Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology.

Najeh Masmoudi Kamoun, Lilian Bossuet, Adel Ghazel

Experimental Implementation of 2ODPA attacks on AES design with flash-based FPGA Technology

Najeh Masmoudi[1] , Lilian Bossuet[2] and Adel Ghazel[1] .
[1]CIRTA'COM, SUP'COM
Tunis, Tunisia
najeh.kamoun@insat.rnu.tn, adel.ghazel@supcom.rnu.tn
[2] IMS, EINSEIRB
Bordeaux, France
lilian.bossuet@ims-bordeaux.fr

***Abstract*—A successful experimental second order Differential Power Analysis (DPA) on an Advanced Encryption Standard (AES) hardware implementation on flash-based FPGA technology with improved product combining function is achieved. Our choice to this combining function is justified. An experimental set-up is elaborated to implement on an FPGA board critical AES modules and DPA attack. As main contribution, this work proved the success of experimental second order DPA attack on Flash-based FPGA with improved product combining function.**

Keywords: AES, Second order DPA,Combining function, masking schemes.

I. INTRODUCTION

Side Channel analysis SCA exploits information that leaks from physical implementations of cryptographic algorithms. This leakage can be the power consumption, the electromagnetic emanations, or time execution of the cryptographic implementation. It is used to extract information on the secret data manipulated by the implementation. If the leakage channel is the power consumption of the design, the attack is called power analysis attack. In this set of attack, there are many types. The first one is the Simple Power Analysis SPA [1]. The adversary, in this attack, uses directly the trace of power consumption to retrieve the secret key. The second one is the Differential Power Analysis DPA [1]. A DPA attack is a statistical one that correlates a physical leakage with a prediction on the values taken by one or several intermediate variable of the implementation that depend on both the plaintext and the secret key. This attack can be done in the first or second order. The difference between the two order that on the first one, the adversary manipulate directly the power consumption traces, on the second one, he combine the same power traces. Moreover in the second order DPA attack, the design under attack must be protected from the first order DPA attack.

To avoid information leakage, the manipulation of sensitive variables must be protected by adding countermeasures to the algorithm. This paper only deals with algorithm Advanced Encryption Standard AES [2]. It is the most used algorithm since 2001. A very common countermeasure to protect AES implementations is to randomize their sensitive variables by masking techniques [3]. Canright *et al*[4] propose in 2008 a very compact masked *SubBytes* function for the AES cipher. Generally this countermeasure protects the AES implementation only from the first order DPA order attack. In the second order DPA [1], the adversary combines the power consumption and use a correlation analysis attack in the preprocessing data. The efficiency of the second order DPA attack is based on the choice of the combining function. The most used ones are the product and the absolute function. E. Prouff *et al.* [5] improve the product combining function. They show that is more efficient than the absolute for software implementation. In our work, we show that this combining function is also suitable to hardware implementation.

Previous research works presented interesting results relative to DPA implementations for different VLSI technologies. A great interest was given to DPA FPGA implementation but published works were limited to SRAM-based FPGA technologies [3-7].

In this paper, authors propose an experimental implementation on Flash-based FPGA of a second order DPA attack on AES. The objective is to verify the robust of this very attractive FPGA technology to higher order DPA attacks. In fact the interest for Flash-based technology comes from its great performance in term of low power consumption [8]. Actel Fusion FPGA, considered in this work, offers several sleep and standby modes of operation to further extend battery life in embedded applications.

This paper is organized as follow. In section 2, we describe the concept of second order DPA attack. In section 3, we give details of the implementation under attack. It is a masked AES implementation using the most compact *SubBytes* function. In section 4, we show our experimental results of second DPA attack on masked AES implementation with improved product combining function. In section 5, we conclude.

II. CONCEPT OF SECOND ORDER DPA ATTACK

A. Attack description

Second order DPA attack is introduced by Paul Kocher [1]. It is considered as High Order DPA attack (HOPDA) [5]. Its objective is recovering information on $Z= g(X,K)$ and then the correct key K by simultaneously considering the leakage signals at the two times t_1 and t_2 that correspond to the manipulations of two intermediate values. The attack starts by combining the two signals $L(t_1)$ and $L(t_2)$ with a combining function C and by defining a prediction function f according to some assumptions on the device leakage model. Then, for every guess k on the value of the secret K, the attacker computes the so-called prediction $f \circ g(X, k)$ and checks its validity by estimating the following correlation coefficient

$$\rho_k = \rho[C(L(t_1), L(t_2)), f \circ g(X,k)] \quad (1)$$

The correlation coefficient ρ_k for the key k is defined as follow:

$$\rho_k = \frac{Cov(C(L(t_1), L(t_2)), f \circ g(X,k))}{\sigma\left(C(L(t_1), L(t_2))\right)\sigma(f \circ g(X,k))} \quad (2)$$

Where $Cov(X,Y)$ is the covariance function between variables X and Y. $\sigma(X)$ is the standard deviation function of the variable X. If the functions f and C are well chosen, the attacker will have a higher correlation coefficient for the correct key K. To estimate the correlation coefficient ρ_k, the attacker process N leakage measurements $L_1(t)$, …, $L_N(t)$. For every key k, the estimation of ρ_k is obtained by computing Pearson coefficient $\hat{\rho}_k(N)$ between the samples f o g (X_i, k) and $C(L_i(t_1), L_i(t_2))$ $i \in [1..N]$ (X_i is the plaintext). Pearson Coefficient is defined as follow for samples x_i, y_i $i \in [1..N]$:

$$\hat{\rho}(x_i, y_i) = \frac{\sum_{j=1}^{N}(x_j - \bar{x})(y_j - \bar{y})}{\sqrt{\sum_{j=1}^{N}(x_j - \bar{x})^2}\sqrt{\sum_{j=1}^{N}(y_j - \bar{y})^2}} \quad (3)$$

As $\hat{\rho}_k(N)$ tends to ρ_k when N increases, for N large enough large, the correct key is that maximizes $\hat{\rho}_k(N)$.

Processing in second order DPA attack can be summarized by the figure 1.

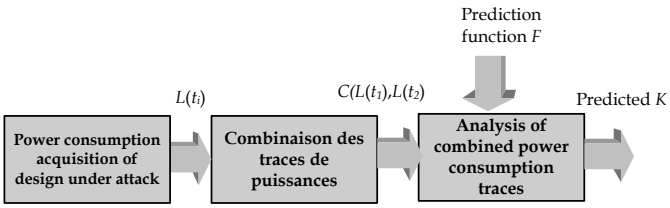

Figure 1. Principales steps of second order DPA attack.

B. Classification of combing function C for second order DPA attack

In the literature, there are two main combining functions C for the leakage signals for second DPA order attack. They are product combining function and the absolute difference one.

1) Product combining function for second order DPA attack

The product combining function is defined as follow

$$C_{prod}(L(t_1), L(t_2)) = L(t_1).L(t_2) \quad (4)$$

It is first combining function introduced by Chari et al in[12]. This function has already been studied by Schramm *et al.* in [6]. In [5], E. Prouff *et al.* give an improvement to product combining function C_p:

$$C_P(L(t_1), L(t_2)) = \left(L(t_1) - \mathrm{E}(\mathrm{L}(\mathrm{t}_1))\right).\left(L(t_2) - \mathrm{E}(\mathrm{L}(\mathrm{t}_2))\right) \quad (5)$$

They show that this combining function is the most efficient one for software implementation. In our work, we will proof that this improved combining function is suitable to hardware implementation also.

2) Absolute difference combining function for second DPA attack

The absolute difference combining function, is given by the equation (6)

$$C_{diff}(L(t_1), L(t_2)) = |L(t_1) - L(t_2)| \quad (6)$$

The absolute difference combining is introduced by Messerges [13]. It has already been studied by Joye *et al.* in [7]. In their paper, the authors consider the idealized model and analyze a single-bit second order DPA attack. In [8], Oswald *et al.* realize a practical implementation of second order DPA attack using the absolute difference combining function.

3) Sine-Based Combining Function

In [14], Oswald *et al.* propose a combining function based on the sine function. It takes as parameters the exact Hamming weights of the mask and of the masked variable:

$$C_{sin}(H(Z \oplus M), H(M)) = \sin(H(Z \oplus M) - H(M))^2 \quad (7)$$

They also suggest using the above combining function together with the following prediction function:

$$F_{sin}(Z) = -89.95 \sin(H(Z))^3 - 7.82 \sin(H(Z))^2 + 67.66 \sin(H(Z)) \quad (8)$$

In ideal case without considering noise signal and attacking the 8 bits, the use of the couple C_{sin} and F_{sin} allows an attacker to reach a correlation of 0.83, which is quite high. However, in noisy model this correlation decreases rapidly. We conclude that the sine-based combining function is not suitable for experimental attack of second order attack.

III. Implementation of Masked AES

Second order DPA attacks concern the protected design from the first order DPA attack. The common countermeasure is algorithmic one and specially the masking method. It is customized for the AES was the transformed masking method [3] by Akkar *et al.* This method was further simplified by Trichina *et al.* [9]. It was noticed in [9, 10, 3] that the multiplicative masking introduced in [3] masked only non-zero values, i.e., a zero byte will not get masked because of the multiplicative nature of the mask. This feature renders the method of Akkar vulnerable to DPAs. A second masking technique for AES is the random representation method by Golic [10]. Similar to Akkar, Golic do not try to show that their technique randomizes all intermediate results. Instead, the authors only argue experimentally that using their methods the Hamming weights of all intermediate results are distributed in roughly the same way, independent of the plaintext and secret key. However two of them, [3] and [10], are both susceptible to a certain type of (first-order) differential side-channel attack, the zero-value attack. The latter one has turned out to be vulnerable even to standard differential side-channel attacks as well. Oswald *et al.* in [11] combine the concepts of multiplicative and additive masking. They show the resistance of their implementation.

The idea of masking the intermediate values inside a cryptographic algorithm is suggested in several papers [3, 5, 8] as a possible countermeasure to power analysis. The technique is generally applicable if all the fundamental operations used in

a given algorithm can be rewritten in the masked domain. This is easily seen to be the case in classical algorithms such as AES. Figure 2 illustrates the implementation of masked AES.

The details of the masking countermeasure are as follows: the input of a cipher is blinded with random masks, which diffuse and propagate during the execution of the cipher. As a result, the side channel leakage of all intermediate, key dependent variables, which are processed by the cipher, does not correlate with the corresponding unmasked variables and side channel attacks are effectively thwarted. The most important step is the final mask correction which removes the evolved masks from the output of the cipher. While it is simple to reproduce the propagation of masks throughout linear functions in a cipher, non-linear functions, such as the substitution function on AES algorithm, require a considerable effort when it comes to the correction step. In our work, we use the most compact masked S-box introduced in [4] by Canright *et al.* They use many corrections terms to achieve the mask in substitution function. They optimize the work of Oswald *et al.* [11] by introducing normal basis in masked S-Box.

IV. Result of Experimental Second Order DPA Attack

A. Experiemental setup for second order DPA attack

Second order DPA attack is done on traces of power consumption of the design under attack. Running a cipher on this design, the attacker measures the corresponding signals. He needs essentially a digital oscilloscope, computer and FPGA board. The figure 3 summarizes the essentials components of signals acquisition. He realizes the communication between the PC and scope 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. He measures the power consumption of our design in the FPGA board by inserting a 0.2 Ω resistor between the power supply and the FPGA Board. A signal trigger is generated by the FPGA board to synchronize acquisition of power consumption and time execution of the design under attack.

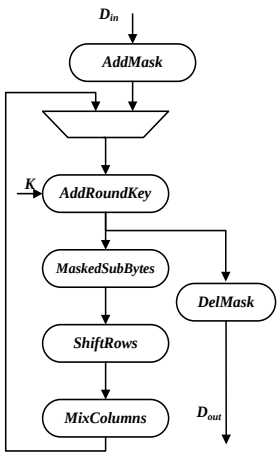

Figure 2. Architecture of masked AES

DPA attacks are generally realized on the first round with known plaintext or on the last round with known cipher text. In our case, we will realize the DPA attack with known plaintext using the Hamming weight model. The design under attack is illustrated in figure 4. It is composed by three modules: *Add mask*, *AddRoundKey* and *Masked SubBytes*. This attack is done in the 8 bits of the output of *Masked SubBytes*. We use the correlation analysis to predict the correct key.

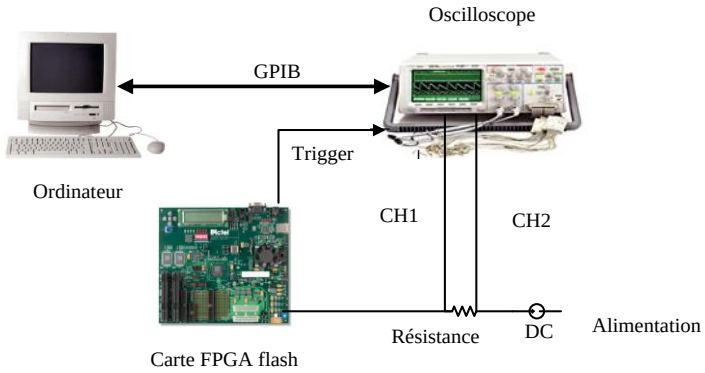

Figure 3. Experimental lab od DPA attack

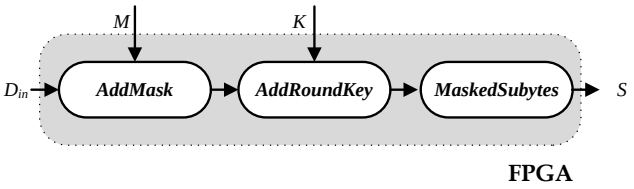

Figure 4. Design under Second order DPA attack

B. Results of first order DPA attack on masked AES

This subsection shows the resistance of the masked countermeasure for the first DPA attack. The figure 5 illustrates an unsuccessful DPA attack. This result is given by the fact of the efficiency of the masked countermeasure. The correct key is equal to 43. The false on is 252. The number of traces is 20480.

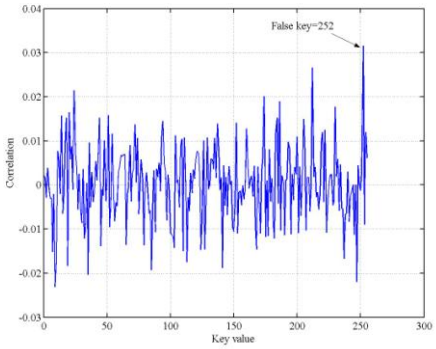

Figure 5. Unsucessuful first order DPA attack on design secured with masking with correct key *K*=43 and with 20480 traces

C. Results of second DPA attack on masked AES with improved product combining function

We use the improved product combining function described in the equation 5. It is shown that is the most efficient one for the attack on software implementation. First, we evaluate the mean of leakage for different sample the power consumption

traces in order to evaluate E($L(t_i)$). We subtract this mean for all the point to have a leakage centered in zero. For each instants $t_1$and t_2 in the power consumption traces we multiply their centered leakage. After the preprocessing step realized by this combined function, we use the correlation analysis to retrieve secret key. Figure 6 shows a successful attack with 20480 traces of power consumption. The correct key is 43. This result demonstrates the efficiency of the improved product combining function of second order DPA attack for hardware implementation.

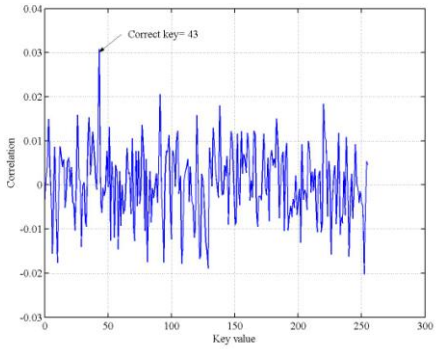

Figure 6. Succesufull second order DPA attack on masking countermeasure with *K*= 43 and 20480 traces with improved product combining function

D. Results of second DPA attack on masked AES with absolute combining function

In this experimental implementation of second order DPA attack, we use the absolute combining function described by the equation 6. For each instants $t_1$and t_2, we calculate the absolute difference leakage between $L(t_1)$ and $L(t_2)$. The numbers of traces is the same as the previous second order DPA attack with improved product combining function. We use the correlation analysis on processed leakage. The result is that the correct key is not detected for all the traces power consumption. That implies this combining function needs more traces than with improved product one. This emphasizes the fact that the improved product combining function is more suitable for experimental attack on hardware design.

V. CONCLUSION

An experimental implementation of a second order Differential Power Analysis (DPA) attack for Advanced Encryption Standard (AES) encryption algorithm on Flash-based FPGA is proposed. After analyzing processing requirements for two different combining functions for second order DPA attack, the choice of the improved product combining function is justified. An experimental set-up is defined to implement on an FPGA board critical AES modules and DPA attack. Main contribution of our work is relative to proving for the first time, according to our knowledge, the success of second order DPA attack on Flash-based FPGA technology with the improved product function. Experimental results showed that for different secret key values a maximum of correlation with the correct key is obtained during 48 h of data acquisition and processing time. Hence this paper contribution shows that this new and low-power technology suffers also from the higher order of side channels attacks. It becomes necessary to define suitable countermeasure for DPA attacks to protect the key. Authors proposed in [7] a masking scheme for SRAM-based FPGA technology. Moreover, we show that the combining improved product function is the most efficient than the absolute difference combining function for second order DPA attack on hardware design.

Ongoing research is being carried by authors to define second order DPA countermeasure technique for Flash-based FPGA technology and introducing a novel combining function.

REFERENCES

[1] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "*Differential Power Analysis*".In Michael Wiener, editor, Advances in Cryptology - CRYPTO '99,19th Annual International Cryptology Conference, Santa Barbara, California,USA, August 15-19, 1999, Proceedings, volume 1666 of Lecture Notes in Computer Science, pages 388–397. Springer, 1999.

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

[3] M.-L. Akkar and C. Giraud "*An Implementation of DES and AES, Secure against Some Attacks*" Workshop on Cryptographic Hardware and Embedded Systems CHES 2001, volume LNCS 2162, pages 309-318. Springer-Verlag, May 14-16, 2001.

[4] D. Canright and L. Batina, "*A Very Compact Perfectly Masked S-Box for AES*", Applied Cryptography and Network Security, ACNS 2008, S. Bellovin and R. Gennaro (eds.), LNCS 5037, Springer-Verlag, pp. 446-459, June 3-6, New York.

[5] 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.

[6] 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.

[7] M. Joye, P. Paillier, and B. Schoenmakers, "*On Second Order Differential Power Analysis*," Workshop Cryptographic Hardware and Embedded Systems (CHES 2005), J. Rao and B. Sunar, eds., pp. 293-308, 2005.

[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. Trichina, D. De Seta, and L. Germani. "*Simplifed Adaptive Multiplicative Masking for AES*". Workshop on Cryptographic Hardware and Embedded Systems CHES 2002, volume LNCS 2523, pages 187-197. Springer-Verlag, 2002.

[10] J.Dj. Golic and C. Tymen. "*Multiplicative Masking and Power Analysis of AES*".Workshop on Cryptographic Hardware and Embedded Systems CHES 2002, volume LNCS 2523, pages 198-212. Springer-Verlag, 2002.

[11] E. Oswald, S. Mangard, N. Pramstaller, V. Rijmen, "*A side-channel analysis resistant description of the AES S-box*". International Workshop on Fast Software Encryption FSE 2005. LNCS, vol. 3557, pp. 413–423. Springer, Heidelberg (2005)

[12] S. Chari, C. Jutla, J. Rao, and P. Rohatgi, "*Towards Sound Approaches to Counteract Power-Analysis Attacks*," Advances inCryptology—Proc. Int'l Crytology Conf. (CRYPTO '99), M. Wiener,ed., pp. 398-412, 1999.

[13] T. Messerges, "Using Second Order Power Analysis to Attack DPA Resistant Software," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES 2000), C¸. . Koc¸ and C. Paar,eds., pp. 238-251, 2000.

[14] E. Oswald and S. Mangard, "Template Attacks on Masking-Resistance is Futile," Topics in Cryptology—Proc. Cryptographers' Track (CT)-RSA 2007 Conf., M. Abe, ed., pp. 562-567, 2007