RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

On the success rate of simple side-channel attacks against masking with unlimited attack traces

Aymeric Hiltenbrand, Julien Eynard, Romain Poussier

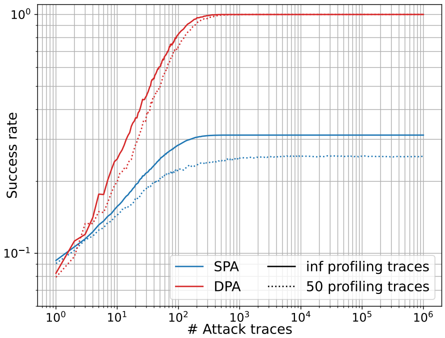
Hotline

Context

DPA scenario
Targeted intermediate value depends on VARYING variables
eg: $Sbox[k \oplus m]\ldots$

SPA scenario
Targeted intermediate value depends on FIXED variables
eg: $KeySchedule(K_0)$, $Kyber$'s $\mathtt{r}\ldots$

How about masking ?

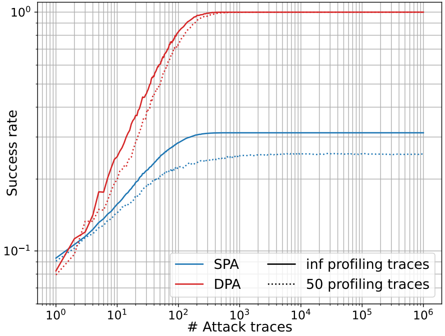


Context: Why is it interesting

DPA scenario
Targeted intermediate value depends on **known** and VARYING variables
eg: $Sbox[k \oplus m]$...

SPA scenario
Targeted intermediate value depends on unknown or FIXED variables
eg: $KeySchedule(K_0)$, *Kyber*'s `r`...

Masking: unknown varying $\implies$ SPA
Does the variability of masking change the behavior of SPA ?



Context: How do we study it: SR_∞

Masking scheme

- Unmasked leakage: $L(V) = \varphi(V) + \mathcal{N}(0, \sigma^2_{noise})$
- Boolean masking: $v = \bigoplus^{t} s_i$
- Arithmetic masking: $v = \sum^{t} s_i \quad mod\ n$

Leakage function φ

- Hamming weight leakage: $\varphi(x) = \sum^{n_{bits}} x_i$
- Linear leakage: $\varphi(x) = \sum^{n_{bits}} a_i x_i$

Profiling

- $\mathcal{N}_p \to \infty$
- "Imperfect" profiling

Perfect profiling: Hamming weight leakage $\varphi(x) = \sum_{i=1}^{n_{bits}} x_i$

Unprotected

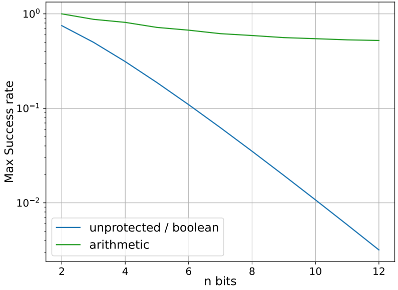
$$SR_\infty = \frac{n_{bits} + 1}{2^{n_{bits}}}$$

Boolean masking

Same SR_∞ as unprotected, for any number of shares (Proved)

Arithmetic masking

- More complex case because of carry propagation
- Seems to converge to 0.5
- With 3 shares, $SR_\infty = 1$ up to 12 bits



Hamming weight leakage: Boolean vs arithmetic masking

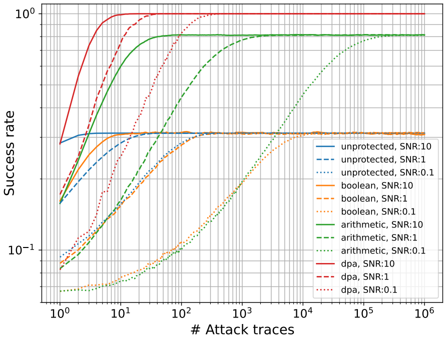
v	sharing 1	sharing 2	sharing 3	sharing 4
(00): HW=0	(00,00): HW=**(0,0)**	(01,01): HW=(1,1)	(10,10): HW=(1,1)	(11,11): HW=(2,2)
(01): HW=1	(00,01): HW=**(0,1)**	(01,00): HW=**(1,0)**	(10,11): HW=**(1,2)**	(11,10): HW=**(2,1)**
(10): HW=1	(00,10): HW=**(0,1)**	(01,11): HW=**(1,2)**	(10,00): HW=**(1,0)**	(11,01): HW=**(2,1)**
(11): HW=2	(00,11): HW=(0,2)	(01,10): HW=(1,1)	(10,01): HW=(1,1)	(11,00): HW=**(2,0)**

Table: **Boolean sharings** of a 2-bit value v, with their Hamming weight leakages. The first column corresponds to v, and the others show the possible sharings.

v	sharing 1	sharing 2	sharing 3	sharing 4
(00): HW=0	(00,00): HW=**(0,0)**	(01,11): HW=(1,2)	(10,10): HW=(1,1)	(11,01): HW=(2,1)
(01): HW=1	(00,01): HW=(0,1)	(01,00): HW=**(1,0)**	(10,11): HW=**(1,2)**	(11,10): HW=(2,1)
(10): HW=1	(00,10): HW=(0,1)	(01,01): HW=(1,1)	(10,00): HW=(1,0)	(11,11): HW=**(2,2)**
(11): HW=2	(00,11): HW=(0,2)	(01,10): HW=(1,1)	(10,01): HW=(1,1)	(11,00): HW=**(2,0)**

Table: **Arithmetic sharings** of a 2-bit value v, with their Hamming weight leakages. The first column corresponds to v, and the others show the possible sharings.

Perfect profiling: simulations for Hamming weight leakages



- SR_∞ is higher for arithmetic masking than for boolean an unmasked
- MI higher for boolean masking than for arithmetic masking

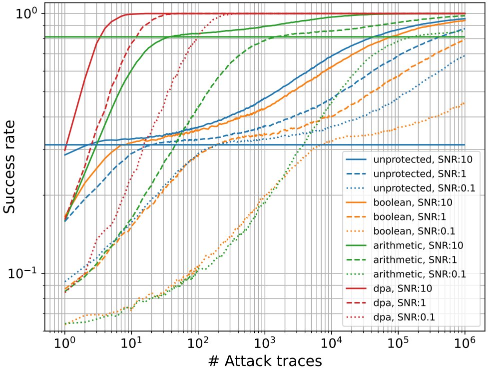
Perfect profiling: linear leakage function: $\varphi(x) = \sum_{i=1}^{n_{bits}} a_i x_i$

Theoretically, for all: $SR_\infty = 1$

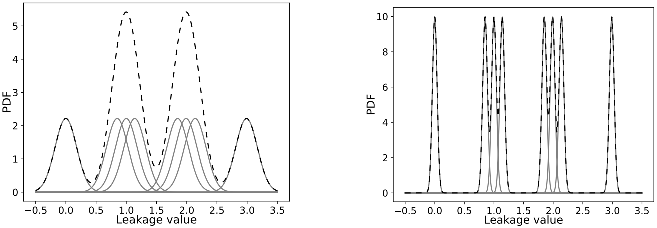
Choice for the a_i's:
$a_i \xleftarrow{\$} \mathcal{N}(1, \sigma^2_{leakage})$ with $\sigma^2_{leakage} = 10^{-4}$

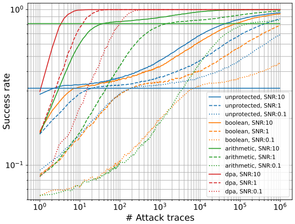
Simulation:

- Two convergence regimes identified
- Bend at SR_∞ for Hamming Weight



Linear leakage function: Two convergence regimes





Conditional PDFs (grey) and PDF mixture (black, dashed) for linear leakage in high noise (left) and low noise (right).

- Small number of traces (left): Distinction between values of **different** *HW*
- Large number of traces (right): Distinction between **same** *HW* values.

Linear leakage function: Limitations of the *SNR*

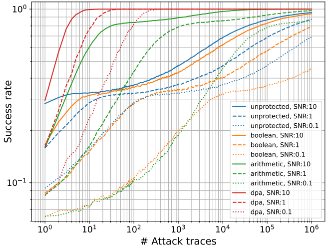


Figure: $\sigma^2_{leakage} = 10^{-4}$

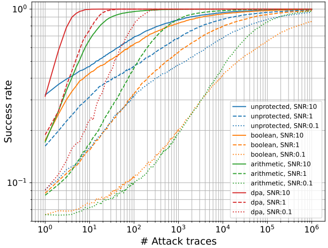


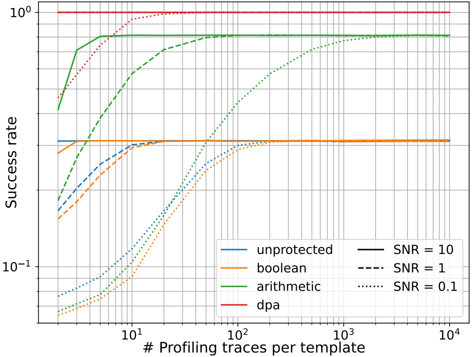
Figure: $\sigma^2_{leakage} = 10^{-2}$

Expression of the *SNR*

$$SNR = \frac{n_{bits}\left(\frac{1}{2} + \sigma^2_{leakage}\right)}{2 \cdot \sigma^2_{noise}}$$

- $\sigma^2_{leakage}$ really has an impact on the SPA convergence, but has almost none on the *SNR* value.

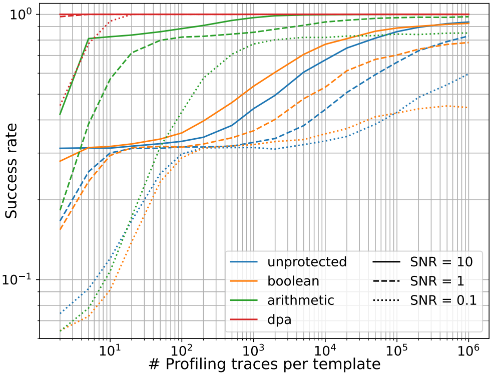
Imperfect profiling: Hamming weight leakage



- Boolean masking impacted the same by imperfect profiling as unprotected
- Arithmetic masking is the most impacted

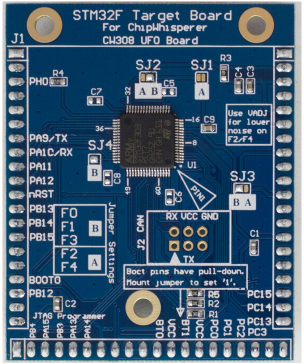
Imperfect profiling: Linear leakage

- SR_∞ can be higher for arithmetic masked implementation than for unmasked
- In the second regime, Boolean masking has higher than unprotected (yet unexplained)



Practical experiments: setup

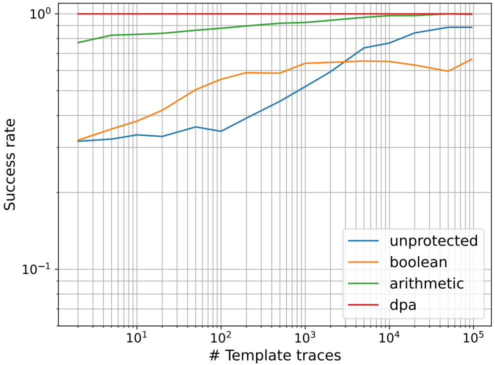
- **Target:** STM32F415 32-bits ARM cortex M4 microcontroller @7.3MHz
- **Acquisition:** ChipWhisperer CW1200 with CW308 UFO Board @29.7MSa/s
- *SNR* ≈ 6
- $\sigma^2_{leakage} \approx 3 \cdot 10^{-4}$



source: rtfm.newae.com

Practical experiments: results

- The arithmetic masking helps the attacker in a imperfect profiling scenario
- The boolean masking can make the attack more successful



Conclusion, discussion

✅ Verified in real-world application

Masking scheme

Impacts the SR_∞ value in the case of a HW leakage (Arithmetic has higher SR_∞)

Leakage function

Impacts the SR_∞ value and SR convergence rate (depends on $\sigma^2_{leakage}$).

Number of profiling traces

Masked implementations can have a higher SR_∞ than unmasked ones.

Even though masking can make an attack reaching a higher SR_∞ , masking should still be used !

Thank You.