Integration, the VLSI Journal 68 (2019) 71–79

Contents lists available at ScienceDirect

Integration, the VLSI Journal

journal homepage: www.elsevier.com/locate/vlsi

A security oriented transient-noise simulation methodology: Evaluation of intrinsic physical noise of cryptographic designs

Kashif Nawaz *, Léopold Van Brandt, Itamar Levi, François-Xavier Standaert, Denis Flandre

ICTEAM Institute, Université Catholique de Louvain, Belgium

A B S T R A C T

Noise in digital circuits has always been minimized to achieve high signal integrity, robust operation and of course high performance. However, for cryptographic applications, increased noise can in fact be beneficial. It can be used effectively to reduce the (cryptographic) Signal-to-Noise (SNR) ratio and to make it harder for an adversary to extract useful information (*e.g.,* secret keys) from the side channel leakage data. A natural question concerns the extent to which intrinsic (internal) noise is required to improve security. In this manuscript, we explore this question and further introduce a methodology to exploit the intrinsic physical noise (*i.e.,* flicker- and thermal-noise) at the secure circuit level. We additionally demonstrate how the values obtained from our methodology translate into relevant cryptographic metrics. Our simulations show that the calculated cryptographic noise values are in close agreement with the noise levels extracted from noisy distributions using transient noise analysis. We finally evaluate (with the proposed methodology) several meaningful parameters which affect the internal noise (and their security extent) such as transistors-sizing and voltage-supply changes.

1. Introduction

Side-channel attacks, such as differential power analysis (DPA) [1], exploit physical-leakage signals from a cryptographic device to extract sensitive information (*e.g.,* cryptographic keys). Circuit logic-styles such as differential dual-rail, have been proposed to reduce the signal within the leakage. However, with technology scaling their (leakage) signal reduction is hindered by increased capacitance imbalances compared to standard CMOS logic styles [2] (*e.g.,* moving from 65 nm to 28 nm nodes). Existing countermeasures against side-channel analysis such as shuffling (adding noise in time domain) and masking (or algorithmic noise, adding noise in the amplitude domain) work well in scenarios where the SNR has been sufficiently reduced. Exploring how to increase the intrinsic physical noise coming from the transistors themselves or its security extent (to reduce the SNR) is very important. Mainly due to the fact that such noise element is inherent (*intrinsic*) to the device itself, and it is quite challenging for an adversary to eliminate/reduce it. In this manuscript, we explore the design of *noisy* CMOS implementations, and propose a methodology to accurately evaluate the *intrinsic* physical MOSFET noise allowing designers to derive insights and understanding of its impact through gate-level simulations. More specifically, we investigate a methodology to answer the following questions, *i.e.,* can we derive a concrete methodology to link inherent MOSFET noise to well established cryptographic merits, how does the noise (and its security implications) scale with the number of transistors/devices or their sizes, and how does it behave as a function of the voltage supply (for e.g, a common side-channel attack scenario in which adversaries lower the supply voltage).

This work is an extension of the paper presented at the *PRIME 2018 conference* [3]. We have extended our analyses to include: (1) a comprehensive Mutual Information (MI) analysis (2) a study of the impact of varying the flicker noise factor, K_f, on the cryptographic metrics such as the SNR and the MI and (3) expanding the experimental section of the manuscript. This paper is divided into 5 sections. We first review the relevant state-of-the-art for this work, then in Section 3 we discuss our methodology to introduce noise sources to the simulated setting, the simulation cost and accuracy tradeoffs and the choice of simulation parameters. In Section 4 we discuss the results of our simulation methodology. We wrap up with conclusions and perspectives in Section 5. We also append the existing material (from the PRIME conference publication) on statistical security analysis of the leakages obtained from our simulations in Appendix section.

2. Background: noise models and security metrics

In this section we layout the basic tools (metrics) which will be used to perform security-evaluation. Namely, the well-known (crypto)[1] *Signal-to-Noise ratio* (SNR) and the *Mutual Information* (MI). We also

* Corresponding author.
E-mail address: kashif.nawaz@uclouvain.be (K. Nawaz).

[1] We use the terms cryptographic and crypto interchangeably, they both denote the one and same thing.

https://doi.org/10.1016/j.vlsi.2019.06.006
Received 7 October 2018; Received in revised form 1 April 2019; Accepted 17 June 2019
Available online 27 June 2019
0167-9260/© 2019 Elsevier B.V. All rights reserved.

briefly discuss a (simplified) physical-noise model which we will refer through out the manuscript.

2.1. Signal-to-noise ratio (SNR)

A simple (fast to compute) metric which is commonly used to quantify the cryptographic leakage from a side channel (leakage from a concrete device) is the univariate Signal-to-Noise ratio metric. In this paper, we use Mangard's SNR defined in Ref. [4] as:

$$\mathrm{SNR} = \frac{\widehat{\mathrm{var}}_x(\hat{\mathrm{E}}_i(L_x^i))}{\hat{\mathrm{E}}_x(\widehat{\mathrm{var}}_i(L_x^i))}, \tag{1}$$

where $\hat{\mathrm{E}}$ (resp. $\widehat{\mathrm{var}}$) denotes the sample mean (resp. variance) operator and L the leakage and the prefix i refers to the number of noisy traces (collected) (or runs simulated) and x to the digital inputs. In our following simulations, this SNR will be computed for noise-based traces of the current consumption of the logic circuit at the supply rail as a function of time, denoted as $i_{DD}(t^*)$ and would include the noise coming from physical *intrinsic* MOSFET noise sources. Briefly revising (1), the numerator represents the signal that is, the "useful" part of the leakage which is obtained by the adversary as a measure of the information leakage. It can be seen as the content of the leakage that is identically reproduced for each given attack and varies with the attack data vector. Ideally, it tries to capture the variance of the leakage as a function of the logical inputs in a noiseless setting. The lower the signal value, the lower the "perceived" side-channel leakage. The denominator represents the noise element within the leakage, i.e the random variation of the leakage that is (at least, partly) ucorrelated with the attack. The maximum signal, as a metric to quantify the leakage in a hypothetical noiseless scenario has been used lately by the authors [2]. It was shown that under technology scaling (from 65 nm bulk to 28 nm FDSOI tech.) dual rail logic styles lose their security advantage whereas, standard CMOS gain in security, especially while lowering the supply voltage, V_{DD}.

Apart from design simplicity, performance and area degradation, the above mentioned results justify the choice of standard CMOS implementations in scaled-down technologies over dual-rail styles and provides the necessary motivation for the design of *noisy* CMOS implementations.

2.2. Mutual information (MI) metric

The Mutual-Information Analysis attack (MIA) has been first introduced by Ref. [5] and expanded to a security-evaluation information theoretic metric in the framework introduced by Standaert et al., [6]. Let $\mathrm{L_q}$ be a random vector representing the leakage functions obtained after q queries (in this case, noisy simulated runs) and $\mathrm{l_q}$ be a realization. X is the attack vector and x is a realization (a single input transition) from X, then the MI is given by:

$$\widehat{\mathrm{MI}(X;L)} = \mathrm{H[X]} - \sum_{\mathrm{x}\in\mathrm{X}} \Pr[x] \sum_{\mathrm{l}\in\mathrm{L}} \Pr_{\mathrm{simu}}[l \mid x].\log_2 \Pr_{\mathrm{simu}}[x \mid l] \tag{2}$$

where, H denotes the entropy, Pr[x] denotes the probability of the input variable x, Pr[l | x] is the conditional probability of the leaked variable for a given input, and Pr[x | l] the conditional probability of the input given the leakage. In essence, the metric quantify how much can be learned on X from the leakage L for any given leakage probability distribution function (PDF), compared to the SNR which is limited to first-order moments only.

In scenarios where the leakage probability distribution function is Gaussian and independent of the noise, i.e. considering univariate Gaussian random variables (as is our case), the SNR and MI metrics are equivalent [7]. However, the MI is a more generic and easy metric to interpret conclusions as a function of parameters like the physical noise or the supply voltage. Additionally, it shows how much further noise needs to be added externally to reduce the information leakage and achieve a desired security level. We use this property intensively in this manuscript to visualize the security level as a function of the (*intrinsic*) noise variance.

The relation between these two metrics has been studied in Ref. [8] under the Gaussian and independence assumptions and it is possible to show that the relation is monotonic (for reasonable SNR levels)[2]

$$\mathrm{MI(X;L)} \approxeq -\frac{1}{2} \cdot \log_2 \left(1 - \left(\frac{1}{\sqrt{1+\frac{1}{SNR}}}\right)\right)^2 \tag{3}$$

2.3. Noise models: a brief review

Thermal (and shot) noise can be modeled for simulations as a Gaussian noise current source connected in parallel to a noiseless element such as a resistor (the resistor is, of course, considered noiseless). The thermal (current) noise across the resistor can then be represented using the following equation [9].

$$i_{th}(t) = \sqrt{\frac{2kT}{R}}\zeta(t) \tag{4}$$

where k is the Boltzmann's constant, T the absolute temperature in K and R the resistance. $\zeta(t)$ is a stationary white noise Gaussian process having a constant power spectral density (PSD). For a MOSFET in strong inversion, the thermal noise can be modeled by:

$$I_{ntg}^2 = 4kT\left(\frac{2g_m}{3}\right) \tag{5}$$

where g_m is the small signal transconductance at the bias point.

It is well known that the Flicker noise is the dominant source of noise in MOS transistors and dominates the noise spectrum at lower frequencies [10]. It is also commonly referred by $1/f$ noise as the spectrum follows $1/f^{\alpha}$ as a function of the frequency, where α is the flicker noise exponent and has a value close to unity ($\alpha = 1 \pm 0.2$). The PSD of flicker noise in a MOSFET can be generalized as

$$S_i(f) = \frac{i_f^2}{\Delta f} = \frac{K_f'}{C_{ox}^2 WL}\frac{1}{f} \tag{6}$$

where $\mathrm{C_{ox}}$ is the gate capacitance per unit area, W the channel width, L the channel length and f the frequency. The constant $\mathrm{K_f'}$ is the flicker noise coefficient and is dependent on the process technology. Hence the PSD of flicker noise is time varying as a function of the frequency. Due to this reason (as shown in (6)), the flicker noise cannot be directly used in a transient noise analysis as it is a non-stationary noise process. However, it is possible to simulate such noise by representing the elements as a white noise current source with a resistor R_m and capacitor C_m connected in parallel [11]. In short, by using a synthesized RC circuit which sums up the Lorentzian spectra and approximates it as a $1/f$ PSD by

$$S(f) = \frac{2kT}{\pi C_m}\sum_{m=1}^{M}\frac{\varphi_m}{\varphi_m^2 + f^2} \propto \frac{1}{f} \tag{7}$$

where φ_m is the pole frequency of each Lorentzian spectra. This is the methodology used by advanced circuit simulators with advanced device modeling and characterization process [12,13].

[2] for real world scenarios this relation does not hold and deviations are observed as the leakge distributions are not strictly Gaussian in nature.

3. Transient noise analysis: a simulation methodology

Conventional noise analyses in analog and RF circuit designs mostly use the ac or the harmonic based approaches. However, in digital cryptographic applications, where each point in a transient run is potentially a source of information leakage (from an adversary perspective), it makes it worth analyzing the effect of noise on *each* time sample. From a cryptographic perspective, this is a univariate analysis compared to a multivariate analysis (where multiple time-samples are used). In the scope of this work, we focus on the univariate aspect only. The time sample with the highest value of signal (or SNR) is chosen as the point-of-interest (POI), as this usually represents the worst case for defending against a side-channel adversary. Using the transient noise simulation tool in Eldo circuit-simulator software (provided by Mentor Graphics) [14], we provide a methodology to evaluate the *intrinsic* physical noise sources (i.e., noise coming from the transistors themselves and *not* externally) and calculate the resulting "cryptographic" signal and noise (units of A^2) as defined in (1), and compare them to the values obtained from ac simulations and variance calculations.

In this section, we aim at validating all the aspects of the methodology, both mathematically and physically, by (1) defining our target designs and simulation settings, (2) determining the simulation parameters in view of a cost-precision tradeoff, and (3) validating the impact of the low-frequency noise factor by an ac analysis. To be complete and fully guarantee the meaningfulness of our results, appendix validates the physics of the first-order statistics of the noise present in the supply current of one circuits of interest.

3.1. Target designs

Our results are based on transient noise simulations in an Eldo environment while using a 28 nm FDSOI PDK (process design-kit) provided by an industrial foundry. This PDK is characterized to provide advanced UTSOI v2 [15] noise-simulation abilities of all the noise-parameters discussed above (and many more). In most experiments performed in this research, the sizing of the transistors is kept minimum to maximize the noise produced (flicker noise especially which is reversely proportional to gate-area). We use a simple 2-bit XOR, a 4-bit PRESENT Sbox and an 8-bit AES S-box to show scalability of our results in a relevant cryptographic context. All of which were custom designed using Cadence Virtuoso software, to show the scaling trends of the signal and noise w.r.t the supply voltage and the number of transistors.

3.2. Simulation settings

Our 3 designs are simulated with the Transient Noise analysis built in Eldo (called *.noisetran* tool) with up to 100 transient noise runs (where the noise variance was verified to converge). The noise sources correspond to the physical flicker and thermal noises intrinsic to the MOS transistors. They are generated by Eldo in the frequency bandwidth specified by the input parameters of the transient noise analysis. Two important simulator choices need to be made, the number of transient noisy runs (*nruns* parameter) and the maximum frequency of the noise generating sources (FMAX parameter). The choice of these two parameters is certainly not arbitrary and forms the basis of our methodology where we provide a framework of how to choose these two important parameters which affect the Figures-of-Merit (FoMs) and the CPU runtime.

The input data signals to the circuits covers all possible arbitrary digital input transitions (i.e. 4, 16 and 256 transitions for the 2-input XOR, 4-bit PRESENT and 8-bit AES S-boxes, respectively) at a clock frequency of 10 MHz. All simulations are done at 298 K, *TT* (typical-typical) process corner and for a supply voltage V_{DD} range of 0.5 V–1 V.

3.3. Simulation cost and tradeoffs

In this subsection, we investigate the cost of our methodology and quantify the total budget, both in terms of CPU runtime and number of runs required to obtain convergence in our metrics which estimate the "crypto" signal and noise.

The noise transient simulations are indeed well known to be time- and memory-intensive [16]. Basically, our simulation budget can be stated as

$$N_{traces} \cdot \frac{T}{\mathrm{d}t}, \tag{8}$$

where N_{traces} is the number of traces,[3] i.e., noise realizations, T is the simulation duration for one trace, and dt is the time step. These parameters correspond to NBRUN, *TSTOP*, and.OUTSTEP of Eldo NOISETRAN [14], respectively. The number of time samples for each trace is given by

$$N_s = \frac{T}{\mathrm{d}t}. \tag{9}$$

We now formally present our *methodology* which is used throughout our work for choosing the simulation parameters of interest and extracting the relevant cryptographic figures-of-merit based on such carefully chosen parameters.

3.3.1. Physical noise versus simulated noise

In physics, every *intrinsic* noise source has an *infinite bandwidth*. Let us take the white thermal noise as the most trivial but illustrative example:

$$S_{i,\mathrm{th}}(f) = \frac{4kT}{R}. \tag{10}$$

PSD such as (10) describes how the expected average intrinsic noise power (or simply the average intrinsic noise power if ergodicity is assumed) is distributed in frequency:

$$\sigma_i^2 \equiv \int_0^{+\infty} S_i(f)\,\mathrm{d}f \quad \text{(definition of the PSD)}. \tag{11}$$

Plugging (10) into (11), we quickly observe the following apparent paradox:

$$\sigma_i^2 = \frac{4kT}{R} \cdot \infty = \infty?$$

If one tries to perform the same calculation using rather a flicker noise PSD, such as (6) presented in section 2, he would again obtain a theoretical infinite noise power.

Such a paradox is fortunately solved by experiment: one never measures such an intrinsic noise source. We mean that there is always some *filtering* or *band limitation* effect arising from the measurement equipment on one hand, from the circuit or device under measurement itself. The MOS transistor provides us a great example to illustrate that fact. The drain current noise $i_D(t)$ is measured as voltage fluctuation $v_o(t)$ at the output, and what one *observes* is actually the signal

$$v_o(t) = H\{i_D(t)\}, \tag{12}$$

where $H\{\cdot\}$ denotes the linear filtering action. The *Wiener-Khinchin theorem* relates the output noise PSD to the input one:

$$S_{v_o}(f) = |H(f)|^2 S_{i_D}(f), \tag{13}$$

$H(f)$ being the (deterministic) *transfer function* from $i_D(t)$ to $v_o(t)$. Due to the presence of small capacitances, there is always a *low-pass* filtering effect which limits the *actual* noise bandwidth and ensures a *finite* noise power. As an example, let us consider the first-order filter

$$H(f) = \frac{H_0}{1 + jf/f_0}, \tag{14}$$

[3] N_{traces} is the same as *nruns* below.

and let us compute the output noise power as

$$\begin{aligned}\sigma^2_{v_o} &= \int_0^{+\infty} S_{v_o}(f)\,\mathrm{d}f \\ &= \int_0^{+\infty} |H(f)|^2 S_{i_D}(f)\,\mathrm{d}f \\ &= H_0 \cdot 4kT\left(\frac{2g_m}{3}\right)\cdot f_0 \cdot \int_0^{+\infty} \frac{\mathrm{d}f/f_0}{1+(f/f_0)^2} \\ &= H_0 \cdot 4kT\left(\frac{2g_m}{3}\right)\cdot f_0 \cdot \frac{\pi}{2}.\end{aligned} \tag{15}$$

We have assumed that the drain current noise consists only in thermal noise of (4), for the sake of illustration. It is clear that the noise power computed in (15) is now finite.

Although it was shown based on an example, the following statement is general: even if intrinsic noise sources are of an infinite bandwidth, these are *never* probed intrinsically, and the power of the noise measured at the output (v_o) or at the supply (i_{DD}) is finite because of low-pass filtering effects. From the simulation point of view, it therefore appears useless to generate noise with excessively high-frequency content, as high-frequency components are *not* observed and hence, are not expected to influence much the extracted circuit FoMs such as the SNR, or the MI. In all, it appears very sound to limit the noise to some frequency FMAX, so that the corresponding supply noise power is computed as

$$\sigma^2_{i_{DD}} \propto \int_0^{\mathrm{FMAX}} S_{i_{DD}}(f)\,\mathrm{d}f. \tag{16}$$

Regarding the flicker noise, a similar discussion should be made regarding the lower integration bound of (16): irrespective of the FMAX,

$$\begin{aligned}\sigma^2_{i_{DD,\mathrm{flicker}}} &\propto \int_0^{\mathrm{FMAX}} \frac{K_f}{f}(f)\,\mathrm{d}f \\ &\propto K_f \log\left(\frac{\mathrm{FMAX}}{0}\right) = \infty?\end{aligned}$$

diverges, which leads to the introduction of a frequency *FMIN_FLICKER* below which the flicker noise is whitened. The existence of such a cut-off frequency arises from the finite duration T of the simulation (or measurement). As the noise is a zero-mean quantity, the first spectral component that one can actually estimate is the frequency

$$\mathrm{FMIN\_FLICKER} = \frac{1}{T}. \tag{17}$$

Processes involving fluctuations slower than $\sim 1\text{–}10 \cdot T$ are treated as *static* or *time-zero variability* in this frame.

3.3.2. Selecting the proper FMAX

Circuits used for cryptographic application quickly become more complex than one single transistor operating in DC condition. However, the previous discussion can be extended as follows. Let

$$\left\{i_D^{(m)}\right\}_{m=1,2,\ldots N_{\mathrm{sources}}}$$

denote the intrinsic noise sources of all the different transistors making the circuit, and let

$$\left\{H^{(m)}(f,t)\right\}_{m=1,2,\ldots N_{\mathrm{sources}}} \tag{18}$$

be the associated time-dependent transfer functions to the supply rail. The time dependence comes from the fact that a digital gate operates in *large-signal conditions*, the bias point is continuously changing, and the noise is a non-stationary stochastic process with a time-dependent PSD:

$$S_{i_{DD}}(f,t).$$

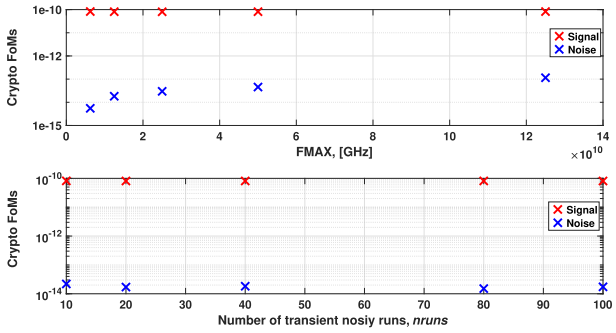

Fig. 1. Impact of f_{max} parameter (top) and the *nruns* (below) parameter on the "Cryptographic" FoMs *Signal* and *Noise* for an XOR gate at $V_{DD} = 0.9$ V.

Invoking again the Wiener-Khinchin theorem and using the superposition principle, we compute

$$S_{i_{DD}}(f,t) = \sum_{m=1}^{N_{\mathrm{sources}}} |H^{(m)}(f)|^2 S_{i_D^{(m)}}(f,t). \tag{19}$$

Thus, due the transistor intrinsic capacitances, (19) tells us that the supply noise is the sum of several low-pass filtered white and flicker noise contributions, and that i_{DD} is finite bandwidth limited and has a finite instantaneous power.

As it looks very difficult or at least very tedious and hence impractical to the authors to estimate all the transfer functions (18), for a large set of relevant bias points and every time for each circuit architecture, the following empirical methodology was adopted to select FMAX. The circuit FoM of interest, such as the SNR, was extracted for a reduced number of FMAX values, typically between a few GHz up to the THz. We expected that the noise power *saturates* with a larger FMAX, and thereby the SNR *flattens out*. Such a behavior, predicted by (19) and the related discussion, is confirmed in Fig. 1(top) and 2(top) for a XOR gate. The SNR of reference is unambiguously

$$SNR^* = \lim_{\mathrm{FMAX}\to\infty} SNR(\mathrm{FMAX}), \tag{20}$$

while the actually computed *SNR*, for a given finite FMAX is always slightly overestimated.[4] However, we can assume that the FMAX is large enough once saturation is reached, i.e. for instance

$$\frac{|SNR^* - SNR(\mathrm{FMAX})|}{SNR^*} < \varepsilon \sim 10 - 20\%. \tag{21}$$

For the purposes of our simulations, we choose an ε tolerance value of $\lessapprox$ 15%. We observe in Fig. 1(bottom) that even with an increasing number of runs, the values of "crypto" signal and noise calculated remain well within our tolerance levels. This justifies the usage of lower number of transient noisy runs to minimize the simulation run-time.

The tradeoff is usually very tough, as the CPU time increases drastically with FMAX, as illustrated in Fig. 2(bottom). For this case study, a FMAX of a few hundreds of GHz yields a satisfying estimation of the SNR while keeping the simulation budget reasonable as the total simulation duration remains below one hour. These considerations are of highest concerns for circuits with rising complexity and number of transistors (such as the Sboxes), as the simulations become more and more computationally intensive.[5]

[4] which is especially not a major concern for cryptographic design, as a higher *SNR* constitutes the worst case for the circuit.

[5] In Appendix A.2, after selecting the NOISETRAN parameters as discussed above, we validate that simulated current traces really contain meaningful physical intrinsic noise. For that sake, we briefly examine the first-order statistics of the noise present in the supply current for one of the above mentioned circuits of interest, i.e. the XOR gate.

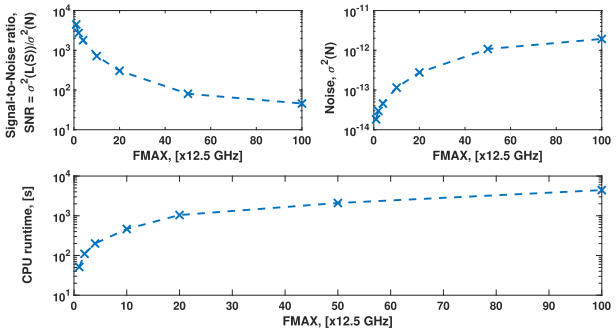

Fig. 2. Impact of FMAX parameter on the "Cryptographic" *SNR*, *Noise* and *CPU runtime* for an XOR gate at $V_{DD} = 0.9$ V.

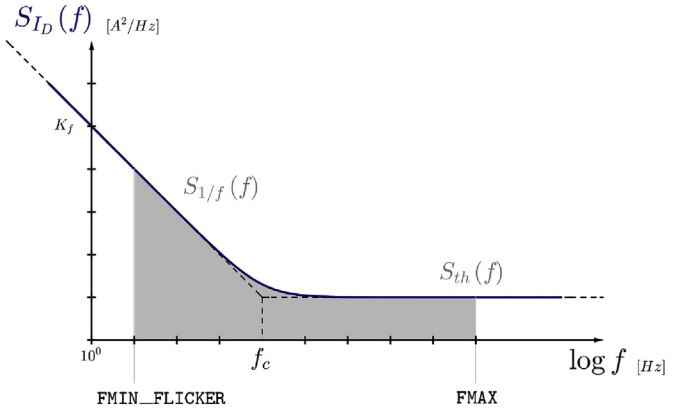

Fig. 3. Computation of Noise power using Power Spectral Density.

3.4. Impact of the low-frequency noise factor

We assume a canonical and general expression for the flicker noise (though actual models in ELDO are more complex),[6]

$$S_{i_{D,flicker}}(f) = \frac{K_f}{f}. \tag{22}$$

From (22), the interpretation of K_f is quite obvious:

$$K_f = S_{i_{D,flicker}}(1Hz). \tag{23}$$

That parameter is also indicated in Fig. 3.

For our study of the impact of the transistor intrinsic noise on the SNR and MI, we have tuned, i.e. increased, the noise by increasing the value of such a K_f for our simulations. Such an approach could firstly sound very artificial, but it is supported by Low-Frequency Noise (LFN) measurements from the literature, shown in Figure *7* in Ref. [17] for the same technology. Among the samples, many transistors exhibit K_f values more than one decade larger that the one we have artificially introduced. An interesting conclusion that arises from this discussion is the actual possibility to obtain dies within which a large number of transistors achieve a large K_f, as desired to make noisy cryptographic circuit design.

3.5. AC analysis

We now present results of *AC analysis* for a given fixed bias, V_{DD}. We show how the flicker noise is increased by tweaking the model parameters whereas the thermal noise power remains constant. This allows us to investigate the impact of the K_f on the crypto FoMs as discussed below. From Fig. 3, we can compute the total noise power (in this case, the noise variance), by integrating the power spectral density over the desired bandwidth,

$$\sigma^2 = \int_{FMIN_{FLICKER}}^{FMAX} S_{i_{DD}}(f)df \tag{24}$$

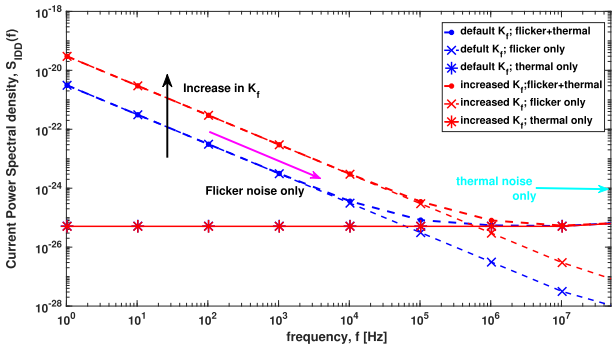

Fig. 4. AC analysis of increased K_f at $V_{DD} = 0.5$ V for 8-bit AES Sbox.

Fig. 4 plots the power spectral density of the current (noise current power spectral density) for a given (constant) bias for an 8-bit AES Sbox. The inputs are set to a constant bias (V_{DD} in this case)[7] and the frequency is swept from 1 Hz to the frequency-of-interest. The lines represent the $S_{i_{DD}}$, for the intrinsic K_f, i.e the default value. However, by increasing the K_f, we obtain the noise curve which clearly shows an increased level of noise due to K_f increase.

By using (24), we can compute the total noise variance and show that the results obtained are in close agreement with the values obtained from a transient noise analysis and a MI analysis, as discussed in details in the next section.

4. Results of the transient noise analysis

In this section, we discuss the results of transient-noise simulation methodology over the implemented designs. That is, for a 2-input XOR, a 4-bit Sbox of the PRESENT encryption and an 8-bit AES encryption Sbox. These include a total of 12, 684 and 1884 transistors, respectively.

4.1. Evaluating crypto FoMs-Signal, noise and SNR from transient noise analysis

After collecting traces from our repeated transient noise runs, we are able to calculate the maximum signal and the maximum noise, (from (1)). Figs. 5 and 6 show the scaling of the maximum signal and noise for a range of V_{DD}, i.e, from 0.5 V to 1 V. We can make the following observations from the 2 plots.

1 By increasing the supply voltage, V_{DD}, the value of the maximum signal and noise increase. This can be explained by the fact that as the V_{DD} increases, the dynamic power consumption, P_{dyn} increases (hence the increase in on current, I_{ON}) which increases the *Signal* value. This is true for the static power leakage as well. The increase in the "crypto" *noise* can be explained by the increase in the thermal noise which increases with the increase of I_{ON}. Reciprocally, signal and noise decrease with V_{DD}. We can observe that the signal decrease is faster than the noise decrease which is of interest for our

[6] we note here the difference in the flicker noise factor with (6); Here and unless specified, the $C_{ox}^2 WL$ term is included in the K_f term.

[7] hence the considered current is the static leakage, whose statistics are studied in appendix.

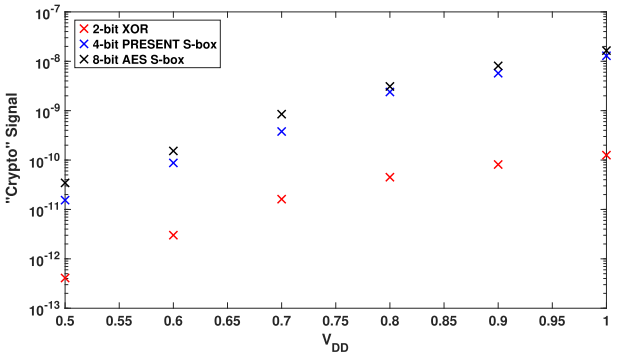

Fig. 5. Scaling of "Cryptographic" *Signal* as a function of V_{DD} for different circuits.

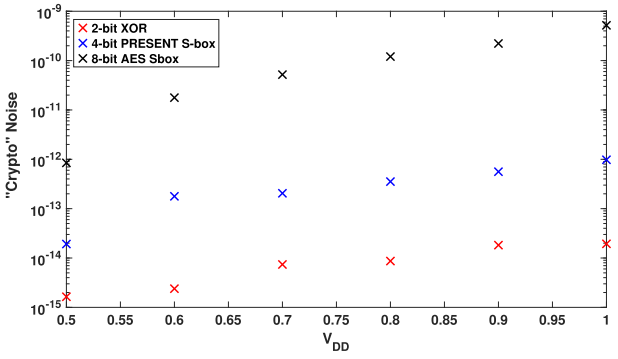

Fig. 6. Scaling of "Cryptographic" *Noise* as a function of the number of transistors, N_T for different V_{DD}.

purpose. A possible reason could be due to the square dependence of the Signal on the supply voltage, V_{DD} whereas the noise behaves in a more linear way with respect to the V_{DD}.

2 For a particular V_{DD}, the signal (and the noise) increase with the increase in design complexity, i.e as the number of transistors increases for a given circuit (*e.g.* moving from a 2-bit XOR to a 4-bit PRESENT Sbox to an 8-bit AES Sbox).

The increase in the signal can be modeled by the following relation

$$\overline{S}_{V_{DD}}^{circuit} = S_{V_{DD}}^{XOR} N_T^{\beta} \tag{25}$$

where $\overline{S}_{V_{DD}}^{circuit}$ is the signal for the target circuit, $S_{V_{DD}}^{XOR}$ is the signal produced by a 2-bit XOR for the same supply voltage, V_{DD}, N_T is the ratio of the increase in the number of transistors w.r.t a 2-bit XOR and β is a technology factor which varies $0.4 < \beta < 1.5$ for our circuits and depends on the value of the supply voltage, V_{DD}.

The increase in the noise can be modeled as

$$\overline{N}_{V_{DD}}^{circuit} = N_{V_{DD}}^{XOR} N_T^{\alpha} \tag{26}$$

where $\overline{N}_{V_{DD}}^{circuit}$ is the noise for the target circuit, $N_{V_{DD}}^{XOR}$ is the noise calculated for a 2-bit XOR at the same V_{DD}, N_T is the ratio of the number of transistors w.r.t a 2-bit XOR and α is a parameter which scales with the supply voltage, is $\lessapprox 2$ for our circuits and depends on the value of the supply voltage, V_{DD}. Consequently, we observe that noise increases faster with the number of transistors than the signal. This could be related to the fact that the intrinsic MOSFET noise sources are not correlated and hence the total contribution to i_{DD} is larger, whereas the signal is more proportional to the number of circuit branches connected to V_{DD}.

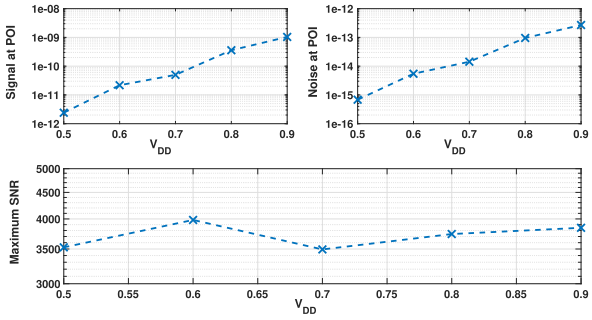

Fig. 7. Scaling of "Cryptographic" *Signal*, *Noise* and *SNR* at *Point-of-Interest (POI)* as a function of V_{DD} for AES Sbox.

Since the calculated "cryptographic" noise is essentially a mean of the variance across different inputs for *nruns* number of traces, we should be able to relate this noise to the histogram of the measured current. We see this in the next section. From Figs. 5 and 6, we see the evolution of the maximum signal and maximum noise (which conclude in the computed SNR (1)); however, in typical *side-channel attacks*, the adversary, chooses a *Point-of-Interest* (POI) in time and exploits this point to extract the relevant information. For our following results, we choose the maximum SNR time point as our POI. This is intuitive, as the maximum information leakage occurs at this point. Hence analyzing the crypto metrics at this point and plotting the relevant figures-of-merit, such as the SNR or MI, provides us with useful information about the extent of information leakage.[8]

In Fig. 7, we plot the "cryptographic" calculated *Signal*, "cryptographic" *Noise* and the "crypto" *Signal-to-Noise* (SNR) ratio at the *Point-of-Interest (POI)*[9] for different supply voltages, *i.e.,* from 0.5 V to 0.9 V. The results obtained are consistent with ones obtained above, *i.e.,* the Signal and Noise metrics increase with the increase of the V_{DD}; however, the SNR only slightly vary. This is of importance as it leads to a conclusion that there is no "perceived" change/gain in the "security" level by varying the supply voltage, V_{DD}. However, as pointed out in previous works [8] the SNR is a first-order metric and is often used by designers only in very early design stages to obtain a very first-hand estimation of the security level. However, for further understanding of the impact of the noise variance and its impact w.r.t the supply voltage, we refer to the Mutual Information Analysis, introduced in sub–section 2.2.

4.2. Evaluation using mutual information -an analysis

In this subsection, we revisit our previous results and explore them using the Mutual Information analysis introduced in sub-section 2.2 for the largest design under investigation, the AES Sbox. As previously explained, the MI metric allows the designer to *quantitatively* estimate the *information leakage* from an implementation and estimate the noise variance needed to achieve a given security level. Concretely, it lets us derive a more general intuition and the effect of parameters such as the noise variance and the supply voltage on the information leakage and how the above parameters vary the MI. Note that the SNR curve is shown for a given number of *nruns*, that is, the SNR as is shown in Fig. 7, does not take into account the noise averaging. In turn, increasing *nruns*[10] reduces the noise and increases the attack success rate. The

[8] We also use this POI for Mutual Information analysis, as explained.

[9] we note here the difference between Figs. 5–7 the former ones plot the *Maximum* Signal and Noise whereas the latter plots the Signal and Noise at the POI.

[10] i.e, averaging over a *very* large number of noisy traces, typically a *million*, in practical side-channel attack scenarios.

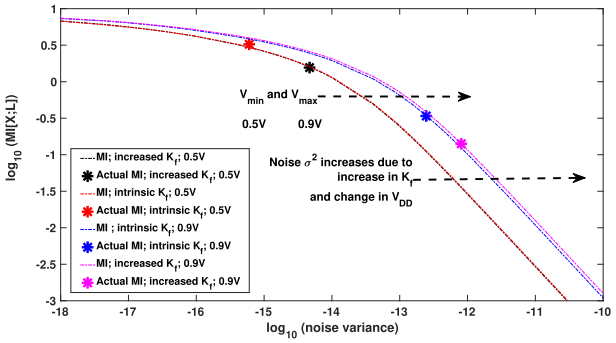

Fig. 8. Effect of the increase in the K_f factor for a CMOS AES Sbox at $V_{DD} = 0.5$ V and 0.9 V. The individual markers * correspond to the actual calculated noise variance from the simulator.

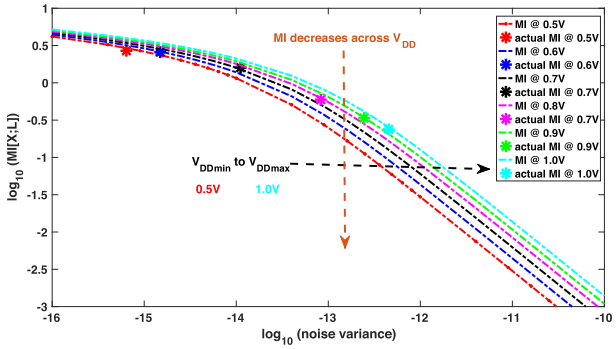

Fig. 9. Impact of the Supply Voltage, V_{DD} on the MI for a CMOS AES Sbox. Devices here have been simulated at the default K_f provided by the model. Individual markers * correspond to the actual calculated noise variance from the simulator.

MI metric, however, does take *nruns* into due consideration. The MI curves enable an asymptotically security evaluation, i.e. it provides a security trend as a function of the noise or the noise-removal/averaging abilities of the adversary. It also provides the designer an upper bound of the noise adding capability to reduce the leakage to achieve a desired security level. The * markers in Fig. 9, represent the inherent device physical noise that an adversary cannot further remove (as compared to external/environmental/algorithmic noise [18]).

4.2.1. *Increasing the K_f factor-revisting using MI*

In this subsection, we revisit our discussion on the K_f factor in the *context of Mutual Information*. Using *transient noise simulations*, we observe from Fig. 8, the results of the increase of the ficker noise *on the MI* for a CMOS AES Sbox (same setup as above), for a supply voltage $V_{DD} = 0.5$ V and 0.9 V. To understand the curve, we must first be clear about the legend of the figure. The dashed line indicates the MI due to the *intrinsic* K_f, i.e., K_f which has not been modified and is the default as provided by the foundry model. The black dashed curve indicates the MI due to the *increased* K_f, i.e K_f which has been modified by changing the parameters of the foundry model. We make the following observations.

- A decrease in the magnitude of the MI is observed (illustrated using the colored * markers), thanks to the increased K_f. As the K_f increases, so does the noise variance and the MI goes down. This is observed for both the supply voltages plotted, i.e 0.5 V and 0.9 V
- We also observe that the noise variance value is higher for the higher supply voltage, i.e 0.9 V compared to 0.5 V. This is an expected trend and validates our results obtained from the Signal and Noise curves above.
- The MI curves nicely validate the results obtained using the SNR metric above and allows the designer to estimate the noise required to be added to achieve a required security level.

4.2.2. *Effect of supply voltage on the mutual information*

In this section, we revisit the results from Fig. 7 in the context of Mutual Information and provide a more detailed analysis of the impact of the supply voltage on the amount of information leakage. From Fig. 9 we make the following observations.

- Reducing the voltage leads to a signal reduction which in turn reduces the MI (for a given noise level). This is clearly illustrated and is an expected trend. This is an interesting result as it makes it clear that lowering the supply voltage does not always necessarily lead to (*more*) leakier implementations, if intrinsic physical noise is taken into account.
- The noise variance increases with the supply voltage. This is consistent with the results obtained using the SNR metric in the previous section which are expected. This allows the designer to estimate the noise required to be added for a given supply voltage to achieve a desired security level.
- Using the actual computed MI values and noise (represented by * in Fig. 9) the corresponding noise variances obtained are in close agreement with the noise variances obtained from transient noise simulations (SNR) and AC analyses, as described in the previous section.

5. Conclusion and open questions

In this manuscript, through a series of case studies, we have for the first time and to the best of our knowledge, proposed a methodology to concretely simulate *intrinsic* MOSFET physical noise and to link the results to concrete security evaluation metrics of cryptographic modules using transient noise simulations. The results of this research are valuable to discuss and answer questions such as, how the physical noise sources from the MOSFETs can be used for effectively deriving the cryptographic SNR or MI values, and especially to concretely perform security evaluation at design stages of a cryptographic implementation. Not limited to security evaluations, the paper would also serve as a design guideline for early stage cryptographic (and digital) designers to incorporate security from the beginning of a product development cycle. Such guidelines include (but not limited to) the design using lower sized transistors (keeping in mind the performance required and respecting the noise margins at the given voltage of operation), architectural level designs such as to maximize the impact of physical noise (by introducing hierarchy in the levels of implementation, using a mix of say, serial and parallel implementations) and using lower voltage (modes of) operation (as has been shown) to reduce the impact of the leaking signal). This allows designers to trade-off between security and other metrics like area, power consumption, etc. keeping in mind the (intrinsic) vulnerability of such devices to Differential Power Analysis (DPA) [1].We believe that our introduced methodology not only provides designers a formal assessment of the security level of a given (leaking) device from the conceptual stage (without added countermeasures) but also quantitatively estimates the amount of noise (increased by addition of externally added countermeasures or by tweaks in the design) to mitigate the ease of a DPA. This leads to computation of metrics such as the correlation coefficient, MTD (the number of traces to disclosure) or the information-theoretically sound metric, mutual information (MI), to quantitatively estimate the security of a device at any

given stage of the design. Some of our concrete observations are that longer transient runs (higher FMAX), which add more noise, come at the expense of increased simulation run times (high CPU time) which does not track back to significant changes in our security metrics. The complexity would further increase with the number of gates in case of a full cryptographic implementation such as the AES or the PRESENT block cipher. We conclude that the use of intrinsic physical noise in MOSFETs to add more cryptographic noise is an effective method (since such noise sources are predicted to increase significantly with further technology scaling and voltage). At this stage we identify an important open question regarding an effective noise simulation and evaluation of correlated noise sources especially for larger circuits.

Acknowledgments

This work has been funded in parts by the UCLouvain ARC Project NANOSEC. Léopold Van Brandt is funded by a grant from FRIA, Belgium. Itamar Levi is funded by the H2020 ERC SWORD project number 25821. François-Xavier Standaert is a Senior Research Associate of the Belgian Fund for Scientific Research (FNRS-F.R.S.).

Appendix A. Statistical properties of the supply current noise of the XOR gate

In this section, we briefly examine the *first-order statistics* of the noise present in the supply current for one of the above mentioned circuits of interest, i.e., the XOR gate.

Fig. A.10 contains noise traces for the set of parameters $N_{traces} = 40$, T = 800ns and dt = 40ps for a total budget of $\sim 8 \times 10^5$ for a supply $V_{DD} = 0.5$ V. FMIN = 1/T and FMAX = (1/2)*dt are chosen as per the described methodology.

Appendix A.1. Statistical characterization of the static region

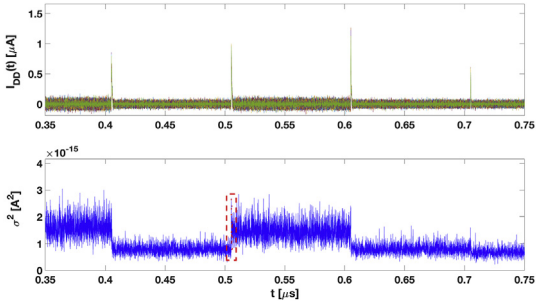

Fig. A.10 Zoom on the dynamic and static regions (top) and associated variance plot based on all the 40 traces (bottom). Noise in the static region is shown to follow a stationary Gaussian distribution.

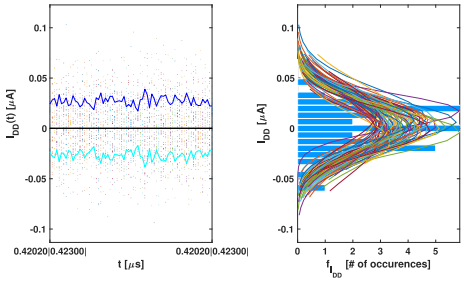

Fig. A.11 Histogram construction for time t = 0.4202 μs - 0.4230 μs within the static region of Fig. A.10 (top). Extracted Gaussian distribution is also shown (right).

The static region indicated in the current vs. time plots in Fig. A.10 (top) is useful to get insight on the noise behavior within the circuit and how it affects the supply current. Input voltages of the gate are fixed, and so are all the averages of the branch currents and node voltages within the circuit (since there are noise fluctuations). Hence, the supply current noise is treated as a *wide-sense stationary* stochastic process, for which a complete definition can be found in Ref. [19]. Especially, the probability density function (pdf) does not depend on t, that is:

$$f\left(i_{DD}\left(t\right)\right) = f\left(i_{DD}\right), \tag{A.1}$$

and the variance is also independent of t:

$$\sigma\left(t\right) = \sigma. \tag{A.2}$$

As a consequence, every sample $i_{DD}\left(t^*\right)$ at any time sample t^* of every trace is understood as a realization of one single random variable i_{DD}. Fig. A.11 demonstrates that noise in the static region follows a stationary Gaussian distribution.

Appendix A.2. Challenges regarding the dynamic region

In order to accurately capture the dynamic region behavior, we plot the time-varying histograms of the very *narrow* dynamic region enclosed by a red rectangle in Fig. A.10(bottom). The supply current noise now is a *nonstationary* stochastic process. Its distribution is explicitly time-dependent:

$$f\left(i_{DD}\left(t\right)\right) = f\left(i_{DD}, t\right), \tag{A.3}$$

as well as the variance $\sigma\left(t\right)$. Since each point in the dynamic region is non-stationary, we observe the *time-varying* histograms for each sample to extract the mean and the variance and show the *envelope* of the $\pm 1\sigma$ over the mean trace as shown in Fig. A.12.appsec1

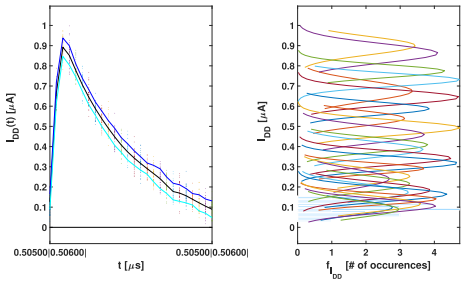

Fig. A.12 Histogram construction for time t = 0.505 μs - 0.506 μs within the dynamic region marked red in Fig. A.10(bottom). Extracted Gaussian distribution mixture is also shown(right).

Our main goal is to extract the variance from the histograms. This is achieved by performing a nonlinear fitting of the histogram. Using the extracted σ values from the distributions above and comparing them with the mathematical "cryptographic" noise values calculated by (1), we obtain a good matching between the data, thus validating the fact that the noise present in the mathematical calculations can indeed be traced back to the results of the transient noise analyses including the MOSFET noise sources.

Appendix B. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.vlsi.2019.06.006.

References

[1] P.C. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Advances in Cryptology - CRYPTO 99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings, 1999, pp. 388–397 [Online]. Available:, https://doi.org/10.1007/3-540-48405-1_25.

[2] K. Nawaz, D. Kamel, F.-X. Standaert, D. Flandre, Scaling trends for dual-rail logic styles against side-channel attacks: a case-study, in: Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, 2017, pp. 19–33. Revised Selected Papers.

[3] K. Nawaz, L.V. Brandt, F. Standaert, D. Flandre, Let's make it noisy: a simulation methodology for adding intrinsic physical noise to cryptographic designs, in: 14th Conference on Ph.D. Research in Microelectronics and Electronics, PRIME 2018, Prague, Czech Republic, July 2-5, 2018, 2018, pp. 61–64 [Online]. Available:, https://doi.org/10.1109/PRIME.2018.8430315.

[4] S. Mangard, Hardware countermeasures against DPA ? A statistical analysis of their effectiveness, in: Topics in Cryptology - CT-RSA 2004, the Cryptographers' Track at the RSA Conference 2004, San Francisco, CA, USA, February 23-27, 2004, Proceedings, 2004, pp. 222–235 [Online]. Available:, https://doi.org/10.1007/978-3-540-24660-2_18.

[5] B. Gierlichs, L. Batina, P. Tuyls, Mutual Information Analysis a Universal Differential Side-Channel Attack, Cryptology ePrint Archive, Report 2007/198 2007https://eprint.iacr.org/2007/198.

[6] F. Standaert, T. Malkin, M. Yung, A unified framework for the analysis of side-channel key recovery attacks, in: Advances in Cryptology - EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings, 2009, pp. 443–461 [Online]. Available:, https://doi.org/10.1007/978-3-642-01001-9_26.

[7] A. Duc, S. Faust, F. Standaert, Making masking security proofs concrete or how to evaluate the security of any leaking device, IACR Cryptology ePrint Archive 2015 (2015) 119 [Online]. Available:, http://eprint.iacr.org/2015/119.

[8] S.M.D. Pozo, F. Standaert, Blind source separation from single measurements using singular spectrum analysis, in: Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings, 2015, pp. 42–59 [Online]. Available:, https://doi.org/10.1007/978-3-662-48324-4_3.

[9] Z.Y. Chang, W. Sansen, Low-noise Wide-Band Amplifiers in Bipolar and Cmos Technologies, 1990.

[10] J.B. Johnson, The Schottky effect in low frequency circuits, Phys. Rev. 26 (Jul 1925) 71–85 [Online]. Available:, https://link.aps.org/doi/10.1103/PhysRev.26.71.

[11] T. Kleinpenning, On 1f noise and random telegraph noise in very small electronic devices, Phys. B Condens. Matter 164 (3) (1990) 331–334 [Online]. Available:, http://www.sciencedirect.com/science/article/pii/092145269090820K.

[12] Y. Ye, C. Wang, Y. Cao, Simulation of random telegraph noise with 2-stage equivalent circuit, in: 2010 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Nov, 2010, pp. 709–713.

[13] T. Komawaki, M. Yabuuchi, R. Kishida, J. Furuta, T. Matsumoto, K. Kobayashi, Circuit-level simulation methodology for random telegraph noise by using verilog-ams, in: 2017 IEEE International Conference on IC Design and Technology (ICICDT), May 2017, pp. 1–4.

[14] Mentor Graphics Corporation, Eldo User's Manual, Release AMS 2008.2, 2008.

[15] T. Poiroux, O. Rozeau, S. Martinie, P. Scheer, S. Puget, M.A. Jaud, S.E. Ghouli, J.C. Barb, A. Juge, O. Faynot, Utsoi2: a complete physical compact model for utbb and independent double gate mosfets, in: 2013 IEEE International Electron Devices Meeting, Dec 2013, pp. 12.4.1–12.4.4.

[16] A. Demir, A. Sangiovanni-Vincentelli, Time-domain non-Monte Carlo noise simulation, in: Analysis and Simulation of Noise in Nonlinear Electronic Circuits and Systems, Springer, 1998, pp. 113–161.

[17] E.G. Ioannidis, S. Haendler, A. Bajolet, T. Pahron, N. Planes, F. Arnaud, R.A. Bianchi, M. Haond, D. Golanski, J. Rosa, C. Fenouillet-Beranger, P. Perreau, C.A. Dimitriadis, G. Ghibaudo, Low frequency noise variability in high-k/metal gate stack 28nm bulk and fd-soi cmos transistors, in: 2011 International Electron Devices Meeting, Dec 2011, pp. 18.6.1–18.6.4.

[18] S.M.D. Pozo, F. Standaert, Getting the most out of leakage detection - statistical tools and measurement setups hand in hand, in: Constructive Side-Channel Analysis and Secure Design - 8th International Workshop, COSADE 2017, Paris, France, April 13-14, 2017, 2017, pp. 264–281 Revised Selected Papers. [Online]. Available:, https://doi.org/10.1007/978-3-319-64647-3_16.

[19] A. Papoulis, Probability, Random Variables, and Stochastic Processes, Ser, McGraw-Hill Series in Electrical Engineering. McGraw-Hill, 1991.