Standard Cell Tuning Enables Data-Independent Static Power Consumption

Jan Bělohoubek, Petr Fišer, Jan Schmidt
Faculty of Information Technology
Czech Technical University in Prague
Prague, Czech Republic
{jan.belohoubek, petr.fiser, jan.schmidt}@fit.cvut.cz

***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 traditional static CMOS bulk structures. To enable data dependency hiding, we propose low-level techniques based on complementary-value induced balancing currents, constant current source behavioral approximation, and light-sensing capability of traditional CMOS structures. The proposed techniques may be used to build a dual-rail circuit balanced from both perspectives: static and dynamic power. The publicly available TSMC180nm node standard cell simulation is used for evaluation.**

I. Introduction

Physical attacks – invasive [1], observation [2] or, combined [3] represent a great challenge for today's digital design [4] since their introduction in the late of 90s. 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, 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 [8], [9], [10] or even light-modulated static power [11], [12] may lead to a successful attack.

In this paper, we describe novel structures and techniques developed to enhance and balance traditional static bulk CMOS structures from the perspective of the light-modulated static power and leakage. Existing CMOS structures leading to increased data-independence in the leakage and light-modulated static power are also described and compared to proposed approaches. Proposed structures increase the circuit resistance against attacks on the CMOS static power and have an acceptable impact on delay, area, and power consumption of protected static CMOS circuits.

The evaluation method we use through this paper is the SPICE simulation of illuminated transistor structures. The models originally presented in [13], [14], [15] were qualified for publicly available TSMC180nm technology node [11]. The simulation is performed in *ngSPICE*[1] and results are based on the publicly available TSMC180nm technology node models and std. cell layouts. The simulated CMOS devices are illuminated by a constant light source with the energy density equivalent to the laser beam focused to a fixed area with power ranging between 0 and 1000mW. The 1.8V supply voltage is used. The models, simulation data, and additional MonteCarlo simulation results are available online[2].

The rest of the paper is structured as follows: In Section II, the data-dependent behavior of CMOS power consumption is described; in Section III, the established attack-resistant design styles are described and in Section IV, the proposed approaches for static CMOS power balancing are enumerated. These approaches are discussed in Section V. Experimental evaluation is provided in VI. The paper is concluded by Section VII.

II. CMOS Structures and Data-Dependent Power Consumption

CMOS (*Complementary Metal Oxide Semiconductor*) processes are used for the manufacturing of the majority of today VLSI (*Very Large-Scale Integration*) digital logic designs [16], 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 the gate inputs) [16]. 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 the *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,

[1] http://ngspice.sourceforge.net/

[2] http://ddd.fit.cvut.cz/prj/CMOS-PLS

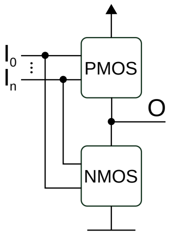
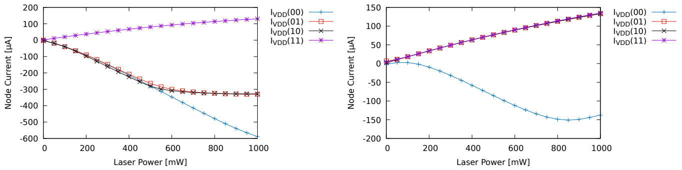


Fig. 1: Generalized CMOS structure: PMOS part contains P-type transistors, NMOS part contains N-type transistors.



(a) (b)

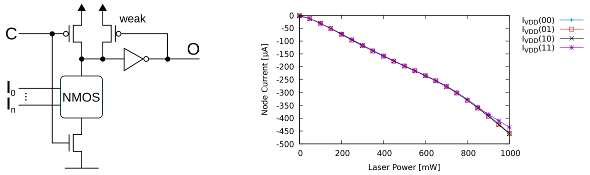
Fig. 2: The simulated OBIC for 2-input NAND (a) and NOR gates for different input patterns

the static power data dependency may be manifested by using a (focused) laser beam [11], [12] increasing the order of magnitude of the 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) [13] may be in tens or even in hundreds of microamps for a single logic gate depending on the CMOS technology node.

In classical literature, e.g., in [16], it can be found, that CMOS leakage (namely the subthreshold leakage) is data-dependent. Based on the NMOS/PMOS behavioral models under illumination, it is also evident, that to induce a significant OBIC in NMOS requires significantly less energy than to induce similar OBIC in PMOS. The OBIC may also be controlled by the gate voltage. Both leakage and OBIC are thus correlated with the CMOS circuit input pattern.

To demonstrate this behavior, the current dependence of the data-dependent part of OBIC on gate input patterns is in Figure 2 for two-input NAND and NOR gates. The generalized CMOS structure is shown in Figure 1 for illustration.

It is evident that the OBIC data dependency is strongly correlated with the state of the PMOS stack of the gate: (i) the serial arrangement of PMOSes in the NOR gate ensures that input patterns leading to at least one open PMOS transistor lead to similar induced currents – see Figure 2b; in contrast (ii) parallel PMOS arrangement in NAND gate implies, that different current is induced for two and for one closed PMOS transistors – see Figure 2a. The data-dependency of power consumption in CMOS under illumination strongly depends on the state and structure of the PMOS stack, because PMOSes have significantly lower conductivity caused by illumination compared to NMOSes. On the other hand, the leakage data-dependency is strongly influenced by the state and structure of NMOS stack, while being several orders of magnitude lower compared to the static current induced by illumination.



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

(b) Domino logic two-input AND gate power imprint

Fig. 3: Domino logic gate structure and power imprint example

Note that a small difference in the OBIC between 01 and 10 input patterns in Figure 2a is caused mainly by an asymmetry in NMOS stack, however, this phenomenon is less significant than the phenomenon connected with PMOSes.

III. CMOS Structures Resistant by Design

The aim of this work is to present techniques allowing construction of circuits resistant to leakage attacks and attacks based on decapsulated circuit illumination, while the emphasis is on light-originated data-dependency, as the data-dependent OBIC is significantly higher than the leakage. The brief analysis in Section II shows that the serial arrangement of PMOSes decreases the data dependency of the OBIC drastically. Natural attack-resistant design style candidates are those, where there appears only the serial arrangement of PMOSes limiting the data dependency. The other option is to employ logic cells with a high level of symmetry. Based on our logic circuit design styles knowledge, we identified two established design styles that provide a significant level of attack resistance. These design styles are described below.

A. 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 by the data-independent precharge transistor.

The problem of the dynamic logic, and domino logic, in particular, is that it requires inverters at the gate outputs to achieve monotonicity in the designed circuit [16]. Conventionally, the inverter is a traditional CMOS inverter with a pair of complementary transistors controlled by a single input signal. This part of the dynamic gate causes data-dependent power consumption. Last but not least, dynamic logic in general and domino logic, in particular, suffers from *charge leakage* [16]. Charge leakage may require keepers, which serve as an additional source of data-dependent power consumption. The complete domino logic gate is in Figure 3a.

Fortunately, the structure of the conventional domino gate provides natural compensation. The traditional approach for the charge leakage problem solution is called a *weak keeper*. The weak keeper is controlled by a signal produced by the gate output inverter. By altering sizes of the weak keeper and the output inverter, the data-dependency in the power imprint for the domino gate under illumination may be decreased significantly. The data dependency of the induced OBIC of the domino gate optimized by hand is in Figure 3b.

B. *Symmetric SecLib Gates*

The known approach 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 [17], [18]. The SecLib dual-rail NAND gate is in Figure 4.

SecLib gates are perfectly symmetric from all: schematic, layout, input and output perspectives. Unfortunately, the SecLib gate is huge, implying significant area, delay and power overhead; one dual-rail 2-input gate is represented by two (balanced) 3-input OR gates and 4 C-elements. According to [12], the cell should be as small as possible to decrease the severity of a possible attack.

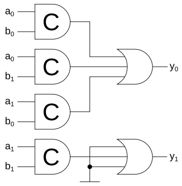


Fig. 4: Secured 2-input NAND gate schematic: all input combinations at C-element inputs are represented; one C-element output is always equal to 1 and three remaining C-element outputs are always equal to 0

Solutions described above share a nice property: those were designed to support dual-rail encoding computation, thus (if employed in a dual-rail circuit) provide (at least) basic level of dynamic power attack resistance. On the other hand, they suffer from some disadvantages. SecLib suffers mainly from gate size. 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 [16].

IV. Structures Enabling Static CMOS Current Balancing

Compared to the dynamic logic, we propose compact static cells that counter the attack by balancing and may complement SecLib as a countermeasure against the vulnerability described in [11], [12].

The circuit vulnerability connected with the OBIC may be compensated only when – in the case of the illumination attack – the entire balanced structure is exposed to the same light intensity. This natural requirement may not be guaranteed for bigger structures. The size of the balanced structure is extremely important.

In this section, we provide a comprehensive description of approaches proposed for balancing of traditional CMOS gates 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 constant current source approximation are – according to best of our knowledge – novel in the security context.

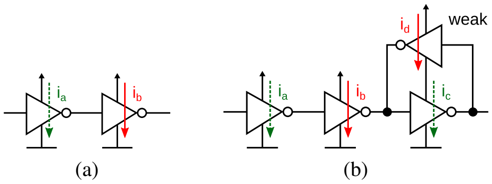


Fig. 5: Two-inverter chain (a) uses complementary power consumption to obtain a constant power imprint: $i_a + i_b = const.$; three-inverter chain with feedback weak inverter (b) uses the identical principle

A. *Inverter Balancing*

The first approach origins in the fact, that two inverters in a serial arrangement work with complementary values, and thus may provide constant (mutually balanced) power imprint. It is simple to balance a two-inverter chain resulting in the buffer with constant static power imprint – see Figure 5a. Note that inverters working with complementary input values at the same time also provide leakage balancing.

If the inverting structure in general, and inverter cell in particular, should be balanced, an odd number of inverters in the linear chain is required. A straightforward balancing strategy is to alter inverter sizes in the chain to provide balancing. An alternative option is to employ the three-inverter linear chain equipped with an in-the-cell compensation feedback inverter. From the integration perspective, it is important to ensure that the balanced cell provides high impedance input, thus it is not a good idea to use a single inverter with feedback.

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 gates in particular. This implies that standard static CMOS positive gates (e.g. AND, OR) provide a limited intrinsic level of balancing. Note that it is relatively simple to enhance balancing efficiency by an output inverter scaling.

Note also that generalization of this approach is the reason, why domino logic described in Section III provides a good level of power compensation by design.

B. *Constant Current Source Approximation*

The other group of current-balancing approaches is based on the idea of the modification of the CMOS gate to mimic the *Constant Current Source* behavior, as shown in Figure 6a.

The standard approach in the constant current source approximation is to employ a fixed serial resistor significantly bigger than the load resistance. The original CMOS stack OBIC is data-dependent: the data-dependent component of the CMOS stack resistivity should be decreased compared to the fixed component of the resistivity. Three approaches at the transistor level are employed.

1) Adding Serial Transistor: A straightforward approach is shown in Figure 6b. Adding a single – normally-closed – transistor in series with the NMOS or PMOS part of the circuit allows to tune the static part of the resistance if the internal arrangement of the NMOS/PMOS is parallel. This transistor is related to R_{SP} and R_{SN} in Figure 6a. Although it is normally

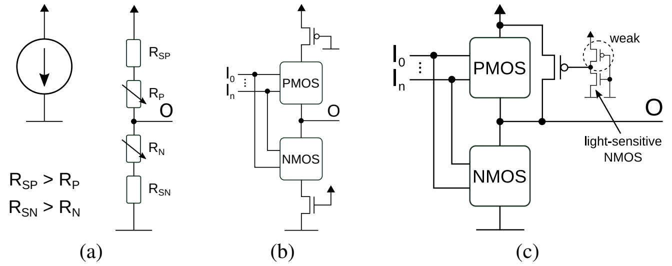


Fig. 6: Constant Current Source approximation (a) by small (data-dependent) potentiometers and larger fixed serial resistors; serial transistors (b) are employed to increase the fixed component of the resistivity; and the parallel transistor (c) is used to decrease the data-dependent component of resistivity

closed, it effectively reduces the OBIC in case of illumination attack.

2) Adding Light-Sensitive Parallel Transistor: The second approach is shown in Figure 6c. The parallel connection of normally-open PMOS transistor to PMOS stack has no significant effect in the case of normal operation (except of the increased leakage). However, when the circuit is under invasive light-attack, the conductivity of NMOSes grows rapidly and the parallel PMOS is closed by a light-sensitive inverter – see Figure 6c. The parallel transistor decreases the significance of the data-dependent resistivity of the PMOS block. The parallel connection of NMOS transistor in the NMOS stack is also possible, but it has almost no effect in the case of invasive light-attack, as the significant conductivity of illuminated NMOSes wipes the data-dependency effect.

3) Disconnecting Rail: The third approach is shown in Figure 8. When the CMOS circuit is under attack, disconnecting one of the rails decreases the data dependency significantly. The same light-sensitive inverter as for parallel PMOS control may be employed to disconnect the VSS rail. This represents a significant increase of the serial resistance denoted R_{SP} and R_{SN} in Figure 6a.

C. Increasing Transistor-Level Symmetry

The next approach related to balancing leakage and OBIC currents is dedicated to balancing asymmetries in the transistor stack. The aim of this modification is to increase the similarity when equivalent input patterns (from the higher-level perspective) – e.g. 01 and 10 – are at the gate inputs. Although such patterns should intuitively imply equivalent leakage and OBIC currents, they do not, due to the *stack effect* asymmetric behavior in NMOS [16]. A simple approach can be used to fight asymmetry, as shown in Figure 7. This approach is not new – it is described in the literature – e.g., in [18] and symmetrized standard cells may be provided in the standard cell library.

Note that the size of the modified structure may be close to the size of the old one; only the resulting structure is a bit complicated. As both structures are functionally equivalent, the transistor sizes can be scaled down (if possible) without affecting the cell performance.

The balancing may also be provided by duplicating an unbalanced standard cell and swapping its inputs. For the price of an increased area, this allows balancing by using standard library cells, without the need of the custom CMOS cell design.

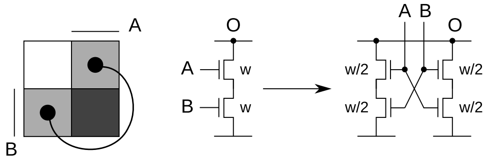


Fig. 7: Removing asymmetries in CMOS to suppress the data dependency in leakage and OBIC induced by the *stack effect* asymmetric behavior

D. Output Voltage Filtering

The careful design of the secured cell also includes the output voltage to be without significant variations and slow slopes. The output inverter may serve as the voltage filter separating the internal node Y suffering from voltage drops. The output inverter, in this case, also provides the balancing, as described in Section IV-A.

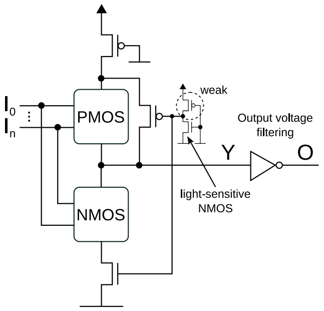


Fig. 8: Completely balanced positive gate: the output inverter serves for power balancing and as the output voltage filter at the same time

V. Proposed Structures Discussion

The proposed structures, in general, affect the gate size and/or performance. On the other hand, only some of the proposed approaches may be employed to find out the trade-off between attack resistance and design cost. Additionally, the performance degradation or design cost is much smaller compared to the best static CMOS alternative, which is up today the SecLib. On the other hand, the dynamic, namely domino logic provides the best area overhead and lower delay. Still, it requires a different design style and a dedicated clock distribution in the combinational logic.

The advantage of the protections presented in Section IV is that the protection mechanisms exploit the 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 the 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 may simplify the protection mechanism adoption.

Note that the light-sensitive structure may be shared 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.

The advantage is that some of the protection mechanisms, namely *inverter balancing* and *transistor-level symmetry*, may be applied by using standard cells only – without the need for custom CMOS cell design. This increases the practical impact of those balancing techniques.

Note that all of the presented approaches increase the data-independence of the induced OBIC, but only the transistor-level symmetry and inverter balancing approaches increase the leakage data-independence significantly.

VI. Experimental Evaluation

In this section, we provide an evaluation of the structures proposed in Section IV. For evaluation, we employed the setup described in Section I: we used the ngSPICE simulation of TSMC180nm technology node standard cells.

Figure 9 shows the power response of the two-inverter chain. It is evident that library inverters provide a solid level of symmetry in the power imprint; however, we were able to optimize the inverter chain by hand to provide an even higher level of symmetry. Comparable results were achieved also for the three-inverter chain with the feedback inverter.

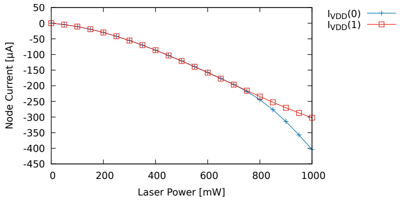


Fig. 9: The power imprint of two-inverter chain: unmodified inverters from the TSMC180nm cell library were used

It is more challenging to balance complex gates compared to the inverter chains. Figure 10 shows a step-by-step balancing of the NAND gate. The balancing procedure converts the NAND gate to the AND gate. The unbalanced two-input NAND gate power imprint is shown in Figure 2a. Note that the AND standard cells have also an unbalanced power imprint, although they are equipped with the output inverter because balancing the power imprint (under illumination) is not a common optimization criterion in the gate design process. In this paper, we show – as a representative – only the procedure of the NAND gate balancing (balanced AND gate design process). Generally speaking: any CMOS structure may be balanced accordingly.

Figure 10a represents a power imprint of the NAND gate with symmetrized NMOS stack balanced by an output inverter(s) only. This provides a high level of symmetry in the power imprint, up to ≈500mW of the laser power. The imbalances are caused by significant voltage drops (at Y node) above 500mW, as shown in Figure 11a – the output inverter input node is denoted V_Y in Figure 11. It is possible to achieve this level of symmetry by employing standard cells only – no transistor-level modifications are required.

TABLE I: Area/Delay overhead comparison of balanced gates with their std. equivalents and with SecLib in TSMC180nm

Standard Cell Gate	Proposed		SecLib (dual-rail)	
Description	Area	Delay	Area	Delay
Two-INV chain (buffer)	≈200%	<200%	–	–
Three-INV chain with feedback	≈400%	<300%	–	–
Custom protected AND2	≈200%	≈110%	–	–
AND2 composed of std. cells only	>300%	<110%	≈600%	≈200%
Custom protected OR2	≈200%	≈200%	–	–
OR2 composed of std. cells only	≈160%	<120%	≈600%	≈200%

Serial resistivity allows further decreasing of the power imprint data dependency, as shown in Figure 10b. Further symmetry increase is achieved by employing light-activated parallel PMOS and the foot NMOS allowing to disconnect the VSS rail, as shown in Figure 10c. The resulting structure provides a high level of symmetry in the power imprint, but the gate operational region is reduced below ≈ 200mW, which is caused by increased light sensitivity causing early voltage drops – see Figure 11b.

As noted above, two regions are easy to distinguish in Figure 11. The first region is below 500mW and 200mW respectively: under that illumination power, the gate is operational, and two voltage groups represent logic 0 and logic 1 gate outputs. Above the critical laser power, the gate output does not represent the gate logic function output. In this region, the data-dependent voltage variance is small, which limits data-dependency propagation to the following gate inputs – the gate output is data-independent.

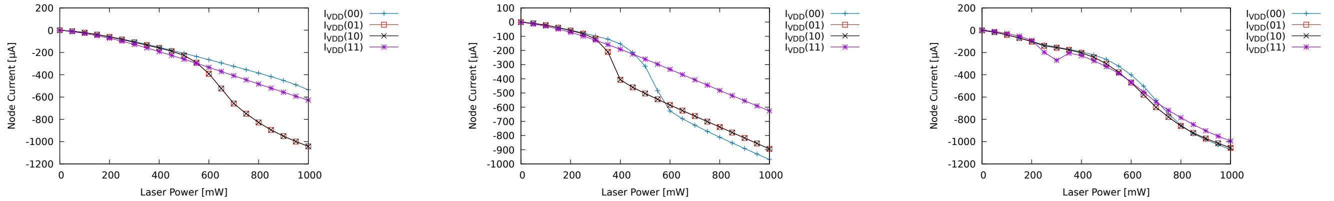
The balanced gate output is denoted V_O in Figure 11. The voltage slope of the gate output when crossing the border between those two regions is high – this is ensured by the output filter inverter. The high voltage slopes are important, because the transient area, where slopes occur, represent the most vulnerable regions in the balanced characteristics, as can be seen in Figure 10. Generally, the slope of V_Y may be lower and more data-dependent, as it is filtered by the output inverter.

Table I provides the relative comparison of gate sizes and delay overheads, related to standard cells for different balancing approaches. The presented static CMOS approaches lead to ≈200% area overhead in single-rail overcoming the dual-rail SecLib ≈600% area overhead. The delay penalty of the presented approach is acceptable and in general lower than in SecLib.

For lower light source power, the balancing is almost perfect for methods employing no light-sensitive structures. The gate balanced also using light-sensitive structures provides almost optimal balancing for the whole light-source power range under the design voltage. We found that the completely balanced structure may be affected by varying supply voltage, however, the gate using light-sensitive structures provides better balancing compared to the unbalanced one even for varying voltage.

VII. Conclusions

In this paper, we summarize the approaches usable for leakage and light-induced static current balancing allowing to suppress the data-dependency in the static power imprint of the balanced CMOS gate. Traditional balancing approaches were presented in the new context and novel balancing approaches for static CMOS were developed.

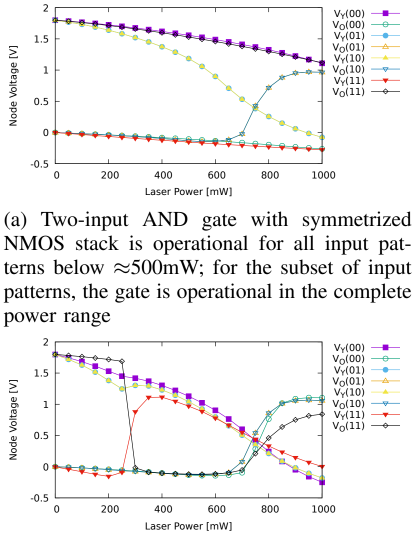


(a) Two-input AND gate with symmetrized NMOS stack balanced by output inverter – 2x unmodified TSMC180nm inverters in parallel

(b) Two-input AND gate with symmetrized NMOS stack balanced by output inverter and serial PMOS resistance

(c) Two-input AND gate completely balanced

Fig. 10: The step-by-step procedure of balancing NAND/AND gate by employing particular approaches



(a) Two-input AND gate with symmetrized NMOS stack is operational for all input patterns below ≈500mW; for the subset of input patterns, the gate is operational in the complete power range

(b) Two-input AND gate completely balanced is operational below ≈ 200mW

Fig. 11: AND gate output (O) and internal node (Y) voltage

In real designs, the presented approaches may be combined with established attack countermeasures such as laser sensors. This allows using just balancing techniques effective for lower laser energies, such as output inverter balancing, as higher energies will be detected by a sensor. The disbalances in the higher energy region are less significant in general, as those may force the attacker to use higher energy close to the target's destructive threshold, making the attack more challenging.

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". The novel structures presented in this paper are subject of the patent application.

References

[1] D. Karaklajić, J. Schmidt, and I. Verbauwhede, "Hardware Designer's Guide to Fault Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 12, pp. 2295–2306, Dec 2013.

[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, and 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*, Sept 2007, pp. 92–102.

[4] S. Ravi, A. Raghunathan, P. Kocher, and S. Hattangady, "Security in embedded systems: Design challenges," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 3, no. 3, pp. 461–491, 2004.

[5] T. Snyder and G. Byrd, "The Internet of Everything," *Computer*, vol. 50, no. 6, pp. 8–9, 2017. [Online]. Available: doi.ieeecomputersociety.org/10.1109/MC.2017.179

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

[7] K. Tiri and 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, and 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, and A. Trifiletti, "Leakage Power Analysis attacks: Well-defined procedure and first experimental results," in *2009 International Conference on Microelectronics - ICM*, Dec 2009, pp. 46–49.

[10] T. Moos, A. Moradi, and B. Richter, "Static Power Side-Channel Analysis – An Investigation of Measurement Factors," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 2019.

[11] J. Bělohoubek and P. Fišer and J. Schmidt, "Using Voters May Lead to Secret Leakage," in *IEEE 22nd International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS 2019)*, April 2019, pp. 1–4.

[12] ——, "CMOS Illumination Discloses Processed Data," in *22nd Euromicro Conference on Digital System Design (DSD 2019)*, Aug 2019, pp. 381–388.

[13] A. Sarafianos, O. Gagliano, V. Serradeil, M. Lisart, J.-M. Dutertre, and 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.

[14] 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.

[15] A. Sarafianos, O. Gagliano, M. Lisart, V. Serradeil, J. Dutertre, and 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)*, July 2013, pp. 22–27.

[16] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 4th ed. USA: Addison-Wesley Publishing Company, 2010.

[17] S. Guilley, F. Flament, Y. Mathieu, and 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.

[18] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, and J. Provost, "CMOS structures suitable for secured hardware," in *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, vol. 2, Feb 2004, pp. 1414–1415 Vol.2.