Scaling Trends for Dual-Rail Logic Styles Against Side-Channel Attacks: A Case-Study

Kashif Nawaz(✉), Dinal Kamel, François-Xavier Standaert, and Denis Flandre

ICTEAM/ELEN/Crypto Group, Université catholique de Louvain,
Louvain-la-Neuve, Belgium
kashif.nawaz@uclouvain.be

Abstract. Dual-rail logic styles have been considered as possible alternatives to CMOS for the design of cryptographic circuits (more) secure against side-channel attacks. The state-of-the-art view on this approach is contrasted as they reduce the exploitable side-channel signal while not being sufficient to fully prevent the attacks. Since the limitations of dual-rail logic styles are essentially due to implementation challenges (e.g. the need of well-balanced capacitances), a natural question is to find out how they evolve with technology scaling. In this paper, we discuss this issue based on the relevant case study of an AES S-box implemented in CMOS and a dual-rail logic style, for two (65 nm and 28 nm) technologies. Our evaluations show that the security vs. performance tradeoff of our dual-rail logic style does not scale well compared to CMOS. It also shows that the scaling trends for CMOS are more positive (i.e. smaller technologies and supply voltages reduce the energy consumption and the side-channel signal). So these results suggest that dual-rail logic style may not be a sustainable approach for side-channel signal reduction as we move towards lower technology nodes.

1 Introduction

Following the first publications on power and electromagnetic analysis against cryptographic implementations, dual-rail (aka dynamic and differential) logic styles appeared as promising candidates to improve security against such attacks. Intuitively, these logic styles aim to solve the issue directly at the circuit level, by trying to reduce the side-channel Signal-to-Noise Ratio (SNR). For this purpose, they typically ensure that the switching activity of the circuits is independent of the manipulated data. However, despite constant switching activity, small data-dependent variations in the current traces can generally be observed, e.g. due to the unbalanced capacitances of the gates differential nodes and their interconnections. Therefore, a large body of work investigated the design of dual-rail logic styles in order to reach the best security vs. performance tradeoff, including but not limited to SABL [36], WDDL [35], DyCML [1], MCML [8] and MDPL [27]. Evaluations based on both simulations and actual measurements then confirmed that getting rid of these data dependencies is extremely challenging [19,26,29,34]. More recent works even showed that filtering effects in

S. Guilley (Ed.): COSADE 2017, LNCS 10348, pp. 19–33, 2017.
DOI: 10.1007/978-3-319-64647-3_2

concrete measurement setups make these small data dependencies reasonably easy-to-exploit, e.g. thanks to linear regression [16]. To complete the picture, most of these dual-rail logic styles usually come with significant performance overheads, some of them additionally requiring full custom-design (which allows further control of the hardware, but is making development and deployment significantly more challenging/expensive).

In parallel, recent progresses have shown that mathematical countermeasures against side-channel analysis, and in particular the mainstream shuffling and masking techniques [6,13,21], can only lead to significant security improvements if the side-channel SNR has been sufficiently reduced beforehand [33,37]. This raises the problem of finding effective (and if possible efficient) hardware techniques allowing to fulfil this condition. Intuitively, it can be done by reducing the side-channel signal, which is what dual-rail logic styles achieve, or by increasing the noise.

Eventually, since the evaluation of secure hardware technologies goes together with technology scaling, another problem is to find out which of those approaches has more potential for the future.

In this paper, we therefore tackle this question of the comparative advantage of dual-rail logic styles as a mean of reducing the side-channel signal over standard CMOS in front of technology scaling. More precisely, we investigate how much the security vs. performance tradeoff of these design styles scales, based on the simple yet reflective case-study of CMOS and Dynamic and Differential Swing-Limited Logic (DDSLL) AES S-boxes, implemented in 65 and 28 nm technologies. DDSLL is yet another (full-custom) dual-rail logic style which has already been analyzed based on simulations and actual measurements [30]. Our choice of DDSLL arises from the fact that its design using 65 nm bulk technology shows 1.5× lower power consumption at the expense of 1.125× increase in area, while increasing the security 10× when compared to CMOS [15]. This compares positively with the typical power/energy and area costs obtained with the previously listed dual-rail logic styles. Therefore, DDSLL can be considered a good candidate to illustrate technology scaling trends (as discussed in conclusions, we expect other dual-rail logic styles to follow similar trends). In this respect, our main conclusions are twofold.

First, and looking at the tradeoff between the side-channel SNR and the implementation performances (here measured with the energy per operation, which is a quite reflective metric to compare cryptographic designs [17]), we see that the comparative advantage of DDSLL over CMOS is vanishing with technology scaling, and we explain this trend by the imbalances in DDSLL gates that gain impact with technology scaling.

Second, and more positively, we also see that technology and supply voltage scaling have a positive impact on the security vs. performance tradeoff of CMOS devices, essentially because such a scaling comes with energy gains and side-channel signal reductions.

Our case study therefore suggests that signal reduction using dual-rail logic styles may not be the best approach w.r.t technological scaling. It also suggests

that the design of noisy CMOS implementations (which is a natural consequence of scaling [10]) appears as a promising strategy for ensuring a sufficiently small side-channel SNR allowing (e.g.) masking and shuffling to be effective in future technologies. Note that by noisy implementations, we do not mean measurement noise or additional external noise but intrinsic noise at the device level (i.e. transistor, interconnect, resistor, ...) as a result of technological scaling.

Cautionary note. The results in this paper are based on simulations. While we admit that in general, they can lead to shortcomings (e.g. regarding the shape/linearity of the leakage traces), the experiments in [30] showed that they can be used as a good predictor for the amount of information leakage in dual-rail logic styles. Since the goal in this paper is to discuss general scaling trends, we believe simulations can therefore be used as an interesting indication of how the comparative advantage of CMOS over DDSLL scales. Note that anyway, we do not expect the shape/linearity of the leakage traces to be significantly different in 65 and 28 nm technologies, nor for CMOS vs. DDSLL, since the main linearization factor is due to filtering effects in the measurement setup and not the internal transistor behavior. So as usual with simulations, they should be interpreted with care (which we try to do in the paper). But as usual with simulations as well, they are a useful tool to get some hints about the best solutions to investigate up to (more expensive) tape outs.

The rest of the paper is structured as follows. Preliminaries are in Sect. 2. Our target implementation and evaluation settings are in Sect. 3. The comparative study between CMOS and DDSLL is in Sect. 4. The positive impact of technology and supply voltage scaling for CMOS implementations is in Sect. 5. Finally, our conclusions and a discussion of the relevance of this case study are in Sect. 6.

2 Preliminaries

2.1 Logic Styles: CMOS and DDSLL

Traditional CMOS circuits have shown a data-dependency in the power consumption leading to exploitable side-channel information, e.g. thanks to Differential Power Analysis (DPA) [18], Correlation Power Analysis (CPA) [5] and Template attacks [7]. The power consumption of a CMOS circuit is modeled by the following equation:

$$\begin{aligned} P &= P_{dyn} + P_{stat}, \\ &= \frac{1}{2}\, N_{nodes}\, \alpha_F\, C_L\, V_{DD}^2\, f_{clk} + I_{leak}\, V_{DD}, \end{aligned} \tag{1}$$

where P_{dyn} is the dynamic power consumption, P_{stat} the static power consumption, N_{nodes} is the number of nodes in the circuit, α_F represents the activity factor of the design, C_L is the load capacitance, V_{DD} is the supply voltage, f_{clk} represents the clock frequency and I_{leak} denotes the leakage current. We assume here that one operation is executed per clock cycle, and thus $\mathrm{f}_{clk} = \mathrm{f}_{op}$, which determines the target throughput of the application. The operation period $\mathrm{T}_{op} = \frac{1}{f_{op}}$

should be more than the critical path delay T_{del} to guarantee correct functionality. The data-dependency of the CMOS logic comes from both its dynamic and static power consumptions. In the dynamic part, α_F directly depends on the data being processed. In the static part, the I_{leak} is the data-dependent parameter. Although the former is dominant, static power consumption can also be exploited if its value is sufficiently high and the operating frequency is low enough allowing the reduction of noise via simple averaging techniques [24,28].[1] Yet, in our following experiments, dynamic power indeed dominates.

In comparison with CMOS, we investigate the Dynamic and Differential Swing-Limited Logic (DDSLL) which aims at low-power implementations and of which the dynamic power consumption is given by:

$$P_{dyn} = \frac{1}{2} N_{nodes} \alpha_F C_L V_{DD} V_{swing} f_{clk}, \tag{2}$$

where α_F equals 1 because all dynamic and differential logic styles ensure one output transition per clock cycle (independent of the data being processed), and V_{swing} is the output voltage swing. DDSLL gates are designed to have limited swing (i.e. $< V_{DD}$) in order to reduce the dynamic power consumption and hence the energy per operation.

Figure 1 shows the circuit of a generic DDSLL gate. A Differential Pull-Down Network (DPDN) is used to evaluate the required function. It mainly consists of NMOS transistors. The DDSLL gate employs a dynamic current source to significantly reduce the static power consumption similar to what is achieved in the DyCML logic style. The cut-off of this current source is performed via a feedback network which signals the end of an operation, so that the self-timing buffer creates a clock signal Clk_{i+1} declaring the termination of the current evaluation phase. This clock signal is used to feed the following DDSLL gate. The precharge transistors are used to precharge the differential outputs of a DDSLL gate to the supply voltage before an evaluation of the gate's function takes place, and the latch transistors preserve the evaluated voltage at the differential output nodes.

The operation of a DDSLL gate is quite simple. It works in two modes: precharge and evaluation. In the precharge mode, when the clock signal Clk_i is low, the outputs out and $\overline{out}$ are precharged to V_{DD}. There is no current path from V_{DD} to GND because transistor M_1 is switched off. However, transistors M_6 and M_2 are switched on. Next during the evaluation phase, Clk_i goes high turning on the transistor M_1 while M_2 is still on (both forming the dynamic current source) as node ENO was previously charged to VDD in the previous precharge phase, thus creating a path to discharge one of the output nodes to GND. The discharge path through the DPDN network is the one with the lowest impedance depending on the inputs being processed. As one of the outputs falls

[1] Note that advanced technologies usually provide multiple flavors such as low-power and high-performance along with different device choices such as high and low threshold voltages, providing circuit designers with various options to reduce the power consumption – and the leakage power as well – which may modify the respective importance of these source of leakages.

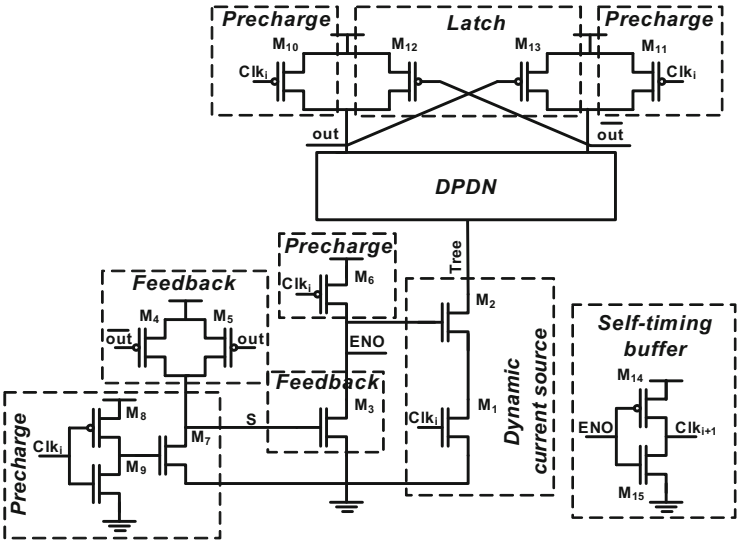

Fig. 1. Schematic of a generic DDSLL gate.

below the threshold voltage of the feed-back transistors (M_4, M_5), one of them will turn on which in turn will discharge the node ENO to GND thus starving the current source. The design of a DDSLL circuit comprising of several functions can benefit from resource sharing (the dynamic current source, parts of the precharge circuit, the feedback circuit and the self-timing buffer of functions that evaluate at the same time), therefore reducing the area cost and the overall power consumption.

In all differential design styles, the unbalanced capacitances are considered as a source of information leakage. They mainly come from either routing imbalances or from internal imbalances. In this paper, we only consider the latter ones. (As mentioned in Sect. 3.3, additionally considering post-layout simulations or variability should amplify the trend we put forward). In this respect, we note that the only way to eliminate internal imbalances is to design circuits with perfectly symmetrical differential gates, which is usually very expensive in terms of area and speed. Hence, our DPDN designs exploit the binary decision diagram technique from [11] in order to improve performances by exploiting more complex gates with minimum imbalance caused by internal capacitances (details can be found in [15]). So essentially, what we show next is that (here internal) imbalances have an increasing impact with technology scaling.

2.2 Evaluation Metrics

Evaluating logic styles across technology scaling and supply voltage scaling is a challenging task, since certain metrics may favour one logic style over another. In order to be as fair as possible in our performance and security evaluations,

we therefore selected generic metrics that are generally more reflective of the "global performance level" of an implementation, and can capture any type of information leakage.

More precisely, and as far as performances are concerned, the energy per operation is a quite discriminant metric, as it corresponds to an integral over time, and therefore is not "compressible" (via architectural tweaks) beyond what is allowed by the total combinatorial cost of an implementation [17]. Concretely, the energy consumption of a logic circuit can be calculated by integrating the power consumption over the time required for the target operation (in our case-study, the AES S-box):

$$\begin{aligned} E_{op} &= \int_t (P_{dyn} + P_{stat})\, dt, \\ &= \underbrace{\frac{1}{2}\, N_{sw}\, C_L\, V_{DD}\, V_{swing}}_{\text{Dynamic}} + \underbrace{V_{DD}\, I_{leak}\, T_{del}}_{\text{static}}, \end{aligned} \tag{3}$$

where $N_{sw} = \alpha_F\, N_{nodes}$ is the number of switching nodes for the operation and T_{del} is the circuit delay (following the investigations in [4]). In the case of CMOS logic style, V_{swing} is equal to the supply voltage being used.

As for the security metrics, our choice was dictated by various constraints and features. First, the shape of the instantaneous dynamic power (i.e. the side-channel signal) changes significantly depending on the technology and the supply voltage used. Therefore, it is important to consider these changes while evaluating the CMOS and DDSLL logic styles, and to consider a multivariate analysis. Second, our target implementations are not masked, and therefore our simulations exclusively exploit first-order leakages. So while in general, a fair comparison of our logic styles would require to compute a mutual information metric [32], in this particular case we can simplify our evaluations by (i) applying a dimensionality reduction to our traces, namely a Principal Component Analysis (PCA) which will capture the shape of the noise-free simulated traces [2], and (ii) computing Mangard's SNR on the reducted traces [20], which is equivalent to the mutual information metric in this case [9,22].

For this purpose, we denote a power trace as $\boldsymbol{l}$, its corresponding random variable as $\boldsymbol{L}$, and assume that this random variable is a function of the S-box input X, and a noise random variable $\boldsymbol{N}$. The multivariate traces are reduced to univariate ones thanks to PCA, which we denote as: $l = \mathsf{PCA}(\boldsymbol{l})$. Giving the trace l a subscript x corresponding to the input and a superscript i corresponding to an index (since the trace for a plaintext x can be measured multiple times), Mangard's SNR is defined as:

$$\mathrm{SNR} = \frac{\hat{\mathsf{var}}_x(\hat{\mathsf{E}}_i(L_x^i))}{\hat{\mathsf{E}}_x(\hat{\mathsf{var}}_i(L_x^i))}, \tag{4}$$

where $\hat{\mathsf{E}}$ (resp. $\hat{\mathsf{var}}$) denotes the sample mean (resp. variance) operator. In our following simulations, this SNR will be computed for noise-free traces. This amounts

to maximizing the signal $\hat{\mathsf{var}}_x(\hat{\mathsf{E}}_i(L_x^i))$ (i.e. we ignore the denominator of Eq. 4 in this case).

Note that for readability, our following results only report the quantification of our experiments with this security metric. However, various other (heuristic) choices could be considered, e.g. computing the SNR for the most informative samples in the traces, or considering more dimensions after the application of the PCA. The same holds with performance metrics (e.g. the throughput over area ratio could be used as alternative efficiency metric). In our study, none of these variations (that we also browsed) lead to different conclusions regarding the two main trends outlined in introduction.

3 AES S-Box Implementations

3.1 AES S-Box

For the sake of simplicity, and in order to demonstrate the technology trends of CMOS and DDSLL, we chose an 8-bit AES S-box as the benchmark circuit. More specifically, we considered a combinatorial implementation of the S-box from [14], based on the architecture proposed in [23,31]. Thanks to mapping the elements of the original field $\mathrm{GF}(2^8)$ to the composite field $\mathrm{GF}(((2^2)^2)^2)$, the gate complexity and the power consumption can be greatly reduced. The adopted S-box consists of 3 stages: a transformation stage to map the elements to the $\mathrm{GF}(((2^2)^2)^2)$ field, an inversion stage and an inverse transformation stage to map the elements back to $\mathrm{GF}(2^8)$, grouped with the affine transformation.

3.2 Target Designs

The CMOS and DDSLL AES S-boxes were implemented in a full-custom fashion, using the CADENCE Virtuoso tools, in a low-power 65 nm bulk technology and 28 nm FDSOI technology. The CMOS implementation of the S-box is made only of 2-input AND/NAND and 2-input XOR/XNOR gates. The total number of transistors is 1,530, with a logic depth of 22 gates. On the other hand, the DDSLL S-box accounts for 1275 transistors, with a logic depth of 13 gates.

The gate design of CMOS and DDSLL S-boxes in both 65 nm bulk and 28 nm FDSOI technologies is kept identical, i.e. the gates used and the number of transistors remain unchanged. However, we respected the minimum feature size of each technology (to decrease the switching capacitance, hence the energy per operation) and resized the transistors' widths adequately to guarantee functionality. In 65 nm bulk technology, standard threshold voltage (SVT) transistors are used to reduce the static current while maintaining good performances with respect to the circuit delay. For benchmarking purposes, we also implemented the CMOS and DDSLL S-boxes using the low threshold voltage (LVT) transistors available from the same technology. In 28 nm FDSOI technology, both SVT and LVT transistors were again used to maintain a fair comparison with the 65 nm technology. Yet, for readability, our following results only report the

quantification of our experiments with SVT transistors (trends are again identical for LVT transistors). Eventually, the widths of the DDSLL S-box transistors were chosen such that the voltage swing is sufficient for the circuit to operate correctly at the lower limit of the supply voltages of each technology.

In our experiments, all the S-boxes are fed with buffered inputs to maintain equal fan-ins and have realistic inputs, yet the DDSLL S-box additionally has a buffered clock. Also, all the outputs of the S-boxes are loaded with equal fan-out buffers. Each S-box is provided with a separate supply voltage than that of the input/output buffers so that the buffers' energy consumptions are not taken into account in our evaluations.

3.3 Simulation Settings

Simulations for the above designs are done at the schematic level (without any extracted post-layout capacitances) using Eldo simulator based on SPICE models provided by the industrial foundries at room temperature of 25 °C. In this respect, we note that any imbalance in the parasitic elements would affect the difference between the delay of the differential routes of the DDSLL S-box, which would impact its power consumption, leading to a higher (exploitable) signal being observed by practical attacks [30]. And this is expected to get only worse with technology scaling and variability, since balancing the capacitances in an implementation naturally becomes more challenging with smaller circuits and smaller routing capacitances. Therefore, and as previously mentioned, taking the parasitic routing capacitances into consideration could only amplify our observation (which is that the comparative advantage of DDSLL over CMOS is vanishing with technology scaling). A similar statement holds for other effects that we did not take into consideration in this work such as crosstalk and the influence of process, voltage and temperature (PVT) variations.

Consequently, we assume our results correspond to an ideal scenario and the inclusion of more physical default(s) should only deteriorate the performance of dual-rail logic styles compared to CMOS.

The frequency of operation is chosen to be 10 MHz, which is in accordance with the usual operating frequencies for cryptographic applications (see, e.g. [3]). The supply voltage is swept across a range of 500 mV, in steps of 100 mV starting from the nominal voltage of each technology, namely, 1.2 V and 1 V for the 65 nm bulk and the 28 nm FDSOI technologies, respectively. The lower limit of the supply voltages is imposed by the correct functionality of the circuit at the target frequency for a given implementation.

Note that operating at high supply voltages and using the 28 nm technology node allows the circuit implementation to run at higher frequencies. But the frequency choice has no impact on our results since we have chosen to use the energy per operation as the evaluation metric and not the total power consumption.

To calculate the energy per operation, we considered 1000 random input signals. As for the security analysis, the S-box input signal has 256 possible values whose transitions are chosen between 0 and an arbitrary input. Restricting the

inputs to a subset from the 256^2 possible inputs was mainly motivated by practical simulation constraints (memory and simulation time) and is not expected to strongly impact the comparison between the logic styles.

4 Comparative Scaling Trends: CMOS vs. DDSLL

In this section, we aim to compare the CMOS and DDSLL logic styles and study how their security versus performance tradeoff evolves with technology and supply voltage scaling. To be able to do that in a comprehensible manner, we plot the ratios between our (security and performance) metrics computed for both CMOS and DDSLL, one in function of the other. More precisely, Fig. 2 shows the PCA signal ratio between CMOS and DDSLL S-boxes versus the energy per operation ratio between these logic styles for the 65 nm bulk and the 28 nm FDSOI technologies (designed using SVT devices). The different points represent the supply voltages we used that span over a range of 0.5 V starting from the nominal supply of each technology (1.2 V and 1 V for the 65 and 28 nm technologies, respectively). This study allows us to make the following observations:

1 By reducing the supply voltage, the energy per operation ratio of CMOS with respect to DDSLL is decreasing for the 65 and 28 nm technologies. This reduction can be explained by the fact that the E_{op} value of the DDSLL style decreases almost linearly with the supply voltage, because it maintains nearly the same voltage swing while E_{op} of CMOS decreases quadratically (see Eq. 3).
2 As for the PCA signal ratio between CMOS and DDSLL (for both technologies), it also decreases with the supply voltage scaling. Again, this is due to the fact that the voltage swing of the DDSLL S-box is kept almost unchanged leading to a slow reduction rate of the transient power consumption. Hence the PCA signal with V_{DD} scaling is less compared to that of CMOS.
3 Most importantly, Fig. 2 illustrates that at 28 nm technology, the PCA signal ratio between CMOS and DDSLL is less than that of the 65 nm technology for similar E_{op} ratios. This figure neatly puts forward that the security vs. performance tradeoff between these logic styles does not scale positively for DDSLL, even though we do not consider any routing parasitics or PVT variations in our simulations.

It is worth emphasizing that similar observations were made by comparing CMOS to DDSLL S-boxes using LVT devices in both technologies. Therefore, changing the device type leads only to either better performance or more power savings, but the technology and supply voltage scaling trends remain the same. Also, and for the sake of completeness, we conducted the same experiments using the maximum SNR (before PCA) as a security metric and the technology and supply voltage scaling trends remained unchanged.

In addition, we note that changing the frequency of operation does not impact our conclusions as long as the dynamic power consumption dominates. We simulated the S-boxes down to 100 kHz and the technology and voltage scaling trends were again the same.

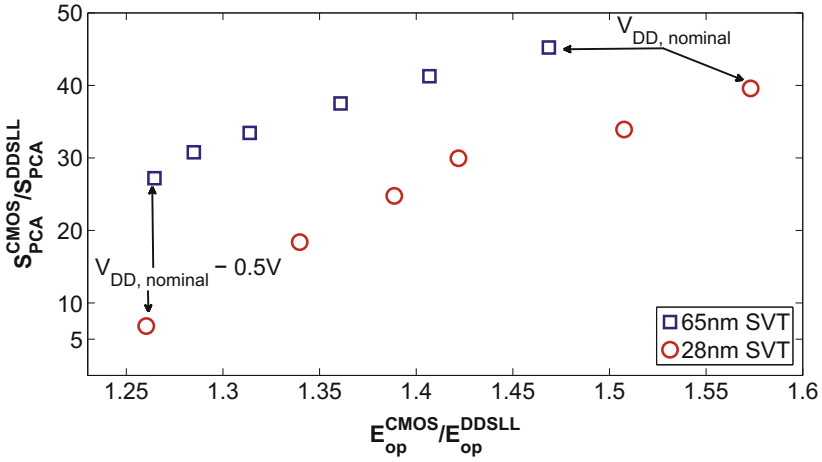

Fig. 2. Evolution of the tradeoff between the PCA signal ratio and the E_{op} ratio for CMOS vs. DDSLL using 65 and 28 nm technology nodes.

Eventually, we note that technology scaling is advancing at a fast pace and secure implementations will soon follow (given the fact that up until now applications such as smart cards tend to lag by one or two technologies). Also, circuit designers generally aim at scaling the supply voltage in order to further reduce the energy consumption of the digital circuits (sometimes operating below the transistor subthreshold voltage leading to minimum energy per operation). Both trends lead us to conclude that the observations in this section may rapidly have concrete relevance.

5 Technology and V_{DD} Scaling Trends for CMOS

Since the comparative advantage of DDSLL over CMOS vanishes in our case study, one natural complementary question is whether scaling trends for CMOS circuits lead to a more positive conclusion. In this section, we answer this question by focusing on the impact of technology and V_{DD} scaling on CMOS circuits only. For this purpose, Fig. 3(a) reports the energy per operation of the CMOS S-box for different supply voltages, using both 65 and 28 nm technologies. We recall that the minimum V_{DD} was chosen such that the CMOS S-box operates correctly at the 10 MHz target frequency for each technology. As expected, the energy per operation of CMOS decreases almost quadratically with the reduction of the supply voltage (see Eq. 3). The figure also shows clearly that technology scaling from 65 to 28 nm reduces the energy per operation (of the CMOS S-box) by a factor of 2.2×. This reduction is compliant with the expected technology scaling trend as explained in [12].

Similarly, Fig. 3(b) shows the signal after PCA of the CMOS S-box for different V_{DD} values, using both 65 and 28 nm technologies. The PCA signal of

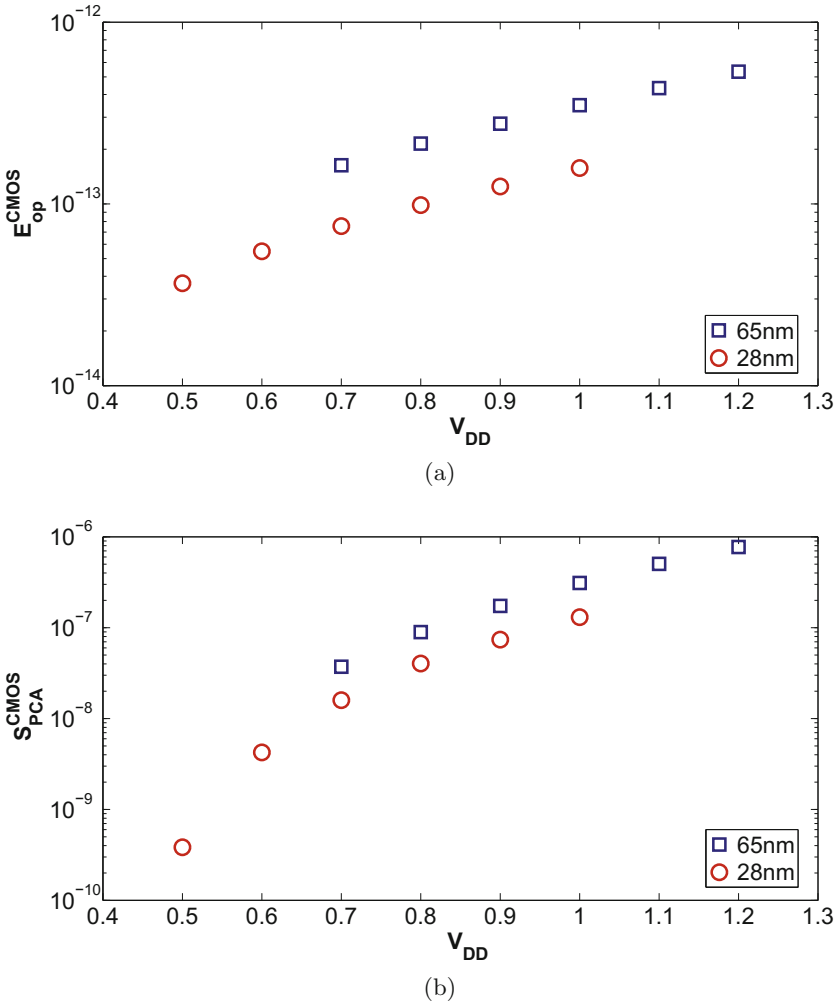

Fig. 3. Scaling trends of E_{op} and the PCA signal for the CMOS S-box across a supply voltage range of 500 mV for 65 and 28 nm tech.

CMOS decreases as the supply voltage scales down. In the 65 nm technology, the S_{PCA} reduction is more than one order of magnitude across the whole V_{DD} range (1.2 V to 0.7 V) and it reaches even more than two orders of magnitude in the 28 nm technology, by reducing the supply voltage from 1 V down to 0.5 V. As for the technology scaling from 65 to 28 nm, it is also clear that the signal after PCA of the CMOS S-box decreases by a factor of 2.3× at comparable supply voltages. So the scaling trends for PCA signal is also positive for CMOS. Here, we note that an analytical explanation of these observations is more challenging, since the small data-dependent current variations that lead to exploitable side-

channel signal are much harder to capture theoretically. (Yet, we can suppose that the aforementioned signal reductions essentially originate from the interactions between reductions of the current and variations of the load capacitance).

6 Conclusion

In this case study, we analyzed for the first time the comparative scaling trends of CMOS and dual-rail logic styles. In short, our evaluations suggest that the interest of DDSLL over CMOS, expressed in terms of a security vs. performance tradeoff, vanishes as circuit sizes shrink. To a good extent, we believe a similar conclusion should be obtained for other dual-rail logic styles. In particular, from the security point-of-view, they all suffer from capacitance imbalances to some extent, and this phenomenon can only be magnified in smaller technologies. While our case study was based on an AES S-box, we believe similar trends should also be obtained for full AES implementations. Indeed, similar energy trends will be integrated over more clock cycles, and the signal variations exploited in a DPA are anyway focused on the first cipher rounds. These results therefore suggest that reducing the SNR in advanced technologies may be better achieved by exploiting the naturally increasing intrinsic noise level than by reducing the signal using dual-rail logic styles. It also suggests the design of noisy and efficient CMOS implementations as an interesting scope for further research.

We finally note that while dual-rail logic styles may not be a sustainable solution for signal reduction purposes, it remains possible that they are helpful ingredients of physically secure implementations for other reasons (e.g. in order to facilitate the independence condition that is required for masking to deliver its security promises [39]), which is an interesting scope for further research.

Acknowledgments. This work has been funded in parts by the ARC Project NANOSEC. François-Xavier Standaert is a research associate of the Belgian Fund for Scientific Research.

References

1. Allam, M., Elmasry, M.: Dynamic current mode logic (DyCML): a new low-power high-performance logic style. IEEE J. Solid-State Circ. **36**(3), 550–558 (2001)
2. Archambeau, C., Peeters, E., Standaert, F.-X., Quisquater, J.-J.: Template attacks in principal subspaces. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 1–14. Springer, Heidelberg (2006). doi:10.1007/11894063_1
3. Bellizia, D., Bongiovanni, S., Monsurro, P., Scotti, G., Trifiletti, A.: Univariate power analysis attacks exploiting static dissipation of nanometer CMOS VLSI circuits for cryptographic applications. IEEE Trans. Emerg. Top. Comput. **PP**(99), 1 (2016)
4. Bol, D., Kamel, D., Flandre, D., Legat, J.-D.: Nanometer MOSFET effects on the minimum-energy point of 45 nm subthreshold logic. In: Proceedings of the 2009 International Symposium on Low Power Electronics and Design, San Fancisco, CA, USA, 19–21 August 2009, pp. 3–8 (2009)

5. Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Joye, M., Quisquater, J.-J. (eds.) CHES 2004. LNCS, vol. 3156, pp. 16–29. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28632-5_2
6. Chari, S., Jutla, C.S., Rao, J.R., Rohatgi, P.: Towards sound approaches to counteract power-analysis attacks. In: Wiener [38], pp. 398–412
7. Chari, S., Rao, J.R., Rohatgi, P.: Template attacks. In: Kaliski, B.S., Koç, K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp. 13–28. Springer, Heidelberg (2003). doi:10.1007/3-540-36400-5_3
8. Deniz, Z.T., Leblebici, Y.: Low-power current mode logic for improved DPA-resistance in embedded systems. In: International Symposium on Circuits and Systems (ISCAS 2005), Kobe, Japan, 23–26 May 2005, pp. 1059–1062. IEEE (2005)
9. Duc, A., Faust, S., Standaert, F.-X.: Making masking security proofs concrete. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 401–429. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46800-5_16
10. Ghosh, S., Roy, K.: Parameter variation tolerance and error resiliency: new design paradigm for the nanoscale era. Proc. IEEE **98**(10), 1718–1751 (2010)
11. Giancane, L., Marietti, P., Olivieri, M., Scotti, G., Trifiletti, A.: 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, pp. 364–367, August 2008
12. Haensch, W., Nowak, E.J., Dennard, R.H., Solomon, P.M., Bryant, A., Dokumaci, O.H., Kumar, A., Wang, X., Johnson, J.B., Fischetti, M.V.: Silicon CMOS devices beyond scaling. IBM J. Res. Dev. **50**(4–5), 339–362 (2006)
13. Herbst, C., Oswald, E., Mangard, S.: An AES smart card implementation resistant to power analysis attacks. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 239–252. Springer, Heidelberg (2006). doi:10.1007/11767480_16
14. Kamel, D., Standaert, F.X., Flandre, D.: Scaling trends of the AES S-box low power consumption in 130 and 65 nm CMOS technology nodes. In: 2009 IEEE International Symposium on Circuits and Systems, pp. 1385–1388, May 2009
15. Kamel, D., Renauld, M., Bol, D., F.-X., Standaert, D., Flandre, D.: Analysis of dynamic differential swing limited logic for low-power secure applications. J. Low Power Electron. Appl. **2**(1), 98 (2012)
16. Kamel, D., Renauld, M., Flandre, D., Standaert, F.-X.: Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations. J. Cryptographic Eng. **4**(3), 187–195 (2014)
17. Kerckhof, S., Durvaux, F., Hocquet, C., Bol, D., Standaert, F.-X.: Towards green cryptography: a comparison of lightweight ciphers from the energy viewpoint. In: Prouff, E., Schaumont, P. (eds.) CHES 2012. LNCS, vol. 7428, pp. 390–407. Springer, Heidelberg (2012). doi:10.1007/978-3-642-33027-8_23
18. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener [38], pp. 388–397
19. Macé, F., Standaert, F.-X., Quisquater, J.-J.: Information theoretic evaluation of side-channel resistant logic styles. In: Paillier and Verbauwhede [25], pp. 427–442
20. Mangard, S.: Hardware countermeasures against DPA – a statistical analysis of their effectiveness. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 222–235. Springer, Heidelberg (2004). doi:10.1007/978-3-540-24660-2_18
21. Mangard, S., Oswald, E., Popp, T.: Power Analysis Attacks - Revealing the Secrets of Smart Cards. Springer, Heidelberg (2007)
22. Mangard, S., Oswald, E., Standaert, F.-X.: One for all - all for one: unifying standard differential power analysis attacks. IET Inf. Secur. **5**(2), 100–110 (2011)

23. Mentens, N., Batina, L., Preneel, B., Verbauwhede, I.: A systematic evaluation of compact hardware implementations for the Rijndael S-Box. In: Menezes, A. (ed.) CT-RSA 2005. LNCS, vol. 3376, pp. 323–333. Springer, Heidelberg (2005). doi:10.1007/978-3-540-30574-3_22
24. Moradi, A.: Side-channel leakage through static power. In: Batina, L., Robshaw, M. (eds.) CHES 2014. LNCS, vol. 8731, pp. 562–579. Springer, Heidelberg (2014). doi:10.1007/978-3-662-44709-3_31
25. Paillier, P., Verbauwhede, I., (eds.) Proceedings of the 9th International Workshop Cryptographic Hardware and Embedded Systems - CHES 2007. LNCS, Vienna, Austria, 10–13 September 2007, vol. 4727. Springer, Heidelberg (2007)
26. Popp, T., Kirschbaum, M., Zefferer, T., Mangard, S.: Evaluation of the masked logic style MDPL on a prototype chip. In: Paillier and Verbauwhede [25], pp. 81–94
27. Popp, T., Mangard, S.: Masked dual-rail pre-charge logic: DPA-resistance without routing constraints. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 172–186. Springer, Heidelberg (2005). doi:10.1007/11545262_13
28. Del Pozo, S.M., Standaert, F.-X., Kamel, D., Moradi, A.: Side-channel attacks from static power: when should we care? In: Proceedings of the 2015 Design, Automation & Test in Europe Conference & Exhibition, DATE 2015, Grenoble, France, 9–13 March 2015, pp. 145–150 (2015)
29. Regazzoni, F., Eisenbarth, T., Poschmann, A., Großschädl, J., Gürkaynak, F.K., Macchetti, M., Deniz, Z.T., Pozzi, L., Paar, C., Leblebici, Y., Ienne, P.: Evaluating resistance of MCML technology to power analysis attacks using a simulation-based methodology. Trans. Comput. Sci. **4**, 230–243 (2009)
30. Renauld, M., Kamel, D., Standaert, F.-X., Flandre, D.: Information theoretic and security analysis of a 65-nanometer DDSLL AES S-Box. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 223–239. Springer, Heidelberg (2011). doi:10.1007/978-3-642-23951-9_15
31. Satoh, A., Morioka, S., Takano, K., Munetoh, S.: A compact rijndael hardware architecture with s-box optimization. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 239–254. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_15
32. Standaert, F.-X., Malkin, T.G., Yung, M.: A unified framework for the analysis of side-channel key recovery attacks. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 443–461. Springer, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_26
33. Standaert, F.-X., Veyrat-Charvillon, N., Oswald, E., Gierlichs, B., Medwed, M., Kasper, M., Mangard, S.: The world is not enough: another look on second-order DPA. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 112–129. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_7
34. Tiri, K., Verbauwhede, I.: Securing encryption algorithms against DPA at the logic level: next generation smart card technology. In: Walter, C.D., Koç, Ç.K., Paar, C. (eds.) CHES 2003. LNCS, vol. 2779, pp. 125–136. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45238-6_11
35. Tiri, K., Verbauwhede, I.: A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation. In: 2004 Design, Automation and Test in Europe Conference and Exposition (DATE 2004), Paris, France, 16–20 2004, pp. 246–251. IEEE Computer Society, February 2004
36. Tiri, K., Verbauwhede, M.A.I.: A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards. In: Proceedings of the 28th European Solid-State Circuits Conference, ESSCIRC 2002, pp. 403–406. IEEE (2002)

37. Veyrat-Charvillon, N., Medwed, M., Kerckhof, S., Standaert, F.-X.: Shuffling against side-channel attacks: a comprehensive study with cautionary note. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 740–757. Springer, Heidelberg (2012). doi:10.1007/978-3-642-34961-4_44
38. Wiener, M.J. (ed.) 19th Annual International Cryptology Conference 1999 Proceedings Advances in Cryptology - CRYPTO 1999. LNCS, Santa Barbara, California, USA, 15–19 August 1999, vol. 1666. Springer, Heidelberg (1999)
39. Wild, A., Moradi, A., Güneysu, T.: GliFreD: Glitch-free duplication - towards power-equalized circuits on FPGAs. IACR Cryptology ePrint Archive 2015:124 (2015)

http://www.springer.com/978-3-319-64646-6

Constructive Side-Channel Analysis and Secure Design
8th International Workshop, COSADE 2017, Paris,
France, April 13-14, 2017, Revised Selected Papers
Guilley, S. (Ed.)
2017, X, 299 p. 127 illus., Softcover
ISBN: 978-3-319-64646-6