Current Mask Generation: A Transistor Level Security Against DPA Attacks

Daniel Gomes Mesquita, Jean-Denis Techer, Lionel Torres, Gilles Sassatelli, Gaston Cambon, Michel Robert, Fernando Gehm Moraes

Current Mask Generation: A Transistor Level Security Against DPA Attacks

Daniel MESQUITA, Jean-Denis TECHER,
Lionel TORRES, Gilles SASSATELLI,
Gaston CAMBON, Michel ROBERT
LIRMM – Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier
Université Montpellier II
161 rue Ada – CEDEX 5 – 34392 – Montpellier – France
Phone : +33 4 67 41 85 69
{*lastname*}@lirmm.fr

Fernando MORAES
FACIN – Faculdade de Informática
Pontifícia Universidade Católica do Rio Grande do Sul
Av. Ipiranga, 6681 – Prédio 30 – Bloco 4
90.619-900 – Porto Alegre – RS – Brasil
Phone: +55 51 33 20 36 11 – R.29
moraes@inf.pucrs.br

Abstract

The physical implementation of cryptographic algorithms may leak to some attacker security information by the side channel data, as power consumption, timing, temperature or electromagnetic emanation. The Differential Power Analysis (DPA) is a powerful side channel attack, based only on the power consumption information. There are some countermeasures proposed at algorithmic or architectural level that are expensive and/or complexes. This paper addresses the DPA attack problem by a novel and efficient transistor-level method based on a power consumption control, without any modification on the cryptographic algorithms, messages or keys.

Categories and Subject Descriptors

B.7.1 [Types and Design Styles]: VLSI. D.4.6 [Security and Protection]: Cryptographic controls.

General Terms: Design, Experimentation, Security.

Keywords: Cryptography, Side Channel Attacks, DPA, countermeasures.

1. Introduction

Cryptography is the enabling technology for e-commerce and secure communication. The robustness of crypto algorithms lies into complex mathematical function and a large key. The key (or a pair of keys, depending of the algorithm class) is a number sequence used to encrypt and decrypt a message, and presently its size can vary from 128 to 2048 bits. For instance, the RSA [1] algorithm is a public key scheme that uses a pair of keys, which has usually 1024 bits (for non commercial or military communications). The function behind the RSA is a modular exponentiation, where the exponent for encryption (public key), the exponent for decryption (private key) and the modulus are arithmetically dependents. The modulus is generated by multiplying two large primes numbers, and the security is granted by the difficulty of factorizing this modulus.

As cryptographic algorithms are composed by complex functions and computes large keys, it is a time consuming class of application. Therefore, a software-only solution leads to a performance overhead. Then development of hardware accelerators to compute crypto algorithms is an obvious issue to address this problem. Such hardware can be ASICs or reconfigurable devices, placed on accelerator cards on PCs or embedded into a cell phone. One example of crypto processor class that has its importance increasing is the smartcard.

In France, each credit card in use is a smartcard with memory and a crypto processor. This secure device is called "*Carte Bleue*" (*CB*) and runs the RSA and de 3-DES[1] [2] crypto algorithms. Nowadays there are 45 million people that uses the *CB*, and the trend is that in the coming years all countries of the European Union start to adopt this system, due its intrinsic security [2].

RSA and AES are crypto algorithms that are proven as being mathematically robust under some conditions. However, the weakness of such algorithms resides frequently on implementation problems. Factors like bad random number generation and others can compromise the whole system security. Concerning hardware implementations, even a carefully designer cannot avoid a specific class of cryptanalysis.

Traditionally, a cryptographic device uses a secret key to process input information and to produce output data. Protocol designs assume that input and output messages can be available to someone who wants to attack the system, but any other information about the key is accessible.

Unfortunately, these assumptions are not completely true. When computing a message, a crypto processor leaks some information, like the time to compute, electromagnetic emanations, and the power consumption. By knowing some of this additional information and the messages that are being processed, one can relate the leaked data with the internal state of the device, and hence to the secret key. This kind of attack is called Side-Channel Attack (SCA).

[1] In the next months, all CB will be substituted by CBs with the AES algorithm

From these SCA's, Differential Power Analysis (DPA), proposed by Paul Kocher et al in 1998 [4] is the most efficient. It relies on statistical analysis and error correction to extract information from power consumption, correlated with the secret key. Power analysis work by exploiting the differences between when a device processes a logical zero and when it processes a logical one. For example, when the secret data on a secure device is accessed, the power consumption may be different depending on the Hamming weight of the data. If an attacker knows the Hamming weight of the secret key, the brute force space is reduced. Given enough Hamming weights of the secret key, and by using statistical analysis techniques, the attacker can deduce the entire secret key.

Several general approaches for reducing the flow of information through power consumption have been proposed. This might be accomplished by adding a secondary circuit to the chip that would do calculations on random numbers. This could mask the power consumed by the other part of the chip handling the encryption. But it is unclear whether enough randomness could be created to resist the more thorough statistical techniques used to break the cards' codes. Random calculations tend to average out over time and are easy for differential power analysis to remove.

At the architectural level, a solution is to add parallel circuits to the chip that would mirror the real encryption calculations. For instance, if the real circuit is multiplying by the binary number 101, then the mirror circuit might multiply by 010. This would smooth out the power consumption because the power consumed by both parts together should be more constant. Still, it is unclear if all information can be blocked by this solution, because the mirroring is not perfect.

After a while, some efficient algorithmic countermeasures have been presented, but most of them rely on the modification at the algorithm level, to avoid the correlation between the power consumption, the message and key data. Our original approach simplifies this task by masking power consumption, without any algorithmic modification.

This paper is organized as follows: Section 2 describes the DPA attack. Section 3 shows previous and related works on DPA countermeasures. Section 4 presents the new method to avoid DPA attacks, and we discuss conclusions and future works in Section 5.

2. DPA Attack

DPA attacks use statistical techniques to determine secret keys from complex, noisy power consumption measurements [4]. For a typical attack, an adversary repeatedly samples the target device's power consumption through each of several thousand cryptographic computations. These power traces can be collected using high-speed analog-to-digital converters, such as those found in digital storage oscilloscopes. Figure 1 illustrates this method.

Because of its widespread use, the Data Encryption Standard (DES) is detailed. For example, in each of the 16 rounds, the DES encryption algorithm performs eight S-box operations. The 8 S-boxes take as input the XOR between the six key bits and the six bits of the R register and produce four output bits.

The method consists in to guess the sub-keys at the input of the S-box, and predict the output. For example, a typical prediction is that the 6 bits entering S-box 1 are "100101". If correct, it allows the attacker to compute four bits entering the second round of the DES computation. If the assertion is incorrect, however, an effort to predict any of these bits will be wrong nearly to half the time.

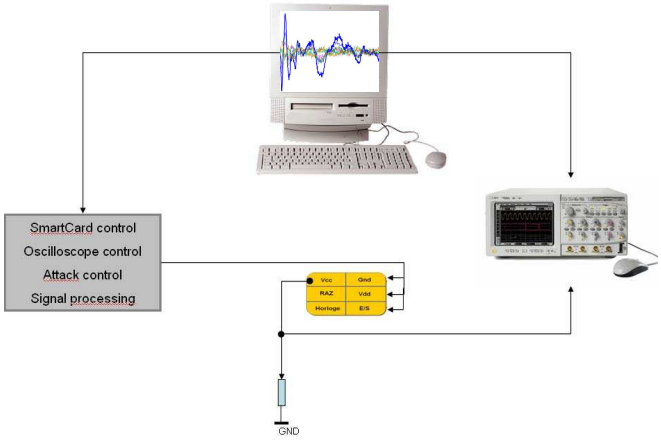

Figure 1 - A DPA attack platform

For any of the four predicted bits, the power traces are divided into two subsets: one where the predicted bit value is 0, and one set where the predicted value is 1. Next, an average trace is computed for each subset, where the nth sample in each average trace is the average of the nth samples in all traces in the subset. Finally, the adversary computes the difference of the average traces.

If the original hypothesis is incorrect, the criteria used to create the subsets will be approximately random. Any randomly-chosen subset of a sufficiently-large data set will have the same average as the main set. As a result, the difference will be effectively zero at all points, and the adversary repeats the process with a new guess.

If the hypothesis is correct, however, choice of the subsets will be correlated to the actual computation. In particular, the second-round bit will have been '0' in all traces in one subset and '1' in the other. When this bit is actually being manipulated, its value will have a small effect on the power consumption, which will appear as a statistically-significant deviation from zero in the difference trace.

The main idea behind this method is that prediction of a single output bit leads the attacker to the 6 bits of the input sub-key, and then, to the rest of the key bits.

3. State of Art of DPA Countermeasures

The countermeasures that have been developed against DPA attacks until now can be classified in two families. The first group is composed by the algorithmic countermeasures. The basic idea from references [5], [6], [7] and [8] is to randomize the intermediate results that are produced during the computation of a cryptographic algorithm. Classical DPA attacks are impracticable if these countermeasures are well implemented. But these randomizations are quite expensive to implement for non-linear operations as they are used in algorithms like DES and AES. Furthermore, the algorithmic approach does not provide sufficient protection against high-order DPA attacks. As consequence, this kind of method needs complementary hardware countermeasures.

The hardware method to counteract DPA attacks differs expressively from the algorithmic one. For the hardware approach

the intermediate results of the cryptographic algorithm computation are not affected. As an alternative, the contribution of the hardware approach is to hide the attackable part of the power consumption with different noises. The noise addition has a direct relation with the needs of measurement. It does not avoid DPA attacks, but makes it quite more difficult. The effectiveness of the countermeasures against DPA is due to the fact that cryptographic devices are typically protected by a combination of algorithmic and hardware techniques, or only the hardware one [9].

In order to decrease the correlation between data inputs and the power consumption of a given circuit, we must be able to increase the samples needed in DPA. Two major hardware countermeasures in this sense have been proposed. The first one concerns the reduction of the signal-to-noise ratio (SNR). For definition of SNR we call I_c the current consumption of the attacked circuit at a given moment t. I_n is the current noise added by the hardware countermeasure. So, the current consumption can be written as I_{total}, $t = I_c + I_n$. The k variable is the signal attenuation caused by the I_n current. The SNR definition can be viewed in Equation 1.

$$SNR = 20 \times \log\left(\frac{I_c}{kR}\right) \qquad (1)$$

The lower SNR is, the lower is the correlation between the correct hypothetical current consumption and the real power consumption of the device. To reduce SNR there are some works that use special logic to minimize the data dependency of the current consumption.

In [10] and [11] the balanced dual-rail logic is proposed. The basic idea is that a logic gate must consume an equivalent power, independently from the incoming input values. The SNR is reduced by this data-independent switching of the standard cells. Unfortunately, the experiments show that this goal is only partially reached. Dual-rail approach is not sufficient to guarantee a complete data independent power signature. One potential problem is that the gate loads may differ due to differences in routing. The design of each dual-rail gate must ensure equal input pin loads and balanced power usage. To achieve this, the process of grouping cells in the placement must be done carefully, which implies a high development effort. Besides that, the final circuit with dual-rail logic takes about tree times the area and two times the consumption of the original circuit.

The second hardware approach to prevent DPA attacks is to reduce the correlation between input data and power consumption by randomly disarrange the moment of time at which the attacked intermediate result is computed. If the time tc is different in every power trace, the correlation between the hypothetical power consumption and the real one is highly reduced. The countermeasure proposed by [12] lies on the insertion of random delays. The countermeasure proposed in [9] counteracts the DPA by using power-managed blocks to mask the power consumption. Both approaches, with the [13] and [14] works, difficult the DPA attack. But, as shown in [15], even if a direct calculation of the maximum probability of a given power consumption occurring at a given time is not practical, it is always possible to approximate it empirically based on a software model of the countermeasure.

This work gives a trend to mask the power consumption not by randomizing the consumption or creating noise but by generating, at the transistor level, a constant consumption. It is a little similar with the work proposed by Adi Shamir in [17], concerning the approach's level of abstraction. But the circuit described in [17] considers only if the attacker probes the Vcc, because the Gnd line remains vulnerable. As explained in next session, our circuit masks the consumption even if the attack occurs in the Vcc or in the Gnd line.

4. Current Mask Generation

This paper proposes a new method to make DPA attacks difficult using an analog approach. The principle is to use a current loop-feedback technique to make the power consumption constant for an external observer. As our circuit uses standard CMOS, it does not require special standard cells, as double rail method mentioned before.

To prevent DPA attacks we must be able to minimize the correlation between the input data and the power consumption. Random noise generation could be an interesting solution, since one idea to mask consumption is randomizing the consumption independently of the data that are being processed. This technique works against SPA attacks, but that is proven inefficient against DPA, since as the number of samples is enormous, it is possible to filter the noise generated, and to detect the real consumption.

Our approach relies on normalizing the power consumption. By identifying previously the peak consumption of the cryptographic circuit (CC), we adjust our novel current mask generation (CMG) to run at the CC's maximal consumption, even when the CC is consuming less current. Even it is not a "low-power" solution, not being well tailored for mobile communications for example; it remains interesting for applications like credit cards, set-top boxes, phone cards and others where the low-power for cryptographic applications is less essential. In banking operations, like cash transactions, the cryptographic operation is not used all the time and the whole user operation is not so time-consuming that justifies a low power approach. The most important in this case is the security.

The CMG is composed essentially by a current mirror and a voltage follower used as an current feedback circuit. Depicted in Figure 2, the cryptographic circuit is no more directly linked neither to the tension source, nor to the ground. The CC is powered only by the CMG circuit, and as the ground is linked inside chip, the attacker has only access to the masked *Vcc* and *Gnd* signals.

The current mirror is a way to accomplish high gain. The four P transistors (P_0 to P_3 with sizes wP_0 to wP_3) make up the high-swing current mirror (see Figure 3). The current mirror acts as the collector load and provides a high effective collector load resistance, increasing the gain. The current provided by this mirror has a relation α comparing with the input current (I_{ext}). This relation is $\alpha = wP_1 / wP_0$. So, the current provided to the cryptographic circuit is $I_2 = \alpha I$, that is not necessarily used by CC all time. Transistors N_0 and N_1 have as task to polarize the high-swing current mirror. Still in Figure 3, a capacitance can be viewed. Its role is to assure a certain lapse of time to the diffAmp, because the loop-feedback is not so rapid to follow the CC consumption oscillation.

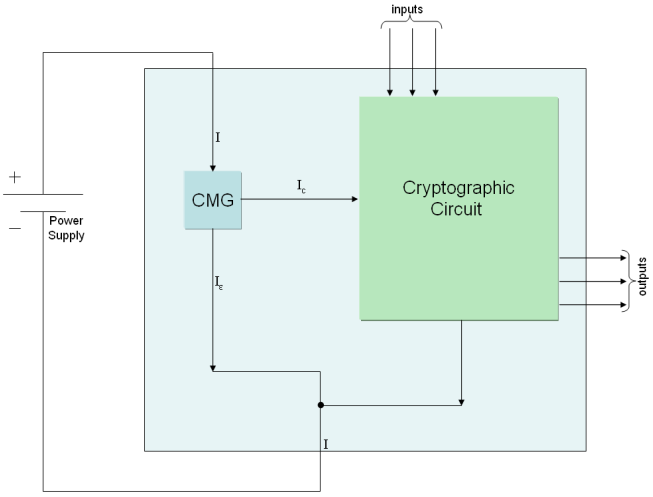

Figure 2 - The Current Mask Generation Circuit Overview

The loop-feedback, with the comparator, acts as an adaptable voltage generator. The differential amplifier (diffAmp) receives a voltage sent by the mirror and compares it with a reference tension (i.e. V_{ext}). If the cryptographic circuit consumes an amount of current less than I_2, the tension at the diffAmp input will be lower than the reference tension. Then the output of the diffAmp will send 0 to the P_4 transistor. So, it will consume an IL current, that is the difference between I_2 and I_c. When the CC consumption is at its peak (i.e. $I_c = I_2$), the diffAmp sends an 1 to the P_4, switching off the transistor, because it is no longer necessary to drain current.

As can be viewed in the same figure, an attacker, who has only access to the points A and B will see the original current – he cannot extract any information about the CC processing.

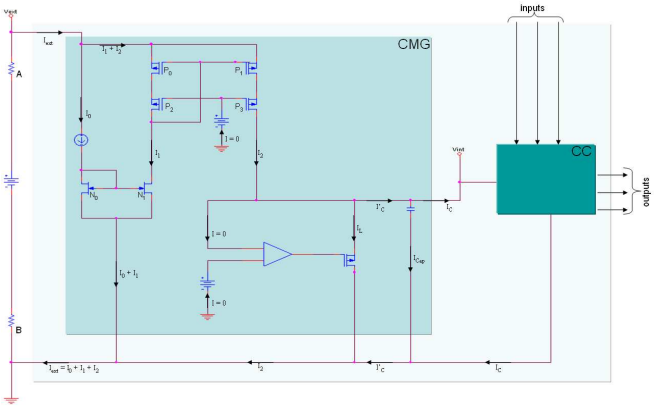

Figure 3 - The CMG circuit in detail

To validate the CMG idea, we used a simple DES S-Box as our CC. We simulate the S-Box current consumption to the worst case, to calculate the transistor parameters for the CMG. As depicted Figure 4, the maximum current needed by the S-Box is about 6mA.

After setup the CMG, we ran different simulations, for different data scenarios. As shown in Figure 5, the CMG works efficiently, masking the CC consumption and making a DPA attack a very difficult task. To define this difficulty, the Figure 6 shows some very little variations at the masked signal. These variations could be exploited to realize a DPA attack. Nevertheless, these oscillations are about 6µA. So, to make the attack it is mandatory to use an oscilloscope with a resolution able to detect these small variations.

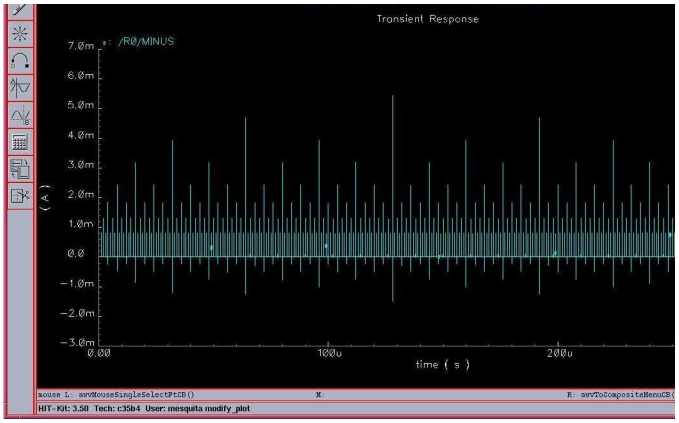

Figure 4 - The S-box current consumption

We assume that the CC's peak consumption is around 6mA, and we have a state of art oscilloscope attaining a resolution of 8 bits. With this resolution, to the given current (gSignal) we can reach the minimum resolution (mR) of 23µA, as can be viewed in the Equation 2, where resolution is equal to $2n$, with n= 8.

$$mR = \frac{gSignal}{resolution} \qquad (2)$$

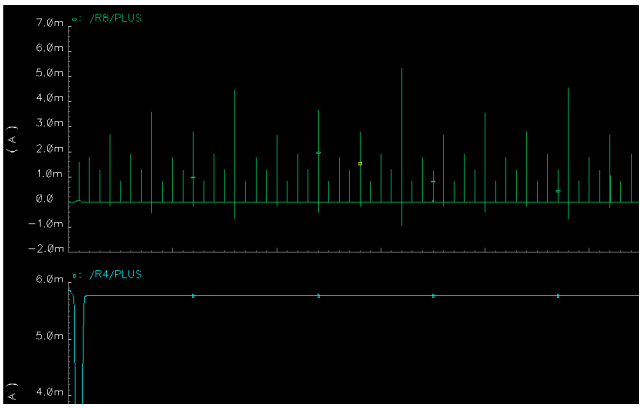

Figure 5 - CC's current consumption and the current provided by the CMG circuit.

The Figure 7 shows, from a top-down view, the current consumption that can be plotted from the external *Vdd* or *Gnd*, the current consumption of the cryptographic circuit, the data input called a1 and the data input called a0. Analyzing the consumption reported to data input, Figure 7 shows that even with a one or a zero, or two ones, or two zeros as entries, the consumption viewed at the attackers side remains the same.

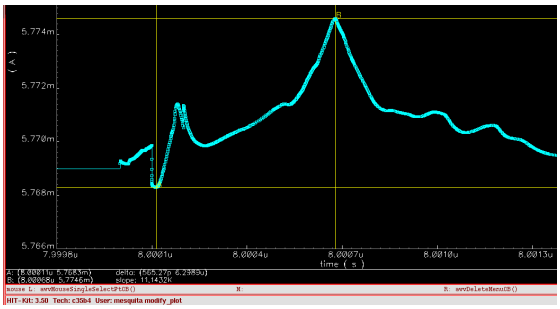

Figure 6 - The data leaked after the Current Mask Generation: the little lapse of time and the little amplitude must be considered in the observation.

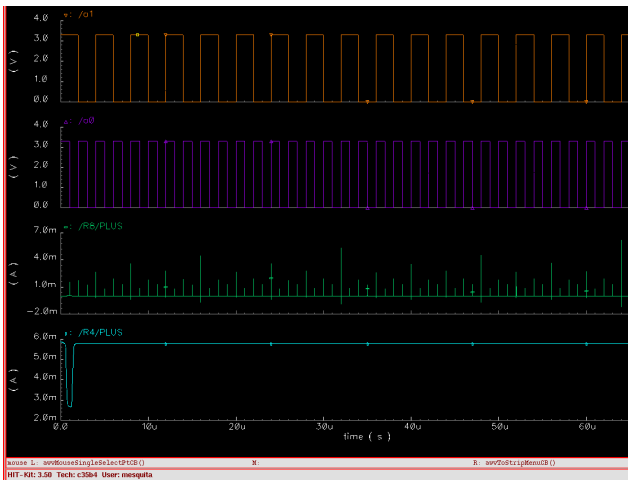

Figure 7 - The current provided by the CMG circuit, the current consumed by the CC, and the data input a1 and a0

Another aspect that must to be considered is the relation between the masked signal and the original signal. With the CMG, the SNR is decreased, as shown in the Figure 8 (Equation 1 shows how to calculate the SNR). The red signal represents the real consumption of the CC, and the blue signal represents the noise.

Then, when adding the CMG, the current consumption signal is attenuated by a k factor. Based on the previous simulation, the attenuation from the I_c signal to the In signal is about 20 times, then k=20. The final Signal to Noise Ration (SNR_{CMG}) is shown in the Equation (3):

$$SNR_{CMG} = 20 \times \log\left(\frac{I_c}{kN}\right) = 20 \times \log\left(\frac{I_c}{N}\right) - 20 \times \log(k) \quad (3)$$

$$SNR_{CMG} = SNR - 20 \times \log(k)$$

To illustrate this phenomenon, Figure 9 shows that if k is big enough, the power consumption signal will be submerged into noise. With a k=20, the attenuation will be 26dB, that leads to preventing the correlation between the signal and the noise.

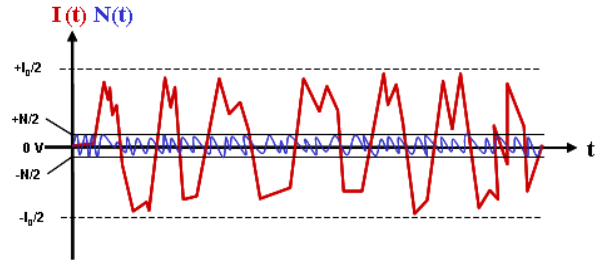

Figure 8 - Power consumption signal and the circuit's noise

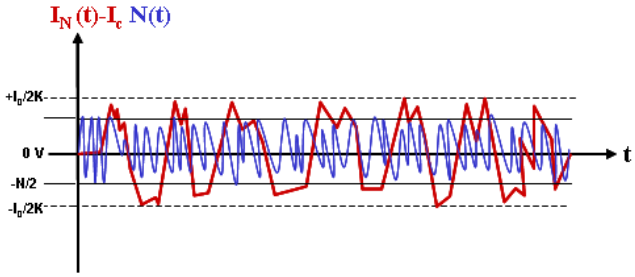

Figure 9 - The current consumption submerged into noise.

5. Conclusion

The presented work improves the robustness of cryptographic circuits against DPA attacks.

In this paper we have proposed a transistor level solution, which has as major contribution the fact that no changes are needed into the cryptographic circuit.

As a drawback, our proposal is not a low power solution. Another problem with this approach is the integration of the capacitance. There are two solutions in study. The first one concerns the capacitance integration in a SIP technology [18]. This is feasible, but we do not made any costs study of this trend. On the other hand, maybe with the improvement of the loop-feedback and the current generator, i.e. with a more efficient mechanism, a large capacitance will not be required.

In spite of the drawbacks, the CMG approach remains interesting. The poor Signal to Noise Ratio generated by the CMG circuit makes a DPA attack very difficult.

6. Acknowledgments

Work started during doctoral program at the Université Montpellier II – LIRMM laboratory, in Montpellier, France. Financially supported by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES), Brazil, under schoolarship grant 0276-02/2.

7. References

[1] Rivest, R., Shamir, A., et al. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". *ACM Communications*, vol 21. pp 120-126. 1978.

[2] – . "Data Encryption Standard (DES)". Federal Information *Processing Standards Publications (FIPS PUBS) N° 46-3*. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. EUA.October 25, 1999.

[3] Groupement des Cartes Bancaires CB. “Les cartes Bancaires en Nombres 2004”. http://www.cartes-bancaires.com/FR/info/communiques/2005/DPchiffresCB2004.pdf. Paris, march 2005.

[4] Kocher, P., Jaffe J., et al.“Differential Power Analysis : Leaking Secrets”. *Advances in Cryptology: Proceedings of CRYPTO'99*, Vol 1666, Springer-Verlag,. pp. 388-397. 1999.

[5] Messerges, T. S., Dabbish E. A., et al. “Power Analysis of Modular Exponentiation in Smartcards”. *Cryptographic Hardware and Embedded Systems - CHES 1999*. Lecture Notes in Computer Science, Vol. 1717, Springer, ISBN: 3-540-66646-X. Pp 144-157, 1999.

[6] Goubin, L., Patarin, J. “DES and Differential Power Analysis – The “duplication” method”. *Cryptographic Hardware and Embedded Systems - CHES 1999*. Lecture Notes in Computer Science, Vol. 1717, Springer, ISBN: 3-540-66646-X. Pp 158-172, 1999.

[7] Trichina, E., De Seta, D. Et al. “Simplified Adaptive Multiplicative Masking for AES”. *Cryptographic Hardware and Embedded Systems - CHES 2002*. Lecture Notes in Computer Science, Vol. 2523, Springer, ISBN: 3-540-00409-2. Pp 187-197, 2003.

[8] Golic, J. D., Tymen, C. “Multiplicative masking and Power Analysis of AES”. *Cryptographic Hardware and Embedded Systems - CHES 2002*. Lecture Notes in Computer Science, Vol. 2523, Springer, ISBN: 3-540-00409-2. Pp 198-212, 2003.

[9] Benini, L., Macii, A., et al. “Energy-aware design techniques for differential power analysis protection”. *Design Automation Conference – DAC 2003*. Anaheim, USA. June, 2003.

[10] Saputra, H. Vijaykrishnan, N., et al. “Masking behavior of DES encryption”. *Design, Automation and Test Europe – DATE 2003*. ACM-Sigda, ISBN 0-7695-1471-5. Munich, Germany, 2003.

[11] Simon M., Ross A., et al. “Balanced Self-Checking Asynchronous Logic for Smart Card Applications”, *Microprocessors and Microsystems Journal*, 27(9). Elsevier, ISSN 0141-9331. pp 421-430, October 2003.

[12] Clavier, C., Coron, J-S., et al. “Differential Power Analysis in the presence of hardware countermeasures”. *Cryptographic Hardware and Embedded Systems - CHES 2000*. Lecture Notes in Computer Science, Vol. 1965, Springer, ISBN: 3-540-41455-X. Pp 252-263, 2000.

[13] Irwin, J., Page D., et al. “Instruction stream mutation for non-deterministic processors”. *International Conference on Application Specific Systems, Architectures and Processors – ASAP 2002*. IEEE press. Pp 286-295. 2002

[14] May, D., Muller H. L., et al. “Non-deterministic processors”. *Information security and privacy – ACISP 2001*. Lecture Notes in computer Science, volume 2119. Springer ISBN 3-540-42300-1. pp 115-129. Sydney, Australia. July 2001.

[15] Mangard, S. “Hardware countermeasures against DPA – a statistical analysis of their effectiveness”. *Topics in Cryptology – CT-RSA 2004*. Lecture Notes in Computer Science, Vol. 2964, Springer, ISBN: ISBN 3-540-20996-4. pp. 222 – 235. San Francisco, USA. February 2004.

[16] Fouque, P.-A., Muller F., et al. “Defeating Countermeasures Based on Randomized BSD Representations”. *Cryptographic Hardware and Embedded Systems - CHES 2004*. Lecture Notes in Computer Science, Vol. 3156, Springer, ISBN: 3-540-22666-4 pp. 312 - 327. Cambridge, EUA. 2004.

[17] Shamir, A. “Protecting smart cards from passive power analysis with detached power supplies”. *Cryptographic Hardware and Embedded Systems - CHES 2000*. Lecture Notes in Computer Science, Vol. 1965, Springer, ISBN: 3-540-41455-X. Pp 71-77, 2000.

[18] Tummala, R. and Madisetti, V. “System on Chip or System on Package?” *IEEE Design and Test of Computers Review*. Vol. 16, N. 2. IEEE Press. ISSN: 0740-7475. pp 48-56, April-June 1999.