# An Integrated Validation Environment for Differential Power Analysis

Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre

# An Integrated Validation Environment for Differential Power Analysis

G. Di Natale, M.-L. Flottes, B. Rouzeyre

giorgio.dinatale@lirmm.fr

*LIRMM - CNRS - University of Montpellier II – France*

*http://www.lirmm.fr/*

## Abstract

*Integrated systems represent the most common solution for storage and transmission of confidential data. However, cryptographic devices can be subject to passive attacks that consist in retrieving secret data by observing physical properties of the device (e.g. execution time, power consumption, electromagnetic field). An attack based on power analysis for instance is very efficient and relatively easy to perform. Designers implement this attack in order to see if their design meets the requirements in terms of resistance. In this project we propose a complete and flexible environment for validation of a digital device when attacked by means of Differential Power Analysis.*

## 1. Introduction

Side-channel attacks exploit the fact that the cryptographic device leaks physical information during data processing. This physical leakage (e.g., power dissipation, electromagnetic emanation, timing information,... ) can be captured externally and used for compromising confidential data as the secret key of a symmetrical cryptographic system for instance.

Side-channel attacks such as Simple and Differential Power Analysis [1] have become popular since, without proper countermeasures, they require the knowledge of the algorithm but not its physical implementation.

DPA is also performed by designers in order to evaluate the susceptibility of their design to this attack, after design modification for mission mode improvement or after implementation of new countermeasures.

From the designer point of view, it is thus crucial to simulate such attacks since the simulation allows estimating the difficulty of performing a real attack before circuit manufacturing and without the drawbacks of the real experiments (experiment setup, noise …).

In this project we describe a new flexible integrated simulation-based environment that allows validating a digital circuit when the device is attacked by means of this attack. With respect to the one proposed in [2], and with respect to all the custom-solutions implemented for a specific design, our solution allows to set most of the parameters and features (e.g., power consumption models, observation mechanisms, and statistical analysis) in such a way that different forms of DPA can be experimented.

## 2. DPA Environment

Figure 1 sketches the basic flow of the validation environment. It is composed of two main parts: *Synthesis & Simulation* environment for acquisition of simulated power traces and DPA Suite for performing DPA attack.

The synthesis & simulation environment takes the VHDL description of the circuit and automatically generates all the scripts required to synthesize it with a given target library. Then it generates the scripts required to perform the transistor level simulation of the circuit for a user defined vector set.

The simulation is performed in such a way that it is possible to gather all the measures that an attacker could have obtained on a real device.

DPA Suite is the core of the environment. It is composed of two main tools: *dpa* and *keyexplore*.

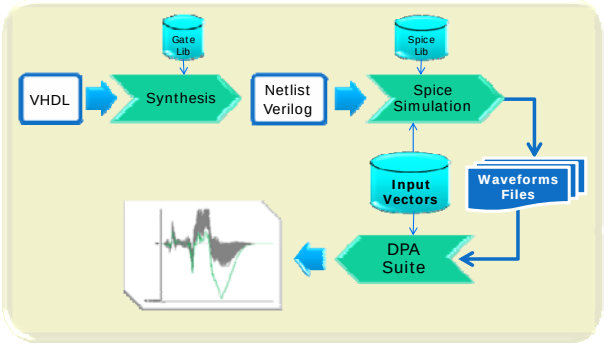


**Figure 1:** DPA environment

Starting from the waveforms and the input vectors, dpa tool generates the DPA traces for each key supposition. In particular, for each key supposition and for the target bit (or bits), it classifies the waveforms based on the logical function implemented by the circuit and according to the chosen power consumption model. dpa handles the three power consumption models presented in Section 2 (Hamming weight, rising transition, and Hamming distance).

dpa is able to target one or more output bits of the circuit's SBox. For instance, up to the 8 AES Sbox output bits can be considered simultaneously. The number of target bits is a user parameter.

Furthermore, for multi-bit DPA we implemented two different methods to calculate the DPA trace:

- Independent: the selection function is applied independently to each target bit ($b_1$, …, $b_n$). In this way the set of waveforms are partitioned in two sets for each target bit ($P_{A1}$ and $P_{B1}$ for bit $b_1$, …, $P_{An}$ and $P_{Bn}$ for bit $b_n$). The final DPA trace is computed as follows:

$$DPA(t) = \sum_{i=1}^{n} \frac{\sum_{x=1}^{|P_{Ai}|} \frac{I_x(t)}{|P_{Ai}|} - \sum_{x=1}^{|P_{Bi}|} \frac{I_x(t)}{|P_{Bi}|}}{n}$$

- All together: waveforms are included in the packet $P_A$ (or packet $P_B$) iff the selection function is 1 (respectively 0) for all the considered target bits. For instance, using the Hamming weight-based selection function and 4 target bits, the waveforms corresponding to the input value that generates "1111" on the target bits are included in the packet $P_A$, while those leading to the value "0000" are included in the packet $P_B$. All the other waveforms are ignored.

The *keyexplore* tool allows detecting the value of the secret key starting from the DPA traces. It associates the secret key to the trace with largest power consumption. We implemented it according to three criteria:

- Amplitude: the curve with the highest absolute value is considered as the one corresponding to the correct key;
- Integral: the curve with the highest average value is considered as the one corresponding to the correct key;
- Time: the curve that has the longest time period during which the curve is the highest is considered as the one corresponding to the correct key.

*Keyexplore* also can generate GIF images and movies containing all the DPA calculated traces or the temporal evolution of the DPA trace related to the number of input vectors required to discover the key.

## 3. Experimental Results

Table 1 shows the time needed for the transistor level simulation (3rd column) and for the execution of the DPA Suite (dpa + keyexplore, 4th column) for several circuits implemented using a 130nm technology provided by STMicroElectronics. In all cases, we performed multi-bit DPA taking into account all the output bits of one SBox, i.e. 4 bits for DES and 8 bits for AES. None of the analyzed architecture implements DPA countermeasures.

To validate the resistance of a design against DPA attack it is necessary to compute the number of input vectors required to conduct a successful attack. For instance, figure 2 depicts the relative position of the curves corresponding to the correct key for different input sequence length. The curve corresponding to the right key is the black one, while all the others are in grey. The sequence we used is composed of 256 vectors, from 0 to 255. First, it can be seen that at least the first 56 patterns of this sequence (from 0 to 55) are necessary to distinguish the curve corresponding to the right key. Secondly, the longer the input sequence, the more evident is the curve corresponding to the right key. The "Time" criterion has been used to identify the correct key.

**Table 1:** Performance evaluation

| Arch. | #Inputs | Simulat. | DPA |
|---|---|---|---|
| Sbox DES | 64 | 27 sec | 4 sec |
| Sbox DES | 4034 | 158 sec | 79 sec |
| Sbox AES | 256 | 86 sec | 14 sec |
| AES | 256 | 12 min | 140 sec |

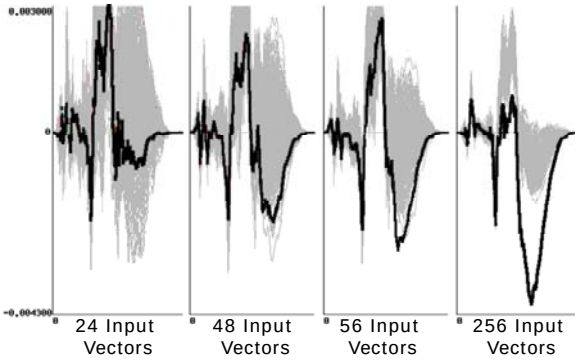


**Figure 2:** DPA efficiency vs sequence length.

## 4. Conclusion

Differential Power Analysis attacks are very effective and not expensive to implement. Therefore, in the context of secure circuits, it's mandatory to validate the resistance of a design against this type of attack.

In this paper we proposed an integrated validation environment for the DPA based on simulation. It quickly allows evaluating the resistance of the circuit without resorting to the physical implementation. With respect to custom-simulators implemented for a specific project, our solution implements most of the parameters and features of the Differential Power Analysis and can be used in a general way, for any design and countermeasure.

In particular, it deals with:

- Real measures or simulated data;
- 3 different power consumption models;
- Any number of target bits;
- Different combinations of the results of each target bit;
- Reports on packets statistics;
- 3 criteria for DPA traces analysis;
- Graphical output.

Since the simulation is performed at transistor level, the power consumption waveforms are very accurate and in agreement with the physics.

Moreover, the circuit simulation is noise-free while practical measurements are affected by different sources of noise. Consequently, an evaluation suite as the one we proposed in this paper is very useful for the designer: if the design is proved to be DPA-resistant, the actual device will be insensitive too.

## 5. References

[1] G. Di Natale, M.-L. Flottes, B. Rouzeyre, "An Integrated Validation Environment for Differential Power Analysis", IEEE International Symposium on Electronic Design, Test & Applications (DELTA 2008), Hong Kong, January 2008, pp. 527-532

[2] M. Bucci, M. Guglielmo, R. Luzzi and A. Trifiletti, "A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors", PATMOS 2004, LNCS 3254, Springer-Verlag, pp. 481-490, 2004.