IEEE Intl. Workshop on Information Forensics and Security
Foz do Iguaçu, Brazil, November 29th - December 2nd, 2011

A Multiresolution Time-Frequency Analysis Based Side Channel Attacks

Nicolas Debande, Youssef Souissi , Aziz El Aabid, Sylvain Guilley and Jean-Luc Danger
Morpho, Telecom-ParisTech
This work is partially funded by JST/ANR SPACES project

1. Introduction

- Physical security of embedded systems has always been an open question and usually treated as an integral part of embedded system design.
- Side-Channel Analysis are one of the most powerful attacks on embedded systems since they are non-invasive, low cost and easily mount in practice.
- Embedded systems should be evaluated against Side-Channel Analyses [1][2].
- We provide the evaluator with a multiresolution analysis (Wavelets transform) based three techniques to assess the robustness of embedded systems against Side-Channel Analysis:
  1) Cryptographic patterns detection.
  2) Side-Channel noise filtering.
  3) Side-Channel Attacks.

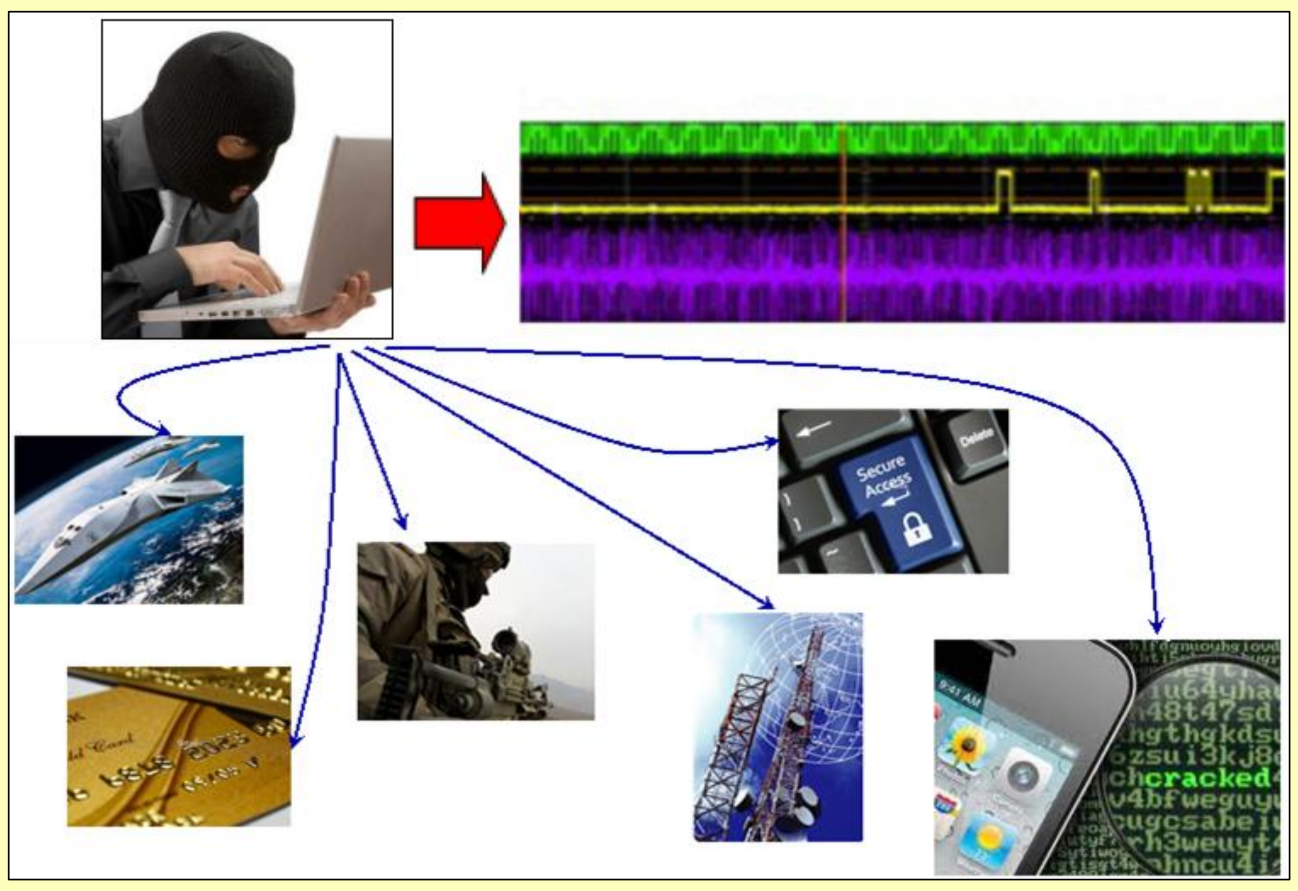

Fig. 1. Side Channel attacks on embedded systems

2. Multiresolution principle

Continuous Wavelets Transform (CWT):

$$WT_X(\tau,s)=\frac{1}{\sqrt{|s|}}\int_{-\infty}^{+\infty}X(t)\psi\left(\frac{t-\tau}{s}\right)\mathrm{d}t$$

- Characterization in both the frequency and temporal domain.
- Multi-scale resolution (shifting and scaling window) to obtain both a good time resolution and a good frequency resolution.

Discrete Wavelets Transform (DWT):

- Filter banks: separate the signal into two different frequency band
  Filter banks increases the frequency resolution
- Down-sampling (↓2): keep only one point in two
  Down-sampling decreases the temporal resolution

- *Approximations* : the coefficients associated to the low frequency band
- *Details :* the coefficients associated to the high frequency band

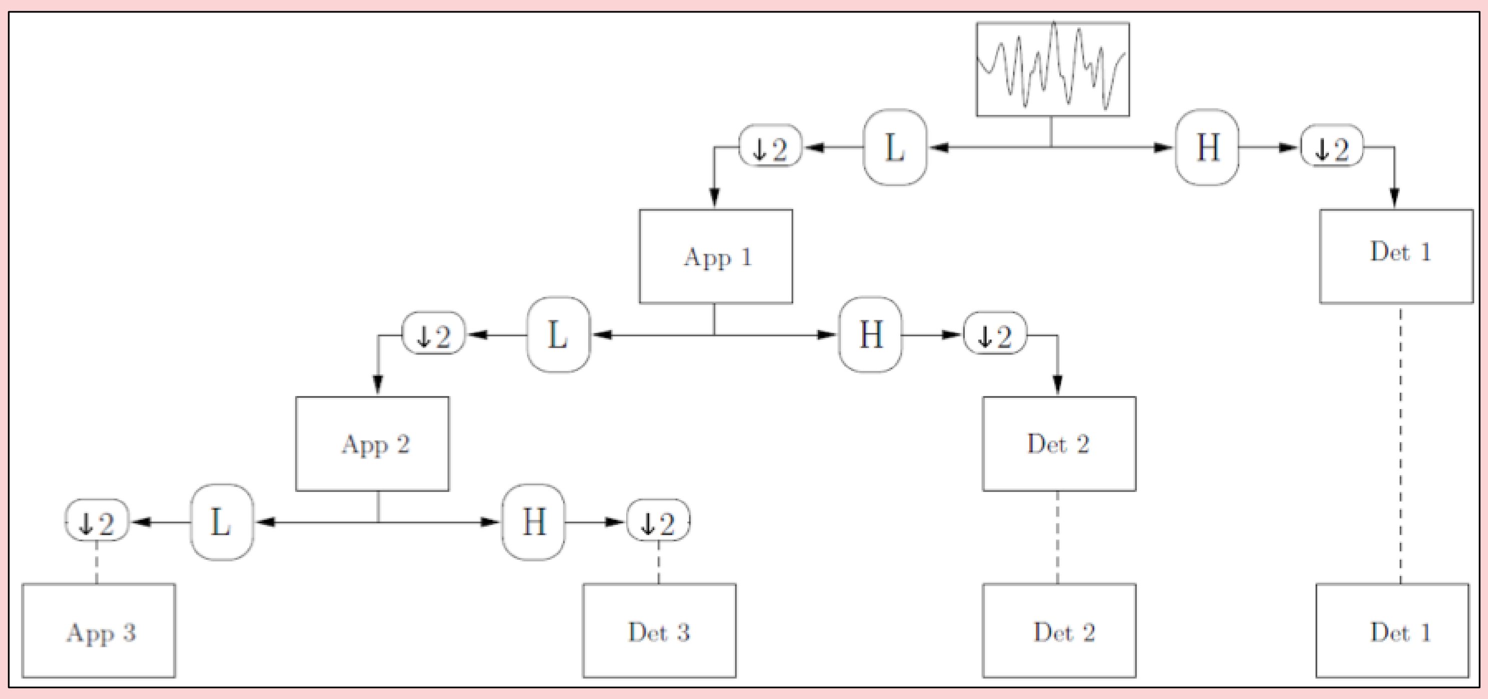

Fig. 2. Illustration of 3-level wavelets decomposition

3. Cryptographic patterns detection

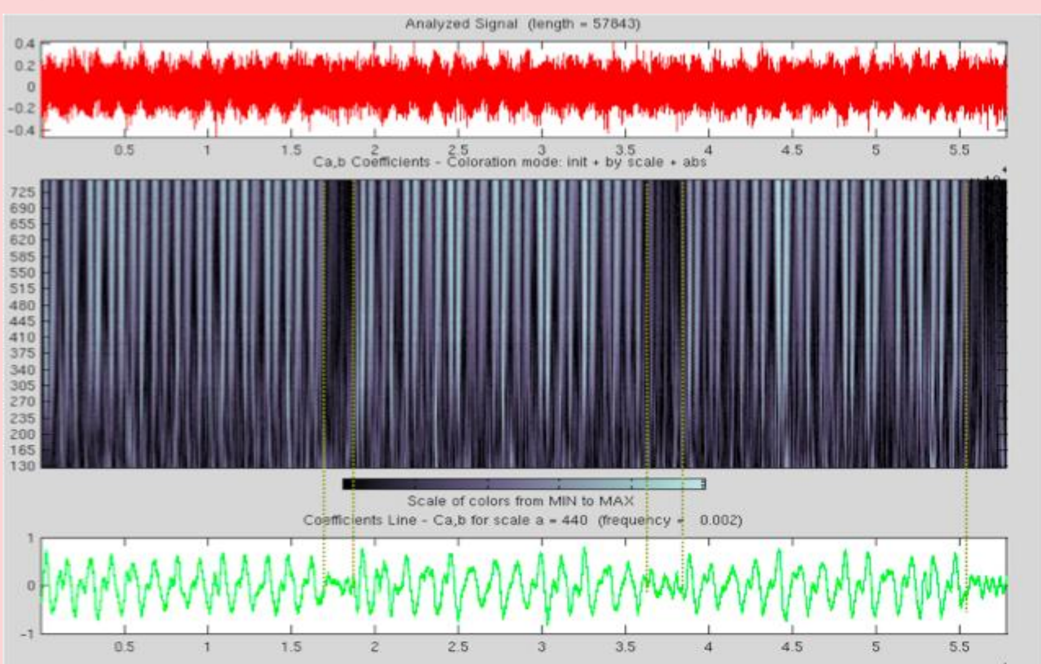

Fig. 3. 2D-CWT representation for AES encryptions detection

4. Side-Channel noise filtering

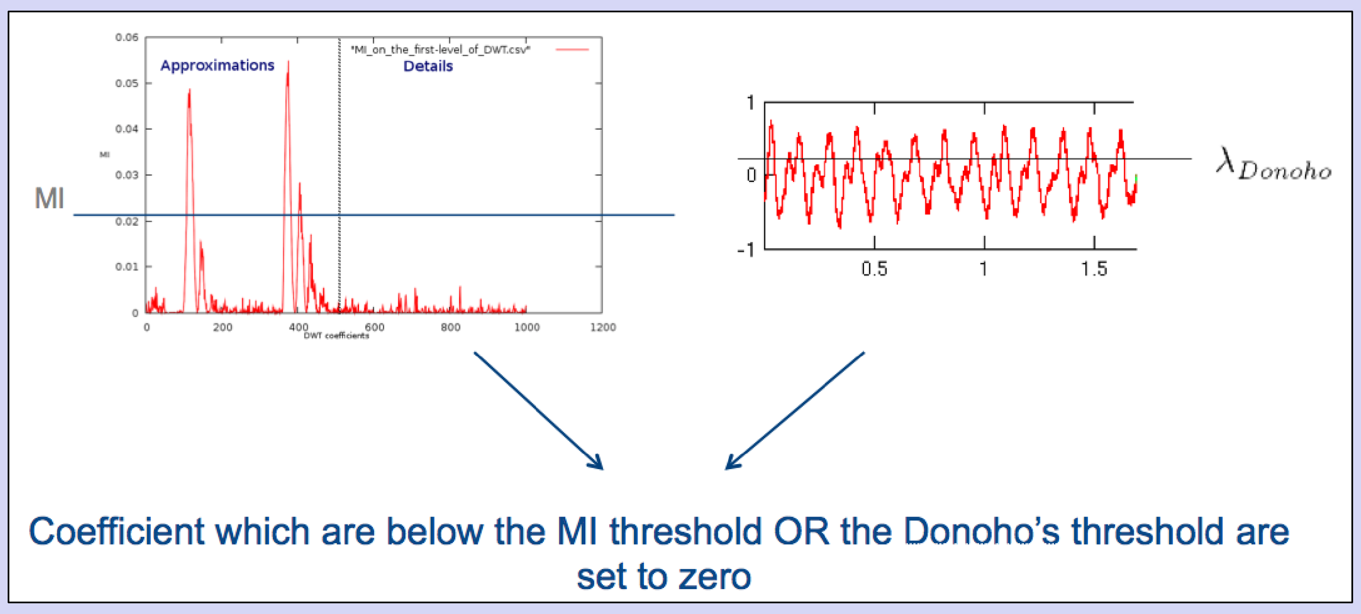

Fig. 4. Combining mutual information and Donoho's threshold to filter noise

5. DWT in the very core of the attack

- Goal : to improve all standard methods (generic)
- Method: to perform standard SCA attacks on the wavelet coefficient
- Benefits:
  - Avoid loss of information caused by wavelet reconstruction
  - Avoid noise due to temporal de-synchronization

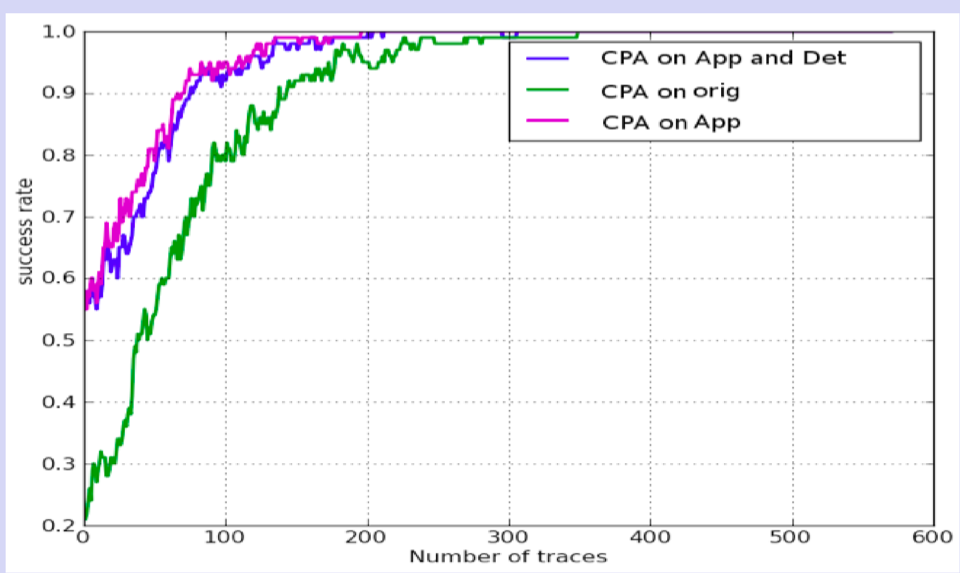

Fig. 5. CPA success rate

6. Conclusion

- Wavelet transform allows many applications in SCA context: patterns detection, noise filtering, traces compression and secret key recovery
- All these applications establish a SCA ethodology

References

[1]: Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential Power Analysis. CRYPTO'99.
[2]: Eric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In CHES 2004.
[3]: FX Standaert, Tal Malkin, and Moti Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In EUROCRYPT 2009.

Authors' contact: nicolas.debande@telecom-paristech.fr