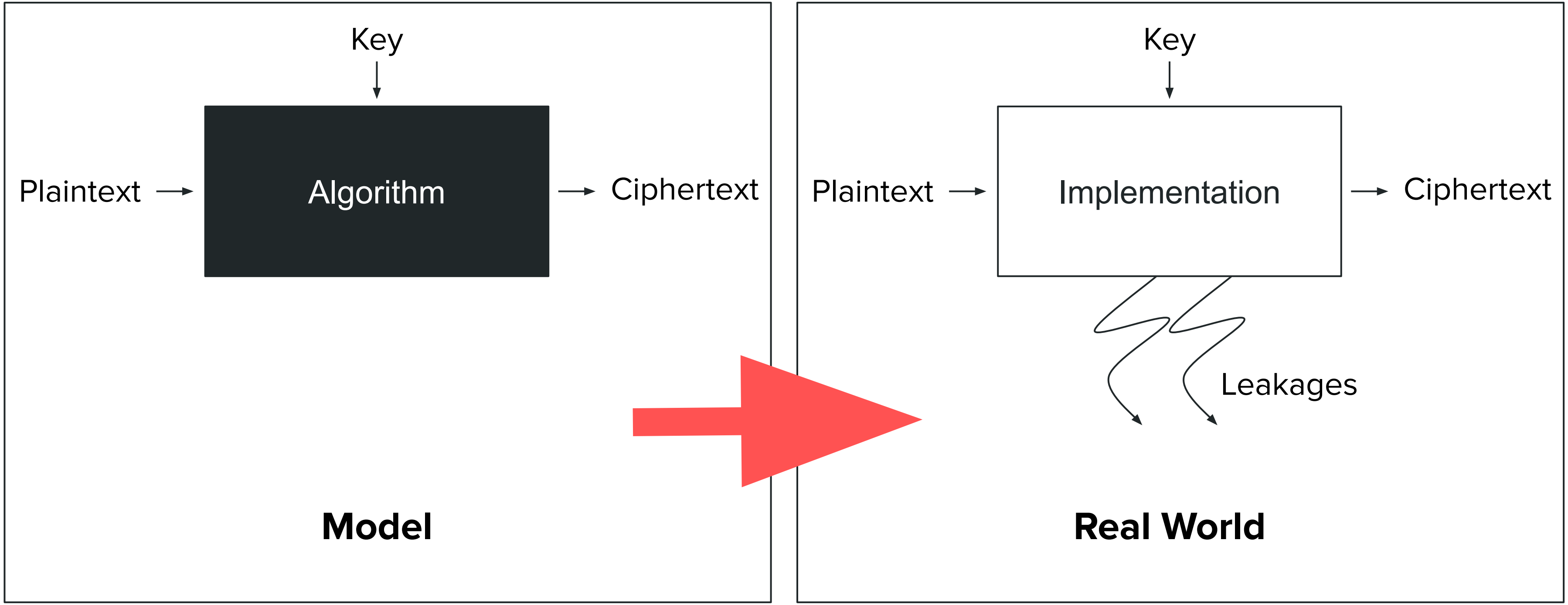
Redundant Code-based Masking Revisited

Nicolas Costes, Martijn Stam

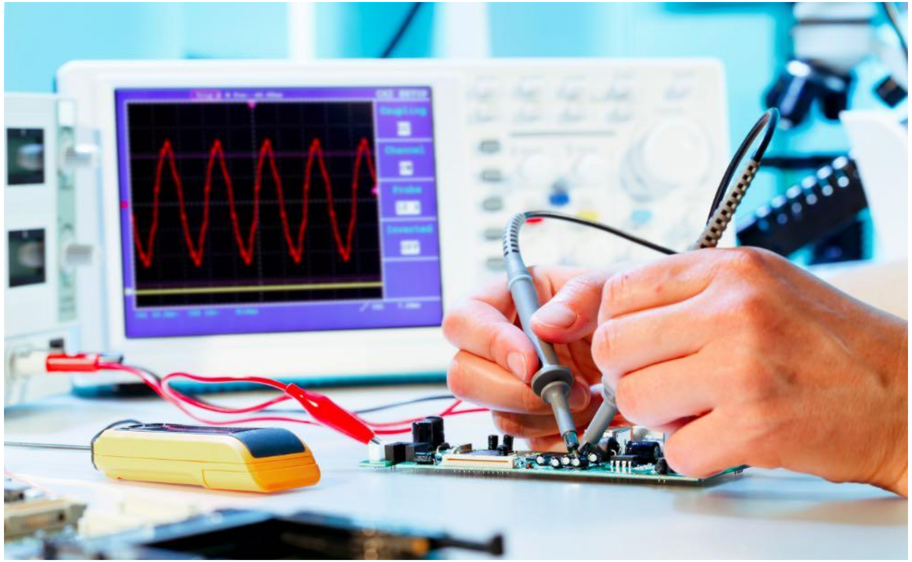
Simula
UiB

Context

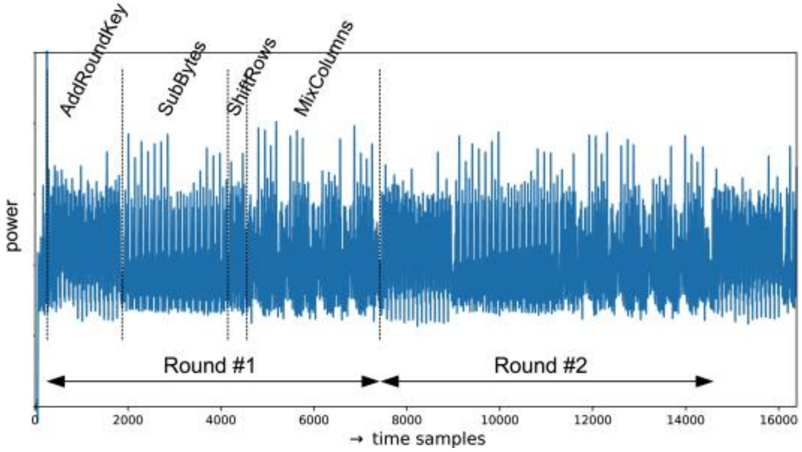
Side-Channel Attacks



Power Analysis Attacks



picture credits: Rambus



picture credits: [DD20]

Popular Countermeasures

Shuffling

Random Delay

Electronic Noise

Masking

➔ **Degradation of the Signal-to-Noise Ratio**

Popular Countermeasures

Shuffling

Random Delay

Electronic Noise

Masking

➜ **Degradation of the Signal-to-Noise Ratio**

Masking

Main countermeasure against SCA

Pick d, the security order, generate d random variables, encode your secret v into $d+1$ shares c_i

Then compute your algorithm without recombining the shares

Main encoding used in software: **Boolean Masking**

$$v = \sum_{i=1}^{d+1} c_i$$

Polynomial Masking

Introduced by Prouff and Roche [PR11]

(d, n) Shamir secret sharing

Evaluate $v + \sum_{i=1}^{d} r_i \cdot X^i$ on the set of points $\mathcal{S}$

Secret value to mask

Fresh Random Coefficients

Public parameter
Set of n points in $\mathbb{F}$

Polynomial Masking

Introduced by Prouff and Roche [PR11]

(d, n) Shamir secret sharing

Evaluate $v + \sum_{i=1}^{d} r_i \cdot X^i$ on the set of points $\mathcal{S}$

Main claims:

- if $n = d + 1$, leaks less than Boolean Masking for low SNR
- if $n > d + 1$, redundant masking, extra shares can defeat glitches

Questions

Are redundant leakages beneficial to an attacker?

How does the choice of $\mathcal{S}$ influences the leakage?

Redundant Leakages

Leakage Model

Noisy Hamming Weight model

For all shares c_i of a masked variable the adversary get:

$$\boxed{\mathrm{Hw}(c_i) + \mathcal{N}(0, \sigma^2)}$$

Widely used [RP12, GM11, BFG15] and convenient for studying masking

In our case: single first round SBOX output, AES-128

CMP18 (1)

Addresses how redundant polynomial masking leaks

Uses MLE as distinguisher

"observing strictly more than d + 1 shares will merely provide the attacker with more noise than information"

CMP18 (2)

MLE Distinguisher mistake

$$s(v, t) = \sum_{(c_2, \ldots, c_n)} \prod_{i=1}^{n} \mathcal{N}(t_i | \mathrm{Hw}(c_i), \sigma^2)$$

Score for each possible value of v based on the traces

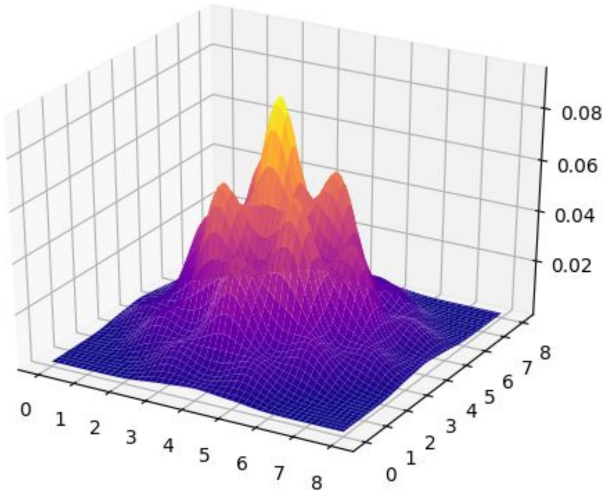
Sum over all possible values of all shares but one

pdf of a Gaussian of mean $\mathrm{Hw}(c_i)$ and variance σ^2 evaluated at t_i

CMP18 (2)

Distinguisher mistake

$$s(v, \boldsymbol{t}) = \sum_{(c_2, \ldots, c_n)} \prod_{i=1}^{n} \mathcal{N}\left(t_i | \mathrm{Hw}\left(\mathrm{c_i}\right), \sigma^2\right)$$



Problem: dimension mismatch

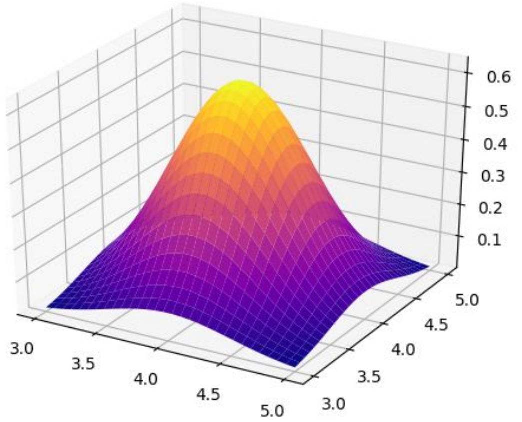
Example: degenerate case, $(d = 0, n = 2)$, repeating the secret

CMP18 (3)

Correct MLE formula:

$$s(v,t) = \sum_{r} \prod_{i=1}^{n} \mathcal{N}\left(t_i | \mathrm{Hw}\left(\mathrm{c}_i\right), \sigma^2\right)$$

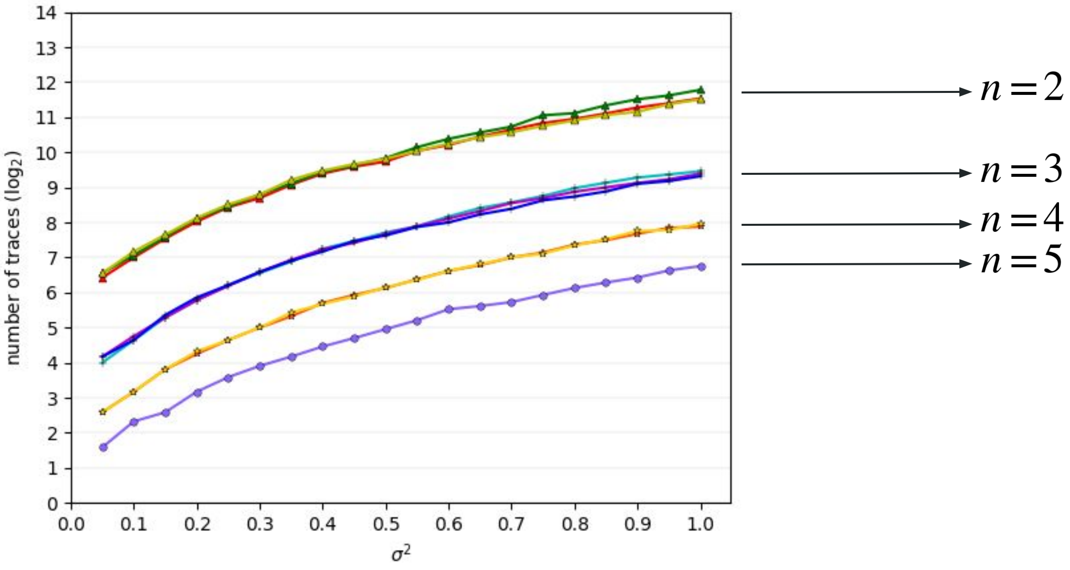
Sum over all values of **the random coefficients**



Back to our degenerate case, $(d=0, n=2)$, no problem

Results

Reusing the $\mathcal{S}$ from [CMP18], empirical experiments on security degradation for $n > d + 1$, targeting 90% success rate for $d = 1$

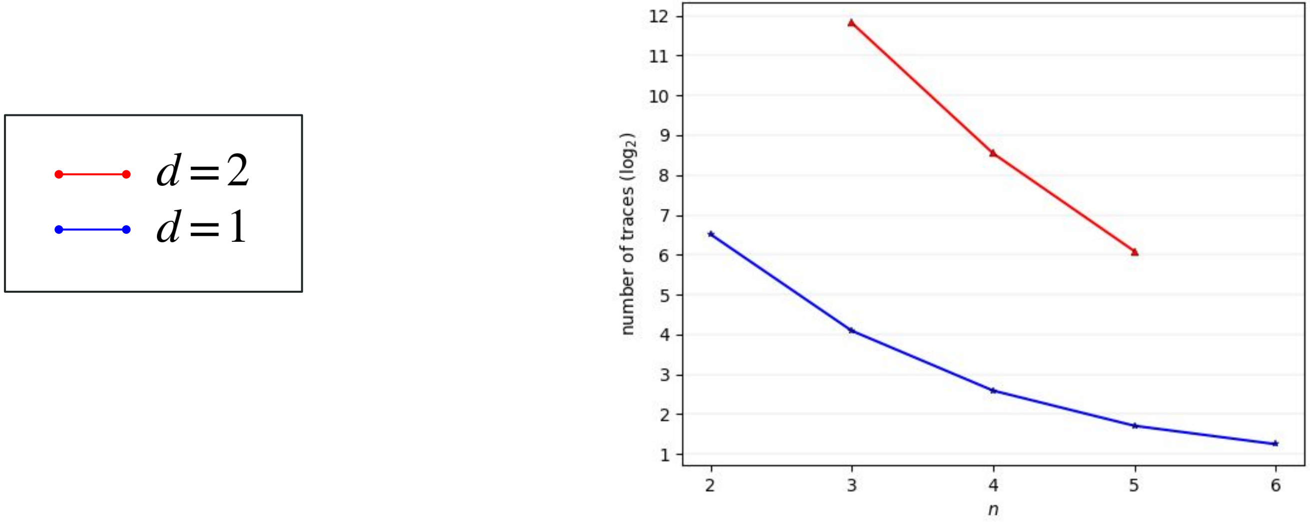


Clear security degradation

A Try at Quantifying

Low noise appears representative, for high noise see [CGC+21]

➡ approximate metric for hardness of attack against (d, n) polynomial masking



Investigating Points

Masking Equivalence

Definition: Two masking scheme are *equivalent* if the adversary can attack them with the same results

Are there some $\mathcal{S}$ leading to an equivalence to other masking?

Are there some $\mathcal{S}$ leading to more leaky shares?

Boolean or Polynomial?

Are there $\mathcal{S}$ where Polynomial masking is *equivalent* to Boolean masking?

➜ $\infty \in \mathcal{S}$ iff d odd and $\sum_{s \in \mathcal{S} \setminus \{\infty\}} s = 0$ if $d > 1$ and $\mathcal{S} = \{1, \infty\}$ if $d = 1$

example: $d = 2, n = 3, \mathcal{S} = \{a, b, a + b\}$

$$\boxed{\begin{aligned} c_1 &= r_1 \cdot a^2 + r_1 \cdot a + v \\ c_2 &= r_2 \cdot b^2 + r_2 \cdot b + v \\ c_3 &= r_1 \cdot a^2 + r_2 \cdot b^2 + r_1 \cdot a + r_2 \cdot b + v \end{aligned}}$$

Quasi-Boolean and Frobenius (1)

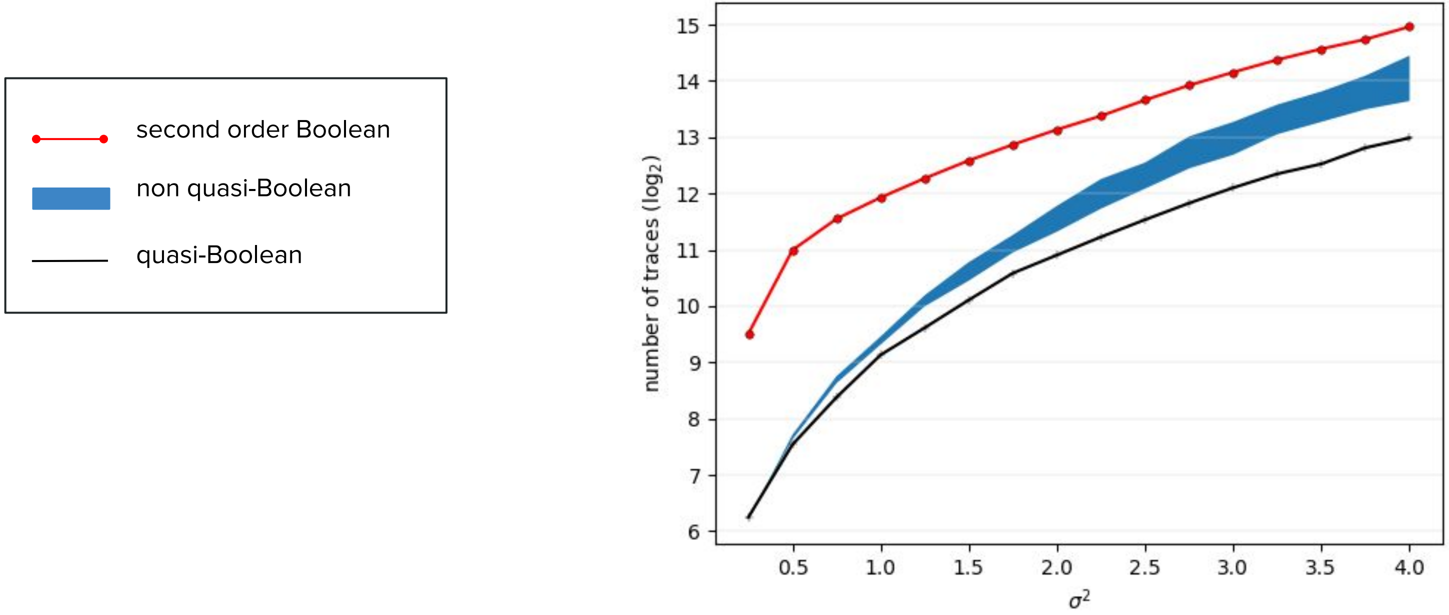
Concept: Redundancy may introduces non-unicity of reconstruction. In quasi-Boolean, alternate reconstruction by summing the shares.

Prouff and Roche [PR12] suggest to use $\mathcal{S}$ stable under the Frobenius automorphism with parameters $(d = 1, n = 3)$

There is a unique $\mathcal{S}$ matching this condition → quasi-Boolean

Quasi-Boolean and Frobenius (2)

Empirical investigation on the leakage profile of quasi-Boolean sets



Conclusion

Summary of results

Correction of [CMP18] → more redundant shares, less security

Formalization of the notion of *equivalent masking*

Investigation of the choice of $\mathcal{S}$ → Boolean equivalent sets, quasi-Boolean sets

Confirmation of our results with experiments in the HW model

References

[DD20]: François Durvaux and Marc Durvaux.SCA-Pitaya: A Practical and Affordable Side-Channel Attack Setup for Power Leakage--Based Evaluations. ACM 2020

[PR11]: Emmanuel Prouff and Thomas Roche. Higher-order glitches free implementation of the AES using secure multi-party computation protocols. CHES 2011

[RP12]: Thomas Roche and Emmanuel Prouff. Higher-order glitch free implementation of the AES using secure multi-party computation protocols - extended version. Journal of Cryptographic Engineering 2012.

[GM11]: Louis Goubin and Ange Martinelli. Protecting AES with Shamir’s secret sharing scheme. CHES 2011

[BFG15]: Josep Balasch, Sebastian Faust, and Benedikt Gierlichs. Inner product masking revisited. Eurocrypt 2015

[CMP18]: Hervé Chabanne, Houssem Maghrebi, and Emmanuel Prouff. Linear repairing codes and side-channel attacks. IACR TCHES 2018

[CGC+21]: Wei Cheng, Sylvain Guilley, Claude Carlet, Jean-Luc Danger and Sihem Mesnager. Information Leakages in Code-based Masking: A Unified Quantification Approach. IACR TCHES 2021

Fin