Hardware Countermeasures against Power Analysis Attacks: a Survey from Past to Present

R. Soares[1], V. Lima[2], R. Lellis[1], P. Finkenauer Jr.[1] and V. Camargo[1]

[1]Graduate Program in Computer Science (PPGC) - Federal University of Pelotas (UFPel) - Pelotas-Brazil
[2] Graduate Program in Microelectronic (PGMicro) - Federal University of Rio Grande do Sul (UFRGS), Porto Alegre-Brazil
e-mail: rafael.soares@inf.ufpel.edu.br

***Abstract*— Modern cryptographic circuits are increasingly demanding security requirements. Since its invention, power analysis attacks are a threat to the security of such circuits. In order to contribute to the design of secure circuits, designers may employ countermeasures in different abstraction levels. This work presents a brief survey of countermeasures to help designers to find good solutions for the design of secure cryptographic systems. A summary is highlighted to compare the pros and cons of the approaches to help designers choose a better solution, or even provide subsidies so that new solutions can be proposed.**

***Index Terms*— Hardware security; Countermeasures; Cryptography; Survey; Side-Channels Attacks.**

I. Introduction

The last few decades have seen an increase in concern regarding the protection of information processed in electronic devices driven by the wide use of smartphones, smart cards, and intelligent nodes in IoT applications. Internet shopping activities, bank transactions, ticket reservation systems are examples of typical applications that require the security of confidential data stored and computed on electronic products, however with the development of new technologies, the range of devices under threat now include sensors in wireless sensor networks [1], which usually are in unsupervised locations, and even Cloud Field-Programmable Gate Arrays [2]. Modern devices provide cryptographic algorithms and authentication protocols to protect the systems against malicious users.

Although cryptography has been continuously developed to ensure that algorithms remain robust to retrieving confidential data, new techniques demonstrate that, through the physical properties of digital systems, it is possible to reveal the processed data. This class of techniques known as Side-Channel Attacks (SCAs) exploits the leakage of sensitive information to quantities such as power consumption, electromagnetic radiation, processing time, and sound. These leakages allow the adversary to discover secret information about a system, especially those protected from encryption. SCAs seek to establish a dependency relationship between the processed data and the analyzed physical quantities. The vulnerabilities arise mainly from the implementation characteristics of the CMOS circuit technology, along with the synchronous paradigm traditionally adopted in the design of digital systems [3].

Power dissipation in digital CMOS circuits can be formally modeled, and its predictable behavior can be explored via SCA [4, 5]. The same occurs with the electromagnetic radiation of the circuit because the electric current variations caused during processing generate proportional variations in the electromagnetic field radiated by the circuit, leaving the system vulnerable to this side-channel as well [6].

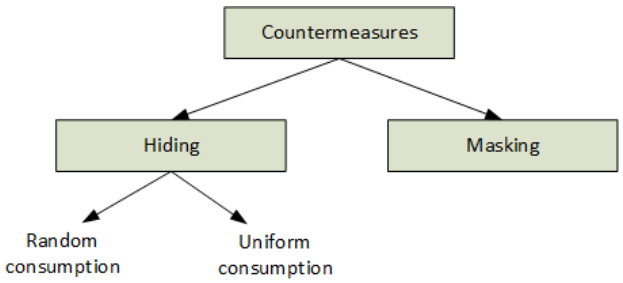

Fig. 1 Countermeasures classified according to Popp and Mangard[3].

Information leakage through side channels has become a concern in digital system design that operates with confidential information such as smart cards. A smart card is an integrated circuit embedded in a plastic card that allows the storage, processing, and communication of data securely in a public communication network. Many works have been proposed to avoid information leakage or neutralize adversaries' actions, proposals known as countermeasures.

Figure 1 presents a classification given by [3] which is well suited to group the strategies used to prevent the leakage of information. According to [3], the hiding strategy can be divided in random consumption, that aims to insert randomness during the execution to ensure that the power dissipation is different in each execution, and in uniform consumption, that aims to ensure that the power dissipation is approximately equal regardless of the data in execution. Conversely, the masking strategy aims to change intermediate data of the circuit to make the dissipation independent of the data in execution, even in a circuit with data-dependent dissipation.

A. Contributions

This work presents a brief survey on hardware countermeasures highlighting the different approaches to mitigate leakage on power dissipation. The main objective is to investigate the various alternatives to reduce the existing correlation between the power dissipation on VLSI systems with the processed data, which allows the attacker to obtain the circuit's secret key. A cost-benefit analysis between area, power, and level of security offered by the method will be presented. In addition, the work analyzes the possibilities of implementing strategies, whether in software or hardware.

Digital Object Identifier 10.29292/jics.v16i2.501

The remaining part of the paper is structured as follows: Section II reviews how power dissipation occurs in CMOS circuits, how to model power consumption, the principle of power analysis attacks and, the primary existing power analysis attacks. Section III presents a survey of countermeasures approaches against power analysis attacks. Section IV summarizes and discusses strategies and critical challenges on mitigating information leakage, and finally, Section V presents the obtained conclusions.

II. Background on power analysis attacks

This section reviews the power dissipation in CMOS, the main power attack strategies and the models used in these. The content of this section serves as a background for the countermeasures section, which is the focus of this review.

A. Power dissipation in CMOS circuits

The total power dissipated by a CMOS circuit is composed mainly by the power in the logic cells, registers, wires and interconnects. Design decisions at different levels of abstraction directly influence the power dissipation and, therefore, the leakage of information, which may be explored in power attacks. As a consequence, countermeasures will be present in different abstraction levels.

As a first order approximation, the power of circuit supplied by a constant voltage V_{DD} with a total current $i_{DD}(t)$ will present an instantaneous power dissipation as P_{Inst} given by the product of V_{DD} and $i_{DD}(t)$. The mean power dissipation P_{Inst} during a period T is defined according to Equation (1).

$$P_{Inst} = \frac{1}{T}\int_0^T p_{Inst}(t)dt \; = \frac{V_{DD}}{T}\int_0^T i_{DD}(t)dt \qquad (1)$$

The total power of a digital circuit can be divided in the static power P_{stat}, which accounts for the consumption while there is no switching activity, and the dynamic power P_{dyn}, which accounts for the consumption while there is switching in the inputs, internal signals or outputs of the circuit.

The static power is dominated by small leakage currents. In the SCAs context, the static power is of great concern as it tends to have a significant correlation with the input data, however the measurement of such small currents imposes a large challenge. The shrinking of transistors due to technology scaling increased the leakage currents to a point that, under the right conditions, they can be properly measured.

The dynamic power dissipates during the switching of the transistors through *High-to-Low* or *Low-to-High* transitions dominates the power in CMOS circuits. The dynamic power is proportional to the clock frequency, the load capacitance and the square of the supply voltage. In a digital circuit, *low-to-high* transitions can be modeled as a capacitive load through the pull-up network, while *high-to-low* transitions result from capacitive discharges through the pull-down network. Such switches lead to very different and distinctive current profiles in the power supply. This issue represents the Achilles heel of digital circuits designed with CMOS technology concerning power analysis attacks.

B. Power dissipation models

As the dynamic power is strongly dependent on the processed data, power analysis attacks were developed to exploit this correlation. The attacks use simplified models to estimate the actual power dissipation. The most used power models are Hamming Weight (HW) and Hamming Distance (HD).

The HW is applicable to predict the power dissipation when the adversary does not know the consecutive values of the data in a target part of the circuit. This model considers that a resulting 0 on a CMOS circuit leads to insignificant power dissipation, whereas a 1 value produces a significant amount of power dissipation. Therefore, this model assumes that the power dissipation is proportional to the number of bits set to 1 for a processed data. Such simplicity makes the HW a attractive model.

The HD is proportional to the number of *low-to-high* and *high-to-low* transitions. This model assumes that the power dissipation for *low-to-high* and *high-to-low* transition produce the same amount of power consumption. Also, it ignores static power dissipation [3]. In this way, the HD model can be simply applied to estimate the power dissipation of a given circuit as shown in Equation (2), where v_0 and v_1 correspond to the HW of the results produced consecutively by the circuit. Therefore, the HD is calculated as the XOR function between the HW of two values, i.e., the difference of HW.

$$HD(v0, v1) = HW(v0) \oplus HW(v1) \qquad (2)$$

The HD and HW models are simple, efficient and widely used for power analysis attacks. Despite this, other models aim to explore specific behaviors of operations performed in both software and hardware. An example is the Zero Value (ZV) model, that exploits a property of the multiplication operation when executed on the value 0 always results in 0 [3].

When it is not possible to correlate the circuit with the previous models, it is possible to build a customized power dissipation model using profiling attacks. Chari et al. [7] highlight that it is possible to make an accurate power dissipation model using statistical techniques and a paired device to be attacked. Other proposals aim to build power dissipation models with different strategies, such as Schindler et al. [8] using stochastic models, and Hospodar et al. [9] using machine learning.

C. Differential Power Analysis

Differential Power Analysis (DPA) has some features that have made it the most popular among SCAs. Firstly, its execution cost is relatively low, and still, it is considered a non-invasive attack for only monitoring the attacked device without the need to investigate internal signals. Furthermore, even in electrical disturbances during the power traces acquisition, it is possible to carry out successful attacks.

DPA exploits the dynamic power dissipation characteristics of CMOS technology, more precisely the premise that *low-to-high* and *high-to-low* transitions cause different consumption. The analysis relates this information leak with

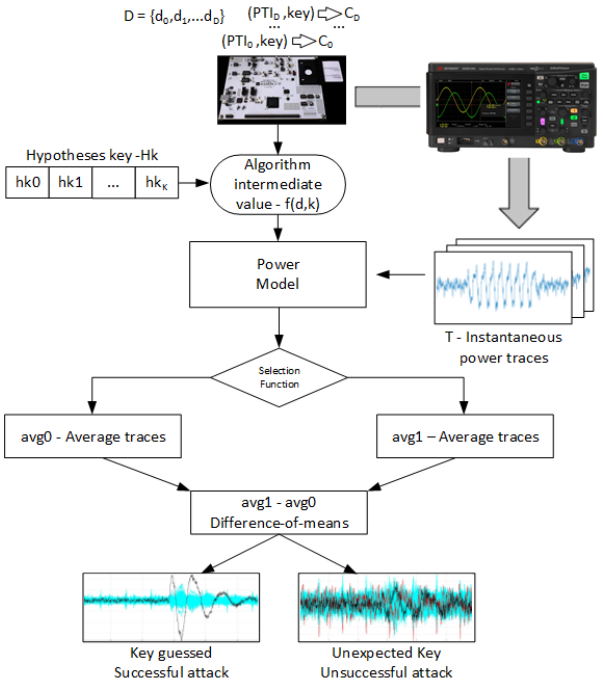

Fig. 2 Differential power analysis overview.

the functional behavior of a digital circuit while data is processed. As proposed to Kocher et al. [5], DPA consists of 5 steps: (i) choosing a target intermediate result, (ii) measuring and collecting traces, (iii) calculating hypothetical intermediate values, (iv) applying the consumption model to the attacked device and (v) evaluating hypotheses of subkeys. An overview of DPA is depicted in Figure 2.

The first step is to choose an intermediate result from the target cryptographic algorithm. This selected result must be a function $f(d,k)$, where k is a portion of the secret key and d is a portion of the known input or output message. If the attacker obtains a function that satisfies this condition, it can be used as the target of the attack to find k. The known message d can be either an incoming message or an outgoing cryptogram, or even other known intermediate data.

In the second step, the power dissipated is measured while various encryptions or decryptions are performed on a set of different data using the same cryptographic key. Thus, D is a set containing random different data d_i, which can be described as follow $D = \{d_0, d_1, ..., d_D\}$. For each encryption or decryption execution, a corresponding power trace is stored. Thus, a set T of power traces is acquired, where each trace t_i is composed by J samples which can be described as $t_ij = \{t_{0,j}, ..., t_{0,J}\}$ for each trace. Finally, these traces are stored in a matrix M_T of size $D \times J$.

The next step consists of calculating hypothetical intermediate results for all possibilities values assumed by k according to $f(d,k)$. Thus, one can define Hk as a set of all possible values assumed by k such that $Hk = \{hk_0, hk_1, ..., hk_K\}$, where K is the total number of key values. Thus, using the set D and the set of hypothetical keys Hk, the attacker can calculate all possible hypothetical intermediate results for $f(d,k)$. A matrix called M_V store the hypothetical intermediate results $v_{i,j}$ as seen in Equation (3), which has the following dimension $D \times K$.

$$M_V = \begin{bmatrix} v_{0,0} & v_{0,1} & v_{0,2} & \cdots & v_{0,K} \\ v_{1,0} & v_{1,1} & v_{1,2} & \cdots & v_{1,K} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ v_{D,0} & v_{D,1} & v_{D,2} & \cdots & v_{D,K} \end{bmatrix} \quad (3)$$

We can observe that each column j of the matrix M_V contains the results calculated for the hypothesis of key hk_j, through $f(d_i, k_i)$. Suppose M_V has intermediate results for all possibilities of key k. In that case, one of its columns has the actual intermediate values calculated by the cryptographic system during data encryption or decryption, performed in the second step.

The secret key is one of the elements contained in Hk. This element is defined as hk_{ck}. Thus, DPA seeks to find out which column of the matrix M_V has the same values produced by $f(d,k)$ during the encryption or decryption of the vector D.

The fourth step of the DPA attack is to define the hypothetical power consumption values from the matrix M_V. This step utilizes the power consumption models. The accuracy level has a direct relation to attack efficiency. The most used models for digital CMOS circuits are HW and HD. Thus, for each hypothetical intermediate values $v_{i,j}$ the defined model is applied according to Equation (2). This produces a matrix M_H with the same dimension as M_V, containing hypothetical power consumption.

The idea to use the difference-of-means method is to determine the relationship between the columns of M_H and T. Based on the assumption that different data leads to other power profiles, for example, when an LSB bit of an intermediate result produces a value of 0, the consumption will be other when this same bit is 1. Based on this assumption, this method proposes the division of the matrix T.

To verify a hypothesis of key hk_{ck}, the method divides T into two groups of power traces according to h_i. One group contains all the lines of T where h_i is 0, and the other group includes the remaining lines. Then, the average trace of each group is calculated, where $avg0$ corresponds to the average of group 0 and $avg1$ to the other group. The difference between avg0 and avg1 indicates whether a correlation exists for the evaluated key hypothesis. The difference between avg0 and avg1 occurs significantly at the moments the intermediate values correspond to h_{ck}. At all other moments, the difference insignificant. If the key hypothesis is not correct, the difference between avg0 e avg1 is more or less zero at all moments.

Finally, the fifth and last step of the DPA attack aims to evaluate the hypotheses of keys hk. Each column h_j of the matrix M_H is compared with the corresponding column t_j of the matrix M_T. In this step, the attacker compares the hypothetical consumption values with the power traces collected from the attacked device. The results are stored in a matrix M_R of size $K \times T$. There are different methods of comparison for this step, depending on the type of attack performed, be it CPA, described in the next section or different-of-means. For example, the popular method of difference-of-means, the result of a DPA attack is a matrix R, where each row of R corresponds to the difference between the $avg0$ and

$avg1$ to each key hypothesis. The correct hypothesis will be the one with the greatest difference value of the means.

Similar to the DPA attack, the Differential Electromagnetic Analysis (DEMA) attack [10] evaluates and monitors the emission of electromagnetic radiation from the attacked device. DEMA attacks capture the traces generated by the electromagnetic fields emitted by the circuits during the execution of encryption or decryption through special probes used in conjunction with amplifier stages due to the low intensity of the produced signal. For this type of attack, the attacker must consider the problems caused by noise and electromagnetic interference from the environment where the attack is carried out, causing errors in the readings of the traces.

D. Correlation Power Analysis

Correlation Power Analysis (CPA) is a power-based attack proposed by [11]. CPA uses a correlation coefficient, the most common way to verify linear relationships between data. In this attack, the correlation coefficient is used to assess the relationship between each column hi of the matrix M_H with each column tj of the matrix T. This results in a comparison between the hypothetical power consumption values and the acquired traces at every time position. The result is stored in a matrix R, where each element represents the estimated correlation coefficients. Thus, one can describe each value $r_{i,j}$ by the Equation (4), where $\bar{h}_i$ and $\bar{t}_j$ represents the mean values of the columns h_i and t_j:

$$r_{i,j} = \frac{\sum_{d=0}^{D}(h_{d,i} - \bar{h_i}) \cdot (t_{d,j} - \bar{t_j})}{\sqrt{\sum_{d=0}^{D}(h_{d,i} - \bar{h_i})^2 \cdot \sum_{d=0}^{D}(t_{d,j} - \bar{t_j})^2}} \quad (4)$$

According to [11] these coefficients, or correlation factors, are capable of rejecting false key hypotheses accepted by the DPA / DEMA.

E. Others power attacks

In addition to the well-known power-based attacks that explore the dynamic power consumption, the Static Power Side-channel Analysis (SPSCA) explores the static power dissipation. While in idle, the leakage current is different and strongly dependent on the input as shown in [12]. This attack is especially efficient on sub-100 nm technologies as the static power increases [13]. Experimental results show that 65 nm is in order of $10\times$ more vulnerable than 90 nm technologies when submitted to SPSCA [14]. Despite this, SPSCA is unpractical in low power dissipation circuits as the values to be measured can be in the order of $\times 10^{-9}$ or even smaller. SPSCA often depends on techniques as clock freeze to allow a viable measurement [15].

Template attack (TA) [7] is a known side-channel attack that explores vulnerabilities of cryptographic circuits whose security is dependent on the assumption that an adversary cannot obtain more than one or a limited number of samples. This attack requires that an adversary has access to an identical experimental device that he can program as he wants. This approach, in contrast to previous attacks, aims at precisely modeling noise and using this to fully extracted information present in a single sample.

Fault injection attacks (FIA), initially introduced by Boneh et al. [16] consists of generating failures in the cryptographic circuit to obtain abnormal behaviors and thereby take advantage of this abnormality to reveal secret information. However, these attacks need to create fault models, requiring particular skills and detailed knowledge of the circuit's internal structure. Its efficiency today represents a threat to the security of cryptographic systems.

Higher-Order Attacks (HODPA) [17] are based on the joint statistical properties of multiple aspects of the signal, joint analysis of power dissipation on two or more points in time. This kind of attack is normally applied to masking countermeasures. It implies higher costs in terms of the number of samples and computational complexity.

There is currently a line of work that explores machine learning and deep learning to attack cryptographic systems. Machine learning (ML) has been used to attack cryptographic circuits similarly to TA attacks, requiring prior training, considered profiled attacks as proposed by Picek et al. [18]. Deep learning (DL) has been applied to SCA mainly because can learn abstract representations that are composed of lower levels features. DL-SCA can be applied to both profiled attacks [19] and non-profiled attacks [20], such as DPA and CPA.

Attacks that explore contemporaneous applications as clouding servers also represent severe threat. Moini et al. successfully retrieved 74% of a victim application image running at amazon web service (AWS) server [2]. The authors explored the cloud service where multi-clients simultaneously operates at the same time. In this case, the attack requires no physical or modifications of any kind over the cloud FPGA.

III. Countermeasures for Power Analysis Attacks

The countermeasures against power analysis attacks are a set of methods introduced to make the power consumption independent of the data executed on cryptographic devices. These strategies can be implemented in both hardware and software. While the software countermeasures have a limited solution space as the software is performed by vulnerable hardware, the hardware ones present a wide design space for the search for solutions to avoid the leakage of information through side-channels. The countermeasures can be clustered by different strategies as depicted in Figure 1. This work presents a survey on the different strategies in order to compare the benefits, limitations, and costs of each solution as follows.

A. Hiding: uniform consumption

This section presents a review of different strategies to reduce leakage targeting an uniform and data-independent power dissipation, i.e., a device should consume equal amounts of energy in each clock cycle, regardless of the data processed. Most studies focus at the gate level design. Such preference occurs as a uniform consumption in the gate level tends to propagate to the system level. Since information leakage is directly associated with differences in the power

consumption produced by low-to-high and high-to-low transitions, dual-rail encoding of information has been usually adopted.

A..1 Dual-rail pre-charge logic - DPL is the encoding scheme most used by secure strategies implemented at gate-level designs. This encoding represents one logical bit of information using two rails, containing the real binary value and its complement as depicted in Figure 3a. The computations are performed in two phases denominated pre-charge and evaluation, which characterize a dynamic logic. Pre-charge propagates before any computation and drives all circuits to the same binary statement, usually zero, known as *all-zeros spacer*, defining the initial statement on both rails. In the literature, it is also known as return-to-zero protocol (RTZ). While the evaluation phase computes the combinational logic function. It is possible to highlight two observations on the influence of this type of logic in the context of countermeasures against power-based attacks:

(i) Limit the attackers' action: The pre-charge phase prevents power-based attacks that estimate power dissipation with the HD model. Computing data from an initial state, all-zeros, prevents transitions from previous data that are sources of information leaks.

(ii) Number of power traces available to perform the attack: the pre-charge phase reduces the number of useful power traces that can be measured. Considering *i* equals to the target input bits, non pre-charged topologies has $2^i \times (2^i - 1)$ possible power traces, while pre-charged countermeasures has only 2^i power traces. For each possible *i* input, the non pre-charged topologies have others $2^i - 1$ previous statement that leads to the respective input. Each of these extra traces leaks more information from the device due to the logic and electrical charges modify according to the previous computation.

A..2 Time Enclosed Logic - TEL is the state-of-the-art encoding to counteract power-based attacks as depicted in Figure 3b. It is based on DPL, but the data are encoded in the time-domain. TEL is synchronized by a clock signal in such a way that 3 phases are required to compute data. An initial pre-charge, such as an RTZ, followed by an evaluation phase where, during a Δ interval, the valid data is properly computed, and, lastly, a post-evaluation phase that makes the rail one logical. This strategy is used to avoid leakage information due to memory effect, i.e. a transition from a valid data to zero. In a clock cycle, to compute any data, TEL starts all rails at logical 0 and ends with all rails at logical 1.

TEL aims to enclose the evaluation phase among two other encoding steps to avoid the adversary to measure it, considering that the attacker has limited time resolution and bandwidth [21]. When compared to DPL, TEL requires $2\times$ more energy per cycle as both tracks are fully charged and discharged. TEL also requires two clock signals to operate, where the second is phased to the first one to generate the Δ. The Δ can also be implemented with a delay element.

A..3 Gate level logic styles - This section reviews proposed works to mitigate information leakage through the logical gate-level design. The secure topologies here presented take advantage of the DPL and TEL targeting a uniform consumption.

Sense Amplifier Based Logic (SABL) is the first topology to counteract dynamic power attacks. SABL is a DPL based topology designed to distribute the small current and internal capacitances by inserting an always ON transistor among the complementary rails [22]. Secure Triple Track Logic (STTL) also implements DPL being the first topology designed to avoid early propagation effects (EPE) [23]. EPE takes place by race conditions caused by propagation time differences between distinct circuit paths producing unwanted switching, also known as glitches, that may propagate along the circuit. EPE is data-dependent which makes it an important source of leakage information. The main drawbacks of STTL are the unbalanced composition among the complementary rails and the high overhead of the output latches. Multi-Threshold Balanced Secure Triple Track Logic (MT-BSTTL) is the first topology to use multi-V_t on power attacks purpose. MT-BSTTL implements multi-V_t and capacitance balancing techniques to minimize the limitations of STTL [24].

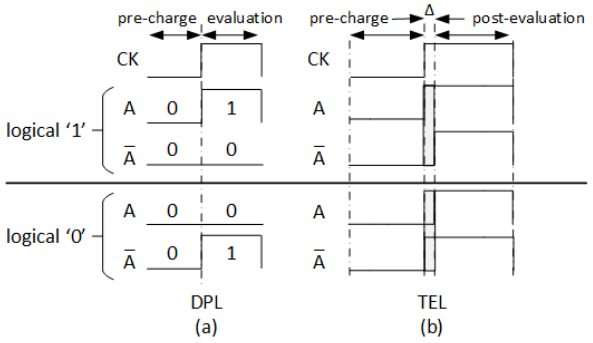

Fig. 3 DPL and TEL encoding.

Dual-spacer Dual-rail Delay-insensitive Logic - (D^3L) proposed by Cilio [25] is a DPL based on asynchronous circuits able to mitigate capacitive unbalances between the dual rails using a dual-spacer protocol to decouple the data correlation with power dissipation during the computation. Furthermore, as asynchronous circuits are strongly data-dependent to compute due to the absence of the clock signal, D^3L inserts random delays to break the timing-data correlation. However, D^3L is implemented based on NULL Convention Logic (NCL) according to a complex design flow. The proposed dual-spacer protocol inserts delay overhead as well as area overhead to asynchronously control the flow of data in the datapath.

Three-phase Dual-rail Pre-charge Logic (TDPL) [26] was designed to be robust to unbalanced routing capacitances which is a concern in DPL circuit design that requires a lot of effort in Place & Route according to [27]. TDPL operates in three phases, pre-charge where all rails are charged to $high$ followed by evaluation where valid data is computed, and lastly, a discharged phase similar to RTZ, doing all rails discharged to low. The TDPL drawback is the area overhead due to the requirement to route the three control signals.

Delay-based Differential Pre-charge Logic (DDPL) [28] implements the time domain for the first time but its implementation suffers from early propagation effect which even results in a data-dependent vulnerability. Improved Delay-based Pre-charge Logic (iDDPL) is the state-of-the-art countermeasure and which implements the time domain encod-

ing, first named here as TEL encoding [29]. Like SABL, iDDPL also implements non-logical transistors among the complementary rail to eliminate the internal memory effects of the gates to solve the problems suffered by DDPL. The authors proved that iDDPL is very resistant even in presence of unbalanced capacitances. For this, the authors performed SPICE simulations and experimental attacks on ASIC @65nm.

Wave Dynamic Differential Logic (WDDL) is the first topology fully implemented with static-CMOS gates available on standard-cell libraries. This compatibility reduces the complexity to design secure circuits due to takes advantage of using the traditional standard-cell design flow. WDDL implements DPL encoding and compared to semi full-custom countermeasures, WDDL cells also insert low overhead [30, 31]. An important drawback of WDDL is the racing condition that makes it susceptible to EPE [32].

Standard-cell delay-based dual-rail pre-charge logic (SC-DDPL) is the state-of-the-art countermeasure implemented since standard-cell. SC-DDPL implements TEL encoding and requires only NAND2 and NAND3 CMOS gates to implement combinational logic. SPICE simulations and experimental results on FPGA have shown that SC-DDPL is resilient even with unbalanced P&R. Combining the lower design effort from the implementation with standard-cell libraries and no need to optimized P&R, SC-DDPL is a straightforward design [33].

A..4 Sizing and Place & Route for semi full-custom topologies - To overcome the unbalance between rails in DPL circuits, some proposals stand out in the literature to find alternatives to enhance the design flow for DPL circuits. For example, the transistor size can change some features of the circuit, such as delay, power dissipation, capacitances, inductive behavior, and area. On the side-channel perspective, each of the cited aspect impact on the current signature.

There are at least three methodologies for security aware sizing. Bhattacharya et al. [34] formulate the sizing problem considering the switching activity of the transistors and the capacitances of each interconnection node of the circuit. In 2009 [35], Lin and Burleson developed an iterative algorithm to resize the higher capacitances gates of the circuit. The algorithm uses a heuristic based on vulnerability metrics and attacks using a predefined level of security as stop criterion. Lima et al. [36] proposed a greedy algorithm based on security metrics and SPICE simulations that clusters sets of transistors according to their similarities in the gate and uses a search heuristic to minimize the leakage on a given logic gate. All three algorithms have shown efficiency to improve the security, at the cost of delay, area, and power dissipation.

The Place & Route (P&R) stages of the design of a secure system can also be improved to minimize the leakage of information in DPLs. Tiri et al. [27] proposed the fat-wire to route the circuit composed by multi-rails topologies, which are the majority of countermeasures on the hiding method. An important benefit of this methodology is the ease of integration with EDA design flow. In the fat-wire methodology, the circuit's netlist (after the logic synthesis) is parsed to the correspondent multi-rails cells. For P&R is used a LEF file with a fat gate library database. The design now is parsed from fat-wire to original technology properties, already with multi-rails placed and routed [37]. The fat-wire strategy guarantees a close matching between the complementary rails since they are routed side-by-side. The similar interconnections reduces the parasitic mismatches which significant increase of robustness, reduction of P&R complexity, smaller congestion, and area.

A specialized P&R can improve the circuit's resilience to both power and electromagnetic vulnerabilities. Ma et al. propose a computer-aided design (CAD) tool that optimizes the placement and the routing steps after the clock tree synthesis, targeting a reduction in electromagnetic leakage [38] [39]. The authors' tool applies the optimizations after achieving other constraints as timing, area, and power. The work uses a numerical optimization method for the placement step that randomly searches for a relative optimum solution. For the routing phase, the algorithm first seeks data-dependent wires considering physical property and then applies wire length adjustment that implies snaking signals. The simulations result reaches a reduction of 67.26% in correlation over unprotected P&R. The security gains are paid with a non-optimal design in terms of traditional performance metrics, generating a increase of 11.7% in the power and a reduction of 22% in the maximum operating frequency in a AES-128 design.

A..5 Current flattening and detached power supply - To hide the leaked information, there is another strategy that aims to flatten the current consumption of a cryptographic circuit to be data independent. Ratanpal et al. [40] propose to use an integrated filter to uniform the current consumption monitored by the adversary. Telandro et al. [41] propose an on-chip voltage regulator to generate an internal power supply voltage from an external power supply aiming to ensure the uncorrelation between the external power supply current and internal power supply current. Plos et al. [42] improves a scheme with two capacitors that supply the target chip in an interleaved fashion, when one supplies the chip the other is being charged. This scheme adds two more phases to the scheme to mitigate the leaked information. In addition, the authors present for the first time results about the security against power-based attacks. Even so, this scheme suffers from current leakage of the off switches which control the charging and discharging of the capacitors and, leakage through the I/O pins. Equalizing consumption with flattening can be costly in energy terms. Therefore, Li et al. [43] propose power-aware hiding (PAH) to balance consumption at the middle level instead of peak energy consumption. It equalizes the power dissipation using an energy-aware strategy reducing the energy penalty produced by current flattening.

Gornik [44] proposes a novel circuit to decouple the main power supply from an internal power supply that is used to drive a single logic gate. The decoupling is done with buffering capacitances integrated into the semiconductor. This approach allows decoupling cells through distributing the decoupling capacitors all over the circuit layout and avoids the requirements of a large capacitor. As a drawback, it imposes an overhead of area. Despite of being a powerful countermeasure against power attacks, these strategies still let the

cryptographic system susceptible to electromagnetic radiation based attacks.

Shan et al. [45] are the first to use machine learning to protect cryptographic hardware against power analysis attacks. The authors propose a power compensation module based on HD redistribution to compensate the probability of the HD of the intermediate data. The results show no correlations up to 1.5 M traces and low costs in terms of area and power dissipation.

B. Hiding: random consumption

Lu et al. [46] investigate the use of random delays insertion (RDI) in cryptographic systems in FPGAs. The authors proved theoretically and experimentally that the technique is effective against power analysis attacks. They also proposed parameters that can be used to optimize the design security in terms of area, performance, and power dissipation. RDI was firstly proposed by Clavier et al. in [47] for software applications to reduce the correlation between a power dissipation model and the power dissipated by the circuit. For this, a chain of programmable delay elements is added to the datapath, to randomize the execution and consequently the power dissipation. The results obtained show that RDI in FPGA reduces the action of the attacks and suffers an area penalty of up to 100%, a relatively low cost compared to other methods. Accordingly [48], pre-processing applied before power attacks have proven that this kind of randomness can be removed and the architecture remains vulnerable to attacks.

Soares et al. [49] propose an architectural solution designed in globally asynchronous and locally synchronous design (GALS) style. In this way, it is possible to combine the random clock and parallel processing in a pipeline architecture to introduce noise into global consumption. On the other hand, Ambrose et al. [50] exploit the parallel processing of a dual-core architecture to introduce noise into power dissipation. While one core processes the data, another core processes the complemented data in parallel. Recently, Moucha et al. [51] propose to use additional dummy rounds in cipher block algorithm to generate noise. These proposals present high costs in area and power. Moreover, also leak information to be obtained with pre-processing steps.

Baylis et al. [52] proposed the insertion of a hardware overlay layer as a way to create a level of abstraction for the configurable logic blocks of the FPGA. The method has two main objectives, firstly to protect the IP cores belonging to the hardware architecture implemented in FPGA from reverse engineering attacks that are capable of identifying the IP cores used in the architecture from the bitstream. The other objective is to insert extra hardware to generate noise and thus reduce the action of the power analysis attacks. The hardware virtualization method uses a ring oscillator as a generator noise. This kind of noise can easily be neutralized by pre-processing techniques applied before the attack according to [48]. Although the method is restricted to architectures implemented in FPGA, it is possible to combine overlay with other countermeasures such as d^th-orders masking which can be more effective to hide the information leak.

Lagasse et al. [53] proposed the combination of two methods for generating noise and randomness in the execution of the Advanced Encryption Standard (AES) cryptographic algorithm implemented in hardware and prototyped in FPGA. The first method is to use a random clock, i.e. a random selection from 4 different phases clock signals from an linear-feedback shift register (LFSR). The other method is a noise generator from a ring oscillator. The authors evaluated the impact on the security of each method applied individually in a hardware implementation of the AES algorithm, as well as the combination of the methods. The results highlight gain in security with the combination of the methods. As an advantage, the method has no significant impact on the area.

Das et al. [54] proposed a method of attenuating energy consumption and inserting noise as a way of hiding information leakage. The method called Attenuated Signature Noise Injection (ASNI) consists of hardware that suppresses electric current variations caused by the computation of the cryptographic algorithm and simultaneously adds a noise injection method to hide the power consumption of the computed algorithm. The results obtained on AES algorithm show that the proposed method has a low impact in area and immunity to CPA with up to 1M traces.

Alternatively, we find in the literature circuits dedicated only to produce noise as proposed by Liu et al. [55]. In this work, the authors use ring oscillators for this purpose. The frequency of the clock signal directly influences the power dissipation of a circuit. Thus, several works in the literature explore this strategy in different ways as recently Jayasinghe et al. [56], Hettwer et al. [57]. These approaches exploit the configurable clock management available in FPGAs to dynamically generate clock signals with a large frequency spectrum. While the approach is promising, for ASIC designs it involves building the entire structure which can be costly.

The converter-reshuffling technique uses a multi-phase switched capacitor voltage converter to insert noise power dissipation in the circuit. Yu and Köse [58] improve this technique by utilizing flying capacitors to withhold a random amount of charge for a random time period to counteract power analysis attacks. Machine learning attacks have the potential to unscramble the noise generated.

Singh et al. [59] use an all-digital low-dropout regulator combined with two randomization circuits, being a switching noise injector and the randomized reference voltage to hide information leakage. The authors show that the combination of the circuits can dynamically change the power signature and difficult the attacks.

Chong et al. [60] propose an asynchronous logic design dedicated to FPGA with dual hiding countermeasures, an amplitude moderation, and a time moderation. It is the first asynchronous AES design evaluated at the first and last rounds of the algorithm. The authors point out that after various power analysis attacks the design is unbreakable with less than 1 M traces. Despite this, the project presents a complex asynchronous circuit design.

C. Masking

Masking aims to randomize the intermediate value using mask bits to modify the real data being computed on the attacked circuit [3]. The idea is to perform all the vulnerable computations on masked data produced by a random mask.

Generally, logic operations such as XOR, AND, and arithmetic operations are executed between the mask and sensible data. The masking scheme first proposed by Chari et al. [61] splits every sensitive intermediate variable into s shares, such that an adversary probing at most v values during the computation is not able to correlate with the sensitive information.

Masking may be applied to the algorithmic level or a circuit level. Algorithm masking methods are vulnerable to DPA, and TA according to [62]. Masking at the circuit level is algorithm agnostic and more amenable to design automation compared to masking at the algorithm level [63]. High-order masking, when d levels of masking operations are applied, offers higher resistance against the power analysis attacks. However, it is difficult to implement in hardware due to the significant increase in design complexity [64].

In the literature, d^{th}-order masking schemes are regarded as theoretically secure methods for protecting the implementations of different encryption algorithms. However, there is a gap between practical and theoretical security. Thus, Ming et al. [65] proposed a sensitive glitch location (SGL) method to locate the leakage points in hardware implementations of encryption algorithms. SGL can locate the d^{th}-order masking scheme, d is the higher bound of the number of probes in the masking scheme. SGL can be used as an evaluation tool in chip design to help designers exploring the vulnerabilities in their hardware implementations [65].

There are many proposed masking schemes in the literature [66] [67] [68]. As a general case of the masking strategy, it is possible to highlight the work proposed by Prouff and Rivain [66]. The strategy uses SBOX as a case study of a block cipher algorithm, where k and pti respectively represent plaintext and key inputs. In the proposal, the function $pti \oplus m_i$ represents the masked plaintext using the random mask m_i. Then, SBOX is computed on the masked plaintext and the key in order to obtain $SBOX((pti \oplus m_i) \oplus k)$. Parallel to this function, a correction term is also computed during the SBOX encryption process to ensure that the output result from SBOX produces the original value, in order not to alter the rest of the algorithm's execution. A XOR function between the masked variable and its corresponding mask mi must produce the original value. In this scheme, a pre-computed SBOX' function produces the term $z_i = SBOX'(((pti \oplus m_i) \oplus k) \otimes m_i)$ which is used for this purpose. In this way, it is possible to affirm that the result of the application of the XOR function between the $SBOX(pti \oplus m_i \oplus k)$ output and the z_i term produces the original term expected for the encryption output.

Ishay, Sahai, and Wagner (ISW) [69] proposed a theoretical study of the security of cryptographic systems, where attackers have the ability to monitor a bounded number of wires of the target circuit. The authors proposed a framework that allows employing several techniques for the construction of circuits that require the confidentiality of processed information and that are resistant to power analysis channels. The work presents a systematic study of the complexity of the obtained circuits, and in addition, they show a formal threat model that is used to measure the security of the circuits obtained with the framework. ISW requires decomposing a circuit into AND, XOR, and NOT gates and then compute masking. It reflects on area overhead and sources of glitches.

Coron et al. [68] describes a new algorithm for masking look-up tables of block-ciphers at any order, as a countermeasure against side-channel attacks. The technique is a generalization of the classical randomized table countermeasure against first-order attacks. They prove the security of their new algorithm against d^{th}-order attacks in the usual ISW model [69]. We also improve the bound on the number of shares from $n > 4^{th}$ for an adversary who can adaptively move its probes between successive executions such as HODPA [17].

Rivain and Prouff [67] presented the first masking scheme dedicated to AES algorithm which is provably secure at any chosen order and which can be implemented in software at the cost of a reasonable overhead.

Masked Dual Rail Pre-charge Logic (MDPL) is a combination of masking and dual-rail pre-charge [70]. MDPL works similarly to WDDL which employs data-independent output switching activity to resist power analysis attacks using a single random mask bit to overcome the routing imbalance problem. As a disadvantage, MDPL suffers from EPE-based attacks. iMDPL is proposed to overcome this attack but has a significant area overhead. Furthermore, MDPL suffers from leakage of the mask bit.

Miyajan et al. [71] present a technique to reduce the execution time of the AES algorithm when implementing high order masking countermeasure. The proposed work aims at software implementations and explores the use of SIMD instructions (single instructions multiple data) available in some processor architectures. The basic concept is to replace the lookup tables used to implement non-linear functions of the AES algorithm such as SBOXs by including SIMD instructions. The approach allows mitigating power analysis attacks with the use of high-order masking, and to mitigate cache attacks by reducing the execution time of the algorithm.

Cedric [72] proposed a method called Orthogonal Direct Sum Masking (ODSM) to resist against SCA and FIA attacks, but its implementation in the whole algorithm is a big open problem when no particular hardware protection is possible. The method is designed as a software masking scheme of AES transformations. It is able to detect and correct errors that can be injected, and furthermore, minimize the costs in terms of memory and computing time as well.

The bus-invert coding technique is proposed as a lightweight countermeasure against power analysis attacks according to Vosoughi et al. [73]. This technique is a low-cost countermeasure similar to the masking technique with reduced overhead. The main idea is to reduce the number of *low-to-high* and *high-to-low* transitions in a circuit. when the number of expected transitions is larger than a threshold HW, the input is coded and processed in order to reduce the transitions required. The authors showed that the number of the measurements to disclose the secret key an SBOX of the AES algorithm can be 571 times than a naive implementation and with a 0.91% reduction in power dissipation.

Ueno et al. [74] propose an AES hardware architecture

Table I. Summary of revised countermeasures.

Summary of countermeasures based on uniform consumption			
Paper	**Method**	**Contributions**	**Limitations**
[22]	SABL	First DPL	Unbalance capacitances
[23]	STTL	Triple rail with validation	Area and delay due to validation rail
[25]	D^3L	Dual spacer asynchronous logic	Delay, area and power overhead
[26]	TDPL	Three phase operation	Extra area and power consumption to route 3 control signals
[28]	DDPL	Time domain signaling using single control signal	Stable control for Δ evaluation
[29]	iDDPL	DDPL immune to EPE	Stable control for Δ evaluation
[30]	WDDL	First DPL implemented with static CMOS	Early Propagation Effect
[33]	SC-DDPL	Flow Standard-Cell to implement DDPL & Route	Stable control for Δ evaluation Δ evaluation
[40]	Current flattening	Filter the electrical current to make it uniform	High power
[41]	Current flattening	Voltage regulator to uniform power dissipation	High power
[42]	Detached power supply	Detached power supply with additional capacitor discharge phase	Capacitor discharge leaks information; Not effective against EM attacks
[44]	Detached power supply	Buffering capacitances	Area overhead; Not effective against EM attacks
[45]	Power compensation module	First machine learning assisted power compensation circuit	DL-SCA can potentially find leaks
Summary of countermeasures based on random consumption			
Paper	**Method**	**Contributions**	**Limitations**
[46]	Random Delay Insertion - RDI	Inserts random delay on the datapath	Area and delay overhead
[49]	GALS Pipeline	Combines random clock and parallel processing	Pre-processing may realign traces and area overhead
[50]	Parallel processing	Dual-core to parallel processing	Pre-processing may remove noise
[51]	Dummy round scheme	Improvements on dummy round scheme	Delay and area overhead
[52]	Hardware virtualization	Hardware overlay layer for noise generation	Area overhead; Filters may remove noise
[53]	Combines two methods	Random clock and ring oscillator noise	Area overhead; Filters may remove noise
[54]	ASNI	Energy consumption reduction and noise insertion	Filter may remove noise
[55]	Ring oscillators	Digital controlled ring oscillators	Filters may remove the noise
[56]	Random Frequency - RFTC	Dynamic clock reconfiguration for FPGA	Limited to FPGAs and costly for ASICs
[57]	Dynamic Frequency Randomization	Applies Dynamic clock management to generate a wide clock frequencies	Limited to FPGAs and costly for ASICs
[58]	Converter-Reshufflin - CoRe	Core technique with flying capacitors withhold random charge	Leakage on flying capacitors
[59]	Integrated all-digital LDO	Combines low-dropout regulator, switching noise injector and randomize reference voltage	Complex design and pseudo-random noise injection
[60]	Dual-hiding async-logic	Amplitude and time moderation using asynchronous circuits	Complex design flow and area overhead
Summary of countermeasures based on masking consumption			
Paper	**Method**	**Contributions**	**Limitations**
[66]	Xor with PTI and Key	Lightweight masking scheme	Needs a reverse function
[68]	Masking LUT for block cipher	Improves security and performance of ISW model	Requires more random generations
[69]	Random states, delays, and bits	Formal threat model	Restricted observation of t-wires within a clock cycle - need to refresh the masks
[70]	MDPL	Combines DPL and masking to randomize power consumption	Early Propagation Effect, area overhead
[71]	SIMD instructions to replace and improve SBOXs implementations	Reduces execution time	Designed for software implementations
[72]	ODMS	Able to detect errors	Designed for software implementations
[73]	Bus-invert coding	Lightweight masking scheme	Hardware implementation
[74]	Threshold Implementation - TI	Combines TI and algebraic characteristics of AES SBOX; Attenuates latency overhead	Latency overhead due to serial computing
[75]	Threshold Implementation - TI	First 2-Shares TI	Latency and area overhead

resistant to power analysis attacks based on threshold implementation (TI), considered the state-of-the-art in masking schemes. TI is designed to deal with non-idealities in hardware and to be able to apply masking at a higher level of abstraction. The proposal combines TI implementation and the algebraic characteristics of AES SBOX. The results highlight a small area overhead and reduced latency compared to conventional TI implementations. With the same goal, Chen et al. [75] propose the first TI limited to 2-shares (2-TI) to attenuate the impacts on the area and latency overhead to implement a secure cryptographic circuit. Chen et al. show that 2-TI is first-order secure and also reduces the size of the sequential logic in hardware implementations.

IV. Summary of Countermeasures and Discussions

The countermeasures against power analysis attacks are summarized in Table I. It summarizes the main strategies found for each group of countermeasures. Initially, it is important to highlight that all proposals contribute to reducing information leakage, but they are not completely secure solutions. After reviewing the literature, it is possible to conclude that even though these methods provide some resilience to different types of attacks, they pay for security with penalties like power, performance, and area overhead.

A traditional countermeasure is to randomize sensitive variables by masking techniques. The architecture still leaks information but the masked sensitive data confuse the ad-

versary to correlate it with power dissipated. In the literature, there are masking schemes implemented in software and hardware. Hardware masking is expensive in terms of area and admits some flaws. As the shares are usually computed at the same time, the instantaneous leakage is dependent on the sensitive variables, which allows some dedicated attacks, such as higher-order attacks [17]. On the other hand, software masking impacts the timing performance and the memory requirements, but in terms of security, it is wide usually to protect block cipher algorithm implementations.

As can be observed in Table I, there are different strategies to obtain uniform power dissipation. Most of these strategies focus on the design at the gate level where there are different logic styles. As the logic styles are dual-rail encoded, serious challenges appear in the Place & Route stage to maintain a required balance between rails. In this context, TEL encoding presents itself as a tolerant alternative to unbalanced path problems. Nevertheless, there is a design complexity inherent in computing only in the Δ period of the evaluation phase.

Alternatively, the current flattening strategy implies high power dissipation, due to equalizing the consumption to the maximum peak required by the circuit. Furthermore, the mechanisms for regulating the current flow still leak information, which keeps the design vulnerable. To detach the power supply appears as another alternative solution. However, it is composed of capacitive cells that should be recharged frequently. The on-chip design of large capacitors demands extra area, and the mechanism to control the capacitor's recharge should be very efficient to does not leak information.

The proposals to randomize power dissipation focus on varying the clock frequency as well as adding extra hardware to parallel compute simultaneously to produce noise. Proposals that compute with a limited amount of frequency can have their effects canceled by pre-processing and become vulnerable. Just processing in parallel does not prevent the attack from taking action. Attacks with a pre-processing and a large number of traces, over 1M, have been successful [48][56].

V. Conclusion and Future Research

In this paper, we describe the three main strategies related to counteracting power analysis attacks. The fundamental issues of information leakage are presented as well as how each strategy acts in such a way to hinder the action of power analysis attacks. Then we present a survey of the approaches to mitigate leakage information so that designers can take it into account when constructing secure cryptographic circuits. In order to help designers to decide the right countermeasures to cope with the threats, this paper describes some solutions presented in the literature. A summary table compiles the main contributions, limitations, and costs associated with the countermeasures. Further, the designers can make use of this survey to propose new robust solutions.

Acknowledgements

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. The authors would like to thank PPGC and UFPel for support our research. R. Lellis would like to thank the IFSUL for his license to pursuing the Ph.D.

References

[1] P. Arpaia, F. Bonavolontà, and A. Cioffi, "Security vulnerability in internet of things sensor networks protected by advanced encryption standard," in *2020 IEEE Int. Workshop on Metrology for Industry 4.0 IoT*, 2020, pp. 452–457.

[2] S. Moini, S. Tian, D. Holcomb, J. Szefer, and R. Tessier, "Power side-channel attacks on bnn accelerators in remote fpgas," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, 2021.

[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, 1st ed. Springer Publishing Company, Incorporated, 2007.

[4] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology — CRYPTO '96*, N. Koblitz, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1996, pp. 104–113.

[5] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 388–397.

[6] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems — CHES 2001*, Ç. K. Koç, D. Naccache, and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 251–261.

[7] S. Chari, J. R. Rao, and P. Rohatgi, "Template attacks," in *Revised Papers from the 4th Int. Workshop on Cryptographic Hardware and Embedded Syst.*, ser. CHES '02. Berlin, Heidelberg: Springer-Verlag, 2002, p. 13–28.

[8] W. Schindler, K. Lemke, and C. Paar, "A stochastic model for differential side channel cryptanalysis," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, J. R. Rao and B. Sunar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 30–46.

[9] G. Hospodar, B. Gierlichs, E. Mulder, I. Verbauwhede, and J. Vandewalle, "Machine learning in side-channel analysis: A first study," *J. Cryptographic Engineering*, vol. 1, pp. 293–302, 12 2011.

[10] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, "The em side–channel(s):attacks and assessment methodologies," in *Proc. of the Cryptographic Hardware and Embedded Syst. - CHES*. Springer, 2008, pp. 29–45.

[11] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," in *Cryptographic Hardware and Embedded Systems - CHES*. IACR, 2004, pp. 16–29.

[12] A. Abdollahi, F. Fallah, and M. Pedram, "Leakage current reduction in cmos vlsi circuits by input vector control," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 12, no. 2, pp. 140–154, 2004.

[13] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 2, pp. 355–367, 2009.

[14] T. Moos, "Static power sca of sub-100 nm cmos asics and the insecurity of masking schemes in low-noise environments," *IACR Trans. on Cryptographic Hardware and Embedded Syst.*, pp. 202–232, 2019.

[15] T. Moos, A. Moradi, and B. Richter, "Static power side-channel analysis—an investigation of measurement factors," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 28, no. 2, pp. 376–389, 2019.

[16] D. Boneh, R. A. DeMillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in *Advances in Cryptology — EUROCRYPT '97*, W. Fumy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 37–51.

[17] E. Peeters, F.-X. Standaert, N. Donckers, and J.-J. Quisquater, "Improved higher-order side-channel attacks with fpga experiments," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, J. R. Rao and B. Sunar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 309–323.

[18] S. Picek, A. Heuser, A. Jovic, S. A. Ludwig, S. Guilley, D. Jakobovic, and N. Mentens, "Side-channel analysis and machine learning: A practical perspective," in *2017 Int. Joint Conf. on Neural Networks (IJCNN)*, 2017, pp. 4095–4102.

[19] R. Benadjila, E. Prouff, R. Strullu, E. Cagli, and C. Dumas, "Deep learning for side-channel analysis and introduction to ascad database," *J. of Cryptographic Engineering*, vol. 10, no. 2, pp. 163–188, 2020.

[20] B. Timon, "Non-profiled deep learning-based side-channel attacks with sensitivity analysis," *IACR Trans. on Cryptographic Hardware and Embedded Syst.*, vol. 2019, no. 2, pp. 107–131, Feb. 2019. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/7387

[21] D. Bellizia, G. Scotti, and A. Trifiletti, "TEL logic style as a countermeasure against side-channel attacks: Secure cells library in 65nm CMOS and experimental results," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3874–3884, 2018.

[22] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. of the 28th European solid-state circuits conf.* IEEE, 2002, pp. 403–406.

[23] A. Razafindraibe, M. Robert, and P. Maurine, "Improvement of dual rail logic as a countermeasure against DPA," in *Proc. of the IFIP Int. Conf. on Very Large Scale Integration*, Oct 2007, pp. 270–275.

[24] V. G. Lima, G. Paim, R. Wuerdig, L. M. G. Rocha, L. da Rosa Júnior, F. Marques, V. V. de Almeida Camargo, E. Costa, R. Soares, and S. Bampi, "Enhancing Side Channel Attack-Resistance of the STTL Combining Multi-Vt Transistors with Capacitance and Current Paths Counterbalancing," *J. of Integrated Circuits and Syst.*, vol. 15, no. 1, pp. 1–11, 2020.

[25] W. Cilio, M. Linder, C. Porter, J. Di, D. R. Thompson, and S. C. Smith, "Mitigating power- and timing-based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic," *Microelectronics J.*, vol. 44, no. 3, pp. 258–269, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0026269212002418

[26] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Cryptographic Hardware and Embedded Systems - CHES 2006*, L. Goubin and M. Matsui, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 232–241.

[27] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Smart Card Research and Advanced Applications VI*, J.-J. Quisquater, P. Paradinas, Y. Deswarte, and A. A. El Kalam, Eds. Boston, MA: Springer US, 2004, pp. 143–158.

[28] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 19, no. 7, pp. 1147–1153, 2011.

[29] D. Bellizia, G. Scotti, and A. Trifiletti, "Tel logic style as a countermeasure against side-channel attacks: Secure cells library in 65nm cmos and experimental results," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3874–3884, 2018.

[30] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure dpa resistant asic or fpga implementation," in *Proc. Design, Automation and Test in Europe Conf. and Exhibition*, vol. 1, 2004, pp. 246–251 Vol.1.

[31] K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 7, pp. 1197–1208, 2006.

[32] F. Zhang, B. Yang, B. Yang, Y. Zhang, X. Ren, S. Bhasin, and K. Ren, "Design and Evaluation of Fluctuating Power Logic to Mitigate Power Analysis at the Cell Level," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, 2020.

[33] D. Bellizia, S. Bongiovanni, M. Olivieri, and G. Scotti, "Sc-ddpl: A novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 7, pp. 2317–2330, 2020.

[34] K. Bhattacharya and N. Ranganathan, "A linear programming formulation for security-aware gate sizing," in *Proc. of the 18th ACM Great Lakes Symp. on VLSI*, 2008, pp. 273–278.

[35] L. Lin and W. Burleson, "Analysis and mitigation of process variation impacts on power-attack tolerance," in *Proc. of the 46th annu. design automation conf.*, 2009, pp. 238–243.

[36] V. G. Lima, P. Finkenauer, V. V. Camargo, F. S. Marques, L. R. Júnior, and R. I. Soares, "A novel sizing method aiming security against differential power analysis," in *2018 25th IEEE Int. Conf. on Electronics, Circuits and Syst. (ICECS)*. IEEE, 2018, pp. 429–432.

[37] K. Tiri and I. Verbauwhede, "A vlsi design flow for secure side-channel attack resistant ics," in *Design, Automation and Test in Europe*. IEEE, 2005, pp. 58–63.

[38] H. Ma, J. He, Y. Liu, L. Liu, Y. Zhao, and Y. Jin, "Security-driven placement and routing tools for electromagnetic side-channel protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 6, pp. 1077–1089, 2020.

[39] H. Ma, J. He, M. Panoff, Y. Jin, and Y. Zhao, "Automatic on-chip clock network optimization for electromagnetic side-channel protection," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, 2021.

[40] G. Ratanpal, R. Williams, and T. Blalock, "An on-chip signal suppression countermeasure to power analysis attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 1, no. 3, pp. 179–189, 2004.

[41] V. Telandro, E. Kussener, A. Malherbe, and H. Barthelemy, "On-chip voltage regulator protecting against power analysis attacks," in *2006 49th IEEE Int. Midwest Symp. on Circuits and Syst.*, vol. 2, 2006, pp. 507–511.

[42] T. Plos, "Evaluation of the detached power supply as side-channel analysis countermeasure for passive uhf rfid tags," in *Topics in Cryptology – CT-RSA 2009*, M. Fischlin, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 444–458.

[43] X. Li, C. Yang, J. Ma, Y. Liu, and S. Yin, "Energy-efficient side-channel attack countermeasure with awareness and hybrid configuration based on it," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst*, vol. 25, no. 12, pp. 3355–3368, 2017.

[44] A. Gornik, A. Moradi, J. Oehm, and C. Paar, "A hardware-based countermeasure to reduce side-channel leakage: Design, implementation, and evaluation," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 8, pp. 1308–1319, 2015.

[45] W. Shan, S. Zhang, J. Xu, M. Lu, L. Shi, and J. Yang, "Machine learning assisted side-channel-attack countermeasure and its application on a 28-nm aes circuit," *IEEE J. Solid-State Circuits*, vol. 55, no. 3, pp. 794–804, 2020.

[46] Yingxi Lu, M. P. O'Neill, and J. V. McCanny, "Fpga implementation and analysis of random delay insertion countermeasure against dpa," in *2008 Int. Conf. on Field-Programmable Technology*, 2008, pp. 201–208.

[47] C. Clavier, J.-S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Cryptographic Hardware and Embedded Systems — CHES 2000*, Ç. K. Koç and C. Paar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 252–263.

[48] R. Lellis, R. I. Soares, and A. Souza, "An energy-based attack flow for temporal misalignment coutermeasures on cryptosystems," in *2017 IEEE Int. Symp. on Circuits and Syst. (ISCAS)*, 2017, pp. 1–4.

[49] R. Soares, N. Calazans, F. Moraes, P. Maurine, and L. Torres, "A robust architectural approach for cryptographic algorithms using gals pipelines," *IEEE Des. Test Comput.*, vol. 28, no. 5, pp. 62–71, 2011.

[50] J. Ambrose, R. Ragel, S. Parameswaran, and A. Ignjatovic, "Multiprocessor information concealment architecture to prevent power analysis-based side channel attacks," *IET Computers Digital Techniques*, vol. 5, pp. 1–15(14), January 2011. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-cdt.2009.0097

[51] P. Moucha, S. Jerábek, and M. Novotný, "Novel dummy rounds schemes as a dpa countermeasure in present cipher," in *2020 23rd Int. Symp. on Design and Diagnostics of Electronic Circuits Syst. (DDECS)*, 2020, pp. 1–4.

[52] A. Baylis, G. Stitt, and A. Gordon-Ross, "Overlay-based side-channel countermeasures: A case study on correlated noise generation," in *2017 IEEE 60th Int. Midwest Symp. on Circuits and Syst. (MWSCAS)*, 2017, pp. 1308–1311.

[53] J. Lagasse, C. Bartoli, and W. Burleson, "Combining clock and voltage noise countermeasures against power side-channel analysis," in *2019 IEEE 30th Int. Conf. on Application-specific Syst., Architectures and Processors (ASAP)*, vol. 2160-052X, 2019, pp. 214–217.

[54] D. Das, S. Maity, S. B. Nasir, S. Ghosh, A. Raychowdhury, and S. Sen, "Asni: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, 2018.

[55] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A low overhead dpa countermeasure circuit based on ring oscillators," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 57, no. 7, pp. 546–550, 2010.

[56] D. Jayasinghe, A. Ignjatovic, and S. Parameswaran, "Rftc: Runtime frequency tuning countermeasure using fpga dynamic reconfiguration to mitigate power analysis attacks," in *2019 56th ACM/IEEE Design Automation Conf. (DAC)*, 2019, pp. 1–6.

[57] B. Hettwer, K. Das, S. Leger, S. Gehrer, and T. Güneysu, "Lightweight side-channel protection using dynamic clock randomization," in *2020 30th Int. Conf. on Field-Programmable Logic and Applications (FPL)*, 2020, pp. 200–207.

[58] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Trans. Circuits Syst., II, Exp. Briefs*, vol. 63, no. 5, pp. 438–442, 2016.

[59] A. Singh, M. Kar, V. C. K. Chekuri, S. K. Mathew, A. Rajan, V. De, and S. Mukhopadhyay, "Enhanced power and electromagnetic sca resistance of encryption engines via a security-aware integrated all-digital ldo," *IEEE J. Solid-State Circuits*, vol. 55, no. 2, pp. 478–493, 2020.

[60] K.-S. Chong, J.-S. Ng, J. Chen, N. K. Z. Lwin, N. A. Kyaw, W.-G. Ho, J. Chang, and B.-H. Gwee, "Dual-hiding side-channel-attack resistant fpga-based asynchronous-logic aes: Design, countermeasures and evaluation," *IEEE Trans. Emerg. Sel. Topics Circuits Syst.*, vol. 11, no. 2, pp. 343–356, 2021.

[61] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," in *Advances in Cryptology — CRYPTO' 99*, M. Wiener, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 398–412.

[62] M. Renauld, F.-X. Standaert, and N. Veyrat-Charvillon, "Algebraic side-channel attacks on the aes: Why time also matters in dpa," in *Cryptographic Hardware and Embedded Systems - CHES 2009*, C. Clavier and K. Gaj, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 97–111.

[63] J.-S. Coron, E. Prouff, M. Rivain, and T. Roche, "Higher-order side channel security and mask refreshing," in *Fast Software Encryption*, S. Moriai, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 410–424.

[64] P. De, U. Parampalli, and C. Mandal, "Secure path balanced bdd-based pre-charge logic for masking," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 4747–4760, 2020.

[65] T. Ming, L. Yanbin, Z. Dongyan, L. Yuguang, Y. Fei, and Z. Huanguo, "Leak point locating in hardware implementations of higher-order masking schemes," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 12, pp. 3008–3019, 2018.

[66] E. Prouff and M. Rivain, "A generic method for secure sbox implementation," in *Information Security Applications*, S. Kim, M. Yung, and H.-W. Lee, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 227–244.

[67] M. Rivain, E. Dottax, and E. Prouff, "Block ciphers implementations provably secure against second order side channel analysis," in *Fast Software Encryption, 15th Int. Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, ser. Lecture Notes in Computer Science, vol. 5086. Springer, 2008, pp. 127–143. [Online]. Available: https://iacr.org/archive/fse2008/50860118/50860118.pdf

[68] J.-S. Coron, "Higher order masking of look-up tables," in *Advances in Cryptology – EUROCRYPT 2014*, P. Q. Nguyen and E. Oswald, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 441–458.

[69] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Advances in Cryptology - CRYPTO 2003*, D. Boneh, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 463–481.

[70] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: Dpa-resistance without routing constraints," in *Cryptographic Hardware and Embedded Systems – CHES 2005*, J. R. Rao and B. Sunar, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 172–186.

[71] A. Miyajan, Z. Shi, C. Huang, and T. F. Al-Somani, "An efficient high-order masking of aes using simd," in *2015 Tenth Int. Conf. on Computer Engineering Systems (ICCES)*, 2015, pp. 363–368.

[72] T. Cedric, C. Carlet, S. Guilley, and A. Daif, "Polynomial direct sum masking to protect against both sca and fia," *J. of Cryptographic Engineering*, vol. 9, 09 2019.

[73] M. A. Vosoughi, L. Wang, and S. Köse, "Bus-invert coding as a low-power countermeasure against correlation power analysis attack," in *2019 ACM/IEEE Int. Workshop on Syst. Level Interconnect Prediction (SLIP)*, 2019, pp. 1–5.

[74] R. Ueno, N. Homma, and T. Aoki, "Toward more efficient dpa-resistant aes hardware architecture based on threshold implementation," in *Constructive Side-Channel Analysis and Secure Design*, S. Guilley, Ed. Cham: Springer Int. Publishing, 2017, pp. 50–64.

[75] C. Chen, M. Farmani, and T. Eisenbarth, "A tale of two shares: Why two-share threshold implementation seems worthwhile—and why it is not," in *Advances in Cryptology – ASIACRYPT 2016*, J. H. Cheon and T. Takagi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 819–843.