UCLouvain

Crypto. group



# *Reducing a Masked Implementation's Effective Security Order with Setup Manipulations*

## And an Explanation Based on *Externally-Amplified Couplings*

Itamar Levi, Davide Bellizia and François-Xavier Standaert

Aug. 2018

# Motivation



Masking - a well understood SCA countermeasure

- Split sensitive variables into *d* shares.
- Compute on those shares only.

Independence assumption – the shares induced leakages are independent, and

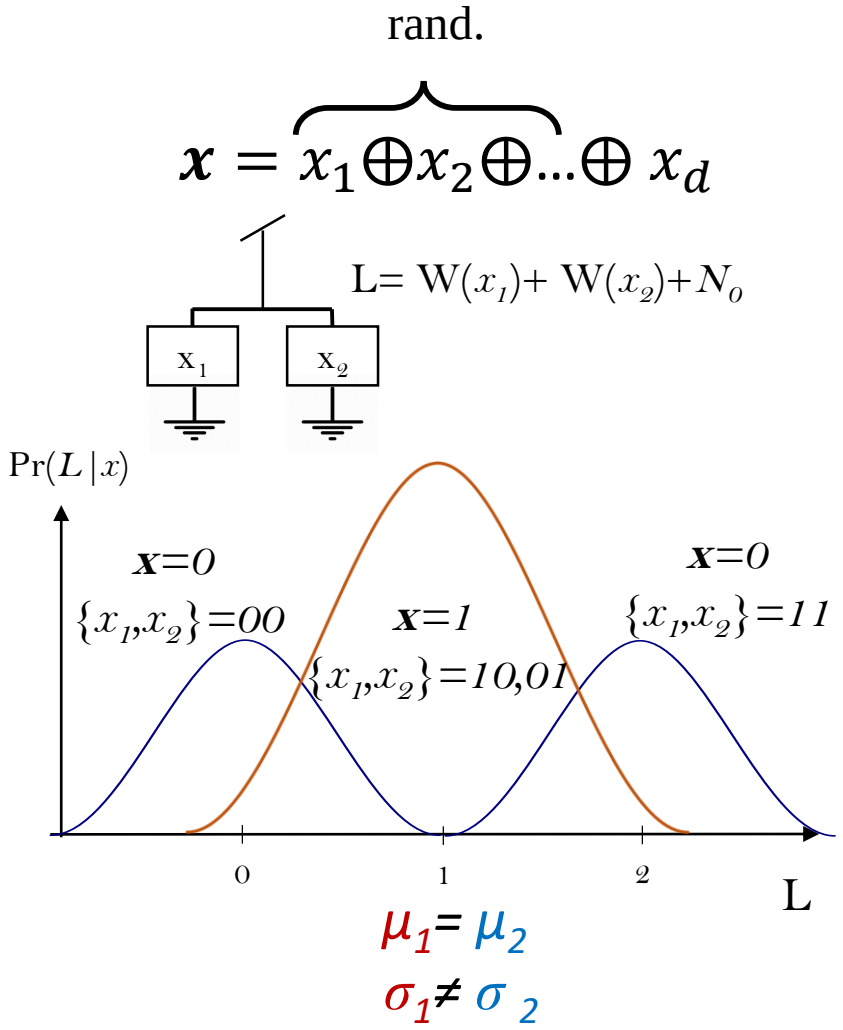
- **they are merged linearly…**

It forces the adversary to estimate a higher-order statistical moment of the leakage

- data complexity grows exponentially with *d* -> amplifies the noise in the leakages

The lowest key-dependent stat. moment - security order

**Concretely though, it is hard to achieve it…**

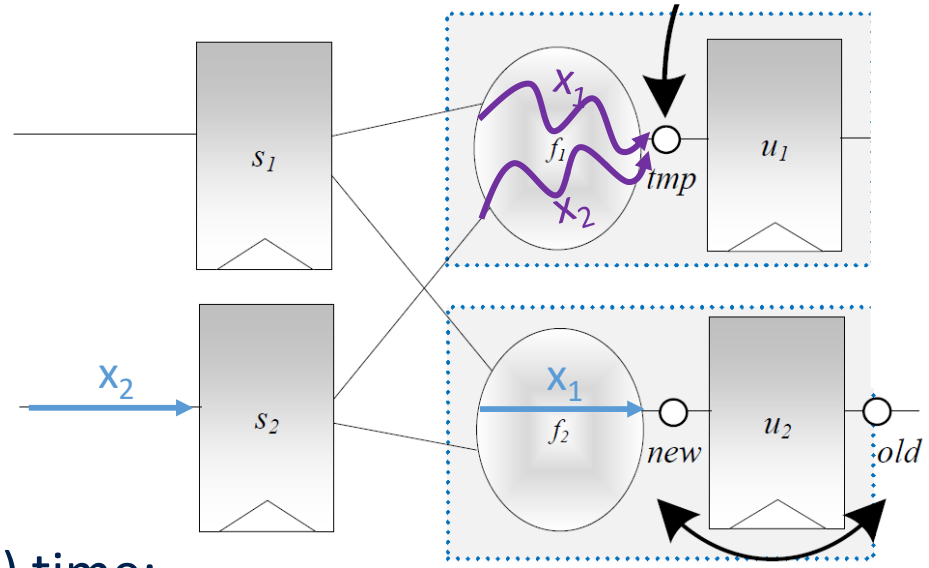


# Motivation

Well understood non-idealities:

- Glitches
- Memory transitions

Can recombine leakages (nonlinear manner)



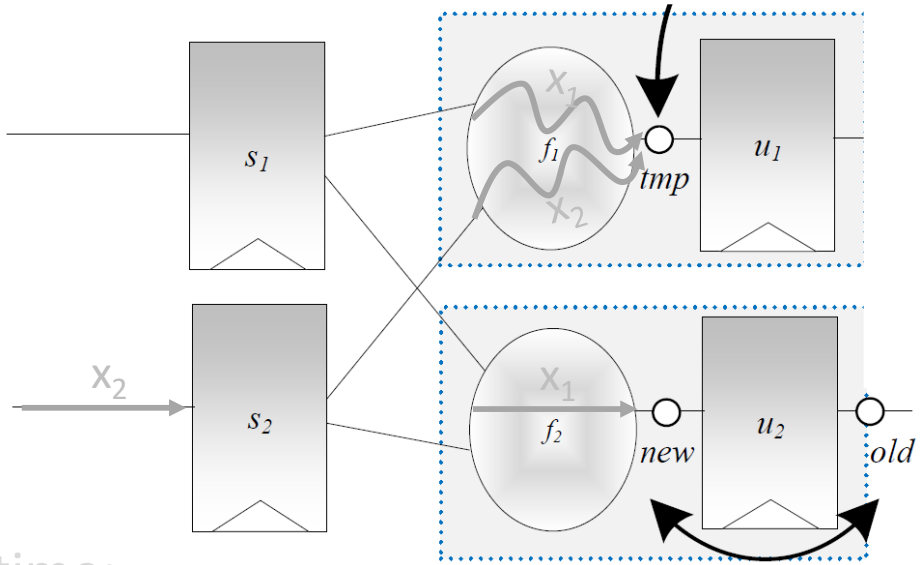

Can be kept under control at design (synthesis) time:

- Threshold Implementations (TIs) - non-completeness [NRS11]
- Transition-based leakages can be mitigated by doubling the number of shares [BGG+14] / adding registers or refreshing [CGP+12]

**=> *logical recombination***, since they can be formulated as logical conditions which can then be verified and prevented [FGP+18] **=>** recalling yesterday's *Session 6*.

# Motivation






Well understood physical defaults:

- Glitches
- Memory transitions

Can recombine leakages (nonlinear manner)

Can be kept under control at design (synthesis) time:

- Threshold Implementations (TIs) - non-completeness [NRS11]
- Transition-based leakages can be mitigated by doubling the number of shares [BGG+14] / adding registers or refreshing [CGP+12]

=> ***logical recombinations***, since they can be formulated as logical conditions which can then be verified and prevented [FGP+18].

This talk: another physical default, ***couplings***, recently reported by De Cnudde et al.

- Electrical dependency between the shares (e.g. capacitive, resistive)

# Outline



What are couplings

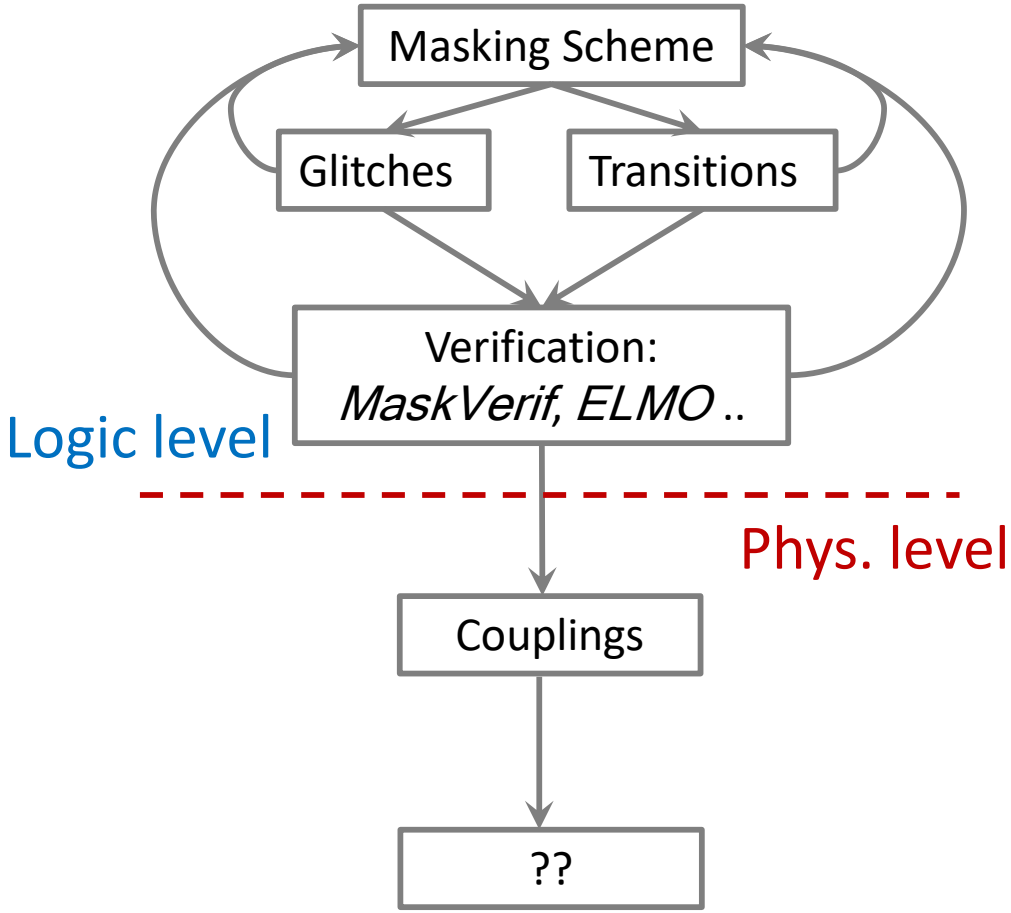
What do we know of them

How to **externally** amplify them

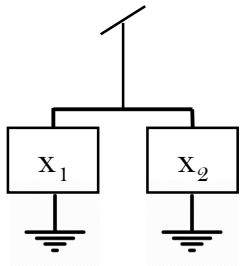
Different test cases (SW/HW)

- Moving from detection to exploitation

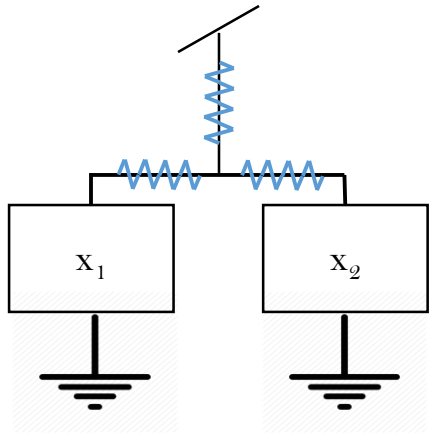
Discussion/ how to advance

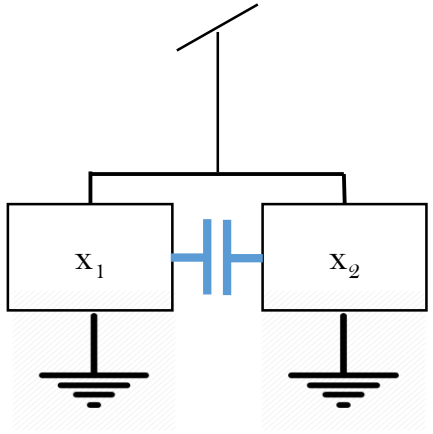


# What are couplings



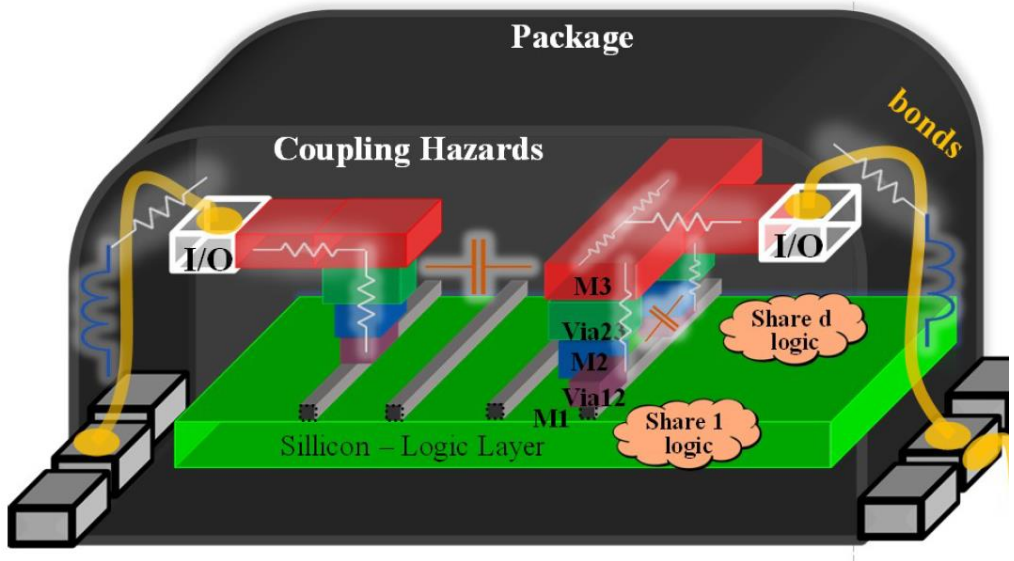

In theory




In practice: *not so linear and not so nice…*

- Electrical
  - Capacitive
  - Resistive
  - Inductive (less local)
  - Memri/Resistive-RAM (consider new devices M/RRAM etc.)
- Affected by
  - Capacitive - proximity
  - Resistive - power-grid / proximity
  - All - Technology params
  - Periodicity (L, RC)
- What can we control?
  - Depend on the device (SW/FPGA/ASIC…) but,
  - Mainly on the power-grid and proximity

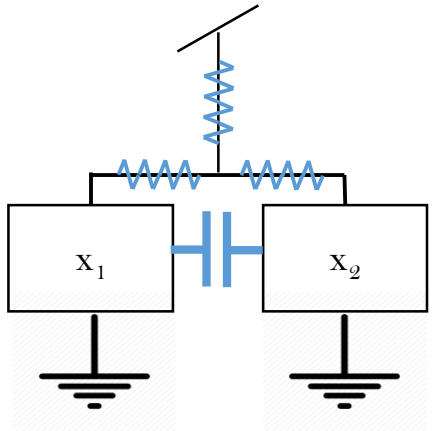


# What do we know of them

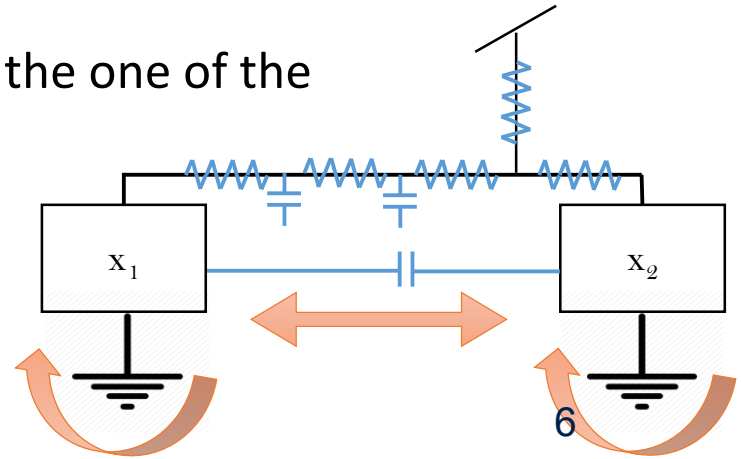


## In the context of SCA

- De Cnudde et al., [CBG+17, CEM18] put forward that even when implemented correctly (glitches, transitions), masking can suffer from re-combinations.
  - Tweaking shares proximity (placement and routing)
  - Iterating/parallelize the shares to increase their signal/re-combination




- *Typically not something an adversary can do .. (designers will aim to prevent)*
- *Practically:*
  - The amplitude of these lower-order leakages was usually lower than the one of the $d^{th}$ order leakages [CBG+17]
  - Were evaluated by detection-tests (T-tests)

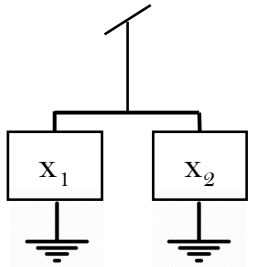



- *Is there a real threat without internal-amplification?*

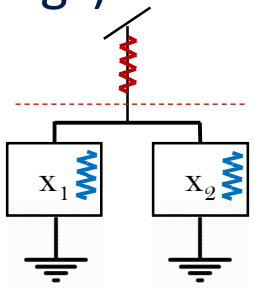
# How to *externally* amplify them



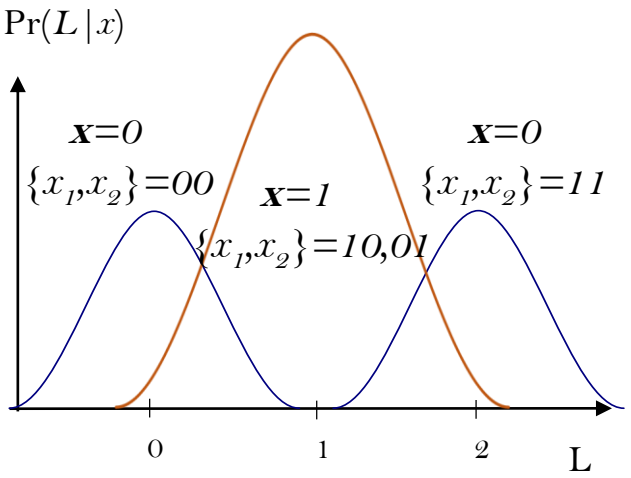
- A simple example (resistive couplings):

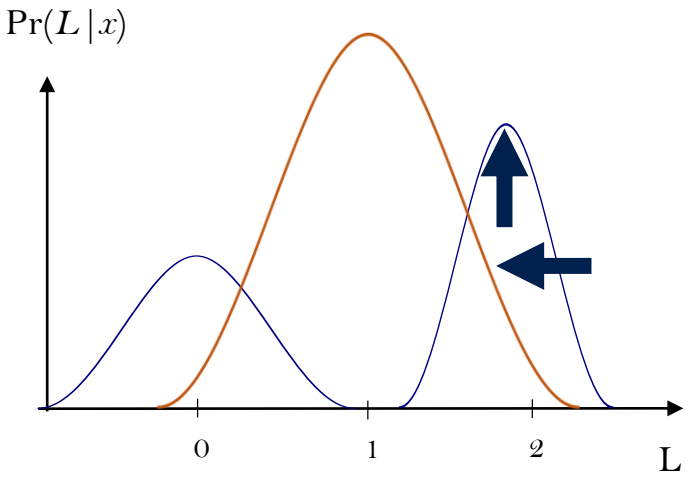


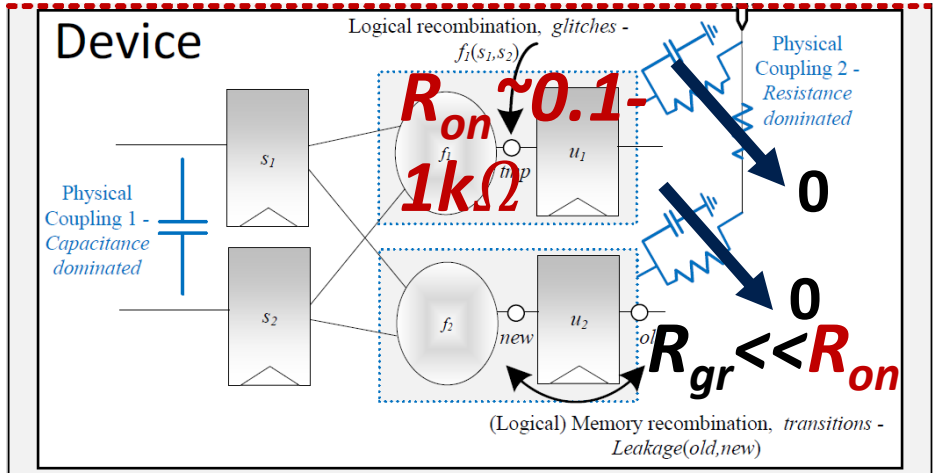

$$L = I_{Sh1} + I_{Sh2}$$




$$L' = \alpha_1 I_{Sh1} + \alpha_2 I_{Sh2} - \beta(I_{Sh1} \cdot I_{Sh2})$$



# How to *externally* amplify them

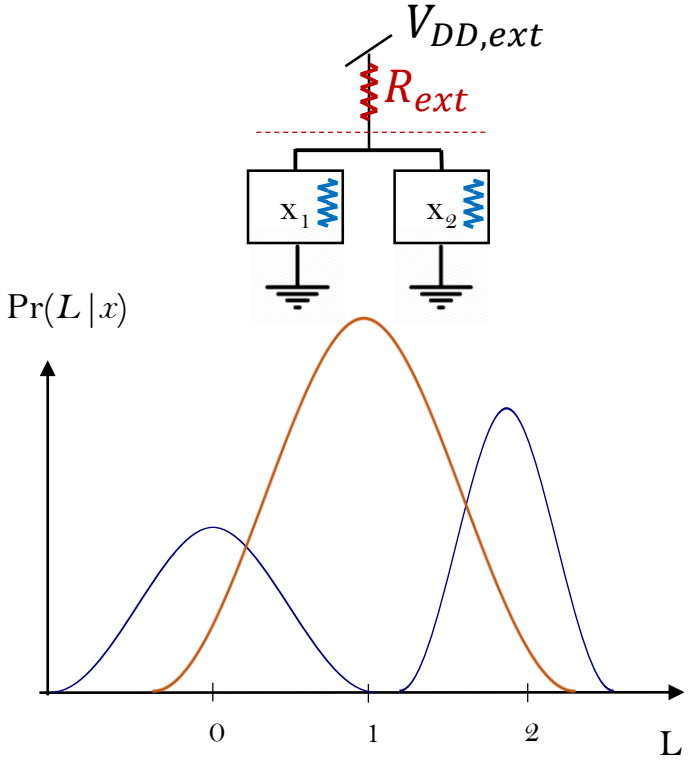


- A simple example:
  - Devices in linear mode..
  - First order approx.
  - No capacitive effects

$$I' = \alpha_1 I_{Sh1} + \alpha_2 I_{Sh2} - \beta(I_{Sh1} \cdot I_{Sh2})$$

$$\alpha_i = \frac{1}{\left(1 + \frac{2R_{ext}}{R_{on\_i}}\right)} \approx 1$$

$$\beta = \frac{R_{ext}}{V_{DD,ext}}\left[\frac{R_{on1}}{2R_{ext} + R_{on1}} + \frac{R_{on2}}{2R_{ext} + R_{on2}}\right]_{R_{ext} \ll R_{on1}, R_{on2}} \cong \frac{2R_{ext}}{V_{DD,ext}}$$




- But, lowering $V_{DD}$ has a *negative effect…*
  - Reduces the signal (typically, SNR ↓)
  - At some point the device will not work

# How to *externally* amplify them

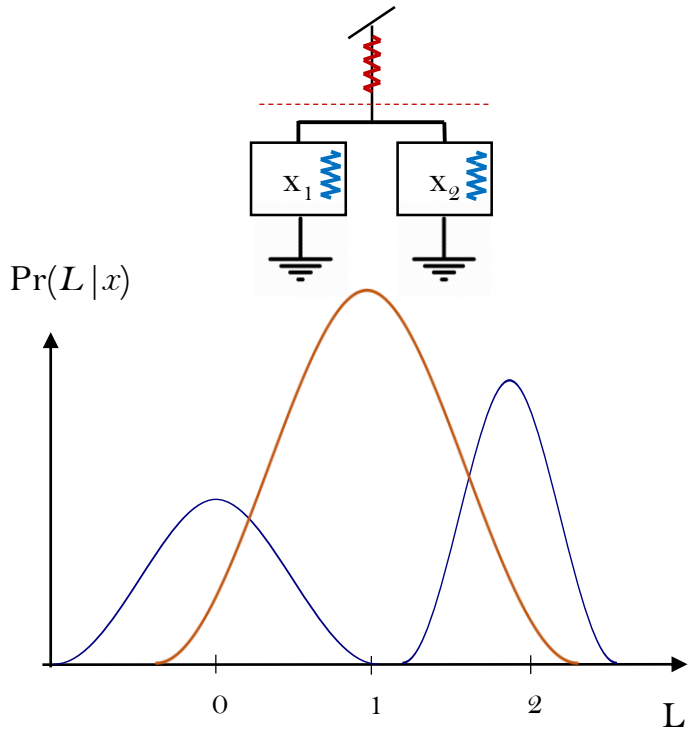


- A simple example:
  - Devices in linear mode..
  - First order
  - No capacitive effects

$$I' = \alpha_1 I_{Sh1} + \alpha_2 I_{Sh2} - \beta(I_{Sh1} \cdot I_{Sh2})$$

$$\alpha_i = \frac{1}{\left(1 + \frac{2R_{ext}}{R_{on\_i}}\right)} \approx 1$$

$$\beta = \frac{R_{ext}}{V_{DD,ext}}\left[\frac{R_{on1}}{2R_{ext} + R_{on1}} + \frac{R_{on2}}{2R_{ext} + R_{on2}}\right]_{R_{ext} \ll R_{on1}, R_{on2}} \cong \frac{2R_{ext}}{V_{DD,ext}}$$




- But, lowering $V_{DD}$ has a *negative effect…*
  - Reduces the signal (typically, SNR ↓)
  - At some point the device will not work

- So, increasing $R_{ext}$ then,
  - Too much- the device will not work
  - We might need to simult. Increase $V_{DD}$
  - *With $R_{ext}$↑ the noise increase*

# How to *externally* amplify them



$$I' = \alpha_1 I_{Sh1} + \alpha_2 I_{Sh2} - \beta(I_{Sh1} \cdot I_{Sh2})$$

$$\beta \cong \frac{2R_{ext}}{V_{DD,ext}}$$

- But, lowering $V_{DD}$ has a *negative effect…*
  - Reduces the signal (typically, SNR ↓)
  - At some point the device will not work

- So, increasing $R_{ext}$ then,
  - Too much- the device will not work
  - We might need to simult. Increase $V_{DD}$
  - *With $R_{ext}$↑ the noise increase*

- No trivial answer to what is the worst-case scenario,
  - Depends on the device, the noise, power regulator (if any).
  - The exploration space for a certification lab is huge …

# How to *externally* amplify them



$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} \boxed{-\frac{R_{\text{ext}}}{V_{DD\_ext}}} \cdot \underbrace{\sum_i \sum_j I_j I'_i}_{1^{st}\ order} + \ldots \underbrace{\quad}_{higher\_powers}$$

The simplified model can be generalized (*d*):

-------> *d* --------> *d*/2 ???

- But,
  - Expected: leakage at all stat.-moments/powers (solve MAXWELL …) ➔ modeling is hard
- So our goals were:
  - To examine weather setup-manipulations can reduce the ***effectively security-order***
  - Our explanation is based on these ***externally amplified couplings***
- The approach we use:
  - To try and falsify
  - To understand if the amplitudes of lower orders leakages can be made significant with amplification

# How to evaluate?



Moving on from a:

- "detection" based approach (T-test)
  - Hard to connect with actual SR

$$T_{value} = (\mu_{Set_0} - \mu_{Set_1}) \Big/ \sqrt{{\sigma_{Set_0}}^2/|Set_0| + {\sigma_{Set_1}}^2/|Set_1|}.$$

- to actual exploitation (MCP-DPA):

$$\tilde{k} = \arg\max_{k*} \quad \hat{\rho}(\hat{M}^d_{x,k*}, \ \left({l^t}_{x,k}\right)^d)$$

  - Profiling moments (*d*=2 use CM, *d*>2 use SM..)
    - Gives us the ability to check the contribution of different statistical orders
  - The asymptotic value gives an estimation of the informativeness /SR /#samples required [MS16]

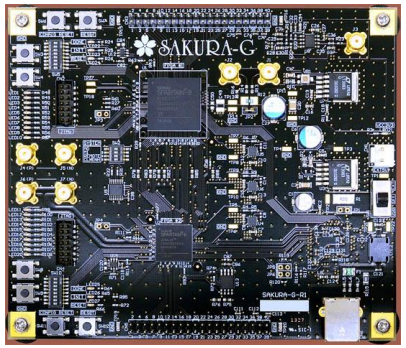
# Test-cases



- We have investigated two designs / platforms:
  - HW: AES128 (8bit) 2-shares implementation adopting Domain Oriented Masking [GMK17] on Spartan6 LX75 FPGA (Sakura G board)
  - SW: 2-shares AES SBOX with the bitslice secure scheme in [JS17] implementation following Barthe et-al. [BDF+17] on an Atmel SAM4C16 (ARM Cortex-M4)

HW

- Picoscope 5244B (quant. 12bit) +
- Sakura G's preamp
- low-noise res. (0 to 20Ω).
- $f_{clk}$ = 4MHz
- $S_R$ = 250MS/s (<- enough)
- $V_{DD}$ from 1 to 1.45 V




SW

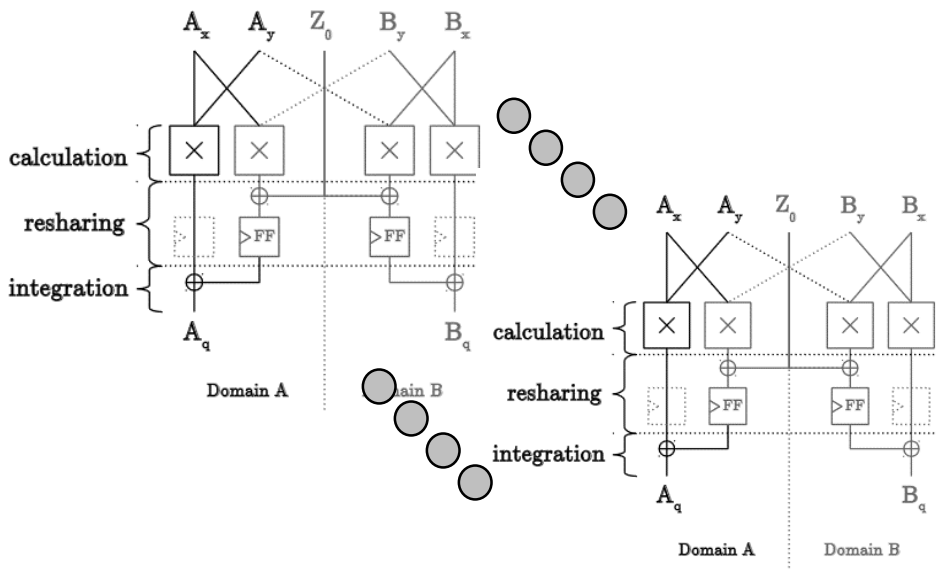
- Lecroy WaveRunner (12bit),
- Tektronix CT1 + res. (1 Ω to 39Ω), benchtop PSU
- $f_{clk}$ = 100MHz
- $S_R$ = 1GS/s
- $V_{DD}$ from 1 to 1.55 V
- Removed - 2.2, 0.1 $\mu F$ Caps...

- Commercial off-the-shelf devices – yet to be explored on ASICs/ specialized devices

# Test-cases



## HW




- HW – *S*box-parallel design

## SW

0: **Input**: shares of $a$ and $b$ $(\boldsymbol{a}, \boldsymbol{b})$ and a uniform randomness vector $\boldsymbol{r}$.

0: **Output**: shares $\boldsymbol{x}$ of $x$, with $a \cdot b = \bigoplus_{i=1}^{d} x_i$.

1: $\boldsymbol{c}_1 = \boldsymbol{a} \cdot \boldsymbol{b}$
2: $\boldsymbol{c}_2 = \boldsymbol{a} \cdot \mathsf{rot}(\boldsymbol{b}, 1)$
3: $\boldsymbol{c}_3 = \mathsf{rot}(\boldsymbol{a}, 1) \cdot \boldsymbol{b}$
4: $\boldsymbol{d}_1 = \boldsymbol{c}_1 \oplus \boldsymbol{r}$
5: $\boldsymbol{d}_2 = \boldsymbol{d}_1 \oplus \boldsymbol{c}_2$
6: $\boldsymbol{d}_3 = \boldsymbol{d}_2 \oplus \boldsymbol{c}_3$
7: $\boldsymbol{d}_4 = \boldsymbol{d}_3 \oplus \mathsf{rot}(\boldsymbol{r}, 1)$
8: $\boldsymbol{x} = \boldsymbol{d}_4$
9: return $\boldsymbol{x}$

- *SW - serial → nicer to interprate …*
- ***Conceptually SW will be more sensitive due to a shared power-grid***

# Is the problem concrete?



Software implementation (*u*C) – ARM32 bit (ATMEGA)

Model/Simulation

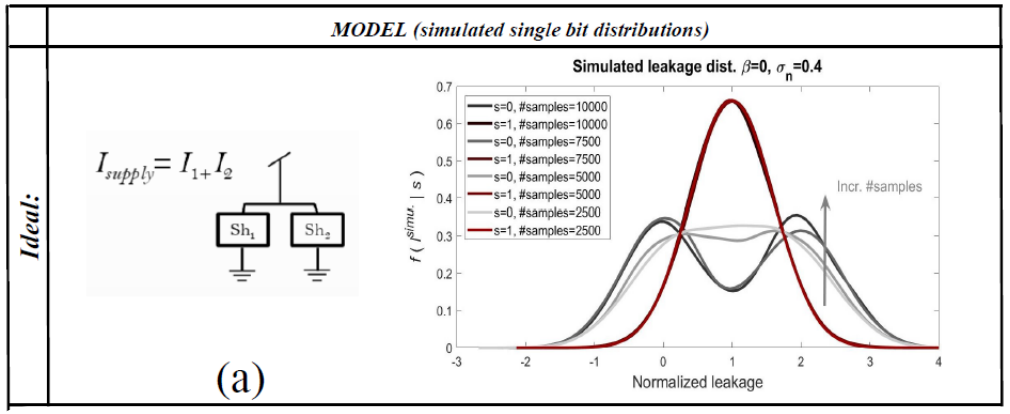



Figure 2: $f(l^{simu.}|s)$: (a) $\beta$=0 (b) $\beta$=0.5

**Measurement (*u*C)**

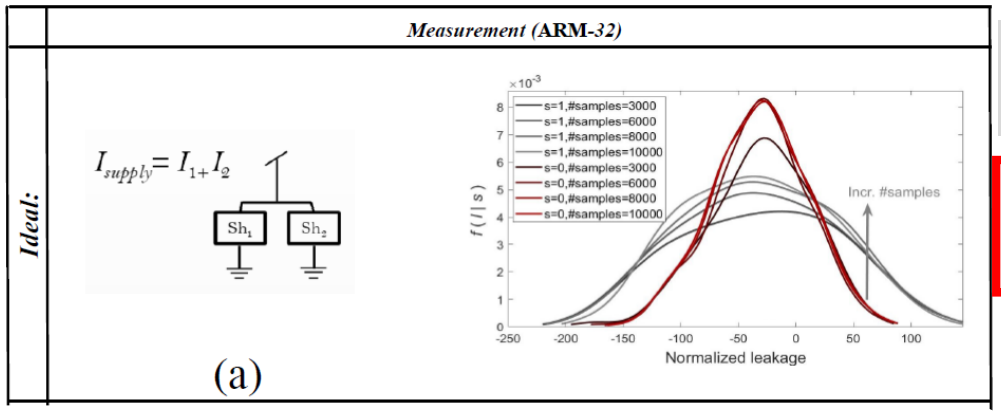



Figure 8: $f(l|s)$, $1 \cdot 10^6$ traces: (a) $R_{ext}$=0Ω (b) $R_{ext}$=20Ω

No ampl.

1ohm
1.4 | 1.2V

# Is the problem concrete?



Software implementation (*u*C) – ARM32 bit (ATMEGA)

Model/Simulation

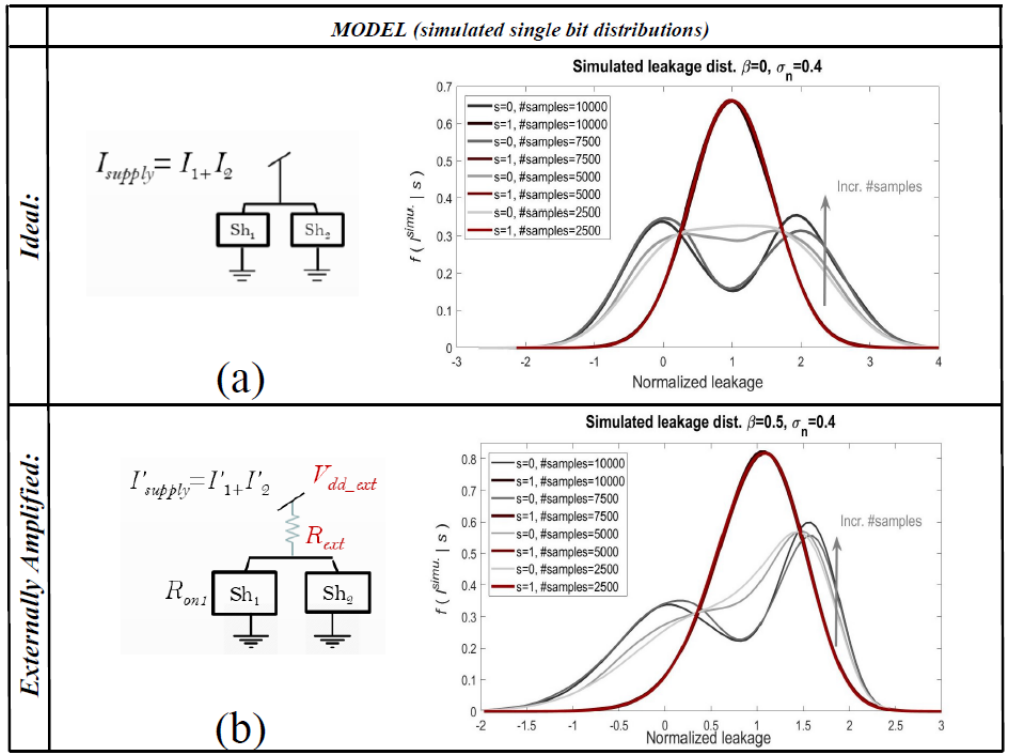



Figure 2: $f(l^{simu.}|s)$: (a) $\beta$=0 (b) $\beta$=0.5

**Measurement (*u*C)**

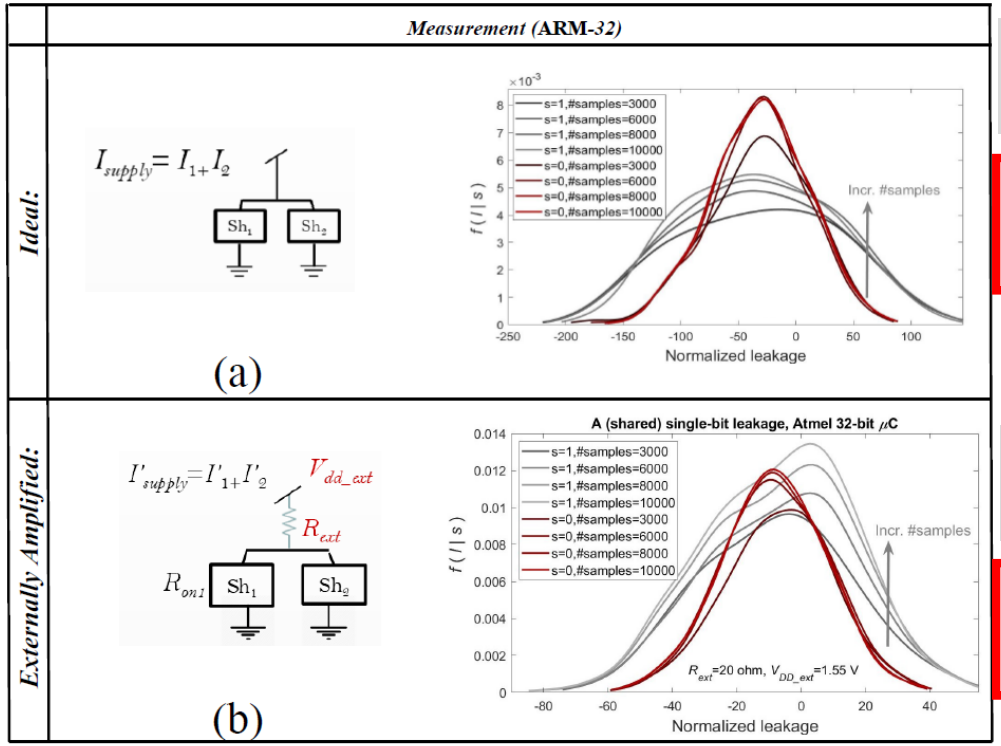



Figure 8: $f(l|s)$, $1 \cdot 10^6$ traces: (a) $R_{ext}$=0Ω (b) $R_{ext}$=20Ω

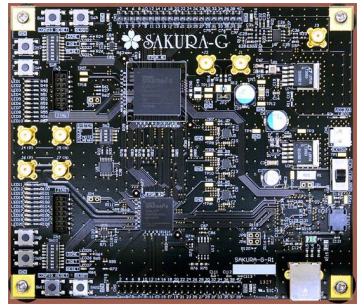
No ampl.

1ohm 1.4 | 1.2V

Ext. ampl.

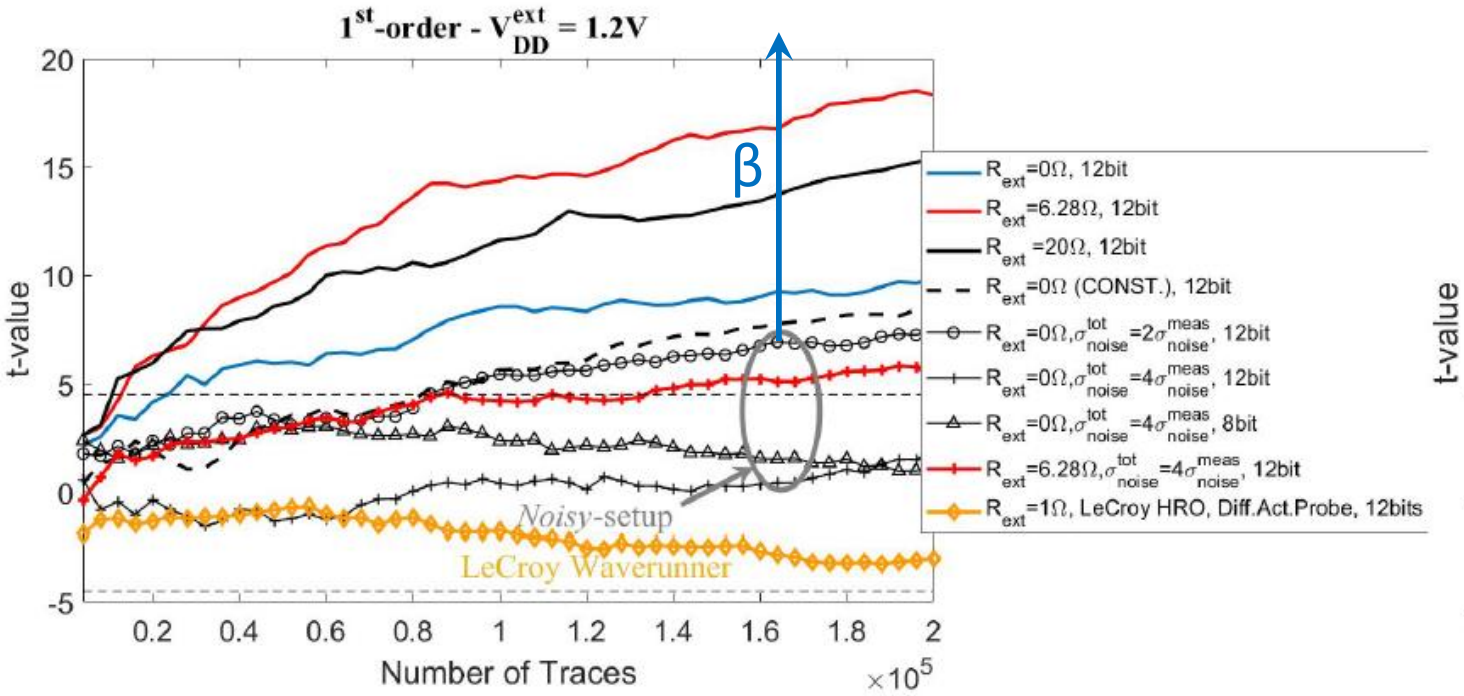
20ohm 1.55V

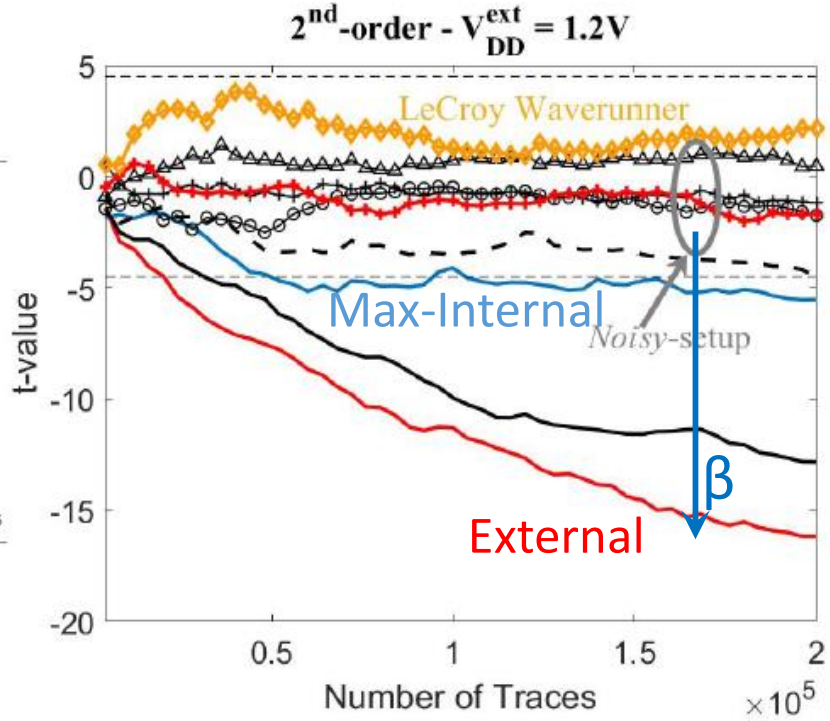
# A T-test sanity check..




* DoM AES (Hannes et-al. [GNK17])
* Hardware – FPGA (Spartan 6) scenario
  - "detection" based approach (T-test)
  - Only one voltage case (nominal), R changing.

$$T_{value} = (\mu_{Set_0} - \mu_{Set_1}) \Big/ \sqrt{{\sigma_{Set_0}}^2/|Set_0| + {\sigma_{Set_1}}^2/|Set_1|}.$$




Baseline

Internal

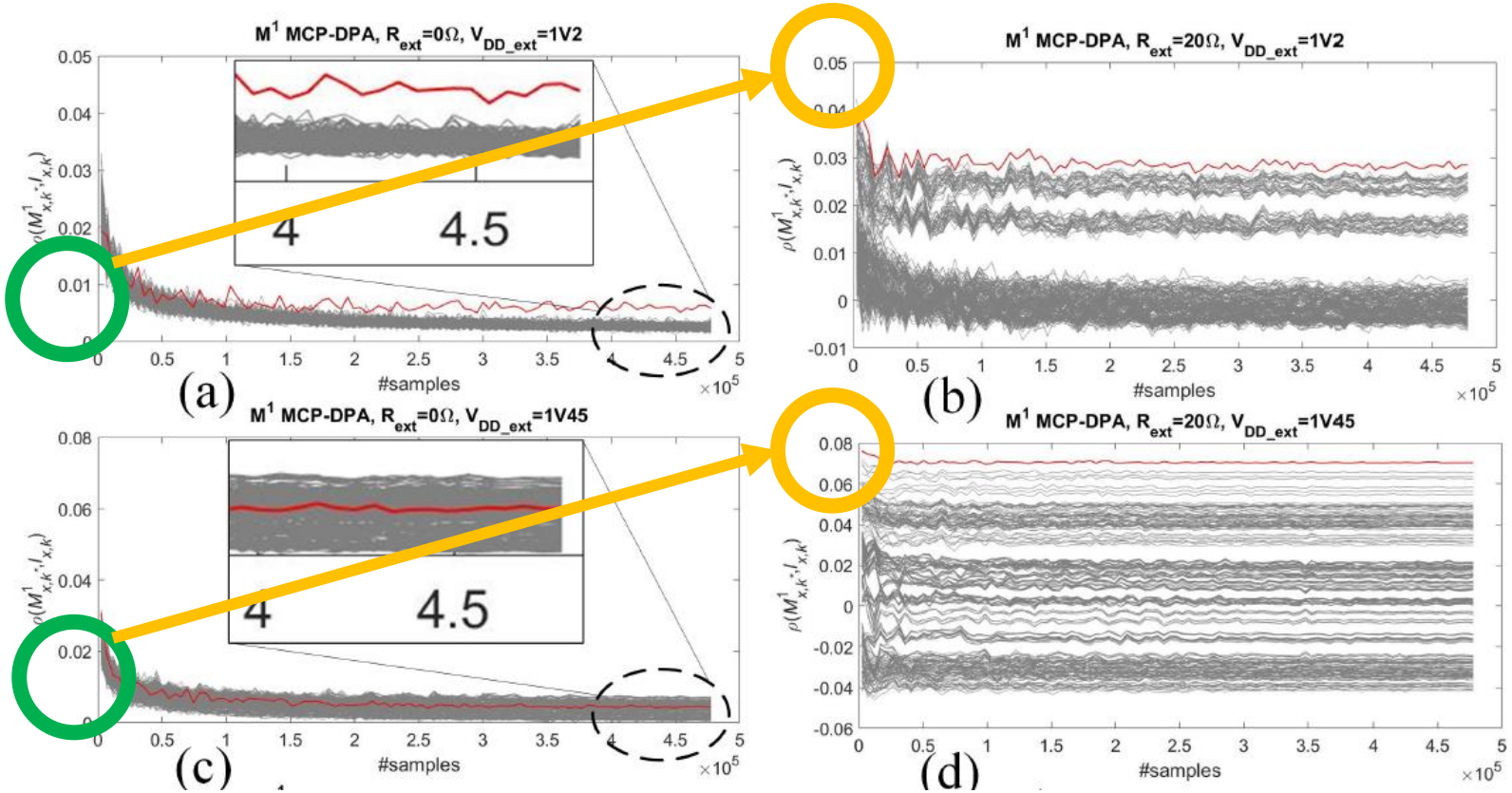
External

# Is the problem concrete?

* DoM AES (Hannes et-al. [GNK17])
* Hardware – FPGA (Spartan 6) scenario
  - Exploitation (MCP-DPA):

$$\tilde{k} = \arg\max_{k*} \quad \hat{\rho}(\hat{M}^d_{x,k*}, \ \left(l^t{}_{x,k}\right)^d)$$

  - Inherent leakage→ ~x10 amplification …
  - No initial leakage → ~x10 amplification and generation



# Is the problem concrete?



* DoM AES (Hannes et-al. [GNK17])
* Hardware – FPGA (Spartan 6) scenario

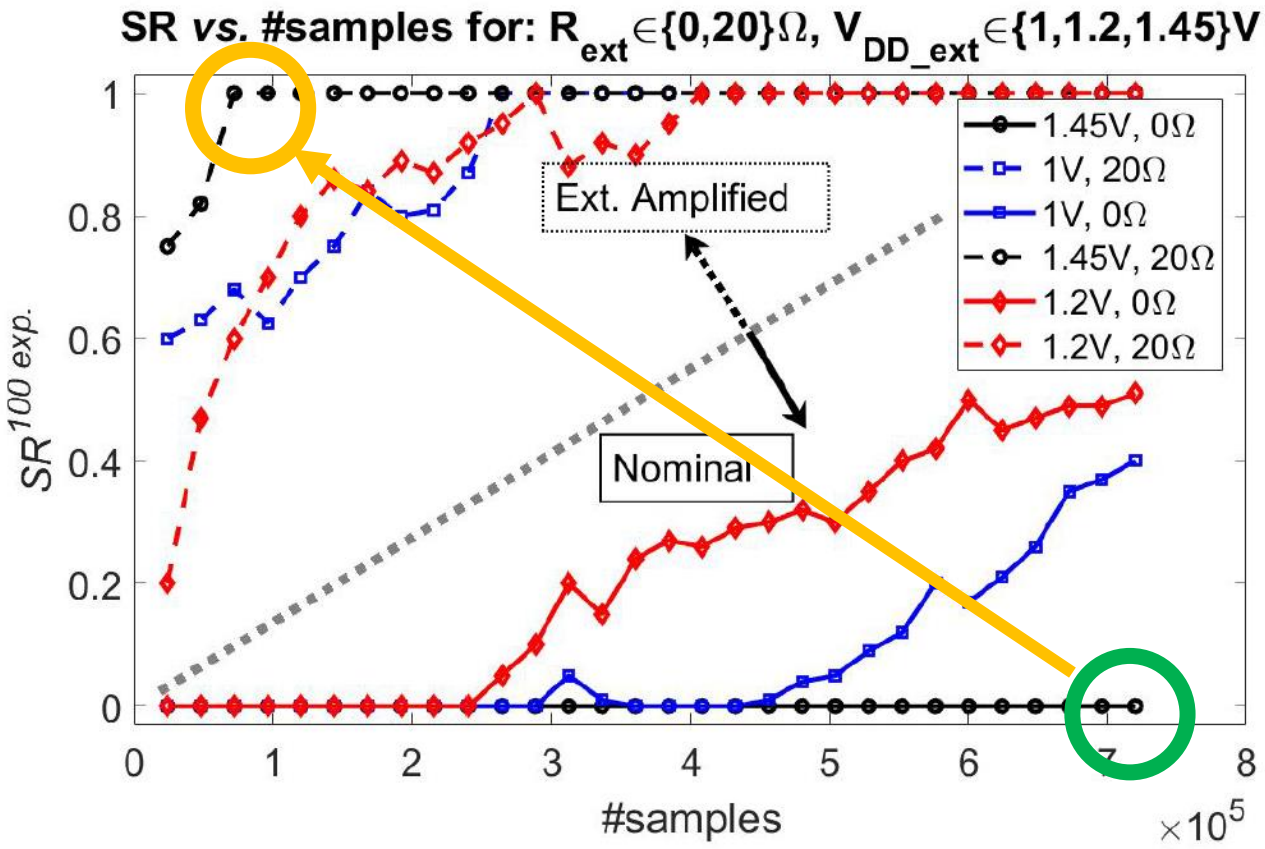
Moving on from a:

- "detection" based approach (T-test)

$$T_{value} = (\mu_{Set_0} - \mu_{Set_1}) \Big/ \sqrt{{\sigma_{Set_0}}^2/|Set_0| + {\sigma_{Set_1}}^2/|Set_1|}.$$

- to actual exploitation (MCP-DPA):

$$\tilde{k} = \arg\max_{k*} \quad \hat{\rho}(\hat{M}^d_{x,k*}, \ (l^t{}_{x,k})^d)$$

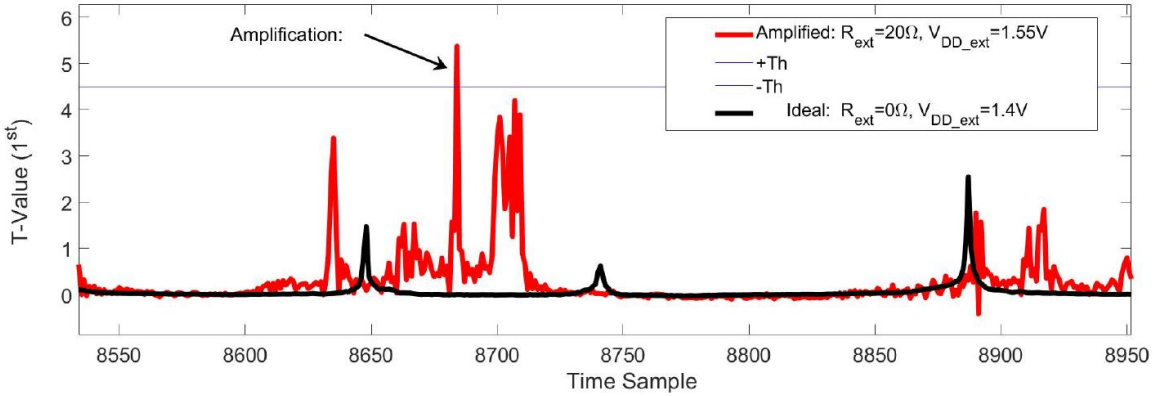


# Is the problem concrete?

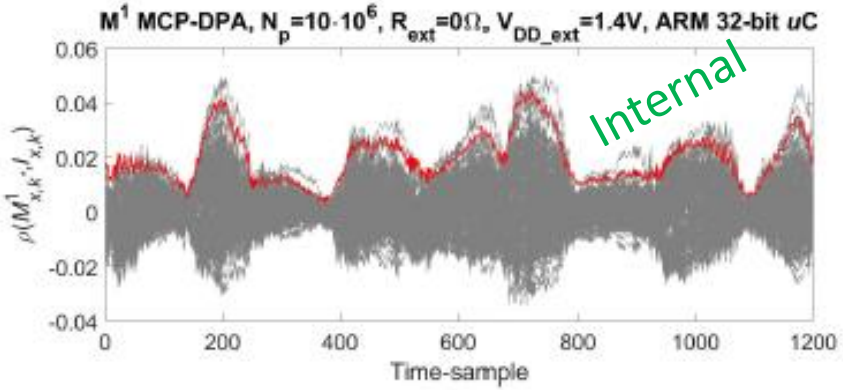
* Bitslice Barthe et-al. [BDF+17]
* Software – uC scenario (ARM32 in ATMEGA)

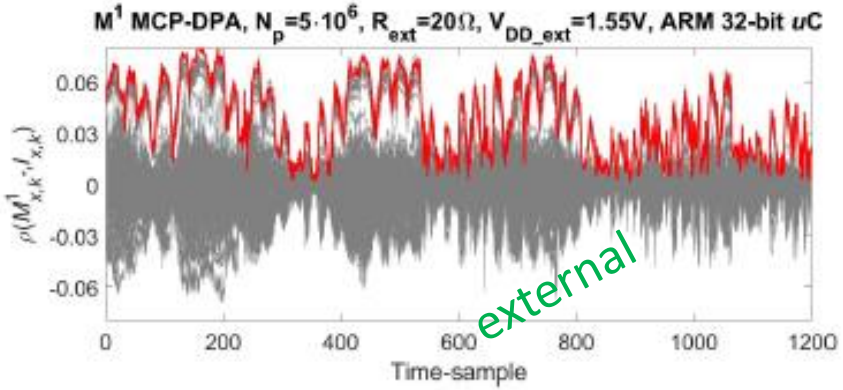
SW - Similar results

- Quite alarming amplification.
- *From externally !*




No. Traces for attack/profiling = 700k/10M



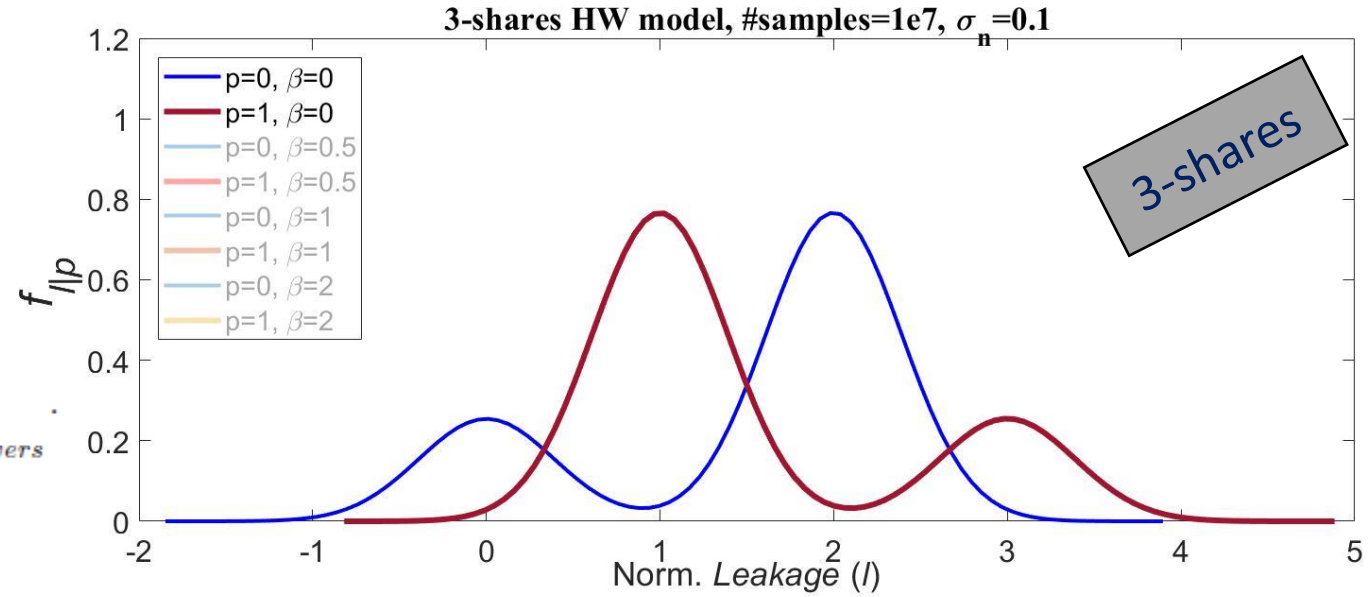



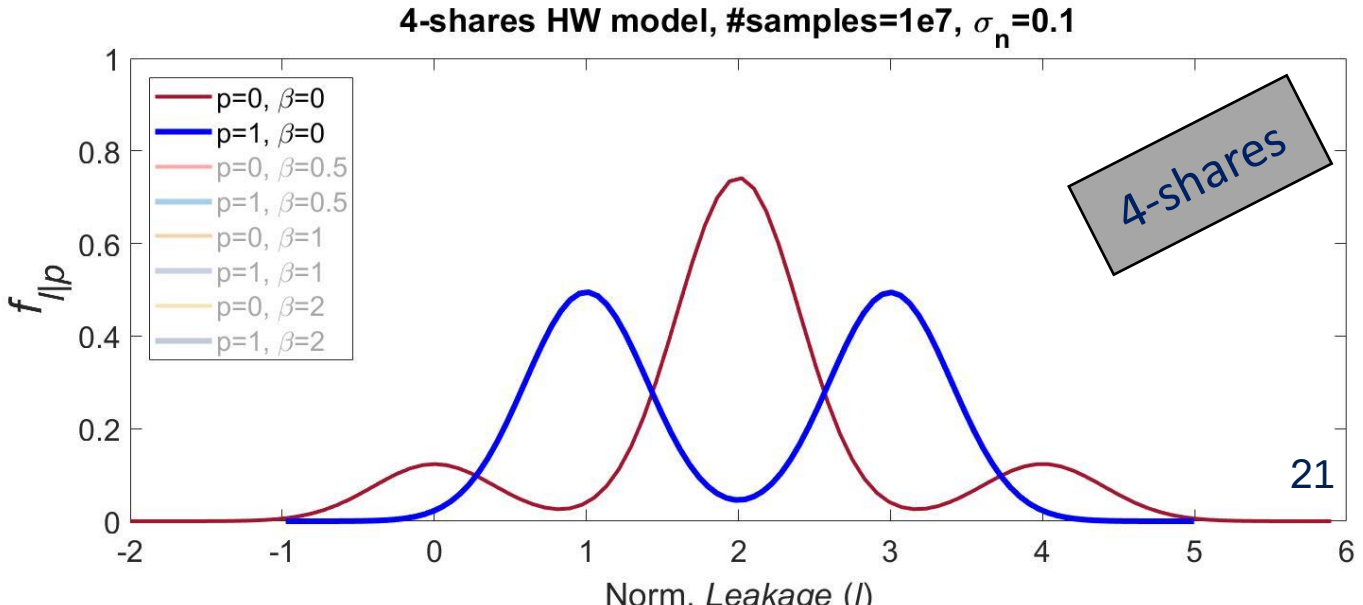
# Open Challenge - Scaling (*d*)



- How would it scale ?
  - Taking only some dominant factors

$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} - \frac{R_{\text{ext}}}{V_{DD\_ext}} \cdot \underbrace{\sum_i \sum_j I_j I'_i + \ldots}_{1^{st}\ order} \underbrace{\quad}_{higher\_powers} .$$



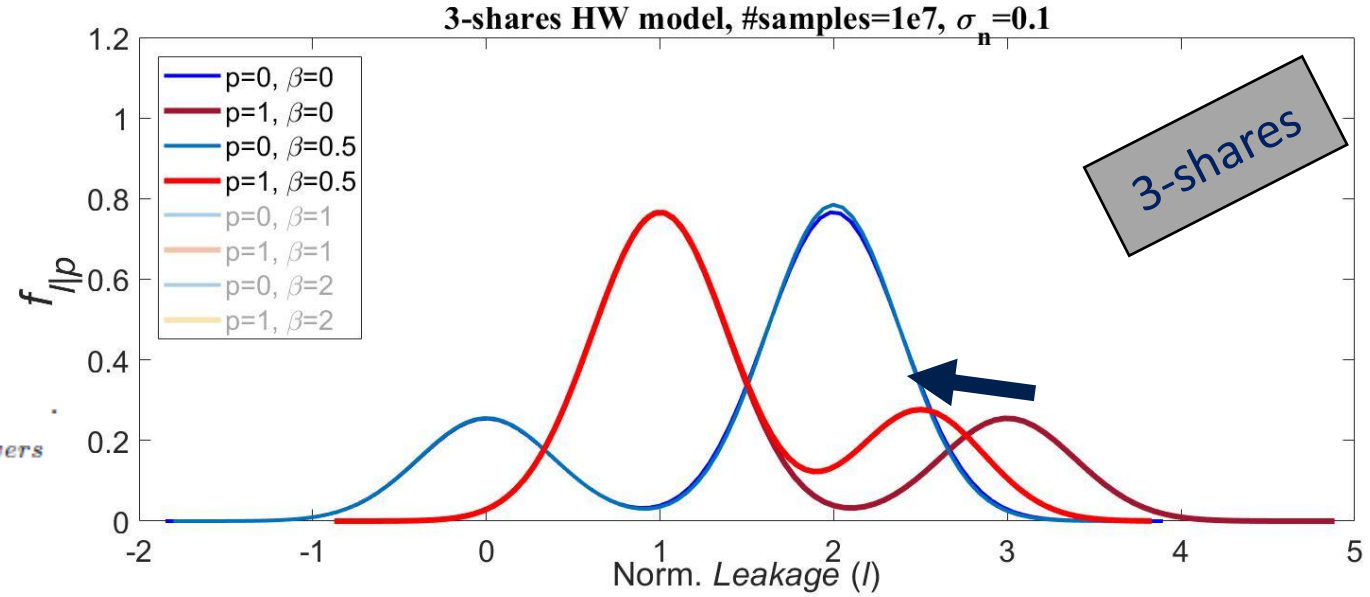



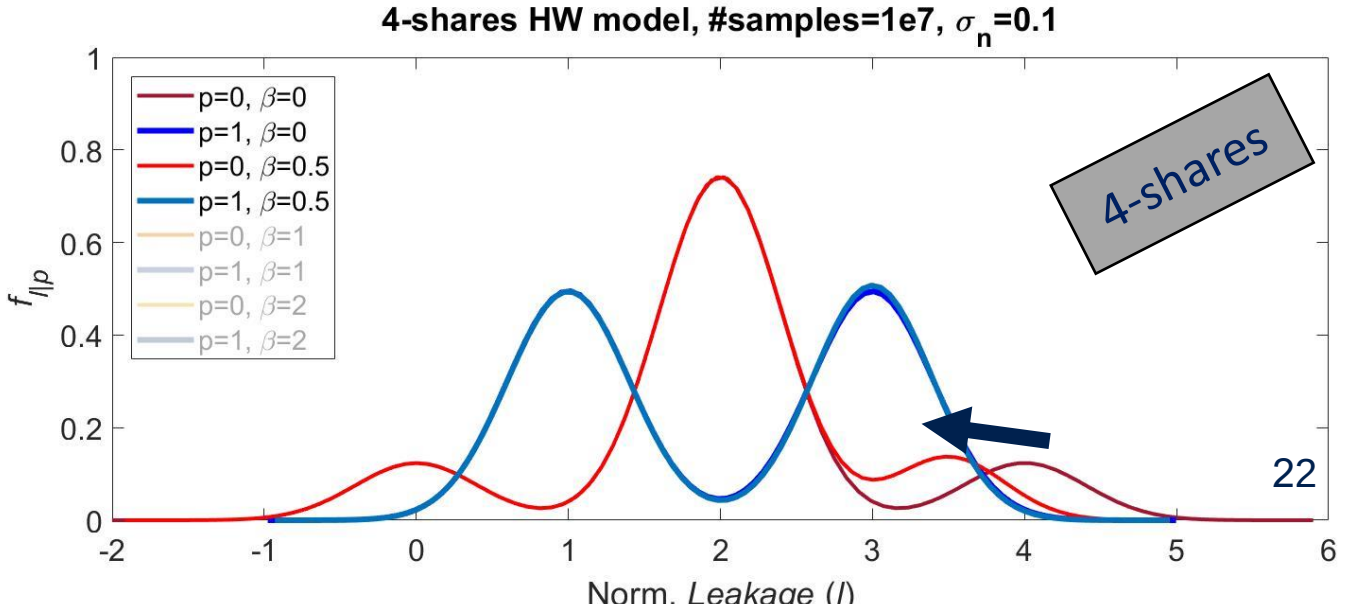
# Open Challenge - Scaling (*d*)



- How would it scale ?
  - Taking only some dominant factors

$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} - \frac{R_{\text{ext}}}{V_{DD\_ext}} \cdot \underbrace{\sum_i \sum_j I_j I'_i}_{1^{st}\ order} + \ldots \underbrace{\quad}_{higher\_powers} .$$



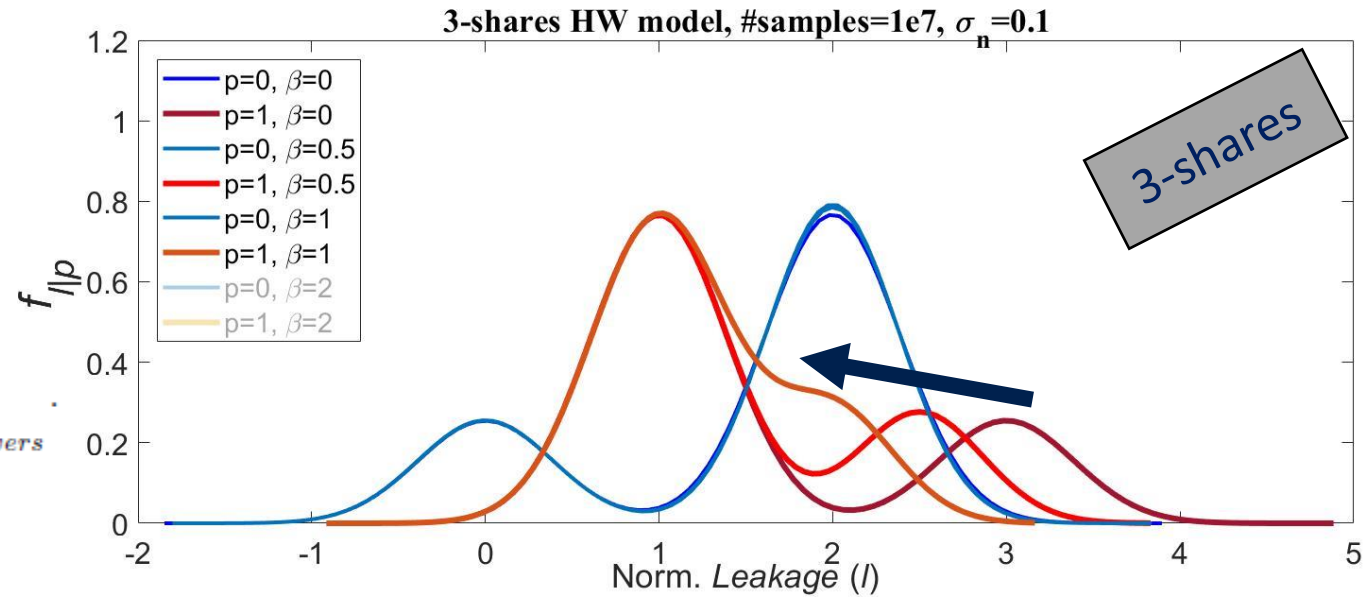



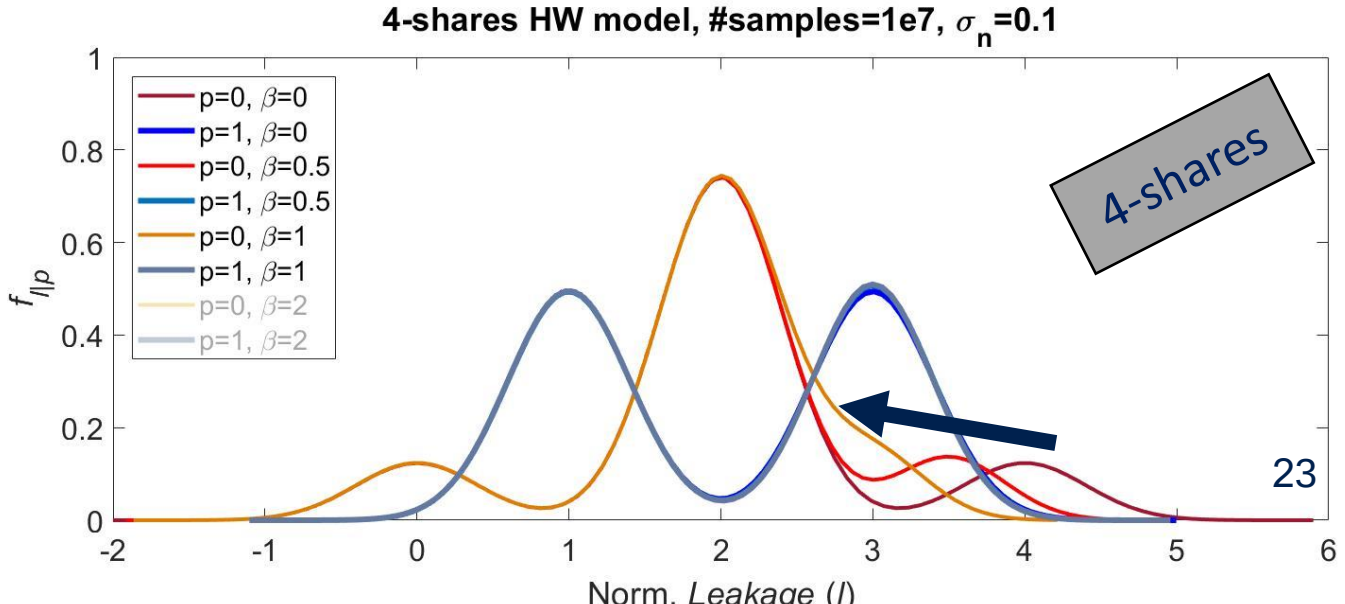
# Open Challenge - Scaling (*d*)



- How would it scale ?
  - Taking only some dominant factors

$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} - \frac{R_{\text{ext}}}{V_{DD\_ext}} \cdot \underbrace{\sum_i \sum_j I_j I'_i}_{1^{st}\ order} + \ldots \underbrace{\quad}_{higher\_powers} .$$



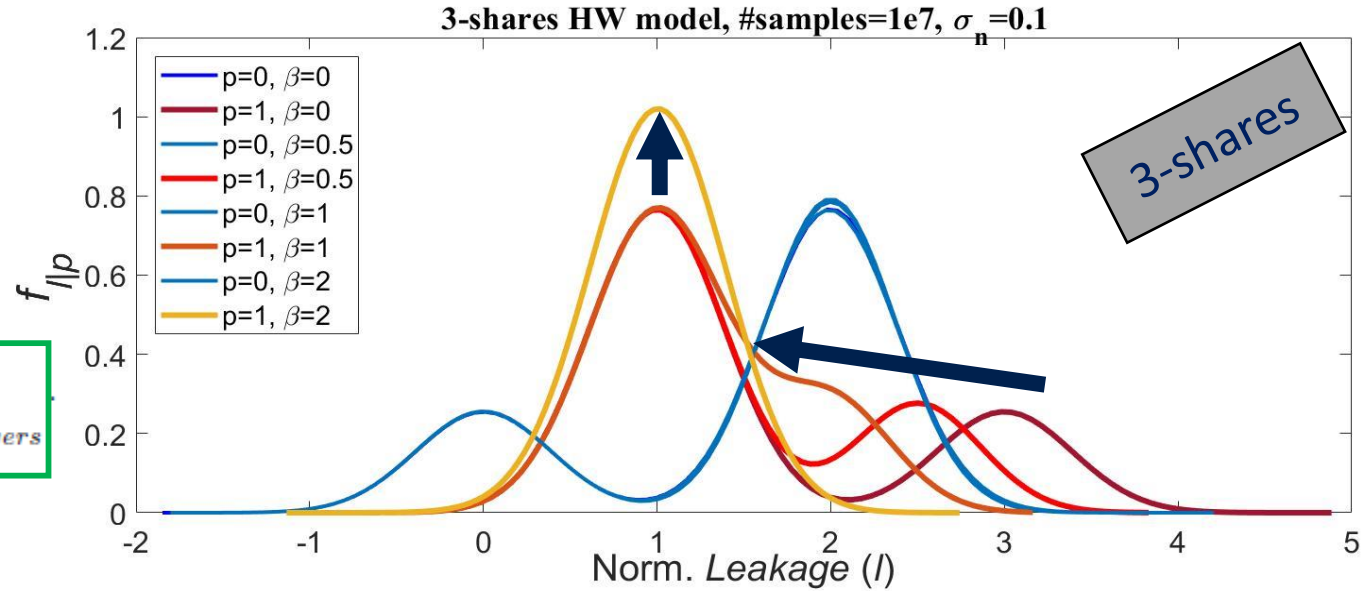
# Open Challenge - Scaling (*d*)

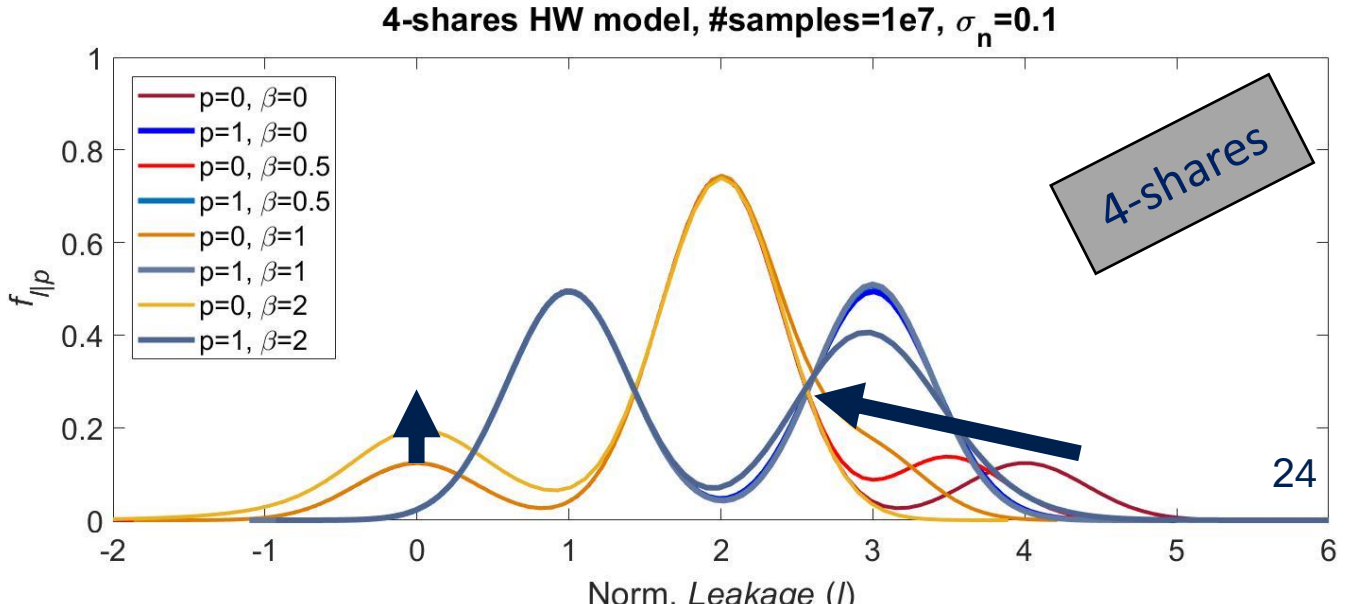


- How would it scale ?
  - Taking only some dominant factors

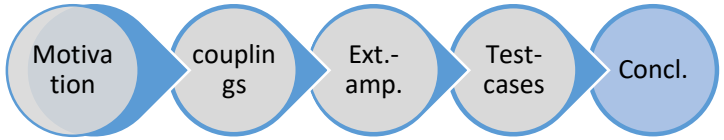
$$I'_{\text{supply}} \approx \underbrace{\sum_i I_i}_{2^{nd}-order} - \frac{R_{\text{ext}}}{V_{DD\_ext}} \cdot \underbrace{\sum_i \sum_j I_j I'_i}_{1^{st}\ order} + \ldots \underbrace{higher\_powers}$$

- In practice, highly design dependent.
- The question is the respective informativeness of these lower orders moments?
- or how concrete is their amplification…



# Conclusions




Setup manipulations (or externally amplifies couplings)

- Can have a significant impact on the security order, not only on the noise level.

We demonstrate that for off-the-shelf devices it actually happens

Open questions:

- How would the security order reduction *scale* with *d* ?
- How is it possible to build realistic "*Extended-Probes*"/ realistic models for such adversaries ?
- Would we see the same results for ASICs / specialized devices (not off-the-shelf)

Existing design-phase tools will not do .. (e.g. *MaskVerif*/ ELMO - *logical tools*)

# Thank you for your attention!