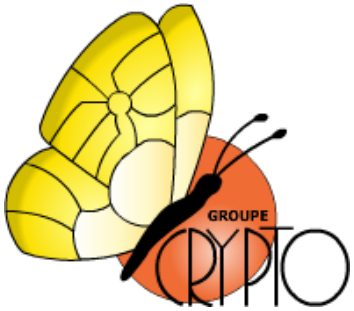
Understanding the Limitations and Improving the Relevance of SPICE Simulations in Security Evaluations

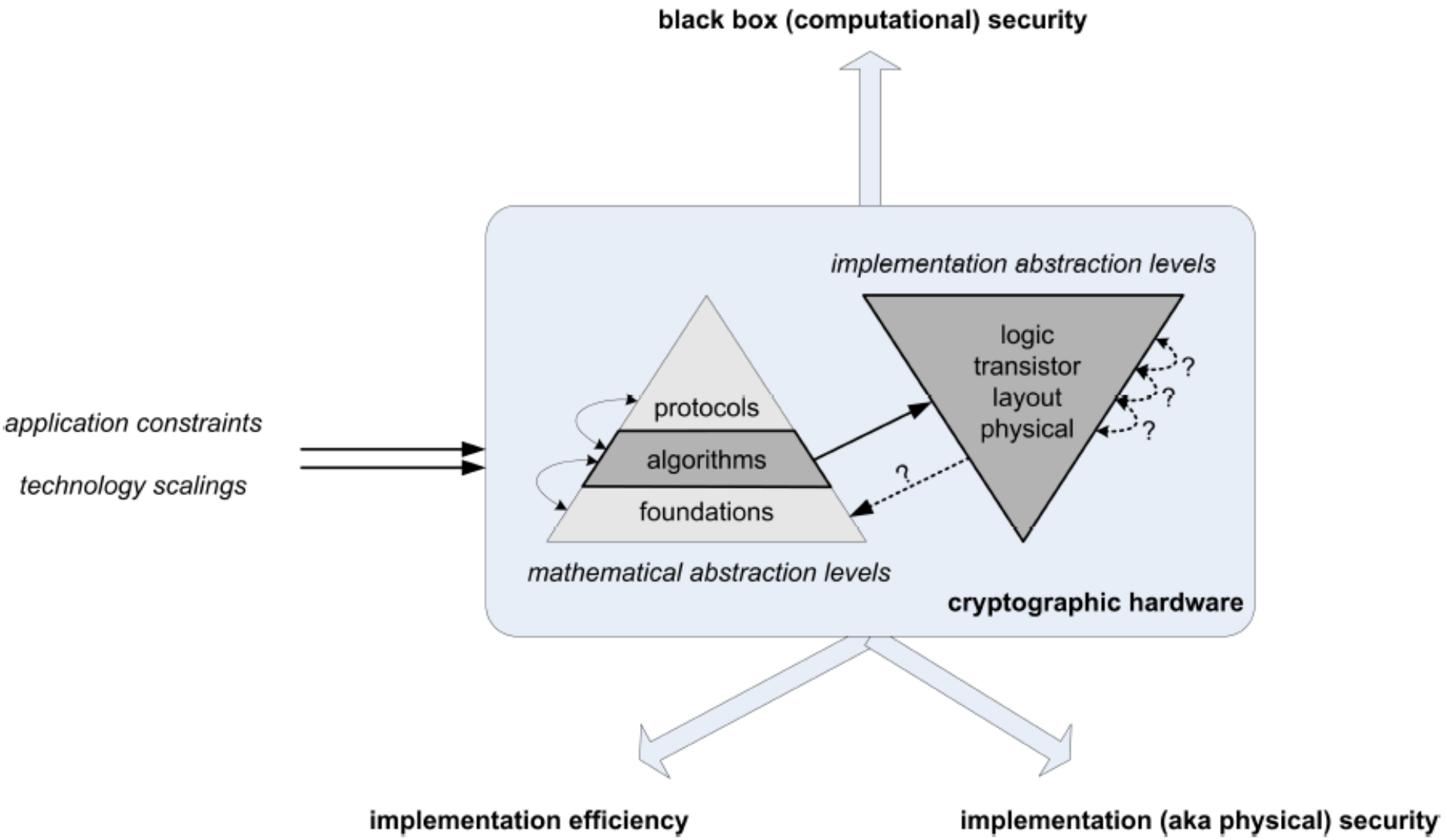
Dina Kamel, Mathieu Renauld, Denis Flandre,
François-Xavier Standaert

UCL Crypto Group

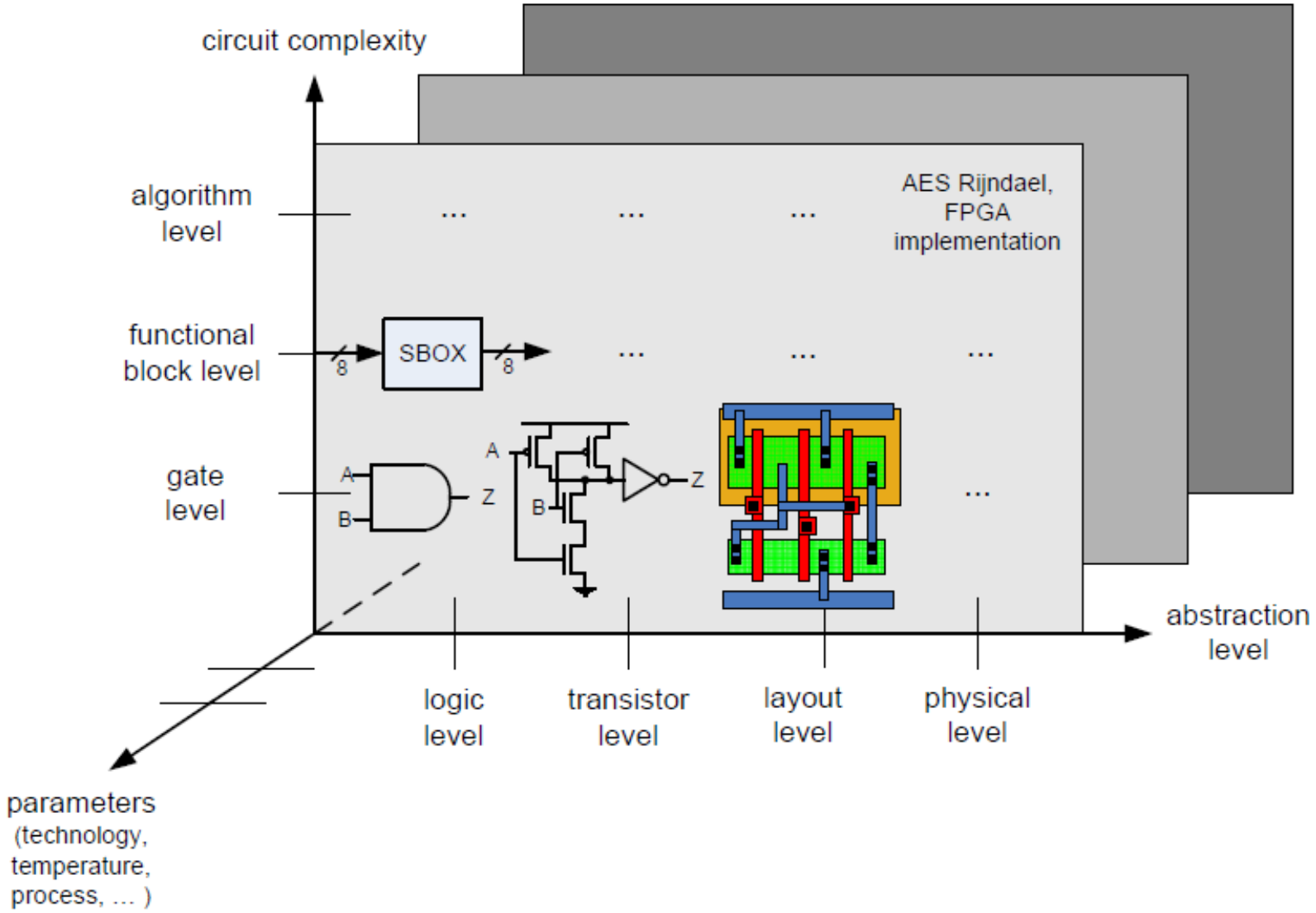


PROOFS 2013
Santa Barbara, USA

The cryptographic HW design space



Multidimensional problem



Problem statement

- SCA countermeasures are expensive
- Confident evaluations require silicon
- But testing all ideas up to silicon is not realistic

$\Rightarrow$ We need to exploit the simulation paradigm

Problem statement

- SCA countermeasures are expensive
- Confident evaluations require silicon
- But testing all ideas up to silicon is not realistic

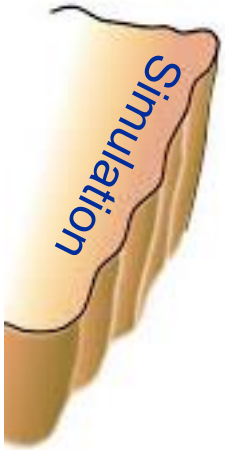
$\Rightarrow$ We need to exploit the simulation paradigm

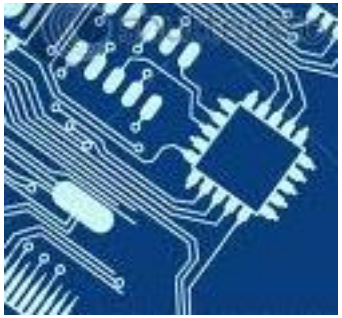
- As for any hardware optimization criteria!
- Being aware of its limitations

(i.e. knowing what can and cannot be learned)

- Main goal: avoid false negatives

Current situation





- Simulations and measurements differ
  - Quantitatively (amount of information leakage)
  - Qualitatively (nature of the information leakage)

Example

- DDSLL (dynamic and differential) S-box
- 65-nanometer technology
- Evaluated with the perceived information

$$\hat{\mathrm{MI}}(K;L) = \mathrm{H}[K] - \sum_{k\in\mathcal{X}} \Pr[k] \sum_{l\in\mathcal{L}} \Pr_{\mathtt{chip}}[l|k] \log_2 \hat{\Pr}_{\mathtt{model}}[k|l]$$

$\hat{\mathrm{PI}}$

= estimator of the MI, biased by the adversary's model

Example

- DDSLL (dynamic and differential) S-box
- 65-nanometer technology
- Evaluated with the perceived information

$$\hat{\mathrm{MI}}(K;L) = \mathrm{H}[K] - \sum_{k\in\mathcal{X}} \Pr[k] \sum_{l\in\mathcal{L}} \Pr_{\mathtt{chip}}[l|k] \log_2 \hat{\Pr}_{\mathtt{model}}[k|l]$$

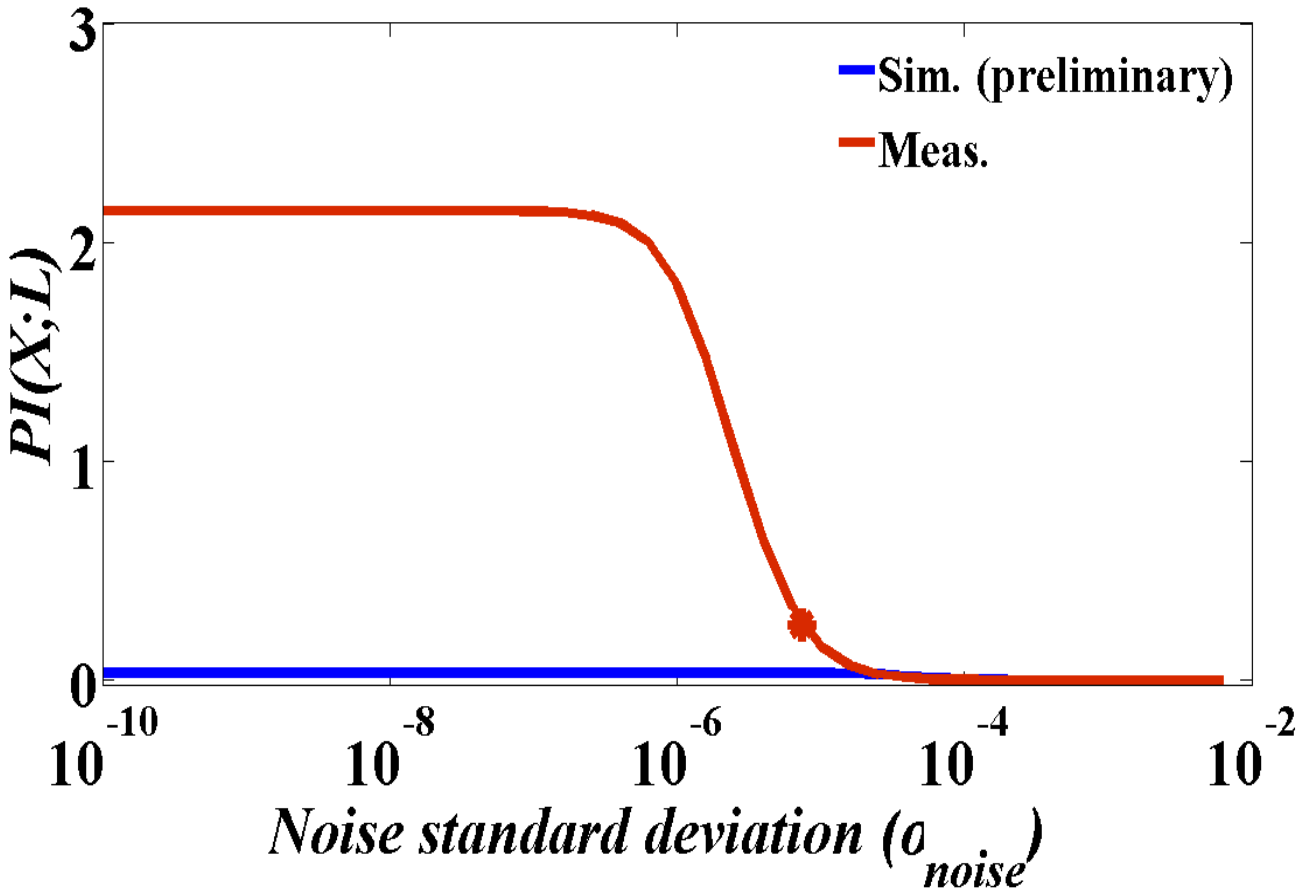
$\hat{\mathrm{PI}}$

= estimator of the MI, biased by the adversary's model

- Can be estimated, e.g. from
  - Gaussian templates
  - Linear regression with linear basis
    - (allows measuring the measurements "linearity")

CHES 2011 results

- Regression-based information theoretic evaluation



Why do we care?

- The linearity of the measurements is an important criteria for the application of non-profiled DPA

Why do we care?

- The linearity of the measurements is an important criteria for the application of non-profiled DPA
- [VS11,WOS12]: generic attacks are only possible in the context of “sufficiently linear” leakages
  - One hope for dual-rail logic styles is to provide highly non-linear leakages (to avoid these attacks)

  $\Rightarrow$ Simulations are misleading with this respect

Why do we care?

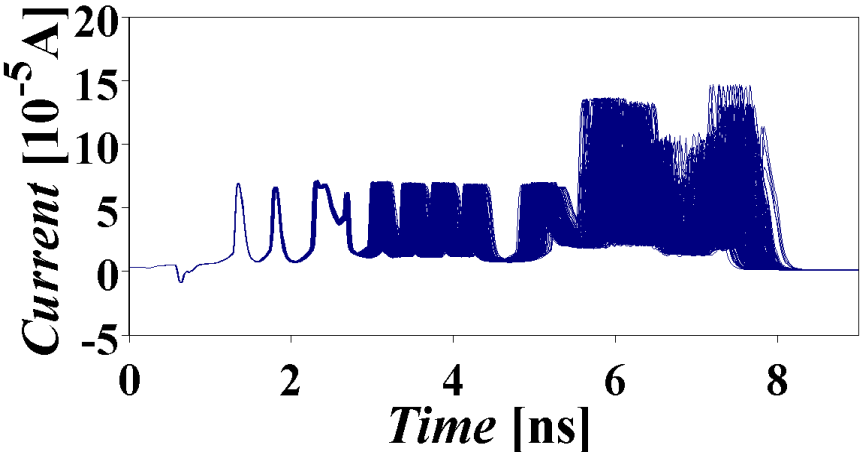
- The linearity of the measurements is an important criteria for the application of non-profiled DPA
- [VS11,WOS12]: generic attacks are only possible in the context of “sufficiently linear” leakages
  - One hope for dual-rail logic styles is to provide highly non-linear leakages (to avoid these attacks)

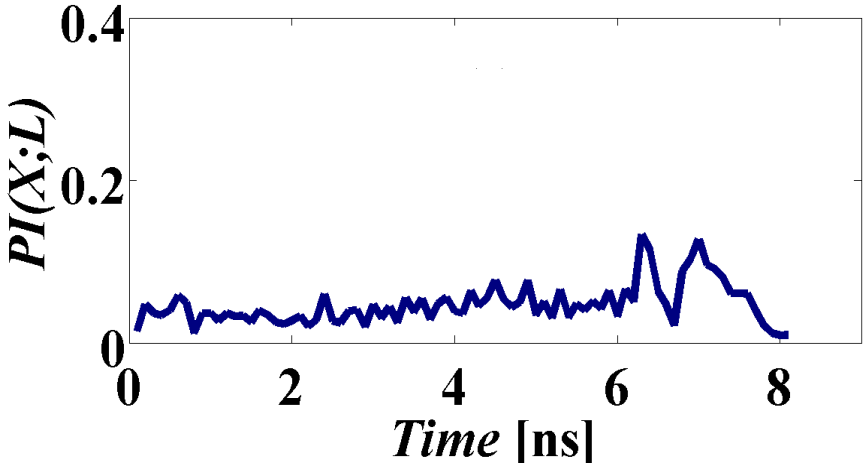
  $\Rightarrow$ Simulations are misleading with this respect

- Our goal: *understanding why, improving if possible!*

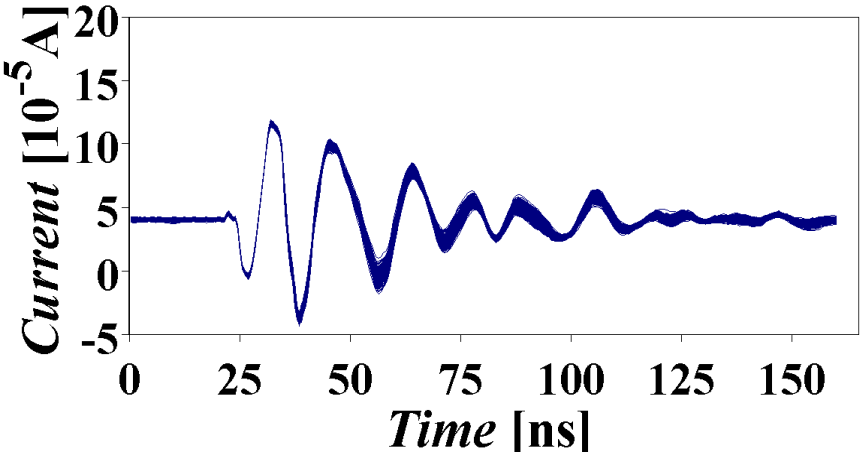
Step 1: looking at the traces

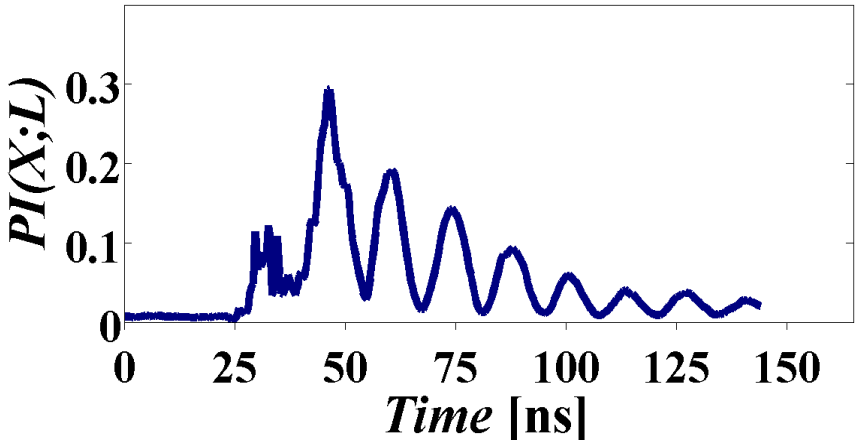
Simulation





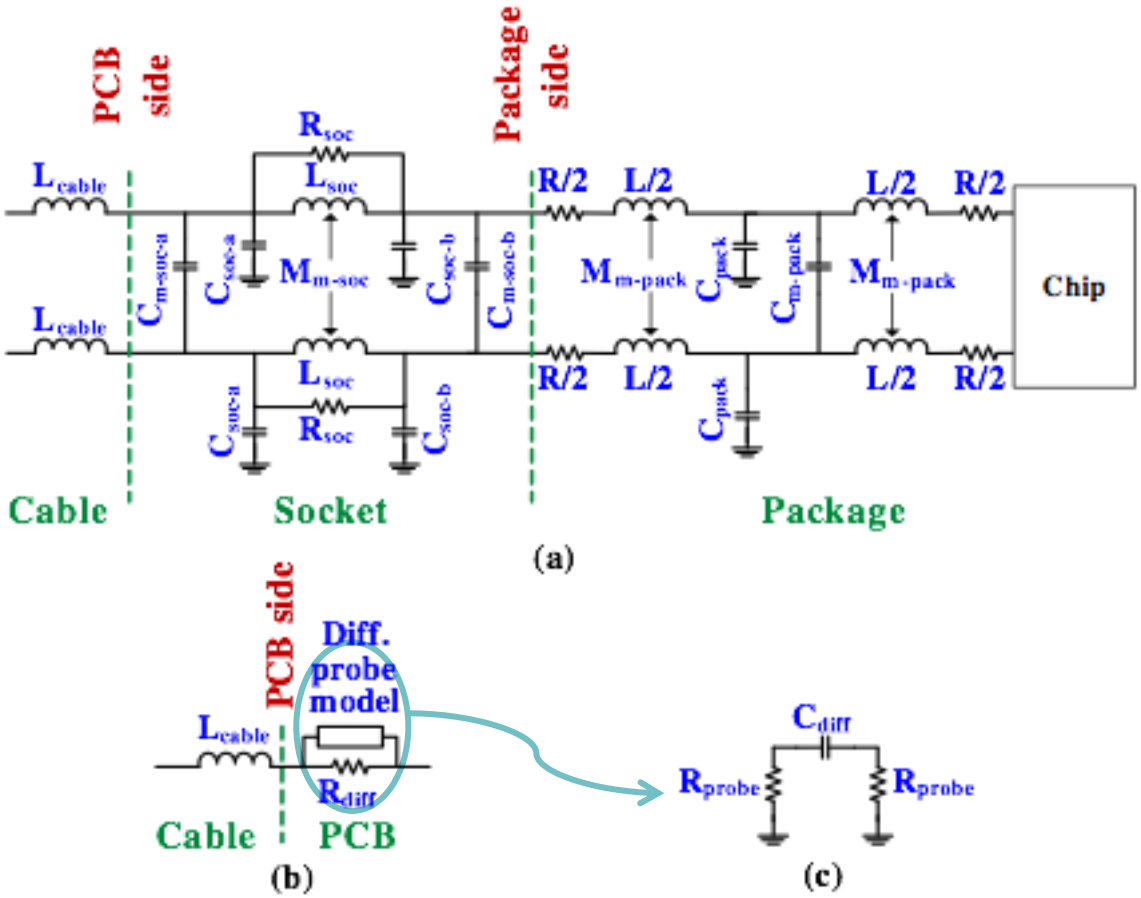
Measurement (real noise 6e^{-6})





Step 2: trying to model

- Equivalent circuit model (generic)



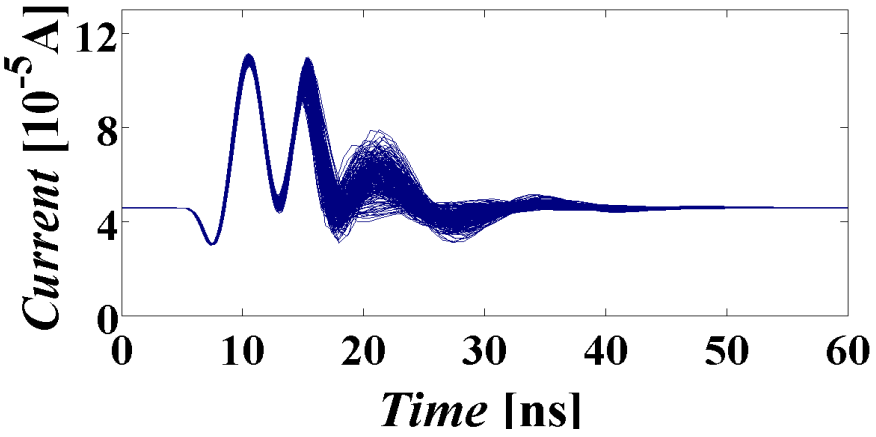
Step 3: instantiating the model

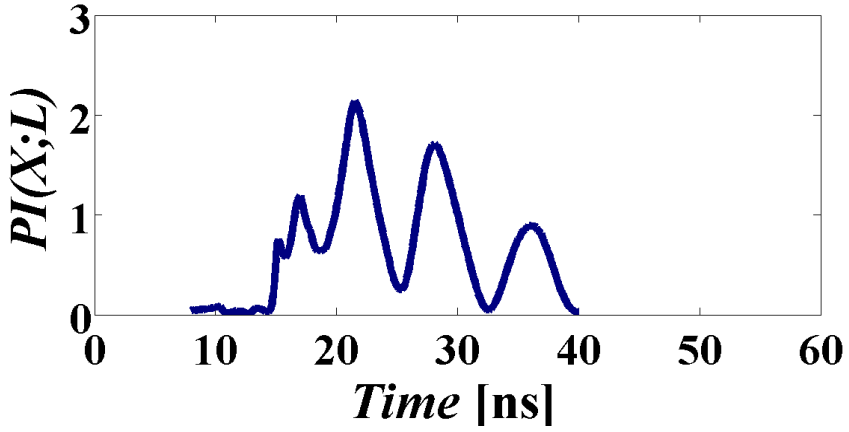
Element	Symbol	Description	Value
Cable	L_{cable}	Supply inductance	688 nH
		In/out inductance	300 nH
		GND inductance	200 nH
Socket	L_{soc}	Lead inductance	1.35 nH
	R_{soc}	Parallel lead res.	600 Ω
	C_{soc-a}	Cap. to GND (PCB side)	0.3 pF
	C_{soc-b}	Cap. to GND (pack. side)	0.45 pF
	L_{m-soc}	Mutual inductance	0.3 nH
	$C_{m-soc-a}$	Mutual cap. (PCB side)	0.09 pF
	$C_{m-soc-b}$	Mutual cap. (pack. side)	0.09 pF
Package	L	Inductance	1.2 nH
	R	Series resistance	0.28 Ω
	C_{pack}	Cap. To GND	0.1 pF
	L_{m-pack}	Mutual inductance	1.3 nH
	C_{m-pack}	Mutual cap.	0.2 pF
Diff. Probe	C_{diff}	Capacitance	0.7 pF
	R_{probe}	Resistance	25 kΩ
	R_{diff}	Res. in S-box VDD path	1 kΩ

- The more precise the better (specific)
  - (but we sometimes had only approximations)

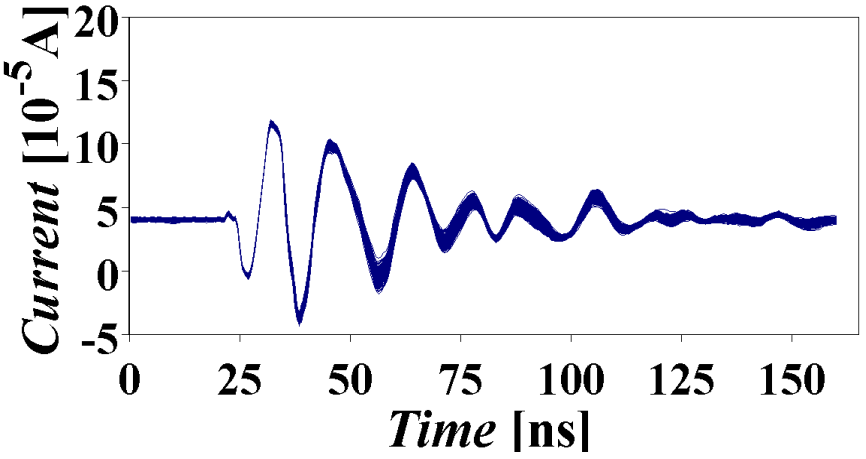
Example: looking at the traces again

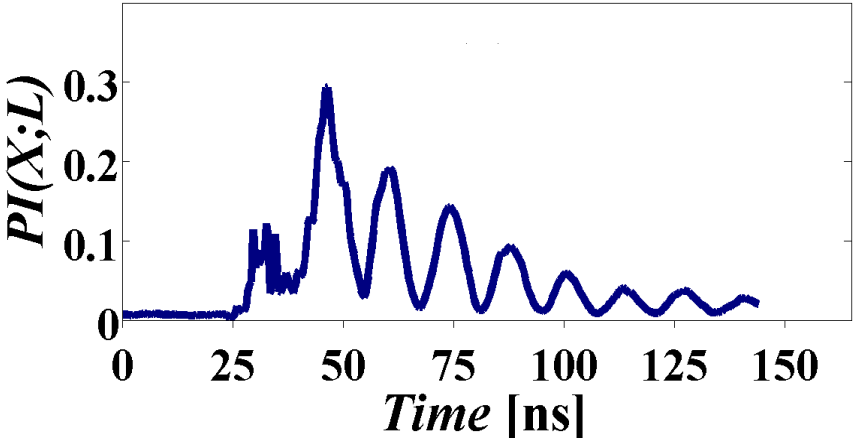
Simulation with circuit model





Measurement (real noise $6e^{-6}$)





Step 4: how precise must the model be?

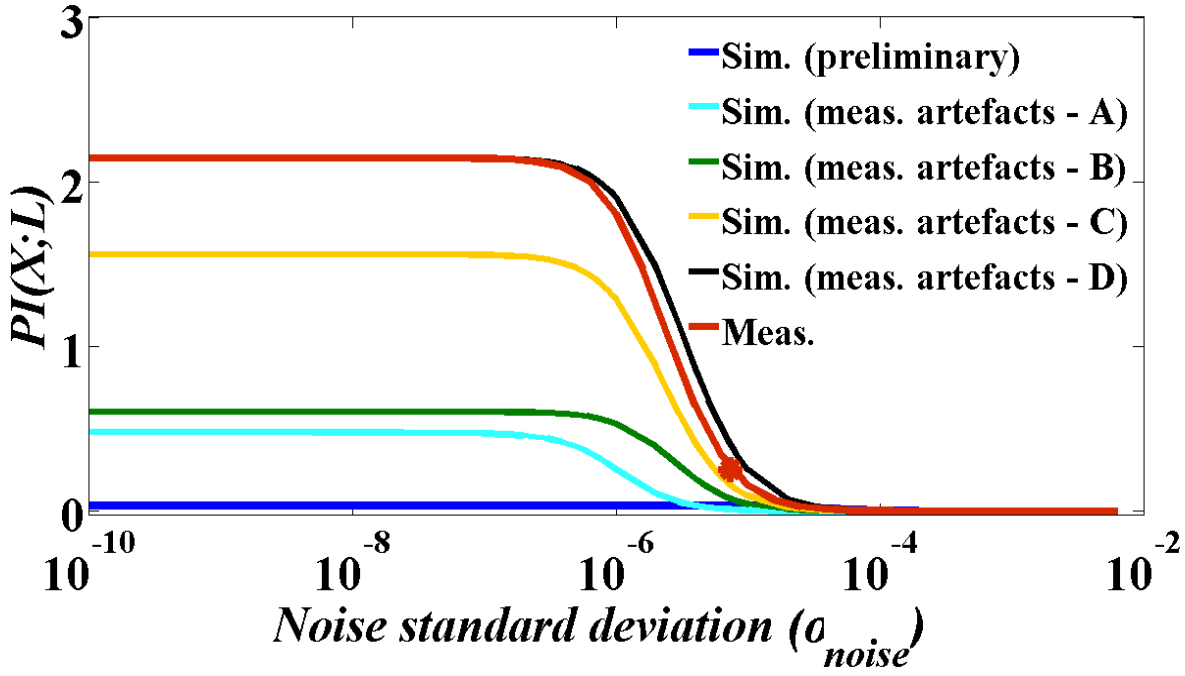
- Our strategy: use increasingly complex ones

Model	Description
A	1 kΩ + diff. probe
B	1 kΩ + diff. probe + pack. and socket
C	1 kΩ + diff. probe + pack. and socket + V_{DD} cable
D	1 kΩ + diff. probe + pack. and socket + V_{DD} cable + GND cable

Step 4: how precise must the model be?

- Our strategy: use increasingly complex ones

Model	Description
A	1 kΩ + diff. probe
B	1 kΩ + diff. probe + pack. and socket
C	1 kΩ + diff. probe + pack. and socket + V_{DD} cable
D	1 kΩ + diff. probe + pack. and socket + V_{DD} cable + GND cable



Conclusions

- Increase of the simulation time negligible
  - (already for a simple S-box circuit)

Conclusions

- Increase of the simulation time negligible
  - (already for a simple S-box circuit)

- Modeling circuit / measurement specificities is crucial
  - It increases the relevance of simulations

  => Reduces the risk of false negatives
  - Even with imprecise instantiation of the model!

  $\Rightarrow$ Reasonably generic approach

Conclusions

- Increase of the simulation time negligible
  - (already for a simple S-box circuit)

- Modeling circuit / measurement specificities is crucial
  - It increases the relevance of simulations

  => Reduces the risk of false negatives
  - Even with imprecise instantiation of the model!

  $\Rightarrow$ Reasonably generic approach

- Designing circuits with highly non-linear leakages seems challenging (filters linearize them)

THANKS

http://perso.uclouvain.be/fstandae/