Information Leakage of Flip-Flops in DPA-Resistant Logic Styles

Amir Moradi[1,⋆], Thomas Eisenbarth[2], Axel Poschmann[2], Carsten Rolfes[2], Christof Paar[2], Mohammad T. Manzuri Shalmani[1], and Mahmoud Salmasizadeh[1]

[1] Department of Computer Engineering and Electronic Research Center
Sharif University of Technology, Tehran, Iran
[2] Horst Görtz Institute for IT Security
Ruhr University of Bochum, Germany
{moradi,eisenbarth,poschmann,Rolfes,cpaar}@crypto.rub.de
{manzuri,salmasi}@sharif.edu

Abstract. This contribution discusses the information leakage of flip-flops for different DPA-resistant logic styles. We show that many of the proposed side-channel resistant logic styles still employ flip-flops that leak data-dependent information. Furthermore, we apply simple models for the leakage of masked flip-flops to design a new attack on circuits implemented using masked logic styles. Contrary to previous attacks on masked logic styles, our attack does not predict the mask bit and does not need detailed knowledge about the attacked device, e.g., the circuit layout. Moreover, our attack works even if all the load capacitances of the complementary logic signals are perfectly balanced and even if the PRNG is ideally unbiased. Finally, after performing the attack on DRSL, MDPL, and iMDPL circuits we show that single-bit masks do not influence the exploitability of the revealed leakage of the masked flip-flops.

1 Introduction

Since Differential Power Analysis (DPA) was introduced by Kocher *et al.* [6] to physically attack cryptographic devices, several countermeasures have been proposed to improve the resistance of implementations. Sense Amplifier Based Logic (SABL) which is a Dual-Rail Pre-charge (DRP) logic has been proposed by Tiri *et al.* [17] as the first DPA countermeasure at the cell level. In fact, using a full-custom design tool enables to equalize the load capacitances of each couple of complementary logic signals and hence to make the power consumption independent of the processed data. Afterwards Wave Dynamic Differential Logic (WDDL) [19] has been introduced in order to avoid the usage of full-custom design tools especially for the routing process. Since some place and route methods such as [20, 5] were proposed to diminish the load imbalances of complementary

⋆ Amir Moradi performed most of the work described in this contribution as a visiting researcher at the Ruhr-University of Bochum.

signals, the data-dependent time of evaluation and the memory effect of WDDL cells make it vulnerable to DPA attacks [16, 7].

Although it has been shown that masking at the cell level can not prevent the information leakage because of the presence of glitches [8], its combination with pre-charge logics led to Random Switching Logic (RSL) [15] in order to equalize the circuit transition probability. However, Tiri and Schaumont [18] showed that the single mask-bit in RSL just add one bit of entropy to the key space. On the other hand, in order to use semi-custom design tools without routing constrains, Masked Dual-Rail Pre-charge Logic (MDPL) [12] was introduced. It works similar to WDDL and employs a single mask-bit to nullify the effect of load imbalances. Moreover, Dual-Rail Random Switching Logic (DRSL) [3] was proposed to be the dual-rail version of RSL and to avoid the need of a central module to control the pre-charge signals.

Suzuki *et al.* showed that MDPL is susceptible to the early propagation effect [14]. The practical evaluation of the SCARD prototype chip[1] proved that the early propagation effect which resulted in a vulnerability of CMOS circuits also exists for MDPL cells [11]. In order to cope with the early propagation issues, the designers of MDPL introduced a so called Evaluation Pre-charge Detection Unit (EPDU), which consists of three (CMOS) AND gates and two (CMOS) OR gates. The EPDU is applied to all improved MDPL (iMDPL) gates, hence it is not surprising that the area requirements for iMDPL gates increased significantly compared to MDPL gates.

Concurrently, Gierlichs [4] presented an attack on MDPL that exploits the slight bias of a Pseudo Random Number Generator (PRNG) in combination with unbalanced wires of the mask signal. In order to mount this attack an adversary requires detailed knowledge on the layout-level of the device under attack. However, in practice this information is not publicly available or requires insider knowledge or expensive equipment and time-consuming efforts, such as reverse-engineering to gain it.

At that time, Schaumont and Tiri [13] showed that already slightly unbalanced complementary wires can be exploited to mount classical DPA attacks after only a simple filtering operation. Contrary to Gierlichs they did not exploit the unbalanced wires of the mask bit signal, but rather use only the unbalanced dual-rail wires of the logical signals.

Note that the attacks of Gierlichs and of Schaumont/Tiri can also be mounted on circuits built in iMDPL, but again require unbalanced wires and detailed knowledge of the device under attack. Therefore both attacks assume a rather strong attacker model. Furthermore, both attacks and also the attacks by Suzuki *et al.* [14] and Popp *et al.* [11] exploit leakage of the combinatorial part of a circuit. Contrary to this, Moradi *et al.* presented an attack on special circuits built in MDPL and DRSL that exploits the leakage of the underlying flip-flops [10]. They gain the Hamming distance of the mask bit with a Simple Power Analysis

[1] During the SCARD (Side-Channel Analysis Resistant Design Flow, `www.scard-project.eu`) project a prototype chip was built, that contains amongst other components three AES co-processors built in CMOS, an DRP logic, and MDPL.

(SPA), which strongly depends on the architecture of the attacked device, and subsequently attack the circuit with a Correlation Power Analysis (CPA) [2]. However, this attack is focused on a special type of flip-flops and a special architecture of the circuit.

In this work first we analyze the information leakage of CMOS flip-flops as well as the flip-flops of the known DPA-resistant logic styles. Using the introduced leakage models, we present an attack on masked logic styles that does not require any knowledge of the layout of the device nor unbalanced wires and hence can be mounted even by amateur attackers. Our attack works even if a masked dual-rail ASIC has perfectly balanced wires. Yet, perfectly balanced loads can never be achieved in practice because electrical effects will always cause different wire capacitances, even when the routing is done manually in a full-custom design process. This however underlines the strength of our attack. Compared to Moradi's attack [10], our attack is more general, because we neither focus on a special type of flip-flop nor on a special device architecture. Instead we use a modified Hamming distance model to find the leakage of the CMOS flip-flops used in masked flip-flops.

The remainder of this work is organized as follows: in Sect. 2 we recall the design of standard CMOS flip-flops which are used in many proposed side-channel resistant logic styles, e.g. WDDL and MDPL. There we also develop leakage models for CMOS, DRP, and masked flip-flops. Based on these leakage models we propose a new attack in Sect. 3. Subsequently, we present our results of a simulated attack on a reduced AES round and a reduced PRESENT round in Sect. 4. Finally, Sect. 5 concludes the paper.

2 Information Leakage of Flip-Flops

In this section we describe leakage models of flip-flops. Starting with CMOS flip-flops in Sect. 2.1, we continue with DRP flip-flops in Sect. 2.2, and finally end with masked flip-flops in Sect. 2.3.

2.1 CMOS Flip-Flops

The information leakage of CMOS flip-flops was already modeled by the first DPA attacks. It is well-known that the dynamic power consumption is higher when the content of a single-bit flip-flop is changed than if the content remains unchanged. Therefore, Hamming distance of the registers is applied to model the power consumption of a circuit. Although the specification of the power consumption of a particular CMOS flip-flop is given by [10], we generally review the structure of an edge-sensitive flip-flop to figure out its information leakage.

Typically, edge-sensitive flip-flops are built using two consecutive latches. The block diagram of a positive-edge flip-flop is shown in Fig. 1. Note that the negative-edge one can be constructed by swapping the CLK and CLKN signals. For instance, the structure shown in [10] for a positive-edge flip-flop is a specific structure which is used by a manufacturer. In fact, each manufacturer has its own

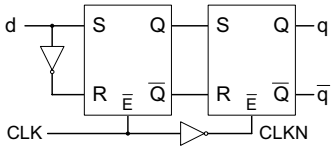


Fig. 1. Typical block diagram of an edge-sensitive flip-flop

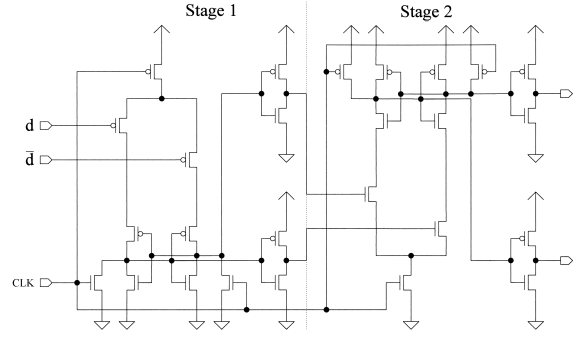


Fig. 2. SABL-DFF [7]

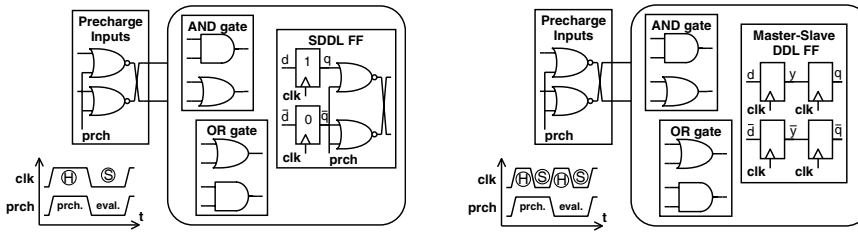
design to build edge-sensitive CMOS flip-flops, but the fundamental architecture corresponds to that shown in Fig. 1. We define two operation phases: sampling phase and hold phase. In a positive-edge flip-flop, the first latch samples the input during the sampling phase while the CLK signal is stable at 0. When the CLK signal switches to 1, i.e., beginning of the hold phase, the connection of the two latches is established and the content of the flip-flop is updated. Obviously, at this point in time the power consumption is influenced by the change of the content of the second latch (i.e., flip-flop content). As mentioned, this leakage is widely used as Hamming distance model. However, during the sampling phase, changing the input signal (i.e., d) results in a change of the content of the first latch, and it also affects the power consumption.

Suppose a circuit with n synchronous flip-flops where all of the flip-flops are controlled and are triggered by a clock signal. As mentioned before, toggling the input signal directly affects the power consumption at the sampling phase. Thus, the toggle count model is the appropriate choice for the power consumption model, $Leak_{\textcircled{S}}$. We model the leakage of the flip-flops as follows:

$$\begin{aligned} Leak_{\textcircled{S}} &= \textstyle\sum_{i=1}^{n} \text{number of toggles at the input signal (d) of FF}_i \\ &= \text{ToggleCount}\left(\mathrm{D} = [\mathrm{d}_n, \ldots, \mathrm{d}_2, \mathrm{d}_1]\right) \end{aligned} \tag{1}$$

In addition to [10], our simulation results show that the difference between the effect of the rising and the falling toggles in the input signal is negligible. Also, the well known Hamming distance model describes the power consumption at the hold phase.

$$\begin{aligned} Leak_{\textcircled{H}} &= \textstyle\sum_{i=1}^{n} \text{number of toggles at the output signal (q) of FF}_i \\ &= \text{HD}\left(\mathrm{Q} = [\mathrm{q}_n, \ldots, \mathrm{q}_2, \mathrm{q}_1]\right) \end{aligned} \tag{2}$$



(a) SDDL FF (b) M-S DDL FF

Fig. 3. WDDL flip-flops [19]

2.2 DRP Flip-Flops

Amongst DRP logic styles, we focus on SABL [17] and WDDL [19], because with regards to side-channel resistance they are the best investigated logic styles. Since SABL is a full-custom logic style, its flip-flop was specifically designed to have a constant internal power consumption independent of the logic values. As shown in Fig. 2, an SABL flip-flop similarly to the CMOS flip-flop consists of two stages. The first stage stores the complementary input values d and $\overline{\mathrm{d}}$ at the negative edge of the CLK, while the second stage is pre-charged. At the next positive clock edge, the second stage stores the data values from the first stage. Then, the first stage is pre-charged and the second one provides the output values q and $\overline{\mathrm{q}}$ [7]. Assuming fully balanced capacitances, the power consumption of an SABL flip-flop is constant in every clock cycle independently of the input and output values. Therefore, leakage models similar to those presented in Sect. 2.1 can not be introduced for SABL flip-flops.

Two ways to launch the pre-charge wave in WDDL have been proposed, hence, there are two types of WDDL flip-flops:

(*i*) Single Dynamic Differential Logic (SDDL) flip-flop which uses two CMOS flip-flops as shown in Fig. 3(a)
(*ii*) Master-Slave Dynamic Differential Logic (M-S DDL) flip-flop which employs four CMOS flip-flops as shown in Fig. 3(b).

In fact, in comparison with SDDL FF's (with the same clock frequency) using M-S DDL FF's causes the operation frequency of the circuit to be divided by 2.

In order to model the power consumption of an SDDL FF, we first consider the power consumption of one of the internal CMOS flip-flops. The input signal, d, is 0 at the pre-charge phase (when CLK is 1). It may switch to 1 once at the evaluation phase (when CLK is 0). Therefore, if there are n synchronous SDDL flip-flops, the leakage is defined as follows.

$$\begin{aligned} Leak_{\textcircled{S}}\,[\mathrm{SDDL1}] &= \textstyle\sum_{i=1}^{n} \text{number of toggles of d of FF}_i \\ &= \mathrm{HW}\,(\mathrm{D} = [\mathrm{d}_n, \ldots, \mathrm{d}_2, \mathrm{d}_1]) \end{aligned} \tag{3}$$

Also, the Hamming distance of the output signals is clearly leaking at the hold phase.

$$Leak_{\textcircled{H}}\left[\text{SDDL1}\right] = \text{HD}\left(\text{Q} = [\text{q}_n, \ldots, \text{q}_2, \text{q}_1]\right) \tag{4}$$

Similarly, the leakages of the second internal CMOS flip-flops are defined as follows.

$$Leak_{\textcircled{S}}\left[\text{SDDL0}\right] = \text{HW}\left(\overline{\text{D}} = \left[\overline{\text{d}_n}, \ldots, \overline{\text{d}_2}, \overline{\text{d}_1}\right]\right) \tag{5}$$

$$Leak_{\textcircled{H}}\left[\text{SDDL0}\right] = \text{HD}\left(\overline{\text{Q}} = [\overline{\text{q}_n}, \ldots, \overline{\text{q}_2}, \overline{\text{q}_1}]\right) \tag{6}$$

Now, the whole leakage for each phase can be easily computed by adding two leakages.

$$\begin{aligned} Leak_{\textcircled{S}}\left[\text{SDDL}\right] &= Leak_{\textcircled{S}}\left[\text{SDDL1}\right] + Leak_{\textcircled{S}}\left[\text{SDDL0}\right] \\ &= \text{HW}\left(\text{D}\right) + \text{HW}\left(\overline{\text{D}}\right) = n \end{aligned} \tag{7}$$

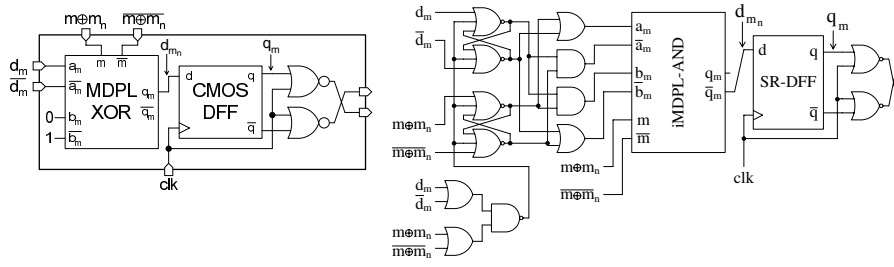
$$\begin{aligned} Leak_{\textcircled{H}}\left[\text{SDDL}\right] &= Leak_{\textcircled{H}}\left[\text{SDDL1}\right] + Leak_{\textcircled{H}}\left[\text{SDDL0}\right] \\ &= \text{HD}\left(\text{Q}\right) + \text{HD}\left(\overline{\text{Q}}\right) = 2 \cdot \text{HD}\left(\text{Q}\right) \end{aligned} \tag{8}$$

Therefore, SDDL flip-flops do not leak any information during the sampling phase, but their leakage is twice of the CMOS flip-flops in the hold phase (again note that we do not consider the unbalanced capacitances of the complementary wires in this article). Thus, successful power analysis attacks can be mounted on hardware where SDDL flip-flops are used.

As shown in Fig. 3(b), there are two sampling and two hold phases in each pre-charge evaluation phase in the case of M-S DDL FF's. During the first sampling phase, none of the input signals d, $\overline{\text{d}}$, y, and $\overline{\text{y}}$ is changed, and hence there is no leakage. Also, in the second sampling phase, signals y and $\overline{\text{y}}$ are not changed. However, since the second hold and sampling phases both are in evaluation phase, one of the input signals d and $\overline{\text{d}}$ may change in the second sampling phase depending on the delay of the combinational circuit which provides them. If so, the leakage model is similar to that defined in Eq. 7, hence, it is data-independent. Whereas in each hold phase of a pre-charge-evaluation phase one set of the master and slave dual-rail flip-flops stores a pre-charge value, i.e., 0, their hold-phase leakage is modeled by Hamming weight too, and it is the same as Eq. 7. As a result, it is not possible to perform a power analysis attack using our leakage model and our assumptions on M-S DDL FF's.

2.3 Masked Flip-Flops

In the case of DRSL, MDPL, and iMDPL flip-flops, each of the logic styles has a special circuit to mask the input signal using the mask bit of the next clock cycle. However, all have in common that they use a CMOS flip-flop. Although the early propagation problem of the MDPL gates is solved in the improved version, i.e., iMDPL, the structure of the flip-flops is the same for both versions. Cell schematic of the original MDPL and iMDPL flip-flops are shown in Fig. 4 (the structure of the DRSL flip-flop is the same as MDPL). The input signal of the internal CMOS flip-flop, i.e., $\text{d}_{\text{m}_\text{n}}$, is 0 at the pre-charge phase (when CLK



(a) (b)

Fig. 4. (a) MDPL-DFF [12] and (b) iMDPL-DFF [11]

is 1). It switches to 1 once at the evaluation phase (when CLK is 0) depending on d and the next mask bit, $\mathrm{m_n}$. Therefore, if there are n synchronous masked flip-flops, the leakage during the sampling phase can be modeled as follows:

$$\begin{aligned} Leak_{\textcircled{S}}\,[\text{Masked}] &= \textstyle\sum_{i=1}^{n} \text{number of toggles of } \mathrm{d_{m_n}} \text{ of } \mathrm{FF}_i \\ &= \mathrm{HW}\left(\mathrm{D_{m_n}} = \left[\mathrm{d}_{n_{\mathrm{m_n}}}, \ldots, \mathrm{d}_{2_{\mathrm{m_n}}}, \mathrm{d}_{1_{\mathrm{m_n}}}\right]\right) \\ &= \mathrm{HW}\left(\left[\mathrm{d}_n, \ldots, \mathrm{d}_2, \mathrm{d}_1\right]_{\mathrm{m_n}}\right) = \mathrm{HW}\left(\mathrm{D} \oplus \mathrm{m_n}\right) \end{aligned} \tag{9}$$

In other words, the Hamming weight of the input values which are masked by a single mask-bit is leaking at the sampling phase. Moreover, the Hamming distance of the output signals is leaking at the hold phase.

$$\begin{aligned} Leak_{\textcircled{H}}\,[\text{Masked}] &= \textstyle\sum_{i=1}^{n} \text{number of toggles of } \mathrm{q_m} \text{ of } \mathrm{FF}_i \\ &= \mathrm{HD}\left(\mathrm{Q_m} = [\mathrm{q}_{n_{\mathrm{m}}}, \ldots, \mathrm{q}_{2_{\mathrm{m}}}, \mathrm{q}_{1_{\mathrm{m}}}]\right) \\ &= \mathrm{HW}\left(\mathrm{Q_m}^{(t)} \oplus \mathrm{Q_{m_n}}^{(t+1)}\right) \\ &= \mathrm{HW}\left(\left(\mathrm{Q}^{(t)} \oplus \mathrm{m}\right) \oplus \left(\mathrm{Q}^{(t+1)} \oplus \mathrm{m_n}\right)\right) \\ &= \mathrm{HW}\left(\left(\mathrm{Q}^{(t)} \oplus \mathrm{Q}^{(t+1)}\right) \oplus \left(\mathrm{m} \oplus \mathrm{m_n}\right)\right) \\ &= \mathrm{HW}\left(\left(\mathrm{Q}^{(t)} \oplus \mathrm{Q}^{(t+1)}\right) \oplus \mathrm{m}'\right) = \mathrm{HD}\left(\mathrm{Q} \oplus \mathrm{m}'\right) \end{aligned} \tag{10}$$

In fact, $Leak_{\textcircled{S}}$ is not used often, and the first time it has been used is in [10] in order to exploit the the difference between consecutive mask bits. Clearly, it is not possible to mount a classical DPA or CPA using the leakages described above, because the mask bit ($\mathrm{m_n}$ or m') which contributes to the leakages is refreshed every clock cycle, e.g., by a PRNG. In the next section we illustrate a new attack strategy to reveal the secret information using these leakages.

MDPL has a timing constraint for the flip-flops. The constraint requires creating the clock tree in a specific manner [12]. An alternative design (similar to the M-S DDL flip-flop) which uses four CMOS flip-flops has been proposed for cases where the timing constraint can not be met [12]. As mentioned for the M-S DDL, this kind of flip-flop requires four times the area and the clock rate must be doubled in order to keep the data rate of the circuit constant. Of course

this results in a significant increase of the power consumption. However, a design employing this type of flip-flop does not leak any information. This design has not been proposed for DRSL and iMDPL, but it is applicable for them with all its disadvantages. However, it was not considered in the literature and in implementations (for instance in the SCARD chip) because no one was aware of this leakage.

Also, the authors in [10] proposed a modification on the structure of MDPL and DRSL flip-flops, i.e., using two CMOS flip-flops in each masked flip-flop in order to prevent the information leakage. The leakage models of the new masked flip-flops are as follows:

$$Leak_{\textcircled{S}}\left[\text{Masked}^*\right] = \text{HW}\left(\text{D} \oplus \text{m}_\text{n}\right) + \text{HW}\left(\overline{\text{D}} \oplus \text{m}_\text{n}\right) = n \tag{11}$$

$$Leak_{\textcircled{H}}\left[\text{Masked}^*\right] = \text{HD}\left(\text{Q} \oplus \text{m}'\right) + \text{HD}\left(\overline{\text{Q}} \oplus \text{m}'\right) = 2 \cdot \text{HD}\left(\text{Q} \oplus \text{m}'\right) \tag{12}$$

Their proposed modification prevents the leakage in the sampling phase, but it increases the leakage of the hold phase compared to the original design.

3 Our Proposed Attack

For simplicity, we assume an 8-bit masked flip-flop as target of the attack. As illustrated in the previous section, during the sampling phase the Hamming weight of the masked input signals, $Leak_{\textcircled{S}} = \text{HW}(\text{D}_{\text{m}_\text{n}})$, is leaking. In fact, we are looking for a technique to discover a relation between the unmasked values D and the Hamming weight of the masked values. Table 1 shows all possible values of the Hamming weight of an 8-bit masked input, $\text{D}_{\text{m}_\text{n}}$. As shown in the fourth column, the average of the Hamming weights, $\mu(\text{HW}\left(\text{D}_{\text{m}_\text{n}}\right))$, is always 4. However, the difference between the Hamming weights when the mask bit is 0 or 1, $|\text{HW}\left(\text{D}_0\right) - \text{HW}\left(\text{D}_1\right)|$, takes certain values depending on the Hamming weight of D. Indeed, there is a relation between the unmasked value, D, and the difference between the Hamming weights. This difference is given in the last column of Table 1. We call it *Difference of Hamming Weights* ($\text{DHW}\left(\text{D}\right) = |\#\text{ofBits} - 2 \cdot \text{HW}\left(\text{D}\right)|$) and use this model to mount an attack without prediction or estimation of the mask bit.

One can also conclude from Table 1 that the distance of one individual leakage $\text{HW}(\text{D}_{\text{m}_\text{n}})$ for an unknown mask bit m_n to the average of the Hamming weights $\mu(\text{HW}(\text{D}_{\text{m}_\text{n}}))$ is the same independent of the mask bit m_n. Hence,

$$|\mu(\text{HW}(\text{D}_{\text{m}_\text{n}})) - \text{HW}(\text{D}_0)| = |\mu(\text{HW}(\text{D}_{\text{m}_\text{n}})) - \text{HW}(\text{D}_1)| = \frac{1}{2}\text{DHW}(\text{D})$$

We can not directly predict the leakage of a masked flip-flop, but by subtracting the average power consumption $\mu(Leak_{\textcircled{S}}) = \mu(\text{HW}(\text{D}_{\text{m}_\text{n}}))$ from the individual power consumption

$$|Leak_{\textcircled{S}} - \mu(Leak_{\textcircled{S}})| = |\text{HW}(\text{D}_{\text{m}_\text{n}}) - \mu(\text{HW}(\text{D}_{\text{m}_\text{n}}))| = \frac{1}{2}\text{DHW}(\text{D})$$

Table 1. Hamming weight of an 8-bit data masked by a single mask bit

HW (D)	HW (D_{m_n})		μ(HW (D_{m_n}))	DHW (D) = | HW (D_0) − HW (D_1) | = | 8 − 2 · HW (D) |
	$m_n = 0$	$m_n = 1$		
0	0	8	4	8
1	1	7	4	6
2	2	6	4	4
3	3	5	4	2
4	4	4	4	0
5	5	3	4	2
6	6	2	4	4
7	7	1	4	6
8	8	0	4	8

we can predict this distance using the Difference of Hamming Weights. We now use the DHW(D) as a hypothetical power model and perform a CPA attack on the pre-processed power traces. For clarity, a pseudocode overview of the attack is given in Algorithm 1.

Algorithm 1 The attack algorithm

1: $\mu(p) = \frac{\sum_{i=1}^{k} p_i}{k}$; $p_i : i^{\text{th}}$ sampled power value, k: # of samples
2: **for all** power values $p_i, 1 \leq i \leq k$ **do**
3: $\quad \widehat{p_i} = |p_i - \mu(p)|$
4: **end for**
5: **Perform** a **CPA** on $\widehat{p}$ **using leakage model** DHW $(\cdot)$

The illustrated leakage model, DHW $(\cdot)$, fits the sampling phase leakage of the masked flip-flops, $Leak_{\textcircled{S}}$. Also, it can be applied to the hold phase leakage, $Leak_{\textcircled{H}}$, by replacing the Hamming weight with the Hamming distance in Table 1. In fact, the table is the same for HD, just the notation will be changed, i.e., *Difference of Hamming Distances*, DHD (Q) = |#ofBits − 2 · HD (Q)|.

Note that the success rate of this attack depends on the estimation of the average of power values. Hence, a large amount of samples is needed to approximate the average leakage. In the next section the simulation results of the attacks performed on several circuits are presented.

4 Simulation Results

In order to evaluate the efficiency of the proposed attack, we analyzed the circuits shown in Fig. 5. The first test circuit shown in Fig. 5(a) consists of an 8-bit key addition and an AES S-box followed by an 8-bit flip-flop, Fig. 5(b) shows

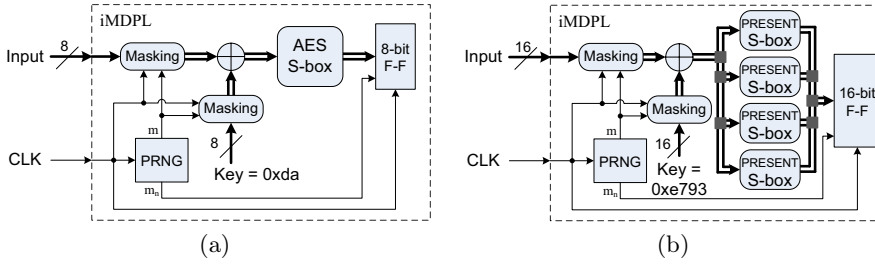


Fig. 5. Block diagram of the attacked devices

a 16-bit key addition, four S-boxes of the PRESENT block cipher [1], and a 16-bit flip-flop. Both are implemented using iMDPL. We simulated the HSPICE description files for thousands of random inputs using *Synopsys Nanosim* version *A-2007.12* in 0.18μm technology and 1.8V supply voltage to obtain the power supply current traces. As mentioned earlier, we do not consider the difference between the capacitances of complementary wires arising from different routings. Thus, we supposed that the capacitances of each couple of complementary wires to be the same. Moreover, in order to simulate the electronic noise that usually affects side-channel measurements, random noise with Gaussian distribution and standard deviation of 1 mA was added to the current measurements.

First, the leakage of the sampling phase $Leak_{\textcircled{S}}$ is taken into consideration. As described in Sect. 2.3, this leakage is caused by the toggling of inputs of the flip-flops that are the outputs of a combinational circuit. Since the depth (and consequently the delay time) of all output signals of a combinational circuit are not the same, the sampling phase leakage does not appear at specific points of the power traces. Moreover, in MDPL circuits, where the time-of-evaluation depends on the processed data (and on the mask bit), the leakage is caused at different time instances of the sampling phase. Therefore, the integral (or the average) of the power values during a specific period of time is used to mount the attack on the sampling phase[2]. Finally, we performed the attack which is described in Algorithm 1 using the leakage model presented in Eq. 9 on the circuit shown in Fig. 5(a). The correlation coefficient of the correct key hypothesis (solid black line) and the wrong hypotheses (gray lines) plotted over the number of measurements is shown in Fig. 6.

Contrary to the sampling phase leakage it is expected that the leakage of the hold phase appears at specific point(s) of the power traces, because the hold phase leakage $Leak_{\textcircled{H}}$ coincides with the positive clock edge (beginning of the pre-charge phase), and all the synchronous flip-flops are triggered at the same time. The previous attack was repeated using the leakage model presented in Eq. 10. As a result Fig. 7 shows the correlation coefficient of the key hypotheses for the

[2] This step needs to be performed because of the high accuracy of the simulations. In power traces measured from a real chip these leakages appear as a single peak [9].

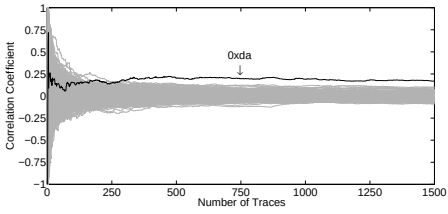


Fig. 6. Correlation coefficient of the key hypotheses vs. the number of traces using the sampling phase leakage model

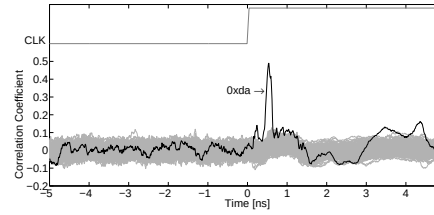
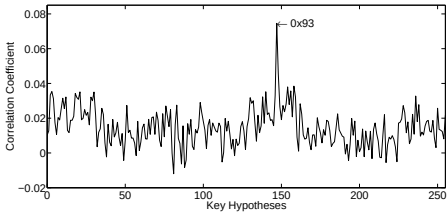
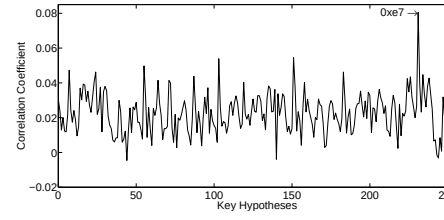


Fig. 7. Correlation coefficient of the key hypotheses using the hold phase leakage model



(a) Low key byte



(b) High key byte

Fig. 8. Correlation coefficient of the key hypotheses

different points of power traces using just $1,500$ measurements. Obviously, the maximum correlation for the correct key guess appears directly after the rising edge of the clock signal.

We repeated the attack on the hold phase leakage $Leak_{\textcircled{H}}$ of the circuit as shown in Fig. 5 (b). In fact, we tried to consider the switching noise in the power values in such a way that we just predicted 8 flip-flops of the circuit (to recover only 8 bits of the secret key). The leakage of the remaining 8 bits of the 16-bit flip-flop can hence be considered as switching noise. Fig. 8 shows the results of the attack using $10,000$ measurements. Due to the additional noise added by the unpredicted registers and additional S-boxes we needed to increase the number of measurements. The attack is still applicable although the difference between the correlation coefficient of the correct hypothesis and the wrong hypotheses is not as high as the result of the attack on the previous circuit.

We limited the attack results to the iMDPL circuits since the structure (and, hence, also our leakage models) of MDPL and DRSL flip-flops are identical to iMDPL. Indeed, we repeated the attack on corresponding MDPL and DRSL circuits as well as the modified structure proposed in [10]. All attacks led to the same results as shown for the iMDPL.

5 Conclusion

In this work we discussed the leakage for a wide range of side-channel resistant logic styles. Unlike most of the previous contributions, we did not focus our analysis on combinational parts of the logic. Instead we analyzed the leakage of flip-flop designs for various side-channel resistant logic styles. Our results show that logic masking where more than one flip-flop shares a single-bit mask does not prevent information leakage of those flip-flops. In other words, using the leakage we found in the masked flip-flops, a single-bit mask can not improve the security and even can not add one bit of entropy to the key space.

We furthermore presented a new attacking scheme that exploits the leakage of masked flip-flops. The attack does neither rely on unbalanced loads for the two parts of a differential signal, nor does the attacker need a detailed knowledge of the target layout or implementation. Instead it uses the newly proposed *Difference of Hamming Weight* (DHW) and *Difference of Hamming Distance* (DHD) model for predicting the data-dependent power consumption of the flip-flops. Using DHW and DHD as power model for a classical Correlation Power Analysis attack simply renders the single bit masks of a flip-flop useless. Hence the attack neither needs a biased PRNG nor is a mask bit detection step needed as in [13]. We proved the feasibility of our attack on two different ciphers and all masked DRP logic styles proposed so far.

Since most of the prior analysis of side-channel resistant logic styles focused on the combinational logic, so did the research to improve those logic styles. We think it is time to switch the focus of research to find methods for designing side-channel resistant flip-flops with a decent area and power consumption and a low impact on the operation frequency. One possible approach could be combining semi-custom design for combinational logic with full-custom flip-flop design.

References

1. A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT - An Ultra-Lightweight Block Cipher. In *CHES 2007*, number 4727 in LNCS, pages 450–466. Springer, 2007.
2. E. Brier, C. Clavier, and F. Olivier. Correlation Power Analysis with a Leakage Model. In *CHES 2004*, volume 3156 of *LNCS*, pages 16–29. Springer, 2004.
3. Z. Chen and Y. Zhou. Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage. In *CHES 2006*, volume 4249 of *LNCS*, pages 242–254. Springer, 2006.
4. B. Gierlichs. DPA-Resistance Without Routing Constraints? In *CHES 2007*, volume 4727 of *LNCS*, pages 107–120. Springer, 2007.
5. S. Guilley, P. Hoogvorst, Y. Mathieu, and R. Pacalet. The "Backend Duplication" Method. In *CHES 2005*, volume 3659 of *LNCS*, pages 383–397. Springer, 2005.
6. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO 1999*, volume 1666 of *LNCS*, pages 388–397. Springer, 1999.
7. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007.

8. S. Mangard, T. Popp, and B. M. Gammel. Side-Channel Leakage of Masked CMOS Gates. In *CT-RSA 2005*, volume 3376 of *LNCS*, pages 351–365. Springer, 2005.
9. S. Mangard, N. Pramstaller, and E. Oswald. Successfully Attacking Masked AES Hardware Implementations. In *CHES 2005*, volume 3659 of *LNCS*, pages 157–171. Springer, 2005.
10. A. Moradi, M. Salmasizadeh, and M. T. M. Shalmani. Power Analysis Attacks on MDPL and DRSL Implementations. In *Information Security and Cryptology - ICISC 2007*, volume 4817 of *LNCS*, pages 259–272. Springer, 2007.
11. T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard. Evaluation of the Masked Logic Style MDPL on a Prototype Chip. In *CHES 2007*, volume 4727 of *LNCS*, pages 81–94. Springer, 2007.
12. T. Popp and S. Mangard. Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints. In *CHES 2005*, volume 3659 of *LNCS*, pages 172–186. Springer, 2005.
13. P. Schaumont and K. Tiri. Masking and Dual-Rail Logic Don't Add Up. In *CHES 2007*, volume 4727 of *LNCS*, pages 95–106. Springer, 2007.
14. D. Suzuki and M. Saeki. Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style. In *CHES 2006*, volume 4249 of *LNCS*, pages 255–269. Springer, 2006.
15. D. Suzuki, M. Saeki, and T. Ichikawa. Random Switching Logic: A Countermeasure against DPA based on Transition Probability. Cryptology ePrint Archive, Report 2004/346, 2004. `http://eprint.iacr.org/`.
16. D. Suzuki, M. Saeki, and T. Ichikawa. DPA Leakage Models for CMOS Logic Circuits. In *CHES 2005*, volume 3659 of *LNCS*, pages 366–382. Springer, 2005.
17. 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 *European Solid-State Circuits Conference - ESSCIRC 2002*, pages 403–406, 2002.
18. K. Tiri and P. Schaumont. Changing the Odds Against Masked Logic. In *Selected Areas in Cryptography 2006*, volume 4356 of *LNCS*, pages 134–146. Springer, 2006.
19. K. Tiri and I. Verbauwhede. A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation. In *Design, Automation and Test in Europe Coneference - DATE 2004*, pages 246–251, 2004.
20. K. Tiri and I. Verbauwhede. Place and Route for Secure Standard Cell Design. In *Conference on Smart Card Research and Advanced Applications - CARDIS 2004*, pages 143–158. Kluwer, 2004.