Side Channel Analysis enhancement: A proposition for measurements resynchronisation

Nicolas Debande, Youssef Souissi, Maxime Nassar
Thanh-Ha Le, Sylvain Guilley, Jean-Luc Danger

June 17, 2011

TELECOM ParisTech · Identity & Security Alliance · SAFRAN Morpho · SPACES[1]

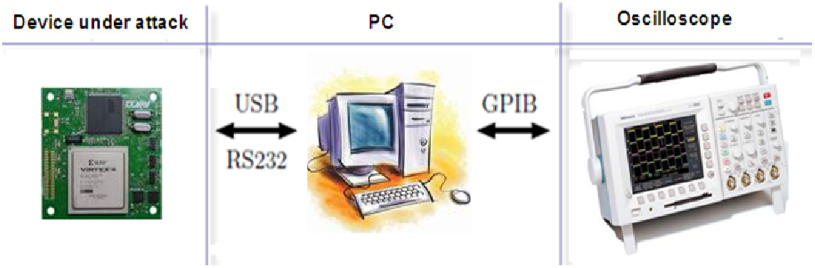
[1] work partially sponsored by the JST-ANR project SPACES

Summary

Summary

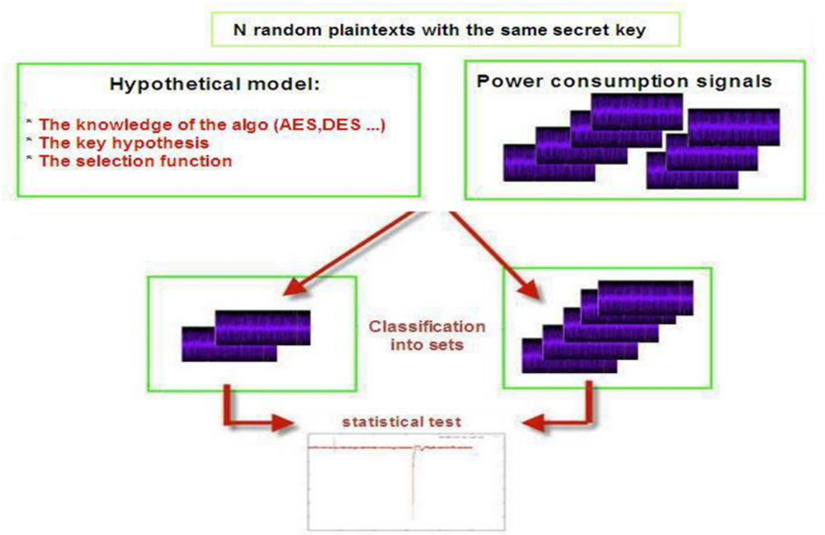

Side Channel Analysis
Many applications

Embedded Device Context



Side Channel Analysis tools

Side Channel Analysis



Summary

Importance of Curves Synchronization

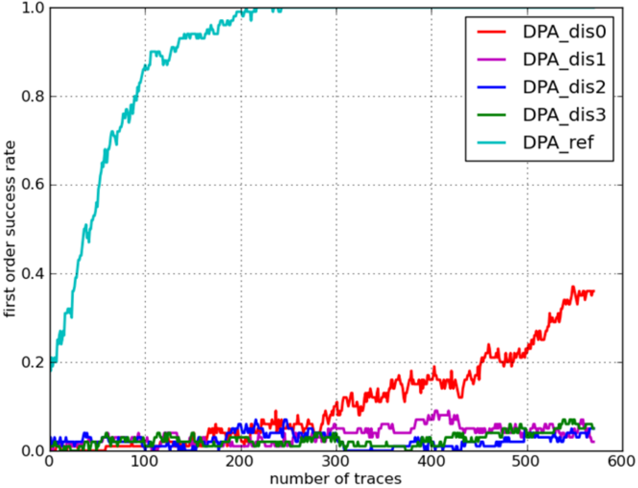


Figure: Desynchronization effect on DPA efficiency

Importance of Curves Synchronization

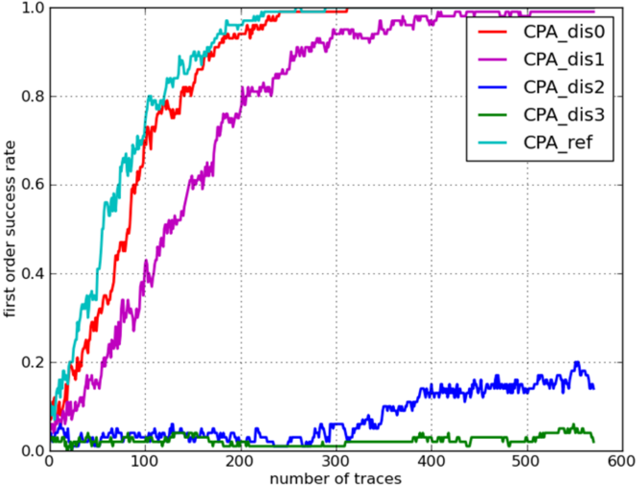
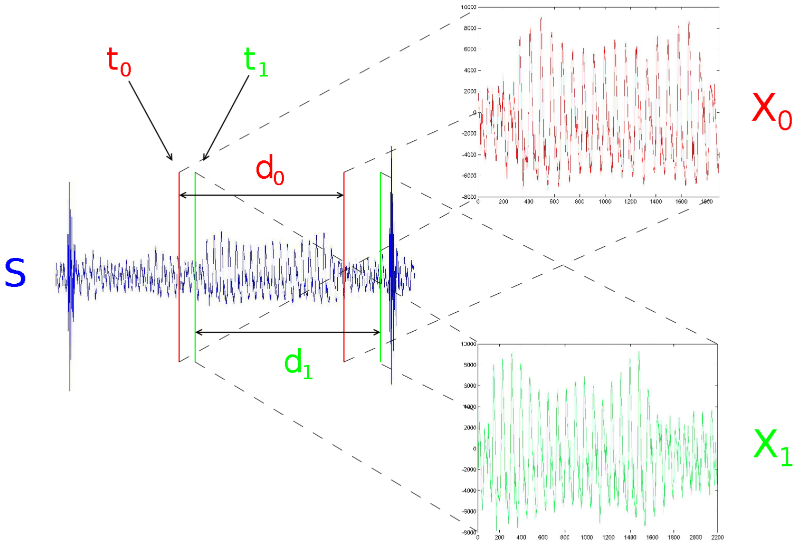


Figure: Desynchronization effect on CPA efficiency

The Problem



The Problem

(t_0, d_0) and (t_1, d_1) are the **temporal basis** of X_0 and X_1

There exists a warping function $W(t)$ such as:

$$X_0(t) = X_1(W(t)) \tag{1}$$

Let's define $W(t) = a + b \cdot t$, where a is the shift and b is the zoom

In our example: $a = t_1 - t_0, \quad b = \frac{d_1}{d_0}$

The Problem

In the Side Channel Analysis context, the evaluator has N curves X_i from N different sources S_i, $i \in [\![1, N]\!]$.

The problem is to find $W_i(t) = a_i + b_i \cdot t$ such as $(t_{\text{ref}}, d_{\text{ref}})$ is the temporal basis of $X_i(W_i(t))$, for all $i \in [\![1, N]\!]$.

Some already known methods:

Cross-Correlation	O(nlog(n))	→ Only for shifted traces
POC[2]	O(nlog(n))	→ Only for shifted traces
DTW[3]	O(n)	→ Works with shifted and streched traces

[2] N. Homma *et al.*, CHES 2006

[3] J. G. J. van Woudenberg *et al.*, CT-RSA 2011

Summary

James method

Moment Based Synchronization [4]

Temporal mean:

$$\mu_{X_i}^{(1)} = \int t.X_i(t)\,\mathrm{d}t \tag{2}$$

$\mu_{X_i}^{(1)}$ allows to find a_i.

Standard deviation:

$$\mu_{X_i}^{(2)} = \int (t - \mu_{X_i}^{(1)})^2.X_i(t)\,\mathrm{d}t \tag{3}$$

$\mu_{X_i}^{(2)}$ allows to find b_i.

[4] G. James, Annals of Applied Statistics 2007

Methodology

For each curve X_i:

- Compute $\tilde{X}_i = S(X_i)$, where $S()$ combines a smoothing and a weighting function
  $\rightarrow$ This step aims to emphasize characteristic patterns of the curve
- Compute $\mu^{(1)}_{\tilde{X}_i}$ and $\mu^{(2)}_{\tilde{X}_i}$
- Compute $b_i = \sqrt{\frac{\mu^{(2)}_{\tilde{X}_i}}{\mu^{(2)}_{\text{ref}}}}$ and $a_i = \mu^{(1)}_{\tilde{X}_i} - b_i.\mu^{(1)}_{\text{ref}}$

In SCA context

Some difficulties . . .

- Each support S_i is different
  $\hookrightarrow$ Implies an error margin on $\mu_{\tilde{x}_i}^{(1)}$ and $\mu_{\tilde{x}_i}^{(2)}$
  $\hookrightarrow$ The weighting phase is important!

- S_i is mainly periodic implies that there is no suitable weighting function

Assumptions

The curves X_i are mainly periodic and its period T_i are known by the evaluator.
$\hookrightarrow$ The evaluator can compute $b_i = \frac{T_i}{T_{\text{ref}}}$

Idea: to work with averaged period $\mathcal{T}_i$ on each curve.
We redefine $\mu^{(1)}$:

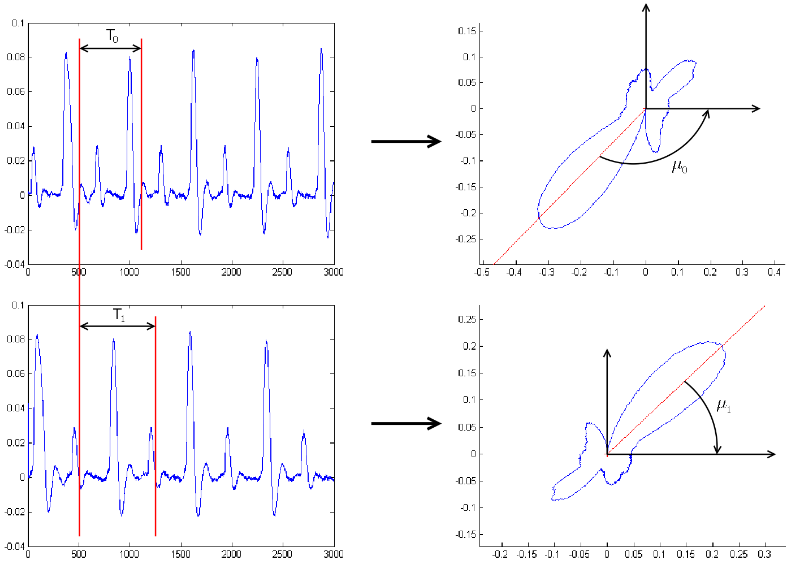
$$\mu^{(1)}_{\mathcal{T}_i} = \sum_{t=1}^{T_i} \mathcal{T}_i(t) e^{\frac{-2\pi i}{T_i} t} \, \mathrm{d}t \tag{4}$$

Methodology

For each curve X_i:

- Compute an averaged period $\mathcal{T}_i$
- Compute $\tilde{\mathcal{T}}_i = S(\mathcal{T}_i)$, where $S()$ combines a smoothing and a weighting function
- Compute $\mu^{(1)}_{\tilde{\mathcal{T}}_i}$
- Compute $a_i = \frac{\arg\left(\mu^{(1)}_{\tilde{\mathcal{T}}_i}\right) \cdot T_i}{2\pi}$

Resynchronization by Moment



Summary

Experimental results

Case of shift only

	Set	X_i	$\mathrm{RM}(X_i)$	$\mathrm{AOC}(X_i)$
Averaged	1	0.1390	0.9937	1.000
	2	0.0444	0.9239	1.000
	3	0.0244	0.8807	0.9919
Noised	1	0.1357	0.8960	0.9240
	2	0.0404	0.8486	0.9239
	3	0.0316	0.8181	0.9176

Table: Difference of efficiency between AOC (cross-correlation) and RM (Resynchronization by Moment)

Metric used: $\rho = \frac{\mathrm{A}(\sum X_i)}{\sum \mathrm{A}(X_i)}$, where $\mathrm{A}(X)$ returns the amplitude of X

Summary

Conclusion

Advantages of RM

- Lower computing complexity (O(n))
- Works with stretched curves

Perspectives

- Experimental results obtained without smoothing and weighting phase
  $\hookrightarrow$ Possible enhancement by working on this step
- Experimental works on shifted and stretched traces
- Synchronization of curves acquired with power varying
  $\hookrightarrow$ Use of a circular standard deviation $\mu^{(2)}_{\tilde{T}_i}$

Thank you for your attention

nicolas.debande@morpho.com
nicolas.debande@telecom-paristech.fr