Modified Current Mask Generation (M-CMG): An Improved Countermeasure Against Differential Power Analysis Attacks

Hedi Besrour[2], Daniel Gomes Mesquita[1], Machhout Mohsen[2], Tourki Rached[2]

[1]Faculdade de Informática – Universidade Federal de Uberlândia – Brazil

[2]Electronics and Microelectronics Laboratory – Monastir University – Tunisia

mesquita@facom.ufu.br

{hedi.besrour, mohsen.machhout, rached.tourki}@fsm.rnu.tn

Abstract. *It has been demonstrated that encryption device leaks some information, which can be exploited by various attacks such as differential power analysis (DPA). To protect an Advanced Encryption Standard (AES) implementation from DPA without any modification of the cryptographic algorithm, we can use the Current Masking Generation (CMG). The CMG countermeasure consists of stabilizing the power consumption, but it presents some limitations concerning temperature variations and the Early effect. The goal of this paper is to update the CMG to address these problems, evolving to the Modified-Current Masking Generation (M-CMG).*

Resumo. *Durante seu funcionamento, dispositivos criptográficos vazam informações, que podem ser exploradas por vários ataques, tal qual a análise diferencial de consumo de potência (DPA). Para proteger o algoritmo de criptografia AES de ataques desse tipo, sem que seja necessário modificar o algoritmo em si, pode-se usar uma contramedida chamada Geração de Máscara de Corrente (CMG). Essa contramedida consiste na estabilização do consumo do circuito criptográfico, dificultando assim a exploração dessa informação. Entretanto, essa contramedida apresenta limitações em termos de estabilidade, especialmente relacionada ao efeito de Early e à variação de temperatura do circuito. O objetivo deste artigo é demonstrar esses problemas e também propor a solução para ambos, criando assim a contramedida M-CMG: Modified Current Mask Generation.*

1. Introduction

In today's ultra connected society, virtually every facet of life involves the flow of information through computer networks. For instance, in online banking transactions or diplomatic communications, the need of a secure flow of information is vital. To provide such security, encryption algorithms are employed, as the Advanced Encryption Standard (AES) [Daemen and Rijmen 2001]. This algorithm is a symmetric block cipher that can process data in 16-byte blocks, using cipher keys with lengths of 128, 192, and 256 bits. The AES won a contest promoted by the US government through its National Institute of Standards and Technology (NIST), but rapidly became an *de facto* standard for commercial transactions and online communications around the world [Parikh and Patel 2007].

Generally, the security of cryptographic algorithms is their mathematical basis. The AES basis are operations over the finite field $GF(2^8)$, which means its security can be easily analyzed using mathematical techniques. The AES cryptanalysis have been studied since the algorithm original proposal, and even if the complexity of these kind of attacks is slightly reduced regarding brute force [Bogdanov et al. 2011], the algorithm is still considered secure.

However, a new type of attacks, no longer aiming the mathematical construction of the algorithm, but the physical characteristics of its implementation has been proposed. The information leaked by the physical implementation, also known side channel information, can be exploited to perform attacks [Kocher et al. 1999]. The so called Side Channel Attacks (SCA) have become an increasingly important design concern for cryptographic implementations [Mangard et al. 2007]. A variation of SCA consists on observing the power consumption of an AES implementation, which can lend information about the operations, operands, and ultimately the secret keys. With a modest investment in a digital oscilloscope and third party software, attackers can execute a Differential Power Analysis (DPA) [Kocher et al. 1999] with little knowledge of the system under attack.

This threat drives to search for secure cryptographic hardware implementations, resistant to SCA. The countermeasures against power analysis proposed to counteract SCA can be algorithmic or physical (gate-level) [Mangard et al. 2007]. On one hand, algorithmic countermeasures have as drawback the need of modifications on the original cryptographic algorithms, attempting against its wide applicability and compatibility with already deployed applications. On the other hand, physical countermeasures may generate an area overhead, but can be more effective in maintaining the algorithmic standards, as the Current Mask Generation (CMG) previously proposed by one of the authors of the current paper, in [Mesquita et al. 2007]. As the DPA attack exploits the variation on current consumption concerning the data computed, the CMG aims to minimize the impact of the AES data processing to the chip power consumption.

Nevertheless, by reviewing the CMG, we found some stability issues related to the Early effect [Early 1952] and concerning the circuit behavior in the presence of temperature variations. This second problem may lead to a weakness of the countermeasure, once the current consumption of the CMG increases as the heat rises. These observations leads to some improvements of the original idea, introduced here as the M-CMG, the Modified Current Mask Generation.

This article is organized as follows. Section 2 highlights the Differential Power Analysis attack principles and a real-world application against an AES implementation. The research method is discussed in Section 3. Section 4 explains the advantages and the problems founded at the CMG countermeasure. Section 5 introduces solutions to counteract the temperature and the early effects on the CMG, demonstrated in a theoretical basis. Finally, Section 6 presents the conclusions and further work within this theme.

2. Differential Power Analysis (DPA) Attack

In the groundbreaking paper [Kocher et al. 1999], it was presented a method to recover a secret key of real world cryptographic systems from power consumption of computers and microchips. The Differential Power Analysis (DPA) is used to attack on either the

first or the last round but it can sometimes be applied to attack on intern rounds of the block ciphers [Messerges et al. 1999]. The main target of a DPA attack is to recover a byte *k* of the secret key *K* that is used to encrypt a plaintext or decrypt ciphertext through a cryptographic chip. In this paper, we use the DPA for the first round of an AES-128 encryption implementation.

2.1. DPA Principles

The DPA attack is based to send N known random plaintexts and measures the corresponding chip power consumption waveforms during their encryption. Therefore, Npower traces $T_{1\cdots M}[1 \cdots M]$ are collected by the adversary, each of which consists of M samples, as shown in Figure 1.

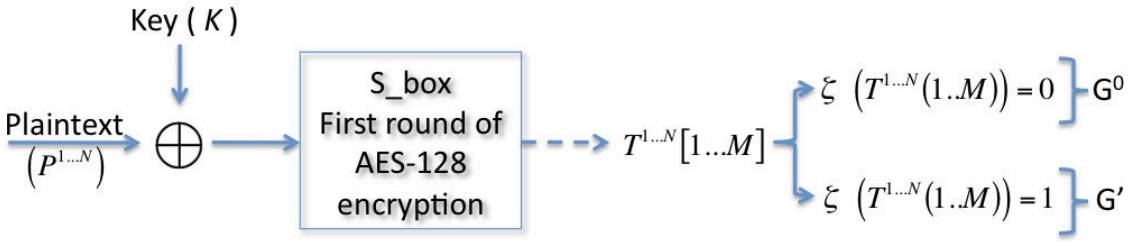

Figura 1. Basis of the Differential Power Analysis Attack

An attacker may create several hypotheses of key k and use the selection function ξ to separate the power traces in some G groups[Guilley 2007]. After, it uses statistics to detect the correct key K. for this reason, the power traces are immediately classified in two groups, $G_0 = \{T_n|\xi(\cdots) = 0\}$ and $G_1 = \{T_n|\xi(\cdots) = 1\}$.

These two groups G_0 and G_1 are averaged in order to eliminate random noise into D_0 and D_1, as represented in Equations 1 and 2, respectively, where $|G_0| + |G_1| = N$.

$$D_0(m) = \left|\frac{1}{G_0}\right| \sum_{G_n(m)\in G_0}^{n,m} G_n(m) \tag{1}$$

$$D_1(m) = \left|\frac{1}{G_1}\right| \sum_{G_n(m)\in G_0}^{n,m} G_n(m) \tag{2}$$

The next step is to subtract the two groups D_0 and D_1 from each other. This result leaves a differential trace $DPA(m) = D_1(m) - D_0(m)$.

If the key guess was incorrect the resultant trace will tend to zero, but if the key guess was correct the differential trace will contain spikes at points of correlation, verifying the correct key guess. The spike under the correct guess is distinguished only if it is sufficiently greater than the maximum spike under a wrong one.

2.2. DPA data acquisition and experimental results

The best evaluation method of DPA attack research is direct measurement. We have developed PCB board with a PIC18F microcontroller, and we have implemented the AES-128

in software. We have been using MATLAB to send the messages via RS-232 to the PCB board. At the beginning of the encryption cycle, the output of PIC18F microcontroller triggers a Lecroy WaveRunner104MXI oscilloscope to start acquisition data for power trios. The setup is show in Figure 2.

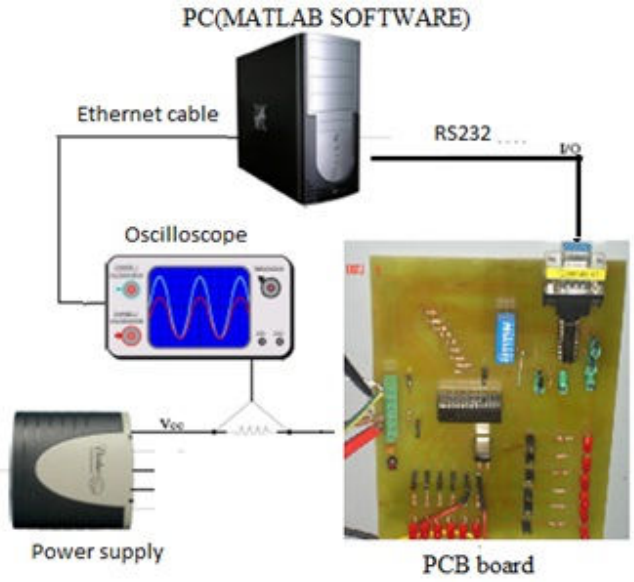

Figura 2. Experimental setup for data acquisition

We made an acquisition for 5000 power traces and they are imported into PC from oscilloscope via Ethernet for statistical analysis with our custom software (runned in MATLAB). We had the following results for DPA attacks in Figure 3. In the same figure, we can observe some ghost peaks that may mislead the key guessing. To minimize these ghost peaks, it is necessary to increase the Signal to Noise Ratio (SNR), as suggested in [Alioto et al. 2006]. The SNR is given by Equation 3, where $\varepsilon = l \times \beta$ and β is the number of output bits by the selection function ξ. The parameter l is constant equal to the voltage difference seen between two data words concerning Hamming weights $N(n)$ and $N(n+1)$.

$$SNR = \frac{\sqrt{N\varepsilon}}{\sqrt{8\sigma^2 + \varepsilon^2(ad + d - 1)}} \tag{3}$$

One way to increase the SNR in Equation 3 is to increase ε. The value of ε depends on the number of bits output by selection function ξ. Then, the power traces are immediately classified in three sets: $G_0 = \{T_n | \xi(\cdots) = 0'\}$, $G_1 = \{T_n | \xi(\cdots) = 1'\}$ and $G_2 = \{T_n | \ni G_0, G_1\}$.

When using the last selection function ξ for DPA attack, the attacker needs more acquisition of power signals. Because all of $1 - 2^{1-l}$ power traces placed in partition G_2 are not used. For this reason, an attacker cannot increase l too much without requiring an excessive number of power traces.

The result of this improvement can be seen at Figure 4. The sub key from $DPA(l = 3)$ using 1000 power samples. We can observe the peak corresponding the

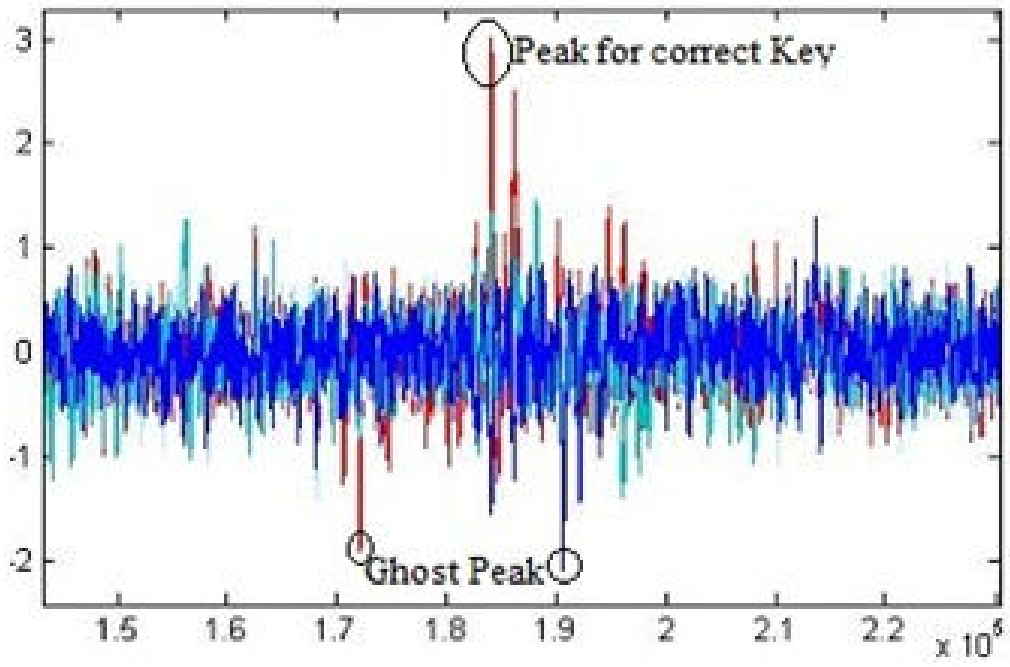

Figura 3. DPA Attack Experimental Results

correct key guessing, even if some ghost peaks are still present.

3. Method

This work was mainly motivated by the two following research questions:

- *Is the CMG stable regarding the* Early effect *[Early 1952]?*
- *How the CMG countermeasure behaves when the temperature rises?*

To address these two questions, firstly, the CMG architecture was replicated. The initial goal is to perform an electrical simulation to evaluate the CMG's normal behaviour. At this point we could verify the same results as presented in [Mesquita et al. 2007]. The variable measured here is the consumed current of the cryptographic circuit and the current masked by the CMG.

Concerning the *Early effect*, a theoretic study, shown in Section 5.1, was performed to verify the existence of the problem, as well to suggest a practical solution. This study is based on both James Early original paper [Early 1952] and an update to simulate the Early effect given by [McAndrew and Nagel 1996]. The variable we measure here is the external current regarding the input current, as detailed in the Section 4.

After, to learn about its behavior regarding temperature, the circuit was simulated with the Cadence P-Spice tool, varying the temperatures from 10^0 $Celsius$ to 150^0 $Celsius$. The variable measured here is the output (masked) current concerning the heat variation. This current must remain stable with the temperature increasing.

Once the problems were plotted, through a theoretical study, modifications on the original CMG were calculated, then simulated, resulting in a updated an upgraded countermeasure.

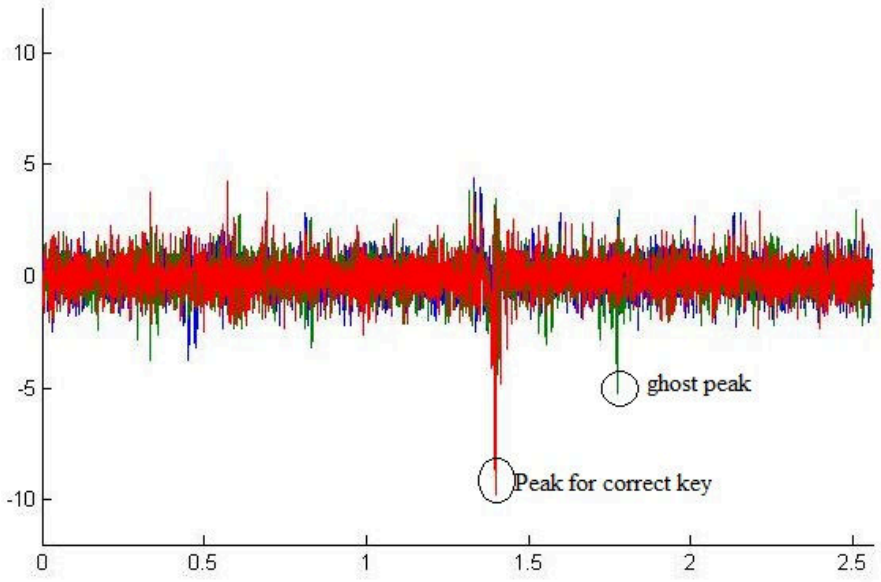

Figura 4. Improved DPA Attack Experimental Results

4. Current Mask Generation: Principles, advantages and weakness

Several countermeasures have been proposed to against DPA attack, as can be viewed at Chapter 7 from [Mangard et al. 2007]. One efficient way to counteract DPA is to lend the power consumption constant, as proposed in [Mesquita et al. 2005]. With this approach, no changes are needed neither on the cryptographic algorithm nor on the cryptographic core.

As seen in Figure 5, The CMG is composed basically of a current mirror and a follower circuit. The current mirror imposes the fixed current I_2 equal at the peak of current consumption for cryptographic circuit.

The operational amplifier receives a voltage sent by the mirror and compares it with a reference tension. If the cryptographic circuit consumes an amount of current less than I_2, the tension at the $Op\ Amp$ input will be lower than the reference tension. Then the $Op\ Amp$ output will send $0V$ in the base of the P_4 transistor. So, it will consume an I_L current ($I_L = I_{ext} - I_2$).

It is important to take a look at the current mirror from Figure 5, so we expanded it to Figure 6. In an ideal situation $\beta \to \infty$. It means that while $V_{BE_{N_1}}$ is fixed, I_0 grows with $V_{CE_{N_1}}$. Also, the $Early\ Effect$ has been neglected. This ca be written as in the Equation 4.

$$I_0 = \frac{I_{ext}}{1 + \frac{2}{\beta}} \tag{4}$$

But, in reality, if the transistors have the same parameters β_0, the transistors N_0 and N_1 needs current as given by Equation 5 (with V_a designating the early voltage), and the relation given by Equation 6.

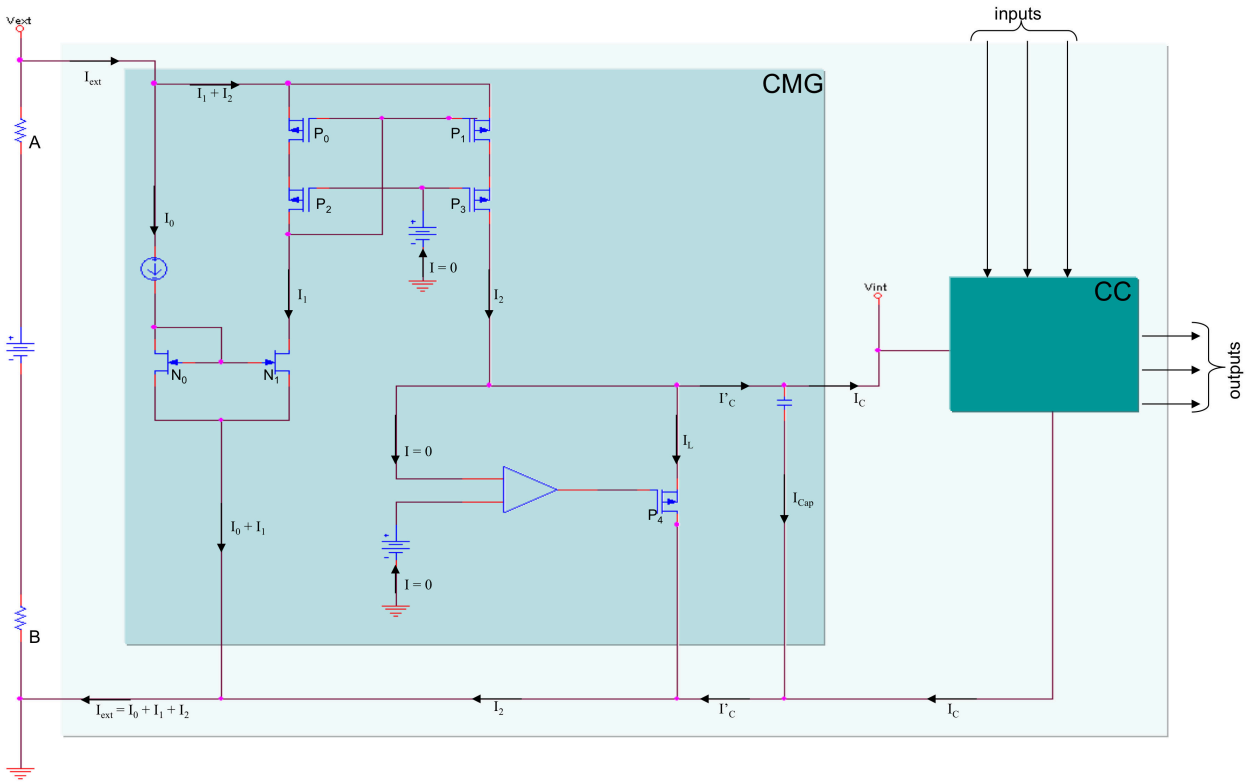

Figura 5. Original CMG: Current Mask Generation

$$I_{b_{N_0}} = \frac{I_{C_{N_0}}}{\beta_0} \; and \; I_{b_{N_1}} = \frac{I_0}{\beta_0(1 + \frac{V_{CB_{N_1}}}{V_A}} \tag{5}$$

$$I_0 = \frac{1 + \frac{V_{CB_{N_1}}}{V_A}}{1 + \frac{2}{\beta_0}} I_{ext} \tag{6}$$

The CMG have been demonstrated efficient to counteract DPA in ideal situations [Mesquita et al. 2007], but the Equation 6 shows that system has stability problems, since the output current I_0 may be grater than the input current I_{ext} due to the *Early Effect*.

Another problem founded may be critical, because may be exploited by an attacker: the current mirror proposed in CMG (Figure 6) may misbehave if the transistors temperature changes [Munro 1991].

In the next Section we propose a single modification that copes with the two presented problems with the original CMG.

5. Modified Current Mask Generation: The M-CMG

To solve the observed CMG problems, we to need introduce a "current-keeping"with negative feedback in the same mirror current used (Figure 6. For this reason, we have added new transistor N_2, seen in Figure 7.

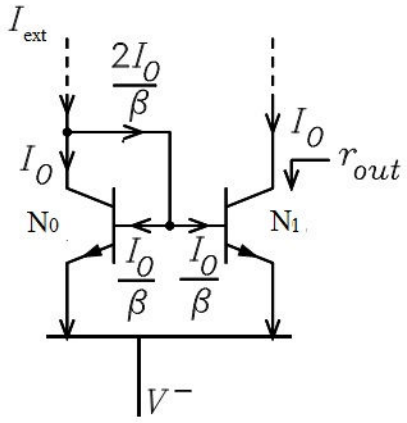

Figura 6. Current Mirror from the Original CMG

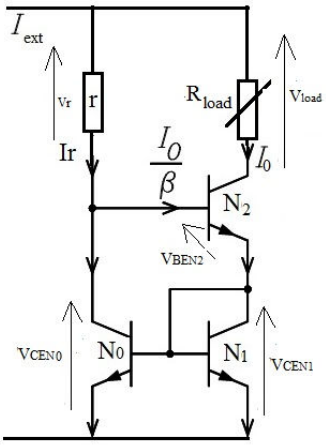

Figura 7. Proposed Current Mirror for the M-CMG

Following, we analyze this modification concerning the *Early Effect* and the temperature issues.

5.1. The M-CMG and the Early Effect

Regarding Figure 7, the transistor N_2 controls the current, through R_{load}, by changing its resistance between the collector and the emitter. For instance, R_{load} increase causes a decrease in the current I_0 and the voltage V_{load}. Or the current I_0 is the input for the simple current mirror N_0 and N_1; thus, the output current will drop and $V_{CE_{N_1}}$ increases. The input voltage $V_{BE_{N_2}}$ of the transistor N_2 increases; it begins opening more until the load current restores its previous magnitude. Doing that, it keeps the current I_r and I_0 constant. And like that, we reached our objective and solved the problem of early effect. So, the current I_0 can be re-written as in Equation 7.

$$I_0 = \frac{\beta^2 + 2\beta}{\beta^2 + 2\beta + 2} I_{ext} \tag{7}$$

Thus, Equation 7 predicts that $I_0 \approx I_{ext}$.

5.2. The M-CMG and the Temperature Issue

Once the *Early Effect* is avoided, it is important to study the stability of the M-CMG (Figure 7) concerning the influence of heat on the countermeasure behavior. The relation between I_0 and temperature is given by Equation 8.

$$\Delta I_0 = S_V \Delta V_{BE} + S_\beta \Delta\beta \tag{8}$$

With:

$$S_V = \left[\frac{\delta I_0}{\delta V_{BR}}\right]_{\beta_{constant}} \tag{9}$$

And:

$$S_\beta = \left[\frac{\delta I_0}{\delta \beta}\right]_{V_{BE constant}} \tag{10}$$

So we use the relation $I_{ext} = \frac{V_{CC}-2V_{BE}}{r}$ and replace I_0 from Equation 7 in Equations 9 and 10, obtaining Equation 11.

$$\Delta I_0 = -\left(\frac{2}{r}\Delta V_{BE} + \frac{4(V_{CC}-V_{BE})}{r\beta^3}\Delta\beta\right) \tag{11}$$

In order to confirm the Temperature Equation 11 stability with heat increase, we simulate de M-CMG circuit with the P-Spice tool. The Figure 8 shows the variation of current consumption in CMG and M-CMG depending on the temperature.

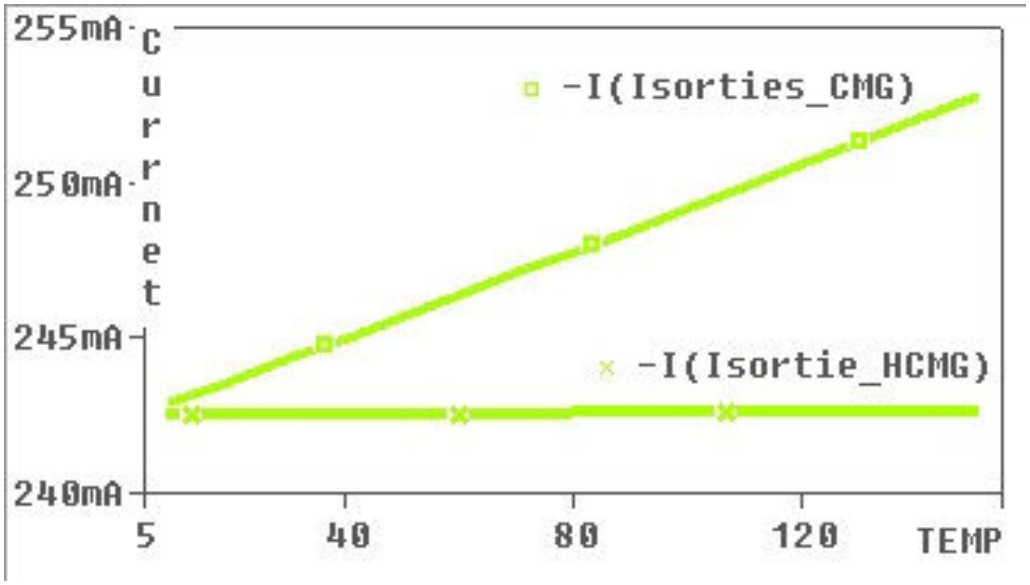

Figura 8. Current consumption behavior of CMG and M-CMG related to temperature increase

In Figure 8, the current variation from the CMG countermeasure varies $9mA$ when the temperature increases from 20^o to 150^o, while the current from M-CMG remains stable.

6. Conclusion and Further Work

In the theoretical terms and in simulation, the M-CMG shows that it can cope with the temperature variations and Early effect more than CMG. The latter characteristics allow the M-CMG to stabilize the power consumption in such a manner that DPA is even more difficult.

Given that the theoretical study of CMG was very rewarding, we are looking forward to implement a single chip with the AES with the M-CMG countermeasure and then to attack it with the DPA, in order to show in practice the efficiency of our countermeasure.

Acknowledgements

The authors are thankful to Dr Benedikt Gierlichs, Dr Josep Balasch and also to Prof. Bart Preneel, from ESAT/SCD-COSIC, Leuven Belgium, for having given us the opportunity to test the DPA and CPA attacks in their research laboratory.

The presentation of this work was founded by the FAPEMIG (Fundação de Apoio à Pesquisa de Minas Gerais), under the project PEP-00760-12.

A apresentação deste trabalho foi financiada pela FAPEMIG (Fundação de Apoio à Pesquisa de Minas Gerais), através do projeto PEP-00760-12.

Referências

Alioto, M., Poli, M., Rocchi, S., and Vignoli, V. (2006). Power modeling of precharged address bus and application to multi-bit dpa attacks to des algorithm. In *Proceedings of the 16th Power and Timing Modeling, Optimization and Simulation*, PATMOS'06, pages 593–602, Berlin, Heidelberg. Springer-Verlag.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011). Biclique cryptanalysis of the full aes. Cryptology ePrint Archive, Report 2011/449. `http://eprint.iacr.org/`.

Daemen, J. and Rijmen, V. (2001). National bureau of standards - advanced encryption standard. Technical Report FIPS Publication 197, National Bureau of Standards.

Early, J. (1952). Effects of space-charge layer widening in junction transistors. *Proceedings of the IRE*, 40(11):1401 –1406.

Guilley, S. (2007). *Contremesures Géometriques aux Attaques Exploitant les Canaux Cachés*. PhD thesis, Ecole Nationale Supérieure de Télécommunications, ENST.

Kocher, P., Jaffe, J., and Jun, B. (1999). Differential power analysis. In *Proceedings of CRYPTO '99*, pages 388–397, Santa Barbara, USA. Springer-Verlag.

Mangard, S., Oswald, E., and Popp, T. (2007). *Power Analysis Attacks: Revealing the secrets of smart cards*. Springer.

McAndrew, C. C. and Nagel, L. (1996). Early effect modeling in spice. *IEEE Journal of Solid-State Circuits*, 31(1):136 –138.

Mesquita, D., Techer, J.-D., Torres, L., Robert, M., Cathebras, G., Sassatelli, G., and Moraes, F. (2007). *IFIP Series: VLSI-SOC: From Systems to Chips*, chapter 7, pages 317–330. Springer Verlag, College Station, Texas.

Mesquita, D., Techer, J.-D., Torres, L., Sassatelli, G., Cambon, G., Robert, M., and Moraes, F. (2005). Current mask generation: A new hardware countermeasure for masking signatures of cryptographic cores. In *Proceedings of VLSI-SoC*, page in press, Perth, Australia.

Messerges, T., Dabbish, E., and Sloan, R. (1999). Investigations of power analysis attacks on smartcards. In *Proceedings of USENIX'99*, pages 151–162.

Munro, P. C. (1991). Simulating the current mirror with a self-heating bjt model. *IEEE Journal of Solid–State Circuits*, 26:1321–1324.

Parikh, C. and Patel, P. (2007). Iperformance evaluation of aes algorithm on various development platforms. In *Proceedings of ISCE'07*, pages 1–6.

