

Enhance Multi-bit Spectral Analysis on Hiding in Temporal Dimension

Qiasi Luo

▶ **To cite this version:**

Qiasi Luo. Enhance Multi-bit Spectral Analysis on Hiding in Temporal Dimension. 9th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications (CARDIS), Apr 2010, Passau, Germany. pp.13-23, 10.1007/978-3-642-12510-2_2 . hal-01056102

HAL Id: hal-01056102
https://inria.hal.science/hal-01056102

Submitted on 14 Aug 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Enhance Multi-bit Spectral Analysis on Hiding in Temporal Dimension

Qiasi Luo

Shanghai Fudan Microelectronics Co., Ltd
Building 4, 127 Guotai Road, Shanghai 200433, China

Abstract. Random delays and dynamic frequency switching are widely adopted in smartcards and embedded systems as temporal hiding countermeasures to side channel attack.Temporal hiding is regarded as efficient to enhance the security of cryptographic devices. However, spectral analysis with Fast Fourier Transform is a powerful method to defeat temporal hiding countermeasures. Spectral analysis shares the same merit with integration different power attack. Multi-bit spectral analysis is enhanced with partitioning power analysis, which is much more effective than the correlation power analysis in the spectral domain. Multi-bit spectral analysis effectively defeats temporal hiding countermeasure with floating-mean dynamic frequency switching countermeasure. It is suggested cryptographic devices should employ other countermeasures together with hiding to ensure side channel security.

Key words: Side channel attack, spectral analysis, differential power analysis, correlation power analysis, partitioning power analysis.

1 Introduction

Nowadays symmetric block ciphers are widely adopted in smartcards and embedded systems to provide security confidence to sensitive data. The implementation of the cryptographic algorithm may leak out side-channel information such as power consumption [1] , electromagnetic emanation [2], etc. These leakage information can be utilized by side channel attack (SCA) to retrieve the key of cipher. Masking, power-balanced logic and Hiding are main countermeasures to SCA [3]. Hiding in the temporal dimension is regarded as an efficient countermeasure in practice, since it is easy to implement together with masking and power-balanced logic to reinforce the security of cryptographic devices.

Hiding is usually implemented by inserting random delays or dummy operations which are called random process interrupts (RPIs) [4]. The RPIs desynchronize the traces of side-channel signals, therefore the leakage information is concealed by noises in the classic SCA. More traces are need to distill the signal out of noise. Random delays can also be inserted at gate-level [5]. Dynamic frequency switching (DFS) [6] is another effective approach of hiding in the temporal dimension. Re-synchronize the random clocks of DFS is

very difficult in practice. More effective way to generate the random delays or frequency switchings is the floating-mean method [7].

Several analysis methods were proposed to attack hiding in temporal dimension. Integration DPA (IDPA) [4] substantially reduces the number of traces with RPIs. Phase-Only Correlation (POC) technique [8] evaluates the displacements between traces, realigns traces or removes bad traces, and defeats countermeasure of random delays [9].

Differential frequency analysis (DFA) [10] is a powerful method against hiding, since the amplitude of Fast Fourier Transform (FFT) is time-shift invariant. To retain leakage position information , differential spectrogram analysis (DSA) [11] uses spectrogram traces generated with short-time Fourier transform. DEMA with DFA technique against HF and UHF tag prototype [12] proved the effectiveness and advantage of DFA over filtering and integration techniques [4] at the presence of noise and hiding both in amplitude and timing dimensions.

In this paper, we propose a significantly more efficient multi-bit spectral analysis method to attack hiding in the temporal dimension. The method avoid large random correlation noise and have much better performance. The method is also capable to attack DFS.

First, We introduce the basic concepts about spectral analysis and generalize the methodology. Analysis of its efficiency on hiding is presented. Then we compare different multi-bit spectral analysis methods both analytically and empirically. Finally, multi-bit spectral analysis method is carried out on two different DFS strategies and the results conform to the analysis.

2 Spectral Analysis Methods

2.1 Differential Power Spectral Analysis

Consider a cryptographic device that carries out encryption with secret key k. Let $d = \{d_1, \ldots, d_{N_d}\}$ be the intermediate data related to k which an adversary attacks, and N_d be the number of data bits. The side-channel measurement such as power consumption or EM trace is $w = \{w_1, \ldots, w_{N_w}\}$, where N_w is the total number of points. Multiple traces are $W = \{w^1, \ldots, w^{N_W}\}$, where N_W is the number of traces. The leakage information in w usually resides within a particular time interval T_l. Let $l = \{l_1, \ldots, l_{N_l}\}$ be the leakage trace during T_l, where N_l the number of sample points of l and $N_l < N_w$. The portion other than l in w is regarded as non-leakage trace and random to the intermediate data, and is denoted as $n = \{n_1, \ldots, r_{N_n}\}$. Thus, the full trace can be written as $w = \{n \bigcup l\} = \{n_1, \ldots, n_i, l_1, \ldots, l_{N_l}, n_{i+1}, \ldots, n_{N_n}\}$.

The original single bit DPA [1] computes difference of means (DOM) as

$$\Delta_w = \frac{\sum_{d_i=1} w^j}{N_{d_i=1}} - \frac{\sum_{d_i=0} w^j}{N_{d_i=0}}$$

where $N_{d_i=1}$ is the number of traces with $d_i = 1$, and $N_{d_i=0}$ the number of traces with $d_i = 0$, both under a particular key hypothesis $\hat{k}$. For the correct

key, the correlation ε_l during T_l indicates the leakage correlation. Theoretically, ε_l converges to the ideal DOM ε with N_w, i.e. $\varepsilon_l \to \varepsilon$ when $N_w \to \infty$. The correlations ε_n at other places are random correlations which converge to zero, i.e. $\varepsilon_n \to 0$ when $N_w \to \infty$. So if we separate l and n in w, then

$$\varepsilon_l = \frac{\sum_{d_i=1} l^j}{N_{d_i=1}} - \frac{\sum_{d_i=0} l^j}{N_{d_i=0}} \to \varepsilon$$

$$\varepsilon_n = \frac{\sum_{d_i=1} n^j}{N_{d_i=1}} - \frac{\sum_{d_i=0} n^j}{N_{d_i=0}} \to 0$$

ε_l of different keys are used for hypothesis test with the maximum likelihood method, i.e. the correct key hypothesis has the maximum ε_l.

Applying the principles of DPA to spectral signals in frequency domain leads to differential power spectral analysis (DPSA). Let the power spectral density (PSD) of l be $\mathbf{L} = \{\mathbf{L}_f, f = 1, \cdots, N_f\}$, where N_f is the number of points in FFT and also indicates corresponding sample frequency. DOM of DPSA at each frequency is computed as follow:

$$\varepsilon_{\mathbf{L}} = \frac{\sum_{d_i=1} \mathbf{L}^j}{N_{d_i=1}} - \frac{\sum_{d_i=0} \mathbf{L}^j}{N_{d_i=0}} \to \varepsilon' \tag{1}$$

$$\varepsilon_{\mathbf{N}} = \frac{\sum_{d_i=1} \mathbf{N}^j}{N_{d_i=1}} - \frac{\sum_{d_i=0} \mathbf{N}^j}{N_{d_i=0}} \to 0 \tag{2}$$

where ε' is the theoretical DOM of DPSA when $N_w \to \infty$.

After computation of $\varepsilon_{\mathbf{L}}$, all frequency components of $\varepsilon_{\mathbf{L}}$ are summed up (SumAll) as the overall evaluation $\hat{e} = \sum_f \varepsilon_{\mathbf{L}}$, to test key hypotheses with maximum likelihood method.

2.2 Generic Spectral Analsyis

Generic spectral analysis method is illustrated in Fig. 1. Two additional steps (in white box) are inserted into the temporal analysis method procedure. The two steps, spectral signal generation and evaluation metrics, are symmetric operations. The former is analytical and the latter synthetical.

The spectral signal generation decomposes original temporal signal into linearly independent components at different frequencies. The evaluation metric accumulates leakage at all frequencies to get the overall evaluation for hypothesis test. There are various PSD estimation methods in digital singal processing. Periodgram is a simple yet effective method, which is employed in this paper.

The straightforward evaluation metric is summation of all frequencies (SumAll), i.e. the leakage at all frequencies are added up to get the overall evaluation. In [13], the side-channel leakage information distributes along a very wide frequency rang from 10 MHz to 400 MHz almost uniformly. The evaluation metric employed in [10] [11] is summation of significance (SumSig), i.e. only correlations larger than a certain significant level are accumulated. This approach

helps to diminish the influence of noise. There are also various forms of noise in SCA such as electronic noise, data dependent switching noise etc [3]. The random correlations of wrong key hypotheses are also considerated as noise while distinguishing keys. The standard deviation of evaluations of all keys is regarded as the threshold level to distinguish leakage correlation and random correlations, and is usually set as the significance threshold. Practical experience shows that the SumAll metric is of good balance between efficiency and robustness.

The sliding-window spectrogram analysis approach can be adopted [11], when the leakage position is not known. A window is set to include a portion of the trace to generate PSD. The window slides along the trace with specified step length to generate the spectrogram with temporal information. Separated spectral analyses are performed on corresponding PSD signals from the same window. As a result, the position of window where the largest correlation rises indicates the leakage position.

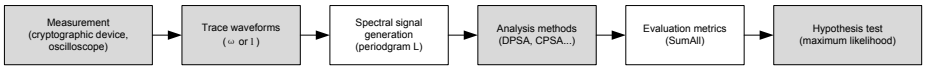


Fig. 1. Spectral analysis method.

3 Spectral Analysis on Hiding

Hiding in temporal dimension is of great practical importance. RPIs increase the amount of traces needed for DPA quadratically, yet integration DPA reduce the quadratical redundancy into linear [4]. In embedded software implementation, RPIs are inserted by integer values. Integration DPA on RPIs adds points of fixed cycle intervals in the traces, which is easy to carry out. However, on DFS [6], this integration operation is not so easy to implement, since the cycles lengths are variant and the positions of leakage in different traces do not align with fixed clock edges.

Spectral analysis has inherent integration property thanks to time-shift invariance of FFT. This makes spectral analysis a natural method against hiding in temporal dimension. A typical DFS scenario is investigated as follow.

Suppose the trace $w = \{n \bigcup l\} = \{n_1, \ldots, n_i, l_1, \ldots, l_{N_l}, n_{i+1}, \ldots, n_{N_n}\}$ is randomly shifted with DFS. For different traces, the positions of l are floating randomly. Suppose the floating range of l falls into a particular interval I called as leakage interval. Let the lower and upper bounds of the leakage interval I be i_l and i_u, i.e. the positions of l_1 and l_u. The bounds i_l, i_u are random variables with mean values u_l, u_u and standard deviations σ_l, σ_u respectively. The statistics of I depend on how many cycles it contains:

– If I contains exact one cycle, then N_l is constant because the leakage information resides within a small interval right after the clock edge. So i_l and i_u have identical statistics.
– If I contains multiple cycles, N_l is variant with different traces. i_l and i_u are independent.

For spectral signal generation, only the portion of waveform falling in the leakage interval is of interest. Denote this portion of waveform as w_I. For simplicity and without confusion, rewrite w as w_I by discarding the portion of waveform out of I. Then $w_I = \{n \bigcup l; n \in I\} = \{n_1, \ldots, n_i, l_1, \ldots, l_{N_l}, n_{i+1}, \ldots, n_{N_n}\}$. Let $\mathcal{F}(\cdot)$ denote the FFT operator.

$$\begin{aligned}
|\mathcal{F}(w_I)| &= |\mathcal{F}(\{n_1, \cdots, n_i, l_1, \cdots, l_{N_l}, n_{i+1}, \cdots, n_{N_n}\})| \\
&= |\mathcal{F}(\{n_1, \cdots, n_i, 0, \cdots, 0, 0, \cdots, 0\})| + \\
&\quad |\mathcal{F}(\{0, \cdots, 0, l_1, \cdots, l_{N_l}, 0 \cdots, 0\})| + \\
&\quad |\mathcal{F}(\{0, \cdots, 0, 0, \cdots, 0, n_{i+1}, \cdots, n_{N_n}\})| \\
&= |\mathcal{F}(\{n_1, \cdots, n_i, \})| + |\mathcal{F}(\{l_1, \cdots, l_{N_l}\})| + |\mathcal{F}(\{n_{i+1}, \cdots, n_{N_n}\})| \\
&= |\mathcal{F}(\{n_1, \cdots, n_i, n_{i+1}, \cdots, n_{N_n}\})| + |\mathcal{F}(\{l_1, \cdots, l_{N_l}\})| \\
&= |\mathcal{F}(n_I)| + |\mathcal{F}(l)|.
\end{aligned}$$

Then the PSD of w_I is

$$\begin{aligned}
\mathbf{W_I} &= |\mathcal{F}(r_I)|^2 \\
&= |\mathcal{F}(n_I)|^2 + |\mathcal{F}(l)|^2 + 2|\mathcal{F}(n_I)| \cdot |\mathcal{F}(l)| \\
&= \mathbf{N_I} + \mathbf{L} + 2N_I L.
\end{aligned}$$

According to formula (1) and (2),

$$\begin{aligned}
\varepsilon_{\mathbf{L}} &\to \varepsilon', \\
\varepsilon_{\mathbf{N_I}} &\to 0, \\
\varepsilon_{N_I L} &\to o(\varepsilon_{\mathbf{L}}) \to 0.
\end{aligned}$$

Thus

$$\varepsilon_{\mathbf{W_I}} = \varepsilon_{\mathbf{N_I}} + \varepsilon_{\mathbf{L}} + 2\varepsilon_{N_I L} \to \varepsilon'.$$

The formulas shows the integration process of spectral analysis method on the shifted leakage intervals. Although leakage positions in different traces are variant, they are all included in, thanks to the time-shift invariance of FFT. Besides, the linearity of FFT helps to eliminate noise and accumulate signal simultaneously.

In practical spectral analysis, the leakage interval is usually set as $I_S = [\mu_l - \sigma_l, \mu_u + \sigma_u]$ to include most of the leakage information and avoid too much noise. If the σ_l and σ_u of the particular DFS are larger, more noise should be

included in spectral signal generation, then the signal-noise-ratio (SNR) of the spectral analysis is less, and the DFS is more resistant to attack.

Consider two DFSs with same mean values u_l and u_u, but different standard deviations σ_l, σ_u and σ'_l, σ'_u respectively. The delay penalties are the same, but the resistances to spectral analysis are different. The leakage interval I_s may contain only one cycle or multiple cycles:

- **One cycle.** The lower and upper bounds of leakage intervals have identical statistics, $\sigma_l = \sigma_u = \sigma$ and $\sigma'_l = \sigma'_u = \sigma'$. To successfully retrieve the key with spectral analysis, the amount of traces needed for DFS with σ is σ'/σ times as much as DFS with σ'.
- **Multiple cycles.** The lower and upper bounds of leakage intervals are independent. Each bound introduces noise independently. The noise level is proportional to the length of I. To successfully retrieve the key with spectral analysis, the amount of traces needed for DFS with σ_l and σ_u is $(\sigma'_l + \sigma'_u + u'_u - u'_l)/(\sigma_l + \sigma_u + u_u - u_l)$ times as much as DFS with σ'_l and σ'_u.

4 Enhance Multi-bit Spectral Analysis

4.1 Correlation Power Spectral Analysis

To improve DPA SNR, analysis methods make use of multi-bit leakage information. The most widely adopted multi-bit power analysis method is correlation power analysis (CPA) [14]. The Hamming distance model of CPA is written as

$$l = ah(d) + b \tag{3}$$

where $h(\cdot)$ is Hamming distance function, a is scalar gain, and b is the overall noise effect independent with $h(d)$.

The Pearson correlation coefficient between the power consumption and Hamming distance is

$$\rho_l = \frac{N_T \sum l^j h^j - \sum l^j \sum h^j}{\sqrt{N_T \sum {l^j}^2 - \left(\sum l^j\right)^2}\sqrt{N_T \sum {h^j}^2 - \left(\sum h^j\right)^2}}.$$

CPA has its corresponding spectral form. Rewrite formula (3) in the frequency domain,

$$\mathbf{L} = ah(d) + \mathbf{B}$$

where $\mathbf{B}$ is the PSD of b and is also independent with $h(d)$.

Pearson correlation coefficients are computed at all frequencies of $\mathbf{L}$ for correlation power spectral analysis (CPSA):

$$\rho_{\mathbf{L}} = \frac{N_T \sum \mathbf{L}^j h^j - \sum \mathbf{L}^j \sum h^j}{\sqrt{N_T \sum {\mathbf{L}^j}^2 - \left(\sum \mathbf{L}^j\right)^2}\sqrt{N_T \sum {h^j}^2 - \left(\sum h^j\right)^2}}. \tag{4}$$

Afterward all frequency components of $\rho_{\mathbf{L}}$ are summed up to get the overall evaluation $\hat{e} = \sum_f \rho_{\mathbf{L}}$. Evaluation $\hat{e}$ is served for key hypothesis test.

Simple CPSA without evaluation metric synthesis has already been employed in [12] [15]. Here in this paper, a CPSA is exemplified on the data set of DPA contest [16]. The Pearson correlation coefficients of all frequencies of the CPSA with 5000 traces are shown Fig. 2(a), and the result along with number of traces are shown in Fig. 3(a). The evaluation metric is SumAll. One major problem with CPSA is the random correlations at higher frequencies. After FFT, the signals at the same frequency are already linear correlated. The Pearson coefficients of CPSA give large values even there are only random correlations at higher frequencies. If these random correlations are summed up with the SumAll metric, it will reduce the efficiency of CPSA.

4.2 Partitioning Power Spectral Analysis

Random correlations at higher frequencies in CPSA mainly originate from the normalization of standard deviations in the denominator of formula (4). The partitioning power analysis (PPA) [17] [18] without standard deviation normalization, has the same even better efficiency compared with CPA.

PPA attacks on multi-bit intermediate data $d_p = \{d_1, \cdots, d_{N_p}\}$, where N_p is the number of data bits PPA attacks and $N_p \leq N_d$. The traces are partitioned into groups by Hamming weights $g = h(d_p) = \{0, \cdots, N_p\}$ under different key hypotheses. Then means of groups are computed and they are summed up with different weights a_g to get the overall correlation ε_l^P.

$$\varepsilon_l^P = \sum_{g=0}^{N_p} a_g \frac{\sum_g l^j}{N_g}$$

where N_g is number of traces partitioned in group g and $\sum_g a_g = 0$. For $N_p = 4$, $a_2 = 0, -2a_0 = -a_1 = a_3 = 2a_4$, or $a_g = \{-1, -2, 0, 2, 1\}$.

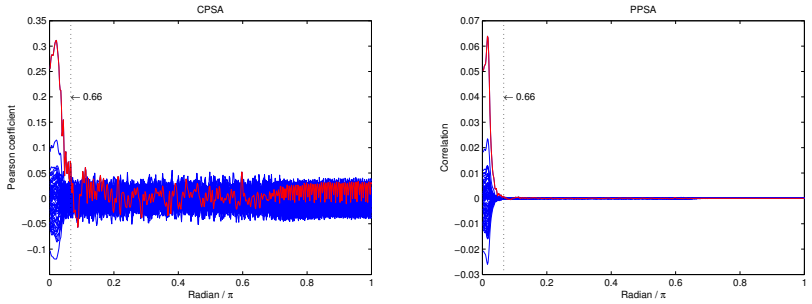
The corresponding partitioning power spectral analysis (PPSA) computes correlations at different frequencies as

$$\varepsilon_{\mathbf{L}}^P = \sum_{g=1}^{N_p} a_g \frac{\sum_g \mathbf{L}^j}{N_g}.$$

Then all frequency components of are summed up (SumAll) as the overall evaluation $\hat{e} = \sum_f \varepsilon_{\mathbf{L}}^P$ for hypotheses test.

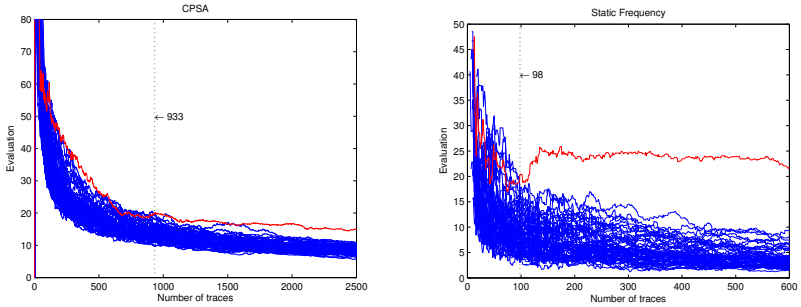
A PPSA is performed on the same data set with the same order of traces as CPSA in Section 4. The correlations of PPSA with 5000 traces are shown in Fig. 2(b), and the results with number of traces are shown in Fig. 3(b). Compared to CPSA, there are no large random correlations at the higher frequencies. The characteristic frequencies where the correlation of correct key begins to sink into the random correlations of CPSA and PPSA are the same, which indicates that the leakage signals extracted by both methods are the same. The difference is

about the noise. The results in Fig. 3 show that amount of traces needed to get the same SNR level with CPSA is nearly 10 times as much as PPSA.



(a) (b)

Fig. 2. (a) Pearson correlation coeffient of CPSA . (b) Correlation of PPSA. The red curves are for correct key and blue curves for wrong keys.



(a) (b)

Fig. 3. Results of (a) CPSA. (b) PPSA. The red curves are for correct key and blue curves for wrong keys.

5 Experimental Results

The original data set is from DPA contest [16], which contains power consumption traces of an unprotected DES crypto-processor on a SoC in ASIC with static frequency. In general ASICs or micro-controllers, the power consumption leakage information all resides within a short time interval right after the clock edges. To generate traces with DFS, random delays of zero values are

inserted into the original trace before the clock edges. DFS traces generated by this method share the same characteristic of randomly shifted leakage with actual DFS traces. The only difference is the actual DFS traces have very small power consumption for the random delays between shifted clock cycles, while the generated DFS traces have zero values. However, the signal, i.e. the leakage information residing right after the clock edges is the same.

Data sets for two kinds of random DFS are generated. The first DFS employs the most commonly used uniform distribution. The random delays follow independently uniform distribution with mean value μ_0 and standard deviation σ_0. For one single trace with 32 frequency switchings, the overall delay is the accumulation of 32 independent uniform delays. So the standard deviation of the overall delay σ_Σ is much less than σ_0, which leads to efficiency degeneration. The second DFS employs more efficient floating mean method [7] with parameters a and b. The standard deviation of the overall delay with the floating mean method does not diminish with accumulation.

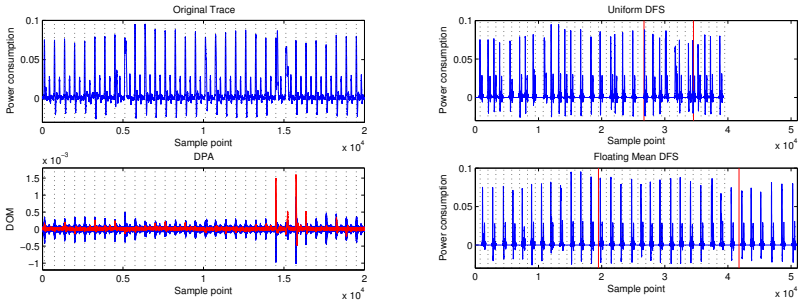
The parameters used for random delay generation in this paper is as follow. Clock cycle length of the original traces is $T = 625$. The statistics of one single random delay of the uniform DFS are mean value $\mu_0 = 625$, and standard deviation $\sigma_0 = 360$. Parameters for floating mean DFS are $a = 1250$ and $b = 250$. The standard deviations of lower and upper bounds of leakage interval I for uniform DFS and floating mean DFS are shown in Table 1. Floating mean DFS has larger standard deviations than the uniform DFS, thus is more resistant to spectral analysis.

Table 1. Parameters of DFSs

	Uniform		Floating Mean	
	i_l	i_u	i_l	i_u
μ	14376	16253	14353	16244
σ	1730	1838	6653	7520

One trace from the original DPA contest data set and the DPA leakage positions are shown in Fig. 4(a). The red curve is for DOM of correct key and blue for wrong keys. One trace with uniform DFS and one with floating mean DFS are shown in Fig. 4(b). The red lines indicates the positions of lower and upper bounds of leakage interval I in spectral analysis on the DFSs. The range of leakage interval with floating mean DFS is much wider than uniform DFS.

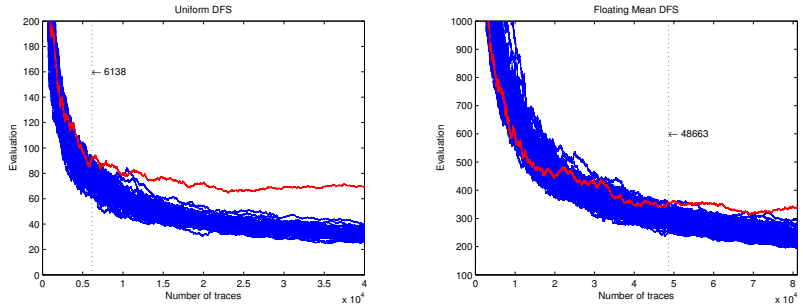
The temporal analysis methods including CPA and PPA on the DFS traces all fail to retrieve the correct key with up to 81000 traces. PPSAs are performed on the original data with static frequency, generated data with uniform DFS and floating mean DFS. The PPSAs attack on the first S-Box of the 16th round in DES. The PPSAs process the data set with the same orders. Evaluation metric is SumAll. The results are shown in Fig. 5(a) and 5(b). According to the analysis in section 3, the ratio of amount of traces needed to retrieved the correct key



(a) (b)

Fig. 4. (a) Up: original trace with static frequency; Down: DPA leakage positions. (b) Up: generated trace with uniform DFS; Down: generated trace with floating mean DFS. The dashed lines are nominal clock edges.

for spectral analysis on two DFSs is $(\sigma_l' + \sigma_u' + u_u' - u_l')/(\sigma_l + \sigma_u + u_u - u_l) = (7520+6653+16244-14353)/(1730+1838+16253-14376) = 2.95$. While in Fig. 5, the ratio is $48663/6138 = 7.92$. The empirical value does ont fit the theoretical value very well, because more leakages are not included in the leakage interval I with the floating mean DFS than uniform DFS. Compared to results in [7] with DPA where the ratio is $45000/2500 = 18$, the PPSA gives much better results.



(a) (b)

Fig. 5. PPSA on (a) uniform DFS and (b) floating mean DFS. The red curves are for correct key and blue for wrong keys.

6 Conclusions

We proposed the spectral analysis method with evaluation metric on hiding in temporal dimension such as RPIs and DFS. The spectral analysis has inherent in-

tegration property thanks to shift-invariance of FFT. We proposed PPSA method to enhance the multi-bit spectral analysis. PPSA does not generate large random correlations at higher frequencies, and is much more efficient than CPSA. Experimental results show PPSA break down DFS. Hiding as a countermeasure can increase the amount of traces needed for successful attacks, but it is not always safe and should be implemented together with other countermeasures such as masking to ensure security.

References

1. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, London, UK, Springer-Verlag (1999) 388–397
2. Agrawal, D., Archambeault, B., Rao, J., Rohatgi, P.: The EM side channel(s). In: Cryptographic Hardware and Embedded Systems - CHES 2002. (2003) 29–45
3. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Springer-Verlag New York, Inc., Secaucus, NJ, USA (2007)
4. Clavier, C., Coron, J.S., Dabbous, N.: Differential power analysis in the presence of hardware countermeasures. In: CHES '00: Proceedings of the Second International Workshop on Cryptographic Hardware and Embedded Systems, London, UK, Springer-Verlag (2000) 252–263
5. Bucci, M., Luzzi, R., Guglielmo, M., Trifiletti, A., AG, I., Graz, A.: A countermeasure against differential power analysis based on random delay insertion. In: IEEE International Symposium on Circuits and Systems, 2005. ISCAS 2005. (2005) 3547–3550
6. Yang, S., Wolf, W., Vijaykrishnan, N., Serpanos, D.N., Yuan, X.: Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach. In: Design, Automation and Test in Europe, 2005. Proceedings. (2005) 64–69 Vol. 3
7. Coron, J., Kizhvatov, I.: An efficient method for random delay generation in embedded software. In: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, Springer (2009) 170
8. Homma, N., Nagashima, S., Sugawara, T., Aoki, T., Satoh, A.: A high-resolution phase-based waveform matching and its application to side-channel attacks. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **E91-A** (2008) 193–202
9. Nagashima, S., Homma, N., Imai, Y., Aoki, T., Satoh, A.: DPA using phase-based waveform matching against random-delay countermeasure. In: Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on. (2007) 1807–1810
10. Gebotys, C., Tiu, C., Chen, X.: A countermeasure for EM attack of a wireless PDA. In: Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on. Volume 1. (2005) 544–549 Vol. 1
11. Gebotys, C.H., Ho, S., Tiu, C.: EM analysis of Rijndael and ECC on a wireless Java-based PDA. In: Cryptographic Hardware and Embedded Systems – CHES 2005. (2005) 250–264
12. Plos, T., Hutter, M., Feldhofer, M.: Evaluation of side-channel preprocessing techniques on cryptographic-enabled HF and UHF RFID-tag prototypes. In: Workshop on RFID Security 2008, July 9th-11th, 2008, Budapest. (2008)
13. Hutter, M., Mangard, S., Feldhofer, M.: Power and EM attacks on passive RFID devices. In: Cryptographic Hardware and Embedded Systems – CHES 2007. (2007) 320–333

14. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Cryptographic Hardware and Embedded Systems - CHES 2004. (2004) 135–152
15. Hutter, M., Medwed, M., Hein, D., Wolkerstorfer, J.: Attacking ECDSA-Enabled RFID Devices. In: Proceedings of the 7th International Conference on Applied Cryptography and Network Security, Springer (2009) 534
16. DPA Contest 2008/2009: (http://www.dpacontest.org/)
17. Le, T.H., Cldire, J., Canovas, C., Robisson, B., Servire, C., Lacoume, J.L.: A proposition for correlation power analysis enhancement. (2006) 174–186
18. Le, T.H., Canovas, C., Cldire, J.: An overview of side channel analysis attacks (2008) 1368319 33-43.