# Signal Pre-Processing to Increase DPA Success on GALS Architectures

Marcelo Fay[#], Luciano Loder [#*], Adão de Souza Junior[*], Rafael Soares[#]

[#]*Universidade Federal de Pelotas – UFPel*
*Rua Gomes Carneiro, 1 Pelotas – RS – Brazil*
[1]{mlcfay,llloder,rafael.soares}@inf.ufpel.edu.br

[*]*Instituto Federal Rio-Grandense - IFSUL*
*Praça 20 de Setembro, Pelotas-RS - Brazil*
[2]adaosjr@gmail.com

***Abstract*— This paper presents a preliminary investigation of DSP techniques to perform frequency sorting, realignment of power traces and noise reduction before Differential Power Analysis (DPA) attacks. DPA has been effective in revealing cryptographic key on cryptosystems. In this sense, several methods to prevent the action of these attacks have been proposed in order to avoid information leakage. Random delay insertion (RDI) causes misalignments in the time domain hindering the action of DPA. However, some Digital Signal Processing (DSP) techniques have being proven efficient as countermeasures to improve DPA rate of success. The GALS pipeline architectures uses random clock frequency and simultaneous processing of two or more pipeline stages to hide leakage information. The results show that applying digital filters and correlation phase adjustment may be efficient to improve DPA attacks.**

***Keywords* — cryptography, side channel attacks, DPA, DEMA, security, DSP.**

## I. INTRODUCTION

Side channel attacks (SCA) are a major concern for cryptographic circuit designers since it was presented by Kocher [1]. SCA exploits leakage information on side channels such as power consumption, electromagnetic radiation, or time propagation to derive confidential information, specifically secret keys used in cryptographic systems. Differential Power Analysis (DPA) uses simple statistical techniques that are almost independent of the cryptographic algorithm implementation to correlate data and power consumption. Differential Electromagnetic Analysis (DEMA) follows the same principle, but measures the electromagnetic radiation of circuits, according to Gebotys et al [2].

DPA evaluates the power signature caused by execution of an intermediate operation of the cryptographic system for a specific plaintext data input, and compares all power signatures obtained by the execution of a set of different plaintexts. As the hardware device is designed according to synchronous paradigm, all operations are executed sequentially in the same order and spending the same runtime. In this way, the power traces are aligned and the attacker is able to compare them.

Since then a lot of proposes have been presented to protect cryptographic circuits from SCA, commonly known as countermeasures [3][4][5][6][12]. Moreover, several works are presented to improve the efficiency of SCA and find vulnerabilities in systems protected with some kind of countermeasure [9][10].

One of the strategies to avoid DPA is execute the cryptographic algorithm at different time instants aiming to scatter power waveforms by inserting random delays. In [3] random delay insertion (RDI) is applied in the software level, interleaving the cryptographic algorithm instructions with dummy instructions. In [4] RDI is applied in the hardware level by the addition of logic gates to the datapath. RDI can be implemented by driving the system at different clock frequencies as mentioned in [8].

Nagashima et al. in [10] prove to be possible unveil secret key on cryptographic systems protected by RDI countermeasure through phase only correlation (POC). Generally pre-processing with signal processing techniques can be effective to align power traces before apply DPA [9].

Combine RDI with extra hardware to compute a cryptographic algorithm is effective against classical DPA. In [12] the authors proposed an architectural countermeasure that implements a hardware pipeline using global asynchronous locally synchronous (GALS) design style able to compute each pipeline stage driven by random clock frequencies.

In a recently search in the literature, there is nothing related using DSP techniques to improve DPA on GALS architecture and this paper brings some of them to this unexplored area.

In this paper is presented a preliminary evaluation of GALS pipeline architecture against DPA attacks using pre-processing techniques such as POC and digital filter. This article is structured as follows: Section II explains the DPA analysis. Section III shows the GALS pipeline architecture. An overview of digital signal processing techniques is presented on Section IV. The experiments and results are discussed on Section V and some conclusions are presented on Section VI.

## II. DPA ANALYSIS

The information leaked in power traces occurs at the transistor level of the system. Logic gates implemented with CMOS technology have distinct power consumption when switching from logic levels '0' to '1' or when switching from '1'

to '0'. An attacker can explore such information by executing on cryptographic system a collection of plaintexts inputs PTI[i], with i = 1, …, N, and measuring the power consumed by the device, obtaining T[i][j] power traces, where j is the discrete time index of the values sampled. The next step is to sort power traces according to the type of switching caused by input data. Thereby, it is necessary to define an intermediary function of the algorithm that relates plaintext and the unknown cryptographic key, the target of attacks. A selection function D(K, P[i]), where K is a part of cryptographic key and P[i] is a part of $P_{TI}[i]$, allows to calculate the intermediate value for all possible K. The power traces are then separate in two groups for a hypothesis of K according to the intermediate value of a specific bit chose to be the target. One group contains all power traces which the value is zero and another contains the rest of power traces where the value is one. Thereafter, the average is calculated for each one of the traces groups, producing $M_0[i][j]$ and $M_1[i][j]$. The next step, a differential trace $T_H[i][j]$ for an hypothetic value of K is obtained by subtraction $M_1[i][j]$ - $M_0[i][j]$. For a correct hypothesis of K, at the time point where the operation target occurs should appear a peak and to the others a slight flat signal. This procedure is repeated for all hypothesis of K. At the end, there are a differential trace $T_H[i][j]$ to each K hypothesis. Comparing all differential traces, the correct hypothesis of key is that has the highest peak. This process is shown in Fig. 1.

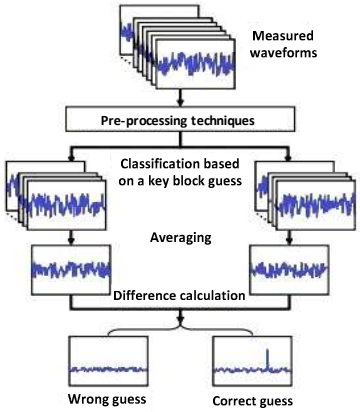


Fig. 1 Proposed DPA using a pre-processing DSP techniques.

## III. GALS PIPELINE ARCHITECTURE

The GALS pipeline presented by [12] is an architecture that implements a cryptographic algorithm in hardware according to a globally asynchronous locally synchronous design style to avoid leakage information. This architecture is composed by synchronous logic blocks that communicate each other using asynchronous interfaces as depicted in Fig 1, also known as *synchronous islands*.

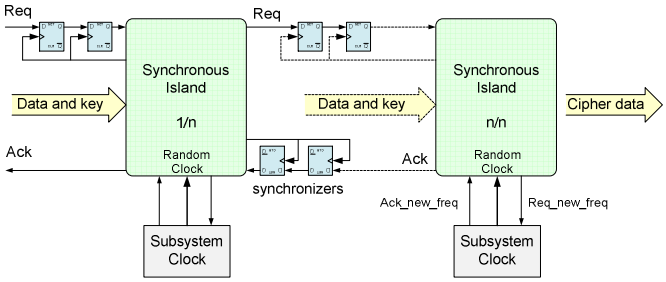


Fig. 2 Structure of the GALS pipeline architecture [12].

Each island is able to process one or more rounds of the algorithm. The islands can be driven by a global or a local clock signal. A subsystem clock is responsible to generate clock signals with different frequencies. A Linear Feedback Shift Register (LFSR) defines the clock signal that drives the island at end of data encryption. Thus, the architectural proposal avoids SCA through execution of pipeline stages on different frequencies in addition to the simultaneous executions of the islands causing amplitude distortions in the power traces [12]. The processing in different clock frequencies causes misalignment in the time domain besides provoke a distortion in the amplitude.

## IV. PRE-PROCESSING TECHNIQUES

Since the power traces are misaligned in time and have different clock frequencies, DPA attack is not able to unveil a secret cryptographic key on GALS pipeline architectures. Three different pre-processing techniques were used in this work to improve DPA success rate: phase-based waveform matching, as presented by [11]; frequency classification and low pass filter de-noising.

### *A. Phase based waveform matching*

Consider two signals, *f(n)* and *g(n)*, where we assume that the index range is $n = -Z, \ldots, Z$ for mathematical simplicity, and hence the length of waveforms $L = 2Z + 1$. Let *F(k)* and *G(k)* denotes the Discrete Fourier Transforms (DFTs) of the two waveforms [10]. *F(k)* and *G(k)* are given by

$$F(k) = \sum_{n=-Z}^{Z} f(n) W_L^{kn} = A_F(k) e^{j\theta_F(k)} \quad (1)$$

$$G(k) = \sum_{n=-M}^{M} g(n) W_L^{kn} = A_G(k) e^{j\theta_G(k)} \quad (2)$$

where $W_N = e^{-j\frac{2\pi}{L}}$, $A_F(k)$ e $A_G(k)$ are amplitude components, and $e^{j\theta_F(k)}$ and $e^{j\theta_G(k)}$ are phase components [10]. The cross-phase spectrum (or normalized cross spectrum) $R_{FG}(k)$ is defined as

$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{|F(k)G(k)|} = e^{j\theta FG(k)} \quad (3)$$

where $\overline{G(k)}$ denotes the complex conjugate of $G(k)$ and $\theta_{FG}(k) = \theta_F(k) - \theta_G(k)$. The POC function $r_{fg}(n)$ is the Inverse Discrete Fourier Transform (IDFT) of $R_{FG}(n)$ and is given by

$$r_{fg}(n) = \frac{1}{L}\sum_{k=-Z}^{Z} R_{FG}(k) W_L^{-kn} \tag{4}$$

If there is a similarity between two waveforms, the POC function gives a distinct sharp peak. (When $f(n) = g(n)$, the POC function becomes the Kronecker delta function.) If not, the peak drops significantly. The height of the peak can be used as a good similarity metric for the waveform matching, and the location of the peak shows the translational displacement between the two waveforms.

Now consider $f_c(t)$ as a waveform defined in continuous space with a real number index $t$. Let $\delta$ represents a displacement of $f_c(t)$ so the displaced waveform can be represented as $f_c(t-\delta)$. Assume that $f(n)$ and $g(n)$ are spatially sampled waveforms of $f_c(t)$ and $f_c(t-\delta)$, and are defined as

$$f(n) = f_C(t)\big|_{t=nT} \tag{5}$$

$$g(n) = f_C(t-\delta)\big|_{t=nT} \tag{6}$$

where $T$ is the sampling interval and the index range is given by $n = -Z, \ldots, Z$. For simplicity, we assume $T = 1$. The cross-phase spectrum $R_{FG}(k)$ and the POC function $r_{fg}(n)$ between $f(n)$ and $g(n)$ will be given by

$$R_{FG}(k) = \frac{F(k)\overline{G(k)}}{\left|F(k)\overline{G(k)}\right|} \cong e^{j\frac{2\pi}{L}k\delta} \tag{7}$$

$$r_{fg}(k) = \frac{1}{N}\sum_{k=-Z}^{Z} R_{FG}(k) W_L^{-kn} \cong \frac{\alpha}{L}\frac{\sin\{\pi(n+\delta)\}}{\sin\left\{\frac{\pi}{L}(n+\delta)\right\}} \tag{8}$$

The peak position $\delta$ of the POC function corresponds to the displacement between the two waveforms [10].

### B. Frequency Separation

The FFT can be used in order to evaluate the clock frequency of a synchronous circuit. The FFT shows the frequency components of a given signal and since all operations in a synchronous circuit depends on the clock frequency, the highest peak of the FFT should be in the operating clock frequency. We realized some experiments and concluded that this assumption is correct. For a more accurate evaluation, boundary effects must be considered. To reduce the boundary effects, the power traces are processed with a window function before the FFT process. An important consideration is that this step is performed before the application of the moving average filter, because this filter attenuates the higher frequencies.

### C. Moving Average Filter

To reduce the influence of the frequencies above the desired frequency, it has been used a moving average filter.

This filter consists of a low-pass Finite Impulse Response (FIR) filter that is used to remove the frequencies above the desired frequency to reduce the noise in order to improve the DPA analysis. This filter is defined by following equation.

$$y[n] = \frac{1}{N}\sum_{k=0}^{N-1} x[n-k] \tag{9}$$

Below is presented two waveforms, as Fig. 3 and Fig. 4 respectively, in order to verify the efficiency of this technique. The window used has n=100 taps. These figures depict the power consumption of the FPGA computing the first eight rounds of DES algorithm. Each round executed by the architecture is identified by a discrete number in the traces.

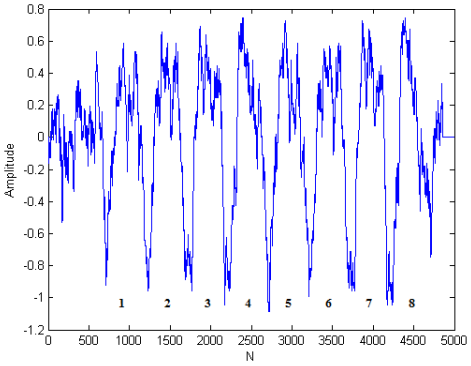


Fig. 3 Waveform before moving average filter.

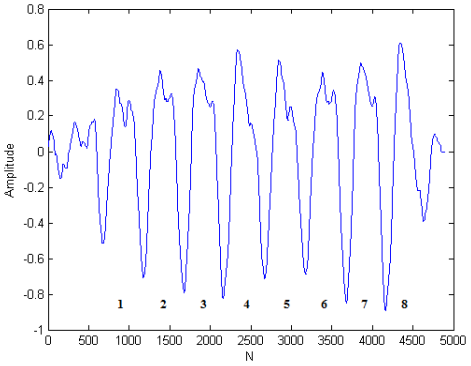


Fig. 4 Waveform after moving average filter.

## V. Experimentation

In this paper we used a collection of traces acquired in [12], so the acquisition step was not performed in this work. Since the power traces obtained had different clock frequencies, frequency classification was performed.

Applying FFT to classify the traces, two clusters of frequencies clearly emerged: one of the groups had a frequency range between 38MHz and 42MHz, and the other between 55MHz and 60MHz. This work was applied in the group with range between 38MHz and 42MHz.

Firstly, an extraction of the first stage of trace is performed. Since power traces obtained had a RDI countermeasure, then

the computation starts in different instants of time for each trace. Thus, the starting point of the computation has been detected using an amplitude criterion.

Moreover, the trace still had a small amount of misalignment. Using POC-based waveform matching in this set, we aligned the entire set accordingly with one reference trace. The longer the trace is, worst will be the misalignment due the frequency difference between traces. To improve even more the results, was used a moving average filter before the DPA attack. The results are summarized in Table 1. In the first row below the substitution box (referred as sbox in the table) is the correct cryptographic key, the second row below is the guessed cryptographic key, the third row below is the rank of the correct key and, at last row, is the minimal number of power traces needed to unveil the respective sbox. The rank sorts the probabilities of all possible keys for each sbox. In a successful attack, the rank of the key guessed must be 1, otherwise the attack fails. Table 1.a shows that only order traces of the same or very close frequencies is not efficient to apply a successful DPA. Table 1.b depicts that the phase alignment is needed and POC is efficient to realign traces. Table 1.c presents the improvement of the rate of a successful DPA when high frequency noise is mitigated.

a. DPA without any pre-processing technique.

| sbox1 | sbox2 | sbox3 | sbox4 | sbox5 | sbox6 | sbox7 | sbox8 |
|---|---|---|---|---|---|---|---|
| 24 | 63 | 33 | 51 | 09 | 54 | 53 | 61 |
| 21 | 03 | 13 | 20 | 53 | 35 | 33 | 42 |
| 40 | 21 | 31 | 08 | 61 | 25 | 32 | 5 |
| - | - | - | - | - | - | - | - |

b. DPA with POC-based waveform matching without moving average filter.

| sbox1 | sbox2 | sbox3 | sbox4 | sbox5 | sbox6 | sbox7 | sbox8 |
|---|---|---|---|---|---|---|---|
| 24 | 63 | 33 | 51 | 09 | 54 | 53 | 61 |
| 24 | 63 | 33 | 51 | 11 | 54 | 53 | 26 |
| 01 | 01 | 01 | 01 | 01 | 01 | 01 | 56 |
| 6943 | 22130 | 29752 | 12211 | 27238 | 15987 | 33511 | - |

c. DPA with POC-based waveform matching and moving average filter.

| sbox1 | sbox2 | sbox3 | sbox4 | sbox5 | sbox6 | sbox7 | sbox8 |
|---|---|---|---|---|---|---|---|
| 24 | 63 | 33 | 51 | 09 | 54 | 53 | 61 |
| 24 | 63 | 33 | 51 | 09 | 54 | 53 | 38 |
| 01 | 01 | 01 | 01 | 01 | 01 | 01 | 22 |
| 1290 | 12932 | 18836 | 4790 | 21516 | 15987 | 13886 | - |

Table 1. Results of some DPA attacks

## VI. CONCLUSIONS

Architectures GALS pipelines are proposed to hide information leaked through power consumption and electromagnetic radiation combining random frequency and noise addition to misalign and disturb power traces. Soares et al. [12] proved that this countermeasure is effective against DPA attacks. However, there are some digital signal processing techniques able to remove misalignment and noise present on power or electromagnetic traces exploring the remaining vulnerabilities. This paper presented a preliminary investigation of DSP techniques to perform frequency sorting, realignment of power traces and noise reduction before DPA attacks. The results show that grouping traces produced with very close clock frequencies combined with phase correlation is effective to ensure DPA success. The attack has been able to reveal 7 out of 8 intermediate keys. In addition, the high frequency noise reduction was able to decrease the number of traces required to unveil the intermediate keys.

Although the sbox8 key was not able to be revealed its position in the hypotheses ranking was improved from 56 to 22 when moving average filter was applied. This preliminary evaluation proves to be efficient to improve DPA attacks against random frequency misalignment traces. In future works, we will use short time-frequency transforms together with interactive sorting and clustering techniques to attack the remaining traces. We also intend to evaluate the robustness of the combination of two pipeline stages processing simultaneously with random clock frequencies to hide leakage information against DPA attacks.

## ACKNOWLEDGMENT

This work was supported by FAPERGS ARD-2011 and program PIBIC/CNPQ.

## REFERENCES

[1] P. Kocher. “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and others Systems”. In: 16th International Cryptology Conference on Advances in Cryptology (CRYPTO’96), Aug 1996, pp. 104-113.

[2] Gebotys, C.; Tiu, C.; Chen, X. "A Countermeasure for EM Attacks of a Wireless PDA". In: International Conference on Information Technology: Coding and Computing, 2005, pp. 544-549.

[3] Clavier, J. Coron, and N. Dabbous. “Differential power analysis in the presence of hardware countermeasures”. In: Cryptographic Hardware Embedded Systems, 2000, pp. 252 – 263.

[4] Guilley, S.; Sauvage, L.; Danger, J.; Graba, T.; Mathieu, Y. "Evaluation of Power-Constant Dual-Rail Logic as a Protection of Cryptographic Applications in FPGAs". In: 2nd International Conference on Secure System Integration and Reality Improvement, 2008, pp. 19-23.

[5] Moradi, A.; Khatir, M.; Salmasizadeh, M.; Shalmani, M. "Charge Recovery Logic as a Side Channel Attack Countermeasure". In: 10th International Symposium on Quality of Electronic Design, 2009, pp. 686-691.

[6] Baddam, K.; Zwolinski, M. "Evaluation of Dynamic Voltage and Frequency Scaling as a Differential Power Analysis Countermeasure". In: 20th International Conference on VLSI Design, 2007, pp. 854-862.

[7] Lu, Yingxi; O'Neill, Maire P. “FPGA implementation and analysis of Random Delay Insertion Countermeasure against DPA”. In: International Conference on Field-Programmable Technology, 2008, pp. 201-208.

[8] Avirneni, Naga Durga Prasad; Somani, Arun K. “Countering power analysis attacks using reliable and aggressive designs”. *IEEE Transactions on Computers*, vol. 99, pp. 1. 2013.

[9] Le, Tanh-Ha; Clédière, Jessy; Servière,Christine; Lacoume, Jean-Louis; *How can signal processing benefit Side Channel Attacks?*. In: Workshop on Signal Processing Applications for Public Safe, 2007, pp. 1-7.

[10] Nagashima, Sei; Homma, Naofumi; Imai, Yuichi; Takafumi, Aoki; Satoh, Akashi. “DPA using phase-based waveform matching against random-delay countermeasures”. In: IEEE International Symposium on Circuits and Systems, 2007, pp 1807-1810.

[11] Nagashima, Sei; Homma, Naofumi; Imai, Yuichi; Takafumi, Aoki; Satoh, Akashi. “High-resolution side channel attack using phase-based waveform matching”. In: Workshop on Cryptographic Hardware and Embedded Systems 2006 (CHES 2006), 2006, pp 187-200.

[12] Soares, Rafael I.” Arquiteturas GALS pipeline para criptografia robusta a ataques DPA e DEMA”. Porto alegre, 2011.