“Re-synchronization by Moments”: an efficient solution to align Side-Channel traces

Anonymous submission to WIFS 2011

Abstract—**Modern embedded systems rely on cryptographic co-processor to ensure security. These cryptographic co-processor are theoretically secure but their physical implementations are vulnerable against Side-Channel Analysis (SCA). Therefore, embedded systems should be evaluated for their robustness against these attacks. In SCA, the preprocessing of acquired traces is crucial to mount an efficient analysis and therefore make a reliable evaluation. This paper mainly deals with the common problem of aligning SCA traces. For this purpose, we put forward an innovative re-synchronization algorithm and show its efficiency compared to existing techniques. Our results are based on real measurements acquired from several cryptographic implementations.**

Keywords: Side-Channel traces alignment, Phase-Only Correlation POC, Amplitude-Only Correlation AOC, Statistical moments, Correlation Power Attack (CPA).

I. Introduction

In SCA, the alignment process is of great concern since deployed analysis are very sensitive to the magnitude of acquired traces. In real life, it is almost impossible to perfectly collect aligned traces due to many factors. A frequent situation is that the trigger signal, which is precisely synchronized with the cryptographic process and used in functional testing, is removed by the designer for security reasons. However, even if the access to a signal indicating the start of the cryptographic process is possible, a jitter related to deviations from the true leak instant of the process is often observed. Therefore, in both situations, secret information can be lost due to errors induced by the displacement of traces. In some other cases, the misalignment results from implemented countermeasures such as instruction shuffling [1] or random delay insertion [2]. Basically, these countermeasures aim at varying the instant where the critical calculation is being performed from one acquisition to another. Generally, any factor responsible for the temporal misalignment of traces is usually connected to either the acquisition environment (*e.g.* oscilloscope resolution, nearby noise, *etc.*) or to the cryptographic architecture itself. The most traditional solutions to bypass this problem is to average the acquired traces or acquire as many traces as possible. However, we believe that these solutions are not suitable for all misalignment cases. Actually, averaging is not possible for masked implementations since the mask is updated from an acquisition to another. Besides, the evaluator might be limited by the number of traces that he can acquire. One other solution, namely Differential Frequency Analysis (DFA) [3], has been proposed to overcome the temporal misalignment problem. Indeed, the DFA, which aims at transposing the Side-Channel analysis to the frequency domain, is mainly based on the time shifting property of Discrete Fourier Transform (DFT) for periodic signals. This property states that a shift in time is equivalent to a linear phase shift in frequency. The frequency content remains unchanged in a time shift, since it depends only on the shape of a signal. Only the phase spectrum will be altered. In this work, we are only interested in preprocessing techniques aiming at re-synchronizing SCA traces. We propose a new algorithm of re-synchronization that is suitable for periodic traces. Compared to other methods, we gain in time processing ($\mathcal{O}$(n)), preserving a proper efficiency, specially when the traces are noisy. Moreover, we highlight new scenarios of time-shifting and show that our algorithm is still efficient when the traces are time-stretched. The general purpose of this paper is to help the evaluator to first get rid off the misalignment and to make its evaluation in the best conditions. Second, it is better to know if the countermeasures used to misalign traces can be broken by an attacker. The rest of the paper is organized as follows. Section II briefly presents the existing techniques offered as solutions to the problem of misalignment. Section III highlights the negative effect of misaligned traces on Side-Channel Analysis. Section IV introduces the proposed algorithm, namely “Re-synchronization by moments” (RM). Section V is devoted to experiments and results. In this section we make a comparative study between RM and existing algorithms. Section VI concludes the paper and opens some perspectives.

II. Related work

In SCA literature, only few re-synchronization algorithms have been offered on the common problem of aligning SCA traces. Moreover, the most interesting algorithms have only recently been presented to the cryptographic community. We mention the Phase-Only Correlation (POC), which is presented by Homma *et al.* [4]. This technique, which was initially used in the computer vision and fingerprint recognition field, employs phase components in the frequential domain using the Discrete Fourier Transform and makes it possible to determine the displacement errors between signals by using the location of the correlation peak. Recently, a new technique, based on the Dynamic Time Warping (DTW) algorithm, has been presented by J. van Woudenberg *et al.* [5]. DTW is an approach that was historically used for speech recognition that has the advantage to work with traces that have different sizes. However, there is no common method to align a set of traces with this algorithm since it is basically used to measure the similarity only between pairs of traces. Moreover, it needs a parameter to trade off between the speed and the quality of the re-synchronization. Recently, S. Guilley *et al.* have proposed a cross-correlation based re-synchronization algorithm [6], namely AOC (Amplitude Only Correlation), and an intermediate algorithm called threshold-POC (T-POC). T-POC involves a parameter $\epsilon \in \mathbb{R}^+$; depending on the value of ϵ, T-POC is rather close to POC or to AOC. This re-synchronization algorithm shows its efficiency particularly when cryptographic countermeasures are deployed. In what follows, we will focus only on the most commonly used re-synchronization algorithms that are POC and AOC.

III. Effect of traces misalignment on SCA

In order to highlight the importance of the re-synchronization process, we created three increasing displacements $disp_1 < disp_2 < disp_3$ between initially aligned traces. Then we performed a Correlation Power Analysis (CPA [7]) and observe the differences. We define a displacement $(disp_i)$ as a random number of time samples shifted left or right. To measure the extent to which an adversary is efficient in turning the side-channel leakage into a key recovery, we computed the guessing entropy (GE) metric [8]. This metric measures the average position of the secret key in a list of key hypotheses ranked by a distinguisher. An attack is considered to be successful when the average rank is being zero. We carried out our experiment on unprotected DES [9] power consumption traces that are made freely available on line, in the context of the first version of DPA Contest [10]. Obviously, as depicted in Fig. 1, the DES implementation is easily breakable by CPA. Indeed, according to CPA_{ref}, around only 250 traces are needed to reach the best rank. Although, the CPA still manages to recover the secret key for a small displacement value $(disp_1)$, its sensitivity is clearly getting higher when increasing the value of the displacement $(disp_2, disp_3)$. From the theoretical point of view, we assume that the misalignment results from a displacement of the traces by a number of time samples in the interval $[\![0, t[\![$. We say that $t \in \mathbb{N}^*$ is the size of the misalignment window. Then, in the extreme case where the misalignment is uniformly distributed over $[\![0, t[\![$, the correlation ρ between the traces and a leakage model with the misalignment is equal to $1/\sqrt{t}$ times that without any misalignment. Now, the speed of a CPA is directly linked to ρ. In fact, S. Mangard in [11] proposed an interesting hypothesis testing approaches that aims at estimating the correlation coefficients that occur in CPA without actually performing the attack in practice. In other words, computations made with the correct key are sufficient to apply this approach. Actually, these estimations of the correlation coefficients are used in a rule of thumb [11], [12] to reliably predict the number N of SCA traces needed to perform a successful CPA (*i.e* extracting the value of the secret key among all key hypotheses). This rule is given by the following Eqn. (1):

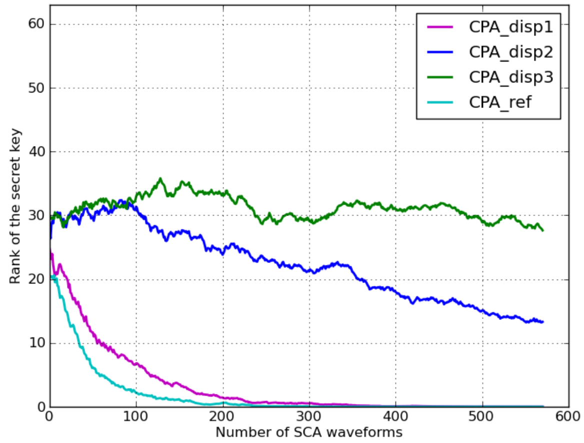

Figure 1. CPA Guessing entropy on misaligned traces.

$$N = 3 + 8\left(\frac{Z_{1-\alpha}}{\ln\left(\frac{1+\rho}{1-\rho}\right)}\right)^2 , \tag{1}$$

where $Z_{1-\alpha}$ is the quantile of a normal distribution for the 2-sided confidence interval with error $1-\alpha$. For low values of ρ, the Eqn. (1) is $\propto \rho^{-2}$. Therefore, all in one, the number of traces N to break a cryptographic implementation with a misalignment window t is roughly multiplied by $\left(1/\sqrt{t}\right)^{-2} = t$. Consequently, the higher the size of the misalignment window, the lower the efficiency of CPA is.

IV. Resynchronization by statistical moments

An interesting statistical moments based technique for signals alignment has been firstly developed by James [13], in the context of signal processing. In what follows, we explore this technique and we test its adequacy for Side-channel analysis.

A. Statistical Moments Based Jame's method principle

Let $X_0(t)$ and $X_1(t)$ be two misaligned traces. By considering the acquisition process, each trace has a temporal basis. Formally, X_0 and X_1 are the discrete time digital representations of different continuous quantities, denoted respectively by $\mathcal{S}_0(t)$ and $\mathcal{S}_1(t)$. We consider that acquired traces are misaligned when their temporal basis are different. In the general case, the traces can be represented by a triplet $(\mathcal{S}_i(t), t_i, d_i)$ with $i \in \{0, 1\}$, where t_i is the instant such as $\mathcal{S}_i(t_i) = X_i(0)$ and d_i is the number of clock cycles within $X_i(t)$, which is related to the resolution of $\mathcal{S}_i(t)$). Thus, $X_i(t)$ is seen as a window, with t_i and d_i which respectively set the shift and the zoom on $\mathcal{S}_i(t)$. In what follows, the couple $\mathcal{B}_i = (t_i, d_i)$ will be called the temporal basis of $X_i(t)$. In this case, there exists two functions W_0 and W_1, called warping functions, such as $X_0(W_0(t))$ and $X_1(W_1(t))$ have the same temporal basis. In our context, the warping functions are first order polynoms, $W = a + b \cdot t$, where a and b are the shift and the zoom coefficients respectively. For sake of convenience, $\mathcal{S}_i(t)$ can be reduced to the corresponding union of all traces:

$$\begin{aligned}&\text{Let } t_0 = \min_i\ (t_i) \text{ and } t_1 = \max_i\ (t_i + d_i),\ \text{then}\\ &S_i(t) = 0,\ \forall t \in]-\infty, t_0] \cup [t_1, +\infty[.\end{aligned} \tag{2}$$

Basically, the problem of re-synchronizing two traces is to set them with a common temporal basis. We suppose now that the misaligned traces have different temporal basis but have exactly the same support $\mathcal{S}(t)$. The main idea behind the James method is to mark a point of reference R_i on each $X_i(t)$. R_i is a temporal mark, which is different for each acquired (discrete-time) trace, but corresponds to the same continuous time on $\mathcal{S}_i(t)$. Thanks to R_i, the warping functions are deduced and the different temporal basis are transformed to a single one. In [13], the author proposes to use the statistical moments to unwarp all the traces to a single temporal basis. If the warping function W is linear, only the first and second moment (mean and variance) are needed. Let $\{X_i, 0 \leq i < N\}$ be the misaligned traces and $\{Y_i, 0 \leq i < N\}$ be the re-synchronized one. First, each trace is smoothed and weighted by some filters and weighting functions. Thus, a new set $\{\tilde{X}_i, 0 \leq i < N\}$ of traces is built. This step aims to emphasize the characteristics of the main pattern within traces X_i. James proposed some weighting functions as $I_X^{(m)}$, I_X^{min} or I_X^{max} defined as follows:

$$I_X^{(m)}(t) = \frac{|X^{(m)}(t)|}{\int |X^{(m)}(s)|\,\mathrm{d}s}, \tag{3}$$

where $X^{(m)}$ is the mth derivative function of X.

$$I_X^{min}(t) = (\max(X(t)) - X(t))^r\,, \tag{4}$$

$$I_X^{max}(t) = (X(t) - \min(X(t)))^r\,. \tag{5}$$

$I_X^{(m)}$ allows to concentrate weights on the shape of the pattern, while I_X^{min} and I_X^{max} respectively weight on the global minimum and maximum of X when r tends to infinity. The second step is to compute the two first moments $\mu_{X_i}^{(1)}$ and $\mu_{X_i}^{(2)}$ of each $\tilde{X}_i$. They are defined as follows:

$$\mu_{X_i}^{(1)} = \int t \cdot \tilde{X}_i(t)\,\mathrm{d}t \quad \text{and} \tag{6}$$

$$\mu_{X_i}^{(2)} = \int (t - \mu_{X_i}^{(1)})^2 \cdot \tilde{X}_i(t)\,\mathrm{d}t\,. \tag{7}$$

Note that $\mu^{(1)}$ is the way chosen in [13] to find a point of reference R, introduced above. With $\{(\mu_{X_i}^{(1)}, \mu_{X_i}^{(2)}), 0 \leq i < N\}$, we can compute the reference moments $(\mu_{\text{ref}}^{(1)}, \mu_{\text{ref}}^{(2)})$, *e.g.* as follows:

$$\mu_{\text{ref}}^{(1)} = \frac{1}{N}\sum_{i=0}^{N-1} \mu_{X_i}^{(1)}, \quad \mu_{\text{ref}}^{(2)} = \left(\frac{1}{N}\sum_{i=0}^{N-1} \sqrt{\mu_{X_i}^{(2)}}\right)^2 . \tag{8}$$

We now aim to find $W_i(t) = a_i + b_i.t$ such as $\tilde{X}_i(W_i(t)) = \tilde{Y}_i(t)$ and $(\mu_{\tilde{Y}_i}^{(1)}, \mu_{\tilde{Y}_i}^{(2)}) = (\mu_{\text{ref}}^{(1)}, \mu_{\text{ref}}^{(2)})$. In other words, we have to find a_i and b_i such as the statistical moments of X_i tends to $(\mu_{\text{ref}}^{(1)}, \mu_{\text{ref}}^{(2)})$. We can determine them as follows:

$$b_i = \sqrt{\frac{\mu_{\tilde{X}_i}^{(2)}}{\mu_{\text{ref}}^{(2)}}}, \qquad a_i = \mu_{\tilde{X}_i}^{(1)} - b_i \cdot \mu_{\text{ref}}^{(1)}\,. \tag{9}$$

1) Adequacy for Side-Channel analysis: Some difficulties arise when James method is applied in the SCA context. Indeed, all traces are different from each other. Actually, the data manipulated during an encryption is dependent on the plain text in input, which is varying from one trace to another. Even if the same plaintext is used, noticeable differences between the acquired traces are often observed due to noise fluctuations. In practice, these differences imply a variation of $\mu^{(1)}$ and therefore an inaccuracy on the point of reference R. These nothings bring us to consider more carefully the step of smoothing and weighting. In fact, we can establish the two following criterions:

$$\tilde{\mathcal{S}}_i \approx \mathcal{S}_{\text{ref}},\ \forall i \in \{0, 1, \ldots, N-1\} \tag{10}$$

and

$$\begin{gathered}\forall i \in \{0, 1, \ldots, N-1\},\ \forall t \in]-\infty, t_i[\cup]t_i + \hat{d}_i, +\infty[,\\ \tilde{\mathcal{S}}_i(t) \approx 0\,,\end{gathered} \tag{11}$$

where $\hat{d}_i$ is the delay for d_i clock cycles. With the choice of suitable filters and weighting functions, we aim to transform each trace such as the corresponding weighted support $\mathcal{S}_i(t)$ are very similar from one to the others (according to the criterion (10)). The higher the similarity is, the lower the error of $\mu^{(1)}$ is. In the SCA context, traces are mainly periodic (*e.g.* with the measured activity of the clock) and in this case, there exists no weighting function which emphasizes a pattern, common to all traces. Indeed, a periodic trace can not satisfy the criterion (11) unless the trace is a null vector.

B. Resynchronization by Moments (RM): the proposed algorithm

Since the problem comes only with periodic traces, a logical approach is to work, for each trace X_i, with a sub-window $\mathcal{T}_i$, such as $|\mathcal{T}_i| = T_i$ and $\mathcal{T}_i(0) = X_i(t_0)$, where T_i is the period of X_i and t_0 is a chosen index in $[\![0, n-1]\!]$ ($|X_i| = n$). From a set of traces $\{X_i, 0 \leq i < N\}$, we compute a new set of averaged and weighted period $\{\tilde{\mathcal{T}}_i, 0 \leq i < N\}$. As shown in Fig. 2, each $\tilde{\mathcal{T}}_i$ is represented around an origin point O, by associating polar coordinates to each point as follows:

$$\begin{aligned}&\forall i \in [\![0, N-1]\!],\ \forall t \in [\![0, T_i - 1]\!],\\ &\tilde{\mathcal{T}}_i(t) \mapsto P_{i,t} = (\tilde{\mathcal{T}}_i(t), \tfrac{t \times 2\pi}{T_i})\,.\end{aligned} \tag{12}$$

Thus, all the $\tilde{\mathcal{T}}_i$ are similar up to a rotation. To each $\tilde{\mathcal{T}}_i$, we associate a new triplet $(\mathcal{S}_i(t), t_i, d_i)$, where $\mathcal{S}_i(t)$ is a circular support, t_i is the angular distance from $\tilde{\mathcal{T}}_i$ to $\mathcal{S}_i(t)$ and d_i is now equal to T_i. With the knowledge of t_i and T_i, all the traces can be transformed such as they have a single temporal basis. Indeed, the warping function $W_i(t) = a_i + b_i.t$ is deduced with:

$$a_i = \frac{t_i \times T_i}{2\pi}, \quad b_i = \frac{T_i}{T_{\text{ref}}}\,, \tag{13}$$

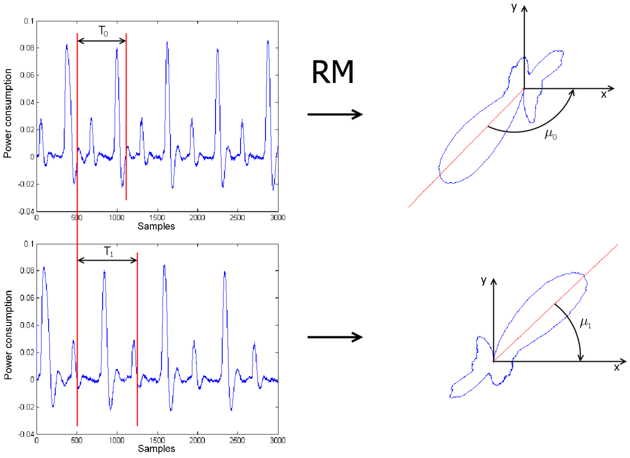

Figure 2. An example to computing $\mu^{(1)}$

where $T_{\text{ref}} = \frac{1}{N}\sum_{i=0}^{N-1} T_i$. We find t_i by searching a point of reference R_i on each period. We propose to find R_i by computing a 'circular mean', that is:

$$\overrightarrow{OR_i} = \sum_t \overrightarrow{OP_{i,t}}\,. \tag{14}$$

As depicted in Fig. 2, the vector $\vec{R_i}$, which is represented in red, coincides approximately with the maximum of the trace over the period. But, looking more in details, it is little offset: the reason is that the Resynchronization by Moment's method (RM) considers all the information contained in one clock period, thus gaining accuracy. By setting $\mathcal{S}_{\text{ref}}$ such as $R_{\mathcal{S}_i}$ has its angular coordinate equal to zero, the angular coordinate of R_i is then equal to t_i. Note that the RM method operates within a clock period. Indeed, all clock periods involved are synchronized only when the possible shift is inferior than $\frac{T_{\text{ref}}}{2}$. In order to rectify these errors, the evaluator can use a giant step phase. It consists in choosing one trace X_{ref} as a reference and computing a cross-correlation between all the traces, by considering a step of T_{ref} temporal points. This phase is necessary to enhance SCA attacks. More details will be given in Section V that puts forward the efficiency of RM without the giant step phase by using the method of the least square modulo clock.

C. *Link With POC*

In the case of periodic traces, the circular mean defined in Eqn. (14) can be written as follows:

$$\mu^{(1)}_{\mathcal{T}_i} = \sum_{t=1}^{T_i} \tilde{\mathcal{T}}_i(t) e^{\frac{-2\pi i}{T_i} t}\,\mathrm{d}t \tag{15}$$

Thus, $\mu^{(1)}_{\mathcal{T}_i}$ is equal to $DFT(\tilde{\mathcal{T}}_i(t))_k$, where $k = \frac{n}{T_i}$. Thus, while POC uses the phase of all component of $DFT(X_i)$, RM uses the phase of only one component of $DFT(\tilde{\mathcal{T}}_i)$, which corresponds to the highest amplitude (since X_i is periodic). Then, a_i is deduced with $a_i = \frac{\arg\left(\mu^{(1)}_{\tilde{\mathcal{T}}_i}\right)\cdot T_i}{2\pi}$. This implies that RM is $\log(n)$ times faster than POC. Furthermore, the RM benefits from any additional knowledge the evaluator has about the measurements. Typically, the evaluator is generally able to identify periods of interest. Thus, he can focus the analysis on them, which eventually leads to a reduction of the noise, especially when compared with a blind POC that would accumulate the noise of the whole trace.

V. Experiments, results and discussion

A. *Evaluation metrics*

In order to compare the efficiency and the genericity of involved algorithms (AOC, POC and RM), we studied two kinds of time warp: Only time-shift and time-shift combined with a dilation (time-stretching). Moreover, for both cases of time warp, we simulated three levels of misalignment. From our point of view, an appropriate metric to evaluate the re-synchronization is to compute the standard variance of the re-synchronization error:

$$S = \frac{1}{n}\sum_{i=0}^{n-1}(s_i + a_i - \overline{m})^2 \tag{16}$$

where the s_i are the simulated shift, the a_i are the shift deduced with the evaluated method that also determines the new reference $\overline{m}$, which corresponds to the ideal a_i when $s_i = 0$. To validate this metric, we check results provided by the Guessing entropy security metric when performing a CPA. However, in practice, the S metric can not be computed as the evaluator does not know the ideal set. In this case, the problem is to quantify the level of misalignment of a given campaign and estimate whether a re-synchronization process is necessary. For this purpose, the Gini coefficient [14][1] is a suitable solution since it provides a value between 0 and 1. Indeed, Gini coefficient can be used to evaluate the amount of power consumption disparity within a set of traces. The higher the disparity is, the lower the value of the Gini coefficient is. Hereafter is the formula:

$$G_t = \frac{1}{n(n-1)}\sum_{i=1}^{n}\sum_{j=1}^{n}|y_{it} - y_{jt}| \tag{17}$$

where n is the number of traces and y_{it} is the set of power consumption values at a given instant t. The metric used in this paper is defined by $G = \frac{1}{s}\sum_{t=0}^{s-1} G_t$, where G is the Gini coefficient averaged over all time samples, which number is equal to s (*i.e.* the size of one trace).

B. *Comparative results*

Our measurement setup consists of one Altera Stratix-II FPGA soldered on an SASEBO-B platform, an 54855 Infiniium Agilent oscilloscope with a bandwidth of 6 GHz and a maximal sampling rate of 40 GSa/s, antennas of the HZ–15 kit from Rohde & Schwarz. We recorded two sets of 5000 side-channel traces related to the activity of an unprotected DES crypto-processor. The averaging (256x) was performed

[1] Gini coefficient is a popular measure of statistical dispersion, which is originally used to quantify the disparity of wealth in a population.

on only one set of traces. The involved re-synchronization algorithms are $\hat{\mathrm{RM}}$, RM and AOC. We note that $\hat{\mathrm{RM}}$ is RM without the weighting phase (*i.e.* $\mu^{(1)}$ is directly computed with $\mathcal{T}_i$). During our experiments, we have empirically noticed that the weighting function described in Eqn.(7) with r equals to 3 is a proper choice in the analysis.

1) Only time-shifting: Results regarding the "Only time-shifting" case are depicted in Table I. The method of least square is computed modulo clock. We notice that AOC provides a perfect re-synchronization when the traces are averaged. However, AOC's efficiency is lower than RM's one, if the traces are noisy. Note that RM is always better when applied with a suitable weighting function. Fig. 4 represents the Guessing entropy metric when a CPA is performed on noisy traces. Clearly, RM converges faster to the best rank, compared to the other methods. Globally, results given in Table I are coherent with empirical attacks, which validates the correctness of the proposed metric (S). Besides, the metric of Gini does not reveal any differences between compared algorithms, but allows the evaluator to distinguish whether a set of traces needs a re-synchronization. For instance, if traces are averaged then a threshold of 0.2 can be adopted. However, we can see that the relevance of G decreases when the noise increases. This fact regards the majority of disparity measures and is often reported in statistics books.

Table I
COMPARATIVE RESULTS FOR THE "ONLY TIME-SHIFTING" CASE.

		Square metric		**Gini metric**	
		Avg	**Noisy**	**Avg**	**Noisy**
desynch	**1**	-	-	0.231	0.137
	2	-	-	0.282	0.140
	3	-	-	0.333	0.149
$\hat{\mathrm{RM}}$	**1**	0.008	1.084	0.120	0.136
	2	0.009	1.171	0.121	0.136
	3	0.021	0.536	0.122	0.136
RM	**1**	0.003	0.295	0.123	0.136
	2	0.003	0.282	0.123	0.136
	3	0.011	0.251	0.123	0.136
AOC	**1**	0	0.405	0.124	0.136
	2	0	0.405	0.122	0.136
	3	0	0.405	0.123	0.136

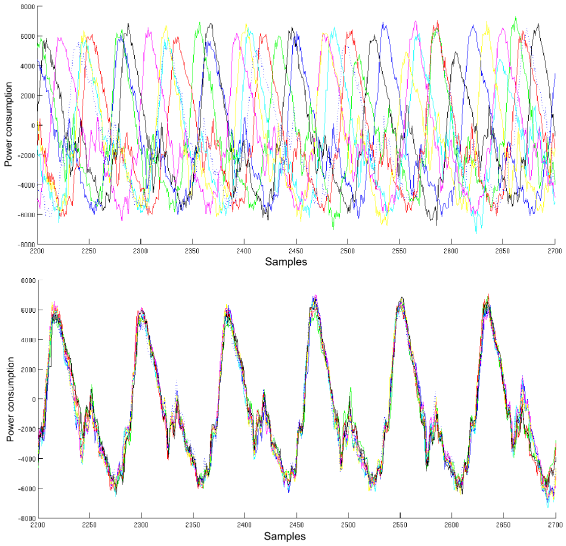

Figure 3. An illustration of DES traces re-synchronization using RM

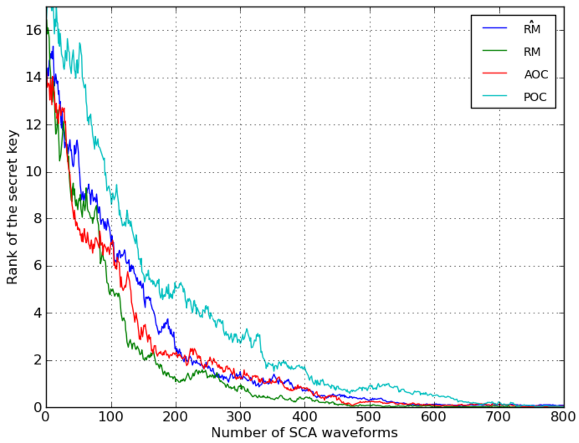

Figure 4. CPA guessing entropy on re-synchronized and noisy DES traces.

2) Time-stretching: Here, we discuss two kinds of dilation, denoted by 'fix' and 'E.E.' (Environmental Effect) in Fig. 5. In the first case, each trace is stretched with a fixed dilation coefficient b_i. This means that the period T_i is varying from one trace to another, but is not varying within one trace. In order to evaluate RM in this context, we simulate these dilations on the same traces used in Section V-B1. Table II shows the results of these experiments. The 'E.E.' case aims at approaching the variation of power voltage or temperature which might occur during one acquisition campaign. These troubles do not affect the clock (so do not change T_i from a trace to another) but they speed up or slow down the computation during the encryption process (and then affect $\mathcal{T}_i$). Considering this type of dilation, we propose a methodology to re-synchronize the misaligned traces as follows: First, the evaluator has to profile the clock of the cryptographic co-processor so as to obtain an averaged clock trace C. Second, he is required to remove this averaged clock component from each trace in order to obtain a new set of traces $Y_i(t) = X_i(t) - C$, over which RM can be applied. Indeed, although each $\mathcal{T}_i$ is different, we can use a circular standard variance to find the dilation coefficient. As $\mu^{(1)}$ can be expressed as a component of a DFT (Eqn 15), we define

Table II
COMPARATIVE RESULTS FOR THE "TIME STRETCHING" CASE.

		Gini metric	
		Avg	**Noisy**
desynch	**1**	0.341	0.157
	2	0.348	0.157
	3	0.354	0.157
R$\hat{\mathbf{M}}$	**1**	0.127	0.136
	2	0.148	0.136
	3	0.137	0.136
RM	**1**	0.127	0.136
	2	0.137	0.136
	3	0.139	0.136

$\mu^{(2)}$ as follows:

$$\mu^{(2)}_{\tilde{\mathcal{T}}_i} = \sum_{t=0}^{T_i-1} \tilde{\mathcal{T}}_i(t)\, e^{(\frac{-2\pi i}{T_i}t-\theta)^2}\,\mathrm{d}t, \tag{18}$$

where $\theta = \arg\left(\mu^{(1)}_{\tilde{\mathcal{T}}_i}\right)$. After the processing of RM, the evaluator add to each trace the clock trace C.

C. Discussion

According to the experimental results, it is clear that the evaluator is required to select the most appropriate re-synchronization algorithm for each case. Indeed, as illustrated in Fig. 5, he might be faced with two problems of misalignment: Time-Stretching or Only Time-shifting. In the case of Time-stretching, RM should be used to re-synchronize SCA traces. However, when traces are Only time-shifted and averaged, AOC and POC should be good choices for the re-synchronization. Besides, AOC is still efficient when traces are noisy but less performant than RM.

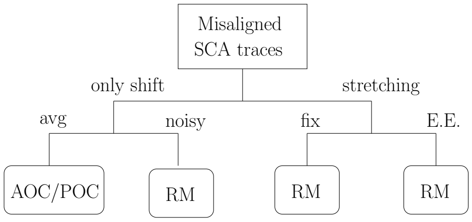

Figure 5. On the choice of the most appropriate re-synchronization algorithm.

VI. CONCLUSION

In this article, we have proposed a new re-synchronization algorithm, namely RM, as a pre-processing step in Side-Channel Analysis (SCA). Firstly, we highlighted the importance of aligning SCA traces and surveyed existing techniques to get round the problem of misalignment. Thereafter, we put forward the theoretical principle of RM algorithm and validate its efficiency empirically with regards to the most common used techniques, Amplitude Only Correlation (AOC) and Phase Only Correlation (POC). Eventually, we will concentrate our works on the choice of weighting functions, from the evaluator point of view. Furthermore, we will explore the possibility of a more complex warping functions W, as high order polynoms.

REFERENCES

[1] M. Rivain, E. Prouff, and J. Doget, "Higher-Order Masking and Shuffling for Software Implementations of Block Ciphers," in *CHES*, ser. Lecture Notes in Computer Science, vol. 5747. Springer, September 6-9 2009, pp. 171–188, Lausanne, Switzerland.

[2] J.-S. Coron and I. Kizhvatov, "Analysis and Improvement of the Random Delay Countermeasure of CHES 2009," in *CHES*, ser. Lecture Notes in Computer Science, vol. 6225. Springer, August 17-20 2010, pp. 95–109, Santa Barbara, CA, USA.

[3] E. Mateos and C. H. Gebotys, "A new correlation frequency analysis of the side channel," in *Proceedings of the 5th Workshop on Embedded Systems Security*, ser. WESS '10. New York, NY, USA: ACM, 2010, pp. 4:1–4:8. [Online]. Available: http://doi.acm.org/10.1145/1873548.1873552

[4] N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching," in *CHES*, ser. LNCS, vol. 4249. Springer, October 10-13 2006, pp. 187–200, Yokohama, Japan.

[5] J. G. J. van Woudenberg, M. F. Witteman, and B. Bakker, "Improving Differential Power Analysis by Elastic Alignment," in *CT-RSA*, 2011, pp. 104–119.

[6] S. Guilley, K. Khalfallah, V. Lomne, and J.-L. Danger, "Formal Framework for the Evaluation of Waveform Resynchronization Algorithms," in *WISTP*, June 1 2011.

[7] É. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *CHES*, ser. LNCS, vol. 3156. Springer, August 11–13 2004, pp. 16–29, Cambridge, MA, USA.

[8] F.-X. Standaert, T. Malkin, and M. Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," in *EUROCRYPT*, ser. LNCS, vol. 5479. Springer, April 26-30 2009, pp. 443–461, Cologne, Germany.

[9] NIST/ITL/CSD, "Data Encryption Standard. FIPS PUB 46-3," Oct 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[10] TELECOM ParisTech SEN research group, "DPA Contest (1st edition)," 2008–2009, http://www.DPAcontest.org/.

[11] S. Mangard, "Hardware Countermeasures against DPA – A Statistical Analysis of Their Effectiveness," in *CT-RSA*, ser. Lecture Notes in Computer Science, vol. 2964. Springer, 2004, pp. 222–235, San Francisco, CA, USA.

[12] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, December 2006, iSBN 0-387-30857-1, http://www.dpabook.org/.

[13] G. M. James, "Curve Alignment by Moments," *Annals of Applied Statistics*, vol. 1, pp. 480–501, 2007.

[14] C. W. Gini, "Variability and mutability, contribution to the study of statistical distributions and relations," *Studi Economico-Giuridici della R. Universita de Cagliari*, 1912, reviewed in: Light, R.J., Margolin, B.H.: An Analysis of Variance for Categorical Data. *J. American Statistical Association*, Vol. 66 pp. 534-544 (1971).