

Introduction

There are two ways to address the security evaluation of a countermeasure[1]:

□ Success of attacks (using metrics such as the success rate or the guessing entropy).

Basically, there are two kinds of high-order attacks:

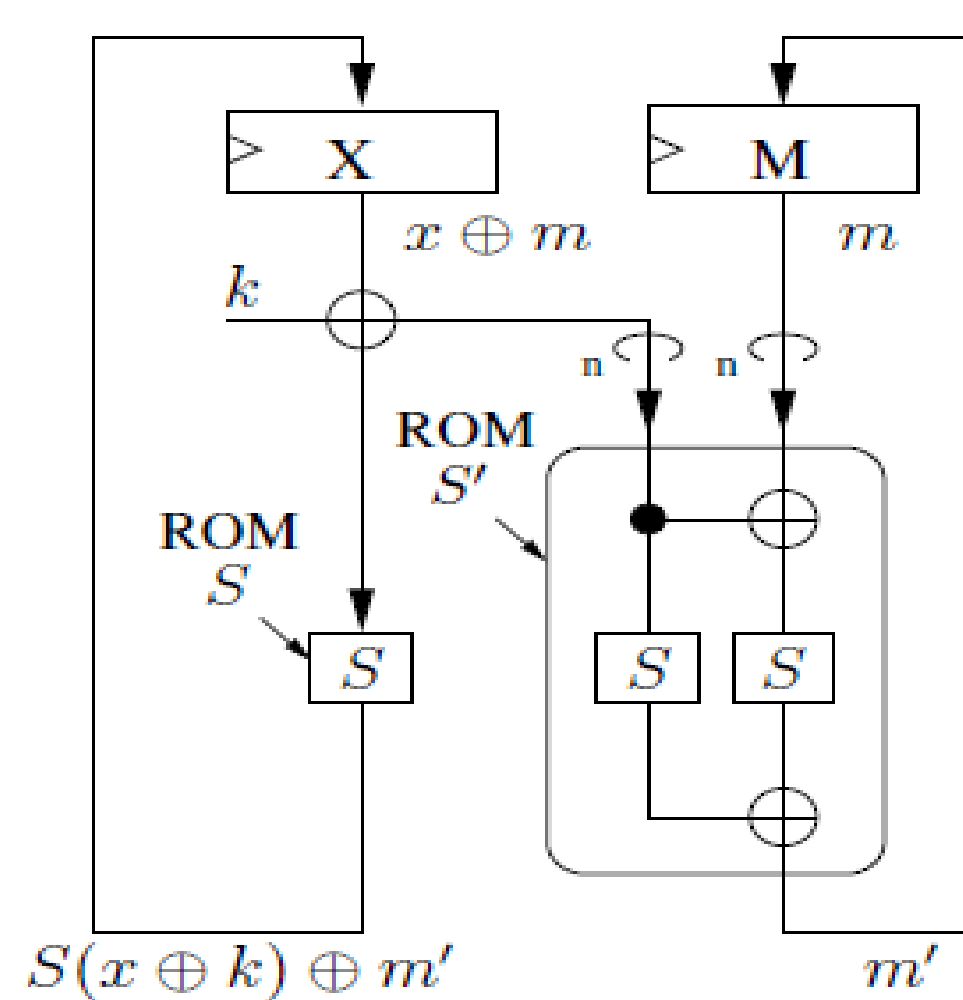
- ✓ CPA, for which the optimal attack (at high orders) is defined in[2];
- ✓ Information theoretic attacks, like the MIA, stochastic or template.

□ Leakage estimation with information theoretic metrics, such as the mutual information between the leakage (observations) and the model.

We extend the work done in [3] so as to conclude about the efficiency of hardware masking implementation.

Boolean Masking In Hardware

Principle



The idea of the Boolean masking is to mask the sensitive data by a XOR operation with a random word, in order to avoid the correlation between the cryptographic device's power consumption and the data being processed.

Leakage Model:

$$L_1 = HW [S(x \oplus k) \oplus m] + HW [m] + B$$

$$L_2 = HW [m] + B$$

Where B is an AWGN of standard deviation σ

2O-DPA Attacks on First-Order Masking

Masking can be defeated if the attacker knows how to combine the leakages corresponding to the masked data and its mask $O = C(L_1, L_2)$.

Mainly two combining functions have been studied:

- The centered product
- The absolute difference

Leakage Estimation with Information Theory

H denotes $HW[S(x+k)]$ and n is the bitwidth of the sensitive word under analysis.

We define μ_h and σ_h the mean and the standard deviation of $(O | H=h)$ (idem μ_{all} and σ_{all} are the first two cumulants of O).

The Mutual Information Metric (MIM) defined as $I(O; H)$ can be written as:

$$-\sum_{h=0}^n P(H=h) \int_{\mathbb{R}} P(O=o | H=h) \cdot \log_2 \frac{P(O=o | H=h)}{P(O=o)} do =$$

$$-\underbrace{\sum_{h=0}^n P(H=h) \frac{(\bar{\mu}_h - \bar{\mu}_{all})^2}{2\sigma^2 + 2\bar{\sigma}_{all}^2}}_{\text{Term1}} + \underbrace{\sum_{h=0}^n \frac{P(H=h)}{2 \ln 2} \ln \frac{1 + \bar{\sigma}_h^2 / \sigma^2}{1 + \bar{\sigma}_{all}^2 / \sigma^2}}_{\text{Term2}}$$

First analytical expression of the mutual information of masking under the Gaussian assumption.

$$\text{Term1} = \frac{-1/2}{\sigma^2 + \bar{\sigma}_{all}^2} \sum_{h=0}^n P(H=h) (\bar{\mu}_h - \bar{\mu}_{all})^2$$

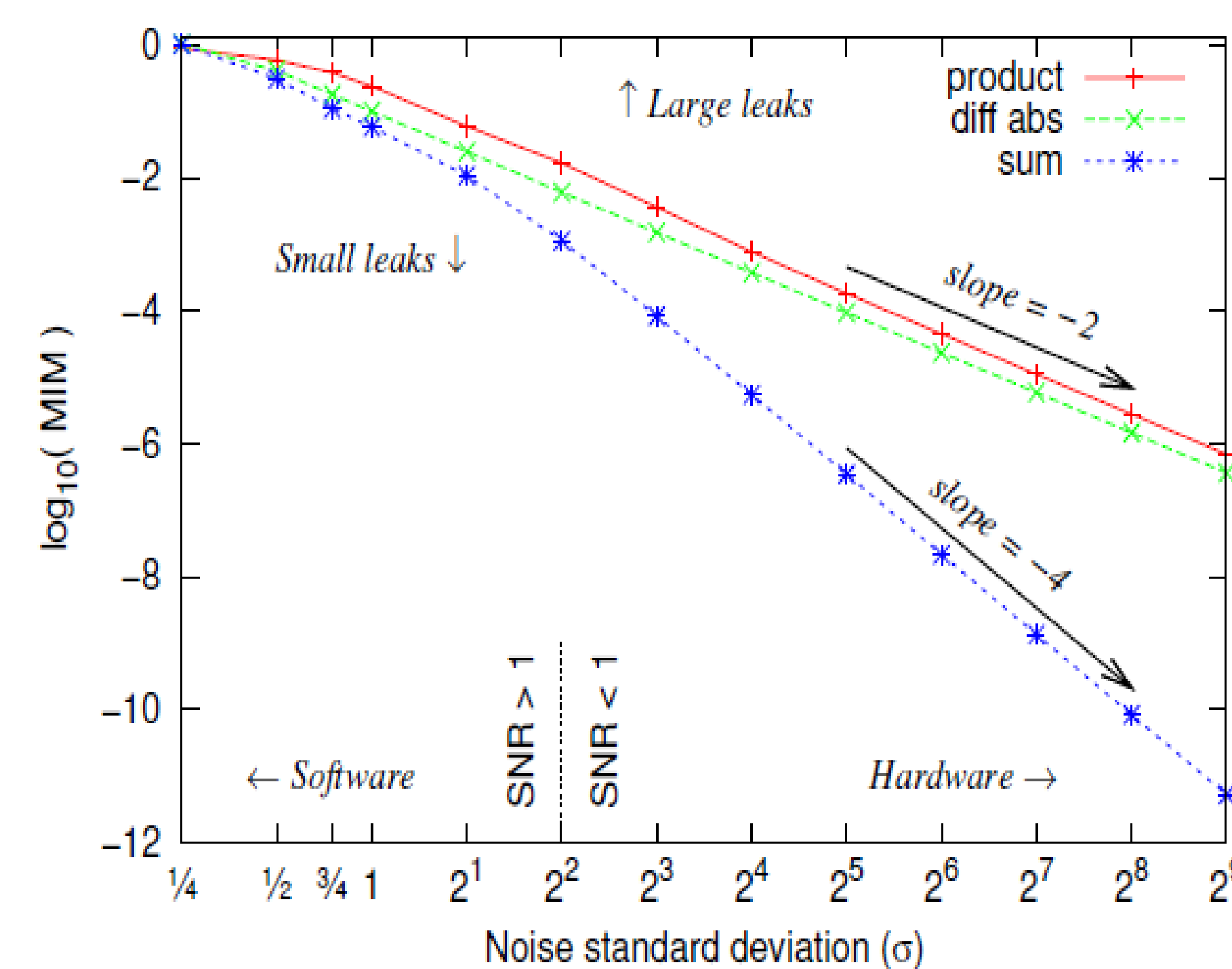
$$\text{Term2} \approx \frac{1}{4 \ln 2 \times \sigma^4} \left(\bar{\sigma}_{all}^4 - \sum_{h=0}^n P(H=h) \bar{\sigma}_h^4 \right)$$

1. For the sum combination:

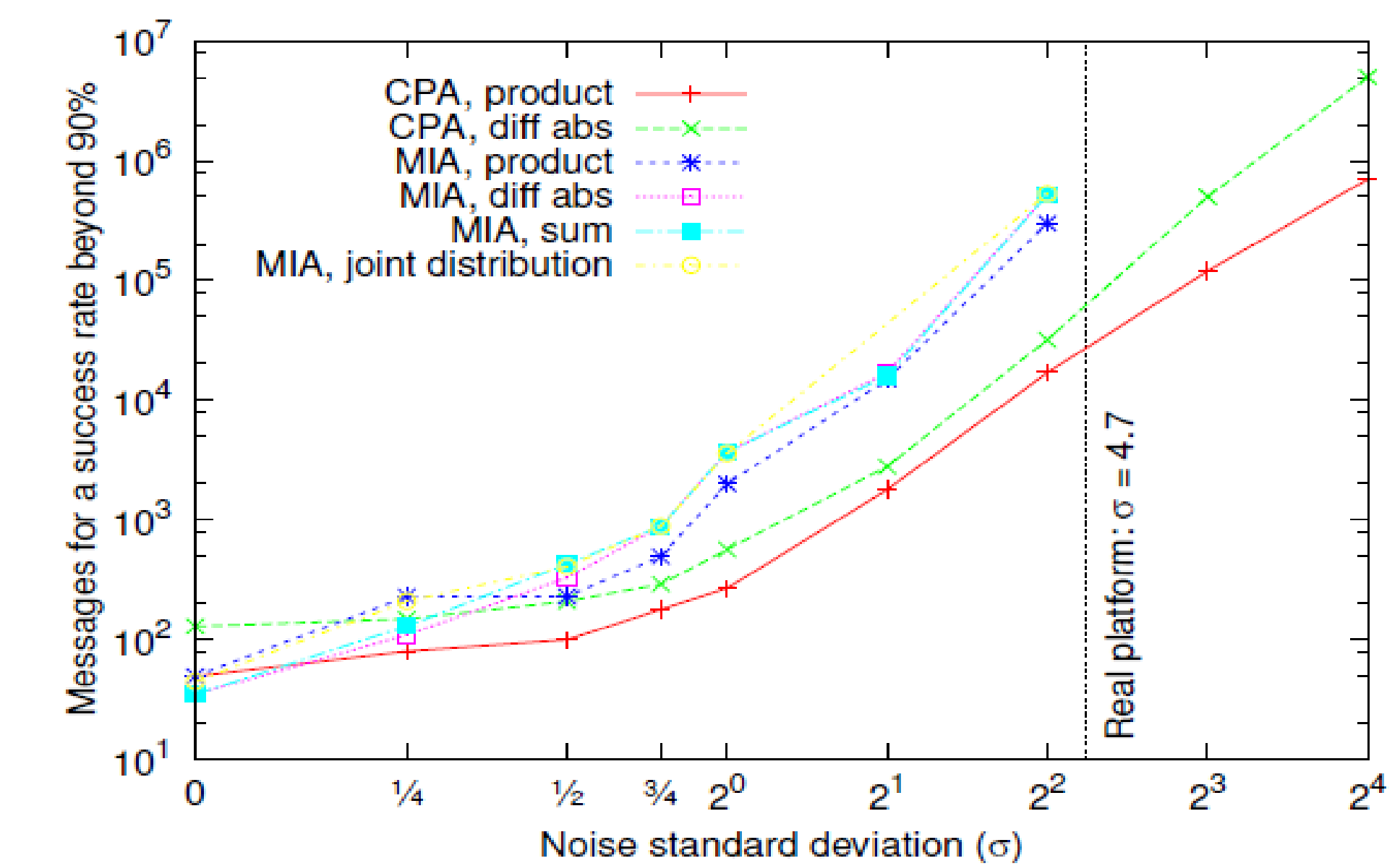
Term 1 is null, because all μ_h are the same \longrightarrow **MIM $\approx \sigma^{-4}$**

2. For absolute difference and centered product combinations:

Term 1 is preponderant \longrightarrow **MIM $\approx \sigma^{-2}$**



Resistance against 2O attacks



An approximation of Pearson's correlation coefficient for absolute difference and centered product is:

$$\rho_C(O_1, O_2) = (O_1 - E(O_1)) \times (O_2 - E(O_2)) \propto \frac{\sqrt{n}}{4\sigma^2} \rho_C(O_1, O_2) = |O_1 - O_2| \propto \frac{\sqrt{n}}{4\sigma^2 \sqrt{2\pi - 4}}$$

We have **MIM/CPA = constant**, differ from that of standard univariate side-channel attack [4] where **MIM/CPA² = constant**.

Conclusions and outlooks

- ➔ The leakage metric allows to characterize perfectly the best attack.
- ➔ The links between leakage and attacks metrics is explicitly exhibited.
- ➔ Masking is a countermeasure more efficient in hardware than in software.
- ➔ A perspective is to use multiple sensors placed at different locations over a Hardware masked cryptoprocessor in order to perform 2O attacks combining two observations with a combination function which is not only the sum.

Acknowledgements

- ANR Project ARPEGE ANR-09-SEGI-013 SecReSoC: "Secured Reconfigurable System on Chip".
- Emmanuel PROUFF (Oberthur Technologies), for precious discussions.

References

- [1] F.-X. Standaert, T. Malkin, and M. Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks, in *EUROCRYPT 2009*.
- [2] E. Prouff, M. Rivain, and R. Bevan. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Transactions 2009*.
- [3] F.-X. Standaert, N. Veyrat-Charvillon, E. Oswald, B. Gierlich, M. Medwed, M. Kasper, and S. Mangard. The World is Not Enough: Another Look on Second-Order DPA. In *ASIACRYPT 2010*.
- [4] S. Mangard, E. Oswald, and F.-X. Standaert. One for All – All for One: Unifying Standard DPA Attacks. *Cryptology ePrint Archive 2009*.