

A Masked Correlated Power Noise Generator as a Second Order DPA Countermeasure to Secure Hardware AES Cipher

Najeh Masmoudi Kamoun, Lilian Bossuet, Adel Ghazel

▶ **To cite this version:**

Najeh Masmoudi Kamoun, Lilian Bossuet, Adel Ghazel. A Masked Correlated Power Noise Generator as a Second Order DPA Countermeasure to Secure Hardware AES Cipher. Proceeding of the 3rd IEEE International Conference on Signals, Circuits and Systems, SCS 2009, pp. 1-6, Djerba, Tunisa, November 2009., Nov 2009, Tunisia. pp.1-6. hal-00679944

HAL Id: hal-00679944
https://hal.science/hal-00679944

Submitted on 16 Mar 2012

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.

A Masked Correlated Power Noise Generator use as a Second Order DPA Countermeasure to Secure Hardware AES Cipher

Najeh Kamoun[1], Lilian Bossuet[2], and Adel Ghazel[1]
[1]CIRTA'COM, SUP'COM
Tunis, Tunisia
najeh.kamoun@supcom.rnu.tn, adel.ghazel@supcom.rnu.tn
[2] Laboartoire Hubert Curien, University of Lyon
Saint-Etienne, France
lilian.bossuet@univ-st-etienne.fr

***Abstract* —Actually, only one Second Order Differential Power Analysis (SO-DPA) countermeasure has been published. This solution is multiple masking solutions. It consume a lot of area and need to design two independent True Random Number Generator (TRNG). This work proposes a new SO-DPQ countermeasure for AES cipher. It combines a simple masking solution with the CPNG countermeasure. Our solution optimizes area overhead and reduces the total number of TRNG. The robustness of the novel method is demonstrated with experimental method using FPGA implementation.**

Keywords: DPA, AES, FPGA, countermeasures, hardware security.

I. INTRODUCTION

Side channel attacks exploit information that leaks from physical implementations of cryptographic algorithms. The analysis of this leakage reveals information on the secret data manipulated by the implementation. Among the side channel attacks, the Differential Power Analysis (DPA) [1] is one of the most powerful against unprotected cryptographic implementations: it allows extracting the value of a secret key with only a few leakage measurements. A DPA is a statistical attack that correlates a physical leakage with the values of intermediate variables that depend on both the plaintext and the secret key. To avoid information leakage, the manipulation of sensitive variables must be protected by adding countermeasures [2-3].

Protected design is secured from the first DPA attack. But they are not secured from Higher Order DPA (HO-DPA) attack. In our work, we are interested only on the Second Order DPA (SO-DPA) attack. It needs a combing function in order to join the mutual information in two points in the traces of power consumption. The number of countermeasure in the first order is rising up to date. Unfortunately, there is a single countermeasure for the SO-DPA attack which uses multiple random masking [4]. It basic idea is to combine two simple masking countermeasures. Its robustness is relied to the dependency between the two TRNGs used in this countermeasure. To optimize the performance of SO-DPA countermeasure, we introduce a new countermeasure. In order to avoid the use of the two TRNGs, we combine two first order DPA countermeasures: the simple masking countermeasure with the Correlated Power Noise generator CPNG [5]. We verify the performance of this solution and its robustness.

This paper is organized in seven parts. The first one is the current introduction. The second one describes the SO-DPA attack principle. It indicate the combined function used in this attack. In the third one, we list the existing countermeasures for this type of attack. In the four one, we present our new SO-DPA countermeasure. In the five one, we give an experimental validation of our solution. In the six one, we compare the performance between our solution and the multiple masking. Finally, we conclude in the seven one.

II. SO-DPA ATTACK PRINCIPLE

A. Attack description

The aim of the SO-DPA attack is to retrieve the secret key K from the leakage signals $L(t)$ during the execution of known plaintext D_{in} unless the existence of the First Order DPA (FO-DPA) countermeasure. The leakage signals in this attack are traces of power consumption. We need then in SO-DPA attack to collect power consumption traces from cryptographic design. Usually, the SO-DPA attack is applied in cryptographic implementation secured from the FO-DPA attack only. In this case, the masked solution is the most used [4]. To surpass the first order countermeasure, the solution is to combine two leakage signals $L(t_1)$ and $L(t_2)$ at two distinct instants t_1 and t_2. The combining functions used in the SO-DPA attack are generally the product one and the absolute difference. The second step of SO-DPA attack is to apply a differential analysis method in order to extract the secret key K. This method can be the mean distance [1], the maximum likelihood [6] test and the correlation analysis [7]. Generally, it is the last processing data is the most used in the SO-DPA attack. For this raison, we choose this method.

B. Combining function of SO-DPA attack

The choice of the combining function is very critical part in SO-DPA attack. It describes the method to join the information in the power consumption traces. In the literature, there are two main combining functions: the absolute difference value [8] function and the improved product function [9]. In our work [10], we have shown that the improved product function is more efficient that the absolute value and it is adapted to second order DPA attack for hardware implementation.

III. SO-DPA ATTACK COUNTERMEASURES

For the second order DPA attack, the only efficient countermeasure is the multiple masking introduced by

Schramm [4]. Its basic idea is to use two independents masks M_1 and M_2 for the same plaintext D_{in}. The figure 1 explains the principle idea of this countermeasure.

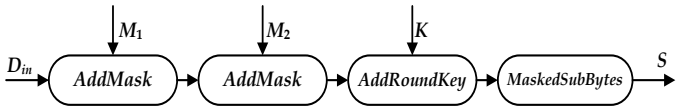


Figure 1. Principales of mutiple masking countermeausre

But this countermeasure can be viewed as the same mask $M=M_1 \oplus M_2$. This intermediate value doesn't generate any leakage signal.

Piret *et al*[11] study the multiple masking countermeasure. This studies permits to improve the robustness of masking countermeasure. The figure 2 presents the adaptation of this countermeasure in hardware solution. *ModifiedSubBytes*1and *ModifiedSubBytes*2 is given by the equation (1)

$$ModifiedSubBytes1(D_{in}, K, M_1, M_2) = SBox(D_{in} \oplus K \oplus M_1 \oplus M_2) \oplus M_1$$

$$ModifiedSubBytes2(D_{in}, K, M_1, M_2) = SBox(D_{in} \oplus K \oplus M_1 \oplus M_2) \oplus M_1 \oplus M_2 \quad (1)$$

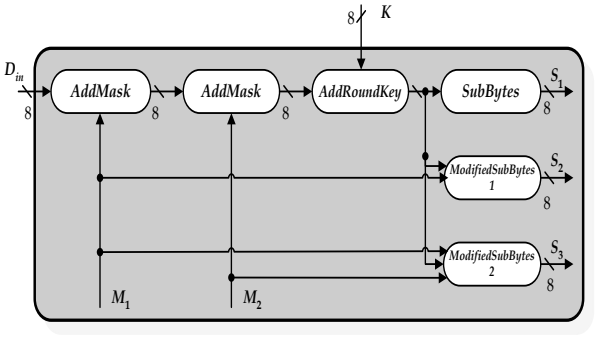


Figure 2. Hardware implmentation of multiple masking countermeasure

The robustness of the multiple masking depends in the independence between the two TRNGs used in this countermeasure. We will introduce a new countermeasure with a one TRNG in the next part.

IV. PRINCIPLE OF MCPNG COUNTERMEASURE

To improve the robustness of the multiple masking countermeasure for SO-DPA attack, we have the idea to replace one of the simple masking solution by the Correlated Power Noise Generator (CPNG) one which have been already published [5]. In fact, the principle of the proposed architectural countermeasure against SO-DPA attack is to combine two first-order-DPA countermeasures: the simple masking countermeasure [12] and the CPNG one. The figure 3 describes the basic idea of this new second order Masked Correlated Power Noise Generator (MCPNG) countermeasure.

The plaintext D_{in} is the input of the function *AddMask*. It applies a xor operation between D_{in} and the random mask M. The input of the first iteration of masked AES mD_{in} is inserted also in the masked correlated noise power generator. This generator is composed of two modules *AddRoundKey* and the *MaskedSubytes*. This last module is generated with the smallest masked S-Box [13]. In the masked correlated noise generator, we use the interference key K_{interf} in order to generate the power noise correlated with the bloc with the useful key K.

The signals S and S_{interf} are protected from the first DPA with the simple masking countermeasure. In order to prevent from SO- DPA attack and make the mutual information unused, we interfere the power of the signal S with the power noise S_{interf}. We will show experimentally the robustness of the MCPNG countermeasure for second order DPA attacks.

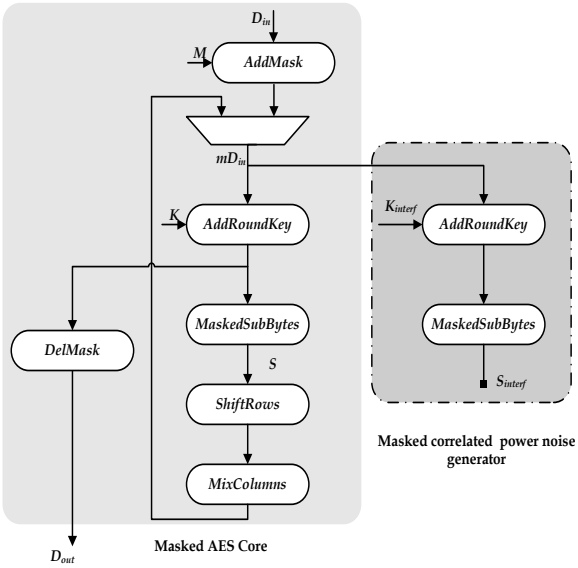


Figure 3. Description of the new second order countermeasure.

V. EXPRIMENTAL VALIDATION AND RESULT

A. DPA experimentation

The second order DPA attack is composed by three parts:

- Collecting the consumed power traces related to secured cryptographic design,
- Combining the power traces with the combining function *C*,
- Predicting the correct key by using the analysis correlation on the combined traces with power model defined by the prediction function.

We realize the second order DPA attack on the secured design from the first order DPA attack only. The experimental setup [10] is composed by a digital oscilloscope, computer and FPGA board. The communication between the computer and the scope is realized by General Purpose Interface Bus GPIB IEEE-488. The digital oscilloscope has 100 MHz bandwidth and 200 MS/s maximum rate sampling. The FPGA board is the Actel flash fusion AFS-600. The measure of the power consumption is done by inserting a 0.2 Ω resistor between the power supply and the FPGA board. A signal trigger is generated by the board to synchronize acquisition of power consumption and time execution of the design under attack. We collect the power consumption traces of design implemented with flash FPGA. We employ the improved product combining function. To retrieve the secret key *K*, we choose the correlation analysis.

B. SO-DPA attack on the simple masking and CPNG countermeasures

In this part, we realize two SO-DPA attacks. The first attack is for design protected by the CPNG countermeasure only. The second one is for AES implementation secured with simple masking solution. In first attack, we consider the AES implementation secured with CPNG countermeasure. The figure 4 gives the different part of this implementation. We realize a SO-DPA attack on this design. We can retrieve the secret key as illustrated by the figure 5. In the second attack, we implement the AES design secured with the simple masking solution. The figure 6 describes design under attack. We realize SO-DPA attack on this design. The figure 7 shows that we can extract key.

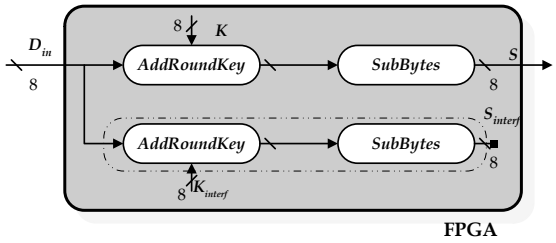


Figure 4. Implemnation of the beginning of the first AES iteration secured with CPNG countermeasure

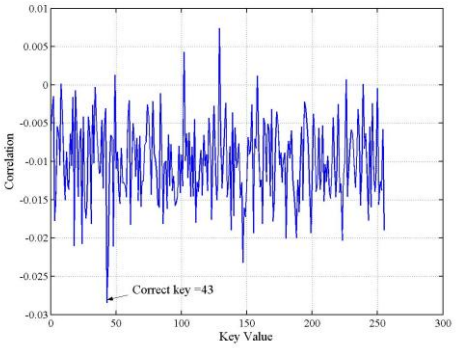


Figure 5. Illustration of secsseful SO-DPA attack secured by the CPNG with a number of traces 20480, the correct key K=43

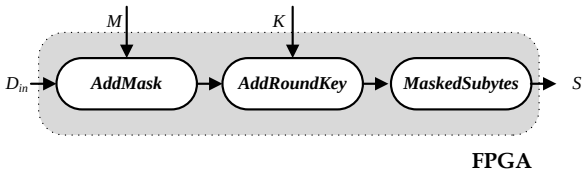


Figure 6. Implemnation of the beginning of the first AES iteration secured with masking countermeasure

C. SO-DPA attack on design secured with MCPNG countermeasure

In this experience, we use the proposed countermeasure MCPNG. In order to generate correlated masked power noise, the same masked input is applied into two blocs composing from *AddRoundKey* and *MaskedSubBytes*. The figure 8 illustrates this design. The bloc that employs the interfering key is considered to be a correlated masked power noise for the other bloc which employs the secret key *K*.

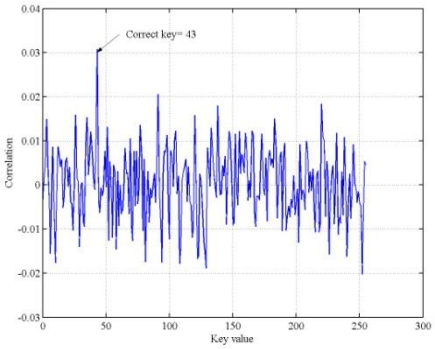


Figure 7. Succesufull second order DPA attack on masking countermeasure with K= 43 and 20480 traces

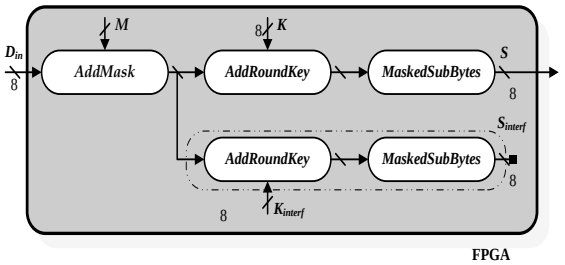


Figure 8. Implemnation of the beginning of the first AES iteration secured with MCPNG countermeasure

The power consumption model chosen for correlation analysis is given by the equation (2) Where $\boldsymbol{H}$ is the Hamming weight.

$$PM = \boldsymbol{H}\left(\left(MaskedSubBytes(D_{in} \oplus K)\right) \oplus (D_{in} \oplus K)\right) \qquad (2)$$

The second order DPA attack on the design secured with MCPNG can't extract the secret key *K*. The number of traces is 20480. It is the same number that is necessary to achieve the attack as mentioned [10]. The figure 9 illustrate the failure of this attack with the correct key is equal to K=43 and the multiplication point P_M=153. The table I gives some correlation values for different points of multiplication. We have done the multiplication for possible values of power consumption. The attack time is about 72 hours calculated with a computer which horologe frequency is 2.8 GHz.

Table I. Simulation results for second order DPA attack on design secured with MCPNG countermeasure

P_M	41	42	43	44	45	46	47	48	49	152
ρ_k	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03
k	249	249	39	138	138	138	138	138	120	246
ρ_K	0,02	0,02	0,02	0,02	0,01	0,01	0,02	0,02	0,02	0,02

VI. IMPLEMENTATION PERFORMANCES OF MCPNG COUNTERMEASURE

The implementation of the countermeasure MCPNG needs to design two modules AddRoundKey and MaskedSubytes. In order to compare the performances of countermeasure to multiple masking, we implement these two modules by three configurations:

- Unsecured AES S-Box using the smallest solution designed by Canright [13],
- Secured AES S-Box with the multiple masking with the smallest masked S-Box [14] ,
- Secured AES S-Box with the countermeasure MCPNG.

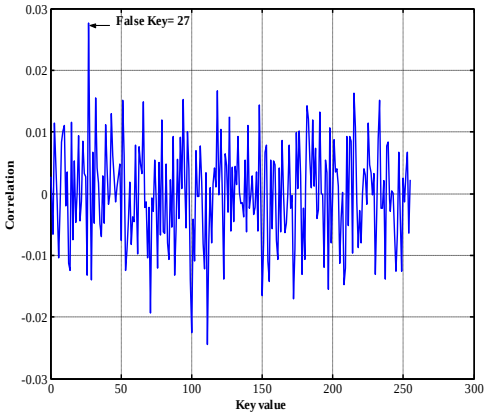


Figure 9. Illustration of unsecsseful SO-DPA attack on secured design by MCPNG countermeausre ,with a number of traces 20480, the correct key K=43

The table II gives the implementation results with a Xilinx Virtex4 SRAM FPGA. It shows that the proposed countermeasure MCPNG use a number of materiel resources lightly small than the multiple masking. The improvement of our solution is 11 slices of Virtex 4 to implement *AddRoundKey* and *MaskedSubytes*. We notice the cost of security from the second order DPA attacks is very high compared with a circuit unsecured from all order DPA attack or secured from the first DPA attack.

In our comparison, we have not considered the surface of the true random generator for masks generation. Our solution needs only one random mask whereas the multiple masking solution uses two different masks. As a consequence, our solution consumes less TRNG than the multiple masking solution. Moreover security is not only base on TRNG but also on the correlated power noise. We think that it is suitable against fault injection method, nevertheless this last point have never been studied. Our solution MCPNG has the same horologe frequency than multiple masking. Actually, the *AddMask* makes the critical path longer in both cases. Moreover, the MaskedSubBytes used in the two solutions has a critical path longer than the usual module SubBytes.

VII. CONCLUSION

In this paper, a new countermeasure called MCPNG for second order DPA attacks against AES is introduced. This solution improves lightly the performances of second order DPA countermeasure. Its basic idea is to combine two first order countermeasures to have a second order DPA countermeasure. Those countermeasures are the CPNG countermeasure [5] and the simple masking solution. This new countermeasure uses the masked correlated power noise generator to prevent the exploitation of mutual information in power consumption traces. The MCPNG countermeasure robustness is proved by experimental attack.

Table II Performance comparaionbetween AES S-Box implementation on Viretex SRAM FPGA with differents configuration

Performance	**SBox AES**		
	Unsecured [13]	***Secure with masking* [14]**	***Secure with proposed method***
Area (slices)	36	239	**228**
Area overhead	0%	+ 563%	**+ 533%**
Frequency (MHz)	184	144.6	**144.6**
Frequency decreasing	0%	-39.4%	**-39.4%**

REFERENCES

[1] P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in the proceedings of Cypto 1999, Lecture Notes in Computer Science, vol 1666, pp 398-412, Santa-Barbara,USA, August 1999, Springer-Verlag.

[2] F.-X. Standaert, E. Peeters, J.-J. Quisquater, *On the Masking Countermeasure and Higher-Order Power Analysis Attacks*, in the proceedings of ITCC 2005 (vol 1), pp 562-567, Las Vegas, USA, April 2005.

[3] K. Tiri, M. Akmal, I. Verbauwhede, «*A Dynamic and Differential CMOS Logic with Signal Independant Power Consumption to Withstand Differential Power Analysis on Smart Cards*», In Proceedings of the IEEE 28th European**.**

[4] K. Schramm and C. Paar, « *Higher Order Masking of the AES*, »Topics in Cryptology—Proc. Cryptographers Track (CT)-RSA Conf. 2006, pp. 208-225, 2006.

[5] N.Kamoun, L. Boussuet , A. Ghazel"*Correlated Power Noise Generator as a Low Cost DPA Countermeasure to Secure Hardware AES Cipher*" SCS'2009 novembre 2009

[6] D. Agrawal, JR Rao , P Rohatgi . «*Multi-channel attacks*», In: C Walter, C Koc¸, C Paar editors. Proceedings of the fifth international workshop on cryptographic hardware and embedded systems (CHES). Lecture notes in computer science, vol. 2779. Cologne, Germany: Springer-Verlag; 2003.

[7] E. Brier, c. Clavier and F. Olivier, « *Correlation Power Analysis with a Leakage Model*», In the Proceeding of International Conference of Cryptographic Hardware and Embedded Systems, CHES04, Lecture Notes in Computer Science, vol. 3156, p. 135-152, Springer, 2004.

[8] E. Oswald, S. Mangard, C. Herbst, and S. Tillich, «*Practical Second Order DPA Attacks for Masked Smart Card Implementations of Block Ciphers*, » Topics in Cryptology—Proc. Cryptographers' Track (CT)-RSA Conf. 2006, pp. 192-207, 2006.

[9] E. Prouff, M. Rivain, R. bevan « *Statistical Analysis of Second Order Differentail Power Analysis* » Computers IEEE transactions on, June 2009 vol 58 Issue 6 p 799-811.

[10] N. Masmoudi Kamoun, L.Boussuet,A.Ghazel" Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology" ICM'2010 Cairo.

[11] G. Piret, F.-X. Standaert, « *Security Analysis of Higher-Order Boolean Masking Schemes for Block Ciphers (with Conditions of Perfect Masking)* », in IET Information Security 2008**.**

[12] National Institute of Standards and Technology (NIST). FIPS-197: *Advanced Encryption Standard*, November 2001. Available online at http://www.itl.nist.gov/fipspubs/.

[13] D. Canright and *L. Batina, «A Very Compact "Perfectly Masked" S-Box for AES*», Applied Cryptography and Network Security, ACNS 2008, June 3-6, New York.

[14] D. Canright « *A Very Compact S-Box for AES*», (on Springer-Verlag site)(2005), Workshop on Cryptographic Hardware and Embedded Systems (CHES2005), Lecture Notes in Computer Science 3659, pp.441-455, Springer-Verlag.