Current Balancing Random Body Bias in FDSOI Cryptosystems as a Countermeasure to Leakage Power Analysis Attacks

KENNETH PALMA1, and FRANCESC MOLL1, (Senior Member, IEEE)
1Department of Electronic Engineering, Universitat Politècnica de Catalunya (UPC), 08034 Barcelona, Spain
Corresponding author: Kenneth Palma (e-mail: kenneth.palma@upc.edu).
This research was funded by Spanish MCIU/AEI/10.13039/501100011033, Project PID2019-103869RB-C33/, by Secretaria d’Universitats i Recerca of Generalitat de Catalunya, and by the European Social Fund

ABSTRACT This paper identifies vulnerabilities to recently proposed countermeasures to leakage power analysis attacks in FDSOI systems based on the application of a random body bias. The vulnerabilities are analyzed and the relative difficulty to obtain the secret key, once the vulnerabilities are taken into account, are compared to the original proposals. A new countermeasure, based on a new body bias scheme, is then proposed. The new countermeasure is based on the equalization of asymmetries in static power consumption dependent on data being stored in registers implemented in FDSOI technology. The countermeasure’s effectiveness is theoretically established through the development of a power model based on technological parameters, and further reinforced through numerical simulations of a dummy cryptosystem implementing part of an AES encrypting round.

INDEX TERMS Body bias, Correlation Power Analysis, Countermeasures, Cryptography, FDSOI, Leakage Power Analysis, Side-Channel

I. INTRODUCTION

The exploitation of power consumption of cryptographic circuits as a source of information and a means to retrieve the secret key has been extensively studied in the last two decades [1]. These so called Power Analysis Attacks (PAA) rely on asymmetries in power consumption that arise from differing circuit states subjected to the data being processed in intermediate stages of encrypting algorithms.

Traditionally, PAA have mainly focused on the dynamic power consumption of cryptographic circuits to derive statistical models of power consumption based on the data being processed. These models of power consumption allow the testing of secret key hypothesis with a minimum setting and quick computation.

PAA traditionally rely on statistical metrics, namely, the Difference of Means or the Pearson Correlation Coefficient (PCC) [2], to test secret key hypothesis given a correct power model. Since power consumption is dependent on processed data which is, in turn, dependent on the secret key, the power consumed by a cryptographic circuit is highly correlated with its correct secret key. Countermeasures to PAA attempt to decorrelate this relation.

As a rule of thumb, countermeasures to PAA can be separated in two categories: those that introduce uncorrelated noise during the execution of the encrypting algorithm, thus obfuscating meaningful correlation between the power consumption model and the measurements taken [3] [4]; and those that attempt to reduce the asymmetries in power consumption that arise from differing circuit states [5] [6]. Both types of countermeasures effectively reduce the Signal to Noise Ratio (SNR) utilizing different principles.

Nonetheless, as transistor nodes progress further into the nanometer scale, the contribution of leakage power to overall power consumption becomes more significant. With the reduction of operating voltages and standard-cell area that accompanies shorter transistors’ channel length, dynamic power consumption is scaled down, while traditional bulk technologies experience an increase in leakage current from various physical phenomena [7]. As a result, the last decade has seen an emergence of PAA based on the static power.
consumption of cryptographic circuits [8] [9], along studies of their feasibility as well as potential countermeasures.

Fully depleted silicon-on-insulator (FDSOI) technologies address some of the short channel effects that contribute to the increase of leakage current in shorter nodes [7]. At the same time, their structure allows the application of a wide dynamic range of body bias. Recent studies [10] [11] have proposed taking advantage of this wide body bias dynamic range as a means to introduce static power noise, thus hindering the acquisition of the secret key.

On the other hand, the authors in [12] have recently developed and simulated standard cells that equalize the static power consumption of combinational and sequential logic in nanometer bulk technology.

In this paper, we explore and analyze the feasibility of utilizing a body bias scheme that can effectively act as a current equalizer between register states. Section II presents a summary of the findings and analyses performed in [10] and [11]. Section III describes how these findings can be undone through a bivariate power model, while Section IV presents a numerical analysis of the effect of this new power model on symmetric random body bias. Sections V and VI describe the new proposed countermeasure and its rationale, as well as how the analyses are performed. The results of these analyses are presented in Section VII. Lastly, conclusions follow.

II. BACKGROUND
An analysis of the different leakage currents in which a register can incur depending on the data that it stores was formalized in [8]. In the article, the authors identify 3 magnitudes of interest; namely, $I_1$, $I_0$ and $\epsilon$ which are, respectively, the leakage current of a register that stores a 1, a 0, and their difference ($\epsilon = I_1 - I_0$).

With these, the authors of [8] established a power model of the leakage current of an $n$-bit register array that stores an intermediate result on an encryption process.

$$I_{\text{leak}}(HW) = n \cdot I_0 + \epsilon \cdot HW$$ (1)

Where $HW$, the Hamming Weight, is the number of ones stored in the register slice of interest. In a block cryptosystem, the $HW$ is a function of the plaintext, the secret key, and the non-linear substitution performed by an S-box.

Given the linear dependence between the leakage current consumed by the register array and the Hamming Weight of the word stored, this power model can be used to perform Correlation Power Analysis Attacks (CPAA) [2].

In [10] and [11], the authors explore the potential of utilizing cryptosystems implemented in FDSOI technology to dynamically modify the leakage currents of the register arrays by changing the body bias so as to introduce uncorrelated noise that decreases the correlation between the Hamming Weight and the leakage consumption.

The countermeasure presented in [10] and [11] relies on the application of a symmetrical random body bias level at the beginning of the encryption process. The body bias level is symmetrical in the sense that its absolute value is the same for NMOS and PMOS transistors: that is, $V_{bb,N} = -V_{bb,P}$. This body bias level is maintained throughout the whole process. At the beginning of a new encryption process, a new body bias level is set, following a random sequence.

Explorations on the leakage consumption of registers under a varying body bias are presented in [11], where it is shown that, for the technology and libraries studied in the article, the different leakage currents of interest (when a register stores a 1, a 0, and their difference) are exponentially dependent on the absolute value of the body bias under the symmetric conditions above described.

Under these conditions, the leakage current of an $n$-bit register slice can be shown to be:

$$I_{\text{leak}}(|V_{bb}|, HW) = n \cdot I_0(|V_{bb}|) + HW \cdot \epsilon(|V_{bb}|)$$ (2)

Where both $I_0(|V_{bb}|)$ and $\epsilon(|V_{bb}|)$ are exponential functions of the form:

$$f(|V_{bb}|) = a \cdot e^{b|V_{bb}|}$$ (3)

With $a$ and $b$ being technological parameters.

Differing values of body bias decorrelate the leakage current values from the Hamming Weight for successive encryption processes.

In fact, it can be shown that, assuming that the distribution of the random variable $|V_{bb}|$ establishes a well-defined distribution of $I_0(|V_{bb}|)$, the Pearson Correlation Coefficient (PCC) between the leakage current and the Hamming Weight of the register array becomes:

$$\rho_{I_{\text{leak}}, HW} = \frac{\epsilon \cdot \sigma_{HW}}{(n^2 \cdot \sigma_{I0}^2 + \epsilon^2 \cdot \sigma_{HW}^2)^{1/2}}$$ (4)

Where $\sigma_{I0}^2$ is the variance of $I_0(|V_{bb}|)$, $\sigma_{HW}^2$ is the variance of the Hamming Weight, and we have assumed that the variance of $\epsilon(|V_{bb}|)$ is comparatively negligible so it can be considered a constant.

The effectiveness of the countermeasure is demonstrated both in [10] and [11]. In [10], the authors provide empirical testing on the countermeasure under a variety of conditions. In [11], an analytical model is developed and contrasted against electrical and Monte Carlo simulations of a dummy cryptosystem.

However, this countermeasure has some limitations. First, as already analyzed in [11], trace averaging can undermine the countermeasure at the expense of an increased number of required measurements. Secondly, once a state of the cryptosystem is identified, the countermeasure can be fully undermined.

In the next section, we present and analyze this problem. The rest of the article is devoted to the development of a new body bias scheme that can address these vulnerabilities.

III. BIVARIATE POWER MODEL
Consider a block cryptosystem that comprises several rounds of encryption. Consider a state register, where intermediate values of the encryption process are stored. In the AES
cryptosystem, this state register is represented by the state matrix. Consider an attack where the \( n \) bits of interest are evaluated at time \( t_2 \). Assume that, at a previous time, at time \( t_1 \), the same state register stores some bits that are known to the attacker.

Assume, also, that the attacker is able to track the progression from the value stored at time \( t_1 \) to the value stored at time \( t_2 \). In the AES cryptosystem, \( t_1 \) can represent the initialization phase, when the plaintext is loaded onto the state register, and \( t_2 \) the evaluation after the first round of encryption. Or, alternatively, \( t_1 \) can represent the time of evaluation of an encryption round for which all previous roundkeys are already known, and \( t_2 \) represents the evaluation time of the following round of encryption.

Regardless of how the attack is conceptualized, we assume that the state value and therefore the HW at time \( t_1 \) is known to the attacker for every possible plaintext, and the progression from the values stored at \( t_1 \) to the values stored at \( t_2 \) is a function of an unknown secret key under attack.

Thus, the leakage currents of this particular register slice at times \( t_1 \) and \( t_2 \) can be expressed as:

\[
I_{\text{leak}}(V_{bb}, HW_{t_1}) = \mu_0(\lvert V_{bb} \rvert) + HW_{t_1} \cdot \sigma(V_{bb}) \tag{5}
\]

\[
I_{\text{leak}}(V_{bb}, HW_{t_2}) = \mu_0(\lvert V_{bb} \rvert) + HW_{t_2} \cdot \sigma(V_{bb}) \tag{6}
\]

While \( HW_{t_2} \) is an unknown value, given that both rounds belong to the same encryption process, the value of \( V_{bb} \) remains constant between equations (5) and (6). As such, it can be seen that in the above equations, only the Hamming Weights are different. It is then possible to obtain a new power model of the leakage current by subtracting equation (6) from equation (5).

\[
I_{\text{leak}}(V_{bb}, HW_{t_1,t_2}) = \sigma(V_{bb}) \cdot (HW_{t_2} - HW_{t_1}) \tag{7}
\]

Since the main source of decorrelated noise introduced by this countermeasure is provided by the factor \( n \cdot I_0(\lvert V_{bb} \rvert) \), which varies between encryption processes, but remains constant during the same encryption process, much of the effectiveness of the countermeasure proposed in [10] and [11] is eliminated by performing this subtraction.

While \( HW_{t_1} \) and \( HW_{t_2} \) might be uncorrelated, given the effect of an S-Box, they are not independent. As such, performing an accurate analysis of the probability distribution that accompanies these variables can be hard to generalize.

Nonetheless, we can perform some simplified analysis by considering that, together, they form a new random variable:

\[
Z = HW_{t_2} - HW_{t_1} \tag{8}
\]

With expected value and variance equal to:

\[
\mu_Z = 0 \tag{9}
\]

\[
\sigma_Z^2 = 2 \cdot \sigma_{HW_{t_1}}^2 = n/2 \tag{10}
\]

Where we have considered that the variance of \( HW_{t_1} \) is \( \frac{n}{4} \), following from a plaintext of \( n \) bits, independent from each other, with a uniform probability distribution. These assumptions are reinforced by numerical simulations that are addressed in later sections.

Thus, equation 7 can be expressed as:

\[
I_{\text{leak}}(\lvert V_{bb} \rvert, Z) = \epsilon(\lvert V_{bb} \rvert) \cdot Z \tag{11}
\]

With these considerations, the PCC between equation (11) and the variable of interest, \( Z \), in the presence of the countermeasure introduced in [11] can be shown to be, without algorithmic or non-algorithmic noise, and with a correct key:

\[
\rho_{I_{\text{leak}},Z} = \frac{\mu_\epsilon}{\sqrt{\sigma_\epsilon^2 + \mu_\epsilon^2}} \tag{12}
\]

Where \( \mu_\epsilon \) and \( \sigma_\epsilon^2 \) are, respectively, the expected value and variance of \( \epsilon(\lvert V_{bb} \rvert) \).

By performing inter-trace averaging, the noise introduced by the countermeasure \( (\sigma_\epsilon^2) \), already significantly smaller once the subtraction has been performed, can be reduced. That is, if for every input plaintext of interest that evaluates to \( z \), the encryption process is repeated \( N \) times, the resulting, averaged traces would see their sources of noise reduced to \( \sigma_\epsilon^2/N \).

In the following section we evaluate the effect that this post-processing has on the countermeasure proposed in [10] and in [11].

IV. SYMMETRIC BODY BIAS BIVARIATE POWER MODEL

In order to compare the effectiveness of the countermeasure against a bivariate leakage model we utilize the same body biasing scheme as in [11]:

\[
\lvert V_{bb} \rvert(S) = V_{bbQ} + \Delta V_{bb} \cdot S \tag{13}
\]

Where \( V_{bbQ} \) is the quiescent point of the body bias, \( \Delta V_{bb} \) the step increase of the body bias, and \( S \) a discrete uniform random variable that can adopt any integer value between \( [-s_{\text{max}}, s_{\text{max}}] \), with probability \( P(S = i) = \frac{1}{2s_{\text{max}}+1} \) for every \( i \) such that \( -s_{\text{max}} \leq i \leq s_{\text{max}} \).

This way, \( \epsilon(\lvert V_{bb} \rvert) \) can be expressed as:

\[
\epsilon(S) = a \cdot b^{-(V_{bbQ} + \Delta V_{bb} \cdot S)} \tag{14}
\]

Utilizing the same registers from the same technological library as in [11], the parameters \( a \) and \( b \) can be extracted and the variance and expected value of \( \epsilon(S) \) calculated.

We perform the comparison by solving equation (12) for different numbers of \( s_{\text{max}} \) and plotting it against the univariate leakage considered in [11] under equal countermeasure conditions: \( V_{bbQ} = 0.5V \), \( \Delta V_{bb} = \frac{DR}{2s_{\text{max}}} \), with \( DR \) being the maximum allowable dynamic range of the body bias for the technology; in this case, \( 1V \), and with \( n = 8 \) bits under attack. The results can be seen in Fig. 1.

It can be seen that, under the same countermeasure conditions, the PCC of the bivariate case is much higher than that of the univariate leakage.

Furthermore, the rate of increase of the PCC under trace averaging conditions is much higher for the bivariate case.

Under trace averaging conditions, with \( N \) traces per plaintext, the different variances are scaled by a factor of \( \frac{1}{N} \).
Table 1 shows the value of the PCC for the univariate and bivariate cases when $s_{max} = 25$, with the maximum body bias Dynamic Range allowed by the technology, for different number of traces $N$.

| $N$  | PCC Univariate | PCC Bivariate |
|------|----------------|---------------|
| 1    | 0.0476         | 0.875         |
| 10   | 0.1489         | 0.985         |
| 100  | 0.4300         | 0.9983        |
| 1000 | 0.8331         | 0.9998        |

It can be seen that, for the bivariate case, very few traces are required to achieve almost maximum correlation, thus significantly facilitating the acquisition of the secret key even in the presence of the countermeasure.

The following sections are devoted to the development of a body bias scheme that can offer protection against these considerations.

V. CURRENT BALANCING BODY BIAS

In order to address these vulnerabilities we begin by noting that the signal of interest that conveys information regarding the secret key is the variable $\epsilon$. Specifically, the expected value of $\epsilon$, which appears in the numerator of equation (12). Thus, the PCC between the leakage current consumption and the Hamming Weight of the bits of interest are directly proportional to $\mu_\epsilon$.

The definition of $\epsilon$, stated above, is the difference between the leakage current consumed by a flip-flop that stores a $1$ and a flip-flop that stores a $0$. Since the body bias allows us to modify the leakage current profile of the registers, we wish to explore if a body bias scheme exists that would arbitrarily reduce this difference, essentially reducing the SNR, not by introducing uncorrelated noise, but by reducing the magnitude of the signal of interest.

In order to do so, sufficient simulations are performed to extract the curves of $\epsilon$ as a function of both $V_{bbn}$ and $V_{bbp}$ for the registers under study. Figure 2 shows a collection of curves resulting from a double parametric sweep. The different curves represent the value of $\epsilon$ for varying $V_{bbp}$ with a fixed value of $V_{bbn}$, whose value ranges from 0 V (the uppermost curve) to 1 V (the one at the bottom).

Observing the set of curves for $\epsilon(V_{bbn}, V_{bbp})$ it can be seen that there exists a subset of values of the $xy$-plane defined by $(V_{bbn}) \times (V_{bbp})$ where $\epsilon \approx 0$. This can be seen by noting the zero-point crossings for different curves in the body bias sweep represented by the horizontal red curve of Fig. 2.

The different curves of $\epsilon(V_{bbn}, V_{bbp})$ are then extracted and with the help of Matlab’s fitting tools, expressed as a bivariate polynomial of degree $n$ of the following form:

$$\epsilon(V_{bbn}, V_{bbp}) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{ij} V_{bbn}^i V_{bbp}^j$$

With $a_{ij}$ as the different polynomial coefficients. A polynomial of degree $n = 4$ is sufficient to fit the data with an $R^2$ value of 1.

An algorithm is then implemented to solve for all the pairs of values of $V_{bbn}$ and $V_{bbp}$ such that $|\epsilon(V_{bbn}, V_{bbp})| \leq c$, where $c$ is a constant that can be set arbitrarily small.

We set $c \leq 1$ nA and solve for the pair of body bias values of $V_{bbn}$ and $V_{bbp}$ that make the register under study present leakage currents such that $|I_1 - I_0| = |\epsilon| \leq 1$ nA. We obtain two contour lines, whose encased area represents the possible pairs of $V_{bbn}$ and $V_{bbp}$ values that solve for the above conditions (Fig. 3).
Once a countermeasure that serves as a countermeasure protecting against leakage power analysis attacks. With these considerations we can establish a body bias scheme. At the beginning of a new encryption process, a new value of \( V_{bbn} \) is chosen independently and at random, and the process begins anew.

These values are maintained during the encryption process. At the beginning of a new encryption process, a new value of \( V_{bbn} \) is chosen independently and at random, and the process begins anew. We consider the positive body bias, \( V_{bbn} \), a random variable of the form:

\[
V_{bbn}(S) = V_{bbq} + \Delta V_{bb} \cdot S
\]

Where the different terms are defined as:

\[
V_{bbq} = \frac{V_{bb_{min}} + V_{bb_{max}}}{2}
\]

\[
DR = V_{bb_{max}} - V_{bb_{min}}
\]

\[
\Delta V_{bb} = \frac{DR}{2s_{max}}
\]

With \( DR \) as the Dynamic Range of the body bias, limited to the domain of the positive body bias \( V_{bb} \) where there exist a value of negative body bias that meets the imposed criterion. The value of the negative body bias is set accordingly following equation (16).

With these considerations we now have a model with which to determine the effectiveness of this proposed countermeasure.

To do so, we solve equation for the PCC between the Hamming Weight of the bits of interest and the bivariate leakage (Equation (12)) under noiseless assumption and in the presence of algorithmic and non-algorithmic noise. It is necessary to determine the expected value and variance of \( \epsilon \) under these conditions. Given the model above derived, these can be determined numerically utilizing the following definitions.

\[
Var(\epsilon(S)) = E[\epsilon(S)^2] - E[\epsilon(S)]^2
\]

\[
E[\epsilon(S)] = \frac{1}{2s_{max} + 1} \sum_{i=-s_{max}}^{s_{max}} \epsilon(V_{bbn}(i), b_1 - b_2 \cdot V_{bbn}(i))
\]

\[
E[\epsilon(S)^2] = \frac{1}{2s_{max} + 1} \sum_{i=-s_{max}}^{s_{max}} \epsilon^2(V_{bbn}(i), b_1 - b_2 \cdot V_{bbn}(i))
\]

**VI. PROPOSED COUNTERMEASURE**

With these considerations we can establish a body bias scheme that serves as a countermeasure protecting against attacks with a bivariate power model described in previous sections.

Consider a countermeasure that fixes the body bias value \( V_{bbn} \) of registers at the beginning of an encryption process. Once \( V_{bbn} \) is fixed, \( V_{bbp} \) is adjusted until the value of \( \epsilon \) reaches a certain threshold. These values are maintained during the encryption process. At the beginning of a new encryption process, a new value of \( V_{bbn} \) is chosen independently and at random, and the process begins anew.

We consider the positive body bias, \( V_{bbn} \), a random variable of the form:

\[
V_{bbn}(S) = V_{bbq} + \Delta V_{bb} \cdot S
\]
It might seem at first that current balancing body bias contemplated in previous sections presents significantly worse values (a higher PCC that can facilitate the acquisition of the secret key). This can be explained by noting that, under noiseless assumptions, the only source of noise is determined by the variance of $\epsilon$ and the variances of the Hamming Weights. Since in the Current Balancing body bias scheme the Dynamic Range of the body bias is limited, the variance of $\epsilon$ is smaller.

However, consider the case of a noisy system. That is, Equations (5) and (6) now present a superposed Gaussian White Noise (GWN) with variance $\sigma_b^2$. By performing the aforementioned subtraction, Equation (7) would now present, by considering additive noise, a GWN of variance $2\sigma_b^2$.

At the same time, if the value of $s_{max}$ is fixed to 32 and we plot the PCC against the number of averaged traces for the same noise conditions, it can be seen (Fig. 6) that the Pearson Correlation Coefficient increases much more slowly when the Current Balancing body bias scheme is applied. That is, non-algorithmic noise severely dominates.

### A. ALGORITHMIC AND NON-ALGORITHMIC NOISE

The results so far consider an n-bit register array, with $n = 8$ bits, subjected to some source of non-algorithmic, white gaussian noise.

A more realistic scenario considers a cryptosystem that processes $n + m$ bits, with $n$ being the the bits of interest under attack, and $m$ the rest of bits not pertinent to the attack that introduce algorithmic noise.

The bivariate power model under these conditions (Equation (11)) becomes:

$$I_{\text{leak}1,2} = \epsilon(S) \cdot (Z_n + Z_m) + B$$

(22)

Where $Z_n$ is defined in Equation (8) as the difference between the Hamming Weight of the bits of interest $n$ after a round of encryption and before the round of encryption. Similarly, $Z_m$ is defined as the difference between the Hamming Weight of the remaining $m$ bits not pertinent to the attack after and before the same round of encryption.

$$Z_m = HW_{mt2} - HW_{mt1}$$

(23)
As in previous discussions, \(HW_{mt2}\) and \(HW_{mt1}\) might be uncorrelated but are not independent. In order to be able to treat them analytically, we make some assumptions regarding the distribution of \(Z_m\).

\[
\begin{align*}
\mu_{Z_m} & = 0 \\
\sigma^2_{Z_m} & = m/2
\end{align*}
\]  

The magnitude \(B\) represents a gaussian white noise term with zero mean and variance equal to \(2\sigma^2_b\) considering additivity.

With this, it can be shown that the PCC between the bivariate power model and \(Z_n\) is:

\[
\rho_{I_{\text{leak}}, Z_n} = \frac{\mu_{I_{\text{leak}}} \sigma_{Z_n}}{\sqrt{\sigma^2_{Z_m} + \sigma^2_{\epsilon}} (\mu^2 + \sigma^2_{\epsilon}) + 2\sigma^2_b}\]  

FIGURE 7. PCC between \(Z_n\) and the bivariate leakage power model with algorithmic and non-algorithmic noise (Equation 26) as a function of noise power under a current balancing body bias, for different number of \(N\) averaged traces.

Figure 7 shows that for small noise powers (below \(-160\) or \(-170\) dBW depending on the number of averages) algorithmic noise dominates as a factor. In fact, it can be shown that for small magnitudes of gaussian noise power the countermeasure, under a bivariate attack, barely introduces noise. As such, the PCC between \(Z_n\) and the leakage current can be approximated as:

\[
\rho_{I_{\text{leak}}, Z_n} = \frac{\sigma_{Z_n}}{\sqrt{\sigma^2_{Z_m} + \frac{\sigma^2_{\epsilon}}{N}}} = \sqrt{\frac{n}{n + \frac{m}{N}}}
\]  

Thus, only when non-algorithmic noise becomes comparatively high is current balancing body bias significantly effective.

On the other hand, Fig. 8 presents a comparison between the PCC (Equation (26)) obtained through current balancing and symmetric body bias under the conditions presented in Table 2 as a function of noise power for a number of averaged traces \(N = 1000\). It can be seen that the current balancing case is much more susceptible to noise power, as expected by the reduction of the signals of interest.

FIGURE 8. PCC between the Hamming Weight and the bivariate leakage power model with algorithmic and non-algorithmic noise (Equation 26), as a function of noise power under a a Symmetrical (blue) and a Current Balancing (orange) random body bias scheme for \(N = 1000\) averaged traces.

**B. NUMERICAL SIMULATIONS**

We mount a numerically simulated CPA attack on a dummy cryptosystem that reflects the bivariate power model described above and summarized in Equation (22), under the countermeasure conditions established in Table 2.

In order to do so, we set an 128-bit secret key that represents a round key. The dummy cryptosystem comprises a round of encryption of the AES up to the \texttt{S-Box} routine, without including the former \texttt{MixColumns} routine, that is, we consider that the whole state matrix after the \texttt{MixColumns} routine is known to the attacker and directly consider this state the input plaintext. Each of the 16 bytes of the plaintext are then XORed with their corresponding byte of the secret key. Each XORed byte is then fed to the AES S-Box and the result is again considered to be stored in the state matrix.

The attack is performed on \(n = 8\) bits (1 byte). For each input plaintext \(i\) of interest (with \(0 \leq i \leq 255\)), \(N\) realizations of Equation (22) are numerically simulated. For each realization, the 15 remaining bytes of the plaintext are generated at random, each bit following a uniform probability distribution. The random variable \(S\) is also realized randomly following the distribution described in Section IV under the constraints described in Section V, thus generating a random body bias value that keeps \(\epsilon \approx 1\) nA. Finally, for each of the \(N\) realizations, a white gaussian noise value following the
distribution described above, for a noise power of -134 dBW is also produced.

The $N$ realizations are then averaged:

$$I_{\text{leak}}(Z_{ni}, \hat{Z}_m, \hat{S}) = \frac{1}{N} \sum_{j=1}^{N} \epsilon(s_j)(Z_{ni} + Z_{mj}) + B_j \quad (28)$$

Thus, a vector comprising 256 $I_{\text{leak}}$ values, one for each possible plaintext is obtained. The PCC between this vector and the vector $Z_n$ solved for each possible 8-bit secret key is calculated.

**TABLE 3.** PCC - Theoretical and Numerical Simulations of a 128 bit system in the absence of non-algorithmic noise

| N    | Theo CPA | Success Rate |
|------|----------|--------------|
| 1    | 0.239    | 0.196        | 0.6          |
| 10   | 0.630    | 0.645        | 1            |
| 100  | 0.932    | 0.933        | 1            |
| 1000 | 0.993    | 0.993        | 1            |

**TABLE 4.** PCC - Theoretical and Numerical Simulations of a 128 bit system in the presence of non-algorithmic noise

| N    | Theo CPA | Success Rate |
|------|----------|--------------|
| 1    | 0.001    | -0.000       | 0            |
| 10   | 0.032    | 0.025        | 0            |
| 100  | 0.100    | 0.0945       | 0            |
| 1000 | 0.302    | 0.305        | 0.7          |

Tables 3 and 4 present the results of the PCC obtained for the secret key under attack for the simulated CPA and the theoretical value obtained through Equation (26) for different number $N$ of averaged traces. It can be seen that, in both cases, as the number of averaged traces increase, the values of the PCC obtained through numerical simulations becomes closer to the theoretical values. The tables also include the success rate of secret key identification for 10 independent experiments.

At the same time, Table 5 presents the values of the expected value and variance of $Z_m$ for increasing number of averaged traces. As $N$ increases, the first and second moment of $Z_m$ more closely resemble the theoretical values that had been previously assumed; namely, that $\mu_{Z_m} = 0$ and that $\sigma_{Z_m}^2 = \frac{m}{2} = 60$, with $m$ being the number of bits not under attack, 120 in this particular simulation.

**TABLE 5.** First and Second Moments of $Z_m$

| N    | $\mu_{Z_m}$ | $\sigma_{Z_m}^2$ |
|------|-------------|------------------|
| 10   | 4.400       | 25.82            |
| 100  | -0.640      | 66.43            |
| 1000 | 0.250       | 62.20            |
| 5000 | -0.018      | 59.16            |

be highly undermined once a known state of the cryptosystem is obtained.

A new countermeasure against leakage power analysis attacks is presented in response to these findings. The countermeasure exploits the backgate of FDSOI transistors to modify the leakage current profile of registers, diminishing the asymmetries that arise from stored data.

Results show that the countermeasure effectiveness is dependent on the magnitude of noise power present in the circuit or measuring system. While no such analysis is presented, the magnitude of $\epsilon$ clearly determines, as well, the effectiveness of the proposed scheme. In this paper the authors have restricted themselves to a value of $\epsilon \approx 1 \text{nA}$, adopting a conservative stance before a system implementation is made.

The results presented are obtained for registers implemented with Low Threshold Voltage (LVT) transistors. However, simulations and analysis have also been performed for registers implemented with higher VT transistors. These results have been omitted for simplicity, as they did not differ significantly from the ones presented.

An important observation that stems from the results obtained is that the variance of $\epsilon$ is negligible as compared to the other sources of noise in the circuit (be them algorithmic or non-algorithmic), and has little impact on the effectiveness of the countermeasure. In a perfect implementation in which the value of $\epsilon$ were to remain exactly the same at all times, the variance of $\epsilon$ would actually be 0. Because of this, it is not necessary to choose the value of the body bias at random. This would free the system implementation of a True or Pseudo Random Number Generator, and design efforts could be devoted to a system that maintains $\epsilon$ as small as possible for differing operating temperatures.

Further studies should focus on circuit design of the proposed countermeasure to study the practical limitations of its implementation.

**REFERENCES**

[1] M. Randolph and W. Diehl, “Power side-channel attack analysis: A review of 20 years of study for the layman,” Cryptography, vol. 4, no. 2, 2020.

[2] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 3156, pp. 16–29, 2004.

[3] N. Zhu, Y. Zhou, and H. Liu, “Counteracting leakage power analysis attack using random ring oscillators,” in PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, pp. 74–77, 2013.

[4] W. Yu and S. Köse, “False key-controlled aggressive voltage scaling: A countermeasure against lpa attacks,” IEEE Transactions on Computer-
Aided Design of Integrated Circuits and Systems, vol. 36, no. 12, pp. 2149–2153, 2017.

[5] C. Palmini and J. V. R. Ravindra, “Calpan: Countermeasure against leakage power analysis attack by normalized ddpl,” in 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1–7, 2016.

[6] D. Bellizia, G. Scotti, and A. Trifiletti, “On-chip analog current equalizer as a countermeasure against side-channel attacks in cmos nanometer technology,” in 2016 MIXDES - 23rd International Conference Mixed Design of Integrated Circuits and Systems, pp. 229–234, 2016.

[7] T. Skotnicki, J. Hutchby, T.-J. King, H.-S. Wong, and F. Boeuf, “The end of cmos scaling: toward the introduction of new materials and structural changes to improve mosfet performance,” IEEE Circuits and Devices Magazine, vol. 21, no. 1, pp. 16–26, 2005.

[8] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, “Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 2, pp. 355–367, 2010.

[9] S. M. Del Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, “Side-channel attacks from static power: When should we care?,” in 2015 Design, Automation Test in Europe Conference Exhibition (DATE), pp. 145–150, 2015.

[10] B. A. Dao, T. T. Hoang, A. T. Le, A. Tsukamoto, K. Suzuki, and C. K. Pham, “Exploiting the back-gate biasing technique as a countermeasure against power analysis attacks,” IEEE Access, vol. 9, pp. 24768–24786, 2021.

[11] K. Palma and F. Moll, “Analysis of random body bias application in fdsoi cryptosystems as a countermeasure to leakage-based power analysis attacks,” IEEE Access, vol. 9, pp. 114977–114988, 2021.

[12] B. Fuadania, T. Moos, and A. Moradi, “Balancing the leakage currents in nanometer cmos logic a challenging goal,” Applied Sciences, vol. 11, no. 15, 2021.

[13] T. Moos, A. Moradi, and B. Richter, “Static power side-channel analysis—an investigation of measurement factors,” IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 376–389, 2020.

[14] N. I. of Standards and Technology, “Advanced encryption standard,” NIST FIPS PUB 197, 2001.

KENNETH PALMA received the B.Sc. degree in Electronic Engineering and the M.Sc. degree in Electronic Engineering, with a focus on microelectronics from the Universitat Politècnica de Catalunya (UPC), Barcelona, Spain, in 2017 and 2019, respectively. He is currently pursuing the Ph.D. degree in Electronic Engineering from the Universitat Politècnica de Catalunya, developing countermeasures to Leakage Power Analysis Attacks in FDSOI circuits.

FANCESC MOLL is a professor in the Department of Electronic Engineering of the Universitat Politècnica de Catalunya (UPC) since 1997. He received in 1991 the equivalent of the M.Sc. degree in physics from the University of Balearic Islands, Spain, and in 1995 the Ph.D. degree in Electronic Engineering from UPC. His research career has been focused on reliability and robustness issues relevant to integrated circuit design especially in advanced technology nodes, such as signal integrity modeling and its impact, manufacturing variability and ultra low power and voltage circuits. 12

***