Optically Induced Static Power in Combinational Logic: Vulnerabilities and Countermeasures

Jan Bělohoubek*, Petr Fišer, Jan Schmidt

Faculty of Information Technology, Czech Technical University in Prague, Thákurova 9, Prague, Czech Republic

Abstract

Physical attacks, namely invasive, observation, and combined, represent a great challenge for today's digital design. Successful class of strategies adopted by industry, allowing hiding data dependency of the side channel emissions in CMOS is based on balancing. Although attacks on CMOS dynamic power represent a class of state-of-the-art attacks, vulnerabilities exploiting data dependency in CMOS static power and light-modulated static power were recently presented. In this paper, we describe structures and techniques developed to enhance and balance the power imprint of the traditional static CMOS bulk structures under invasive light attack.

The novel standard cells designed according to the presented techniques in the TSMC180nm technology node were used to synthesize the dual-rail AES SBOX block. The behavior of the AES SBOX block composed of the novel cells is compared to classical approaches. Usage of novel cells enhances circuit security under invasive light attack while preserving comparable circuit resistance against state-of-the-art power attacks.

Keywords: standard CMOS cell; custom CMOS cell; SPICE; AES SBOX; design for security; dual-rail; SecLib

1. Introduction

Physical attacks – invasive [1], observation [2], or combined [3] represent a great challenge for today's digital design [4] since their introduction in late 1990s. The secret stored in devices with loose physical security – such as smart-cards or constrained long-mission IoT devices deployed in the field – is endangered [5, 4]. The compromised secret may lead to a wide range of damages, including loss of credit, financial, material, or even health damages.

A successful class of strategies adopted by industry, allowing hiding data dependency of the side channel emissions in CMOS (*Complementary Metal Oxide Semiconductor*), is based on balancing. Many techniques employing dynamic behavior balancing (often based on dual-rail logic encoding [6]) were developed. An example of such a successful technique employing dual-rail complementary encoding is the conventional WDDL (*Wave Dynamic Differential Logic*) [7].

Although static side-channel emissions are less significant compared to dynamic emissions, the recent research has shown that, at least in theory, exploiting data dependency in CMOS bulk *static* power/leakage is possible [8, 9, 10, 11].

The light attacks, and in particular laser attacks, represent a diverse group of approaches allowing to compromise even a secured CMOS circuit. The mainstream of laser attack methods is represented by fault injection techniques [1]. Our contribution to the class of light attacks is non-conventional, as it is connected with combinational logic. In [12], we described how the light-modulated static power of a small combinational circuit, namely the conventional voter, may be used to retrieve processed data, and in [13], we described the data dependency of different CMOS structures under illumination and one possible attack scenario. We have also found that simple dynamic power balancing approaches do not represent the right solution to this vulnerability and most of today's circuits are potentially vulnerable.

The great advantage of the light attacks on combinational logic is that no permanent fault is introduced into the device. Thus, fault-detection or intrusion detection mechanisms used as countermeasures may be overcome [1].

In this article, we describe and evaluate novel techniques and CMOS structures designed to increase the attack resistance considering light attacks targeted on *combinational parts* of CMOS circuits. Specifically, the power imprint of the illuminated circuit – sequential or purely combinational blocks – may reveal the (register) values feeding the combinational parts. We present novel AND and OR standard cells using the presented techniques. These designed cells are used to synthesize a protected implementation of AES SBOX and we compare the vulnerability of the circuit to traditional approaches.

To preserve the consistency of the article, we recall the novel CMOS structures and techniques developed to

*Corresponding author

Email addresses: jan.belohoubek@fit.cvut.cz (Jan Bělohoubek), petr.fiser@fit.cvut.cz (Petr Fišer), jan.schmidt@fit.cvut.cz (Jan Schmidt)

enhance and balance traditional static bulk CMOS structures from the perspective of the light-modulated static power and leakage first described in [14]. Competing and traditional CMOS structures are also described and compared to the proposed approach.

In our previous work [14], we provided only an overview of design technique candidates. In this article, we provide a deeper analysis of SecLib gates, where we identified a novel vulnerability, while we recall the principal description of each design technique candidate to retain completeness of the list of related techniques.

The proposed structures increase the circuit resistance to attacks on the CMOS static power and have an acceptable impact on delay, area, and power consumption.

The evaluation method we use throughout this article is the SPICE simulation of illuminated transistor structures. The models of transistors under illumination originally presented by Sarafianos et al. [15, 16, 17] were qualified for publicly available TSMC180nm technology node [12]. The TSMC180nm technology advantage is the availability of the open standard cell library provided by Oklahoma State University (OSU) [18] and available transistor SPICE models [19]. The simulation is performed in *ngSPICE* [20]. The simulated structures are SPICE netlists extracted from TSMC180nm layouts. The results are based on publicly available TSMC180nm SPICE models extended by the mentioned models by Sarafianos et al. The simulated CMOS devices are illuminated by a constant light source with energy density equivalent to the laser beam focused to a fixed area with power ranging between 0 and 600mW. The 1.8V supply voltage is used. The models, simulation data, and additional simulation results including evaluation of manufacturing variances or supply voltage are available online [21].

This article represents the contribution in the following topics:

- we describe the novel SecLib vulnerability,
- we recall and contextualize the principles of the secure cell design introduced in [14],
- we present design rules for protected CMOS cells,
- we describe novel protected cells extending the standard TSMC180nm library,
- we examine the impact of protected standard cells to the variability of the data-dependent photocurrent decreasing the vulnerability of the implemented combinational crypto block (AES SBOX).

In Section 2, we summarize our recent research related to attacks exploiting light-modulated static power. In Section 3, we describe the related work and design methods decreasing circuit vulnerability as a side effect including our approach presented in [14]. In Section 4, we formulate design rules for the standard CMOS cell design process and we present new protected standard cells in the TSMC180nm library. A comparison with conventional and competing approaches is presented. The protected gates were carefully evaluated and simulation results demonstrating the proposed cells benefits in a large combinational circuit are provided in Section 5.3. The presented approaches and results are discussed in Section 6.

2. CMOS Structures and Data-Dependent Power Consumption

CMOS processes are used for manufacturing of the majority of today VLSI (*Very Large-Scale Integration*) digital logic designs [22], as CMOS provides low leakage power. Additionally, most of today's designs are static CMOS. Although the leakage is low in standard CMOS designs, there is still a dependency between the gate leakage and processed data (values at gate inputs) [22]. E.g., in [8, 9] it is demonstrated that leakage can be used to mount an implementation attack.

The dependency between the single gate or subcircuit input patterns and static power is typically hidden in a *cocktail* of thousands of gates composing the digital circuit, making such an attack more challenging compared to attacks mounted on dynamic power. However, as it has been shown, the static power data dependency may be manifested by using a focused laser beam [12, 13, 14]. The illumination may increase the order of magnitude of the data-dependent static current of the specific circuit part by a factor 4–5: leakage currents are in the order of (tens of) nanoamps, but the data-dependent part of the static *Optical Beam Induced Current* (OBIC) [15] may be in tens or even in hundreds of microamps for a single logic gate. The data-dependency amplification depends on the CMOS technology node and the *exposure energy* (illumination energy/laser power).

A potential inconvenience connected with any practical static power monitoring attack is that the attacker needs to monitor the static component of the circuit power. The need for static component monitoring requires precise synchronization with the device-under-attack. The measurement setup may also require underclocking or even temporarily stopping the target. The difficulty of the clock manipulation is given by the circuit architecture, its knowledge, and also by the CMOS technology node.

A significant advantage of the OBIC monitoring over conventional leakage monitoring approaches is that OBIC is induced only in the illuminated area. By focusing the light source, it is possible to induce the data-dependent current in a defined area-of-interest only. The focusing may decrease the complexity of the attack on static power significantly, as the number of *cocktail ingredients* decreases significantly. This fact may be potentially exploited to mount a more powerful attack.

The induced data-dependent OBIC imprints into VDD and GND rail currents where it can be monitored. We call the data-dependent part of OBIC imprinted into the rail

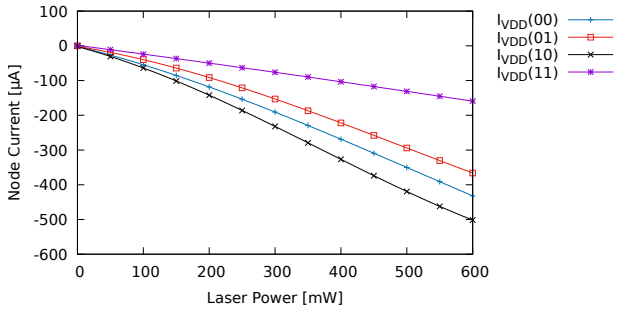


Figure 1: The simulated power imprint for two-input NAND gate (NAND2X1 standard cell) in TSMC180nm technology library; data-dependent patterns may be observed also for other basic standard cells

current the *power imprint*. In this article, the simulated power imprints are always related to the VDD rail.

For higher exposure energy, the illumination time must be short, to avoid CMOS destruction. Only for low exposure energies, the illumination might be continuous. Following the related works [1, 15, 23], the simulated power represents OBIC of a pulsed nature – the simulated currents represent a peak, not a continuous current.

The power imprint can be potentially used to compromise the integrated circuit, as it embeds information about processed data. In our recent work [13, 14], we identified that the data dependency is significant. This fact is demonstrated by standard cell *power imprints* in the TSMC180nm technology node in Figure 1. The power imprint, in general, allows distinguishing (some of) the Hamming weights of the inputs. This fact may be potentially used to compromise even a bigger CMOS circuit, as the differences are significant and even "cocktails" of power imprints composed from contributions of many gates are data-dependent [13].

The state-of-the-art side-channel attacks employ statistical methods to exploit the data-dependency contained in the side channel emissions of the circuit [2, 24]. This article deals with the data-dependent power imprint of CMOS induced by illumination. Using OBIC for side-channel analysis brings several advantages, as described above, however, direct reading of processed bits might be possible in a special (and probably rare) case, and with sophisticated equipment only. In most cases, statistics should be employed – as for any conventional side-channel observation or combined attack.

2.1. Attacker Model

To compromise the circuit by a combination of CMOS illumination and static power consumption monitoring, the attacker must be able to decapsulate the circuit, while preserving it operational. This is possible with basic equipment [25, 26]. Next, this attacker must be able to synchronize the light source and the measurement equipment. Additionally, if the attacker can control the clock signal, it is a plus simplifying the attack.

Aligned with our previous work [12, 13, 14], we assume that attackers considering light attacks on combinational logic would be of two kinds. We distinguish (i) *a sophisticated attacker* who has access to sophisticated equipment capable of targeted attacks to a small circuit area, who has constant power light source with the ability to perform repeatable experiments including short, area-constrained light pulses (e.g. sophisticated laser bench) and then (ii) *a mid-equipped attacker* with cheaper equipment allowing simpler attacks targeted to larger circuit areas, e.g., a poorly focused light source with limited repeatability, especially for short pulses. Both scenarios are possible, even if somehow challenging. The possibility of targeting an attack even to a very constrained circuit area by a laser beam is proven [1, 15, 16, 17, 23].

2.2. Attacks on OBIC

Based on the attacker abilities, we distinguish two attack scenarios:

2.2.1. Precisely-Targeted Attack

The sophisticated attacker can perform an attack *precisely targeted* to few standard cells, small CMOS structures, or even to a single CMOS cell area only.

If the attacker can determine the location of the cell or a small CMOS structure of interest and he can illuminate predominantly only the structure of interest, he may directly read the value at the moment present at the structure inputs. E.g., in [12], we have shown that conventional TMR voters represent significantly vulnerable structures. If a conventional 3-input voter operates in a fault-free environment, its inputs are equal. Then, the overall voter structure is driven by three equal inputs and works as an amplifier when illuminated: the difference between `000` and `111` inputs in the current induced by illumination is significant. Additionally, the area of several standard cells forming a voter circuit may be targeted simpler than the area of a single cell. This might be possible even in advanced technology nodes, where the voter area approaches the order of micrometers.

2.2.2. Block-Targeted Attack

The *mid-equipped attacker* can only target a wider circuit area (e.g. a block) and can use limited illumination energy only. The illumination of the combinational logic block can be used to highlight its data-dependent power in the power trace of the device.

For the *Block-Targeted Attack* or *Precisely Targeted Attack* with complex power imprint cocktails, we consider a statistical method following the well-known *Correlation Power Analysis attack* (CPA) procedure from [24]. The difference from a standard CPA attack is in the power model only. Conventional CPA attacks use simple models like Hamming Distance (HD) or Hamming Weight (HW) of the data, but the attack exploiting OBIC needs a more precise power model.

Simple models are unable to characterize the OBIC of the CMOS logic well enough. Ideally, the power model should be created by SPICE simulation of the target structure under all input vectors. Our SPICE models can be used even for similar bulk CMOS technologies.

As an alternative to SPICE simulation, a template-based model [27] may be used analogously to the simulation in case of both *Precisely-Targeted* and *Block-Targeted* attacks.

2.3. Simplified Power Model of Complex Structures

The attacks exploiting OBIC require a relatively precise power model. In the case of the *Block-Targeted* attack, exhaustive simulation of bigger CMOS circuits might be required. To further ease the attack, a simplified composite power model can be used.

The simplified power model does not require electrical simulation of large circuits. From the attacker's point of view, simpler approaches employing open tools only potentially reduce the attack cost.

The simplified power model for a given circuit is a *tuple* containing the OBIC for each circuit input vector. To construct this power model, only standard cells (single gates) must be pre-simulated in SPICE (or characterized another way). Their responses are then placed in the *tuple* P, and are used in connection with the knowledge of the circuit configurations under all given input vectors to *compose* the complete power model. The circuit configuration extraction under the given input vector is a straightforward task[1] producing the *tuple* N. The power model for a given input vector is the sum of data-dependent OBICs of all standard cells (pre-simulated in SPICE) in the given circuit configuration. As a result, only the standard cells used in the circuit are to be simulated in SPICE, instead of the whole circuit.

The circuit configuration for a given input vector can be described by the following *tuple*:

$$N = \{g_0(00), g_0(01), g_0(10), g_0(11), \ \ldots \\ \ldots \ g_{n-1}(10), g_{n-1}(11)\}, \tag{1}$$

where the respective g_i's represent the numbers of gates in the respective configuration, and n represents the number of gate types used in the circuit. The pre-simulated power for each gate in the circuit is organized in the following *tuple*:

$$P = \{p_0(00), p_0(01), p_0(10), p_0(11), \ \ldots \\ \ldots \ p_{n-1}(10), p_{n-1}(11)\}, \tag{2}$$

where the respective p_i's represent the pre-simulated power for the respective gates in the given configuration.

[1] Circuit configuration extraction is provided by input vector simulation in the TSaCt2 framework [28]

The power model for the j-th circuit input vector is given by the following sum:

$$m_j = \sum_{i \in [0, n-1]} p_i \cdot g_i, \tag{3}$$

while the complete power model for the circuit is a *k-tuple*, a lookup table, composed of power models for every circuit input:

$$M = \{m_0, \ldots m_{2^k-1}\}, \tag{4}$$

where k is the number of circuit inputs.

To illustrate the power model generation, we use the AES SBOX circuit composed of 866 2-input NAND gates only ($n = 1$) as an example. The SBOX circuit has 8 inputs ($k = 8$). Figure 2 shows the resulting power model for all 256 distinct circuit configurations related to 256 different circuit input vectors.

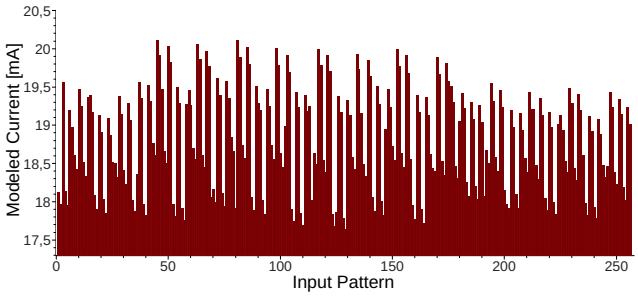


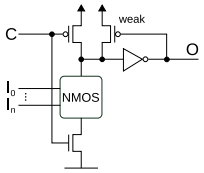
Figure 2: Simplified power model of the example AES SBOX circuit composed of 866 NAND gates illuminated by 50mW of the equivalent power – the power model is related exclusively to the *time of illumination* – the attacker's point-of-interest

The advantage of the look-up table-based approach is that it can be mount on a bigger circuit without the need for time-intensive simulation or templating and only a standard cell characterization is required. Its disadvantage is that it becomes less accurate with rising illumination power, as higher illumination powers cause voltage drops in the circuit, affecting the induced currents – the simple look-up table reflects reality less accurately [13].

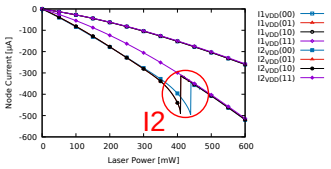
3. Related Work

This work presents methods to construct circuits that are resistant to leakage attacks even if the leakage is amplified by illumination – the data-dependent *Optical Beam Induced Current* (OBIC) is significantly higher than the leakage. Therefore, we also review existing design methods that provide a notable level of data-independence in this section.

The design techniques providing significant level of data-independence include namely dynamic logic, where PMOS stack is reduced to a single transistor [22], and methods employing SecLib gates [29, 30]. Their relevance was first



(a) Footed domino logic gate employing standard *weak keeper*



(b) Domino logic two-input AND gate without keeper (I1) and with the standard weak-keeper (I2) power imprints

Figure 3: Domino logic gate structure and power imprint example

identified in [14]. In this article, we provide a deeper analysis of SecLib gates, where we identified a new vulnerability.

3.1. Domino Logic Employing Single Precharge PMOS

We identified the dynamic logic circuit design styles as promising, as they limit the data dependency in the PMOS stack by replacing the stack with a data-independent precharge transistor.

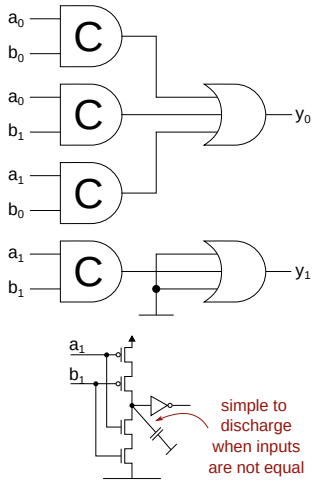
The structure of conventional dynamic (domino) gates provides natural masking. The masking is given by the *charge leakage* [22], as the precharged internal node in the domino gate tends to discharge fast even for small illumination energy, leading to a (almost) constant state of the gate under any input pattern – see I1 in Figure 3b. In dynamic logic, the charge leakage is often compensated by a *weak keeper* [22] – see Figure 3a. The domino gate with a weak keeper has commonly a data-dependent power imprint with a notable drop in the current characteristics at the characteristic illumination energy which is able to change the output of the gate – see I2 in Figure 3b. Fortunately, by altering the sizes of the weak keeper and the output inverter, the data-dependency may be decreased significantly.

3.2. Symmetric SecLib Gates

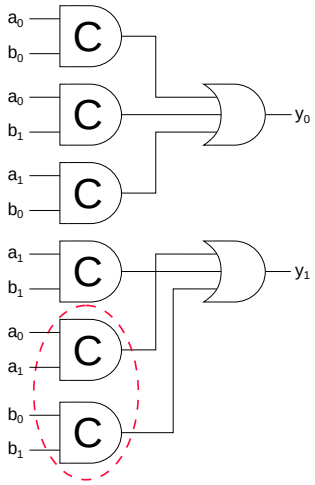
One of the known approaches employing classical static CMOS with increased symmetry – at both schematic and layout levels – is called SecLib. The symmetry is achieved by following the SecLib gate design guidelines described in [29, 30]. The original SecLib dual-rail AND gate is shown in Figure 4a.

Originally, we assumed that the perfect SecLib symmetry leads to perfect balancing, however, we discovered a hidden asymmetry in the area-efficient SecLib version.

If the SecLib gate is designed to be area-efficient, it should employ *dynamic C-elements*. Unfortunately, dynamic C-elements suffer from *charge leakage* [22] if C-element inputs are not equal. Charge leakage in combination with circuit illumination (even for small energies) turns the C-element output to `1`. This uncovers a hidden asymmetry in SecLib: the second OR gate is fed by one C-element only, while two other inputs are grounded and the grounded inputs are not affected by the charge leakage.

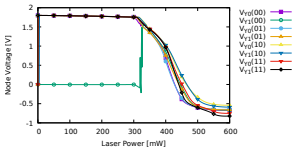


(a) Original SecLib gate and the dynamic C-element structure

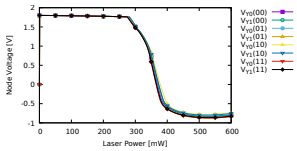


(b) Optimized gate providing better OBIC balancing and consistent output

Figure 4: Secured 2-input AND gate schematics: all input combinations at C-element inputs are represented; if not illuminated, one C-element output is always equal to 1 and remaining C-element outputs are always equal to 0



(a) SecLib

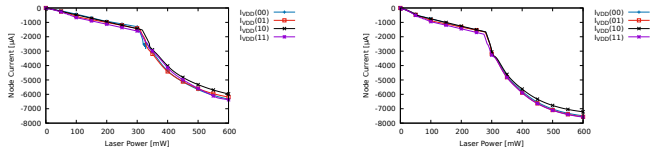


(b) Optimized SecLib

Figure 5: Output voltages for SecLib and the optimized SecLib

In most cases, both outputs of the SecLib gate under illumination are `1`, as the charge leakage causes at least one input of both ORs to be `1` – the C-element parasitic capacitance shown in Figure 4a is discharged when C-element inputs are not equal. However, when the input of the dual-rail SecLib gate is `00` ($a_1 = 0$, $b_1 = 0$, $a_0 = 1$ and $b_0 = 1$), the bottom C-element does not experience charge leakage, as both of its inputs match and it produces output equal to `0`. The other inputs of the lower OR gate are also `0`, thus the OR gate output is `0`, not `1`. This allows distinguishing the `00` input of the SecLib gate – the gate experiences a data-dependency: the voltage output is data-dependent and subsequently also the power imprint is imbalanced. The output data-dependency is shown in Figure 5a. The lower OR gate switches its output when the illumination power is high enough to cause the C-element to change its output – see Figure 5a – the input pattern is masked for high energy only.

Although we identified this vulnerability in connection with OBIC, it can arise in different contexts as well and it enables fault-attacks in general. In a different context, it might be less obvious but it is still present. The output of the dynamic C-element depends on the charge



(a) SecLib (b) Optimized SecLib

Figure 6: Induced photocurrents for SecLib and the optimized SecLib

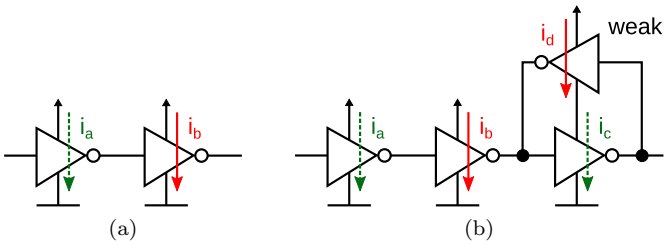
stored in the parasitic capacitance – see Figure 4a. Even a small increase in subthreshold leakage caused, e.g., by temperature, may have a similar effect [22] leading to data-dependent fault injections. Also the traditional fault-injection techniques [1] targeted at the secLib gate area will cause that the secLib gate output for the 00 input pattern will be different than the output of other input patters. This is a principal vulnerability that can be exploited in a fault-attack or a combined-attack [1]. As a result, the secLib structure employing dynamic C-elements should be considered vulnerable in general.

A possible solution to the problem with SecLib asymmetry is shown in Figure 4b: two additional C-elements producing constant 0 are added. These C-elements *are* prone to charge leakage, as their inputs during the dual-rail evaluation phase do not match. It is possible to omit one of the added C-elements and still obtain a data-independent output and subsequently also increased balance in power imprint for photocurrent, as shown in Figures 5b and 6b respectively. On the other hand, by omitting one of the C-elements, the SecLib gate becomes unbalanced from the dynamic power perspective: loads of all input signals will not be equal. Thus, using both C-elements is recommended.

Note that even SecLib optimized by added C-element(s) experiences a power imprint imbalance – see Figure 6. The remaining imbalances are given mostly by asymmetries in the serial CMOS transistor stacks.

To further decrease the power imprint data dependency of SecLib, mainly the asymmetries connected with signal ordering in the serially arranged transistor stacks should be removed. The parallel arrangement of duplicated CMOS stacks with permuted inputs would lead to further suppression of the data dependency, for a price of further increase of the SecLib gate area.

Both domino logic and SecLib share a nice property: they were designed to support dual-rail encoding computation, thus (if employed in a dual-rail circuit) provide (at least) a basic level of dynamic power attack resistance. On the other hand, they suffer from significant disadvantages. SecLib suffers mainly from a large gate size. The increased gate size influences not only the circuit static power or delay, but also the circuit security [13]. On the other hand, domino logic provides a small area footprint, but it suffers from general dynamic logic disadvantages including the need for careful clocking or increased dynamic power [22].



(a) (b)

Figure 7: Two-inverter chain (a) uses complementary power consumption to obtain a constant power imprint: $i_a + i_b = const.$; three-inverter chain with feedback weak inverter (b) uses the same principle

3.3. Structures Enabling Static CMOS Current Balancing

Compared to the dynamic logic and domino logic in particular, we proposed compact static CMOS structures [14] that counter the attack by balancing and may complement SecLib as a countermeasure against attacks on light-modulated static power, first described in [12, 13].

We have shown that the circuit vulnerability connected with the light-induced static current (OBIC) may be compensated only when – in the case of the illumination attack – the entire balanced structure is exposed to the same light intensity [12]. This natural requirement may not be guaranteed for bigger structures: for larger exposure areas, a precise attack employing disbalancing becomes feasible. The size of the balanced CMOS gate is extremely important.

In the following paragraphs, we recall the approaches proposed in [14], which we turn into standard cell design rules in Section 4. The proposed approaches are used to balance traditional CMOS gates and to decrease data dependency between leakage or OBIC and gate input patterns. The severity of OBIC data-dependency is more significant, and thus the emphasis is on breaking OBIC data-dependency. The approaches employing inverter balancing and the proposed transistor-level modifications are – according to the best of our knowledge – novel in the security context.

3.3.1. Inverter Balancing

The first approach originates in the fact that two equally sized cascaded inverters work with complementary values, and thus may provide a constant (mutually balanced) power imprint. It is simple to balance a two-inverter chain resulting in a buffer with constant static power imprint – see Figure 7a. Note that the equally sized inverters working with complementary input values at the same time provide both illumination-induced power imprint and leakage balancing. An inverter chain containing an odd number of inverters may be balanced by altering inverter sizes or by employing a feedback inverter – see Figure 7b [14].

Note that the output inverter may also be used for (at least partial) balancing of the power consumption of arbitrary negative CMOS structures – such as NAND or NOR

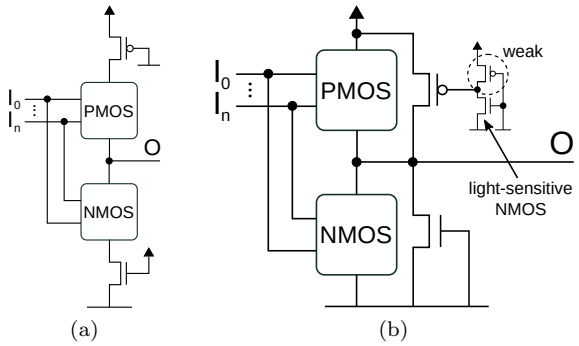


Figure 8: Serial transistors (a) are employed to increase the gate symmetry and allow to disconnect power rails; and the parallel transistors (b) are used to decrease the share of the data-dependent component of the photocurrent

gates in particular. This is the reason why static CMOS positive gates (e.g. AND, OR) provide a limited intrinsic level of balancing, overcoming the negative gates. We found that it is relatively simple to enhance the balancing efficiency by an output inverter scaling, which provides an opportunity to increase the circuit attack resistance by a small modification of existing positive gates, namely in circuits employing only positive gates (e.g. dual-rail circuits).

In general, any approach employing positive gates, where the output inverter is comparable to the negative part of the gate provides an intrinsic balancing. It is also the reason why the mentioned domino logic provides a good level of power compensation by design.

3.3.2. Adding Serial Transistor

Another approach increasing symmetry of the CMOS gate NMOS/PMOS stacks is shown in Figure 8a. A single – normally closed – transistor with constrained channel width is added in series with the NMOS or PMOS part of the circuit. It converts the parallel arrangement of the PMOS or NMOS block to quasi-serial with decreased data dependency conditioned by the ability of the serial transistor to limit the current. Although it is normally closed, it effectively reduces the OBIC in case of higher illumination power.

3.3.3. Adding Light-Sensitive Parallel Transistor

The other approach decreasing data-dependency is shown in Figure 8b. The parallel connection of normally open PMOS and NMOS transistors to PMOS and NMOS stacks has no significant effect in the case of normal operation (except for the increased leakage), however, they increase the share of the data-independent current in case of light attack (a significant current-generating PN junction area is provided).

We have noticed that NMOSes themselves can be efficiently used as light sensors (for higher illumination intensity), as their conductivity under illumination grows rapidly. The NMOS parallel transistor control can thus be realized only by grounding its gate. On the other hand, the PMOS requires control by a dedicated light sensor.

Our simple light sensor is an ordinary CMOS inverter, whose light-sensitivity is increased by strengthening its NMOS part and weakening its PMOS part – see Figure 8b. This arrangement ensures that the light sensor is easy to integrate into a CMOS cell, it requires no additional process tuning, and has a very small footprint.

The resulting geometry employing parallel transistors decreases the significance of the data-dependent component of the power imprint related to PMOS and NMOS blocks under illumination.

3.3.4. Disconnecting Rail

The final approach is shown in Figure 9. When the CMOS circuit is under attack, disconnecting one or both of the rails feeding the NMOS and PMOS parts decreases the data dependency significantly. The same light-sensitive inverter is a source of the first control signal (`C1`) – the first control signal may be employed for parallel PMOS control and to disconnect the VSS rail, however, one additional inverter is required to generate the second control signal (`C2`) to disconnect the VDD rail.

Connecting the second inverter to the light sensors makes two control signals accessible in the CMOS cell. These two signals can be used to control all additional serial and parallel transistors in the cell, thus gates of all transistors can be controlled by the single light sensor, not by multiple independent transistors with grounded gates. The resulting behavior of the cell is then more deterministic.

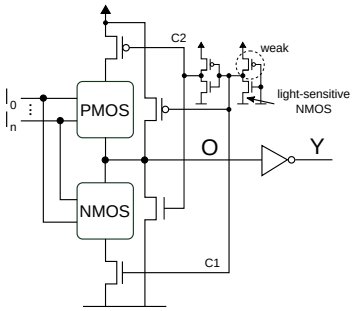


Figure 9: Completely balanced positive gate: the output inverter serves for power balancing and as the output voltage filter at the same time

The careful design of the secured cell also includes the output voltage to be without significant variations and far from the *intermediate voltage* region. The output inverter serves as a voltage filter separating the internal node Y suffering from voltage drops and variations, which can fall into *intermediate voltage* level. In the case of the previously described approaches are used, the internal node voltage is strongly influenced by the added balancing logic and the importance of the inverter as a voltage filter is increased.

The output inverter, in the case of our method, also provides balancing, as described in Section 3.3.1.

In [14], we proposed the use of the established transistor stack symmetrization technique based on transistor stack duplication and input permutation [30], however, the research presented in this article has shown that the negative impact on the cell area causes that the utilization of this technique is problematical.

4. Proposed Standard Cells

Conventional CMOS design utilizes standard building blocks called *standard cells* – see Figure 10. The cells are carefully designed to optimize the circuit area and performance. In this section, we propose standard cell design rules with an additional dimension in mind: a constant power imprint under illumination for enhanced security.

During our experiments with the TSMC180nm technology standard cell library, we carefully iterated through the design space to find out an optimal design for enhanced standard cell security. We followed the principles described in Section 3.3, and we formulated design rules for our method. Some of the rules extend the original proposals presented in [14]. The rules can be used to design custom cells according to our method:

1. the light-sensitive inverter N-channel width approaches the allowed maximum for the given standard cell height and the width of the P-channel approaches the minimum;
2. the control inverter connected to the output of the light-sensitive one is designed with opposite channels widths;
3. serial transistors are used to disconnect only the functional PMOS and NMOS part of the CMOS cell, not to disconnect parallel transistors;
4. parallel transistors are connected directly between the internal node and `GND` or `VDD` respectively;
5. the size of transistors controlled by the gate inputs is as small as possible (the size requirement may collide with the transistors symmetrization proposed in [14], as the symmetrization increases the minimal area of the transistor stack);
6. the output inverter is optimized to balance the power imprint for lower light energies only, while its size ensures low light-sensitivity and acceptable load capacity for normal circuit operation;

By applying the proposed rules in the TSMC180nm, we designed two complementary standard cells – see Figure 10d and 10e. Their layouts correspond to the schematic presented in Figure 9. The proposed layouts follow the MOSIS SCMOS rules and passed all DRC checks provided by Magic. The cells employ all approaches described in Section 3.3. The cells extend the OSU TSMC180nm cell library and are compatible with other library cells. The proposed cells were optimized according to SPICE models reflecting the data-dependent behavior of the CMOS under illumination.

Rule 1 allows to increase the sensitivity of the light sensor and increases the falling edge slope of the first control signal and Rule 2 helps to increase the rising edge slope of the second control signal (Figure 11c).

Rules 3 – 6 represent a *Divide-and-Conquer* approach and make the overall CMOS structure more robust and easier to optimize: the parallel transistors are open for lower illumination intensities (laser powers), thus the voltage in node `O` (Figure 9) is given by the configuration of PMOS and NMOS blocks, while the overall structure balancing is provided by parallel transistors and the output inverter. The inverter balancing is relatively easy for lower illumination intensity.

For higher illumination intensity, the NMOS and PMOS parts are completely disconnected, while the parallel transistors are closed bringing the structure into a *short* – this fact further restricts longer light pulses with high energy, as they would lead to CMOS structure destruction. The internal node voltage is fixed to a value close to logic zero and the gate output is fixed to logic one implying a constant power imprint for any input pattern. The size of the output inverter must also ensure low voltage drops even for high energies to minimize affecting subsequent circuit levels – near-threshold voltage values may lead to imbalances.

5. Evaluation

For evaluation, we employed the setup described in Section 1:

- we performed the simulation in ngSPICE,
- we simulated exclusively the circuits implemented in TSMC180nm technology,
- we use the standard cell library provided by Oklahoma State University (OSU) [18] extended by the proposed protected cells.

5.1. Illumination Response of Proposed Cells

To counter a *sophisticated attacker*, every single cell of the circuit must provide a well-balanced power imprint to make the attacker's job challenging. The simulated power imprints (OBICs) of proposed cells are presented in Figures 11a and 11b. The behavior below and above the specific illumination power, ≈150mW in Figure 11 and the voltage changes shown in Figure 12 clearly distinguish two standard and one transient region. The regions are shown in Figure 13. For lower illumination powers, the gate performs a normal operation (operational region). For higher powers, the gate output is constant and the gate experiences a short circuit (constant-output region) – see Figure 12.

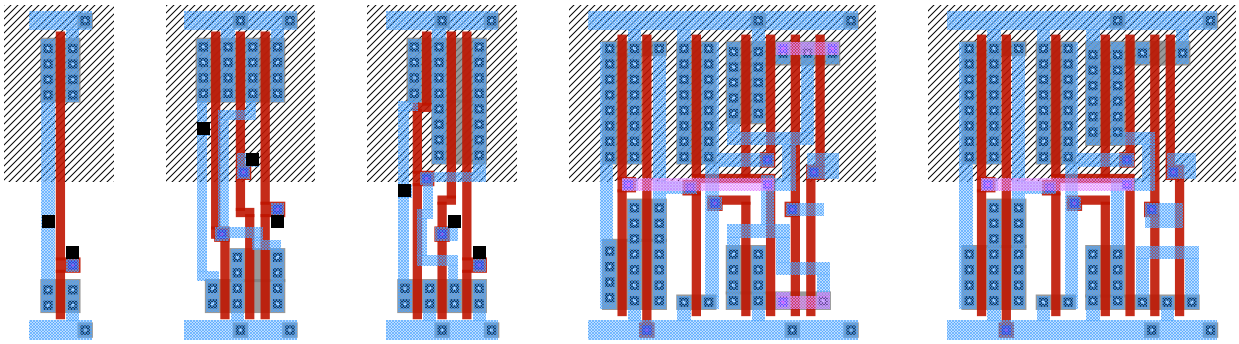


Figure 10: Standard cell layouts in TSMC180nm: (a) `INVX1`, (b) `AND2X1` and (c) `OR2X1` from the TSMC180nm library provided by Oklahoma State University (OSU); and proposed: (d) `PAND2X1` and (e) `POR2X1`

The proposed gate power imprint provides a balanced OBIC imprint even in the single-rail arrangement, while the SecLib can only be employed in the dual-rail circuit.

The proposed standard cells provide significantly decreased data-dependency of OBIC making *sophisticated attack* more challenging. Additionally, to fight with a *mid-equipped attacker*, the cocktail of many power imprints in the circuit must provide ideally negligible variances, to make the correlation between the circuit power and processed data hard to catch. We expect that if the building blocks of the circuit – standard cells – are well balanced, then the overall circuit data-dependency will also be significantly decreased. This is evaluated in Section 5.3.

5.2. Area Comparison

The proposed cell comparison with the standard – unprotected – library cells and SecLib cells composed of library cells[2] is provided in Table 1, while the proposed cell layouts are shown in Figure 10d and 10e. The original library cell layouts `INVX1`, `AND2X1`, and `OR2X1` are shown for comparison in Figures 10a, 10b, and 10c.

The protected cell size is increased compared to the unprotected standard cells, however, the delay remains acceptable. Additionally, the input load of the protected cells is, in general, lower, and the output drive strength of the proposed cells is increased compared to standard cells due to the requirements given by the optimization process and design rules presented above. These facts allow lower delay penalty in a real circuit. The competing dual-rail SecLib gates are much bigger and are affected by a great increase in the input load.

5.3. SBOX case study

To analyze the proposed structure implications to real circuits, we synthesized a larger combinational circuit implementing a crypto-function, namely the AES SBOX [31].

[2]SecLib approach uses library cells, custom C-elements were drawn for TSMC180nm library

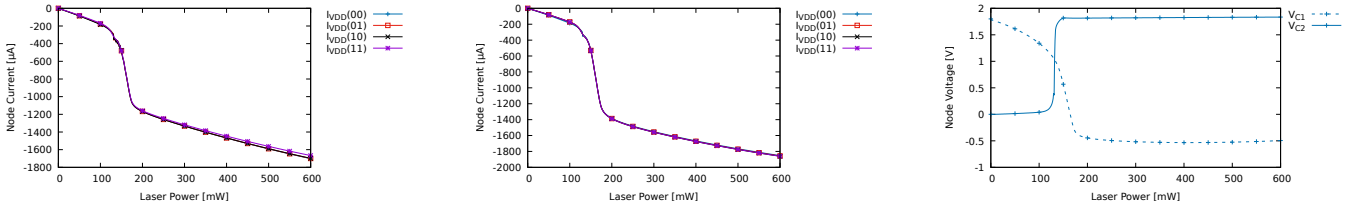
Larger combinational logic blocks might potentially be compromised by a mid-equipped attacker. We synthesized five different circuit variants of the SBOX combinational function. One unprotected single-rail implementation and four implementations employing dual-rail encoding as a dynamic attack countermeasure:

- *singleRail* variant employs only two-input NAND gates (`NAND2X1` and `INVX1`)
- *dualRailAS* variant is a non-conventional dual-rail implementation with alternating spacer [32] employing only two-input NAND and NOR gates and inverters (`NAND2X1`, `NOR2X1` and `INVX1`) allowing lower area overhead
- *dualRail* variant is a conventional dual-rail implementation [7, 6] employing only two-input AND and OR gates (`AND2X1` and `OR2X1`)
- *pDualRail* variant is a conventional dual-rail implementation employing only proposed two-input AND and OR gates (`PAND2X1` and `POR2X1`)
- *secLibDualRail* variant is a protected implementation employing secLib gates based on six dynamic C-elements and library cells (`INVX1` and `NOR3X1`)

The SBOX was described in Verilog, then synthesized and optimized by *Yosys* [33] and *Berkeley ABC* [34] respectively and finally mapped by a custom tool TSaCt2 [28] to obtain netlists for all variants under evaluation. For details on the Yosys script used, see [21].

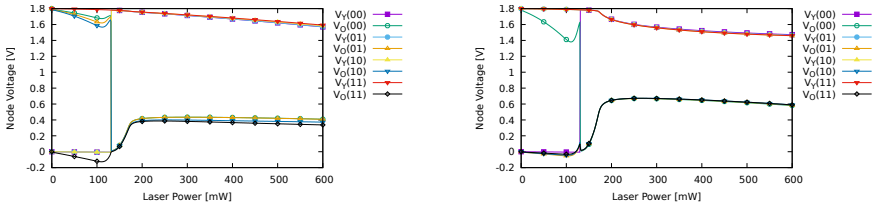
The mapped netlists for all variants were then placed by *GrayWolf* [35] and routed by *QRouter* [36]. *Magic* [37] was used as a primary VLSI layout tool, while custom scripts were used for model extraction, simulation control, and data processing.

For evaluation, we employed the setup described in Section 1: we used the ngSPICE simulation of TSMC180nm technology node standard cells: the layout models were simulated in ngSPICE. The largest netlists (pDualRail,



(a) Proposed PAND2X1 power imprint (b) Proposed POR2X1 power imprint (c) Control signals

Figure 11: PAND2X1 and POR2X1 power imprints and control signals in the point-of-interest



(a) Proposed PAND2X1 node voltages (b) Proposed POR2X1 node voltages

Figure 12: PAND2X1 and POR2X1 internal node (`O`) and output node (`Y`) voltages in the point-of-interest

Table 1: Comparison of Proposed Cells, SecLib Cells and their Standard Counterparts

Standard Cell	Area	Delay	Input Load	Drive Strength
Protected AND (PAND2)	≈260%	≈250%	≈ 30%	≈ 200%
Protected OR (POR2)	≈260%	≈280%	≈ 20%	≈ 200%
Dual-Rail Cell	**Area**	**Delay**	**Input Load**	**Drive Strength**
Protected (PAND2 + POR2)	≈260%	≈280%	≈ 25%	≈ 200%
SecLib	≈434%	≈250%	≈ 400%	≈ 100%
Optimized SecLib	≈525%	>250%	≈ 600 %	≈ 100%

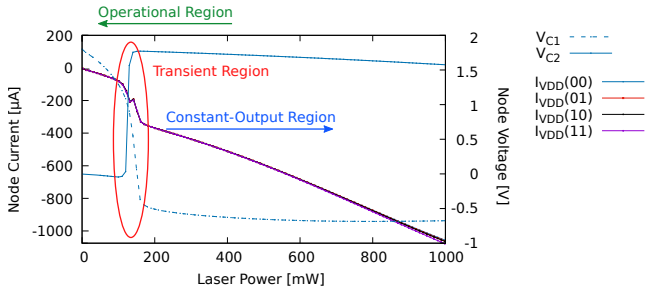


Figure 13: Proposed cell operation regions: (i) normal-operation region; (ii) constant-value-output region and (iii) transient region

secLibDualRail) were partitioned employing a custom procedure to enable a step-by-step simulation, as an en-bloc simulation in ngSPICE was not possible. The partitioning guarantees that the simulated dynamic power given by the load capacitance is pessimistic; however, the influence of glitches must not be preserved in all cases. The static light-induced power simulation accuracy is not affected significantly.

The disadvantage of proposed gates is that they utilize two metal layers compared to a single metal layer used by simple library cells. The complexity of the routing inside the proposed cells is closer to, e.g. `XOR` gate than to `AND` or `OR` gates.

Table 2: Area/Delay overhead comparison of different SBOX implementations

SBOX implementation	Area [mm^2]	Delay [ns]
singleRail	0.038 (100%)	≈ 9 (100%)
dualRailAS	0.057 ≈150%	≈ 11 (≈120%)
dualRail	0.066 (≈170%)	≈ 11 (≈120%)
pDualRail	0.158 – 0.196 (≈400% – 530%)	≈ 12 (≈130%)
secLibDualRail	0.294 – 0.431 (≈780% – 1150%)	≈ 15 (≈ 160%)

Table 2 shows the resulting layout sizes of the five SBOX implementations for comparison (pessimistic and optimistic routed layouts of the pDualRail and secLibDualRail versions are shown).

The pessimistic results in Table 2 represent the layouts obtained by the used open design flow. The used open-source QRouter is not the state-of-the-art router: it provides significantly worse results in complex designs than up-to-date commercial alternatives (see the maintainers' note in [36]). In our case, the router has problems with dense local interconnect. In the SBOX variants denoted pDualRail and secLibDualRail, we have to add increased cell spacing for successful routing.

Even if QRouter is not capable to route densely placed designs, state-of-the-art routers could success. The number of failed nets for dense placement is low and the manual layout inspection shows that there is room to finish the routing job. Therefore, we report the dense layout area as the optimistic data in Table 2.

As reported in Table 2, the circuit variant pDualRail, which is composed of proposed standard cells, brings only a small delay penalty compared to the area-efficient circuit variants and has lower delay than the SecLib-based secLibDualRail circuit variant.

Our approach is a masking approach decreasing the measurement SNR [10] by decreasing the variability in the data-dependent current component. The simulation results presented in Figure 14 show the variability of the data-dependent current at the time when the circuit is illuminated (in the point-of-interest). We evaluated different SBOX implementations employing different kinds of countermeasures. To visualize the data-dependent current variability, we use the statistical *probability density function* (PDF). Figures 14a – 14d show the power imprint variability for selected illumination powers for all circuit variants, while Figure 14f shows the power imprint variability for the dynamic power, and Figure 14e for the static power consumption (subthreshold leakage only was included). The variability of the power imprint is directly connected with circuit vulnerability: more variability in power traces decreases the attack cost. More variability in power traces also enables a successful attack to be performed by a less sophisticated attacker: the number of power traces required for a successful attack is lower, or simpler equipment might be used to obtain the power trace set of the required quality.

The routing procedure used is not able to balance complementary signals in dual-rail implementations. This does not significantly affect static circuit behavior, which is the focus of our research. In practice, dynamic power imbalances in dual-rail implementations can be further reduced by careful routing. For comparison, the dynamic behavior of all circuit variants is presented.

The simulation results show that our dualRailAS circuit version is significantly worse in dynamic power balancing compared to the other dual-rail implementations. In our comparison, we expect a more sophisticated attacker than the original dualRailAS authors. Nevertheless, our implementation still brings a little improvement compared to the single-rail circuit[3]. Figure 14f shows that dualRail, secLibDualRail and pDualRail implementations are balanced competitively from the dynamic power point of view. The implementation of the proposed pDualRail cells, however, offers much lower variability in power imprints induced by illumination at low illumination intensity.

Interestingly, the static power variability, presented in Figure 14e, follows the size of the implementation – smaller circuits are less vulnerable – except for the proposed implementation. The proposed implementation offers the lowest variability thanks to the size reduction of the input-controlled parts of the CMOS stack.

Figure 14 represents a serious issue for state-of-the-art protected dual-rail implementations (dualRail, dualRailAS, and even secLibDualRail). By delivering 50mW to 100mW of equivalent power to the area of the protected SBOX, the variability of the power trace set is increased to the level observed for dynamic power of the unprotected implementation (singleRail).

Although the attack setup is complex (it needs to control the clock or to synchronize illumination and power measurement), it can be effective. When delivering about 50 mW of equivalent power, the static power trace sets have comparable variability to the variability of the dynamic power traces obtained from an unprotected single-rail implementation. From an alternate perspective, we observed that about an order of magnitude lower measurement resolution is required for an illumination attack as for a dynamic power attack on protected implementation to obtain the power trace set with a comparable variability. The simulation shows that the illumination attack has the potential to circumvent the dynamic power countermeasures based on balancing.

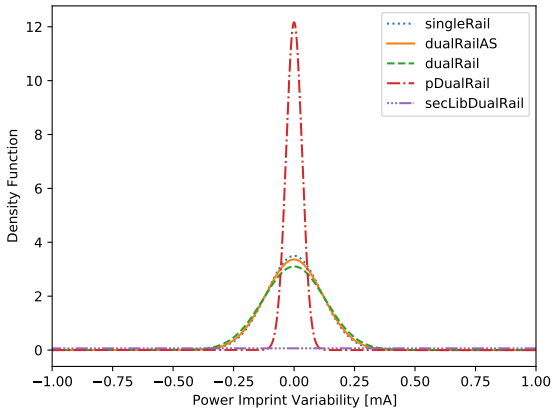
6. Discussion

The proposed structures, in general, affect the standard cell size and performance. On the other hand, only some of the approaches described in Section 3.3 may be employed to find out the trade-off between attack resistance and design cost – e.g. a smaller cell may be designed for lower illumination energy balancing only.

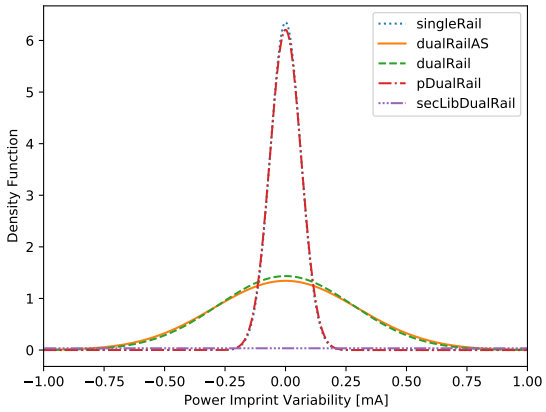
The advantage of the protections presented in Section 3.3 is that the protection mechanisms exploit natural properties of the CMOS technology, and thus all added transistor structures may be constructed accordingly to the original gate transistors – no process tuning is required. Although doping changes may increase the sensitivity of light sensors or increase/decrease the conductivity of added parts, good performance may be obtained by tuning transistor sizes only. This fact may simplify the protection mechanisms adoption.

Note that the light-sensitive structure may be shared between several standard cells to decrease the area overhead; however, any light-sensitive structure must be placed close to the protected structures to ensure that they will be exposed to the same light intensity in case of light-attack; in case of shared light-sensitive structures, considering bigger, while more sensitive structures [38] is possible.

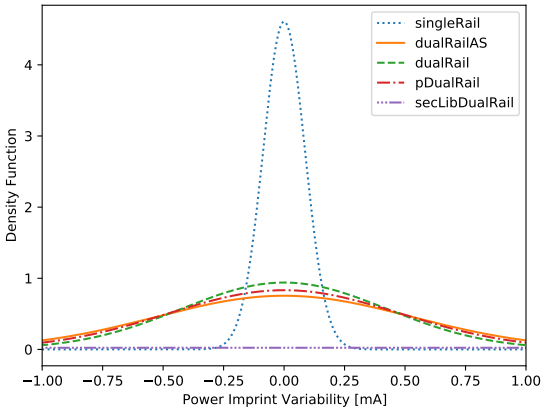
[3] dualRailAS circuit variant employs alternating spacer and it provides – in theory – the best dynamic power balancing when the attacker is only able to observe the integral dynamic power over following spacers. We considered only transition from the first (00) spacer to evaluation phase (as for the other dual-rail circuit variants), which disadvantages this version compared to the theoretical assumptions and other dual-rail variants – see [32] for details



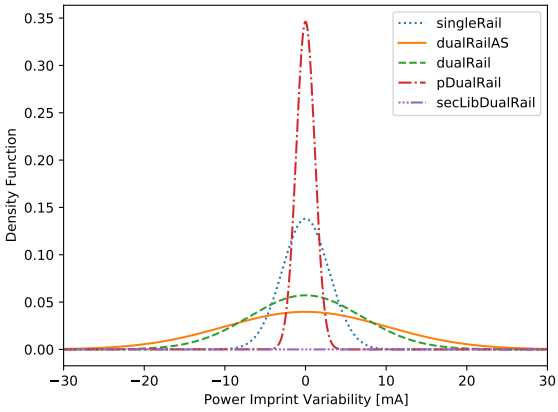
(a) 50mW



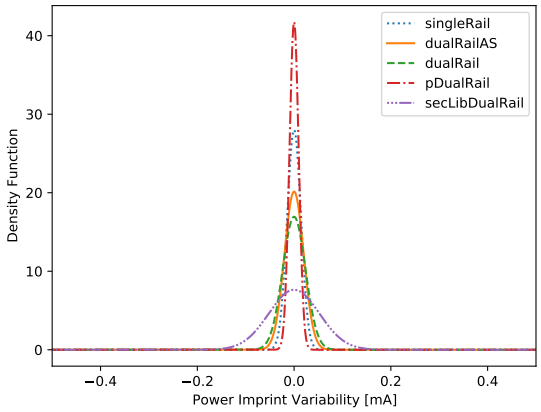
(b) 100mW



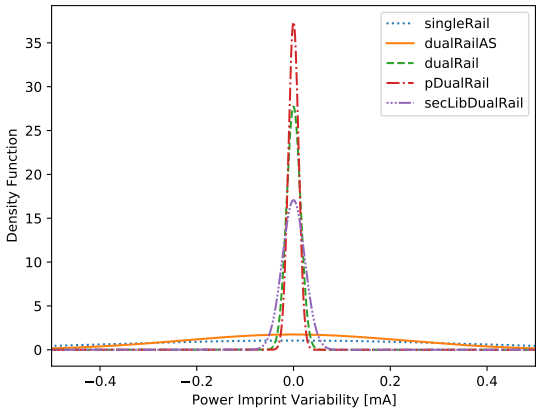
(c) 150mW



(d) 600mW



(e) Static Power



(f) Dynamic power

Figure 14: Selected density functions (PDF) for power imprints of all implementations - a narrower curve means a better protection. The proposed implementation overcomes its competitors significantly, except the *transient region*, where the results are comparable and smaller circuit size is an advantage

The advantage is that *inverter balancing* may be applied using standard cells only, without the need for custom CMOS cell design. This increases the practical impact of this balancing technique.

All of the presented approaches increase the data independence of the induced OBIC, but the inverter balancing approach and the size reduction of the input-controlled transistors in a protected gate reduce the data-dependent part of the leakage significantly.

The performance degradation or design cost is much smaller compared to the best static CMOS alternative, which is up today the SecLib [14].

As the proposed standard cells operate in two main regions (the operational and the constant value output), we believe that the whole circuit may be illuminated only by lower light intensities – in the operational region. Inducing a great current in a wider area would lead to circuit destruction: the cells out of the operational region are defacto shorted and only short light pulses guarantee that the circuit will survive. Additionally, the presented experimental results provide only the data-dependent part of the light-induced current – the light attack induces also data-independent current contributing to possible circuit destruction.

The disadvantage of our approach is that it can potentially simplify the fault-injection attacks. As the proposed cell output is a constant fixed value outside the operational region, it can be used to induce a fixed-value fault into a combinational circuit. This may lead to glitches or even register value changes depending on the attack timing. Even this kind of attack requires a sophisticated setup and it is possible to induce a fixed value fault to a selected location even with classical CMOS cells [1, 15, 23]. The proposed cells make the attack simpler, however, sophisticated equipment is still required. Inducing random faults by illumination may also be simplified; at least, the attacker can use the fact that the probability that the induced fault is (close to) 1. This kind of attack in general requires system-level countermeasures.

The proposed structure is most vulnerable – power imprint imbalances occur – when the illumination intensity is in the transient region, which is given by the supply voltage and illumination intensity.

Higher supply voltage may also increase imbalances in the transient region, as it affects the slope of the first control signal produced by the light-sensitive inverter – see Figure 15. A possible solution of this issue is adding other inverters into the inverter chain generating the control signals, to correct the control signals slope. Two inverters are recommended, as better results are obtained only if the first control signal precedes the second control signal. This simple approach helps with narrowing the transient region, however, the imbalance is still present. As the other source of imbalances in a bigger circuit composed of proposed cells, we identified voltage drops at the gate inputs deep in the illuminated circuit. The proposed standard cells were carefully designed to provide an almost perfectly balanced constant power imprint even under-voltage drops at the cell inputs, however, induced imbalances may still occur, especially in the transient region.

We have also a surprising result connected with the secLibDualRail circuit version. We originally expected that the secLibDualRail will provide the best protection, however, the sensitive region of the secLibDualRail circuit, which represents the standard SecLib approach, is in the lowest illumination power region, which is caused by charge leakage. This fact, connected with the huge area of the SecLib implementation, potentially enables a simpler attack to be performed, as bigger structures naturally lead to increased data-dependent variances observable in the power trace.

7. Conclusions

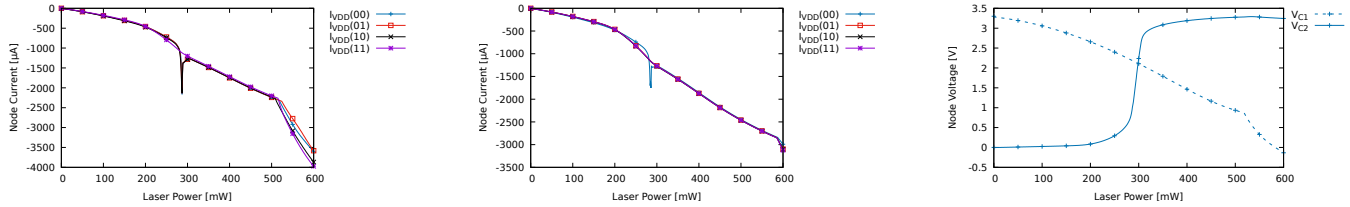
In this article, we have summarized our recent research related to attacks exploiting light-modulated static power. We described and evaluated related work and existing methods decreasing circuit vulnerability, and we proposed and evaluated new approaches in static CMOS circuit design leading to decreased light-modulated static power data-dependency overcoming existing alternatives. Attacks exploiting OBIC are potentially much more serious than those exploiting leakage, as OBIC attacks may be targeted and the induced currents are higher and thus simpler to measure.

The practical part of this article presents design rules for the standard CMOS cell design process and describes new protected standard cells in TSMC180nm library. A comparison with conventional and competing approaches was also presented. The protected gates were carefully evaluated and simulation results demonstrating the proposed cell benefits in a large combinational part of a CMOS circuit, namely the AES SBOX, were presented.

In practical designs, the presented approaches may be combined with established attack countermeasures such as laser sensors. This potentially allows using just balancing techniques effective for lower laser energies below the transient region and thus avoid the transient region vulnerability in our method.

We expect that the imbalances in the higher energy region are less significant in general, as those may force the attacker to use a higher energy close to the target's destructive threshold, making the attack more challenging and in general require a more experienced and equipped attacker.

Our approach offers significantly smaller area and delay overhead compared to the SecLib approach and improved static power balancing compared to common dynamic power balancing approaches at the same time. We have also identified a significant asymmetry in the SecLib countermeasure and proposed a straightforward solution. Even when our solution is applied, SecLib remains vulnerable to lower laser energies, which represents a severe vulnerability.



(a) Proposed PAND2X1 power imprint (b) Proposed POR2X1 power imprint (c) Control signals for PAND2X1

Figure 15: PAND2X1 and POR2X1 power imprints and control signals in the point-of-interest under the increased supply voltage

CRediT Author Statement

Jan Bělohoubek: Conceptualization, Methodology, Investigation, Data Curation, Writing - Original Draft, Visualization; **Petr Fišer:** Conceptualization, Resources, Writing - Review & Editing, Supervision; **Jan Schmidt:** Conceptualization, Resources, Writing - Review & Editing, Supervision

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The authors acknowledge the support of the OP VVV MEYS funded project CZ.02.1.01/0.0/0.0/16_019/0000765 "Research Center for Informatics". Computational resources were supplied by the project "e-Infrastruktura CZ" (e-INFRA LM2018140) provided within the program Projects of Large Research, Development and Innovations Infrastructures. The novel structures presented in this paper are subject of the patent application.

References

[1] D. Karaklajić, J. Schmidt, I. Verbauwhede, Hardware Designer's Guide to Fault Attacks, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 21 (12) (2013) 2295–2306. doi:10.1109/TVLSI.2012.2231707.

[2] P. Kocher, J. Jaffe and B. Jun, Differential power analysis, in: Annual International Cryptology Conference, Springer, 1999, pp. 388–397.

[3] F. Amiel, K. Villegas, B. Feix, L. Marcel, Passive and active combined attacks: Combining fault attacks and side channel analysis, in: Fault Diagnosis and Tolerance in Cryptography, 2007. FDTC 2007. Workshop on, 2007, pp. 92–102. doi:10.1109/FDTC.2007.12.

[4] S. Ravi, A. Raghunathan, P. Kocher, S. Hattangady, Security in embedded systems: Design challenges, ACM Transactions on Embedded Computing Systems (TECS) 3 (3) (2004) 461–491.

[5] T. Snyder, G. Byrd, The Internet of Everything, Computer 50 (6) (2017) 8–9. doi:10.1109/MC.2017.179.
URL doi.ieeecomputersociety.org/10.1109/MC.2017.179

[6] J. Sparsø, S. Furber, Principles of Asynchronous Circuit Design: A Systems Perspective, 1st Edition, Kluwer Academic Publishers, Boston, 2001.

[7] K. Tiri, I. Verbauwhede, A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation, in: Proceedings Design, Automation and Test in Europe Conference and Exhibition, Vol. 1, IEEE, 2004, pp. 246–251.

[8] J. Giorgetti, G. Scotti, A. Simonetti, A. Trifiletti, Analysis of data dependence of leakage current in CMOS cryptographic hardware, in: Proceedings of the 17th ACM Great Lakes symposium on VLSI, ACM, 2007, pp. 78–83.

[9] M. Alioto, L. Giancane, G. Scotti, A. Trifiletti, Leakage Power Analysis attacks: Well-defined procedure and first experimental results, in: 2009 International Conference on Microelectronics - ICM, 2009, pp. 46–49. doi:10.1109/ICM.2009.5418592.

[10] T. Moos, A. Moradi, B. Richter, Static Power Side-Channel Analysis – An Investigation of Measurement Factors, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 28 (2) (2020) 376–389. doi:10.1109/TVLSI.2019.2948141.

[11] B. Fadaeinia, T. Moos, A. Moradi, BSPL: Balanced Static Power Logic., IACR Cryptol. ePrint Arch. 2020 (2020) 558.

[12] J. Bělohoubek, P. Fišer, J. Schmidt, Using Voters May Lead to Secret Leakage, in: 2019 IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2019, pp. 1–4. doi:10.1109/DDECS.2019.8724663.

[13] J. Bělohoubek, P. Fišer, J. Schmidt, CMOS Illumination Discloses Processed Data, in: 2019 22nd Euromicro Conference on Digital System Design (DSD), 2019, pp. 381–388. doi:10.1109/DSD.2019.00062.

[14] J. Bělohoubek, P. Fišer, J. Schmidt, Standard Cell Tuning Enables Data-Independent Static Power Consumption, in: 2020 IEEE 23rd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS), 2020, pp. 1–6. doi:10.1109/DDECS50862.2020.9095656.

[15] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J.-M. Dutertre, A. Tria, Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology, in: IEEE International Reliability Physics Symposium (IRPS), 2013, IEEE, 2013, pp. 5B–5.

[16] A. Sarafianos, R. Llido, O. Gagliano, V. Serradeil, M. Lisart, et al., Building the electrical model of the pulsed photoelectric laser stimulation of an NMOS transistor in 90nm technology, in: 38th International Symposium for Testing and Failure Analysis, (ISTFA) 2012, 2012, pp. 5B–5.

[17] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J. Dutertre, A. Tria, Building the electrical model of the pulsed photoelectric laser stimulation of a PMOS transistor in 90nm technology, in: Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA), 2013, pp. 22–27. doi:10.1109/IPFA.2013.6599120.

[18] Oklahoma State University (OSU), MOSIS SCMOS: Standard Cells for AMI 0.6um, AMI 0.35um, TSMC 0.25um, and TSMC 0.18um (1999 – 2016).
URL https://vlsiarch.ecen.okstate.edu/flows/MOSIS_SCMOS

[19] J. Bělohoubek, Open CMOS SPICE Model Collections (2019).
URL https://github.com/DDD-FIT-CTU/CMOS-SPICE-Model-Collections

[20] H. Vogt, M. Hendrix, P. Nenzi, D. Warning, Ngspice users man-

ual version 34 (2021).
[21] J. Bělohoubek, Photoelectric Laser Stimulation of Combinational Logic (2019 – 2021).
URL https://github.com/DDD-FIT-CTU/CMOS-PLS/
[22] N. Weste, D. Harris, CMOS VLSI Design: A Circuits and Systems Perspective, 4th Edition, Addison-Wesley Publishing Company, USA, 2010.
[23] S. P. Skorobogatov, R. J. Anderson, Optical fault induction attacks, in: International workshop on cryptographic hardware and embedded systems, Springer, 2002, pp. 2–12.
[24] E. Brier, C. Clavier, F. Olivier, Correlation power analysis with a leakage model, in: International workshop on cryptographic hardware and embedded systems, Springer, 2004, pp. 16–29.
[25] H. Endoh, T. Naoe, Copper Wire Bonding Package Decapsulation Using the Anodic Protection Method, Microelectronics Reliability 55 (1) (2015) 207–212.
[26] J. Bělohoubek, R. Vik, Low-Cost CMOS Power Consumption Data Dependency Demonstrator Concept, in: Prague Embedded Systems Workshop 2019, 2019.
[27] S. Chari, J. R. Rao, P. Rohatgi, Template attacks, in: International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2002, pp. 13–28.
[28] J. Bělohoubek, TSaCt2 (2015 – 2021).
URL https://github.com/DDD-FIT-CTU/TSaCt2
[29] S. Guilley, F. Flament, Y. Mathieu, R. Pacalet, Security evaluation of a balanced quasi-delay insensitive library (seclib), in: Conference on Design of Circuits and Integrated Systems, 2008, pp. 6–pages.
[30] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, J. Provost, CMOS structures suitable for secured hardware, in: Proceedings Design, Automation and Test in Europe Conference and Exhibition, Vol. 2, 2004, pp. 1414–1415 Vol.2. doi:10.1109/DATE.2004.1269113.
[31] J. Daemen, V. Rijmen, The Rijndael block cipher: AES proposal, in: First candidate conference (AeS1), 1999, pp. 343–348.
[32] D. Sokolov, J. Murphy, A. Bystrov, A. Yakovlev, Design and analysis of dual-rail circuits for security applications, IEEE Transactions on Computers 54 (4) (2005) 449–460.
[33] C. Wolf, Yosys Open SYnthesis Suite (2012 – 2021).
URL http://www.clifford.at/yosys/
[34] A. Mishchenko, ABC: A System for Sequential Synthesis and Verification (2005 – 2021).
URL https://people.eecs.berkeley.edu/~alanmi/abc/
[35] Graywolf contributors, Graywolf – a fork of TimberWolf 6.3.5 (2014 – 2021).
URL https://github.com/rubund/graywolf5
[36] R. T. Edwards, Qrouter (2013 – 2021).
URL http://opencircuitdesign.com/qrouter/
[37] R. T. Edwards, Magic VLSI (2004 – 2021).
URL http://opencircuitdesign.com/magic/
[38] Marinet, Fabrice and Fort, Jimmy and Sarafianos, Alexandre and Mercier, Julien, Device for Detecting a Laser Attack in an Integrated Circuit Chip (Dec. 9 2014).