# A Transient Noise Analysis of Secured Dual-rail based Logic Style

Kashif Nawaz, Itamar Levi, François-Xavier Standaert and Denis Flandre
ICTEAM institute, Université catholique de Louvain, Belgium

***Abstract*—Dual-rail logic circuits have been used as an effective countermeasure towards a more secure circuit design. However, with technology scaling and lowering of $V_{DD}$, they lose interest as the signal reduction is less significant compared to CMOS. In this work, we revisit dual-rail logic designs (more specifically DDSLL) while focusing on intrinsic physical device noise using a transient noise analysis methodology and show that there exists a potential for such circuits to reduce the signal and concretely increase the noise. Our analysis, which extends to meaningful cryptographic figures-of-merit (FoMs) such as the SNR (Signal-to-Noise ratio) and Mutual-Information (MI), better clarifies the potential of DDSLL circuits to leverage the noise.**

## I. Introduction

With the growing advent of Internet-of-Things (IoT), connected devices are becoming more ubiquitous. As such, they are more vulnerable to attacks, most notably side-channel attacks, which utilize the power/eletromagnetic radiation of a device and exploit it to retrieve secret information [1]. Countermeasures, not limited to algorithmic or mathematical, are often employed to reduce the side channel leakage information and hide the informative signal as much as possible. Circuit level countermeasures, such as supply voltage randomization [2] or shuffling [3] are often used to "hide" the signal. Although effective, such methods which typically utilize *external* randomness, makes them more susceptible to attacks than methods which harness *intrinsic* device-level noise. Logic and device level countermeasures such as dual-rail logic [4], which seek to equalize the power consumption at each clock cycle, have proven to be effective against such attacks by lowering the informative part of the signal to a considerable extent, and hence lowering the SNR. Lately in [5] it has been shown that technology-scaling has a detrimental effect on the signal reduction.

Thanks to the methodology introduced in [6], in this work we revisit the utilization of dual-rail logic in the presence of *intrinsic MOSFET physical noise*, coming from the transistors. Since, the intrinsic MOSFET noise depends on the number of transistors in the implementation, with larger number of transistors in dual-rail based logics, we expect a significant noise increase in dual-rail logic implementation. In addition, the operational mode of this logic, which consists of having two clock phases (a pre-charge and an evaluation phase), the distribution of the noise is intuitively expected to be larger than say, sampling with a single rising-edge clock signal in CMOS. We perform concrete physical security evaluation which takes transient noise into account while utilizing the *SNR* and the *MI* as a security based Figures-of-Merit (FoMs).

This paper is divided into 5 sections. We first review the background (in terms of logic style and crypto FoMs) in Section II, then in Section III we discuss our simulation settings to introduce noise sources. In Section IV we discuss the results of our methodology and finally wrap up in Section V with conclusions and perspectives.

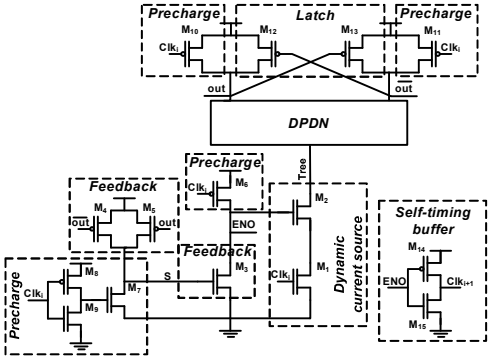


Figure 1: Schematic of a generic DDSLL gate.

## II. Background: DDSLL and Security Metrics

### A. DDSLL

In this subsection, we briefly review a simple Dynamic-differential switching level logic (DDSLL) gate, as shown in Figure 1 [5]. DDSLL is a dual rail differential switching logic style and has been shown to be effective in decreasing the Signal [7]. In the precharge phase, the logic gates are pulled to the supply voltage level, and during the evaluation phase, due to the switching of the current source transistor (M1 in Figure 1), a current path is created and the drain voltage of the device falls to $V_{DD}$ - $V_{th}$.

### B. Security Metrics

Analyzing leaking cryptographic implementations is a challenging task. In this paper we will focus on the univariate approach, where each time sample is assumed to be independent, using the SNR and the MI as security metrics for a quantitative understanding of the effects of noise on DDSLL based logic implementations. Let $\overrightarrow{L}$ denote a physical leakage (e.g. current trace) from a crypto implementation:

$$\overrightarrow{L} = \left( \sum_{j=0}^{N_{inputs}} f_j(\overrightarrow{X}_{\text{input}}, \sigma_{intrinsic}) \right) + \overrightarrow{N}_{\text{physical}}(\mu, \sigma^2) \quad (1)$$

$$\sigma^2_{intrinsic} = \sigma^2_{flicker} + \sigma^2_{thermal} \quad (2)$$

where $\sigma_{\text{intrinsic}}$ is the variance due to the *intrinsic* noise produced by the MOSFET devices, $f(\overrightarrow{X}_{\text{input}}, \sigma_{intrinsic})$ represents the cryptographic function being implemented on the $X_{input}$; and under the assumption of an additive Gaussian noise due to the measurement setup, $\overrightarrow{N}_{\text{physical}}(\mu, \sigma^2)$ . In this work, which involves a stand-alone simulation setup with no peripherial components nor measurement noise, we have $\overrightarrow{N}_{\text{physical}} = 0$ (which in practice serves as an adversary best-case).

We assume the underlying distribution of the noise to be Gaussian and *i.i.d* (independent and identically distributed) (as is often done in security analysis literature)[1].

For the SNR, we use Mangard's SNR defined in [8] as:

$$\text{SNR} = \frac{\hat{\mathsf{var}}_x(\hat{\mathsf{E}}_i(L_x^i))}{\hat{\mathsf{E}}_x(\hat{\mathsf{var}}_i(L_x^i))}, \tag{3}$$

where $\hat{\mathsf{E}}$ (resp. $\hat{\mathsf{var}}$) denotes the sample mean (resp. variance) operator and $L$ the leakage. The numerator corresponds to the crypto[2] *"Signal"* and the denominator, the crypto *"Noise"*(units of $\text{A}^2$) Using eqn (3), the signal is the "useful" part that is obtained by the adversary to extract the secret key/message. The lower the signal value, lower the *exploitable* side-channel leakage. The maximum signal, as a metric to quantify the leakage, in case of noiseless simulations [5], has been used by the authors to show the scaling trends of the signal with respect to technology scaling from 65nm bulk to 28nm FDSOI for standard CMOS and dual rail differential logic styles.

In the next section, the SNR has been computed over *noisy* traces of the current consumption as a function of time, denoted as $I_{DD}\,(t^*)$ and this includes the noise coming from physical *intrinsic* MOSFET noise sources. The point of maximum SNR is chosen as the point-of-interest (POI) at which, the *Signal* and *Noise* are computed.

$$SNR : \{SNR_1, SNR_2, ...SNR_i\} \tag{4}$$

$$t^* = t|_{SNR=max(SNR)} \tag{5}$$

We also compute the Mutual-Information (MI) metric, first introduced in [9]. For our work, where we consider the leakage function to be Gaussian distributed, the SNR and MI metrics are equivalent [10]. We use the MI as a better metric to visualize the security level as a function of the (*intrinsic*) noise variance.

$$\widehat{\text{MI}}(\text{X};\text{L}) = \text{H}[\text{X}] - \sum_{\text{x}\in\text{X}} \Pr[x] \sum_{\text{l}\in\text{L}} \Pr_{\text{simu}}[l|x].\log_2 \Pr_{\text{simu}}[x|l] \tag{6}$$

where, $H$ denotes the entropy, $\Pr[\text{x}]$ denotes the probability of the input variable x, $\Pr[\text{l}|\text{x}]$ is the conditional probability of the leaked variable for a given input, and $\Pr[\text{x}|\text{l}]$ the conditional probability of the input given the leakage.

[1]We acknowledge, however, that this assumption is generally violated in real world situations where the leakage distributions are unknown and stronger correlations exist between the noise variables themselves

[2]We use the term cryptographic and crypto interchangeably, they both denote the one and same thing

## III. Transient Noise Analysis: A simulation methodology

### A. Target Designs

The target designs for this case-study are CMOS and DDSLL 8-bit AES S-boxes. The underling DDSLL gates were implemented (with Cadence Virtuoso) utilizing minimum sized transistors from the 28nm FDSOI PDK (process desgin kit). The sizing of the transistors has been kept minimum to maximize the noise (especially the flicker noise). Using the methodology introduced in [6], we simulate *flicker* and *thermal* noise from the transient noise analysis by Eldo simulator (from Mentor Graphics). The currents drawn from the modules-under-test are recorded from the simulator (over multiple supply voltages), i.e $(I(V_{DD}(t)))$, and the security metrics computed as described in the previous subsection.

### B. Simulation settings

The designs are simulated using the Eldo simulator with intra-cell layout characteristics only. The *Transient-Noise* analysis built in Eldo (called by the *.noisetran* command) has been repeated upto $\text{N}_{runs}$[3] transient noise simulations. The noise sources correspond to the physical flicker and thermal noises intrinsic to the MOS transistors were generated by Eldo within the frequency bandwidth specified by the input parameters of the transient noise analysis (eqn 2).

The chosen minimal flicker noise value, $\text{f}_{\text{min}}$ = 1/T, where T represents the total simulation time for all possible inputs. The input data signals to the circuits are a recurring 0 to an arbitrary input of 256 transitions at a clock frequency of 10 MHz and $\text{f}_{\text{max}}$ = 1/(2**dt*), where $\text{f}_{\text{max}}$ represents the maximum frequency of the noise generating sources, *dt* is the minimum time step being used by the simulator or specified by the user and as such that increasing it did not increase the signal variance. This was done to reduce expensive simulation time (as explored in [6]). All simulations are done at 298°K, *TT* corner and for a $\text{V}_{\text{DD}}$ range from 0.5V to 0.9V

## IV. Transient Noise Analysis: Results

In this section, we analyze the results of our transient noise analysis using the security metrics described in section II. The examined first order univariate metrics provide a first hand early stage security level of a cryptographic implementation. In this work, we do not specify a target SNR or MI value; rather, our goal is to exploit the methodology introduced in [6] for dynamic dual-rail logic level implementations and show that the amount of noise needed to be added to reach a given security level is smaller when fully (and correctly) analyzing the intrinsic noise.

### A. CMOS vs DDSLL- Analysis using the SNR

1 We first analyze the impact of the *Signal* metric as shown in Figure 2a. We make the following observations from this,
the Signal increases with the increase in the supply voltage, $\text{V}_{\text{DD}}$, for both CMOS and DDSLL circuits.

[3]$\text{N}_{runs}$ was chosen as such that the computed variance has converged

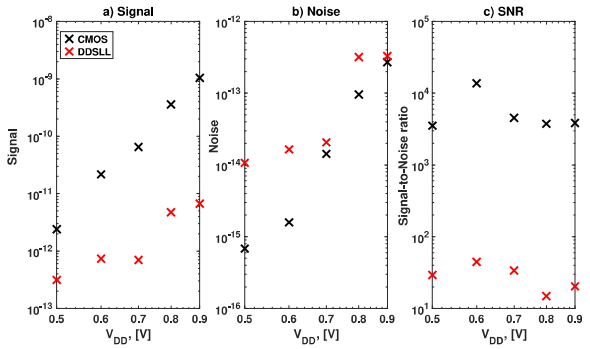


Figure 2: Impact of the $V_{DD}$ on "Cryptographic" *Signal*, *Noise* and *SNR* for CMOS & DDSLL Sboxes across $V_{DD}$=0.5V to $V_{DD}$=0.9V

This is expected as the device *on* current increases with the voltage. In addition, CMOS leaks higher signal as compared to DDSLL.

2 Figure 2b shows the "cryptographic" noise as a function of the supply voltage for the two designes. We observe the following,

- At a given voltage, $V_{DD}$, DDSLL has a higher noise impact than CMOS. This is an interesting result and is attributed to the larger number of transistors which make up the DDSLL circuit (as shown in [6] for non-dual-rail devices, the noise increases with the increase in the number of transistors).
- Second, and more importantly, we see that the noise contribution of DDSLL (as compared to CMOS), is higher at lower supply voltages, e.g. 0.5V-0.6V than at higher voltages say, 0.8V-0.9V.

3 From Figure 2c, we see the expected trend of the *estimated* SNR; due to its lower signal value and higher noise compared to CMOS, the DDSLL has much smaller SNR values for all supply voltages.

To conclude, whereas in [5], only the signal part of DDSLL as a function of the supply voltage was evaluated, here we complement this results by the positive affect of the noise as a function of the supply voltage (and as compared to CMOS). This in turn, translates to an SNR reduction of 2x orders-of-magnitude across a 400mV voltage span.

### B. Analysis of noise variance

In this subsection, we visually analyze the *intrinsic*-noise variance. We show that DDSLL presents a stronger noise independence with respect to the inputs as compared to CMOS. Without the loss of generality (and as was observed across supply voltages) for this discussion, we use a supply voltage of $V_{DD}$ = 0.5V. We plot the noise variance computed over $N_{runs}$ transient noisy runs, for all possible inputs. The variances are plotted as bar plot as a function of the S-box inputs, and as a scatter plot vs. the simulation time side-by-side (the scatter plot is used to better illustrate the distribution) for CMOS (Figure 3)

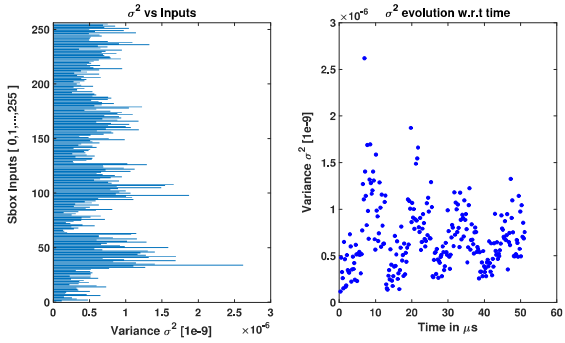


Figure 3: *Noise Variance* as a function of the *Inputs* for a CMOS Sbox at $V_{DD}$=0.5V

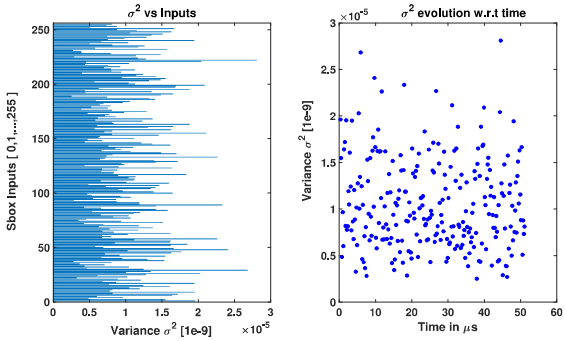


Figure 4: *Noise Variance* as a function of the *Inputs* for a DDSLL Sbox at$V_{DD}$=0.5V

and for DDSLL (Figure 4) respectively. We make the following observations,

- For CMOS, the noise variance is clearly data (input) dependent. In addition, the distribution that is observed contains multiple repeated patterns.
- For DDSLL (Figure 4), it is observed that there exists a much uniformly distributed noise variance. e.g. as in contrast to CMOS, the noise is more independent.
- More importantly, we observe that DDSLL has a higher quantitive noise-variance as compared to CMOS by almost an order of magnitude. This reinforces the notion that the noise calculated from equation 3 provides a good estimate for calculating the SNR from transient noise simulations. We explore this in further detail in the next section.

It is important to note that an attractive property of the DDSLL design is the increased independence of the noise from the inputs. In fact, it is a common criteria for masked hardware and software applications.

### C. Mutual Information Analysis

The MI for CMOS and DDSLL implementations for supply voltages (0.5V & 0.8V) is plotted as a function of the simulated noise variance. The actual noise variances calculated from the transient noisy simulations are shown using markers on the curves. We make the following observations from Figure 5:

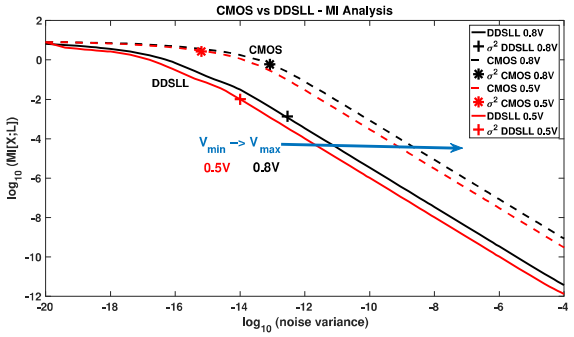


Figure 5: Mutual Information as a function of the *intrinsic* Noise Variance of CMOS and DDSLL circuits for 0.5V and 0.8V. The individual points correspond to the actual calculated noise variance from the simulator.

- For CMOS circuits, the amount of information leakage (MI) is higher than for the corresponding DDSLL leakage for all noise variances across all supply voltages. This confirms our intuition, that although DDSLL loses its advantage w.r.t technology scaling, [5], it continues to be a design-of-choice when physical *intrinsic* noise is taken into account. This advantage is especially attractive at lower voltages.
- Generally, CMOS leaks more information for a given noise level than a DDSLL implementation. Futhermore, a DDSLL implementation inherently has more noise, which contributes to its security.
- It is possible to see that the difference of the MI value of DDSLL between 0.8V to 0.5V is smaller than the same for the CMOS designs, which reassures the conclusions from the previous subsection.

A nice property of the MI curves is that it enables a designer to estimate the amount of noise required to be added to a design (to make it more secured). In our case, for a reasonable and similar security level (below $10^{-1}$), CMOS design will have to incorporate two order-of-magnitude more noise than DDSLL designs.

## V. Conclusion and Open Questions

In this case study, we have for the first time and to the best of our knowledge, provided a comparison between CMOS and DDSLL logic based styles using transient noise analysis while providing results from several concrete first-order univariate security metrics. Our evaluations show that a noisy DDSLL logic style exhibits a lower SNR (and hence a lower MI) trend at different supply voltages compared to a noisy CMOS implementation, mainly due to the considerable increase in *intrinsic* physical noise between the two technologies. We also show that the noise variances exhibit a strong independence w.r.t the inputs for a dual-rail logic implementation compared to a CMOS design. While our results are for an 8-bit AES S-box, we believe similar trends will be observed for a full AES implementation. The results can also be used to discuss the effectiveness of using the *intrinsic* physical noise of the MOSFETs and its behavior across different cryptographic implementations and different supply voltages. The extension of this work to larger circuits (especially for dual rail styles) and correlated noise sources at the cost of a larger area overhead while maintaining a higher security level compared to CMOS remains an open and interesting question.

**Acknowledgments.** This work has been funded in parts by the UCLouvain ARC Project NANOSEC. 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 (F.R.S.-FNRS)

## References

[1] P. C. Kocher, J. Jaffe, and 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: http://dx.doi.org/10.1007/3-540-48405-1_25

[2] D. Kamel, G. de Streel, S. M. D. Pozo, K. Nawaz, F. Standaert, D. Flandre, and D. Bol, "Towards securing low-power digital circuits with ultra-low-voltage towards securing low-power digital circuits with ultra-low-voltage vdd randomizers," in *Security, Privacy, and Applied Cryptography Engineering - 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings*, 2016, pp. 233–248.

[3] S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks - revealing the secrets of smart cards*. Springer, 2007.

[4] L. Giancane, P. Marietti, M. Olivieri, G. Scotti, and A. Trifiletti, "A new dynamic differential logic style as a countermeasure to power analysis attacks," in *15th IEEE International Conference on Electronics, Circuits and Systems, ICECS 2008, St. Julien's, Malta, August 31 2008-September 3, 2008*, 2008, pp. 364–367.

[5] K. Nawaz, D. Kamel, F.-X. Standaert, and 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, Revised Selected Papers*, 2017, pp. 19–33.

[6] K. Nawaz, L. V. Brandt, F. Standaert, and 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

[7] M. Renauld, D. Kamel, F. Standaert, and D. Flandre, "Information theoretic and security analysis of a 65-nanometer DDSLL AES s-box," in *Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings*, ser. Lecture Notes in Computer Science, B. Preneel and T. Takagi, Eds., vol. 6917. Springer, 2011, pp. 223–239. [Online]. Available: https://doi.org/10.1007/978-3-642-23951-9_15

[8] 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: http://dx.doi.org/10.1007/978-3-540-24660-2_18

[9] F. Standaert, T. Malkin, and 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*, ser. Lecture Notes in Computer Science, A. Joux, Ed., vol. 5479. Springer, 2009, pp. 443–461. [Online]. Available: https://doi.org/10.1007/978-3-642-01001-9_26

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