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...

\[
\begin{align*}
x &= x_1 \oplus x_2 \oplus \ldots \oplus x_d \\
L &= W(x_1) + W(x_2) + N_0
\end{align*}
\]

\[
\begin{align*}
\mu_1 &= \mu_2 \\
\sigma_1 &\neq \sigma_2
\end{align*}
\]
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)
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

- 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

In theory

In practice: not so linear and not so nice...
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):

\[ L = I_{S1} + I_{S2} \]

\[ L' = \alpha_1 I_{S1} + \alpha_2 I_{S2} - \beta (I_{S1} \cdot I_{S2}) \]
How to \textit{externally} amplify them

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

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

\[ \alpha_i = \frac{1}{\left(1 + \frac{2R_{ext}}{R_{on,i}}\right)} \approx 1 \]

\[ \beta = \frac{R_{ext}}{V_{DD,ext}} \left[ \frac{R_{on1}}{2R_{ext} + R_{on1}} + \frac{R_{on2}}{2R_{ext} + R_{on2}} \right] \approx \frac{2R_{ext}}{V_{DD,ext}} \]

- But, lowering $V_{DD}$ has a \textit{negative effect}...
  - Reduces the signal (typically, SNR $\downarrow$)
  - 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

\[ I' = \alpha_1 I_{sh1} + \alpha_2 I_{sh2} - \beta (I_{sh1} \cdot I_{sh2}) \]

\[ \alpha_i = \frac{1}{1 + \frac{2R_{ext}}{R_{on,i}}} \approx 1 \]

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

\[ \approx \frac{2R_{ext}}{V_{DD,ext}} \]

- 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 \textit{externally} amplify them

\[ I' = \alpha_1 I_{sh1} + \alpha_2 I_{sh2} - \beta (I_{sh1} \cdot I_{sh2}) \]
\[ \beta \approx \frac{2R_{\text{ext}}}{V_{DD,\text{ext}}} \]

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

- So, increasing \( R_{\text{ext}} \) then,
  - Too much- the device will not work
  - We might need to simult. Increase \( V_{DD} \)
  - \textit{With} \( R_{\text{ext}} \uparrow \text{ the noise increase} \)

- No trivial answer to what is the worst-case scenario,
  - Depends on the device, the noise, power regulator (if any).
  - The \textit{exploration space for a certification lab} is huge ...
The simplified model can be generalized ($d)$:

\[ I'_{\text{supply}} \approx \sum_i I_i - \frac{R_{\text{ext}}}{V_{\text{DD\_ext}}} \sum_j \sum_i I_i I_j' + \ldots \]

• But,
  • Expected: leakage at all stat.-moments/powers (solve MAXWELL ...) $\Rightarrow$ modeling is hard

• So our goals were:
  • To examine whether 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

\[
T_{value} = \frac{\mu_{Set_0} - \mu_{Set_1}}{\sqrt{\frac{\sigma_{Set_0}^2}{|Set_0|} + \frac{\sigma_{Set_1}^2}{|Set_1|}}}
\]

- to actual exploitation (MCP-DPA):
  \[
  \tilde{k} = \arg \max_{k*} \hat{\rho}(\hat{M}^d_{x,k*}, (l^t_{x,k})^d)
  \]

- 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)

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

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

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

- HW – Sbox-parallel design

- SW - serial → nicer to interpret ...

  - Conceptually SW will be more sensitive due to a shared power-grid
Is the problem concrete?

Software implementation ($\mu$C) – ARM32 bit (ATMEGA)

Model/Simulation

Measurement ($\mu$C)

<table>
<thead>
<tr>
<th>Ideal:</th>
<th>MODEL (simulated single bit distributions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I_{\text{supply}} = I_1 + I_2$</td>
<td>Simulated leakage dist. $\beta \neq 0, \beta \neq 0.4$</td>
</tr>
</tbody>
</table>

(a)

<table>
<thead>
<tr>
<th>Ideal:</th>
<th>Measurement (ARM32)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$I_{\text{supply}} = I_1 + I_2$</td>
<td>Simulated leakage dist. $\beta \neq 0, \beta \neq 0.4$</td>
</tr>
</tbody>
</table>

(a)

Test-cases

Motivation

Ext.-amp.

Concl.

1ohm

1.4 | 1.2V

Figure 2: $f(I_{\text{simul}}|s)$: (a) $\beta = 0$ (b) $\beta = 0.5$

Figure 8: $f(I|s)$, 1 $\cdot$ 10$^6$ traces: (a) $R_{\text{ext}} = 0 \Omega$ (b) $R_{\text{ext}} = 20 \Omega$
Is the problem concrete?

Software implementation (uC) – ARM32 bit (ATMEGA)

Model/Simulation

Measurement (uC)

![Diagram](attachment:image.png)

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

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

Is the problem concrete?

Software implementation (uC) – ARM32 bit (ATMEGA)

Model/Simulation

Measurement (uC)

![Diagram](attachment:image.png)

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

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

\[ T_{value} = \frac{(\mu_{Set_0} - \mu_{Set_1})}{\sqrt{\frac{\sigma_{Set_0}^2}{|Set_0|} + \sigma_{Set_1}^2/|Set_1|}}. \]
Is the problem concrete?

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

• Exploitation (MCP-DPA):

• Inherent leakage $\rightarrow$ $\sim x10$ amplification ...

• No initial leakage $\rightarrow$ $\sim x10$ 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)

\[ T_{value} = \left( \frac{\mu_{set_0} - \mu_{set_1}}{\sqrt{\sigma_{set_0}^2/|Set_0| + \sigma_{set_1}^2/|Set_1|}} \right) \]

- to actual exploitation (MCP-DPA):

\[ \tilde{k} = \arg \max_{k^*} \hat{\rho}(\hat{M}_{x,k^*}^d, (l_{x,k}^t)^d) \]
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

\[ I'_{\text{supply}} \approx \sum_{i} I_i - \frac{P_{\text{ext}}}{V_{DD_{\text{ext}}}} \cdot \sum_{i} \sum_{j} I_j I_i' \cdot \text{higher\_powers} \]
Open Challenge - Scaling ($d$)

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

$$I'_{\text{supply}} \approx \sum_i I_i \cdot \frac{R_{\text{ext}}}{V_{\text{DD,ext}}} + \sum_i \sum_j I_j I'_i + \ldots$$

- 3-shares HW model, #samples=1e7, $\sigma_n = 0.1$
- 4-shares HW model, #samples=1e7, $\sigma_n = 0.1$
Open Challenge - Scaling ($d$)

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

$$I'_{\text{supply}} \approx \sum_{i} I_i - \frac{R_{\text{ext}}}{V_{DD_{\text{ext}}}} \sum_{i} \sum_{j} I_j I_i' + \ldots$$

3-shares HW model, $\#\text{samples}=1e7$, $\sigma_n=0.1$

4-shares HW model, $\#\text{samples}=1e7$, $\sigma_n=0.1$
Open Challenge - Scaling \((d)\)

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

\[
I'_{\text{supply}} \approx \sum_i I_i - \frac{R_{\text{ext}}}{V_{DD_{\text{ext}}}} \sum_i \sum_j I_i V_{ij} + \ldots
\]

- 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!