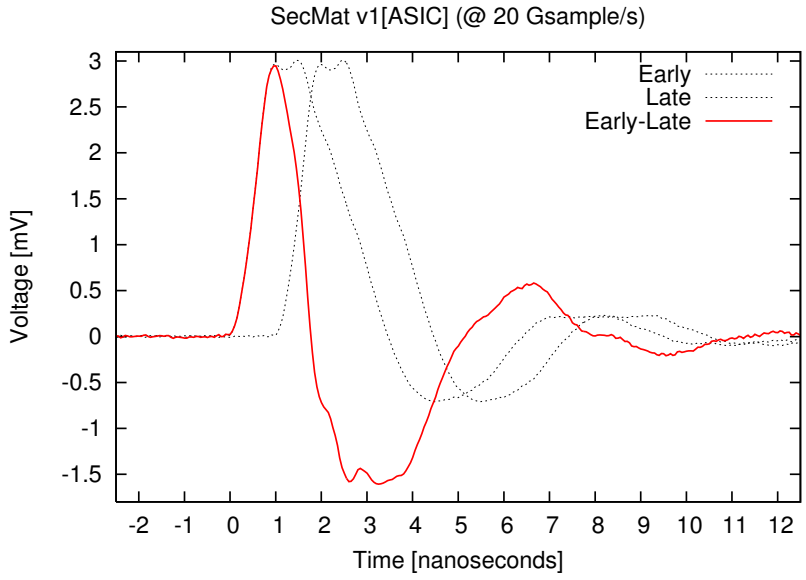
⇒ DES sbox #3



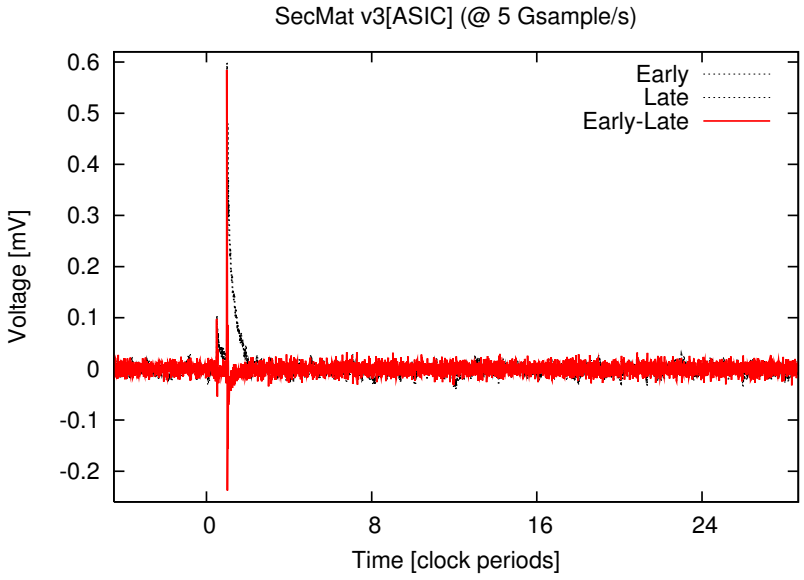
The 64 evaluation dates.

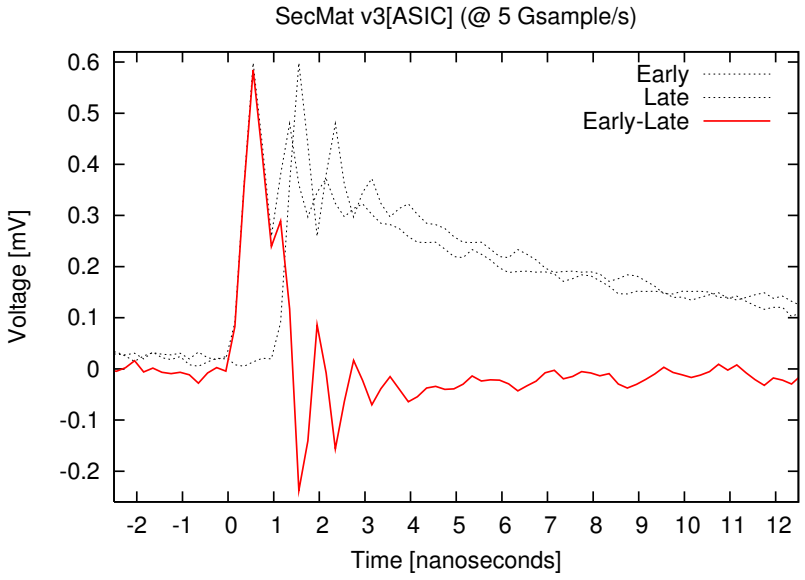
SecMat v1[ASIC] – Simulation of WDDL with 1 ns early evaluation



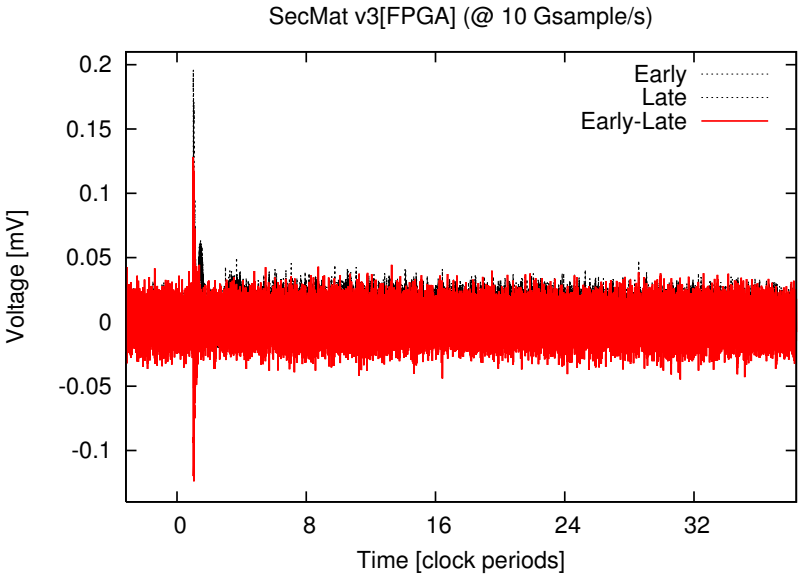


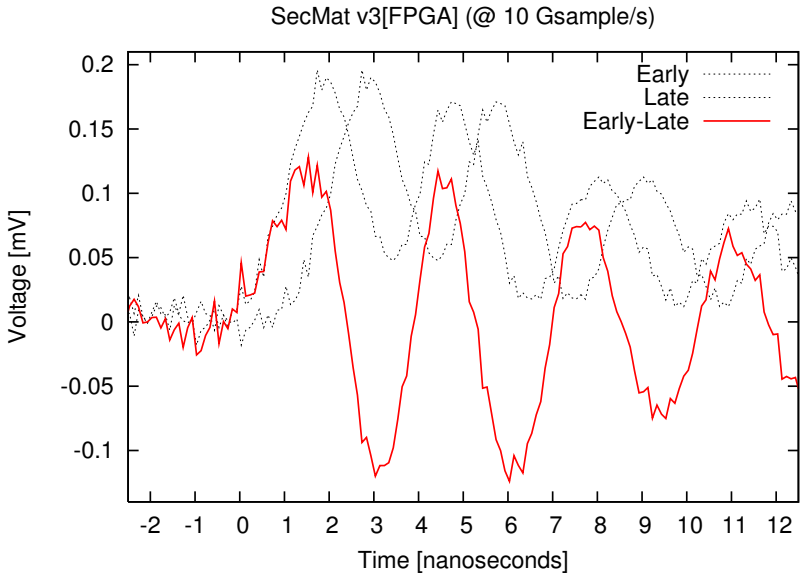
SecMat v3[ASIC] – Simulation of WDDL with 1 ns early evaluation





SecMat v3[FPGA] – Simulation of WDDL with 1 ns early evaluation





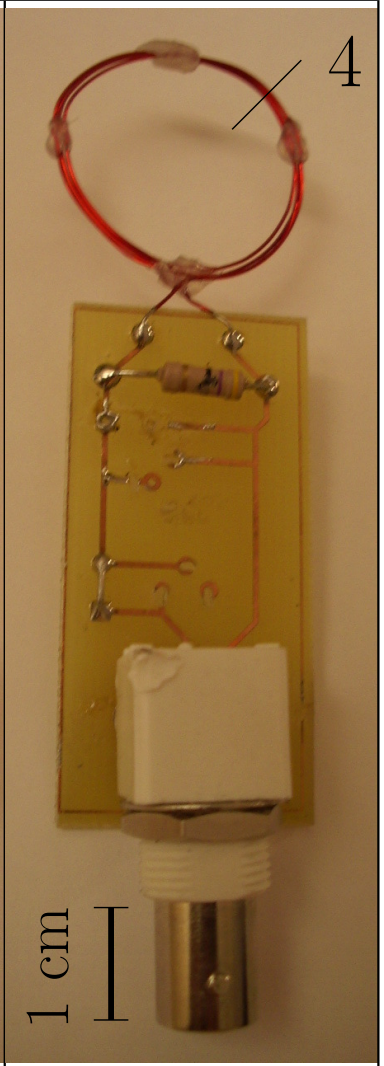
Summary about Power Leakage

- **1.0 % signal** in **99 % algorithmic noise** for a 32-bit register.
- Hence a $|\log_2(\frac{0.01}{32})| = \mathbf{11.6\text{-bit}}$ ADC for an acquisition w/o noise ...
- ... or at least $2^{11.6-8} = \mathbf{12\ times}$ averaging with an 8-bit ADC.

- For **unprotected** circuits,
  high Y-resolution is the key of success.

- For **protected** circuits,
  high X-resolution is the key of success.

Hand-Made ElectroMagnetic Sensors

Stranded copper core denuded coaxial cable (1)	**PCB coil (2)**	**Loop coil (3)**
Field: $\vec{E}$	**Field:** $\vec{H}$	**Field:** $\vec{H}$
		

ElectroMagnetic Attacks (EMA)

		# traces to break the key	
Sensor	**Averaging**	**Sbox #1**	**All sboxes**
50 Ω **resistor**	1×	176	940
50 Ω **resistor**	64×	231	518
Antenna (1)	256×	1,695	1,883
Antenna (2)	256×	1,066	1,786
Antenna (3)	256×	707	1,008

- *Less noise* in power than in EMA measurements
- However, EMA measurements are definitely *less intrusive*

Presentation Outline

DFA on AES: Attack of Gilles Piret & Jean-Jacques Quisquater [12]

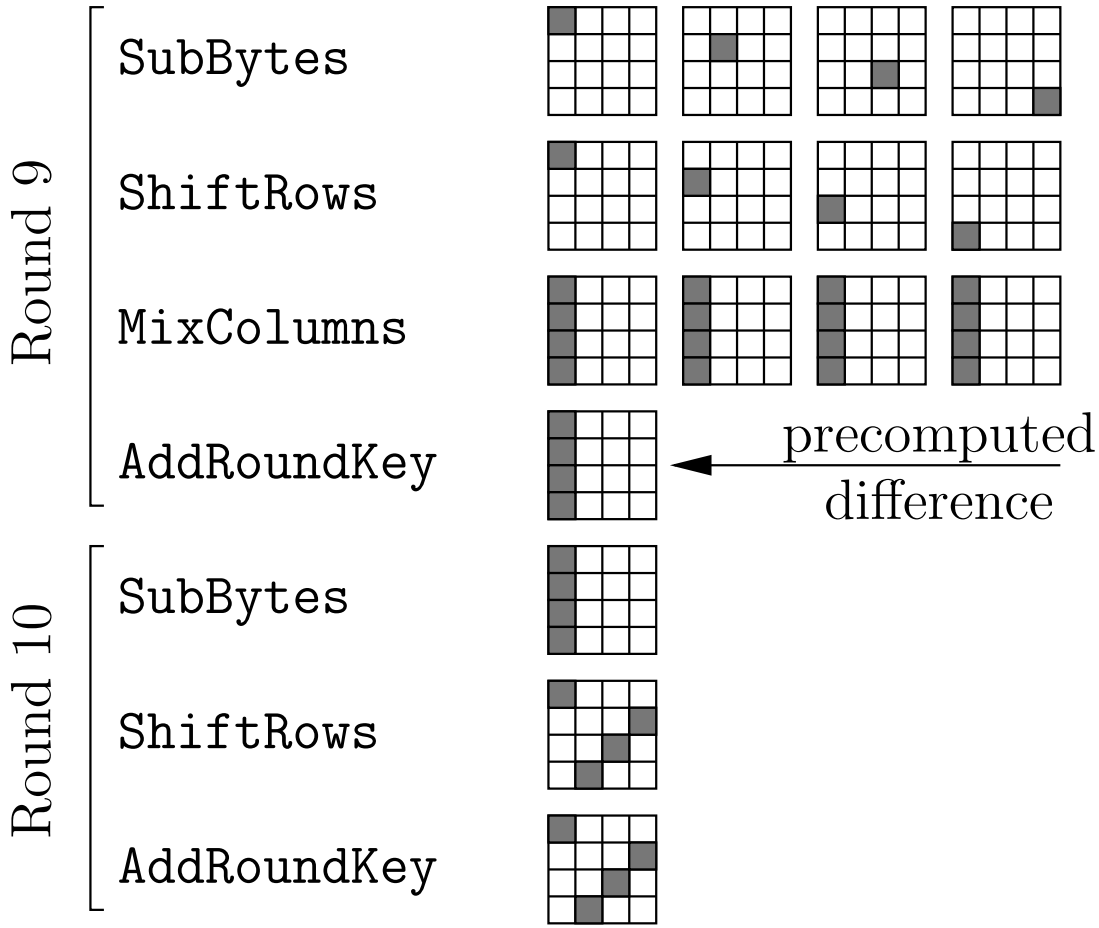
Fault Model

- A "byte-flip" fault is expected: this is a relaxed constraint w.r.t. Eli Biham & Adi Shamir's DFA.
- The fault spatio-temporal location needs not be known.

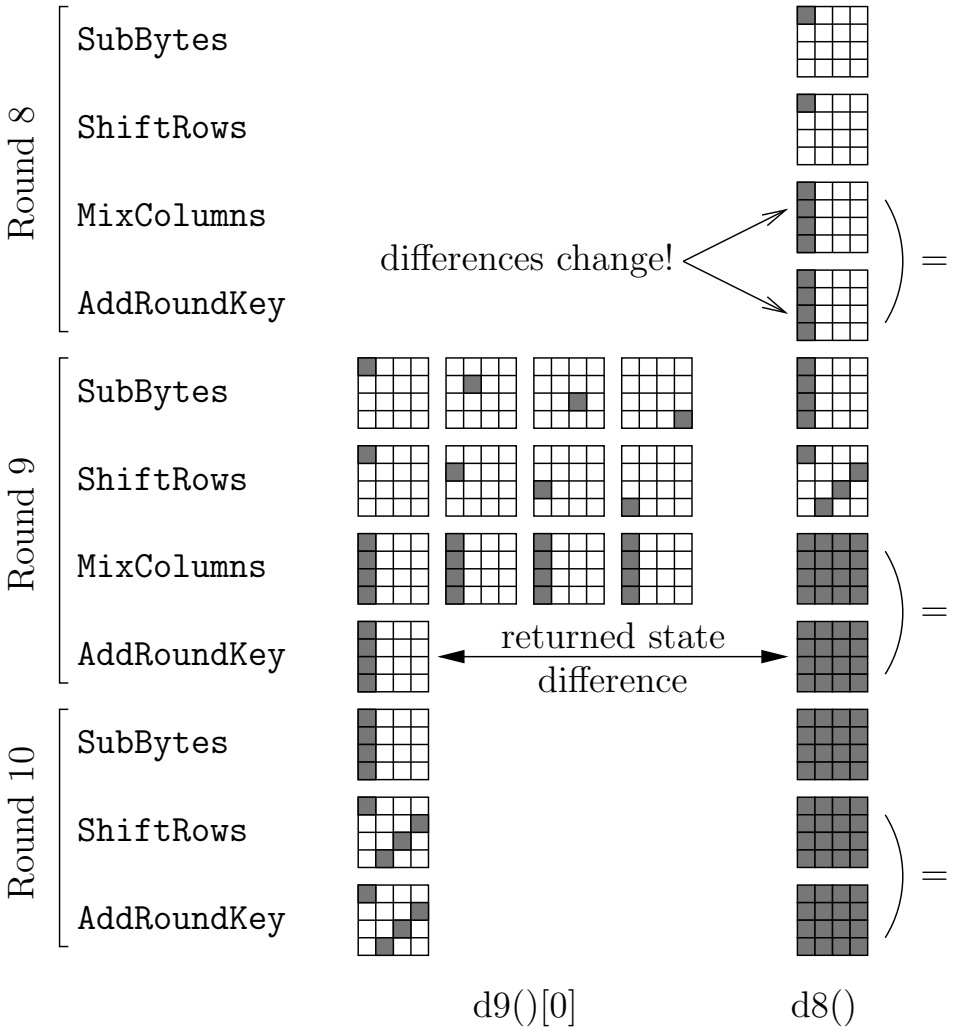
Attack Scenario

- The key is retrieved by columns.
- For all the $1\,020 = 255 \times 4$ hypotheses, find a collision.

G. Piret & J.-J. Quisquater in 2003



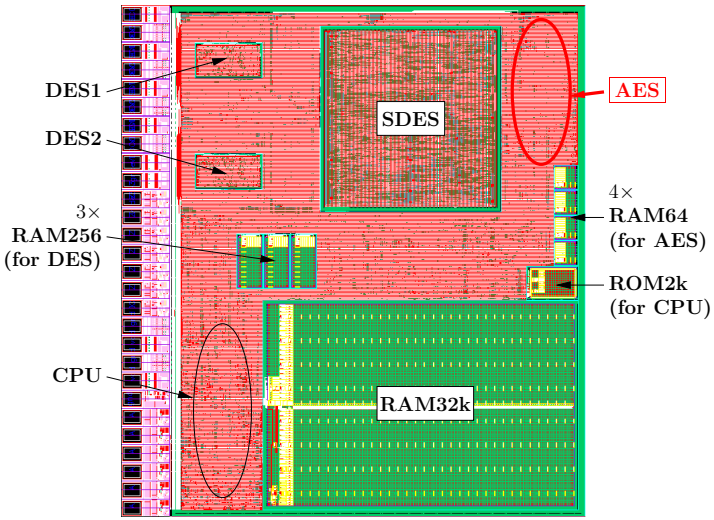
G. Piret & J.-J. Quisquater in 2003

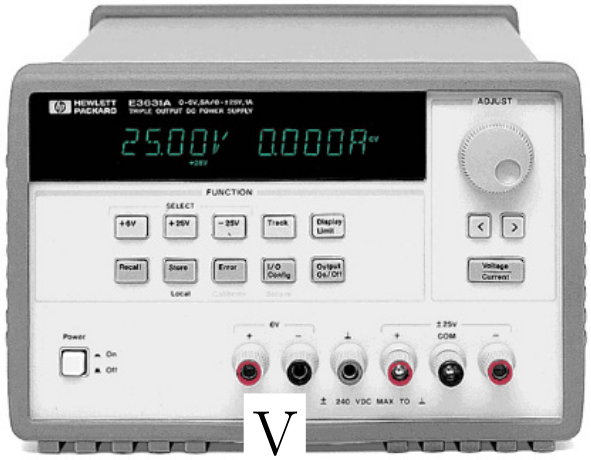


Kill 4 birds with one stone

A fault at round 8 yields 4 faults at round 9! This is optimal...

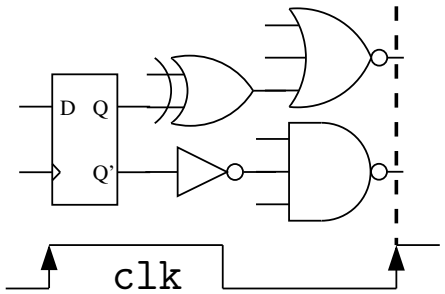
Faults Injection: Setup-Time Violation Attack Sketch



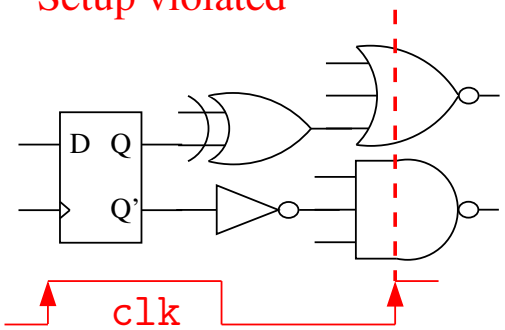


$$V \downarrow \quad \Rightarrow \quad T_{propagation} \uparrow$$

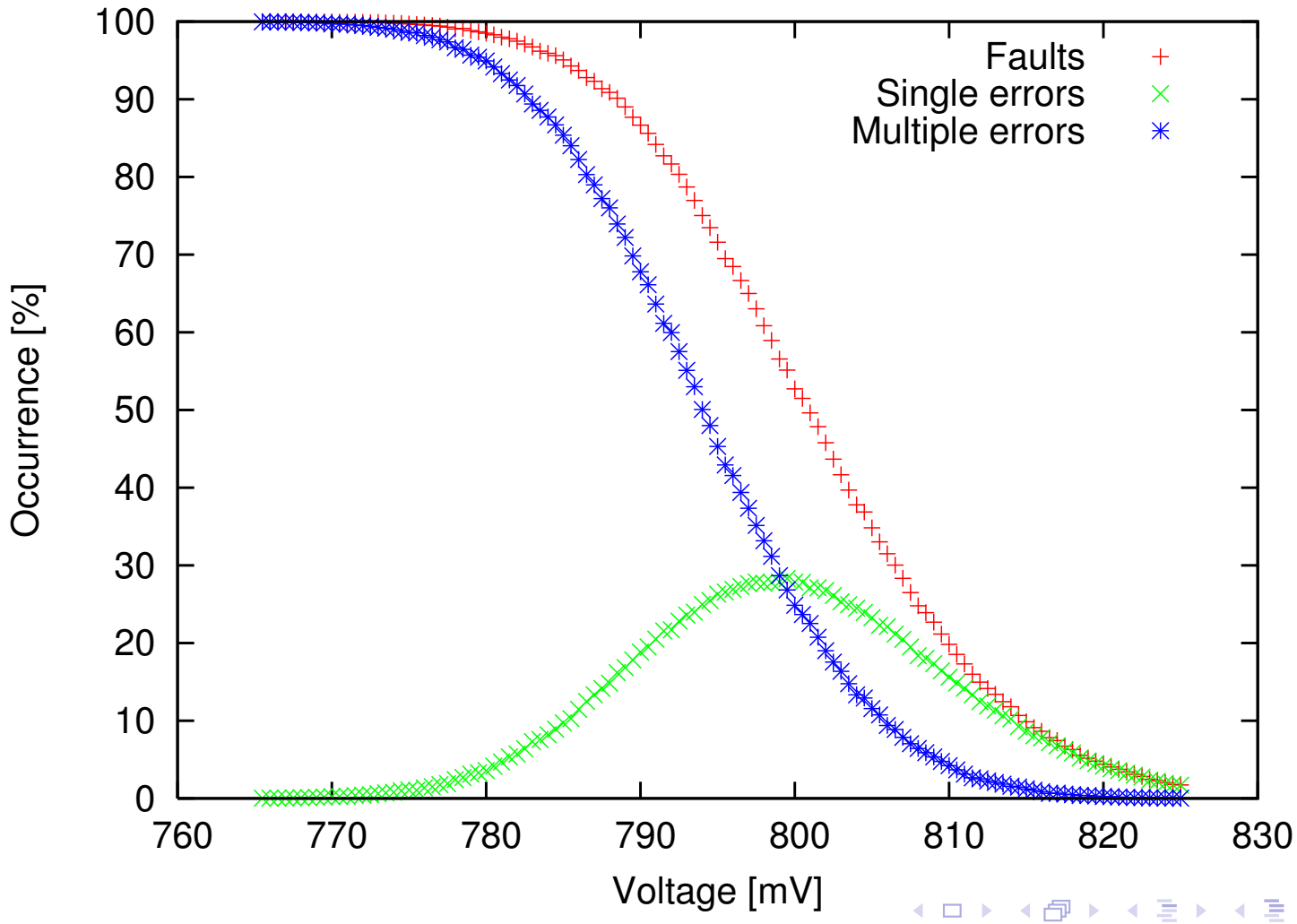
Setup met



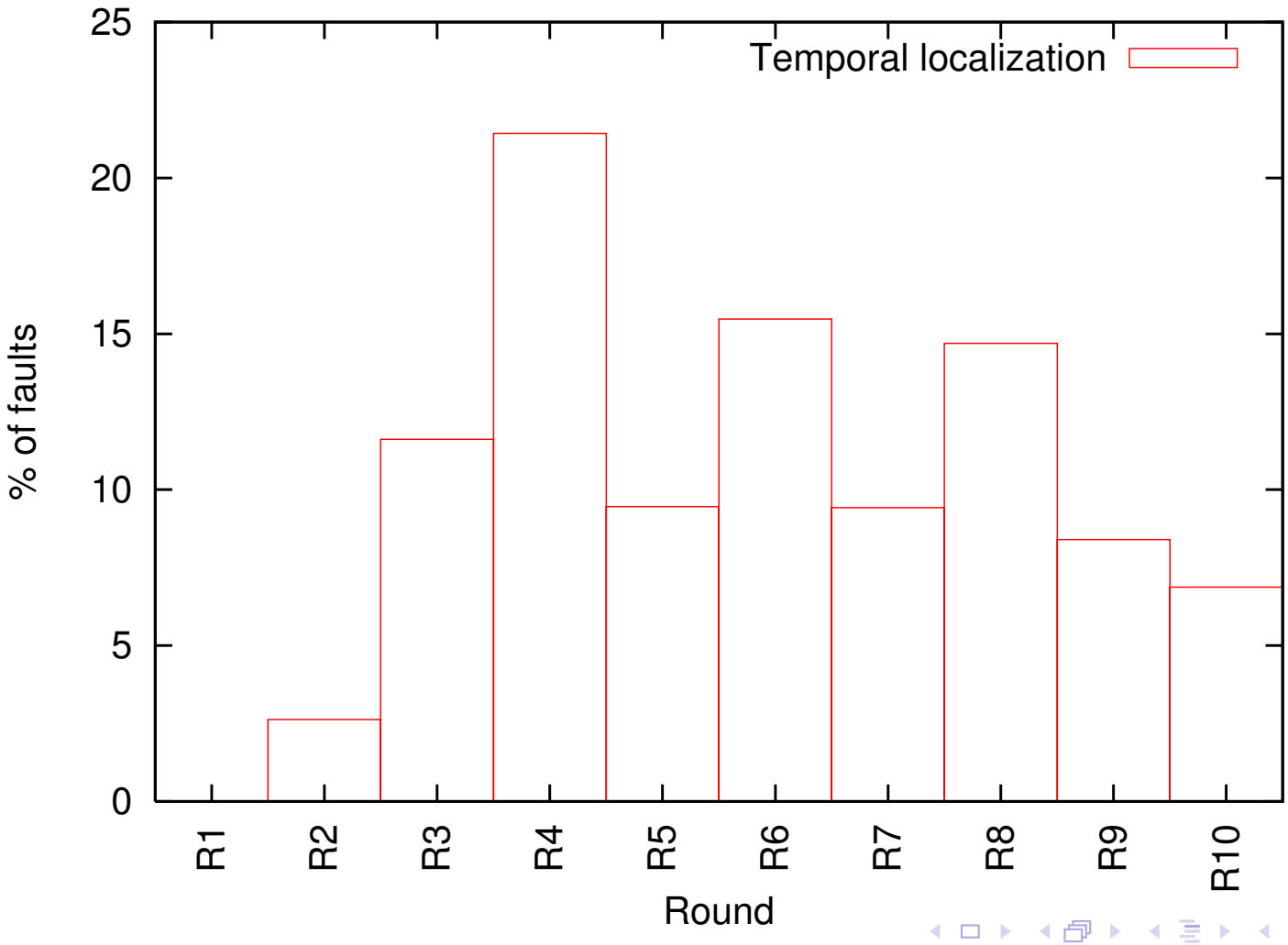
Setup violated



Occurrence [based on 2 000 000 encryptions on SecMat v1]

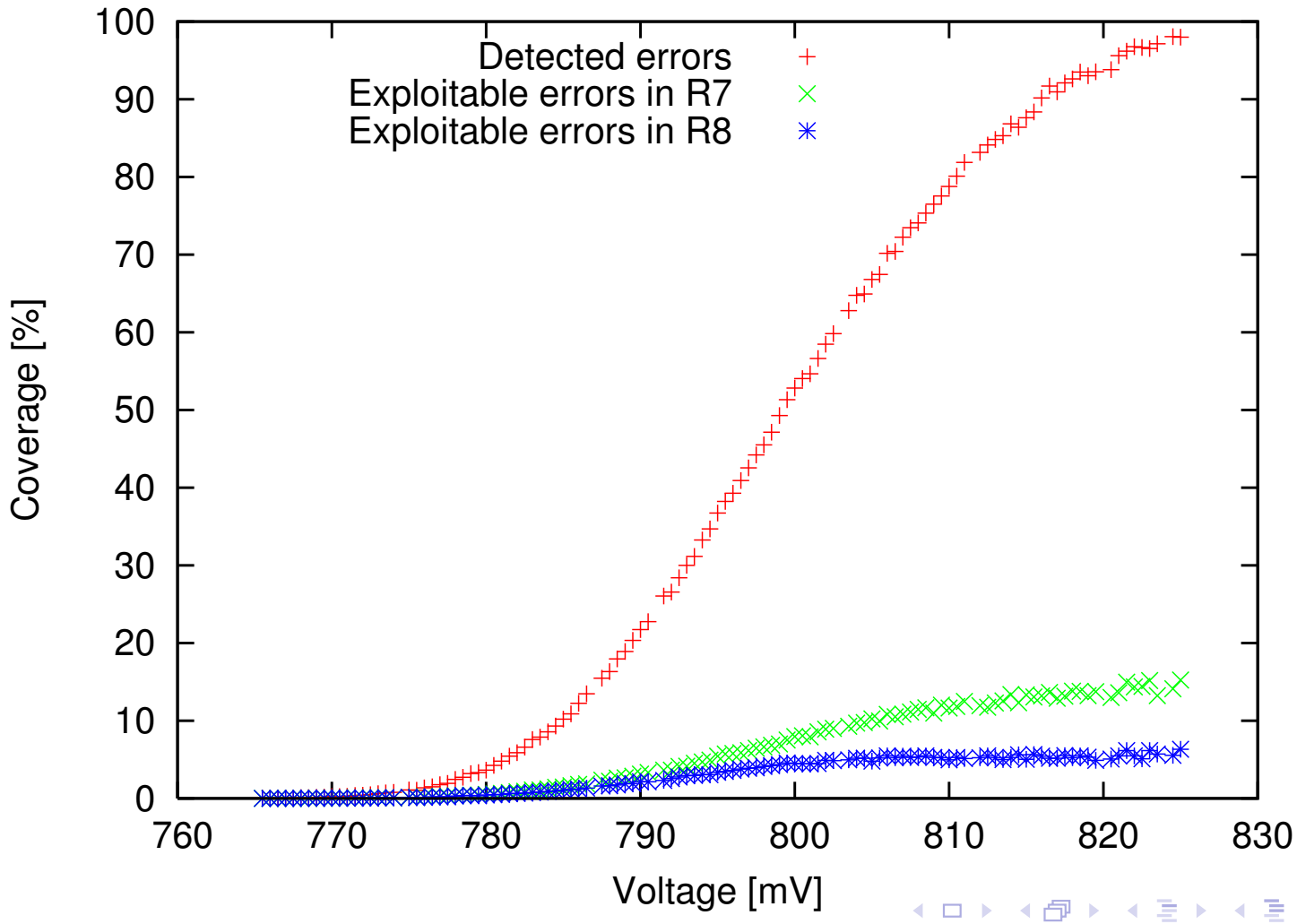


Round statistics

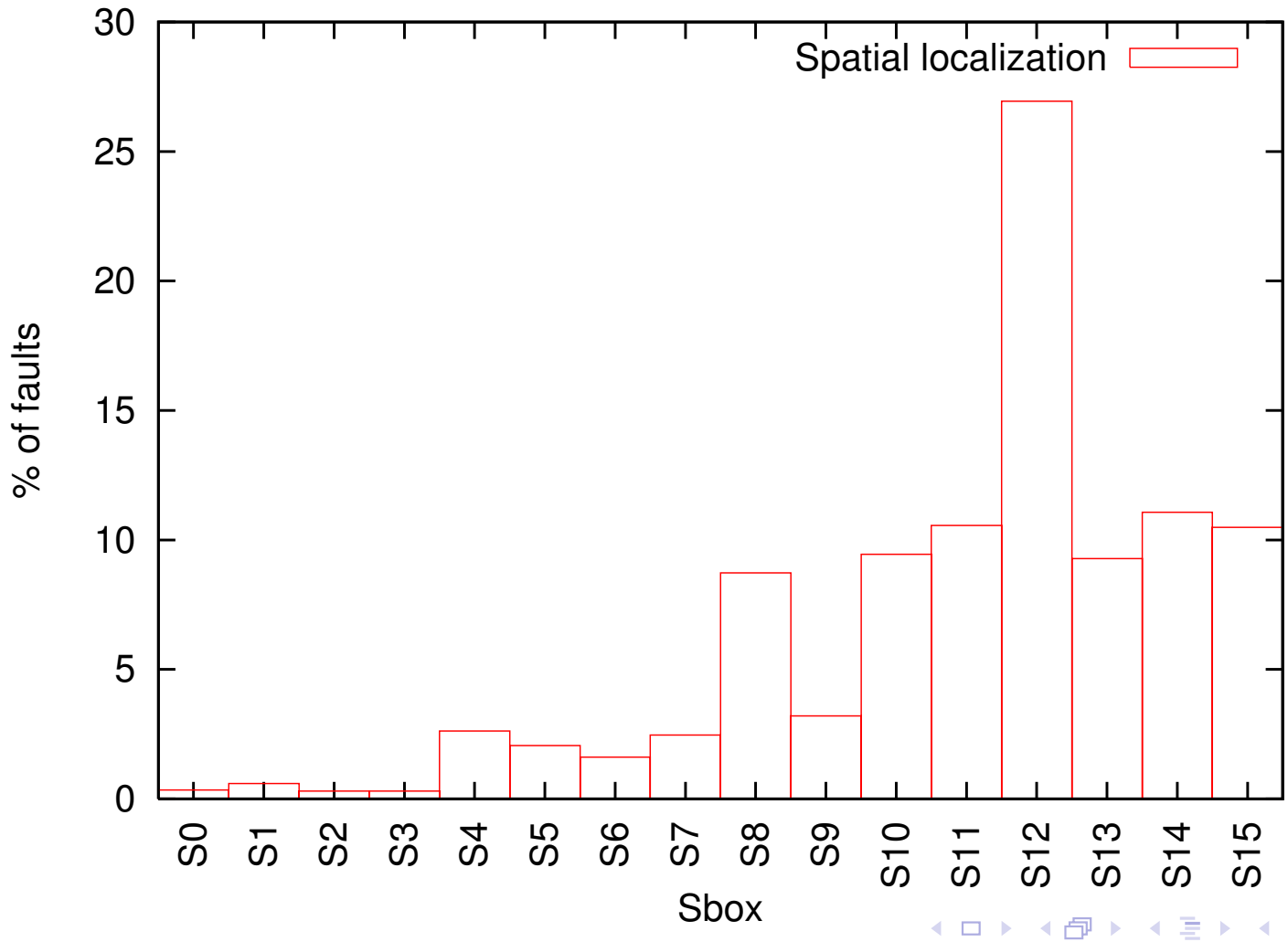


Coverage

About 20 % of Errors are Exploitable



Sbox statistics



Conclusion on DFA

- Confer to EDCC'08 [13] for the complete vulnerability analysis
- Non-intrusive DFA are possible
- Realized on SecMat v1[ASIC] and on an FPGA (forthcoming presentation @ NTMS'08).
- Works also if the **clock frequency** is changed
- Similar work done **on DES** successfully:
  randomness of errors is high enough for Biham & Shamir's attack [2]

Presentation Outline

DPA & DFA Canonical Counter-Measures

DPA Counter-Measures

- Combinatorial Logic:
  - $2\times$ for WDDL
  - $10\times$ for SecLib
- Routing:
  - $4\times$ for WDDL (2×2)
  - $9\times$ for WDDL with shield (3×3)

DFA Counter-Measures

- Captors: intensive, *i.e.* $\not\propto$ area,
- Error detection codes: $\alpha \propto$ area, with $\alpha \ll 1$.

Comparison between attacks

For an attack to be **successful**:

- DPA: about 1k traces
- DFA: $\frac{1}{20\ \%} \times 2 = 10$ interactions (*only!*).

Defense **cost**:

- DPA: at least 2× overhead
- DFA: a couple of sensors + "cheap" coding logic

In **summary**:

- DPA: easy to protect; but expensive
- DFA: difficult to protect; but inexpensive

Open Problems

- How to choose the most suitable correlation in CPA?
- How to make DPA counter-measures acceptable?
- How to efficiently merge DPA & DFA countermeasures?

Acknowledgements

- We sincerely acknowledge the compilation work done by http://www.sidechannelattacks.com/.
- Advanced Systems Technologies (AST) division of STMicroelectronics (Rousset in France and Milano in Italy).
- French Conseil Régional de la Région PACA.
- The Secure-IC team for intellectual support.
- DPA book [10], as a good introduction for students.

References

[1] Moulay Abdelaziz El Aabid, Sylvain Guilley, and Philippe Hoogvorst.
Template Attacks with a Power Model.
Cryptology ePrint Archive, Report 2007/443, December 2007.
http://eprint.iacr.org/2007/443/.

[2] Eli Biham and Adi Shamir.
Differential Fault Analysis of Secret Key Cryptosystems.
In *CRYPTO*, volume 1294 of *LNCS*, pages 513–525. Springer, 1997.

[3] Éric Brier, Christophe Clavier, and Francis Olivier.
Correlation Power Analysis with a Leakage Model.
Proc. of CHES'04, 3156:16–29, August 11–13 2004.
ISSN: 0302-9743; ISBN: 3-540-22666-4; DOI: 10.1007/b99451; Cambridge, MA, USA.

[4] Sumanta Chaudhuri, Sylvain Guilley, Florent Flament, Philippe Hoogvorst, and Jean-Luc Danger.
An 8x8 Run-Time Reconfigurable FPGA Embedded in a SoC.
In *DAC*, pages 120–125, Anaheim, CA, USA, jun 2008.

[5] S. Guilley, F. Flament, R. Pacalet, Ph. Hoogvorst, and Y. Mathieu.
Security Evaluation of a Secured Quasi-Delay Insensitive Library.
In *DCIS, full text in HAL, http://hal.archives-ouvertes.fr/hal-00283405/en/*, pages 1–7, November 2008.
DCIS'08, Grenoble, France.

[6] Sylvain Guilley, Sumanta Chaudhuri, Laurent Sauvage, Tarik Graba, Jean-Luc Danger, Philippe Hoogvorst, Ving-Nga Vong, and Maxime Nassar.
Shall we trust WDDL?
In *Future of Trust in Computing*, volume 2, Berlin, Germany, jun 2008.

[7] Sylvain Guilley, Philippe Hoogvorst, Renaud Pacalet, and Johannes Schmidt.
Improving Side-Channel Attacks by Exploiting Substitution Boxes Properties.

In *BFCA – http://www.liafa.jussieu.fr/bfca/*, pages 1–25, 2007.
May 02–04, Paris, France.

[8] Thanh-Ha Le, Cécile Canovas, and Jessy Clédière.
An overview of side channel analysis attacks.
In *ASIACCS*, pages 33–43, 2008.

[9] Thanh-Ha Le, Jessy Clédière, Cécile Canovas, Bruno Robisson, Christine Servière, and Jean-Louis Lacoume.
A Proposition for Correlation Power Analysis Enhancement.
In *CHES*, volume 4249 of *LNCS*, pages 174–186. Springer, 2006.
Yokohama, Japan.

[10] Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
Power Analysis Attacks: Revealing the Secrets of Smart Cards.
Springer, December 2006.
ISBN 0-387-30857-1, http://www.dpabook.org/.

[11] Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan.
Investigations of Power Analysis Attacks on Smartcards.
In *USENIX — Smartcard'99*, pages 151–162, May 10–11 1999.
Chicago, Illinois, USA (Online PDF).

[12] Gilles Piret and Jean-Jacques Quisquater.
A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD.
In *CHES*, volume 2779 of *LNCS*, pages 77–88. Springer, 2003.
(Online PDF version).

[13] Nidhal Selmane, Sylvain Guilley, and Jean-Luc Danger.
Setup Time Violation Attacks on AES.
In *EDCC, The seventh European Dependable Computing Conference*, pages 91–96, Kaunas, Lithuania, may 2008.
ISBN: 978-0-7695-3138-0, DOI: 10.1109/EDCC-7.2008.11.