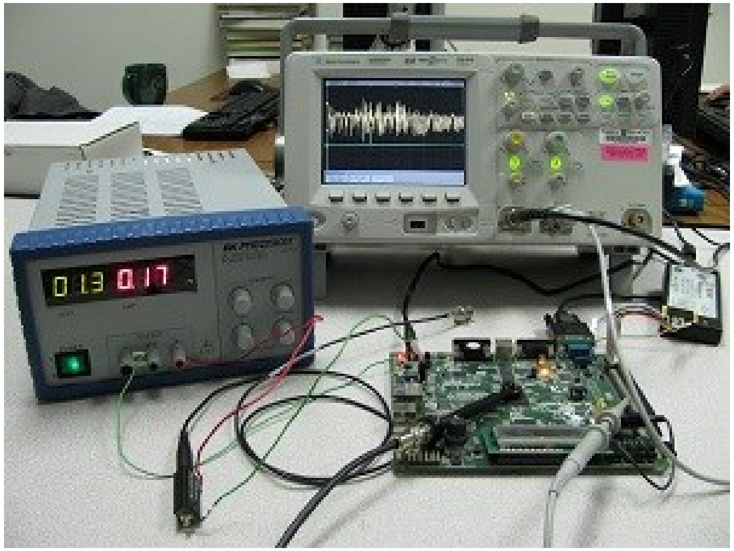
Towards Easy Leakage Certification



F. Durvaux, ***F.-X. Standaert***, S. Merino Del Pozo
UCL Crypto Group, Belgium

CHES 2016, Santa Barbara, USA

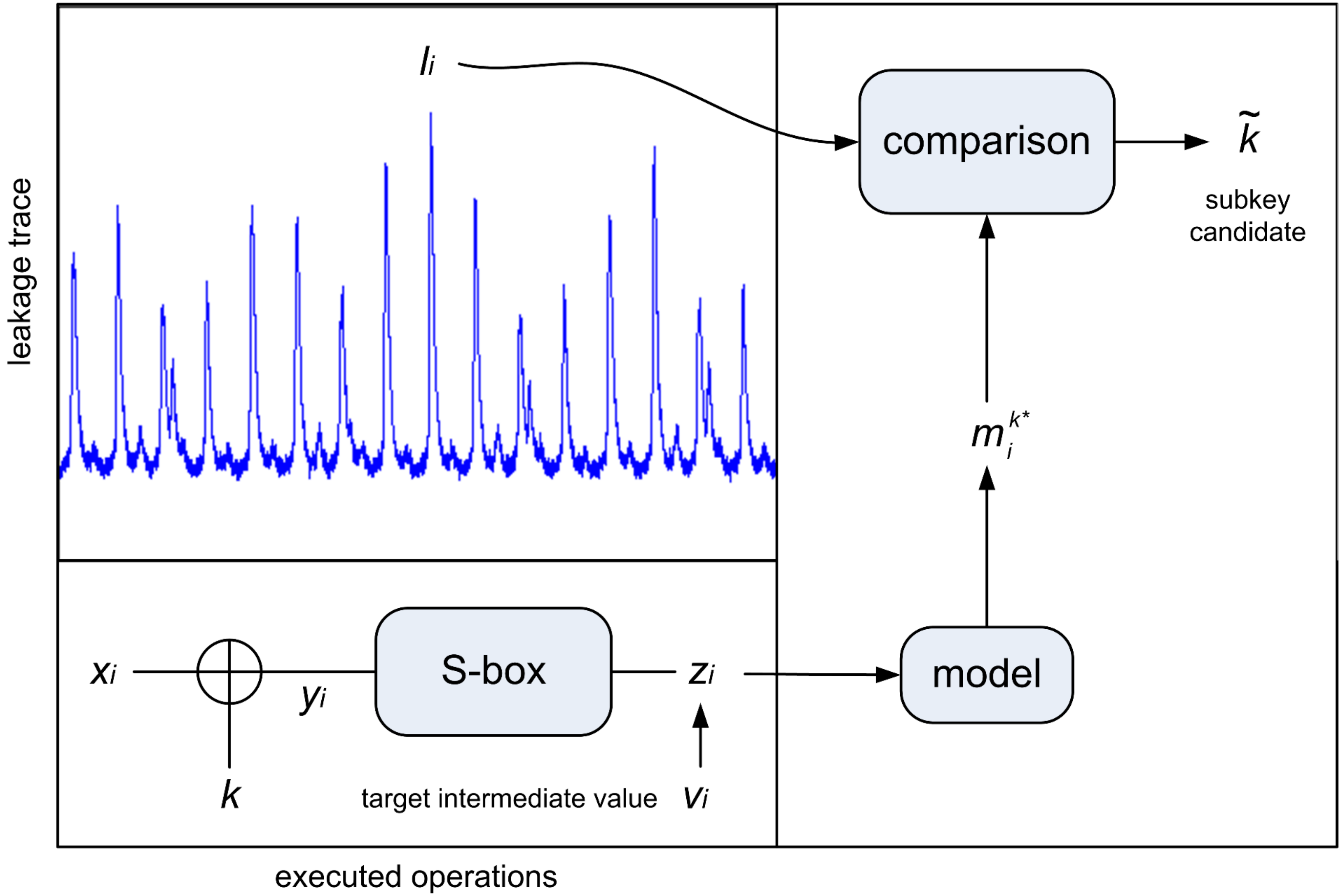
Outline

1. Introduction & motivation
2. (Easy) Leakage certification
3. Experiments
   - Simulations
   - Unprotected software
   - Masked hardware
4. Conclusions

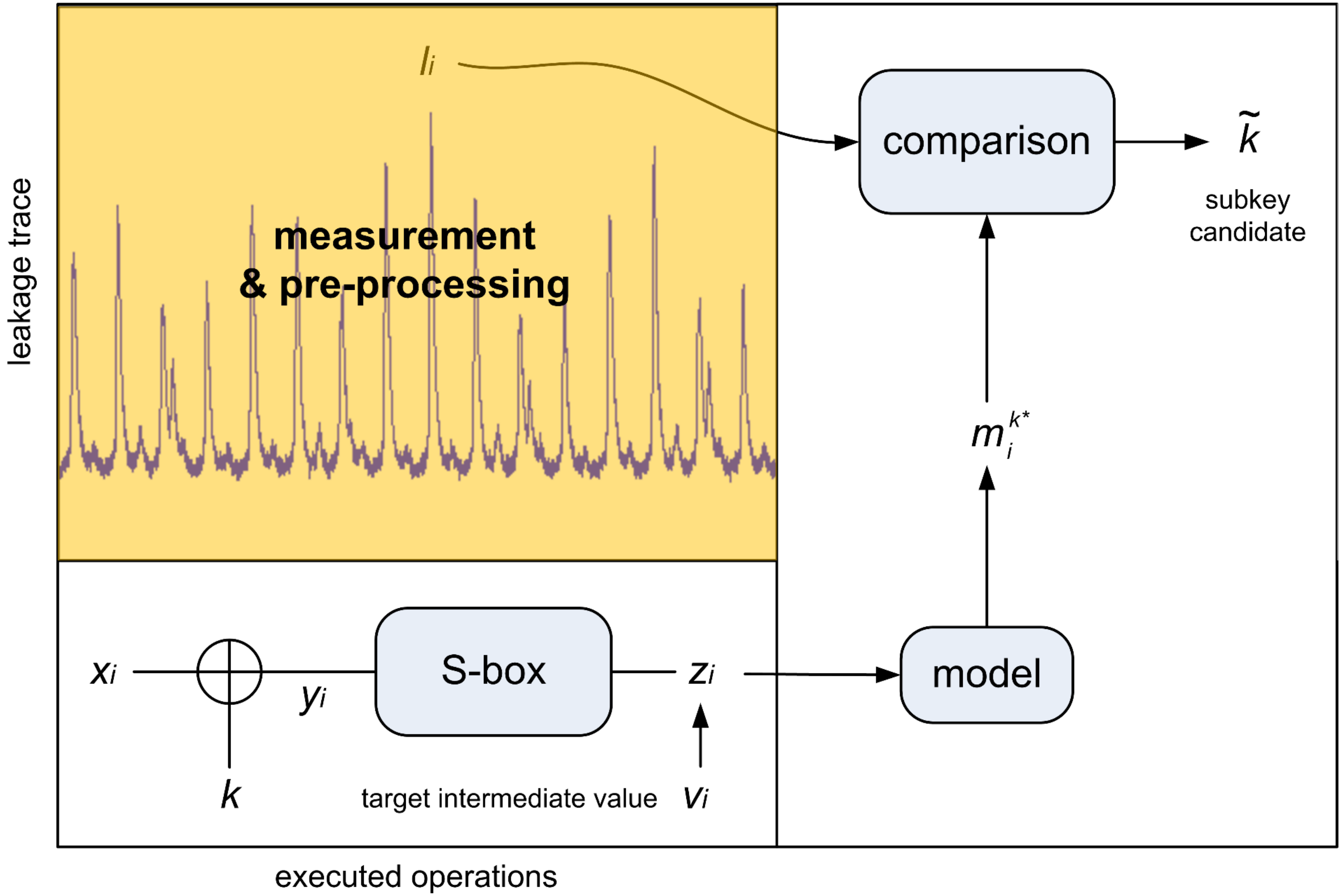
Outline

1. **Introduction & motivation**
2. (Easy) Leakage certification
3. Experiments
   - Simulations
   - Unprotected software
   - Masked hardware
4. Conclusions

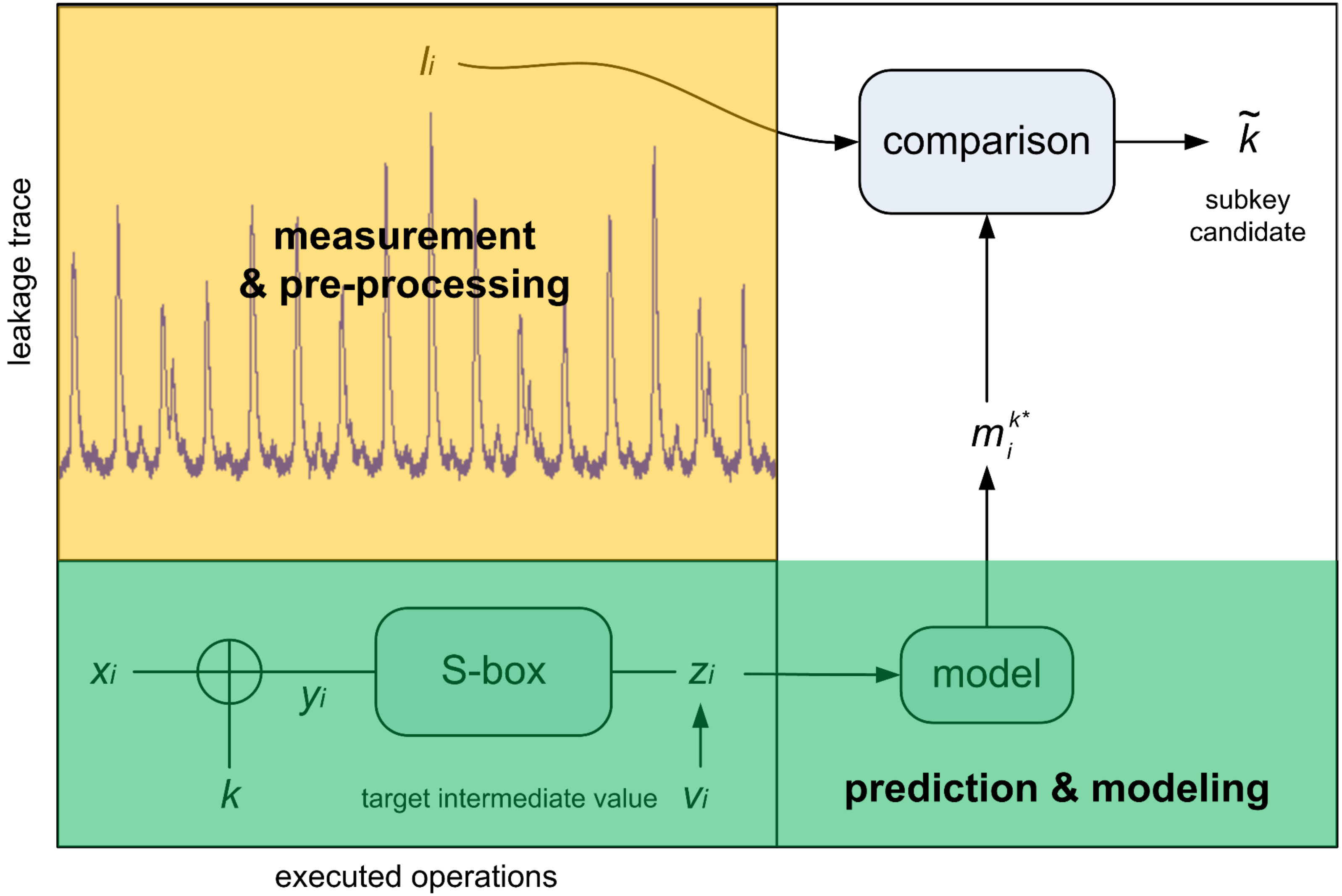
Standard DPA



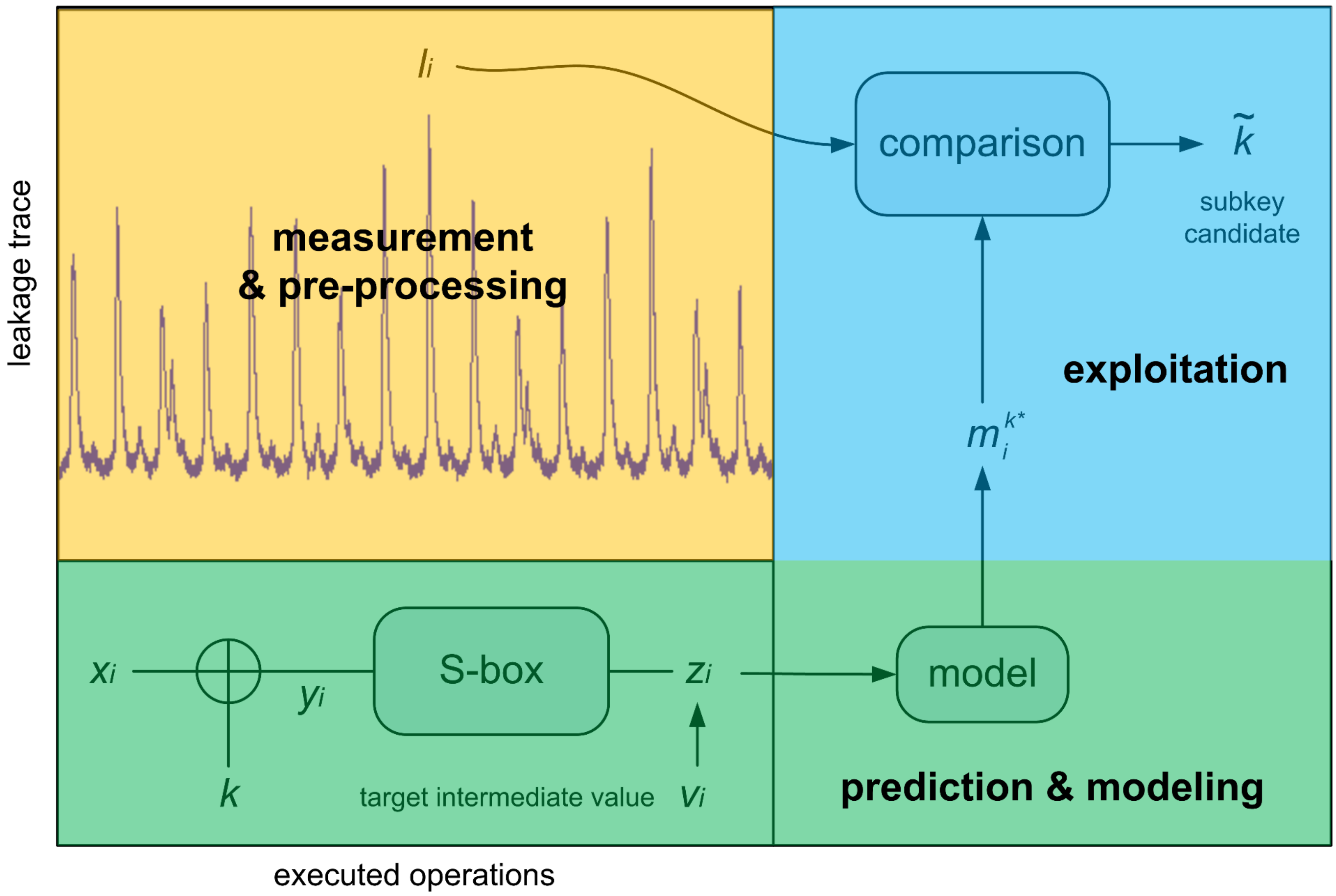
Standard DPA



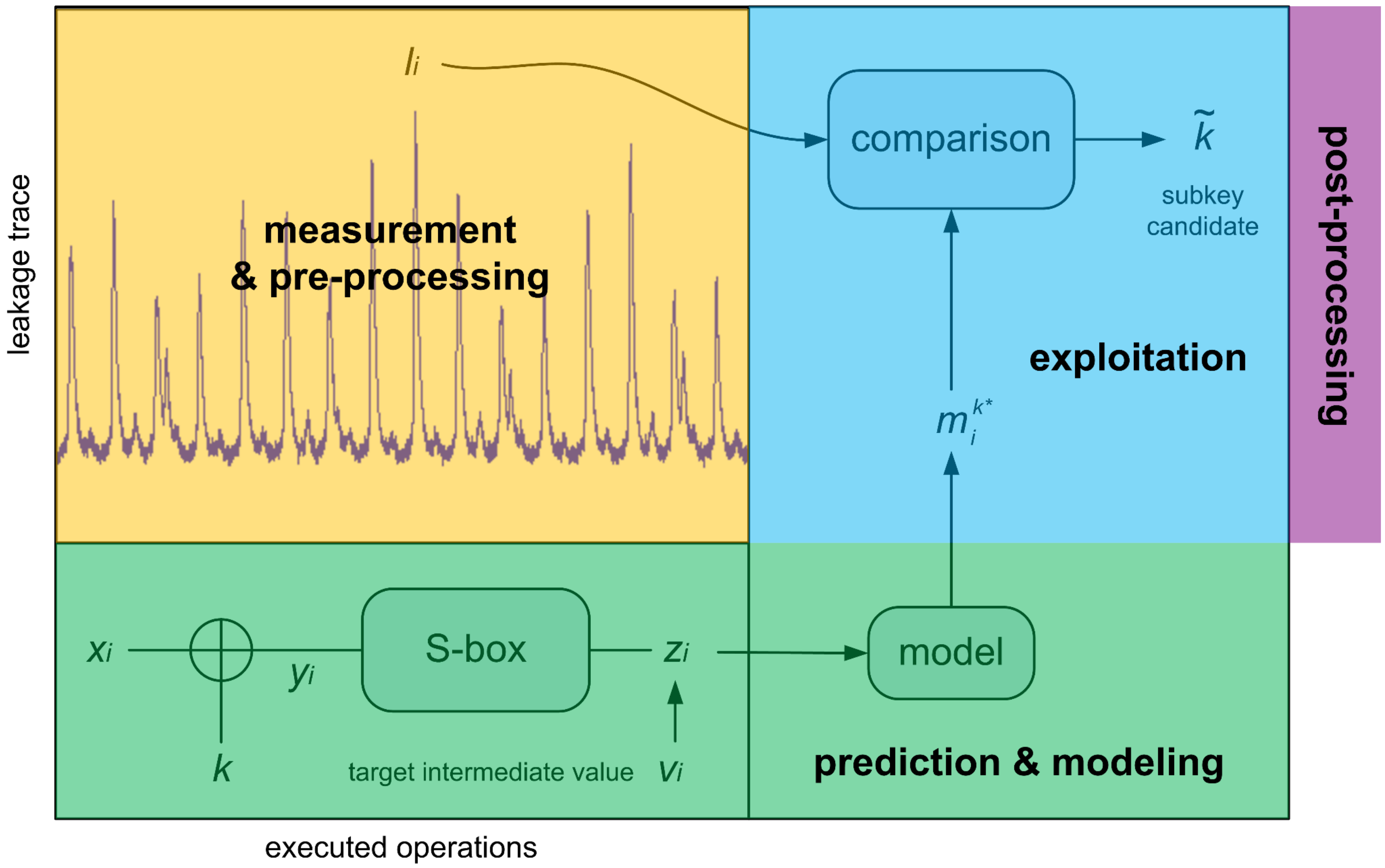
Standard DPA



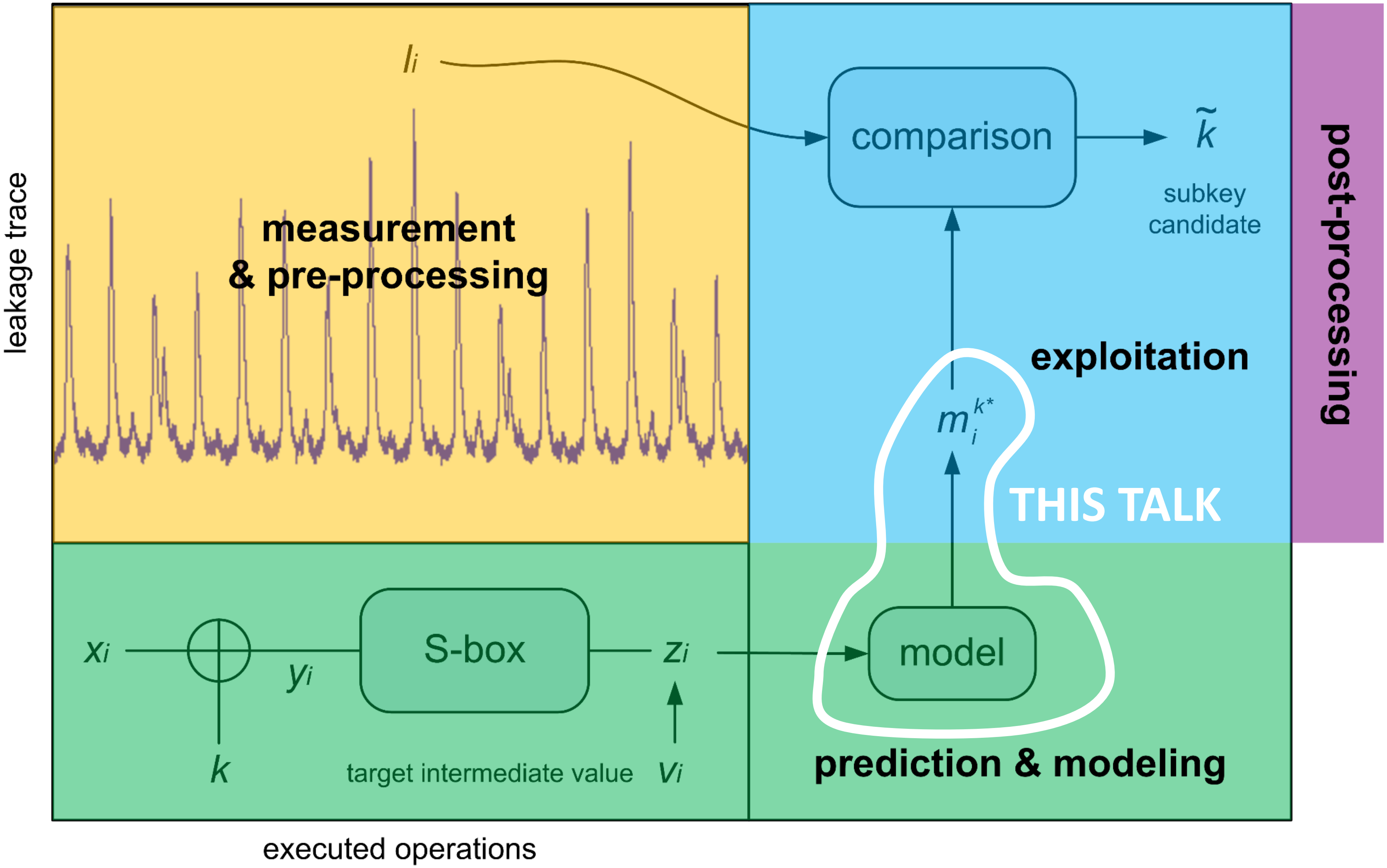
Standard DPA



Standard DPA



Standard DPA



Why do we care?

Why do we care?

model: m_i^{k*}

Why do we care?

model: m_i^{k*} → Hyp. 1: key candidates

Why do we care?

model: m_i^{k*} → Hyp. 1: key candidates

↓

Hyp. 2: implementation

Why do we care?

- For the key candidates, we try them all

Why do we care?

- But it is impossible to try all models! [W12]

[W12] M. Wagner, *700+ Attacks Published on Smart Cards: The Need for a Systematic Counter Strategy*, COSADE 2012.

Why do we care?

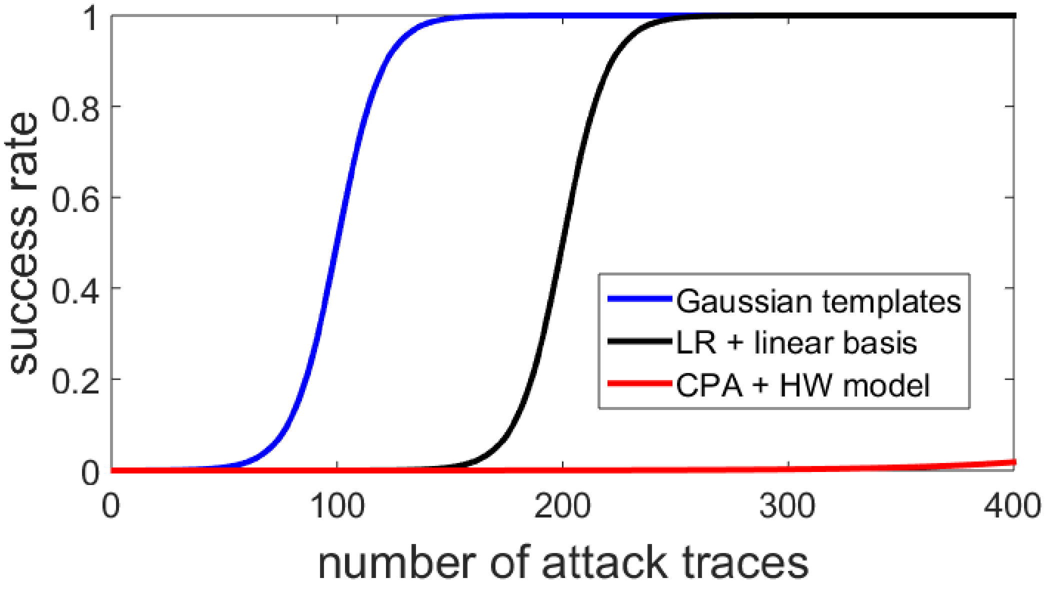
⇒ How to be sure the model is “good enough”?

Why do we care? (II)

- Does it really happen in practice?

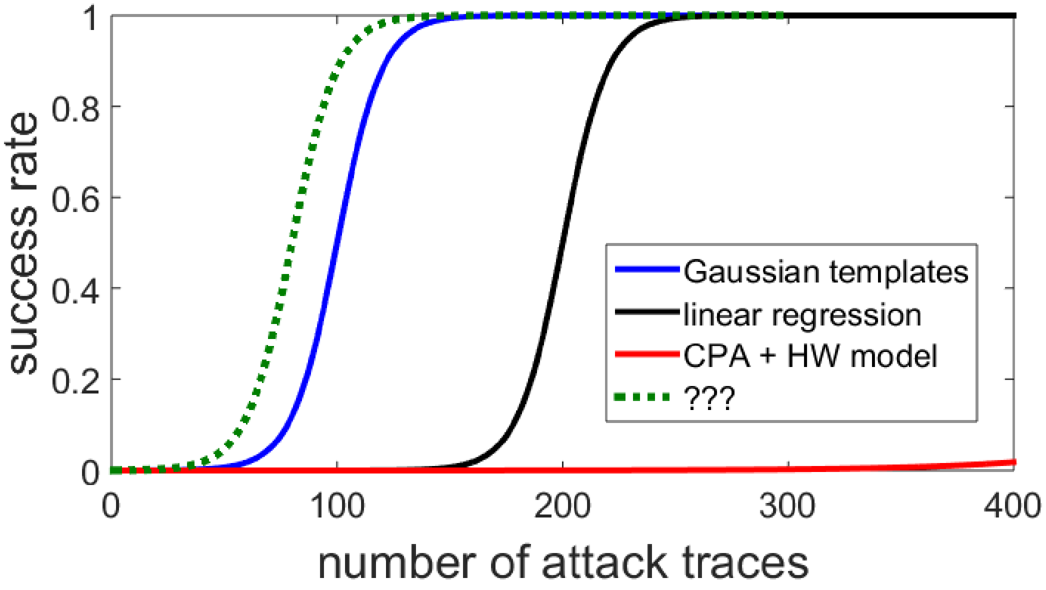
Why do we care? (II)

- Does it really happen in practice?



- Each time a model performs better than another

Why do we care? (II)



⇒ How to be sure the model is “good enough”?

Model optimality caveats

- A model is optimal if $\widehat{\Pr}_{model}\,[l|k] = \Pr_{chip}\,[l|k]$

Model optimality caveats

$\Rightarrow$ Theory would say it is ε-close to optimal if

$$\mathrm{SD}(\widehat{\Pr}_{model}\,[l|k],\ \Pr_{chip}\,[l|k]) < \varepsilon$$

- (with SD a statistical distance)

Model optimality caveats

- Convenient since ε would quantify the loss
  - That could be reported in SR bounds [DFS15]

[DFS15] A Duc, S. Faust, F.-X. Standaert, *Making Masking Security Proofs Concrete […]*, EUROCRYPT 2015.

Model optimality caveats

- Problem: $\Pr_{chip}[l|k]$ is unknown

Outline

1. Introduction & motivation
2. **(Easy) Leakage certification**
3. Experiments
   - Simulations
   - Unprotected software
   - Masked hardware
4. Conclusions

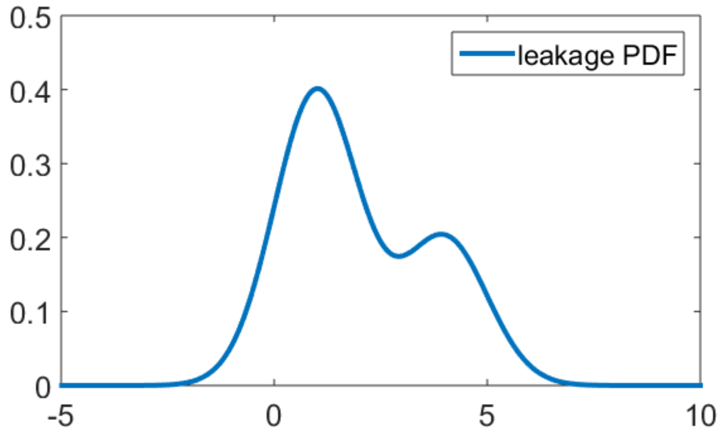
Leakage certification [DSV14]

- Distinguish estimation & assumption errors
  - Recall estimation errors decrease with # meas.

[DSV14] F. Durvaux, F.-X. Standaert, N. Veyrat-Charvillon, *How to Certify the Leakage of a Chip*, EUROCRYPT 2014.

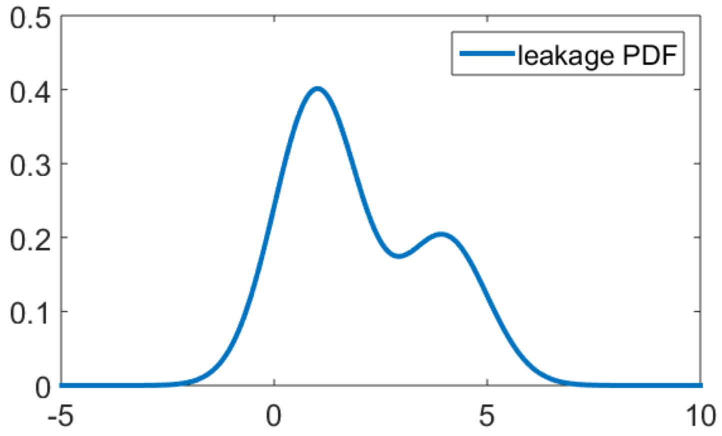
Leakage certification [DSV14]

- Example:

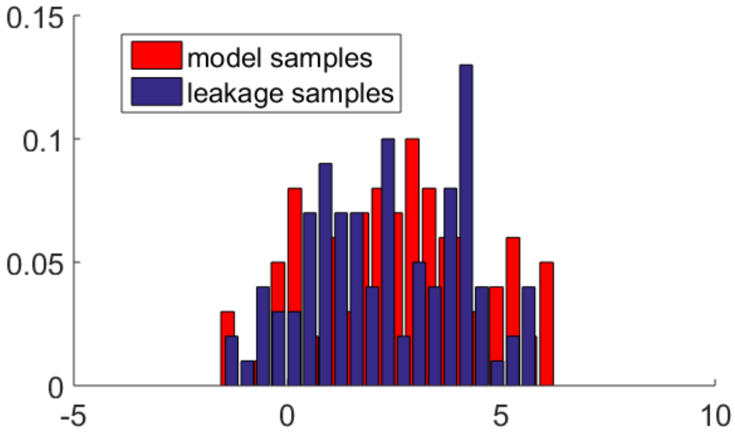


Leakage certification [DSV14]

- Example:

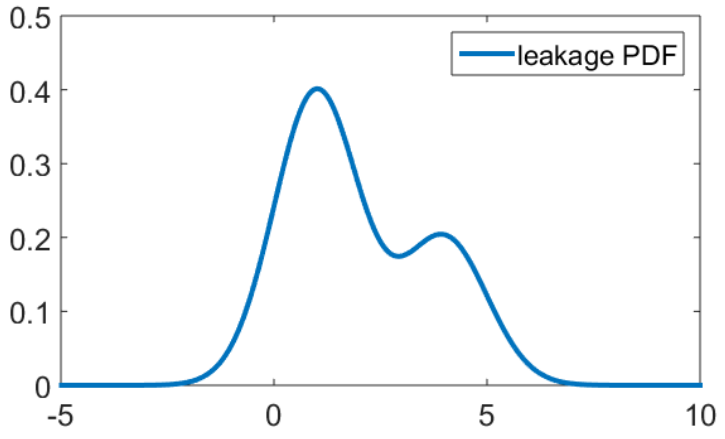


N_0 samples

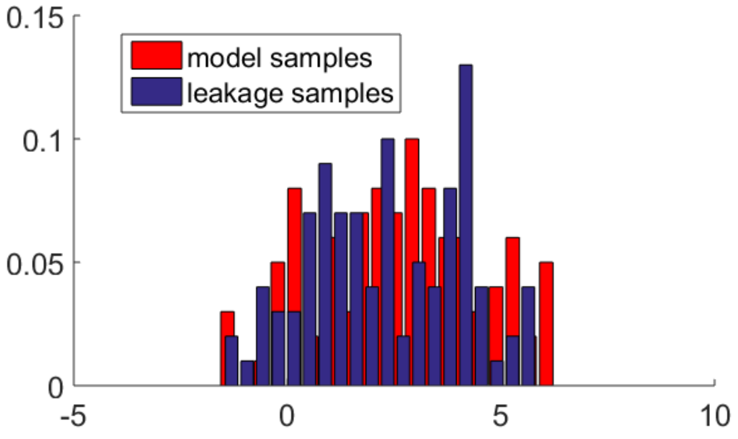


Leakage certification [DSV14]

- Example:



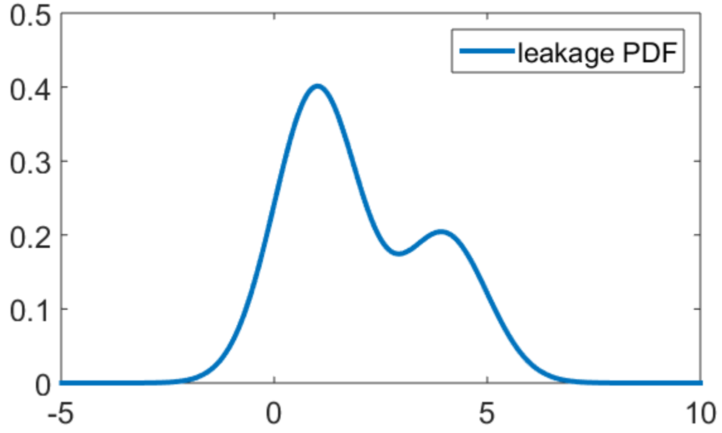
estimation errors dominate



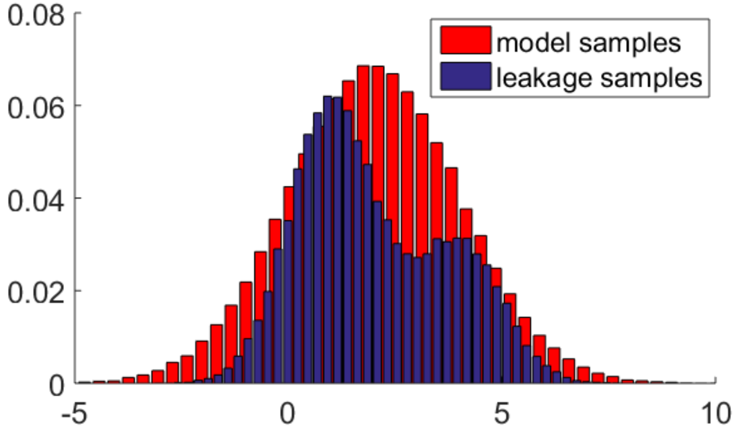
⇒ need to measure more

Leakage certification [DSV14]

- Example:



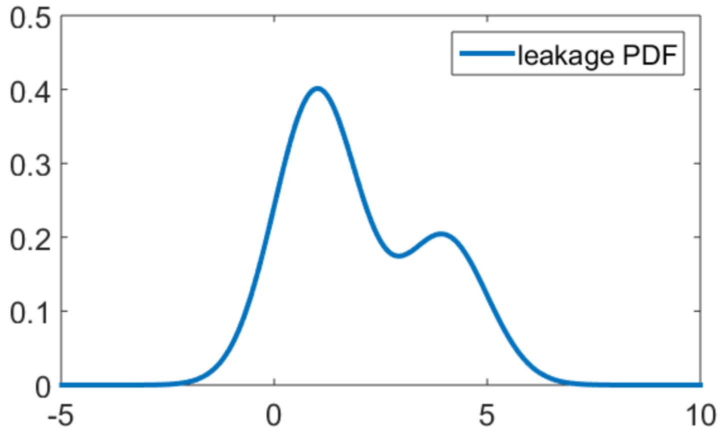
$N_1 > N_0$ samples

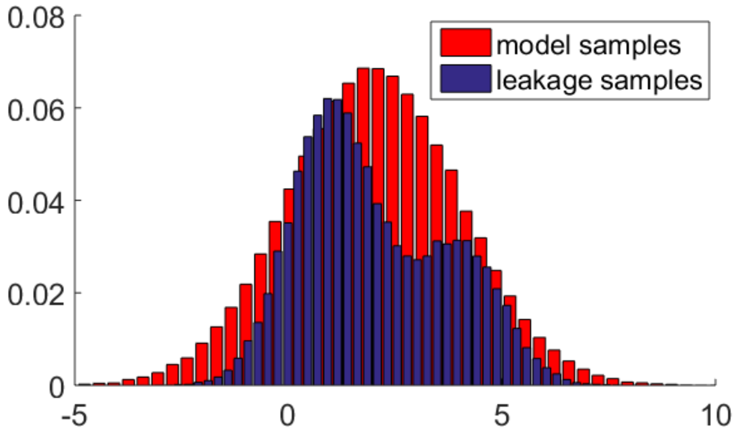


Leakage certification [DSV14]

- Example:

assumption errors dominate





⇒ **need another model**

Leakage certification [DSV14]

$\Rightarrow$ good enough model: *ass. err* << *est. err*. given *N*

Leakage certification (II)

- Test the hypothesis that

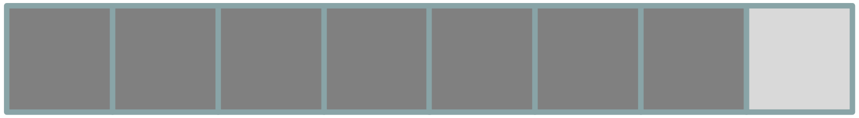
$$\widehat{\mathrm{Pr}}_{model}\,[l|k] \overset{N}{=} \mathrm{Pr}_{chip}\,[l|k]$$

Leakage certification (II)

- Taking advantage of cross-validation

■ modeling samples

□ test samples

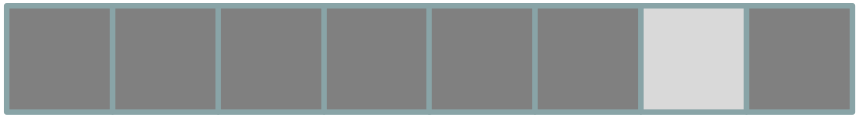


Leakage certification (II)

- Taking advantage of cross-validation

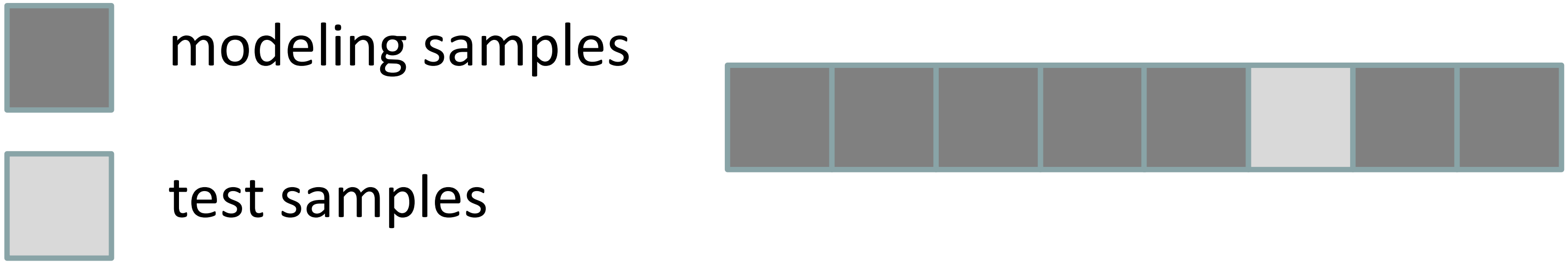
■ modeling samples

□ test samples



Leakage certification (II)

- Taking advantage of cross-validation



■ modeling samples

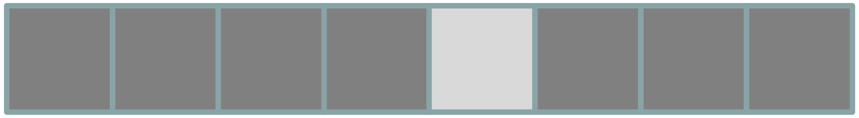
□ test samples

Leakage certification (II)

- Taking advantage of cross-validation

■ modeling samples

□ test samples



Leakage certification (II)

- Output a p-value p(*N*)
  - Small p’s indicate hyp. is likely incorrect

Leakage certification (II)

- Output a p-value p(N) Eval. lab. limit

Leakage certification (II)

- Main drawback: cost (of sampling distributions)

Towards easy certification

Towards easy certification

- Compare moments (rather than distributions)

1. $\widehat{M}_d \overset{N}{\leftarrow} \widehat{\Pr}_{model}\,[l|k]$
2. $\widetilde{M}_d \overset{N}{\leftarrow} \Pr_{chip}\,[l|k]$

3. Test equality

$$\widehat{M}_d = \widetilde{M}_d$$

Towards easy certification

+ Can be done with simple univariate tests

- e.g., T-test (assuming $\widehat{M}_d, \widetilde{M}_d$ are Gaussian)

Towards easy certification

– Is it theoretically sound? No!

Towards easy certification

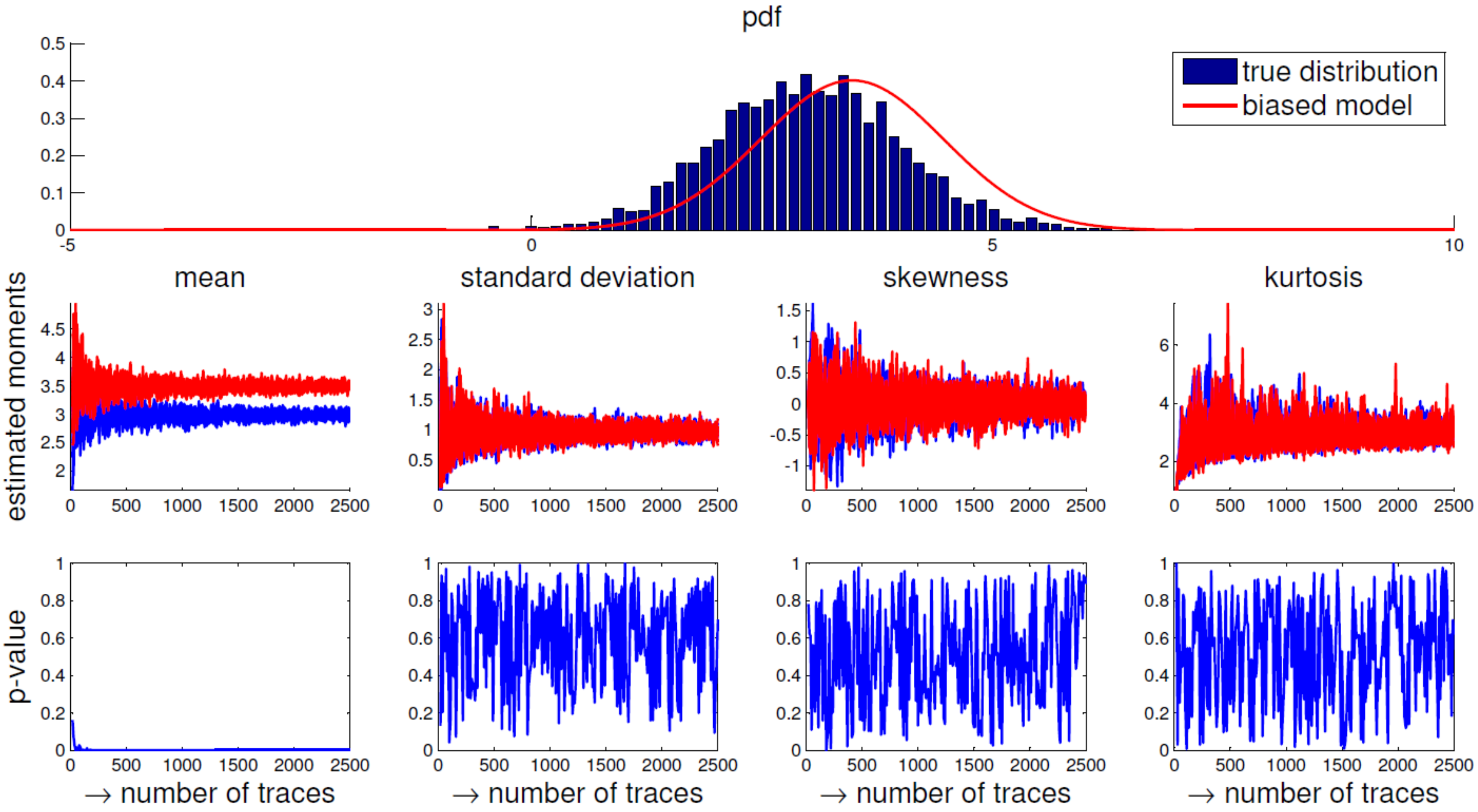
– Is it theoretically sound? No!
    - But counterexamples are involved
    - & SCA literature frequently does it
        - Leakage detection, HO attacks, … [SM15]

[SM15] T. Schneider, A. Moradi, *Leakage Assessment Methodology […]*, CHES 2015.

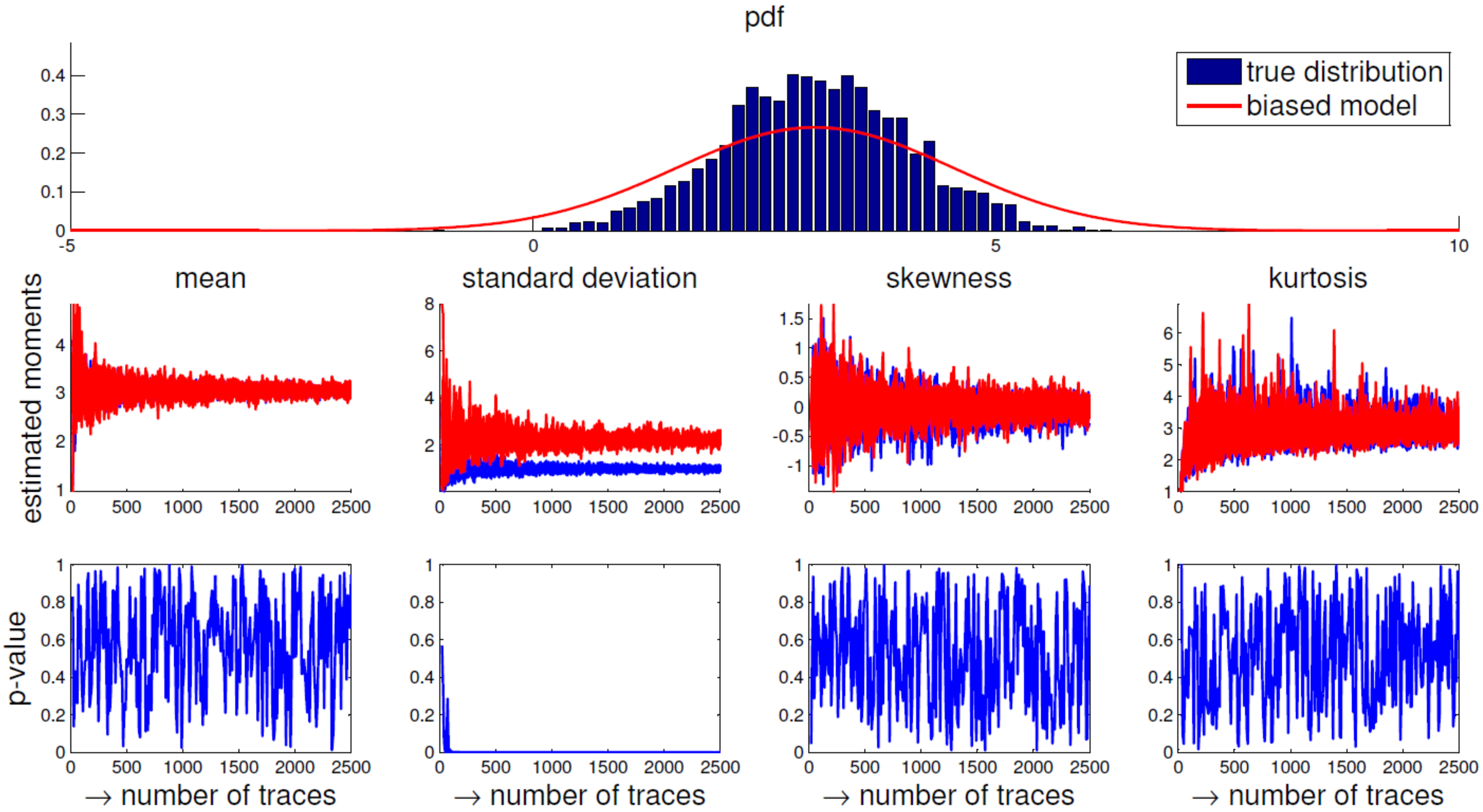
Outline

1. Introduction & motivation
2. (Easy) Leakage certification
3. **Experiments**
   - **Simulations**
   - Unprotected software
   - Masked hardware
4. Conclusions

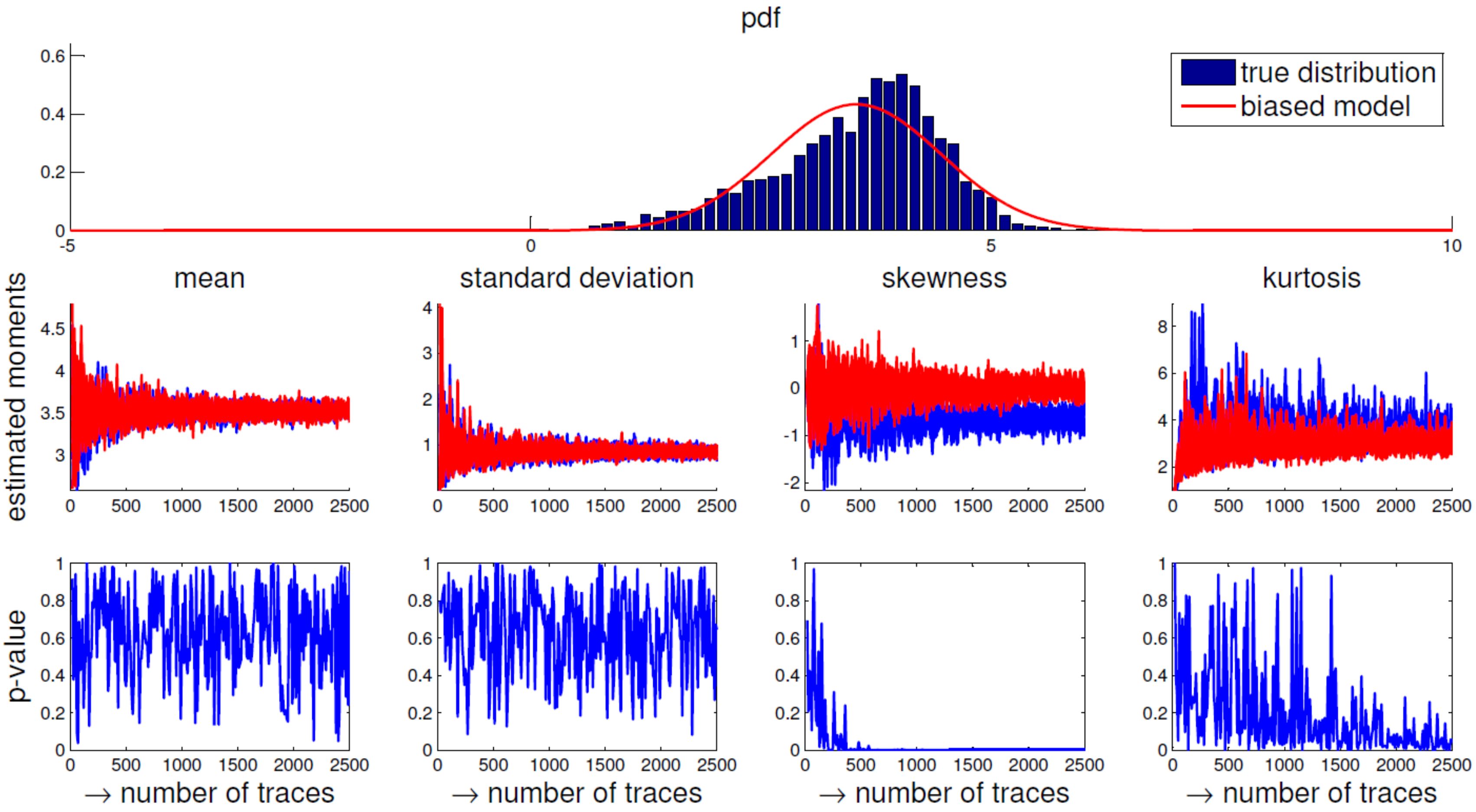
Simulated example



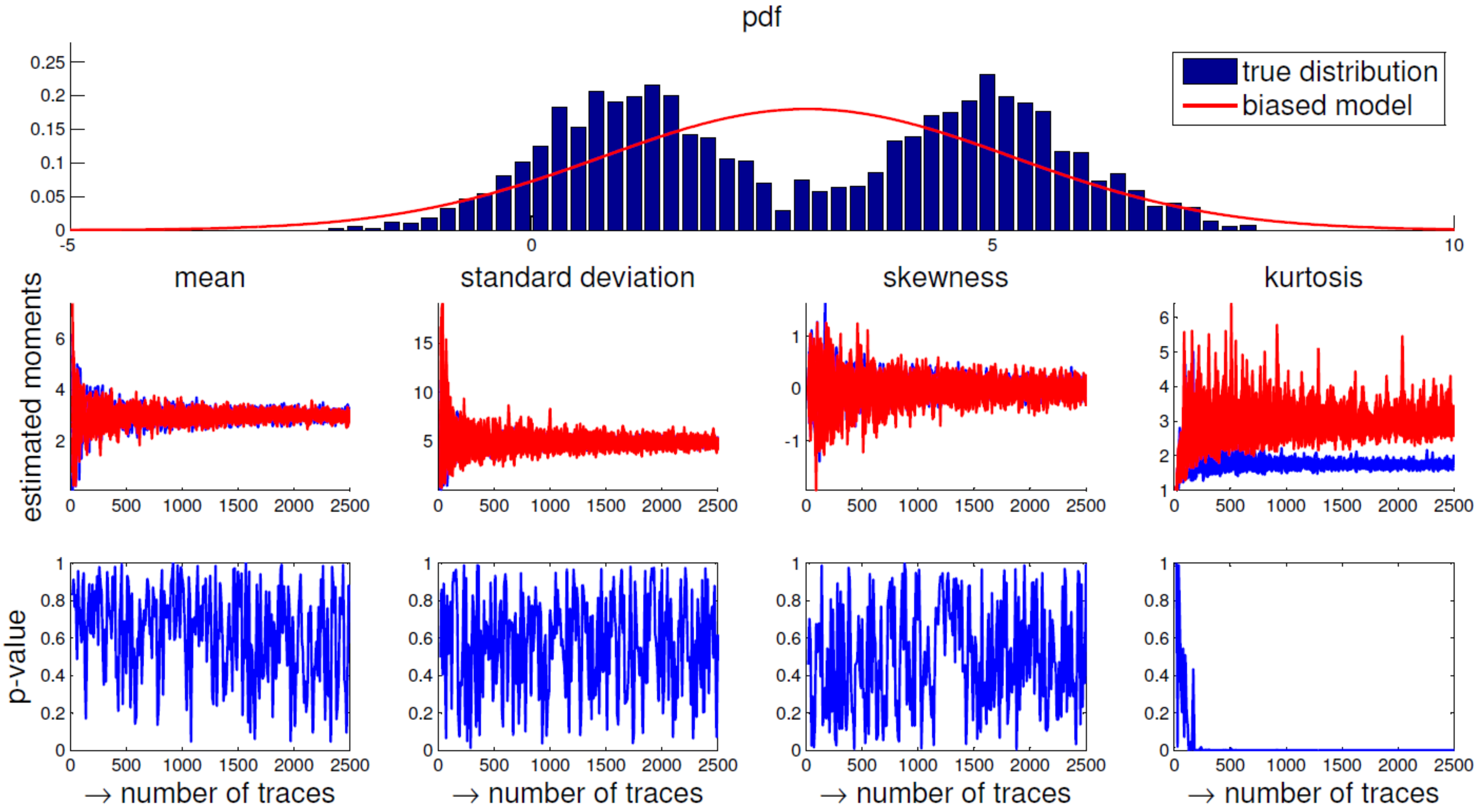
Simulated example (II)



Simulated example (III)



Simulated example (IV)



Outline

1. Introduction & motivation
2. (Easy) Leakage certification
3. **Experiments**
    - Simulations
    - **Unprotected software**
    - Masked hardware
4. Conclusions

Software experiments

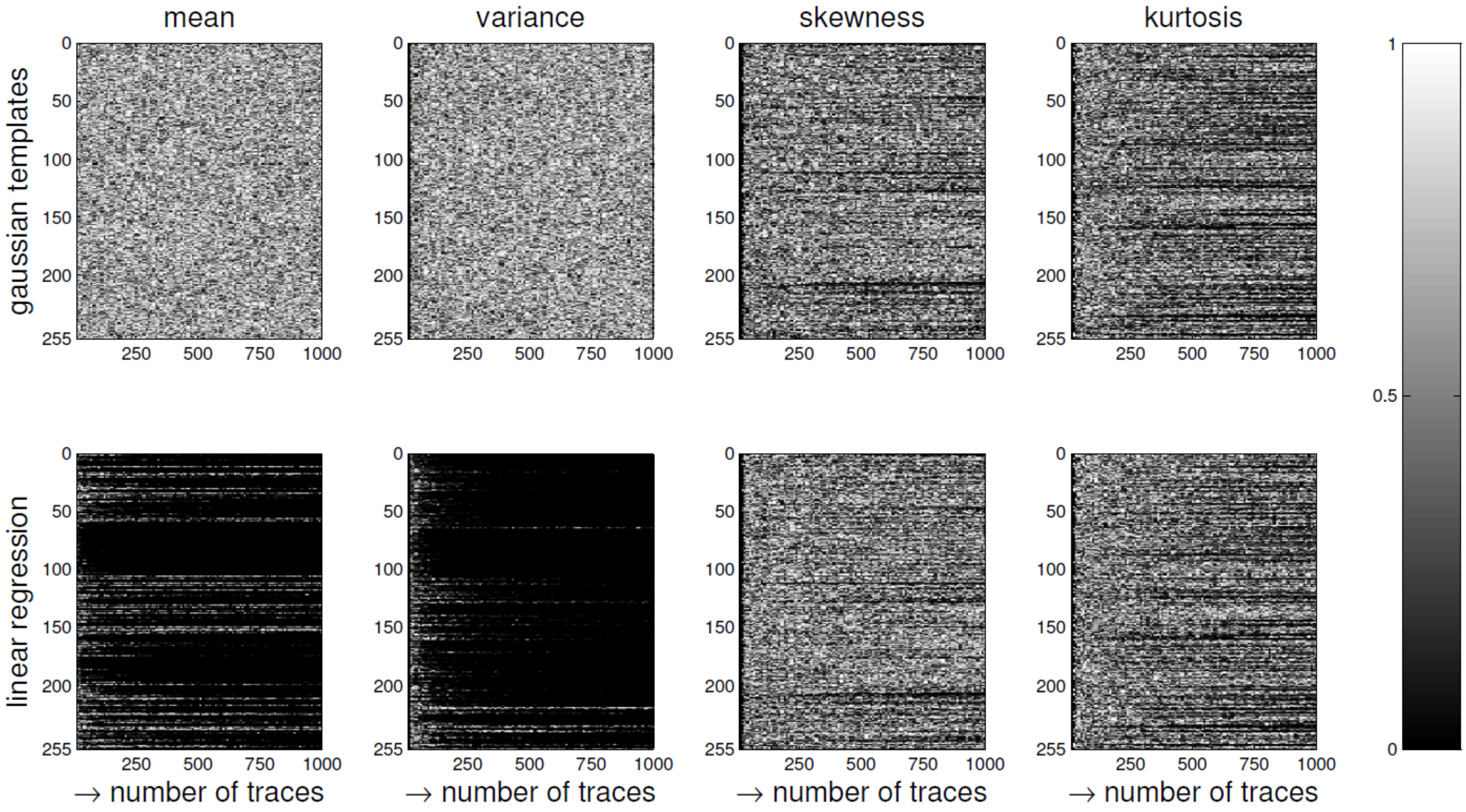
- Repeating the Eurocrypt 2014 case study

Software experiments

- Unprotected AES implementation, Atmel AVR

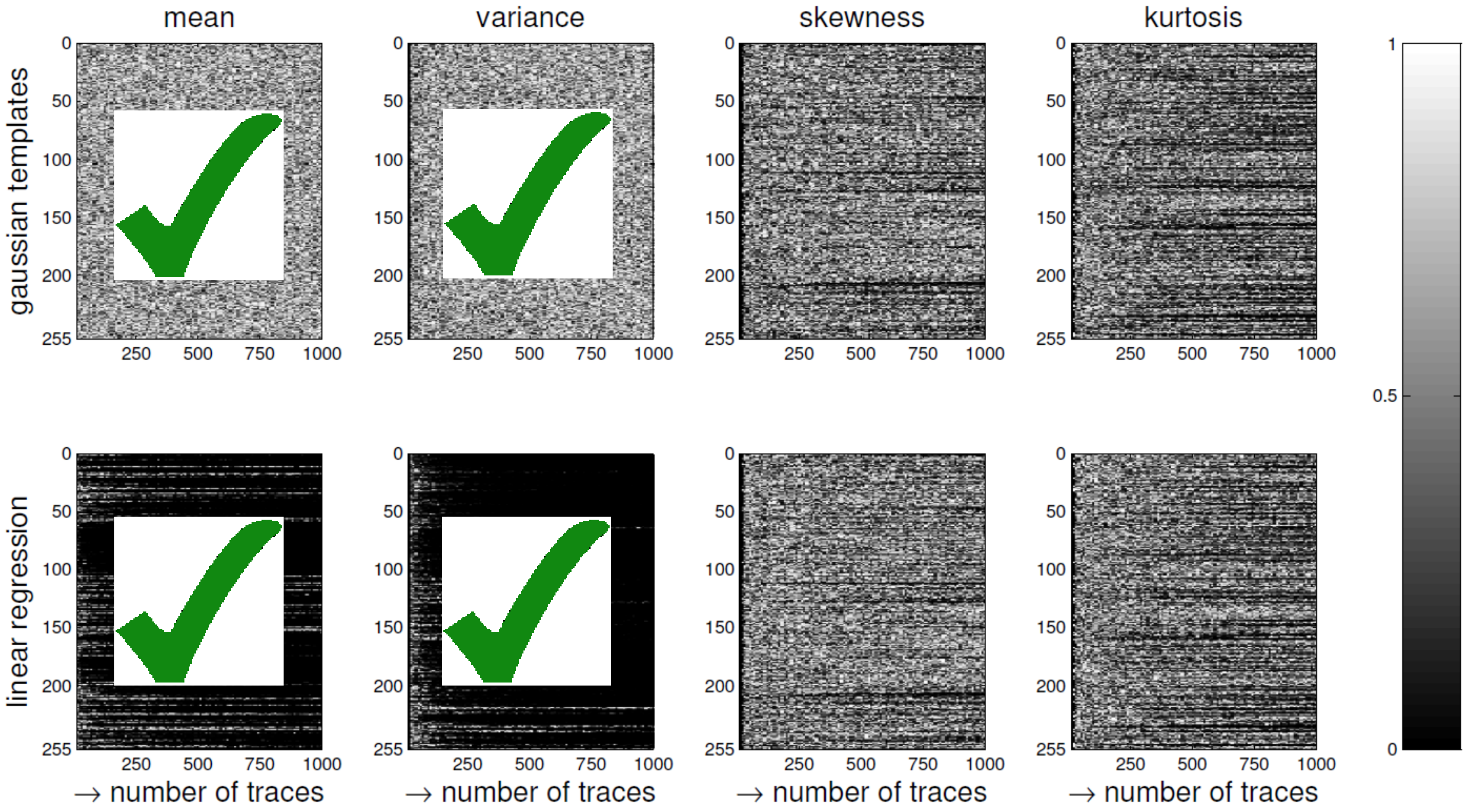
Software experiments

- Unprotected AES implementation, Atmel AVR



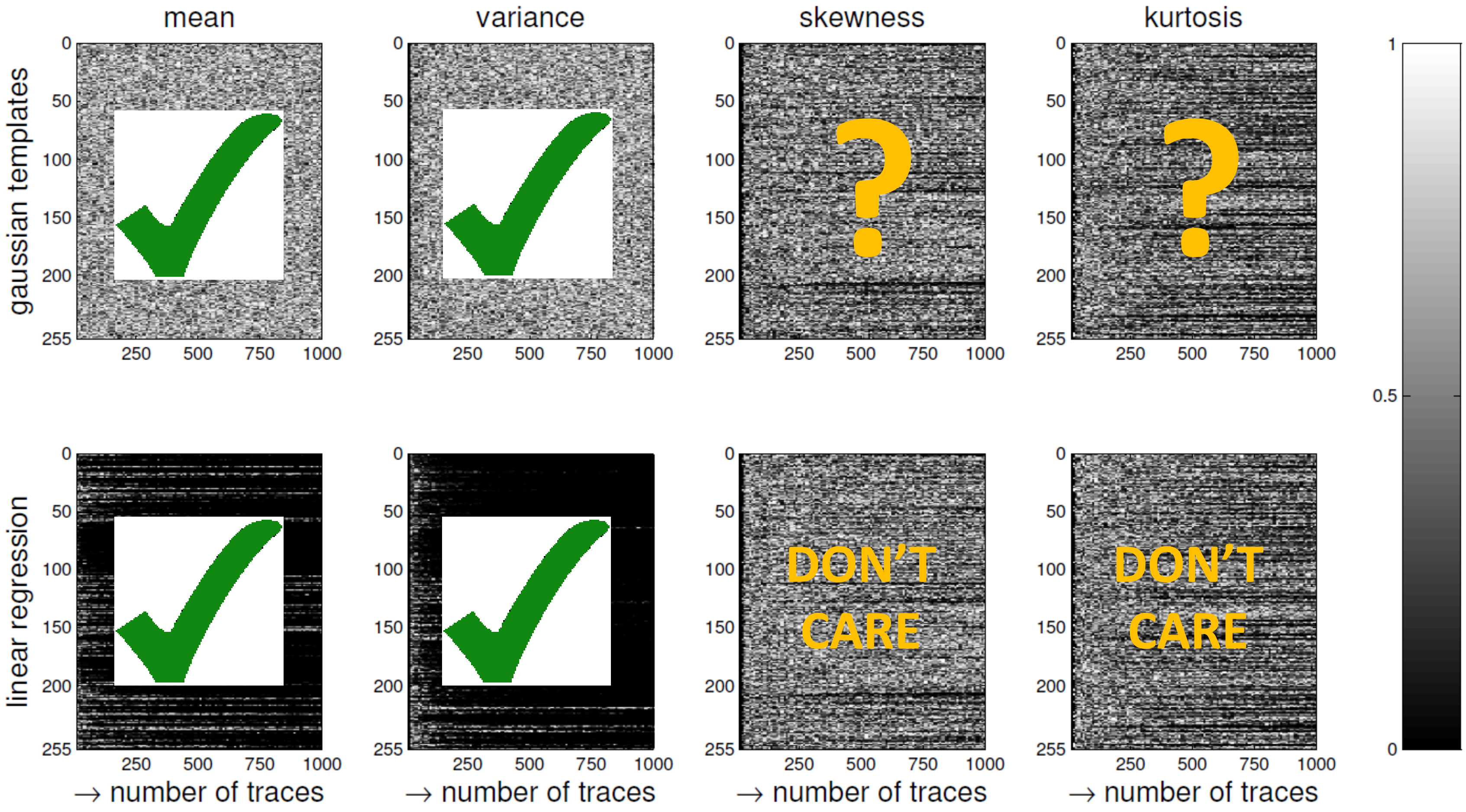
Software experiments

- Unprotected AES implementation, Atmel AVR



Software experiments

- Unprotected AES implementation, Atmel AVR



Software experiments (II)

- Eurocrypt 2014: no errors detected with up to 256x1000 measurements & Gaussian template
- CHES 2016: small errors in $\widetilde{M}_3$ and $\widetilde{M}_4$

$\Rightarrow$ *Is there an inconsistency in our results?*

$\Rightarrow$ Do these errors lead to significant information loss

Software experiments (II)

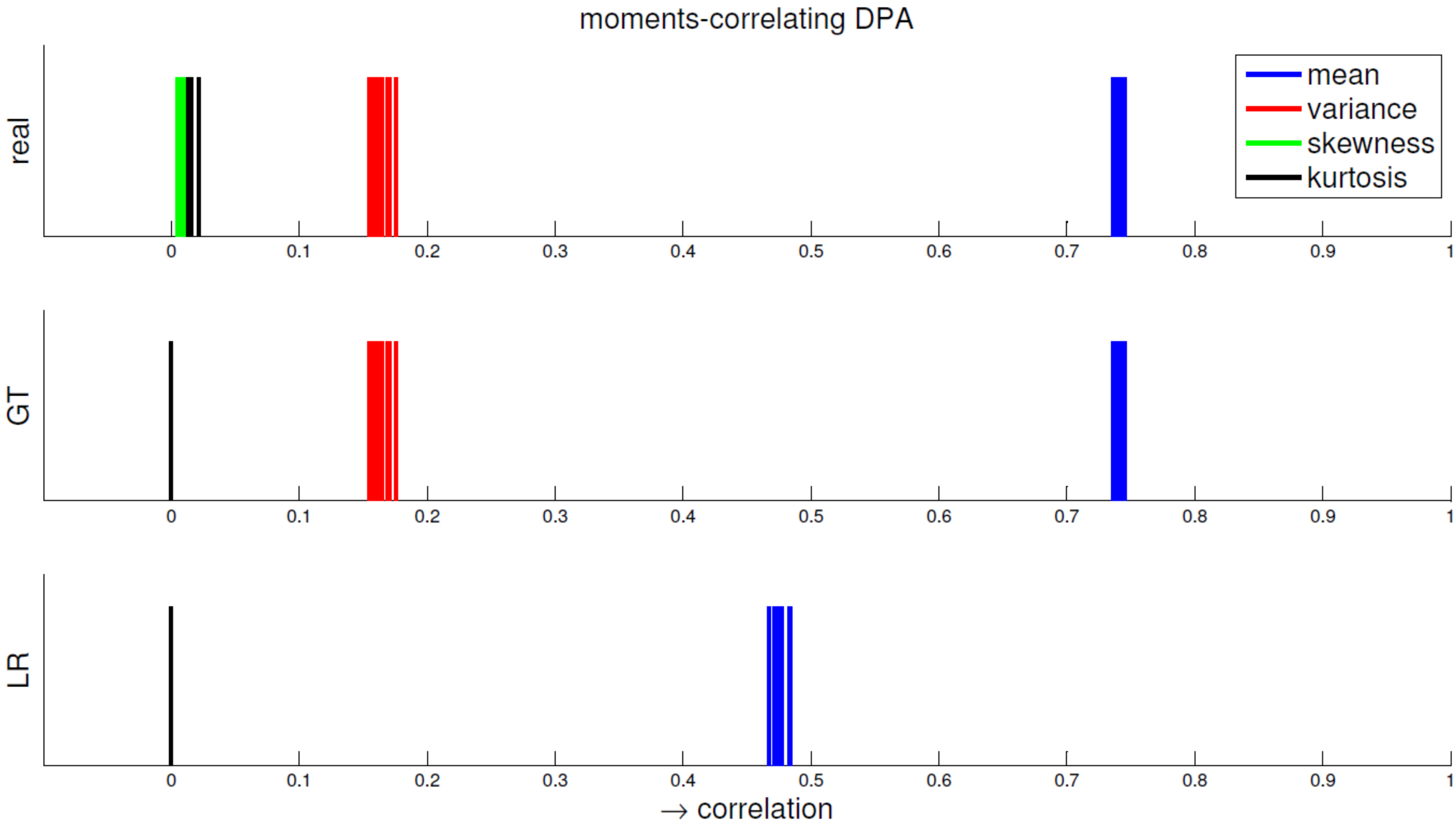
- Additional test: Moments-Correlating DPA [MS14]

$$\text{MPC-DPA}(d) = \hat{\rho}(\hat{M}_d, l^d)$$

- Metric intuition: $N_s = \frac{c}{\hat{\rho}(\hat{M}_d, l^d)^2}$

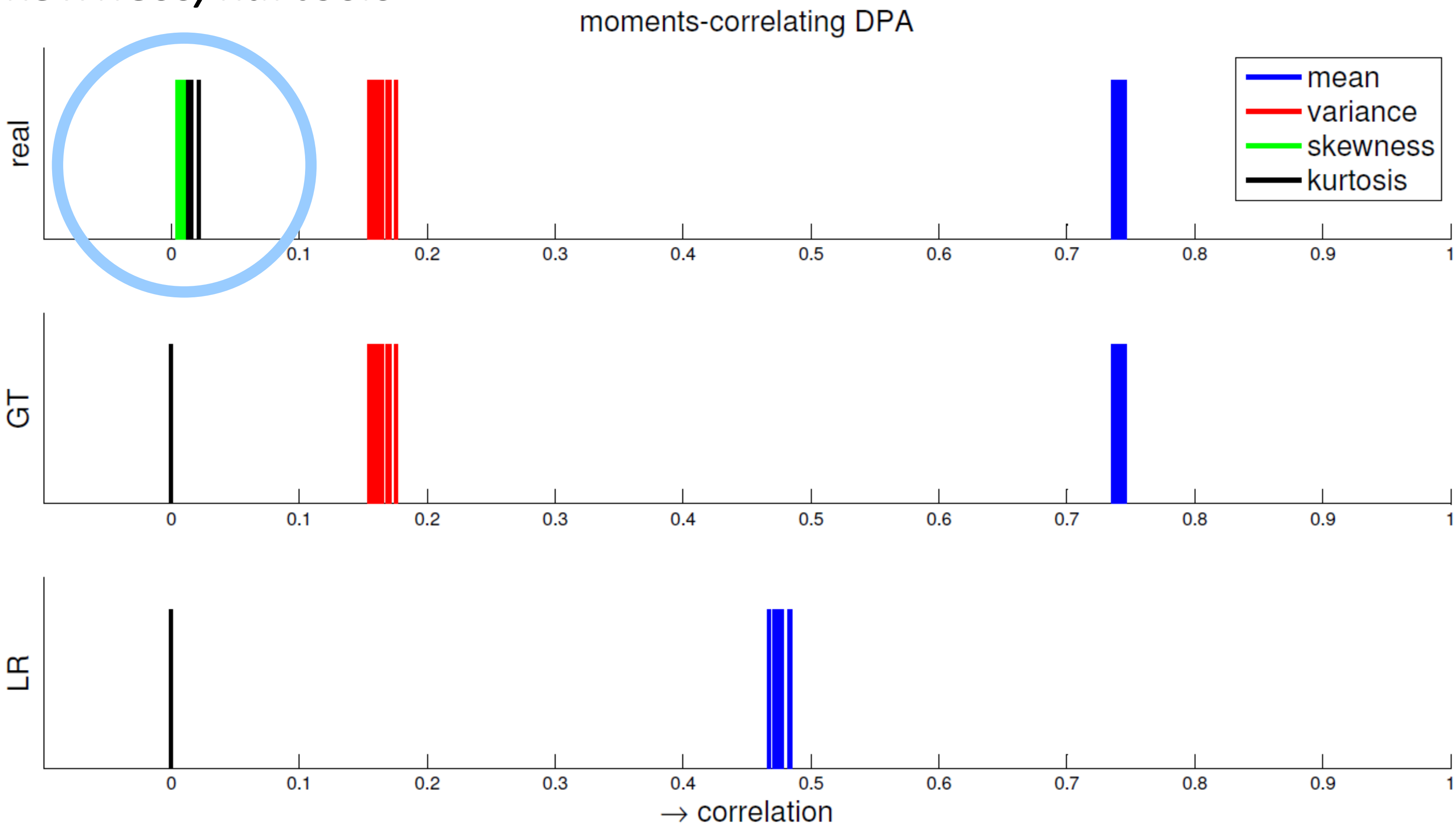
[MS14] A. Moradi, F.-X. Standaert, Moments-Correlating DPA, IACR ePrint Archive, 2014.

Software experiments (III)

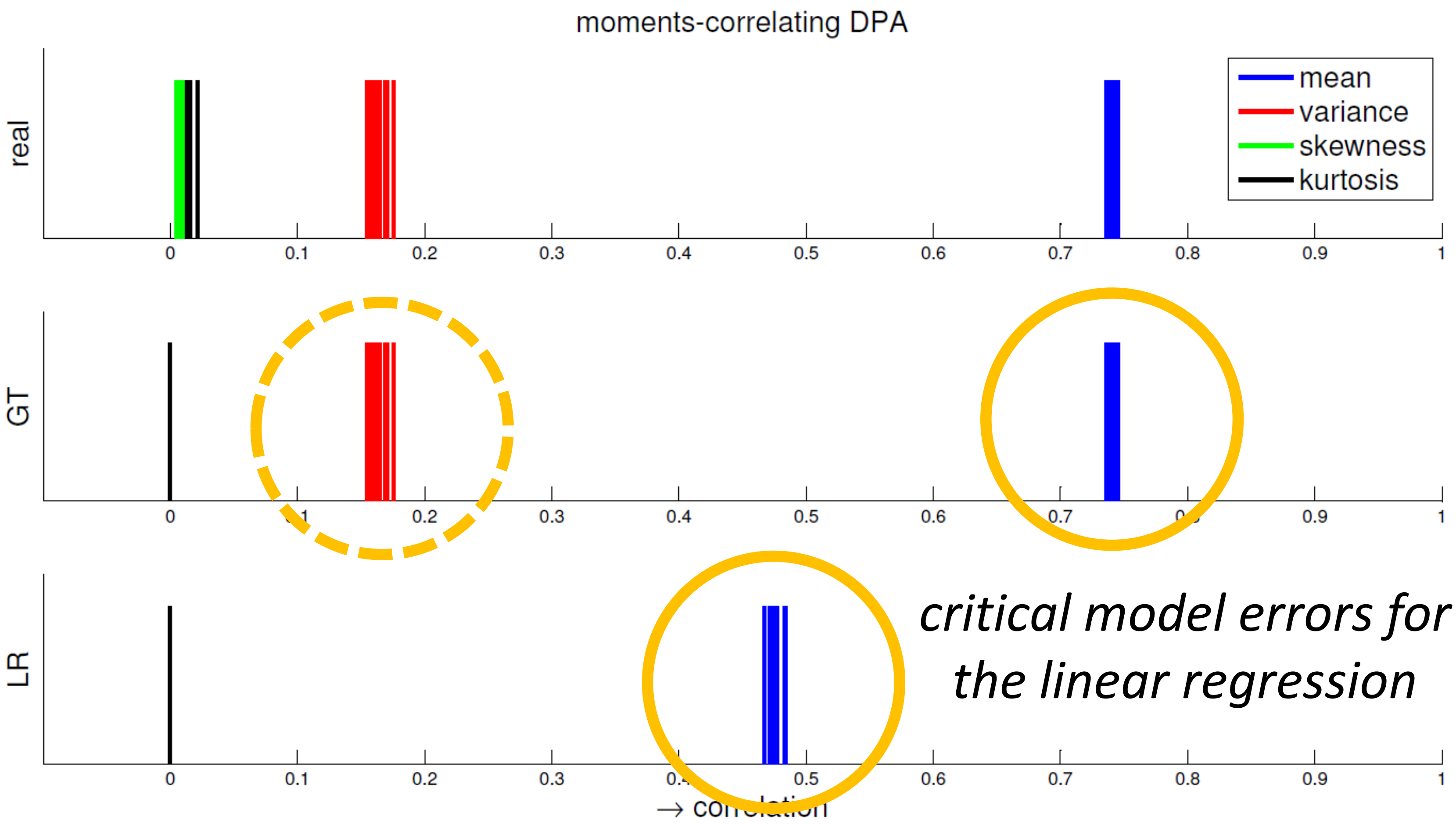


Software experiments (III)

little information in skewness/kurtosis



Software experiments (III)



critical model errors for the linear regression

Outline

1. Introduction & motivation
2. (Easy) Leakage certification
3. **Experiments**
    - Simulations
    - Unprotected software
    - **Masked hardware**
4. Conclusions

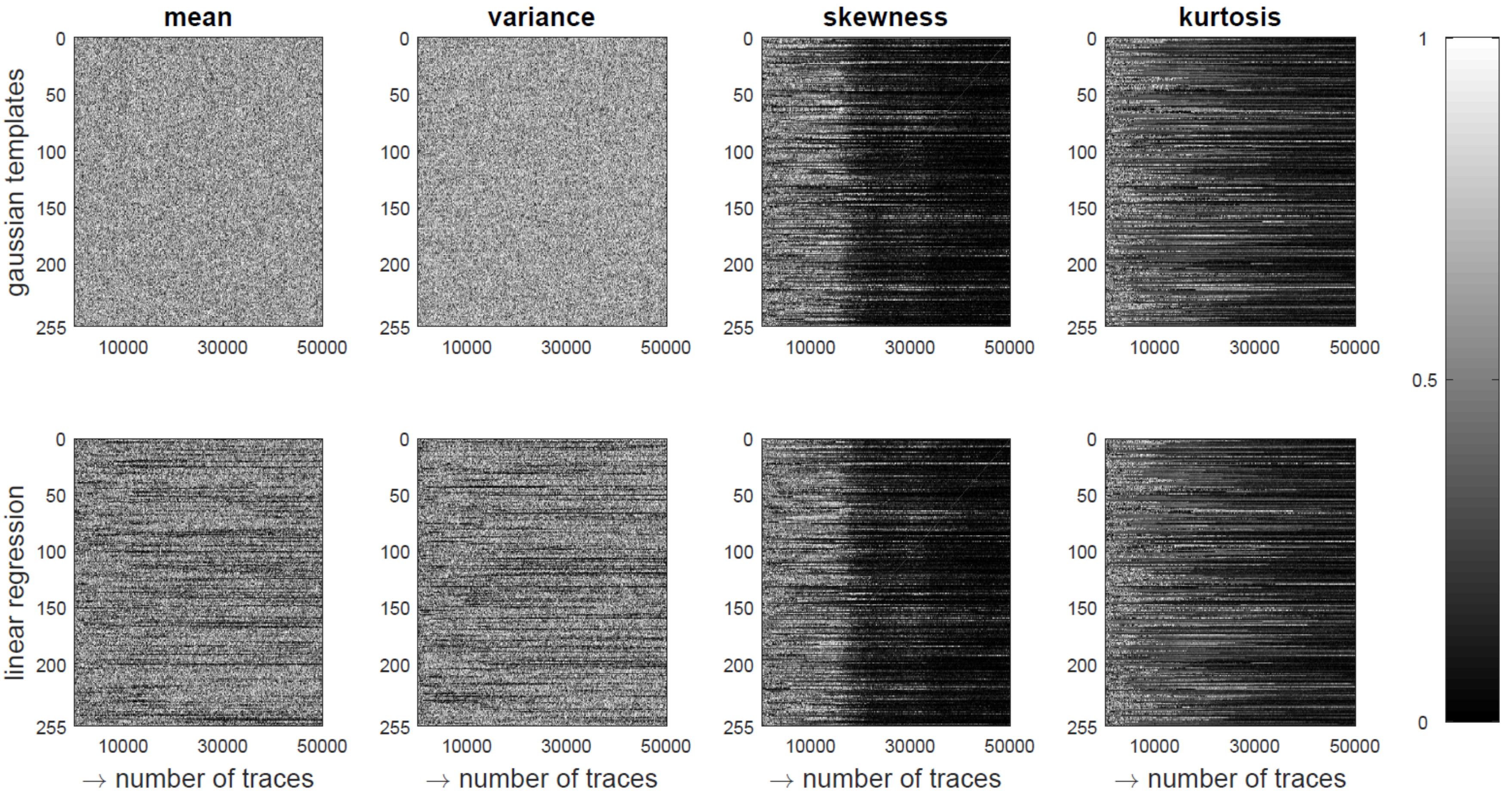
Masked hardware experiments

- 1^{st}-order secure threshold implementation [P+11]

[P+11] A. Poschmann et al., *Side-Channel Resistant Crypto for Less than 2,300 GE*, Journal of Cryptology, 2011.

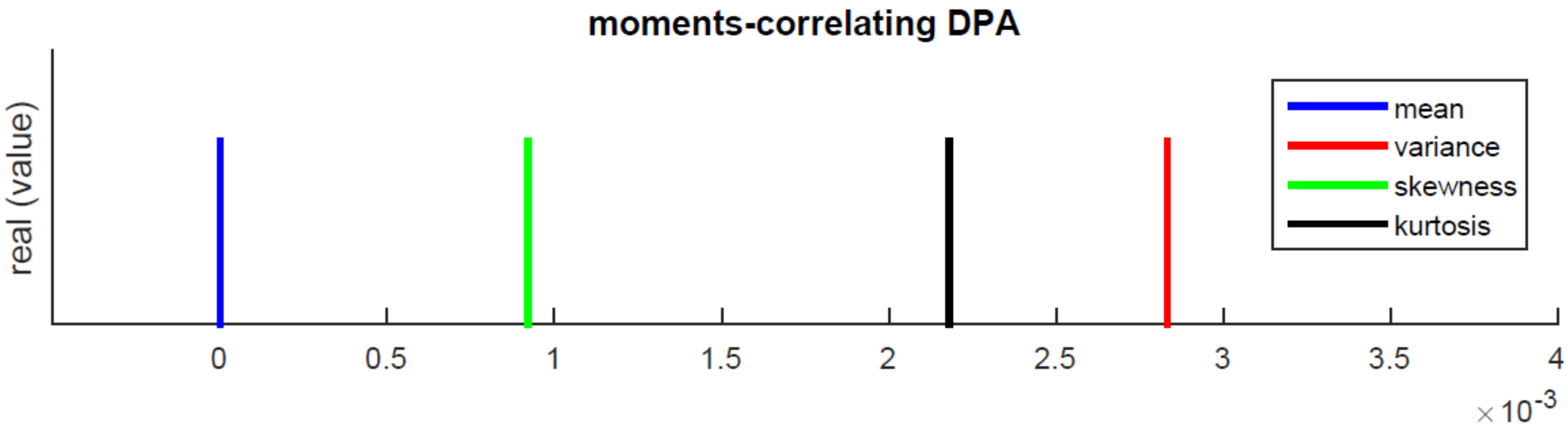
Masked hardware experiments

- 1st-order secure threshold implementation [P+11]

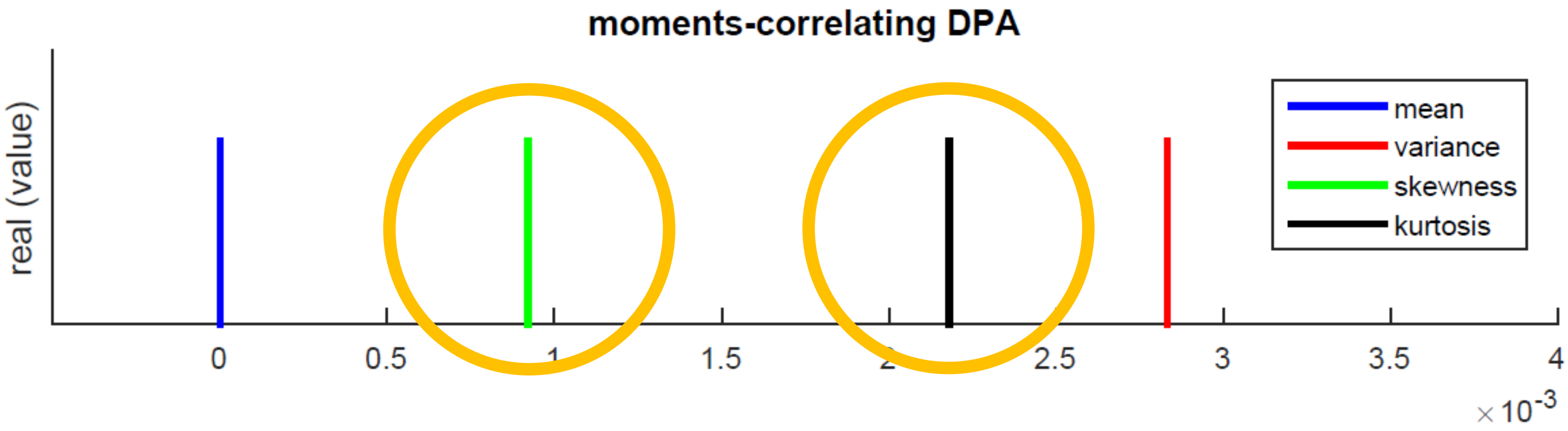


[P+11] A. Poschmann et al., *Side-Channel Resistant Crypto for Less than 2,300 GE*, Journal of Cryptology, 2011.

Masked hardware experiments (II)



Masked hardware experiments (II)



critical model errors for the Gaussian templates

Masked hardware experiments (II)

- As expected since GT capture only 2 moments

$\Rightarrow$ More complex models needed in this case [S+16]

[S+16] T. Schneider et al., *Bridging the Gap: Advanced Tools for Side-Channel Leakage Estimation […]*, SAC 2016.

Outline

1. Introduction & motivation
2. (Easy) Leakage certification
3. Experiments
   - Simulations
   - Unprotected software
   - Masked hardware
4. **Conclusions**

Wrapping up

- Less formal but more efficient/intuitive tool

Wrapping up

- Less formal but more efficient/intuitive tool
  - ≈ as efficient as profiled CPA
    - (But still benefits from POI detection)
  - Provides hints about the information losses

Wrapping up

- Prototype open source code:

http://perso.uclouvain.be/fstandae/PUBLIS/171.zip

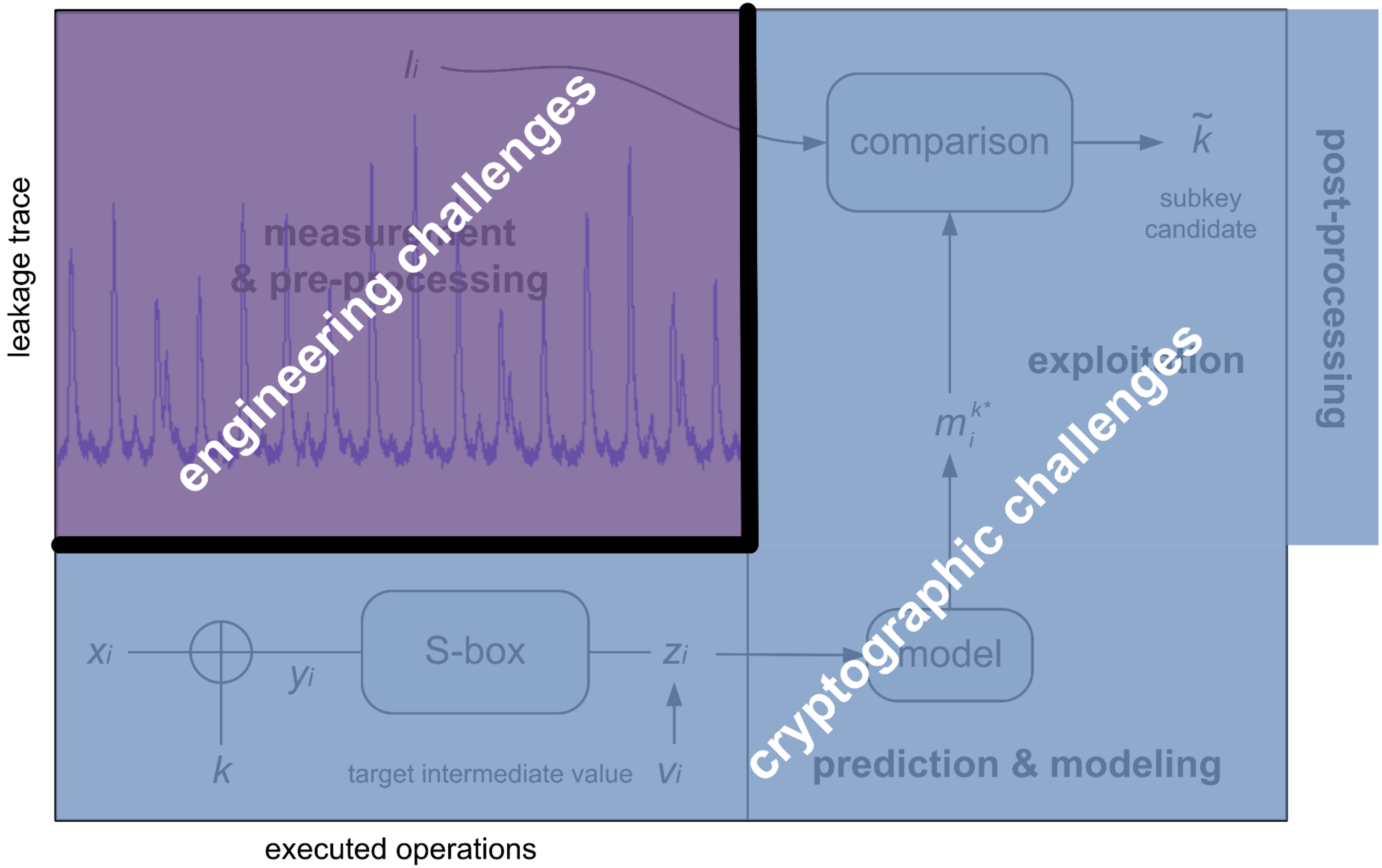
Wrapping up

- Open problems: how to efficiently deal with multivariate & higher-order distributions
- Moment- vs. distribution-based evaluations?

Wrapping up

PS. *No assumption errors if non-parametric estimations*

Thanks!


leakage trace
l_i
measurement
& pre-processing
engineering challenges
comparison
$\tilde{k}$
subkey
candidate
post-processing
exploitation
$m_i^{k^*}$
cryptographic challenges
x_i
y_i
S-box
z_i
model
k
target intermediate value
v_i
prediction & modeling
executed operations