Information Theoretic Evaluation of Side-Channel Resistant Logic Styles

François Macé[*], François-Xavier Standaert[**], Jean-Jacques Quisquater

UCL Crypto Group, Université Catholique de Louvain.
e-mails: mace,fstandae,jjq@uclouvain.be

Abstract. We propose to apply an information theoretic metric to the evaluation of side-channel resistant logic styles. Due to the long design and development time required for the physical evaluation of such hardware countermeasures, our analysis is based on simulations. Although they do not aim to replace the need of actual measurements, we show that simulations can be used as a meaningful first step in the validation chain of a cryptographic product. For illustration purposes, we apply our methodology to gate-level simulations of different logic styles and stress that it allows a significant improvement of the previously considered evaluation methods. In particular, our results allow putting forward the respective strengths and weaknesses of actual countermeasures and determining to which extent they can practically lead to secure implementations (with respect to a noise parameter), if adversaries were provided with simulation-based side-channel traces. Most importantly, the proposed methodology can be straightforwardly adapted to adversaries provided with any other kind of leakage traces (including physical ones).

1 Introduction

In modern cryptography, a side-channel attack is generally defined as an attack based on information gained from the physical implementation of a cryptosystem, rather than theoretical weaknesses in the algorithms. As typical examples, timing information [12], power consumption [13] or electromagnetic emanations [1] provide a source of information that can be exploited to break a particular system. Since their introduction in the 1990s, such attacks have been demonstrated extremely powerful to defeat a variety of algorithms (*e.g.* secret or public key) implemented on different platforms (*e.g.* smart cards, ASICs, FPGAs). Following these findings, a significant research effort has been devoted to the development of countermeasures against these physical leakages. Such protections are usually classified between software and hardware countermeasures.

Software countermeasures typically rely on time or data randomization techniques in order to decorrelate the physical leakages from the target data. Because of their fast development time, such countermeasures have been intensively studied in the open literature. Although none of them is sufficient to completely prevent side-channel attacks, it is generally admitted that they increase the difficulty of performing a key recovery. Hardware countermeasures rely on modifications

[*] François Macé is a PhD student funded by the FRIA, Belgium.

[**] Postdoctoral researcher of the Belgian Fund for Scientific Research (FNRS).

of an implementation's physical structure. As a typical example, asynchronous designs have been investigated in order to evaluate the extent to which they decrease the side-channel leakages, *e.g.* in [8]. Similarly, the use of dynamic and differential logic styles for which the power consumption is (ideally) independent of the data handled, *e.g.* in [11, 15, 21, 22], the use of masked logic gates, *e.g.* in [9], or the combination of both, *e.g.* in [17] have been proposed as solutions to increase to security of an implementation against side-channel adversaries. Although side-channel attacks have been intensively investigated in the recent years [6], the fair evaluation of these different countermeasures has been a long standing open question. In [18], a theoretical framework was consequently introduced and suggests analyzing side-channel attacks with a combination of information theoretic and security metrics. These metrics respectively aim to evaluate the amount of information provided by a leaking implementation and the possibility to turn this information into a successful key recovery. They allow considering the quality of an implementation and the strength of an adversary separately.

This paper has three distinct goals. First, we aim to *analyze* different *hardware countermeasures* against side-channel attacks *with the information theoretic metric* introduced in [18]. We also justify this evaluation criteria with respect to previous attempts to quantify the effectiveness of side-channel countermeasures. Unfortunately, due to the length and cost of their design process, only a few realizations of hardware countermeasures have been publicly detailed, evaluated and compared. As a consequence, an alternative goal of the paper is to *improve* the previously proposed *simulation-based security evaluations* for side-channel resistant logic styles. We note that such simulation-based investigations are not intended to replace the need of actual measurements in side-channel attacks but to serve as a meaningful first step in their evaluation. As intuitively pictured in Figure 1, a target implementation can be viewed at different levels of complexity, ranging from an abstract logic level to the actual physical level. As a matter of fact, side-channel attacks are performed at the physical level. The aim of a simulation-based security evaluation is to get some insights on a physical attack without performing measurements, by carefully investigating higher abstraction levels. The figure immediately suggests the limitations of such an approach. Namely, each time the abstraction level decreases, new imperfections may appear in the design process, possibly increasing the amount of information provided to the adversary. For example, certain masking schemes work fine at the logic level but fall under attacks if the circuits glitching activity is taken into account [16]. Similarly, dual-rail circuits are highly dependent on how perfectly balanced the routing process is [10, 23]. Otherwise said, the best security evaluation is (obviously) performed at the physical level, using actual measurements. Hopefully, this does not mean that the simulation-based approach is meaningless, but that it only pictures a part of the physical reality that has to be confirmed by subsequent analyzes at lower abstraction levels. This latter point relates to the third objective of the paper. Namely, we aim to illustrate how the evaluation methodology introduced in [18] can be turned into a *bottom-up approach for the security evaluation* of any countermeasure against side-channel attack.

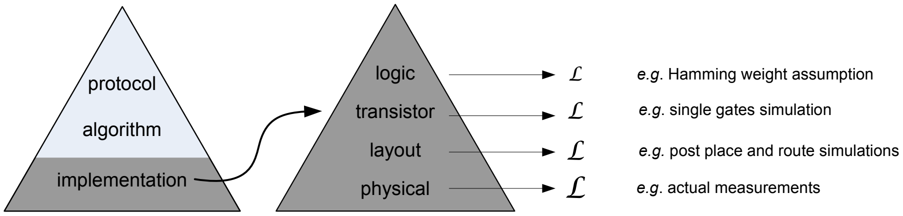

protocol
algorithm
implementation
logic
transistor
layout
physical
ℒ
ℒ
ℒ
ℒ
e.g. Hamming weight assumption
e.g. single gates simulation
e.g. post place and route simulations
e.g. actual measurements

Fig. 1. Circuit abstraction levels and side-channel leakages.

Otherwise said, the transistor-level simulated traces we analyze in this report only provide the bottom of a complete evaluation process for side-channel resistant logic styles. Lower level (*e.g.* post-layout) simulations are intermediate steps and physical measurements constitute the top-level. But contrary to most previous (ad hoc) solutions for the analysis of side-channel attacks and countermeasures, the proposed methodology and metrics are expected to remain meaningful against any implementation, at any abstraction level.

2 Brief description of the investigated logic styles

In this section, we briefly present the different logic styles we considered for our security investigations. Among the various proposals that have been proposed in the open literature (that could be similarly investigated), they were selected in order to obtain a representative panel of countermeasures acting at the gate level. Namely, we analyzed standard CMOS gates for reference, dual-rail pre-charged logic styles and masked logic styles. We also selected countermeasures requiring full custom design *vs.* countermeasures that can be implemented using CMOS standard cell libraries. These features are summarized in Table 1.

- **Sense Amplifier Based Logic (SABL):** is a full custom logic style proposed in [21]. SABL uses dual-rails and pre-charges with an internal structure allowing the full discharge of all the internal capacitances.
- **Wave Dynamic Differential Logic (WDDL):** is a dual-rail pre-charge like logic style based on standard cell libraries [22]. It uses a combination of complementary logic gates in order to balance the activity in the circuit.
- **Dynamic Current Mode Logic (DyCML):** is a dual-rail pre-charge logic style using current mode behavior. It was originally proposed in [2] and the first investigations of its security features have been proposed in [15].
- **Low-Swing Current Mode Logic (LSCML):** is a dual-rail pre-charge logic style presented in [11] using current mode logic behavior as DyCML. In LSCML, the value of the swing is independent of the value of the load capacitances and of the size of a particular transistor.
- **Masked Dual-Rail Pre-charge Logic (MDPL):** is a masked dual-rail pre-charge logic style, introduced by Popp and Mangard [17] in order to get rid of the routing constraints usually required for dual-rail gates to resist side-channel attacks. It can be implemented using a standard majority gate.

- **Gammel-Fischer Logic (GF):** relates to the work presented in [9], in which the authors formalize the problem of information leakage due to glitches for masked logic and propose a combination of operations that do not reveal information about the data handled, even in the presence of glitches.

Logic styles	Dual-Rail	Masked	Pre-Charged	Standard Cell
CMOS				✓
SABL	✓		✓	
WDDL	✓		✓	✓
DyCML	✓		✓	
LSCML	✓		✓	
MDPL	✓	✓	✓	✓
GF		✓		

Table 1. Summary of logic styles.

3 Evaluation criteria & methodology

3.1 Old proposals and limitations

Since the first logic styles were proposed in order to improve the security against side-channel attacks, several evaluation criteria have been introduced to quantify their effectiveness. The aim of this section is to detail some of the most frequently used criteria and to point out their limitations.

Among the first ones, the Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD) were introduced in [21] and used in a number of works. They both categorize the quality of a logic style according to the variance of the power consumption over different keys. The main limitation of this approach is that it does not allow a fair comparison of masked and dual-rail logic styles. Dual rails typically reduce the variances while masking does not. NED and NSD are therefore heuristic metrics rather than sound criteria. An improvement of the variance-only approach is to consider a particular side-channel adversary and see how good it behaves against various logic styles. For example, [17] suggested comparing the difference-of-mean-energies of different logic styles which directly relates to Kocher's DPA [13]. Tiri and Verbauwhede similarly used a correlation attack [25]. The limitation is then that the security evaluation relates to one particular adversary. In theory, it would be interesting to discriminate the logic styles, independently of a particular attack.

As a consequence of these limitations, an evaluation methodology for side-channel attacks was introduced in [18] and suggests quantifying them with a combination of security and information theoretic metrics. Intuitively, the aim of a security metric is to measure the strength of a side-channel adversary while the aim of an information theoretic metric is to determine the amount of information leaked by a given implementation (or logic style). It is shown in [18] that the mutual information relates to the asymptotic success rate of a Bayesian adversary that is usually assumed to be the strongest one for side-channel attacks, if a perfect noise model is available to the adversary [5]. Since the mutual information measures the extent to which the side-channel information allows discriminating different keys, it is the method of choice for the evaluation of different countermeasures. In the following, we will consequently compute this information for various logic styles. In addition, and contrary to previous approaches for the evaluation of side-channel countermeasures, we will evaluate the information available with respect to the amount of noise in the side-channel measurements in order to determine the noise thresholds for which a given countermeasure becomes a better (or worse) solution than another one.

3.2 Information theoretic approach

In this section, we define the mutual information as it will be used to evaluate different side-channel resistant logic styles. For this purpose, we define S_g as a variable denoting the correct target signal (*e.g.* typically, a part of a secret key) in a side-channel attack and s_g as a realization of this variable. Similarly, the variable S denotes any possible candidate value of the correct signal S_g and s is a particular value of S (*i.e.* a key candidate). Let $\mathbf{L}^q_{s_g}$ be a random vector containing the side-channel observations generated by the correct key class s_g with q queries to the target cryptographic implementation and $\mathbf{l}^q_{s_g}$ be a realization of this random vector. In practice, we have: $\mathbf{l}^q_{s_g} = [l^1_{s_g}, l^2_{s_g}, \ldots, l^q_{s_g}]$, where each $l^i_{s_g}$ is the side-channel trace corresponding to one given query. We evaluate the amount of information in the side-channel leakages with the conditional entropy:

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = \underset{s_g}{\mathbf{E}} \; \underset{\mathbf{l}^q_{s_g}}{\mathbf{E}} \; -\log_2 \Pr[S = s_g|\mathbf{L}^q_{s_g} = \mathbf{l}^q_{s_g}]$$

From which we derive the mutual information:

$$\mathrm{I}(S_g;\mathbf{L}^q_{s_g}) = \mathrm{H}[S_g] - \mathrm{H}[S_g|\mathbf{L}^q_{s_g}],$$

where $\mathrm{H}[S_g] = \mathbf{E}_{s_g} -\log_2 \Pr[S_g = s_g]$ is the entropy of the key class S_g before any side-channel attack has been applied. In the following, we typically investigate the security of 2-input or 3-input logic gates for which $\mathrm{H}[S_g] = 2$ or $\mathrm{H}[S_g] = 3$.

In order to include the various types of noise that affect the side-channel leakages in our analysis, we assumed that the overall effect of all the noise sources in a side-channel attack can be modeled by a Gaussian distribution. That is, we considered leakages of the form: $\mathbf{l}^q_{s_g} = \mathbf{d}^q_{s_g} + \mathbf{n}^q$, where $\mathbf{d}^q_{s_g}$ is the leakage deterministic part (typically provided by the simulations in the next sections) and $\mathbf{n}^q$ is the normally distributed noise with variance σ_n^2. These definitions can be straightforwardly applied to our different logic styles as follows.

Pre-charged/not masked logic styles: SABL, WDDL, DyCML, LSCML. This is the easiest situation since there is one single leakage trace per secret s_g:

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \int \Pr[\mathbf{l}^q|s_g] \cdot \log_2 \Pr[s_g|\mathbf{l}^q] \; dl,$$

where $\Pr[s_g|\mathbf{l}^q] = \frac{\Pr[\mathbf{l}^q|s_g]\cdot\Pr[s_g]}{\sum_s \Pr[\mathbf{l}^q|s]\cdot\Pr[s]} = \frac{\Pr[\mathbf{l}^q|s_g]}{\sum_s \Pr[\mathbf{l}^q|s]}$. Note that due to the particular structure of our leakages, *i.e.* $\mathbf{l}^q_{s_g} = \mathbf{d}^q_{s_g} + \mathbf{n}^q$, the integral over the leakages is equivalent to an integral over the noise values.

Not pre-charged/not masked logic styles: CMOS. The situation is now slightly more complex. Since there is no systematic pre-charge, each secret s_g can give rise to different leakage traces, corresponding to the different input transitions. If we denote the possible input transitions by a variable T and a particular transition by t, we find:

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \sum_{t} \Pr[t] \int \Pr[\mathbf{l}^q|s_g, t] \cdot \log_2 \Pr[s_g|\mathbf{l}^q] \; dl,$$

where $\Pr[s_g|\mathbf{l}^q] = \frac{\Pr[\mathbf{l}^q|s_g]}{\sum_s \Pr[\mathbf{l}^q|s]}$. Since the input transitions t are known by the adversary, the probability $\Pr[\mathbf{l}^q|s_g]$ can be directly computed as $\Pr[\mathbf{l}^q|s_g, t]$.

Pre-charged/masked logic styles (MDPL). The situation is similar to the previous ones: one single secret s_g can again give rise to different leakage traces, corresponding to the different mask values m. It yields:

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \sum_{m} \Pr[m] \int \Pr[\mathbf{l}^q|s_g, m] \cdot \log_2 \Pr[s_g|\mathbf{l}^q] \; dl,$$

where $\Pr[s_g|\mathbf{l}^q] = \frac{\Pr[\mathbf{l}^q|s_g]}{\sum_s \Pr[\mathbf{l}^q|s]}$. However, contrary to the case of known input transitions, the mask values are *not* known by the adversary. Therefore, we have to compute $\Pr[\mathbf{l}^q|s_g] = \sum_m \Pr[\mathbf{l}^q|s, m] \cdot \Pr[m]$.

Not pre-charged/masked logic styles (GF). This context finally combines a non pre-charged type of gate with known input transitions and unknown masks:

$$\mathrm{H}[S_g|\mathbf{L}^q_{s_g}] = -\sum_{s_g} \Pr[s_g] \sum_{t} \Pr[t] \sum_{m} \Pr[m] \int \Pr[\mathbf{l}^q|s_g, t, m] \cdot \log_2 \Pr[s_g|\mathbf{l}^q] \; dl,$$

where $\qquad \Pr[s_g|\mathbf{l}^q] = \frac{\Pr[\mathbf{l}^q|s_g]}{\sum_s \Pr[\mathbf{l}^q|s]}$,

and $\qquad \Pr[\mathbf{l}^q|s_g] = \Pr[\mathbf{l}^q|s_g, t] = \sum_m \Pr[\mathbf{l}^q|s, t, m] \cdot \Pr[m]$.

Mutual information *vs.* security metric. Before moving to the practical aspects of our analysis, let us finally mention that this paper only considers the information leaked by different logic styles. This is motivated by the fact that the mutual information allows comparing different implementations, independently of the adversary's algorithmic details. Nevertheless, as will be underlined later in the paper, a security metric such as the adversary's success rate would be required if the security of an implementation had to be measured in terms of, *e.g.* number of measurements required to perform a successful attack. The complete evaluation methodology in [18] considers both information and security.

3.3 Side-channel leakage source and simulation environment

As stated in the introduction, one purpose of the present work is to improve the simulation-based security evaluations of side-channel resistant logic styles by the use of good metrics. In order to do so, we investigated transistor level descriptions of different logic styles and extracted the necessary leakages from single gate simulations. Since this level of complexity allows relatively simple descriptions while still giving good insights on the behavior of the different proposed countermeasures, it was a good starting point for the application of our bottom-up security evaluations. The simulations were run on ELDO© [7], an electrical circuit simulator. We used a $0.13\mu m$ Bulk CMOS process thoroughly described in the BSIM3 [4] notice. We simulated the current driven from the power supply during different events of the gates. According to the logic style, the actual part of the power consumption curve was either the one relative to the transition between two different inputs or the one relative to a transition between the evaluation phase and the pre-charge phase. Simulations were run with a 1.2 V power supply and using a time resolution of 10^{-4}ns[1]. Single gates under investigation were driven and loaded by gates in a similar logic style connected to another power node. Finally and as far as possible, our circuit configuration respects the descriptions given in the original papers describing the logic styles (*e.g.* in terms of matched output loads, input rise/fall or arrival time). For each countermeasure, the following functions were simulated, in order to represent a panel of the basic logic blocks needed to build a complete circuit:

- AN2: 2 inputs AND gate
- OR2: 2 inputs OR gate
- EO2: 2 inputs XOR gate
- AN3: 3 inputs AND gate
- OR3: 3 inputs OR gate
- MAJ: majority gate $Z = (B + C)A + BC$

We note that, as also mentioned in the introduction, considering lower abstraction levels (and possibly real measurements) would increase the quality of our analysis. For example, the power consumption behavior of a complex circuit (rather than simple gates) and/or the use of conditions that do not respect the description made in the seminal papers could be considered. This was done in several papers like in [20], where the influence of unmatched output loads and input arrival time was detailed on WDDL and MDPL. Refinements of the simulation models could be similarly developed, including the study of the interconnect, diffusion, routing and/or cross-talk capacitances, as proposed in [25]. Finally, for dynamic and differential logic styles, the influence of transition between data states should also be analyzed as some *history effect* can be the source of additional information leakages. Importantly, the evaluation methodology described in this paper could be similarly applied at *all* abstraction levels (*e.g.* post place-and-route or physical), by just changing the leakage source. This is the main advantage of our proposal compared to previous ad hoc approaches for such evaluations. As already mentioned, simulated gate-level evaluations are only aimed to be the first step in the complete analysis of a logic style.

[1] This time resolution is not intended to model the sampling frequency of an actual adversary but to feed our analyzes with the best possible leakage traces.

3.4 Information extraction: template attacks in principal subspaces

Assuming that our evaluations are provided with simulation-based leakage traces $\mathbf{l}_{s_g}^q$, a practical question remains to properly evaluate the probability density function $\Pr[\mathbf{l}_{s_g}^q|s_g]$ necessary to compute the mutual information. Due to the large dimensionality of the leakage traces, a number of heuristics have been proposed in the open literature in order to reduce the number of leakage samples to tractable values. In this paper, we consider the Principal Component Analysis (PCA) described in [3], of which we now recall the necessary background. For more details, we refer to the original paper. PCA is a standard statistical tool for dimensionality reduction. It looks for a linear transformation T that projects high dimensional data into a low-dimensional subspace while preserving the data variance. PCA usually works in two steps. First, it looks for a rotation of the original axes such that the new coordinate system indicates the successive directions in which the data have maximal variance. Second, it only retains the D most important directions in order to reduce the dimensionality. Note that for practical reasons, a maximum of $(K-1)$ directions can be efficiently computed, where K is the number of key classes targeted in the attack.

Let us assume single query leakage traces l_{s_g} with N_s samples, obtained from our simulation environment. In the following and for each logic style/gate investigated, we first compute the $N_s \times (K-1)$ PCA linear transform T that maps the high-dimensional traces l_{s_g} to $(K-1)$-dimension vectors $l_{s_g}^* = \mathsf{T}(l_{s_g})$. Then, we keep the D highest dimensions of the transformed leakage traces. Note that if each sample of the original trace is affected by an independent Gaussian noise with variance σ_n^2, then each principal direction also is. Consequently, in practice, the main parameters in our security evaluations are:

1. The number of dimensions D kept in the transformed leakages[2].
2. The noise variance σ_n^2 in the leakage samples.

We note that all our following results are meaningful to the extent that the PCA properly extracts and compresses the information from the original leakage traces. On the one hand, this was verified in [3] for practical measurements. On the other hand, the proposed PCA optimizes the inter-classes variance without considering the intra-classes variances. As a consequence, other statistical tools could possibly improve the quality of our conclusions. Again and most importantly, the methodology would be exactly the same (only the evaluation of the probabilities $\Pr[\mathbf{l}_{s_g}^q|s_g]$ would have to be changed). But using the PCA already allows improving the previous (*e.g.* variance-based) evaluation criteria.

[2] Since we only investigate single events of logic gates, the first PCA dimension is largely dominating in our examples. Therefore, the information was usually extracted from 1- or 2-sample transformed leakage traces.

4 Single gates evaluation results

In this section, we first provide the average and standard deviation of the currents supplied to our logic gates, as preliminary results of our simulations. Then, we selected a number of illustrations of our systematic analysis in order to put forward meaningful intuitions on different logic styles and gates.

4.1 Preliminary results

The average and standard deviation of the currents flowing from the power supply node (for the parts of the leakage traces that were used in our analysis) are given in Tables 2 and 3. We first mention that these currents in individual gates barely give an image of the power consumption for complex circuits. For example, DyCML and LSCML have to generate a completion signal to indicate to the next gate stage of the circuit that the inputs are stable and ready. The current generated by this completion signal generation is included in our simulations. By contrast, the currents produced by the clocktree network required for other logic styles was not considered. In general, it is hard to extrapolate the behavior of a complex circuit from its component gates. This is true both in terms of average power consumption and security. Still, we can analyze logic styles at the gate level to put forward theoretical strengths/weaknesses in their design criteria.

Table 2. Average power supply current [μA].

	AN2	OR2	EO2	AN3	OR3	MAJ
CMOS	1.1964	5.7654	6.5587	0.1744	6.5332	2.8254
WDDL	9.6736	9.6736	26.6118	12.5295	12.5295	17.5892
MDPL	17.5892	17.5892	52.6239	35.7938	35.7938	70.4666
DyCML	11.9831	11.9831	11.8661	12.0787	12.0787	11.9373
LSCML	9.3266	9.3266	9.0547	9.3971	9.3971	9.0531
SABL	6.0025	6.0025	6.0033	6.4585	6.4585	7.3581
GF	31.0162	24.4751	5.8440	N.A.	N.A.	N.A.

The results presented in table 2 illustrate that full custom logic styles produce very close average currents across the different logic functions. Other logic styles show more dependencies, depending on the complexity of their internal structures. For example, the Gammel-Fischer logic style has quite complex structures for the AN2 and OR2 gates while the EO2 is much simpler. Similar observations can be drawn from the standard deviation table. If we consider the current standard deviations as an evaluation criteria, it suggests that SABL achieves the best security improvement respectively followed by DyCML, LSCML, WDDL, MDPL, CMOS and GF, for all logic gates but the EO2 gate for which the correct ordering is DyCML, LSCML, MDPL, GF, CMOS and WDDL. We remark that for full custom logic styles, the standard deviations for the EO2 gate are extremely low, due to a very well balanced structure of the gate. Let us finally mention that those values have to be carefully interpreted since the number of curves from which it has been computed varies for the different logic styles (depending

Table 3. Power supply current standard deviation [μA].

	AN2	OR2	EO2	AN3	OR3	MAJ
CMOS	4.1049	3.9061	5.7183	3.1113	2.9890	5.5226
WDDL	0.7933	0.7933	6.7263	1.5183	1.5183	1.1398
MDPL	1.2311	1.2311	1.1257	1.6451	1.6451	2.4790
DyCML	0.1222	0.1222	$8.30\ 10^{-14}$	0.1525	0.1525	0.1928
LSCML	0.1271	0.1271	$6.56\ 10^{-10}$	0.1713	0.1713	0.2061
SABL	$9.64\ 10^{-4}$	$9.64\ 10^{-4}$	0	$2.68\ 10^{-2}$	$2.68\ 10^{-2}$	$1.97\ 10^{-3}$
GF	21.9866	17.7882	5.0805	N.A.	N.A.	N.A.

on the number of gate inputs, mask bits, use of a pre-charge, . . .). Additionally, the existence of non-consuming events (see below) artificially increases the leakage variances. More generally, and as already stated, variance-based criteria are not sufficient for the fair evaluation of side-channel attacks.

4.2 Analysis Results

Figures 2, 4, 5 and 6 (the last ones in Appendix) illustrate the amount of information in the side-channel leakages *vs.* the noise standard deviation, respectively for the AN2, EO2, OR3 and MAJ logic functions. We limited ourselves to these gates since the shapes of the information curves are similar for the couples (AN2-OR2), (AN3-OR3) in all the logic styles (besides CMOS). Indeed, the gate structures are identical (for SABL, DyCML, LSCML and Gammel-Fischer), or use complementary gates (for WDDL and MDPL) and thus generate the same current curves. In the remainder of the section, we pointed out a number of interesting (and intuitive) facts that can be observed from the different figures.

Existence of close and undistinguishable leakages. Undistinguishable leakages typically cause initial values for the information curves below the theoretical expectations. As a typical example, the CMOS AN2 and EO2 gates do not have an initial mutual information of 2 bits. This is caused by the existence of events with identical leakages, namely, the 0 → 0, 1 → 1, 2 → 2 and 3 → 3 input transitions. The same phenomenon occurs for the GF gates, the SABL EO2 gate and for DyCML and LSCML EO2 and MAJ gates. In these examples, certain different inputs lead to identical simulated leakages. Similarly, certain inputs give rise to close leakages. As a result, an increase in the noise level may cause certain inputs to become undistinguishable, which is observed in the figures with the stepped shape of certain information curves.

Full custom designs *vs.* standard cells. For all the logic gates investigated, the information *vs.* noise curve illustrates a much quicker reduction of the information leakages for full custom logic styles than for the standard cell-based ones. Amongst these full custom logic styles, SABL achieves the best result since its internal structure yields a better suppression of the influence of the internal capacitances than the reduced output swing used by DyCML and LSCML.

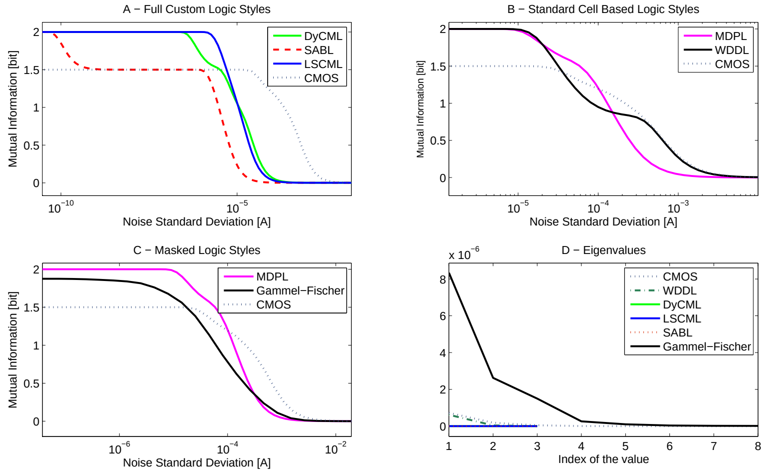
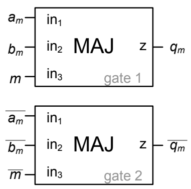


Fig. 2. Information extraction results for the AN2 gate.

Number of masking bits. Our analysis also allows putting forward the different behaviors of masked logic styles, depending on the number of mask bits used in their implementation. Informally, the presence of mask bit(s) in a circuit ideally generates confusion since the same input value to the gates can leak different shapes of power curves depending on the mask values. The more mask bits are used, the more confusion can be expected. For example, MDPL uses a single mask bit to protect the AN2 gate while GF uses two ones. As a result, we could theoretically expect a better resistance of the GF logic style . In fact, looking carefully at the MDPL gates additionally suggests that *at this abstraction level*, the mask does not actually improve the confusion at all.

The cause of this phenomenon is illustrated in figure 3. In this figure, a_m, b_m, $\overline{a_m}, \overline{b_m}$ represent the masked inputs and their complementary values, m and $\overline{m}$ the mask value and its complementary, a and b the unmasked values. Let L_{G1} and L_{G2} stand for the power consumption events relative to the inputs occurring within gates 1 and 2. Let finally L_i, $i = 1, ..., 8$ be the possible values of these events. This figure illustrates that for any possible input of the first majority gate, the second majority gate will generate the complementary event. Therefore, the combined leakage of both majority gates is independent of the mask values. By contrast, for the GF logic, the masking scheme is such that the same input event can indeed leak different information, depending on the mask values. This explains the behavior of these two logic styles in our simulations. Again, let us mention that these observations relate strongly to the abstraction level we consider. As far as MDPL is concerned, the mask is mainly used to get rid of routing constraints in the dual-rails, which cannot be observed from our gate level simulations: it becomes useful when unbalanced dual-rails allow distinguishing complementary events. Note finally that our approach is information theoretic which involves that our adversaries take advantage of all the information in the



a_m	b_m	m	$\overline{a_m}$	$\overline{b_m}$	$\overline{m}$	a	b	L_{g1}	L_{g2}	L_{Tot}
0	0	0	1	1	1	0	0	L1	L8	L1+L8
0	0	1	1	1	0	1	1	L2	L7	L2+L7
0	1	0	1	0	1	0	1	L3	L6	L3+L6
0	1	1	1	0	0	1	0	L4	L5	L4+L5
1	0	0	0	1	1	1	0	L5	L4	L4+L5
1	0	1	0	1	0	0	1	L6	L3	L3+L6
1	1	0	0	0	1	1	1	L7	L2	L2+L7
1	1	1	0	0	0	0	0	L8	L1	L1+L8

Fig. 3. MDPL gate structure for the AN2 function and corresponding event table.

simulation curves: they have access to a perfect leakage model which may not be the case in practice. Additionally, when low noise variances are considered, the simulations allow discriminating most events, which makes the masking a relatively inefficient method, from a theoretical point of view.

Differences between logic gates and size dependencies. These are simple statements. First, the inner structure of certain logic gates *(e.g.* EO2) makes them inherently easier to protect against side-channel attacks, because of a better balanced internal structure. Second, one can observe that our conclusions do not significantly differ when we increase the gate sizes (*e.g.* AN2 *vs.* OR3). On the other hand, moving towards higher circuit complexities is expected to illustrate other facts about the logic styles, as detailed in Section 3.3.

Interpretation of the results. The information plots in this section allow comparing different logic styles in function of the noise level in the observations. For example, Figure 2.B shows that beyond a certain noise threshold, MDPL becomes a better countermeasure than WDDL at the gate level (*i.e.* it provides less information to the adversary). But information plots *do not* tell how much better a countermeasure is in terms of, *e.g.* number of measurements required to perform a successful attack. For these purposes, a security metric such as the adversary's success rate needs to be computed. As detailed in [18], there is no straightforward way to turn the information theoretic metric into a security metric: they quantify different aspects of a side-channel attack. Otherwise said, since the present paper aims to compare different logic styles, the information theoretic evaluation is sufficient. But the security of these logic styles against any given adversary could be similarly investigated, as in [19].

Importantly, these experiments confirm the limitations of the variance-based (and other ad hoc) evaluations of logic styles. In particular, our different figures show that the respective effectiveness of different countermeasures depends on the amount of noise in the observations and therefore cannot be properly explained from simple tables as in Section 4.1. By contrast, it is expected that our information theoretic approach allows analyzing any countermeasure in a unified evaluation methodology. For example, both masked and dual-rail logic styles can be fairly compared thanks to the information theoretic metric[3], although they have opposite impacts on the leakage variances.

[3] If the leakages have been generated in a similar way, which can be a practical issue.

5 Conclusions and open problems

This paper describes an information theoretic evaluation methodology to analyze the effectiveness of side-channel resistant logic styles. It allowed us to put forward a number of meaningful observations about recently proposed countermeasures against such physical attacks. Among the advantages of the proposed approach is the possibility to apply the same metrics and methodology at *all* design stages of a cryptographic device. We considered gate-level simulations as a first step in such evaluations. A practically interesting scope for further research is therefore to extend our analysis to more complex simulation models and to actual measurements. Moving from theory to practice will allow exhibiting additional strengths and weaknesses of the various logic styles and is therefore necessary for their better evaluation and understanding.

Our results exhibit (once again) that no perfect logic style exists to prevent side-channel leakages. They also show that different categories of solutions (*e.g.* full custom *vs.* standard cells) allow reaching different security levels. From a practical point of view, this security has to be traded with the implementation cost of the countermeasures. A central objective of this paper is therefore to allow a good evaluation of this security *vs.* efficiency tradeoff, with fair metrics. We finally suggest the development of a full custom logic style, combining dual-rails, pre-charges and masking as an interesting research direction.

Acknowledgements: The authors would like to thank anonymous CHES reviewers for their interesting comments. Since we could hardly address all of them in the present paper, we refer to [26] for further details on this line of research.

References

1. D. Agrawal, B. Archambeault, J. Rao, P. Rohatgi, *The EM Side-Channel(s)*, in the proceedings of CHES 2002, Lecture Notes in Computer Science, vol 2523, pp 29-45, Redwood City, California, USA, August 2002.
2. M.W. Allam and M.I. Elmasry, *Dynamic Current Mode Logic (DyCML): A New Low-Power High-Performances Logic Styles*, IEEE Journal of Solid State Circuits, vol 36, num 3, pp 550-558, March 2001.
3. C. Archambeau, E. Peeters, F.-X. Standaert, J.-J. Quisquater, *Template Attacks in Principal Subspaces*, in the proceedings of CHES 2006, Lecture Notes in Computer Science, vol 4249, pp. 1–14, Yokohama, Japan, October 2006.
4. Berkley MOSFET Simulation Model, Device Research Group, Department of of Electrical Engineering and Computer Science, University of California, Berkeley, http://www-device.eecs.berkeley.edu/ bsim3/
5. S. Chari, J. Rao, P. Rohatgi, *Template Attacks*, in the proceedings of CHES 2002, Lecture Notes in Computer Science, vol 2523, pp 13-28, CA, USA, August 2002.
6. ECRYPT Network of Excellence in Cryptology, *The Side-Channel Cryptanalysis Lounge* , http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html.
7. http://www.mentor.com/products/eldo
8. J.A. Fournier, S. Moore, H. Li, R.D. Mullins, G.S. Taylor, *Security Evaluation of Asynchronous Circuits*, in the proceedings of CHES 2003, Lecture Notes in Computer Science, vol 2779, pp 137-151, Cologne, Germany, September 2003.

9. W. Fischer, B. M. Gammel, *Masking at the Gate Level in The Presence of Glitches*, in the proceedings of CHES 2005, Lecture Notes in Computer Science, vol 3659, pp 187-200, Edinburgh, Scotland, August 2005.
10. S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, *The Backend Duplication Method: A Leakage-Proof Place-and-Route Strategy for ASICs*, in the proceedings of CHES 2005, LNCS, vol 3659, pp 383-397, Edinburgh, UK, Sept. 2005.
11. I. Hassoune, F. Macé, D. Flandre, J.-D. Legat, *Low-swing current mode logic (LSCML): a new logic style for secure smart cards against power analysis attacks*, in Microelectronics Journal, vol 37, num 9, pp 997-1006, Elsevier, September 2006.
12. P. Kocher, *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS and Other Systems*, in the proceedings of Crypto 1996, Lecture Notes in Computer Science, vol 1109, pp 104-113, Santa Barbara, California, USA, August 1996.
13. P. Kocher, J. Jaffe, B. Jun, *Differential Power Analysis*, in the proceedings of Crypto 1999, LNCS, vol 1666, pp 398-412, Santa-Barbara, USA, August 1999.
14. H. Li, T. Markettos, S. Moore, *Security Evaluation Against Electromagnetic Analysis at Design Time*, in the proceedings of CHES 2005, Lecture Notes in Computer Science, vol 3659, pp 280-292, Edinburgh, Scotland, August 2005.
15. F. Macé, F.-X. Standaert, I. Hassoune, J.-D. Legat, J.-J. Quisquater, *A Dynamic Current Mode Logic to Counteract Power Analysis Attacks*, in the Proceedings DCIS 2004, pp 186-191, Bordeaux France, November 2004.
16. S. Mangard, T. Popp, B. Gammel, *Side-Channel Leakage of Masked CMOS Gates*, in the proceedings of CT-RSA 2005, Lecture Notes in Computer Science, vol 3376, pp 351-365, San Fransisco, USA, 2005.
17. T. Popp, S. Mangard, *Masked Dual-Rail Pre-Charge Logic: DPA-Resistance Without Routing Constraints*, in the proceedings of CHES 2005, Lecture Notes in Computer Science, vol 3659, pp 172-186, Edinburgh, Scotland, August 2005.
18. F.-X. Standaert, T.G. Malkin, M. Yung, *A Formal Practice-Oriented Model for the Analysis of Side-Channel Attacks*, Cryptology ePrint Archive, Report 2006/139, 2006, http://eprint.iacr.org.
19. F.-X. Standaert, E. Peeters, C. Archambeau, J.-J. Quisquater, *Towards Security Limits in Side-Channel Attacks*, in the proceedings of CHES 2006, Lecture Notes in Computer Science, vol 4249, pp. 30–45, Yokohama, Japan, October 2006.
20. D. Suzuki, M. Seaki, *Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-Charge Logic Style*, in the proceedings of CHES 2006, Lecture Notes in Computer Sciences, vol. 4249, pp 255-269, Yokohama, Japan, October 2006
21. K. Tiri, M. Akmal, I. Verbauwhede, *Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand DPA on Smart Cards*, in the proceedings of ESSCIRC 2002, pp 403-406, Florence, Italy, September 2002.
22. K. Tiri, I. Verbauwhede, *A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation*, in the proceedings of DATE 04, vol 1, pp 10246 - 10251, Paris, France, February 2004.
23. K. Tiri, I. Verbauwhede, *Place and Route for Secure Standard Cell Design*, in the proceedings of CARDIS 2004, pp 143-158, Kluwer, August 2004.
24. K. Tiri, I. Verbauwhede, *Design Method for Constant Power Consumption of Differential Logic Circuits*, in the proceedings of DATE 2005, pp 628-633.
25. K. Tiri, I. Verbauwhede, *Simulation Models for Side-Channel Information Leaks*, in the proceedings of DAC 05, pp 228-233, San Diego, CA, USA, June 2005.
26. UCL Crypto Group, *Theoretical Models for Side-Channel Attacks*, home page and FAQs: http://www.dice.ucl.ac.be/ fstandae/tsca

A Figures

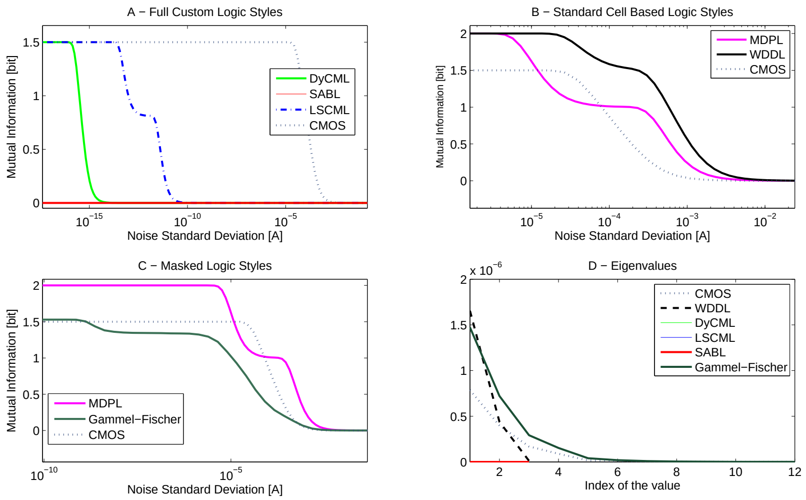


Fig. 4. Information extraction results for the XOR2 gate.

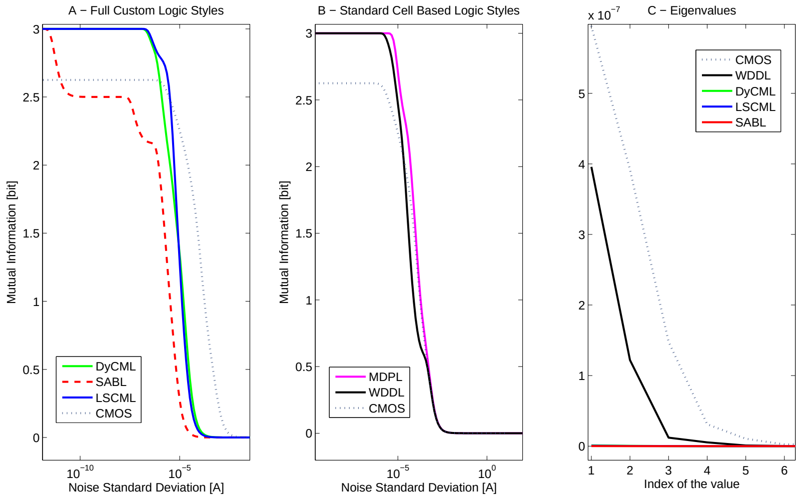


Fig. 5. Information extraction results for the OR3 gate.

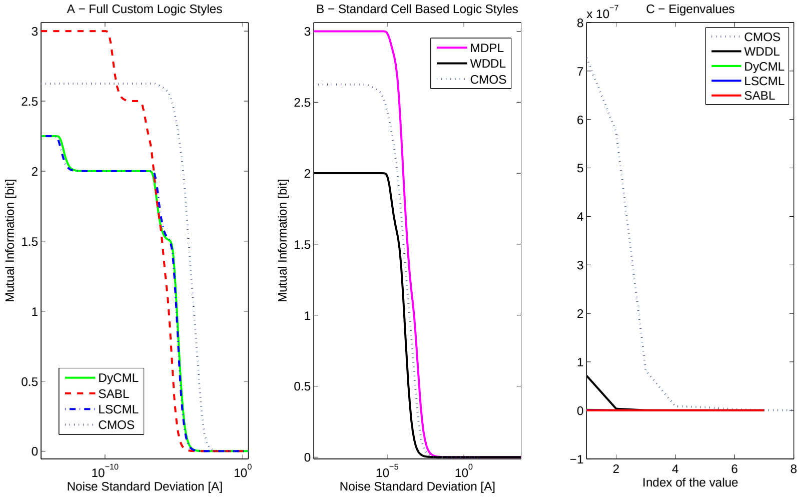


Fig. 6. Information Extraction Results for the MAJ gate