SECNUM: an Open Characterizing Platform for Integrated Circuits

Morgan Bourrée, Florent Bruguier, Lyonel Barthe, Pascal Benoit, Philippe Maurine, Lionel Torres

▶ **To cite this version:**

Morgan Bourrée, Florent Bruguier, Lyonel Barthe, Pascal Benoit, Philippe Maurine, et al.. SECNUM: an Open Characterizing Platform for Integrated Circuits. European Workshop on Microelectronics Education (EWME), May 2012, Grenoble, France. hal-01139176

HAL Id: hal-01139176
https://hal.science/hal-01139176

Submitted on 3 Apr 2015

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

SECNUM: an Open Characterizing Platform for Integrated Circuits

Morgan Bourrée, Florent Bruguier, Lyonel Barthe, Pascal Benoit, Philippe Maurine, Lionel Torres
LIRMM – UM2 - CNRS
e-mail: {firstname.lastname}@lirmm.fr

Abstract:
Nowadays, digital systems are becoming the main information support. This evolution implies a growing interest for the domain of cryptology regarding the conception of these systems. The hardware/software implementation has become one of the main weaknesses of security applications and hardware attacks, or "side channel attacks", such as DPA (Differential Power Analysis) and CPA (Current Power Analysis), have become standard. They are now identified as the most dangerous attacks, *i.e.* they allow ciphering algorithm keys discovery, like those used in smartcards, with minor cost and effort. In this context, the missions of this platform, supported by the "Région Languedoc Roussillon" and the "Université Montpellier 2", are to analyze the security potentialities of hardware platforms and embedded systems. This platform involves disciplinary competencies like Mathematics (I3M laboratory, Montpellier), Informatics and Microelectronics (LIRMM laboratory, Montpellier) and Electronics (IES laboratory, Montpellier). Our equipment allows us to perform process characterization as well. This platform is clearly part of a scientific and technical transverse approach in the "Université Montpellier 2" and "Pôle MIPS" (Mathematics, Informatics, Physics and System) scene.

I. Introduction

Hardware security has aroused a major interest in the research community over the past 15 years, since the introduction of the first attacks published in the literature, based on timing analysis. In this context, we have developed a platform, called SECNUM [1] (Fig.1), dedicated to the side-channel analysis (electromagnetic emanations, power consumption) of integrated circuits. The primary objective of this platform is to implement a complete lab equipment in order to study and develop attacks and countermeasures, and to perform the characterization of integrated circuits. Another goal is to propose an open research and education framework for hardware applied cryptography and circuits characterization.

Side-channel attacks are powerful cryptanalysis techniques, which allow retrieving the cryptographic keys from different channels (power consumption, electromagnetic waves, light emissions, etc.). For the sake of simplicity, this is possible because power consumption in a CMOS circuit is correlated to the processed data and operations [2]. Provided that the cryptographic algorithm is known, it is possible to find out the secret key. This is performed by simply observing the power consumption traces (for instance) and the input /output data.

Our lab equipment is fully automated with scripts and is described in Fig.1. It allows both power and electromagnetic analyses. It is composed of a high frequency near-field probe [3] positioned above the chip (Fig.2), connected to a Low Noise Amplifier [4]. The amplified signal is then transmitted to a 3.5GHz oscilloscope [5]. An XYZ stage is used to accurately place the near field probe.

Once collected, power/electromagnetic traces are processed with powerful algorithms (e.g. DPA / DEMA), which statistically try to extract the correct key.

This platform has been now for several years the ground for experimentally search, study and development of new countermeasures, *i.e.* hardware/software mechanisms able to hide or mask the link between the processed data and the power traces. Currently, we are getting a high interest in securing RISC processor architectures. We have proven that the processor pipeline is an additional threat to side-channel attacks. From this observation, we aim at developing efficient countermeasures to secure the whole datapath of the processor including pipeline stages and the Arithmetic and Logical Unit (ALU) part.

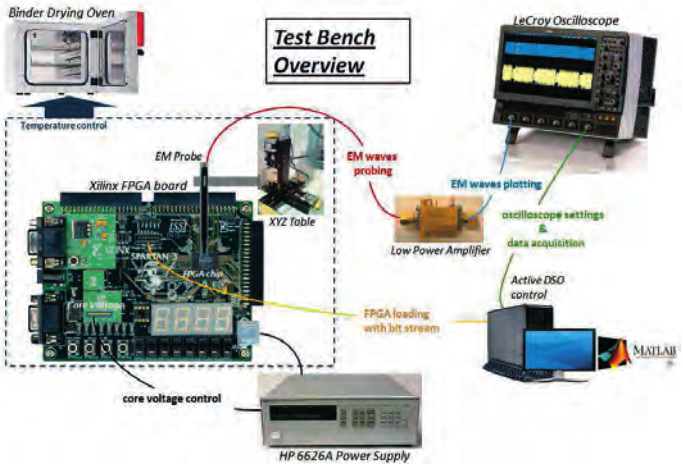

Fig.1: SECNUM Platform

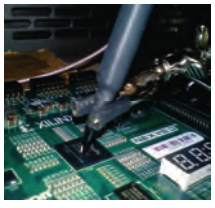

Fig.2: Near Field Probe above FPGA chip

 ISBN: 978-2-35500-019-5

Another application of this platform is dedicated to process characterization. Indeed, our lab equipment allows the study of monitoring parameters such as temperature and voltage by non-invasive probing, to determine their influence on electronic devices behavior.

II. Working Environment

The platform is accessible by an online reservation system and dedicated authorization, allowing users to schedule their experiments in advance. Currently, many PhD and Master students, engineers, who are constantly providing improvements to its functionalities, use it.

Most of the test circuits are FPGA boards, easy to program and academically efficient. The main software used for the experiments is Matlab [6], with automated scripts available from devices setup to results analysis. The communication among the various devices is made through many different ways, like Ethernet, ActiveDSO, GPIB or RS232.

III. Process Characterization case study

This kind of experiment consists in characterizing a process using a FPGA board (or dedicated IC) using near field probing. For instance a basic test performed in our lab is made by evaluating the speed of ring oscillators by injecting them into the chip, then observing the results. The sensor used to capture process variations is a simple 3-inverter ring oscillator (Fig. 3). This asynchronous structure has two advantages: the emitted frequency directly depends on the process capabilities and no clock signal is required to operate.

Further investigations on the process sensor might be conducted, in order to particularly discuss the coverage rate of such a structure. The main advantage herein is to characterize electrical parameters without connecting any electronic interfaces with the device. An EM probe above the circuit is able to recover emitted signals.

The measurement of process variability could be done by listening to the electromagnetic waves through a magnetic probe, then acquiring and analyzing the results, or performing a power analysis on the core voltage source of the chip.

In [7], the experimental protocol is divided into three main steps. The process variation is first captured with an asynchronous sensor, which emanates electromagnetic waves. These emanations are measured, amplified and collected by our lab equipment (EM probe, low-noise amplifier, and an oscilloscope as shown in Fig. 1). The signal is then processed to identify the ring oscillator frequency. The sensor is successively placed at each location to characterize the whole reconfigurable array.

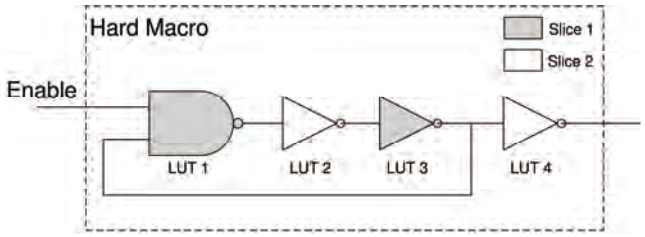

Fig.3: Ring Oscillator Sensor

Once collected, the data are transmitted from the oscilloscope to an external computer. A signal processing is then performed with Matlab. A Hanning window is first applied to avoid the spectral leakage, and a Fast Fourier Transform (FFT) is performed to convert data from time to frequency domain. Finally, an analysis of the power density spectrum is conducted to extract the frequency of the process sensor.

This platform is also very efficient to perform chip cartography, for instance on a Xilinx Spartan-3 Starter Kit Board with a XC3S200-4FTG256, nominal operating point of 1:2V @ 25_C. To ensure reproducible results, the temperature and voltage are kept constant at the nominal values in a thermal chamber, with a fine core voltage control, during the whole process acquisitions. The FPGAs operated at their nominal operating point. The ring oscillator was alternately placed and moved by reconfiguration of the FPGA at each CLB location (20 * 24 positions).

Fig.4 gives an example of the result obtained after analyzing the data from the previously described cartography. The different frequencies clearly indicate the location of the ring oscillator's sensors.

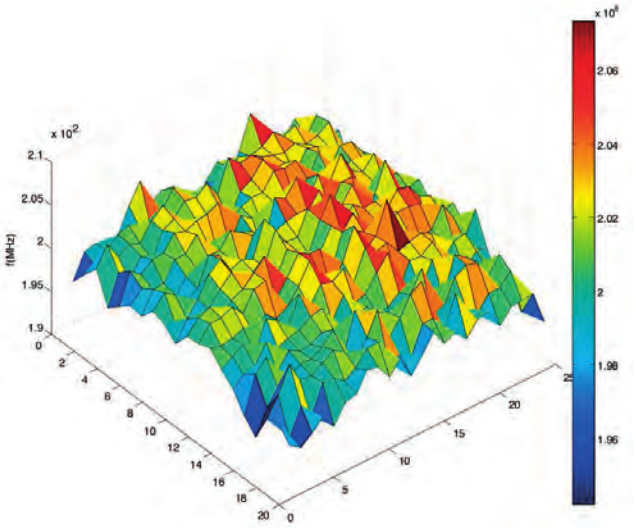

Fig.4: Electromagnetic frequency cartography

IV. Electromagnetic Analysis

This kind of experiment is conducted to retrieve the key of a cryptographic algorithm without any contact with the chip. It consists in exploiting a physical leakage of the circuit: the electromagnetic emanations emitted by the device.

During this experiment, we are assuming to be in the best conditions for the attacker, *i.e.* we are pretending that he knows exactly the location of the ciphering algorithm in the chip and the time when it is computed.

In [8], a Software DES implementation has been performed to demonstrate the efficiency on an attack on such kind of device. Indeed, the secret key of the unprotected DES implementation was discovered with very few measurements: less than 500 electromagnetic traces with different experimental settings were sufficient to break the crypto-algorithm. The traces are submitted to common attacks to retrieve the key, as shown in Fig.5.

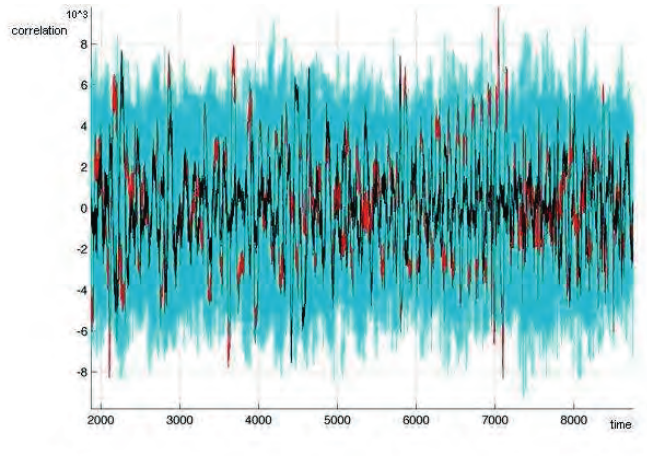

Fig.5: Attack on EM traces

The black curve indicates the correct sub-key, while the others correspond to the wrong sub-key hypotheses. Note that, according to the theory of differential analyses, the guessed sub-key is characterized by the highest amplitude. After all sub-keys are discovered, the whole key is computed and the security algorithm is broken, as shown in Fig.6, where only the black curve is remaining.

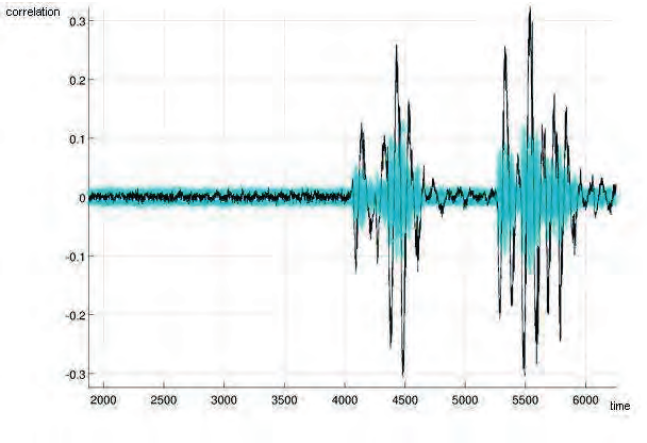

Fig.6: Broken Key after EM Attack

V. Countermeasures

In order to reduce the feasibility of such attacks, countermeasures have been developed on the platform. Data masking is one of the main ones. Basically, the idea of this countermeasure is very simple: the sensible data (messages, keys) are masked with various random numbers during the execution of the cryptographic algorithm. Obviously, a mask correction is performed at key steps in order to re-establish the expected data value.

However, a typical masking implementation for embedded processors requires some considerations. It is essential to remark that the mask should be generated within the chip and should be updated for each execution [9].

Furthermore, if two masked intermediate values are processed, we need to ensure that the result is still masked, i.e. special attention is requisite to avoid intermediate data sharing the same mask. Finally, the most important part is to guarantee the behavior of all processor's instructions.

If we consider the security of a processor, experimental results suggest that pipelined processors increase the risk of SCAs, and have to be considered with care. Therefore, one solution to counter crypto-attacks consists in implementing a dual pipelined datapath. Basically, the idea is to introduce a special datapath for the mask itself, which can be coupled to a classic RISC pipeline. Hence, instead of directly handling raw data, the processor operates on a dual datapath with masked data. The main role of the new datapath is to keep the corresponding mask for each masked data along the pipeline.

It is important to notice that RISC-based architectures are structured around load-store instructions. Indeed, RISC processors are characterized by the following key properties:

- all mathematical operations on data are performed from register to register,
- the only operations that affect memory are load and store operations.

Such properties can be effectively exploited by a masking scheme. All potential critical data are coming from the data memory, and thus, use load instructions. By taking into account that any ALU operation is a register-register instruction, the need of a special mask register file becomes obvious. This approach not only offers the advantage to handle any instruction using a masking scheme but also provides a full compatibility with the processor's instruction set. It is also important to note that cryptographic algorithms implemented on embedded processors usually require several thousands of clock cycles to complete, and consequently, present a large number of unsafe operations. That is why the dual masked datapath must be implemented in a generic and efficient way to cover all possible scenarios.

VI. The SecretBlaze

Implementing hardware countermeasure into crypto-processors is an interesting case study. We worked on this topic through the development of a dedicated processor, the SecretBlaze, available as an open processor core [10], which is part of the SECNUM platform.

This embedded processor was developed from [11] (Microblaze). We wish to clarify that the analysis and the results obtained with this MicroBlaze-like were identical to the original version: they share the same architecture, and therefore, the same weakness. From the MicroBlaze-like, we implemented the ideas of the RISC-based masked datapath. Among different types of masking, the Boolean masking was chosen because of its low overhead cost and its good integration into the pipeline. Hence, the masked data result from XOR operations between the raw data and the mask values. Fig.7 gives an overview of the SecretBlaze architecture.

The performance impact and the resource overhead of the proposed countermeasure were evaluated in Table. I. Two different implementations of the register file(s) were realized: either with distributed RAM (first values in Table. I) or with Xilinx's Block RAM (values between round brackets).

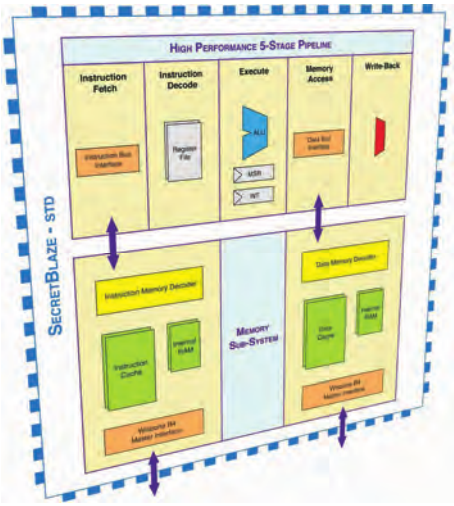

Fig.7: SecretBlaze Architecture Overview

Table I: Performance and resource overhead of the Secret-Blaze.

	MicroBlaze-like	SecretBlaze	Overhead
Max Freq. (MHz)	52.70	46.98	-11.2%
# Flip-Flops	310 (254)	576 (458)	+86%(+80%)
# Slices	1060(816)	1421(1013)	+34%(+24%)
# LUTs	1971(1493)	2526(1705)	+28%(+14%)
# BRAMs	4(7)	4(10)	+0%(+4.3%)

Not surprisingly, the most significant overhead is obtained on the number of flip-flops, owing to the introduction of the PRNG and mask pipeline registers. Note that a better PRNG would lead to higher resource requirements. Then, we observe a slight increase in the usage of slices and LUTs, related to extra-logic for the datapath of the mask. As expected, the number of LUTs is decreased when register files are implemented with BRAMs. In terms of performance, the operating frequency is only reduced by 11.2%, in both implementations.

Many experiments were conducted with the SecretBlaze, especially electromagnetic analysis to evaluate this processor against side-channel attacks.

Table II shows the comparison of results between the MicroBlaze-like and the SecretBlaze, which were obtained with the two best probe positions during the experimental evaluation: 1th Pos. next to one supply voltage plot, 2th Pos. over the die. The Measurement To Disclosure (MTD) is defined as the minimal number of traces needed to correctly guess the secret key. The stability is the number of traces required to recover the full key at least 1000 consecutive times. The latter metric suggests that the key is definitely broken.

Table II: Robustness comparison MicroBlaze-like - SecretBlaze.

	MicroBlaze-like		SecretBlaze	
	1th Pos.	2nd Pos.	1th Pos.	2nd Pos.
MTD	431	601	7177	1387
Stability	1524	2093	11968	2577

According to Table II, we first conclude that the SecretBlaze offers a better resistance against DEMA/CEMA than the MicroBlaze-like. Furthermore, these results highlight the importance of the probe's position over the FPGA's surface.

Indeed, the ratio of MTD and stability between the SecretBlaze and the MicroBlaze-like strongly varies from one position to another. In the worst case (2nd Pos.), the robustness of the SecretBlaze is just improved by a factor of 2.

VII. Educational Application

Several applications are being held using SECNUM platform to add hardware countermeasures to SecretBlaze and perform new experiments on FPGA boards. Thus, involving students into the development of the platform is a natural way of enhancing our work and training futur engineers and researchers in the same time, through various internships and thesis focusing on security or variability topics.

VIII. Conclusion

As a conclusion, the main idea of this platform is to propose a unique environment for research and education using EM analysis. EM analysis has become an essential tool for the characterization of circuits and SCA attacks. This platform opens new possibilities for many applications, and now we want to open the SECNUM platform to the community to conduct different types of experimentation.

Keywords

Side-Channel Attacks, Electromagnetic Analysis, Security Platform, Cryptographic Countermeasures, Process Characterization.

About the Author

Morgan Bourrée obtained a Master Degree in Microelectronics, Electronics and Automation Engineering from the University of Montpellier, France, in 2008. Then he joined the company STMicroelectronics in Crolles to start an assignment in the United States for 18months with IBM in Vermont, where he worked as a Design Kit Engineer. He contributed to the ISDA (International Semiconductor Development Alliance) composed of major Microelectronics companies, like Toshiba, Samsung, Global Foundries or IBM. He took part into new technologies development, from 32nm to 20nm. Since March 2010, he is a Study Engineer at the LIRMM, the Montpellier Laboratory of Informatics, Robotics, and Microelectronics.

REFERENCES

[1] "SECNUM Plateform," 2011. [Online]. Available: http://www.lirmm.fr/Secnum/
[2] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," in CRYPTO, 1996, pp. 104-113.
[3] "Rohde & schwarz hz-15 near-field probe set," 2011. [Online]. Available: http://www.testequity.com/products/1519/
[4] "Miteq," 2011. [Online]. Available: http://www.miteq.com/
[5] "Lecroy wavepro 735zi-a," 2011. [Online]. Available: http://www.lecroy.com/Oscilloscope/OscilloscopeModel.aspx?modelid=4718&capid=102&mid=504
[6] "Matlab - The Language of Technical Computing," 2011. [Online]. Available: http://www.mathworks.com/products/matlab/
[7] Florent Bruguier, Pascal Benoit, Philippe Maurine, and Lionel Torres, "A New Process Characterization Method for FPGAs based on Electromagnetic Analysis", in proceedings of FPL 2011, 2011.
[8] Lyonel Barthe, Pascal Benoit, Lionel Torres, "Investigation of a Masking Countermeasure against Side-Channel Attacks for RISC-based Processor Architectures" in proceedings of FPL 2011, 2011.
[9] F.-X. Standaert, G, Rouvroy, and J.-J. Quisquater, "FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks," in proceedings of FPL 2006, 2006.
[10] "SecretBlaze", [Online]. Available: http://janela.lirmm.fr/~barthe/index.php/page/secretblaze.html
[11] MicroBlaze Processor Reference Guide, Xilinx. UG081(v10.3), 2009.