A Hardware-based Countermeasure to Reduce Side-Channel Leakage

– Design, Implementation, and Evaluation –

Andreas Gornik*, Amir Moradi†, Jürgen Oehm*, Christof Paar†, *Fellow, IEEE*
*Analogue Integrated Circuits Research Group, Ruhr-Universität Bochum, Germany
†Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
{andreas.gornik, j.oehm}@ais.rub.de {amir.moradi, christof.paar}@rub.de

***Abstract*—Side-channel attacks are one of the major concerns for security-enabled applications as they make use of information leaked by the physical implementation of the underlying cryptographic algorithm. Hence, reducing the side-channel leakage of the circuits realizing the cryptographic primitives is amongst the main goals of circuit designers. In this work we present a novel circuit concept, which decouples the main power supply from an internal power supply that is used to drive a single logic gate. The decoupling is done with the help of buffering capacitances integrated into semiconductor. We also introduce – compared to the previously known schemes – an improved decoupling circuit which reduces the crosstalk from the internal to the external power supply. The result of practical side-channel evaluation on a prototype chip fabricated in a 150 nm CMOS technology shows a high potential of our proposed technique to reduce the side-channel leakages.**

***Index Terms*—side-channel analysis, side-channel countermeasure, circuit-level countermeasure, ASIC, hardware-based countermeasure.**

I. Introduction

State-of-the-art differential power analysis attacks (so called DPA [1]) exploit information related to the device internals which leak through its power consumption. Nowadays, counteracting DPA attacks is a must for cryptographic devices which may fall into the hands of an adversary. Until recently several schemes to counteract such attacks at different levels of abstraction have been proposed. One well-known category of countermeasures – called *masking* (secret sharing) – try to provide resistance by randomizing the intermediate values of the underlying algorithm [2]. Introducing noise [3], [4] and randomizing the program flow or the order of the operations [4], [5] fit into the category of *hiding* which aim at reducing the data dependency of the power consumption measurable by the adversary. At the same category there exist other schemes which intend to solve the problem from scratch by equalizing the power consumption of the circuit independent of its processed data. These countermeasures at the cell level, usually called DPA-resistant logic styles (as some examples see [6]–[8]), suffer from the necessity of making the routes of dual-rails balanced [9], [10]. This issue is problematic because process variation makes perfectly balanced routing impossible.

State-of-the-Art: As a hiding countermeasure there exist several proposals for flattening the current consumption of a circuit independent of its data processing. Some of these techniques try to suppress information leakage through power supply pin by means of (1) an internally integrated filter [11], (2) an internal voltage regulator [12], [13] or (3) a current mask generator to maintain the total current of the circuit constant [14], [15].

Along the same lines, Shamir has proposed a circuitry to decouple the supply voltage of e.g., a smart card, from the main power supply [16]. His proposal is based on two capacitors which supply the target chip in an interleaved fashion; when one supplies the chip, the other one is being charged. Since the capacitors should be quite large and – according to the original proposal – need to be integrated externally out of the semiconductor, the circuit needs also tamper resistance. Otherwise, the adversary can easily bypass the capacitors or measure the current passing through them. Further, a realization of this concept has been evaluated in [17], where – in addition to that of the basic concept – evaluation result of an enhanced version of the same scheme has been presented. The enhanced version adds two more phases to the scheme thereby discharging the capacitors to avoid probable leakage during the charging phases. The evaluation results of [17] indicate inability of the – even enhanced – scheme to prevent the side-channel leakage. The main reasons have been reported as (1) current leakage of the off switches which control the charging and discharging the capacitors and (2) side-channel leakage through the I/O pins.

Based on the same principle a couple of other schemes have been developed, but they suffer from two issues:

- Their effectiveness strongly depends on specification of the underlying switches with respect to the leakage current when they are not conducting. Since there exist no ideal semiconductor-based switches, there is – even small – leakage current which can be exploited by an adversary equipped with a sophisticated setup.
- They are implemented to protect a complete chip or a large circuit. Therefore, they cannot be reused and have to be redesigned for the use with every other circuit. Additionally, a mixed-signal design has to be done to check whether the capacitors are large enough to supply the circuit.

One of such schemes is the work in [18] which presents

a semiconductor-based approach. The authors introduced "switching capacitor modules" consisting of a 100 pF capacitor made of NMOS transistors and three switches to control the charging, discharging, and decoupling the capacitor. Then, three of such modules are connected together to build a "current equalizer block" which supplies the target cryptographic circuit. Compared to the original Shamir's scheme, it integrates the capacitors inside the chip, and hence the aforementioned tamper resistance is not mandatory. Also, similar to the enhanced version of [17] it considers a discharging phase for each capacitor. According to their practical evaluation results, the underlying cryptographic circuit, i.e, an AES encryption module, could not be attacked using 10 million measurements while the similar unprotected circuit can be broken by around 10 000 measurements.

Another work following the same principle is presented in [19], [20], where a three-phase charge-pump system is introduced. The main goal of this principle is to supply the connected logic circuit with a constant voltage using a charge-pump. Therefore, the used integrated capacitances have to be charged and discharged permanently to prevent a voltage drop. To reach this goal the charge-discharge cycles are synchronized by the main clock of the target circuit thereby several charges and discharges are performed during each clock cycle. Although not a proper practical side-channel evaluation is reported, the authors claimed a significant effectiveness of their proposed approach in providing a high level of security.

Our Contribution: In order to address the issues expressed above, following the same concept we present a novel architecture in this work. In contrast to the formerly-proposed countermeasures, each logic gate in our scheme is protected by a dedicated so-called decoupling cell as shown in Fig. 1. It is used for decoupling the external power supply from an internal one which is supplied by an integrated capacitance. Due to the special design of the decoupling cell, the crosstalk between internal and external power supply is reduced compared to the formerly-proposed techniques.

The internal power supply is used to power a single logic gate. Therefore, this decoupling cell only has to be designed once for each logic gate and can be reused for other designs. In fact, a combination of the decoupling cell and the logic gates of a standard-cell library can form a new library to be used for security-related applications. With the new library the digital circuit designer can hence make use of the same design flow as for other digital ASICs. So, no analog- or mixed-signal design flow is required when the decoupling cell is reused.

Further, since each logic gate is protected by its own decoupling cell, the current flowing through the logic gate is kept locally. Therefore, we expect, in contrast to all above cited works, the EM radiation of a chip – protected by our countermeasure – to be significantly reduced.

We first describe the circuit concept of our proposed countermeasure in Section II. Afterwards, in Section III we explain how we developed and fabricated an exemplary circuit made by our proposed scheme in order to examine its functionality and efficiency in practice. Moreover, all the details of the practical side-channel evaluations we performed on several chips of our exemplary circuit are given in Section IV. Finally we discuss about the efficiency of our proposed scheme and conclude our research in Section V.

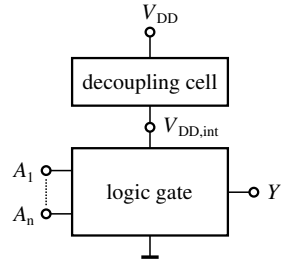

Fig. 1: Basic concept of the countermeasure

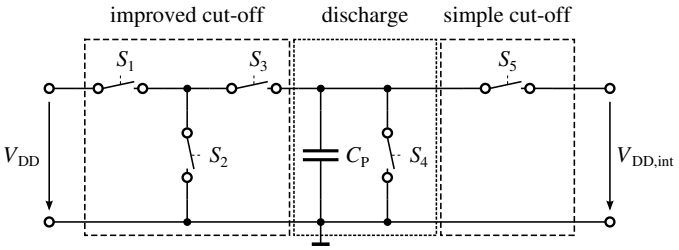

Fig. 2: Basic concept of the decoupling circuity

II. Concept of the Circuit

The main concept of the presented countermeasure is to decouple the power supply of the logic gates from the main power supply of a chip. Therefore, the energy required for the switching of the logic gates is not directly provided by the main power supply. Hence the instantaneous power consumption of the chip due to its dynamic activities – ideally – should not be observable by a side-channel adversary who monitors the current passing through the main power supply. As already explained, the decoupling cell is placed between the power supply and a single gate, as shown in Fig. 1. Each decoupling cell contains capacitances which supply the logic gate for several transitions. Clearly, before the charge stored in the decoupling capacitances becomes smaller than a threshold, they must be recharged to supply the corresponding logic gate.

Before describing the architecture of a decoupling cell, we introduce its main submodule namely decoupling circuit. A detailed view of such circuitry is presented in Fig. 2. It consists of three parts: two cut-off circuits and a discharge circuit. The main difference to the formerly-proposed circuits (e.g., in [18]) is the improved cut-off circuit. It is used to reduce the current leakage from the power supply of a logic gate to the external supply voltage V_{DD}, and therefore reduce the side channel information leakage. The improved cut-off circuit is made of three switches S_1, S_2 and S_3 while the simple cut-off circuit consists of a single switch S_5. When S_1 and S_3 are closed and S_2 is open, the improved cut-off circuit is conducting, and the V_{DD} is connected to the capacitor C_{P}. If S_1 and S_3 are open and S_2 is closed, the improved cut-off circuit is not conducting. Here S_2 plays an important role as it lowers the crosstalk between internal and external wires by shorting the signal path to ground. This can be seen in Fig. 3, where MOS transistors are used as switches. This figure shows the transfer function

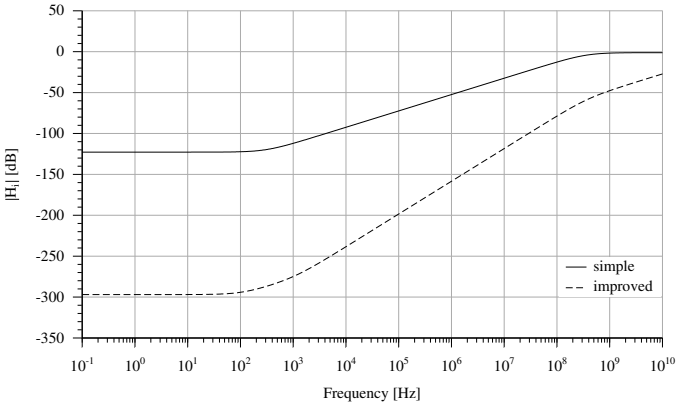

Fig. 3: AC-analysis of the simple and improved cut-off circuits

$|\mathrm{H_i}|$ for a current passing from $V_{\mathrm{DD,int}}$ to V_{DD}. Compared to the simple cut-off, the improved cut-off performs way better in damping high frequency signals and with this side-channel leakage. The simple cut-off circuit is made of S_5 and is just connecting the buffering capacitor C_{P} to $V_{\mathrm{DD,int}}$. It could be built also similar to the improved cut-off circuit, but due to area overhead it is realized by only one switch. Further, the discharge circuit is composed of only switch S_4, whose job is to discharge the capacitor C_{P} to ground. Due to the fact that the capacitor is discharged by a local switch, the discharge current does not flow through the power supply lines. Employing the improved cut-off circuit is essential; otherwise the discharge current could cause a crosstalk to the external power supply V_{DD}, which represents a side-channel leakage.

In order to get the intended purpose, the whole circuit is operated in three different states: **discharge**, **charge**, and **buffer**.

- During the **discharge** state both improved and simple cut-off circuits are not conducting, and the discharge circuit is active. So, the buffering capacitor C_{P} is discharged to ground by switch S_4.
- In the **charging** state the improved cut-off circuit is conducting. The discharge circuit is inactive, and the simple cut-off circuit is not conducting. Therefore, the logic gate is decoupled from $V_{\mathrm{DD,int}}$ while the capacitor C_{P} is being charged.
- During the **buffer** state the logic gate is supplied by the buffering capacitor C_{P} and decoupled from V_{DD}. Therefore, the improved cut-off circuit is not conducting. The discharge circuit is inactive, and the simple cut-off circuit is conducting.

The capacitance of C_{P} is adjusted to be able to supply the logic gate for several transitions. Therefore, the internal supply voltage $V_{\mathrm{DD,int}}$ is not only decoupled from V_{DD} but also is not fixed and steadily decreases depending on the gate activities. The internal power consumption (and respectively the EM radiation) of the chip will be hence slightly variable even for certain processes. This is because the switching power consumption P_{sw} depends on the supply voltage as

$$P_{\mathrm{sw}} = f \cdot C_{\mathrm{L}} \cdot V_{\mathrm{DD,int}}^2,$$

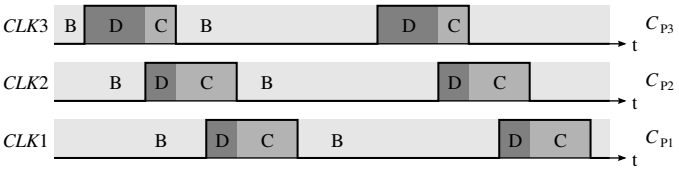

Fig. 4: Control scheme for the different states of the decoupling cell

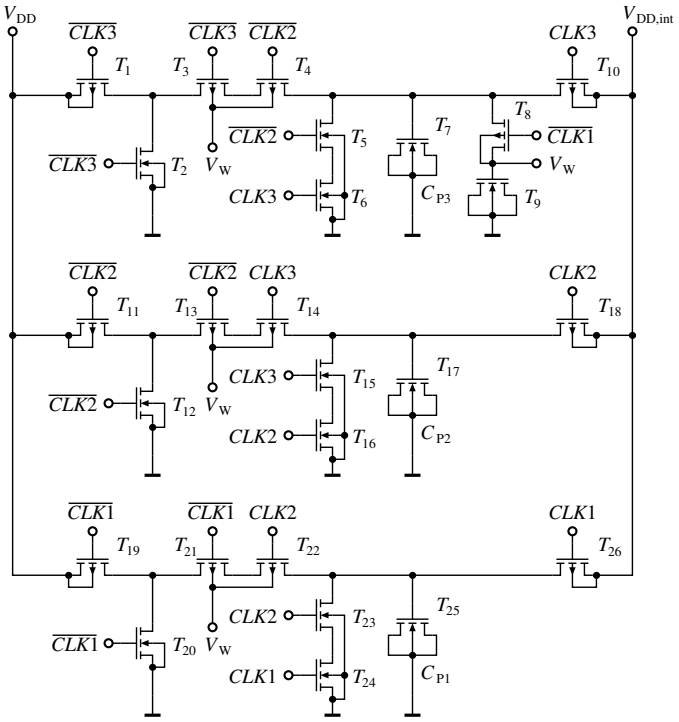

Fig. 5: Circuit implementation of the decoupling cell

where C_{L} stands for the load capacitance and f for the switching frequency of the gate.

Three of such decoupling circuits are connected together in parallel to form a decoupling cell. To coordinate the three states of each decoupling circuit, the scheme represented by Fig. 4 is used, which shows two complete charge-discharge cycles. In this scheme the letters B, C and D stand for **buffer**, **charge**, and **discharge** states respectively. Further, C_{P1} to C_{P3} indicate the buffering capacitor of corresponding decoupling circuits. The states are arranged in a way that always at least one of the buffering capacitors supplies $V_{\mathrm{DD,int}}$ while the others are being discharged or charged.

The circuit implementation of a decoupling cell, which is controlled by the signals *CLK*1 to *CLK*3, is depicted in Fig. 5. In this circuit transistors T_1 to T_{10} build the first decoupling circuit, where T_7 is used as the buffering capacitor C_{P3}. A biasing circuit, made of transistors T_8 and T_9, is needed to generate the bias voltage V_{W} for the well of the PMOS transistors. This biasing circuit has to be included once to get the best switching behavior of the PMOS transistors. It is sufficient to recharge the capacitor, that is made of T_9, just once in a charge-discharge cycle because the self-discharging of the capacitor is very small. So, this part of the circuit is not repeated in other decoupling circuits. The second decoupling

circuit is composed of transistors T_{11} to T_{18}, and the third one from transistors T_{19} to T_{26}.

For the sake of simplicity we consider the first decoupling circuit to explain the structure of the decoupling cell. Here, transistors T_1 to T_4 are used to build the improved cut-off circuit, where T_3 and T_4 represent switch S_3 (see Fig. 2). As stated before, this structure is necessary to reduce the crosstalk between the internal supply voltage $V_{\mathrm{DD,int}}$ and the external V_{DD}. Transistors T_5 and T_6 are used as the discharge circuit for capacitor C_{P3}. Finally, the simple cut-off circuit is realized just by transistor T_{10}.

The same concept is followed for the next two decoupling circuits excluding the biasing circuit (T_8 and T_9). Moreover, a suitable connection of signals *CLK*1, *CLK*2, and *CLK*3 to control the transistors of the decoupling circuits makes the decoupling cell to operate according to the scheme presented in Fig. 4.

Unlike the PMOS transistors T_1, T_{11} and T_{19}, whose bulk and source contacts are connected together, the bulk contact of the PMOS transistors T_{10}, T_{18}, and T_{26} are connected to their drain contacts. This has to be done because the voltage at the buffering capacitors can drop below the voltage of $V_{\mathrm{DD,int}}$ during their corresponding **discharge** state. If the source and bulk contacts would be connected, the bulk-drain diode would be conducting and the transistor could be destroyed. Therefore, the drain and bulk contacts of these transistors have to be connected together. As a side note, a patent for the decoupling cell is pending.

III. Test Chip

In order to examine the efficiency of the decoupling cell to prevent side-channel attacks, we developed a prototype chip. It consists of two functionally-equivalent exemplary cores: one **unprotected** CMOS, and one **protected** by means of decoupling cells. Although the cores partially share some I/O pins, each core can be operated completely independent of the other. An overview of the exemplary circuit – identical for both cores – is shown in Fig. 6.

We should mention that the fabricated chip, which is used for practical side-channel analysis, contains two realizations of this circuit, an **unprotected** core and a **protected** core. The main functionality of the exemplary circuit is the realization of a PRESENT Sbox [21]. The reason behind this choice is due to its lightweight 4-bit architecture which requires considerably lower area and design effort compared to the 8-bit AES Sbox.

As shown in Fig. 6, we put a couple of 4-bit register stages between each combinatorial part of the circuit. That is to isolate each combinatorial part and prevent the propagation of glitches thereby separating the side-channel leakage of each combinatorial circuit. Each 4-bit register can be enabled separately while a global clock signal *clk* is connected to all registers that synchronizes the processing of data.

A 4-bit secret key k and a 4-bit plaintext p, which are both provided externally at the core input pins, are stored in registers `reg_key` and `reg_plain` respectively. They are used to supply the XOR circuitry whose result is saved in register `reg_XOR` and later in register `reg_Sbox_in`. We have put these two registers in series at the Sbox input to be able to differentiate the side-channel leakages associated to (1) solely register cells, i.e., `reg_XOR` and (2) the combinatorial circuit, i.e., the PRESENT Sbox. Finally, the output of the Sbox is stored by register `reg_Sbox_out` which drives the output pins of the core. It is noteworthy that the global asynchronous reset $\overline{R}$ has been considered into the design to preset all the register cells. One more point to mention is that each register cell has been made by master-slave D-latches.

Due to the low manufacturing costs as well as the convenient tape-in/tape-out schedules the chip was manufactured in a 150 nm CMOS technology supplied by the EUROPRACTICE program. For the **unprotected** core as well as for the **protected** core a standard-cell library was used, but in the latter one each gate is protected by its own decoupling cell. In order to reduce the design effort we used only 2-input gates from the standard-cell library and designed a unique decoupling cell which can drive the most power-consuming gate, i.e., XOR. Because of this the master-slave D-latches were made out of 2-input NAND gates from the standard-cell library, where each is protected by a decoupling cell. Otherwise, the area we reserved in each decoupling cell to include one gate had to be increased in order to fit a D-FF as well. That would have wasted space and increased the overall overhead.

Due to the glitches happening at the internal signals of a combinatorial circuit, the output of a gate (supplied by a decoupling cell) may toggle a couple of times between two consecutive charge-discharge cycles. Therefore, we adjusted the buffering capacitors to buffer enough energy for at least five transitions of the XOR gate. We should note that the $V_{\mathrm{DD,int}}$ of all cells are connected together. If a gate toggles more than five times, the other buffering capacitors can supply the necessary energy. Hence, the circuit designer should consider the maximum of the whole number of toggles of the circuit divided by the number of cells to not exceed than five. Figure 7 shows an abstract view of the layout of the designed decoupling cell. For a better view only the layers related to poly-Si, active, and metal 1 to metal 4 are shown. The upper part of the layout includes the improved cut-off and the discharge circuitries for all three decoupling circuits of the decoupling cell. This area is chosen to keep the control signals *CLK*1 to *CLK*3 separated from $V_{\mathrm{DD,int}}$ and therefore reduce the crosstalk between these wires. Around the free space for the target logic gate and the simple cut-off circuit, the buffering capacitors as well as the capacitor for the generation of V_{W} are placed. So, in addition to all integrated guard rings, we obtain protection against crosstalk from the target logic gate through the substrate. Therefore, in contrast to all other previously proposed schemes a single decoupling cell per gate is preferred as it is in the same line as our main goals.

In total the buffering cell has an area of $259.78\,\mu\mathrm{m}^2$. It is roughly 10 times bigger than an XOR gate with an area of $24.16\,\mu\mathrm{m}^2$, that is the largest gate used for the test circuit from the underlying standard-cell library. It should be noted that according to this developed structure each logic gate, that was used for the test circuit, fits to the free space provided inside

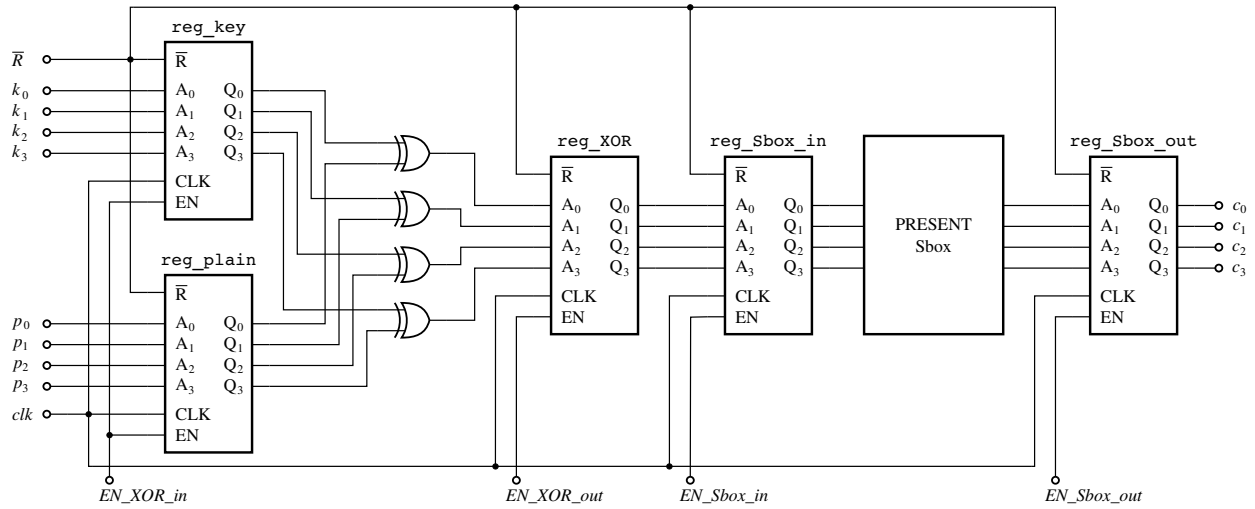

Fig. 6: Test circuit used for practical side-channel evaluations

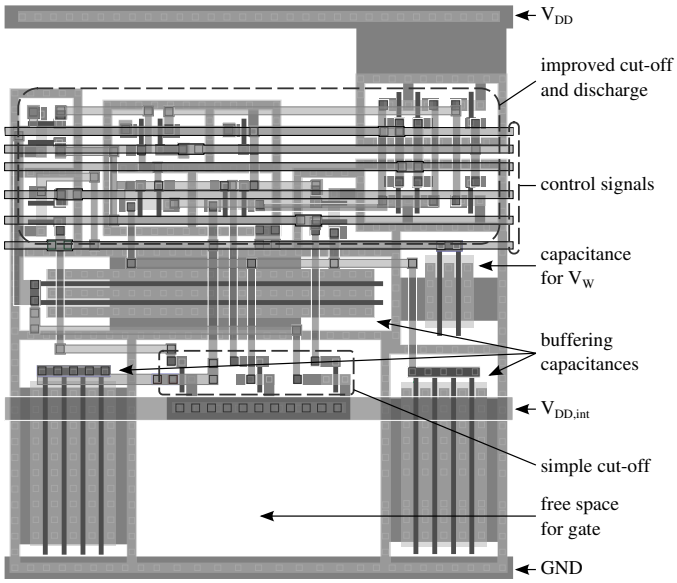

Fig. 7: Abstract layout view of the decoupling cell

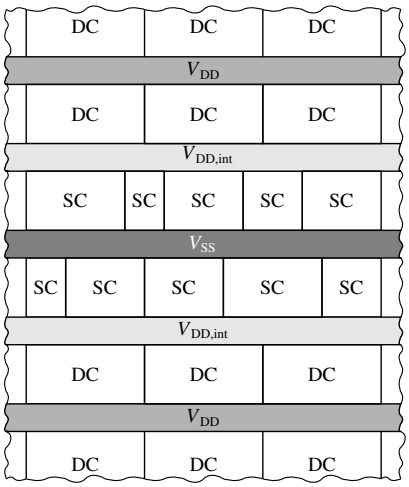

Fig. 8: Decoupling cell as decoupling layer

the decoupling cell. So, every logic gate – from an inverter to 2-input XOR – equipped with a decoupling cell needs the same area. The gap in the upper part of the layout is due to the distance design rules between n-well and p-well and is specific to the underlying process technology. Therefore, the size of the decoupling cell can be reduced using a different CMOS technology.

When using a smaller technology node, the needed area will scale together with the gate size, because the logic gate needs less current for the operation and therefore the area of the capacitances can be reduced too. Although the leakage current of the MOS transistors increases by shrinking the technology node, the performance of the decoupling cell should not be affected, because switch S_2 of the improved cut-off circuit will still short this leakage current to ground as shown in Fig. 2.

Another option to address the area overhead is to design the decoupling cell in such a way that it can protect more than one gate. Standard cells are built with a fixed height and a width that can vary in fixed steps. This width depends on how many transistors are used in each gate. Therefore, the width of a standard cell is somehow proportional to the number of transistors used and therefore to the power consumption of that gate. With this in mind a decoupling cell can be designed, which is able to provide a protection for a certain width of standard cells and can be implemented as an additional layer which provides the internal supply voltage $V_{\mathrm{D,int}}$. This concept is shown in Fig. 8. It also allows a reduction of the design effort and helps to integrate the decoupling cell into the digital design flow. Nevertheless, further research has to be done on this concept.

In order to realize the **protected** core we avoided developing a library to be used by the synthesizer tools, but using these tools is planned for the future, with the concept of the decoupling layer. Instead, due to the small size of the exemplary circuit – mainly related to the PRESENT Sbox – we could manually design the layout of the **protected** core by moderate efforts. This includes manual placement of the decoupled gates and routing of the signals. Figure 9 shows a die photo of the test chip.

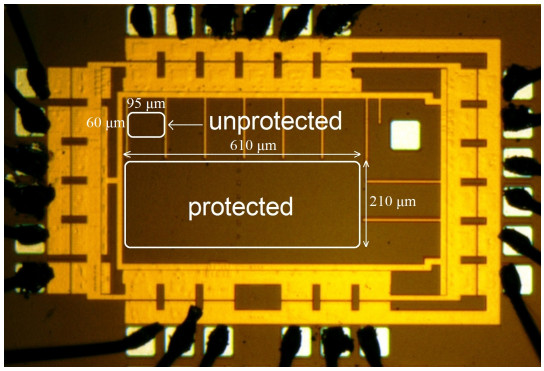

Fig. 9: Microphotograph of the test chip

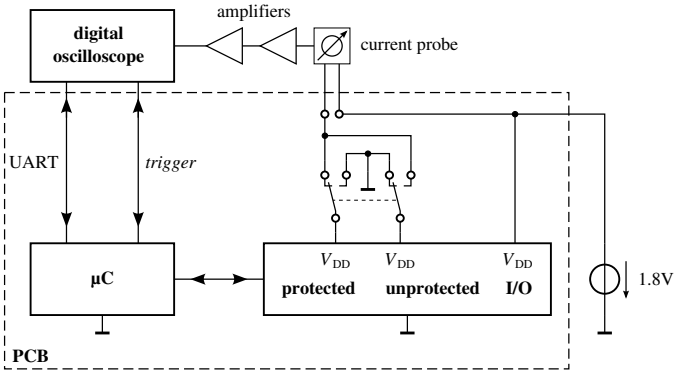

Fig. 10: An overview of the evaluation platform

To compare our proposed scheme with the known countermeasures at the same abstraction level we provided Table I where WDDL [7], MDPL [24], and iMDPL [8] are taken into account. We should here emphasize that both WDDL and MDPL have known security issues (e.g., *early propagation* [25]), which prevent them to be considered as secure solutions. Further, it has been shown in [26] that sophisticated attacks can also overcome the security provided by iMDPL. One advantage of our proposed scheme is its null frequency overhead, which cannot be achieved by any other countermeasure in the same field. Considering the microphotograph (Fig. 9), the area overhead factor is around 20, which is due to our manual placement and the area we left empty in this part of the test chip. The overhead factors are calculated by dividing the corresponding value of the countermeasure by the one from the standard CMOS implementation presented in the same article. In order to calculate the power overhead of our proposed scheme, we considered the maximum peak-to-peak power consumption of a charge-recharge cycle when the buffering capacitors are refreshed versus the same of an operational phase of the **unprotected** core. Note that the type of the circuit under test, its architecture, and the technology node of the given comparisons are not the same. Hence, the provided overhead figures might be different in a more fair comparison. The area overhead will not change much by transferring to a smaller technology node, because scaling is done proportionally. However due to some design-rule change there might be minor differences. With this in mind, our proposed countermeasure lies – regarding the area overhead – roughly in the middle of the range of the other countermeasures.

IV. Practical Evaluation

A. Platform

We developed a dedicated board to evaluate the functionality as well as the side-channel vulnerability of the test chip.

TABLE I: Comparison between the overhead factors

Countermeasure	Area	max. Frequency	Power
WDDL [22]	3.1	0.26	3.7
MDPL [8]	4-5	0.50	3-7
iMDPL [23]	18-19	0.30	5-10
this work	≈10	1.00	≈3.5

It includes a microprocessor which communicates with a PC via UART, and according to the requested operation it controls the test chip by providing the desired input at its I/O pins and monitors its output signals. The board has been designed to facilitate the side-channel measurements by (1) providing a jumper at the internal core V_{DD} supply path as an appropriate place to measure the power consumption, and (2) assigning one of the microprocessor's I/O pins as the *trigger* signal which can be seen by the oscilloscope to start the measurements. The microprocessor also provides signals $CLK1$ to $CLK3$ for the **protected** core.

In order to evaluate both the **unprotected** and the **protected** cores under the same conditions and avoid the noise of the other core, the board has been designed to completely deactivate the other core by connecting its internal V_{DD} pin to ground. Figure 10 shows a detailed overview of the developed board.

B. Measurement Setup

In order to measure the power consumption of the target chip we used a CT2 Current Probe [27] from Tektronix, and put it at the internal core V_{DD} path – provided by the developed platform – to convert the passing current to a voltage level measurable by the oscilloscope. Due to very low amplitude of the signal we also used two low-noise AC amplifiers in series, each of which as ZFL-1000LN+ [28] from Mini-Circuits with $20\,\mathrm{dB}$ gain. As the sampling device we employed a LeCroy WavePro 715Zi digital oscilloscope and measured the power traces at the sampling rate of $1\,\mathrm{GS/s}$. Further, we limited the oscilloscope bandwidth to $20\,\mathrm{MHz}$ to decrease the electrical/environmental noise thereby obtaining clear and noise-free traces.

C. Measurement Scenario

As explained in Section III, we considered a couple of register stages in the design architecture to separate the probably-observable leakage of each combinatorial part of the circuit. Before starting each measurement the following operations are performed:

- by controlling the reset signal $\overline{R}$ the content of all registers are cleared,
- `reg_key` is filled by a constant 4-bit key k,

- a randomly-selected 4-bit input p (as plaintext) is transferred to `reg_plain`, and
- all input signals of the chip are cleared (set to LO) to prevent any effect of I/O levels on the measurements.

We followed the timing diagram given in Fig. 11 as the covered period of time. Each measurement – that starts by rising the *trigger* signal – covers

- loading `reg_XOR` which stores the result of $p \oplus k$, and
- loading `reg_Sbox_In` which provides the new input for the PRESENT Sbox.

As shown in Fig. 11, these two parts are completely independent of each other as the corresponding registers are controlled by separate enable signals (*EN_XOR_out* and *EN_Sbox_in*). Further, we did not consider the leakage associated to the loading of `reg_Sbox_out` as it directly appears at the output signals of the chip and may have a significant effect on the measurements. We kept this procedure during the power consumption measurement of both the **unprotected** and the **protected** cores. The only difference is due to the charge-discharge cycle of the **protected** core.

Since the *CLK*1 to *CLK*3 must not be necessarily synchronous with the main clock of the target circuit (*clk*), a couple of operations (e.g., five Sbox computations) can be performed between two consecutive charge-discharge cycles. So, before following the above explained procedure the below steps are done

- a charge-discharge cycle is performed,
- for a random number of times $r < 4$
  - `reg_plain` is filled by a random input, and
  - all enable signals *EN_XOR_out*, *EN_Sbox_in*, and *EN_Sbox_out* are kept active while clocking the registers three times.

Hence, right before each measurement we indeed emulate a random number of dummy operations performed by the **protected** core that should partially consume the charge stored in the corresponding decoupling capacitors. Note that by dummy operations we do not mean any shuffling, misalignment of the traces, or varying the point in time where the real operation starts. All the collected traces are very well aligned.

Following this procedure no charge-discharge cycle is performed during each measurement. It is noteworthy that following this process for the **unprotected** core does not affect its measured power consumption as it does not contain any decoupling capacitor. Figure 11 also shows two sample traces corresponding to each core, that indicate the lower power consumption of the **protected** core. The oscillations shown in the sample traces at each clock edge are due to the current probe used in our measurement setup.

D. Evaluation Metrics

In order to evaluate the side-channel leakage of the prototype chip and to compare the vulnerability of the **unprotected** and the **protected** cores from different perspectives, we considered four different metrics which are given below after expressing the notations.

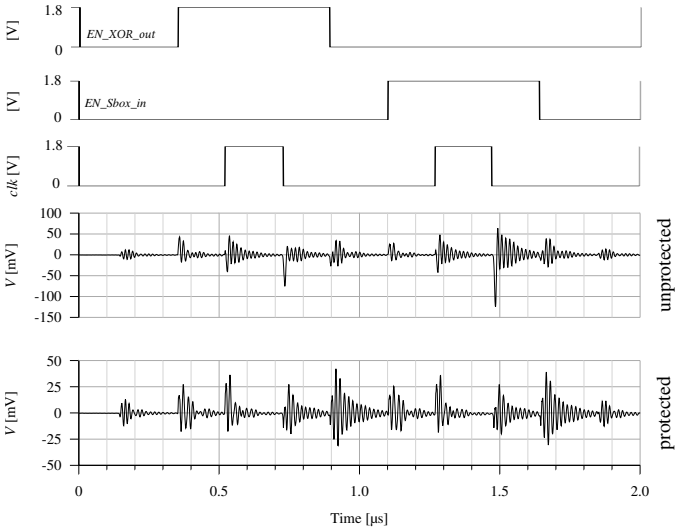

Fig. 11: Timing diagram of the measurement scenario and sample trace

Notation: For each core we collected n number of traces with associated plaintext nibbles $p_{i\in\{1\ldots n\}}$ which are randomly selected from $\{0,1\}^4$ with a uniform distribution. Respectively, the output of the PRESENT Sbox corresponding to measurement i is denoted by c_i. Each trace $t_{i\in\{1\ldots n\}}$ consists of $m = 2000$ sample points $(t_i^1, \ldots, t_i^m)$ which according to Fig. 11 covers a window of $2\,\mu$s. With the help of the *trigger* signal as well as a stable crystal oscillator supplying the microprocessor of the developed platform, all traces are well aligned together. It is noteworthy that the 4-bit key k is kept constant during all measurements.

During the evaluations of the **protected** core we observed very diverse results. In fact, the robustness provided by the **protected** core was significantly different from chip to chip while we did not observe such different behavior by the **unprotected** core of different chips. Therefore, here we present the evaluation result of the **protected** core of two chips with the most extreme different behavior. To distinguish these cores we use the terms "chip 1" and "chip 2" in the description below. As a side note, we observed that the **protected** core of chip 1 follows the simulation results while it is not the case for that of chip 2. In other words, the **protected** core of chip 1 could buffer the energy required for up to eight transitions. However, the **protected** core of chip 2 could operate multiple times the eight transitions without malfunction between two consecutive charge-discharge cycles. In order to give a complete view of their behavior, the results of both cores are presented in this section.

Due to the different behavior of the two cores, the evaluation of the **protected** core of chip 1 is performed on $n = 100\,000$ traces, and the evaluation of the **unprotected** core and the **protected** core of chip 2 are based on $n = 10\,000$ traces.

1) Information Theoretic (IT) metric: It examines the amount of available information which can be exhibited by the *worst-case* adversary [29]. In short, we estimate the mutual information by means of conditional entropy as

$$\mathrm{I}(S;\mathrm{L}) = \mathrm{H}[S] - \mathrm{H}[S|L],$$

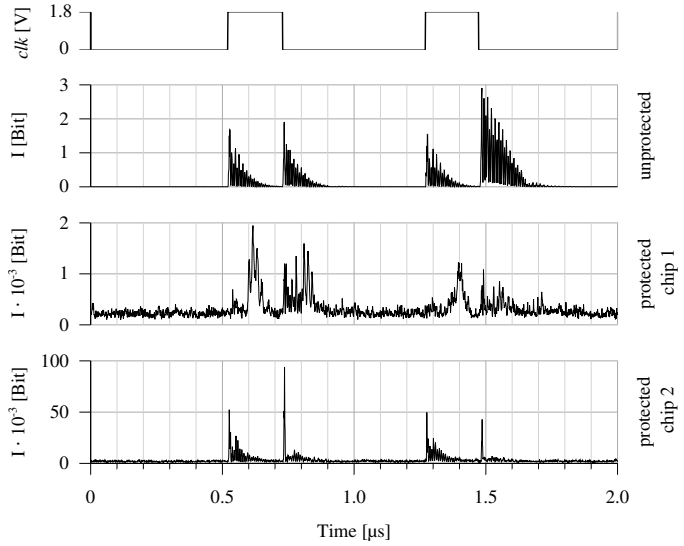

Fig. 12: Mutual Information curves as IT metrics

where L denotes the side-channel leakages and S a secret internal. Since we cleared the content of all registers before each measurement (by global reset $\overline{R}$), a valid selection for S can be plaintext p, Sbox input, or Sbox output c. Due to the linear key addition and the bijective PRESENT Sbox, all above mentioned choices for S lead to the same result.

To compute the entropies we need to estimate the probability distribution of side-channel leakages. Therefore, at each sample point $j \in \{1 \dots m\}$ we estimated the mean and variance of the traces associated to each plaintext value p. So, we first categorize the traces into 16 sets $Q_{s\in\{0\dots15\}}$ as

$$Q_s = \{i | p_i = s\}, \qquad n_s = |Q_s|,$$

and estimate the means and variances as

$$\mu_s^j = \frac{\sum_{i\in Q_s} t_i^j}{n_s}, \qquad {\delta^2}_s^j = \frac{\sum_{i\in Q_s} (t_i^j - \mu_s^j)^2}{n_s}.$$

As the next step, probability distributions at each sample point j for each s are separately estimated by a Gaussian distribution. Finally, the conditional entropy can be estimated by means of integral over l as

$$\mathrm{H}[S|L] = -\sum_s \Pr[s] \int \Pr[l|s] \cdot \log_2 \Pr[s|l]\, dl.$$

Following the above procedure and using all $n = 10\,000$ traces of the **unprotected** core and the **protected** core of chip 2, and $n = 100\,000$ traces of the **protected** core of chip 1 we obtained the mutual information curves depicted in Fig. 12. As mentioned before in Section III, the registers are realized by master-slave latches. Therefore, we observe leakages on both edges of the clock signal. As shown by the graphics and stated before, the **protected** cores behave very differently. Compared to the **unprotected** core the available information is reduced from 2.9 bit to 0.002 bit on chip 1 and to 0.09 bit on chip 2. These numbers directly correspond to the success rate of a univariate template attack [30]. However, it cannot be concluded that the leakage is avoided and no attack is possible.

2) t-test: An evaluation methodology which aims at detecting whether there exists a leakage observable by an attacker is known as t-test [31]. Its goal is not to quantify how much leakage exist, rather it can provide an overview of feasibility of an attack with respect to classical DPA [1]. Following the concept of *specific* t-test, according to a selected intermediate value the traces are categorized into two groups G_1 and G_2. Then, Welch's (two-tailed) t-test at sample point j is computed as

$$test^j = \frac{\mu(t^j_{i\in G_1}) - \mu(t^j_{i\in G_2})}{\sqrt{\frac{\delta^2(t^j_{i\in G_1})}{|G_1|} + \frac{\delta^2(t^j_{i\in G_2})}{|G_2|}}},$$

where μ and δ^2 denote sample mean and sample variance respectively, and $|.|$ stands for the cardinality. The t-test indeed examines the validity of the *null hypothesis* as the samples in both groups were drawn from the same population. If the null hypothesis is correct, it can be concluded that – with a high level of confidence – using the number of traces n a DPA attack based on the selected intermediate value is not feasible. For such a conclusion the straightforward way is to estimate the degree of freedom v as

$$v^j = \frac{\left(\frac{\delta^2(t^j_{i\in G_1})}{|G_1|} + \frac{\delta^2(t^j_{i\in G_2})}{|G_2|}\right)^2}{\frac{\left(\frac{\delta^2(t^j_{i\in G_1})}{|G_1|}\right)^2}{|G_1|-1} + \frac{\left(\frac{\delta^2(t^j_{i\in G_2})}{|G_2|}\right)^2}{|G_2|-1}},$$

and by means of Student's t cumulative distribution function determine the probability p to accept the null hypothesis. In other words, small p values (alternatively big t-test values) give evidence to reject the null hypothesis.

For the sake of simplicity, usually a threshold for $|test|$ as > 4.5 is defined to reject the null hypothesis and conclude that an attack is feasible. We selected the following intermediate values for each target core to examine the t-test:

- bits of the Sbox input (4 tests),
- bits of the Sbox output (4 tests), and
- value of the Sbox output (16 tests).

For the first 8 tests the groups are formed based on the target bit e.g., the first Sbox input bit as

$$G_1 = \{i \mid (p_i \oplus k)\&1 = 0\}, \quad G_2 = \{i \mid (p_i \oplus k)\&1 = 1\},$$

where $\&$ denotes the bit-wise AND operation. For the last 16 tests the groups are made as

$$G_1 = \{i \mid S(p_i \oplus k) = X\}, \quad G_2 = \{i \mid S(p_i \oplus k) \neq X\},$$

where in each test X is arbitrary selected in a way that all last 16 tests cover full range $X \in \{0,1\}^4$.

Using the same number of traces as stated before for each targeted core we followed the above procedure and examined the t-test. The results which are shown by Fig. 13, Fig. 14 and Fig. 15 indicate that – using the considered traces – there are potential DPA attacks on all cores. However, the tests based on the Sbox output bits of the **protected** core of chip 1 do not show a leakage as high as the other tests and the other cores.

This overall result is along the same lines as that of the IT metric, but still we cannot quantify how much harder – compared to the **unprotected** core – the attacks on the **protected** cores are.

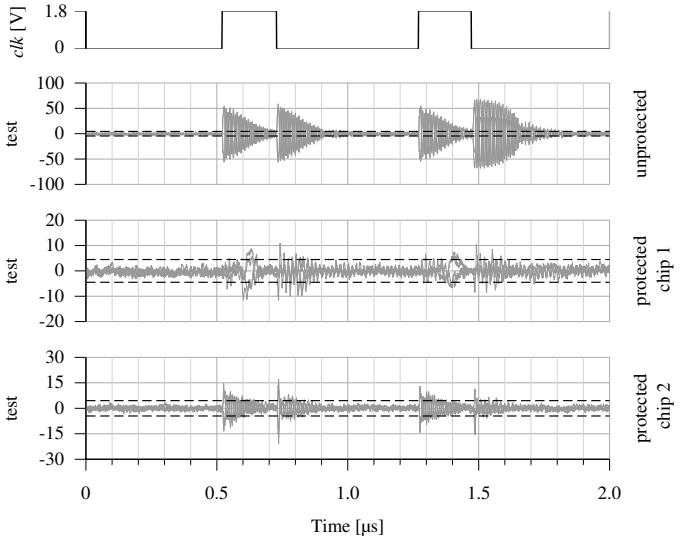

Fig. 13: T-test results based on the Sbox input bits

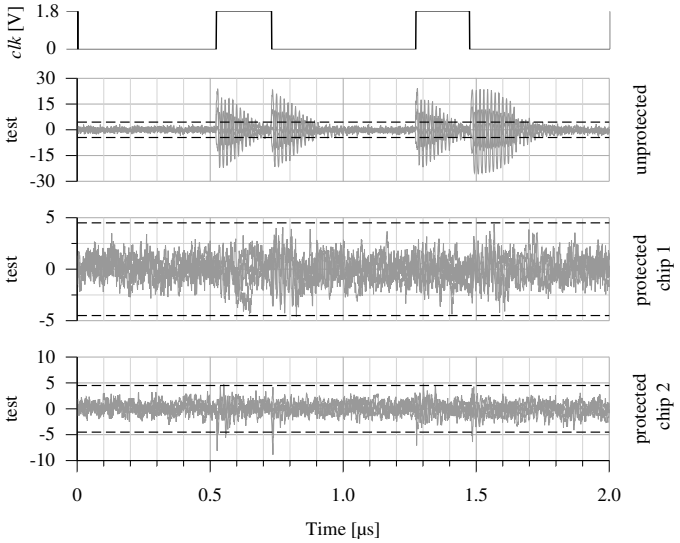

Fig. 14: T-test results based on the Sbox output bits

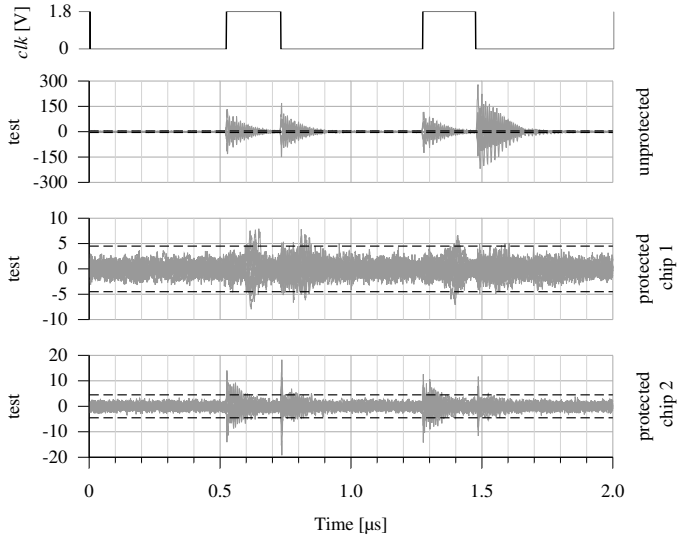

Fig. 15: T-test results based on the Sbox output nibbles

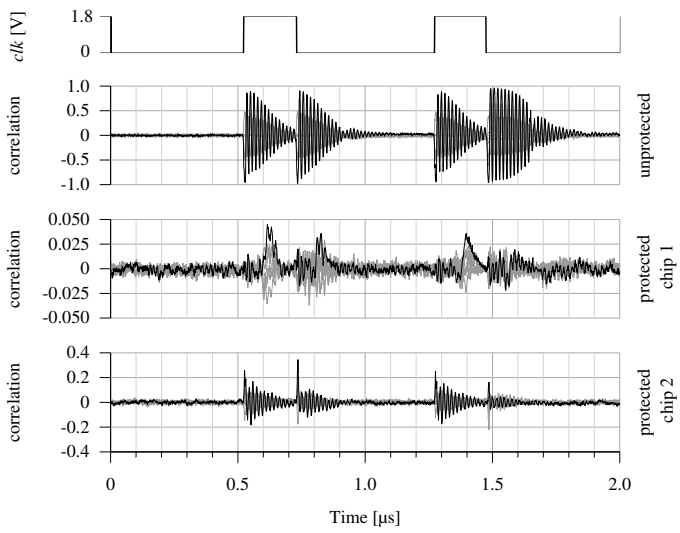

Fig. 16: CPA results based on the HW of the Sbox input

3) CPA with a leakage model: As one of the most common attack schemes we performed a correlation power analysis (CPA) attack with Hamming weight (HW) of the Sbox input as the hypothetical model. The result of the attacks on all three targeted cores are depicted by Fig. 16, where the correlation curve associated to the correct key is plotted in black. Thanks to the metric feature of CPA, we can now use the rule-of-thumb [32], [33] to approximate the number of required traces based on the squared inverse of correlation.

The highest correlation coefficient obtained for the **unprotected** core is 0.969 while 0.0449 and 0.346 have been obtained for the **protected** core of chip 1 and chip 2 respectively. This directly corresponds to a ratio R between the data complexity of the corresponding attacks – on the **protected** vs **unprotected** core under the same condition – as $R = \left(\frac{0.969}{0.0449}\right)^2 \approx 466$ for chip 1 and $R = 8$ for chip 2. The ratio R represents compared to the **unprotected** core approximately how many times more traces are needed to perform a successful attack. This shows a huge difference between the two chips as the **protected** core of chip 1 is considerably efficient to reduce the leakage, but that of chip 2 is not.

We should mention that we performed more CPA attacks with different power models, e.g., HW of the Sbox output, but the best results have been achieved by means of HW of the Sbox input as expressed above. It is due to the architecture of the underlying circuit (Fig. 6). The output of the Sbox is only saved in a register which does not supply a combinatorial circuit. Since dynamic power consumption of CMOS circuits is mainly due to the glitches happening in the combinatorial circuits, in case of our test chip the changes at the Sbox input play the most important role in amount of the chip power consumption. As explained in Section IV-C, before each measurements we cleared the content of all registers. Therefore, changes at the Sbox input (HD) is the same as the value of the Sbox input (HW).

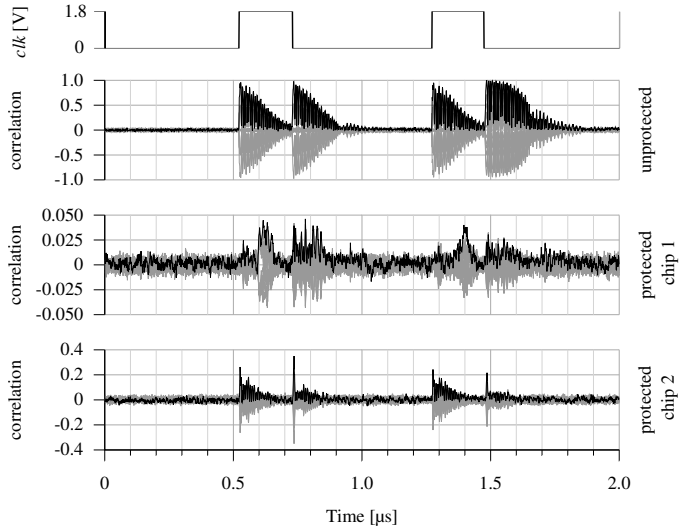

Fig. 17: MCDPA results

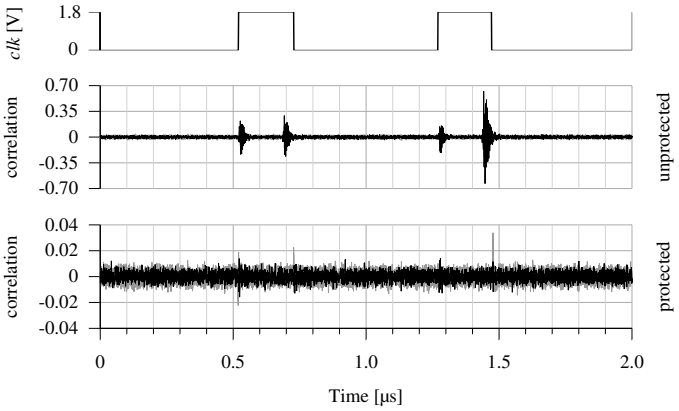

Fig. 18: EM analysis results based on the HW of the Sbox input

4) Moments-Correlating DPA: The feasibility and effectiveness of CPA attacks depend on the selected hypothetical power model, e.g., HW model above. In order to relax this requirement moments-correlating DPA (MCDPA) [34] can be applied, that tries to make use of a perfect leakage model by profiling. Therefore, in each core and each chip we divided the collected measurements (n traces) into two halves, and used the first half ($n/2$ traces) as profiling traces $t_{i\in\{1\dots\frac{n}{2}\}}$. The power models at sample point j for a first-order MCDPA attack are obtained as

$$\mu_x^j = \frac{\sum_{i;p_i=x}^{\frac{n}{2}} t_i^j}{|p_i = x|}.$$

Then, a MCDPA for a key guess k^* is applied on the second half ($n/2$) traces by estimating the correlation coefficients between the traces and the model at sample point j as

$$\rho_{k^*}^j = \hat{\rho}\big(t^j_{i=\{\frac{n}{2}+1,\dots,n\}}, \mu^j_{p_i\oplus k^*}\big).$$

Repeating this procedure for all sample points and all key candidates $k^* \in \{0,1\}^4$ led to the correlation curves shown by Fig. 17 as the profiling MCDPA results on all three cores. The results, which are very similar to that of the CPA with HW model, indicate that (1) the HW of the Sbox input model was selected appropriately as a suitable hypothetical power model, and (2) the conclusion given on comparison between the data complexity of the attacks on the targeted cores is also valid for profiling MCDPA.

E. EM Analysis

We also investigated the efficiency of our proposal in reducing the EM side-channel leakages. Due to the small size of the exemplary circuit we had to use a tiny near-field probe to be able to adjust it at the top of the **unprotected** or the **protected** core. The tiny near-field probe has manually been constructed by five times turning a $150\,\mu\mathrm{m}$ copper wire with an inner diameter of $500\,\mu\mathrm{m}$. The low-amplitude signal picked up by this coil is amplified using two Infineon BGA427 low-noise high-bandwidth AC amplifiers connected in series yielding an overall gain of more than 40 dB in the frequency range from 100 MHz to 1 GHz. At the sampling rate of 10 GS/s and without any bandwidth limit, i.e., 1.5 GHz, we obtained EM traces with a considerably-high quality. We should emphasize that we have currently the EM analysis result of only one chip whose power analysis result is very similar to that of chip 2. In other words, its power analysis results do not show a high level of resistance. However, the corresponding EM analysis, shown by Fig. 18, confirms the ability of our proposal to reduce the EM leakages. For the presented analysis we adjusted the EM probe at the top of the **unprotected** core and measured 10 000 traces. The same was done for the **protected** core and 100 000 traces were collected. As its effectiveness was confirmed by the presented power analysis results, we used the HW of the Sbox input as the hypothetical model to perform the attacks on the EM traces as well. It is indeed confirmed that the used hypothetical model suits the EM leakages as the correct-key correlation value for the **unprotected** core reaches 0.6 (see Fig. 18). More importantly, the same attack on the **protected** core using 10 times more traces still does not show an exploitable leakage.

Generally speaking, the observable EM radiations are usually due to V_{DD} bonding wire as well as the V_{DD} paths inside the chip. In case of our protected core, the V_{DD} bonding wire does not drive the core except during the charge-recharge cycles. Moreover, in our design the buffering capacitors are distributed over the chip and each cell receives its required energy (current) from its nearest buffering capacitor. Hence, the current does not flow through long wires inside or outside the chip and thus cannot radiate huge emission. Therefore, the observable EM is expected to be significantly reduced.

Further, the underlying circuit is very small, that limits the observable EM radiations. As explained before, we developed a very accurate power measurement setup. Therefore, obtaining better results using our very-low noise power measurement setup (compared to the case using EM) is not improbable. Comparing the results (EM vs. power) on the unprotected core actually confirms this claim.

V. Discussions

In this work we presented a complete design, implementation and evaluation of a side-channel countermeasure, whose concept has been proposed at the early age of side-channel academic activities. As a countermeasure which fits into hiding category, it aims at decoupling the main power supply line from the internal voltage of the chip. Our novel design of the decoupling cells allows distributing the decoupling capacitors all over the circuit layout and avoids the necessity of a large capacitor inside the semiconductor. Also, we should emphasize that such countermeasures – like DPA-resistant logic styles e.g., [6] – are independent of the underlying algorithm and are capable of being used to increase the side-channel resistance of any implementation at the cell level.

In order to fairly compare our proposed scheme with other countermeasures, the architecture of our test chip should be implemented with the same technology node, and all the practical evaluations should also be performed in a same way. Since we have not considered any other countermeasure techniques in our test chip, such a fair comparison is not currently possible. However, we have provided an overview about the overheads of our proposed scheme compared to a couple of DPA-resistant logic styles (gate-level countermeasures). For a first rough comparison with the other proposed countermeasures, especially iMDPL, the used area of our countermeasure seems to be reasonable in regard to the protection that is achieved.

With respect to many side-channel evaluation metrics we presented a comprehensive assessment of our proposed countermeasure based on a couple of prototype chips of an exemplary circuit fabricated with a 150 nm process technology. Our evaluations show a very diverse result of the ability of the countermeasure to provide security against power analysis attacks. Indeed, some chips (from the same design, the same wafer, and the same package) show a high level of robustness while some others provide nearly no protection.

By means of simulation as well as practical investigations we have examined many different possible sources for such a failure. The only reason that we found yet is the quality of the bondings. We have received our test chip as unpackaged untested prototypes, and we had to proceed with the packaging and bonding ourselves. We have used standard DIL-24 packages, and manually performed the bonding using a pressure-and-ultrasonic *wedge* bonding machine with *gold* wires. Such a bonding technique (wedge) may lead to some scratches and particles between the adjacent pads. It is more probable if the bonding of one pad has to be repeated. Note that after the bonding we are not able to clean the chip as the bonding wires are not firm connections. This issue is negligible in case of digital signals, but for analogue signals and sensitive circuits (e.g., our test chip) this may lead to unexpected current leakage between the adjacent pads which control the **discharge**, **charge**, and **buffer** states. We predict that this issue is amongst the probable reasons for the diverse side-channel evaluation results. In order to examine this issue, we removed all bonding wires of an already evaluated test chip and re-bonded it completely. By repeating the same side-channel evaluations on the re-bonded test chip we did not achieve the same results. The result showed more vulnerability after the re-bonding. Indeed, this experiment confirms that the quality of the bonding plays a role on the diversity which we have observed. One option to avoid such an issue is to use an automated *ball* bonding machine to achieve the best bonding quality without any effect between the adjacent pads.

One more point which we should highlight is regarding our measurement setup. As shown by the evaluation results, e.g., Fig. 16 and Fig. 17, the correlation coefficient of the attacks on the **unprotected** core is approaching the highest value '1'. This indeed indicates the very low-noise and proper measurement setup that we developed for these evaluations. This result can be compared with that of [8] and [18], where a CPA attack on an unprotected CMOS core reached at most 0.3 and 0.025 respectively. Although the exemplary circuit contains a few gates, and at some clock cycles only the content of a solely 4-bit register changes, with the help of our measurement setup we could diminish the electrical noise and observe very clear side-channel traces. So, the highest correlation value we obtained from the analysis of the **protected** core of chip 1 can be dramatically reduced in presence of either switching or higher electrical noise. Furthermore, as mentioned before, during each measurement of the **protected** core no charge-discharge cycle was performed, which is not always the case in real scenarios. If a charge-discharge cycle is not synchronized with the measurements and they happen out of the control of the adversary, the attacks become much more difficult due to the strong noise added to the signals.

References

[1] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun, "Differential Power Analysis," in *CRYPTO 1999*, ser. LNCS, vol. 1666. Springer, 1999, pp. 388–397.

[2] S. Nikova, V. Rijmen, and M. Schläffer, "Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches," *J. Cryptology*, vol. 24, no. 2, pp. 292–321, 2011.

[3] Tim Güneysu and Amir Moradi, "Generic Side-Channel Countermeasures for Reconfigurable Devices," in *CHES 2011*, ser. LNCS, vol. 6917. Springer, 2011, pp. 33–48.

[4] Stefan Mangard and Elisabeth Oswald and Thomas Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007.

[5] Christoph Herbst and Elisabeth Oswald and Stefan Mangard, "An AES Smart Card Implementation Resistant to Power Analysis Attacks," in *ACNS 2006*, ser. LNCS, vol. 3989. Springer, 2006, pp. 239–252.

[6] 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 *Solid-State Circuits Conference - ESSCIRC 2002*, 2002, pp. 403–406.

[7] K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," in *DATE 2004*. IEEE Computer Society, 2004, pp. 246–251.

[8] Thomas Popp and Mario Kirschbaum and Thomas Zefferer and Stefan Mangard, "Evaluation of the Masked Logic Style MDPL on a Prototype Chip," in *CHES 2007*, ser. LNCS, vol. 4727. Springer, 2007, pp. 81–94.

[9] Sylvain Guilley and Philippe Hoogvorst and Yves Mathieu and Renaud Pacalet, "The "Backend" Duplication Method," in *CHES 2005*, ser. LNCS, vol. 3659. Springer, 2005, pp. 383–397.

[10] Kris Tiri and Ingrid Verbauwhede, "Place and Route for Secure Standard Cell Design," in *CARDIS 2004*. Kluwer, 2004, pp. 143–158.

[11] Girish B. Ratanpal and Ronald D. Williams and Travis N. Blalock, "An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks," *IEEE Trans. Dependable Sec. Comput.*, vol. 1, no. 3, pp. 179–189, 2004.

[12] Telandro, V. and Kussener, E. and Malherbe, A. and Barthelemy, H., "On-Chip Voltage Regulator Protecting Against Power Analysis Attacks," in *Circuits and Systems 2006*, vol. 2, 2006, pp. 507–511.

[13] Telandro, Vincent and Kussener, Edith and Barthélemy, Hervé and Malherbe, Alexandre, "A bi-channel voltage regulator protecting smart cards against power analysis attacks," *Analog Integrated Circuits and Signal Processing*, vol. 59, no. 3, pp. 275–285, 2009.

[14] Daniel Mesquita and Jean-Denis Techer and Lionel Torres and Michel Robert and Guy Cathebras and Gilles Sassatelli and Fernando Gehm Moraes, "Current Mask Generation: an Analog Circuit to Thwart DPA Attacks," in *VLSI-SoC 2005*, ser. IFIP, vol. 240. Springer, 2007, pp. 317–330.

[15] Daniel Mesquita and Jean-Denis Techer and Lionel Torres and Gilles Sassatelli and Gaston Cambon and Michel Robert and Fernando Moraes, "Current mask generation: a transistor level security against DPA attacks," in *SBCCI 2005*. ACM, 2005, pp. 115–120.

[16] Adi Shamir, "Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies," in *CHES 2000*, ser. LNCS, vol. 1965. Springer, 2000, pp. 71–77.

[17] Thomas Plos, "Evaluation of the Detached Power Supply as Side-Channel Analysis Countermeasure for Passive UHF RFID Tags," in *CT-RSA 2009*, ser. LNCS, vol. 5473. Springer, 2009, pp. 444–458.

[18] Carlos Tokunaga and David Blaauw, "Securing Encryption Systems With a Switched Capacitor Current Equalizer," *J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, 2010.

[19] Pasquale Corsonello, Martin Margala, and Stefania Perri, "Charge Pump Based Subsystem for Secure Smart-Card Design," Patent WO 2006/076591 A2, 2006.

[20] Pasquale Corsonello and Stefania Perri and Martin Margala, "An integrated countermeasure against differential power analysis for secure smart-cards," in *ISCAS 2006*. IEEE, 2006.

[21] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher," in *CHES 2007*, ser. LNCS. Springer, 2007, vol. 4727, pp. 450–466.

[22] K. Tiri, D. D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype IC with WDDL and Differential Routing - DPA Resistance Assessment," in *CHES 2005*, ser. LNCS, vol. 3659. Springer, 2005, pp. 354–365.

[23] M. Kirschbaum and T. Popp, "Evaluation of a DPA-Resistant Prototype Chip," in *ACSAC 2009*. IEEE Computer Society, 2009, pp. 43–50.

[24] T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints," in *CHES 2005*, ser. LNCS, vol. 3659. Springer, 2005, pp. 172–186.

[25] D. Suzuki and M. Saeki, "Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style," in *CHES 2006*, ser. LNCS, vol. 4249. Springer, 2006, pp. 255–269.

[26] A. Moradi, M. Kirschbaum, T. Eisenbarth, and C. Paar, "Masked dual-rail precharge logic encounters state-of-the-art power analysis methods," *IEEE Trans. VLSI Syst.*, vol. 20, no. 9, pp. 1578–1589, 2012. [Online]. Available: http://dx.doi.org/10.1109/TVLSI.2011.2160375

[27] "AC Current Probes," Tektronix, http://www.tek.com/sites/tek.com/files/media/media/resources/AC_Current_Probes.pdf.

[28] "Low Noise Amplifier," Mini-Circuits, http://217.34.103.131/pdfs/ZFL-1000LN+.pdf.

[29] François-Xavier Standaert, Tal Malkin, and Moti Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," in *EUROCRYPT 2009*, ser. LNCS, vol. 5479. Springer, 2009, pp. 443–461.

[30] Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi, "Template Attacks," in *CHES 2002*, ser. LNCS, vol. 2523. Springer, 2003, pp. 13–28.

[31] G. Goodwill, B. Jun, J. Jaffe, and P. Rohatgi, "A testing methodology for side channel resistance validation," in *NIST non-invasive attack testing workshop*, 2011, http://csrc.nist.gov/news_events/non-invasive-attack-testing-workshop/papers/08_Goodwill.pdf.

[32] Stefan Mangard, "Hardware Countermeasures against DPA ? A Statistical Analysis of Their Effectiveness," in *CT-RSA 2004*, ser. LNCS, vol. 2964. Springer, 2004, pp. 222–235.

[33] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proceedings of the IEEE*, vol. 94, no. 2, pp. 383–394, 2006.

[34] Amir Moradi and François-Xavier Standaert, "Moments-Correlating DPA," Cryptology ePrint Archive, Report 2014/409, 2014, http://eprint.iacr.org/.