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 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", are to analyze the security potentialities of hardware circuits and embedded systems and to evaluate their robustness against side channel attacks.

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 side-channel analysis (electromagnetic emanations, power consumption) of integrated circuits.

![SECNUM Platform](image1)

The primary objective of this platform is to evaluate the robustness of integrated circuit against side channel analysis, by understanding these attacks and developing countermeasures against these threats. We need research, industrial and education domains to complete these goals. As shown in Fig.2, we have several research projects going on with local and national partners, allowing us to explore the security mechanisms and propose innovative countermeasures to improve the security level of embedded systems. We also aim to offer a first evaluation before sending integrated circuits to official certification, which is a major gain of time for any industrial in need of enhanced security.

![SECNUM research environnement](image2)

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. Fig. 3 shows a Power Analysis performed on a 16-round DES (Data Encryption Standard) cryptographic algorithm. We can observe the relation between current consumption and DES rounds.

![Power Analysis on DES algorithm](image3)

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

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. RISC processor evaluation
Evaluating the security level of a common RISC processor is an interesting case study for the SECNUM platform. Indeed, this kind of processor is widely used, in credit cards or laptops for instance, but they present some hardware weaknesses that need to be evaluated. The basic architecture of such processors has been represented in Fig.4.

![Figure 4: RISC processor architecture](image)

The main known weakness of this architecture is the ALU part [4], but we highlighted a new one thanks to the SECNUM platform: the pipeline zone. Indeed, after acquiring 1000 electromagnetic traces in only 4 minutes on this area and performing a 15-minute attack, we were able to retrieve the secret key. The total time did not exceed 20 minutes, which would make this analysis really easy to perform for malicious people.

In this context, we developed a RISC-based side channel resistant processor, the SecretBlaze, embedding hardware countermeasures against side-channel analysis [5]. Then we perform the same attack with better results, as shown in Fig.5.

![Figure 5: RISC processor vs. SecretBlaze robustness evaluation](image)

III. Industrial Application
As shown in Fig.6, we have developed many partnerships with local and global companies around the SECNUM platform. Indeed, it is providing a first evaluation of industrial circuits before sending them to official certification, but most of all developing this platform insures to improve the protection of intellectual properties, which is a main concern in worldwide industry.

![Figure 6: SECNUM industrial partners](image)

IV. 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 future engineers and researchers in the same time, through various internships and thesis focusing on security or variability topics. We are also providing digital security courses at the engineering school of Polytech’Montpellier, and we are planning to do the same on an european level through the Eurodots program, giving PhD students access to advanced courses. The main contribution of SECNUM for the education domain is the IDEFI project FINMINA. Indeed, this project involves training and courses to students from high school to PhD and provides financial support to the platform for the next 8 years. All these contributions are represented in Fig.7.

![Figure 7: SECNUM education environnement](image)

V. 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 allows students and industrial to improve their knowledge about digital security. The sensitization of future researchers and engineers is a key for a better protection of private data.

REFERENCES