Power Analysis of Single-Rail Storage Elements as used in MDPL*

Amir Moradi[1], Thomas Eisenbarth[1], Axel Poschmann[2], and Christof Paar[1]

[1] Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
{moradi, eisenbarth, cpaar}@crypto.rub.de
[2] Division of Mathematical Sciences, Nanyang Technological University, Singapore
aposchmann@ntu.edu.sg

Abstract. Several dual-rail logic styles make use of single-rail flip-flops for storing intermediate states. We show that single mask bits, as applied by various side-channel resistant logic styles such as MDPL and iMDPL, are not sufficient to obfuscate the remaining leakage of single-rail flip-flops.
By applying simple models for the leakage of masked flip-flops, we design a new attack on circuits implemented using masked single-rail flip-flops. 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 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.* [5] 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 Precharge (DRP) logic, has been proposed by Tiri *et al.* [17] as the first DPA countermeasure at the cell level. In fact, in theory 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 [4, 20] were proposed to diminish the load imbalances of complementary signals, the data-dependent time of evaluation and the memory effect of WDDL cells make it vulnerable to DPA attacks [6, 15].

* The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.

Although it has been shown that masking at cell level can not prevent the information leakage because of the presence of glitches [7], its combination with precharge logics led to Random Switching Logic (RSL) [16] in order to equalize the circuit transition probability. However, Tiri and Schaumont [18] showed that the single mask-bit in RSL just adds one bit of entropy. On the other hand, in order to use semi-custom design tools without routing constraints, Masked Dual-Rail Precharge 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) [2] was proposed as the dual-rail version of RSL and to avoid the need of a central module to control the precharge signals.

Suzuki *et al.* showed that MDPL is susceptible to the early propagation effect [14]. The practical evaluation of the MDPL microprocessor 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 early propagation issues, the designers of MDPL introduced a so called Evaluation-Precharge 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.

Concurrently, Gierlichs [3] presented an attack on MDPL that exploits a deviation in the mask bit distribution and unbalanced dual-rails in the target cell. In order to mount this attack an adversary requires detailed knowledge on the layout-level of the target device. However, in practice this information is not publicly available or requires insider knowledge or expensive equipment and time-consuming efforts, such as reverse-engineering.

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, a key recovery attack on special circuits built in MDPL and DRSL that exploits the leakage of the underlying flip-flops has been presented in [9]. The authors gain the Hamming distance (HD) of the mask bit with a Simple Power Analysis (SPA) and subsequently attack the circuit with a Correlation Power Analysis (CPA) [1]. Note that the success rate of any SPA

[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 MC 8051s and three AES co-processors built in CMOS, a DRP logic, and MDPL.

strongly depends on the architecture of the attacked device. However, this attack is focused on a special type of flip-flops and a special architecture of the circuit that might not lead to a successful result in practice.

Moreover, practical attacks on the MDPL AES co-processor of the SCARD chip presented in [10] show that not only the early propagation effect of MDPL cells does not break the masked hardware but also the attack proposed by Schaumont/Tiri is not capable of revealing the secrets in this case. Further, it has been shown that a bias of the mask bit in the SCARD chip does not threaten the resistance of the device.

In this work first we analyze the information leakage of CMOS flip-flops as well as the flip-flops of some known DPA-resistant logic styles. Using the introduced leakage models, we present an attack on certain types of flip-flops in masked logic styles that does not require any knowledge of the layout of the device nor unbalanced wires. 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. Indeed, our attack is based on the fact that although combinational parts of the masked logic styles, e.g., iMDPL, are in dual-rail mode and decrease the leakage significantly, their sequential parts are built in single-rail leading to a serious vulnerability.

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. 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 implementations of a reduced round AES in Sect. 4. Further, we discuss on practical issues in Sect. 5, and finally Sect. 6 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, HD of the registers is applied to partially model the power consumption of a circuit. 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. 6. Note that the negative-edge one can be constructed by swapping the CLK and CLKN signals. In fact, each manufacturer has its own design to build edge-sensitive CMOS flip-flops, but the fundamental architecture corresponds to that shown in Fig. 6. We define two operation phases for a flip-flop: 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 HD 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 k 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 at the sampling phase directly affects the power consumption. Our simulation results show that the difference between the effect of the rising and the falling toggles in the input signal is negligible. Thus, the toggle count model is an appropriate choice to model the leakage of the flip-flops at the sampling phase as follows:

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize S}} &= \textstyle\sum_{i=1}^{k} \text{number of toggles at the input signal d of the } i\text{th FF} \\ &= \text{ToggleCount}\left(\mathrm{D} = [\mathrm{d}_k, \ldots, \mathrm{d}_2, \mathrm{d}_1]\right) \end{aligned} \tag{1}$$

Also, the well known HD model describes the power consumption at the hold phase.

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize H}} &= \textstyle\sum_{i=1}^{k} \text{number of toggles at the output signal q of the } i\text{th FF} \\ &= \text{HD}\left(\mathrm{Q}^{(\mathrm{t})} = \left[\mathrm{q}_k^{(\mathrm{t})}, \ldots, \mathrm{q}_2^{(\mathrm{t})}, \mathrm{q}_1^{(\mathrm{t})}\right], \mathrm{Q}^{(\mathrm{t}+1)}\right) \end{aligned} \tag{2}$$

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 independently of the logic values. As shown in Fig. 7, 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 precharged. At the next positive clock edge, the second stage stores the data values from the first stage. Then, the first stage is precharged and the second one provides the output values q and $\overline{\mathrm{q}}$ [6]. 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 precharge 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. 8(a)

(ii) Master-Slave Dynamic Differential Logic (M-S DDL) flip-flop which employs four CMOS flip-flops as shown in Fig. 8(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 precharge phase (when CLK is 1). It may switch to 1 once at the evaluation phase (when CLK is 0). Therefore, if there are k synchronous SDDL flip-flops, the leakage is defined as follows.

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{SDDL1}\right] &= \textstyle\sum_{i=1}^{k} \text{number of toggles at signal d of the } i\text{th FF} \\ &= \mathrm{HW}\left(\mathrm{D} = \left[\mathrm{d}_k, \ldots, \mathrm{d}_2, \mathrm{d}_1\right]\right) \end{aligned} \tag{3}$$

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

$$\mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{SDDL1}\right] = \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})} = \left[\mathrm{q}_k^{(\mathrm{t})}, \ldots, \mathrm{q}_2^{(\mathrm{t})}, \mathrm{q}_1^{(\mathrm{t})}\right], \mathrm{Q}^{(\mathrm{t+1})}\right) \tag{4}$$

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

$$\mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{SDDL0}\right] = \mathrm{HW}\left(\overline{\mathrm{D}} = \left[\overline{\mathrm{d}}_k, \ldots, \overline{\mathrm{d}}_2, \overline{\mathrm{d}}_1\right]\right) \tag{5}$$

$$\mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{SDDL0}\right] = \mathrm{HD}\left(\overline{\mathrm{Q}}^{(\mathrm{t})} = \left[\overline{\mathrm{q}}_k^{(\mathrm{t})}, \ldots, \overline{\mathrm{q}}_2^{(\mathrm{t})}, \overline{\mathrm{q}}_1^{(\mathrm{t})}\right], \overline{\mathrm{Q}}^{(\mathrm{t+1})}\right) \tag{6}$$

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

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{SDDL}\right] &= \mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{SDDL1}\right] + \mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{SDDL0}\right] \\ &= \mathrm{HW}\left(\mathrm{D}\right) + \mathrm{HW}\left(\overline{\mathrm{D}}\right) = k \end{aligned} \tag{7}$$

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{SDDL}\right] &= \mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{SDDL1}\right] + \mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{SDDL0}\right] \\ &= \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t+1})}\right) + \mathrm{HD}\left(\overline{\mathrm{Q}}^{(\mathrm{t})}, \overline{\mathrm{Q}}^{(\mathrm{t+1})}\right) \\ &= 2 \cdot \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t+1})}\right) \end{aligned} \tag{8}$$

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. 8(b), there are two sampling and two hold phases in each precharge-evaluation phase in the case of M-S DDL FF's. In each clock cycle every dual-rail flip-flops contain precharge value, i.e., $(0, 0)$, and are replaced by a differential value, $(1, 0)$ or $(0, 1)$, or vice versa. Thus, both leakage models in sampling and hold phases are similar to that defined in Eq. 7, hence they are data-independent. 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. 9. The structure of the DRSL flip-flop is the same as MDPL; a DRSL XOR gate is used instead of the MDPL XOR [2]. The input signal of the internal CMOS flip-flop, i.e., $\mathrm{d}_{\mathrm{m_n}}$, is 0 at the precharge phase (when CLK 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 k synchronous masked flip-flops, the leakage during the sampling phase can be modeled as follows:

$$\begin{aligned} Leak_{\circledS}\,[\text{Masked}] &= \textstyle\sum_{i=1}^{k} \text{number of toggles at } \mathrm{d}_{\mathrm{m_n}} \text{ of the } i\text{th FF} \\ &= \mathrm{HW}\left(\mathrm{D}_{\mathrm{m_n}} = \left[\mathrm{d}_{k_{\mathrm{m_n}}}, \ldots, \mathrm{d}_{2_{\mathrm{m_n}}}, \mathrm{d}_{1_{\mathrm{m_n}}}\right]\right) \\ &= \mathrm{HW}\left(\left[\mathrm{d}_k, \ldots, \mathrm{d}_2, \mathrm{d}_1\right]_{\mathrm{m_n}}\right) = \mathrm{HW}\left(\mathrm{D} \oplus [\mathrm{m_n}, \ldots, \mathrm{m_n}]\right) \end{aligned} \tag{9}$$

In other words, what is leaked at the sampling phase is the HW of the masked input values. Moreover, the HD of the output signals is leaking at the hold phase.

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

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 secrets using the presented leakage models.

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 under our assumptions. 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, e.g., the SCARD chip.

Also, a modification on the structure of MDPL and DRSL flip-flops has been proposed in [9], i.e., make use of two CMOS flip-flops in each masked flip-flop in order to prevent the leakage. The leakage models of the new masked flip-flops are as follows:

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize S}}\left[\mathrm{Masked}^*\right] &= \mathrm{HW}\left(\mathrm{D} \oplus \left[\mathrm{m_n}, \ldots, \mathrm{m_n}\right]\right) + \mathrm{HW}\left(\overline{\mathrm{D}} \oplus \left[\mathrm{m_n}, \ldots, \mathrm{m_n}\right]\right) \\ &= k \end{aligned} \tag{11}$$

$$\begin{aligned} \mathit{Leak}_{\textcircled{\scriptsize H}}\left[\mathrm{Masked}^*\right] &= \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t}+1)} \oplus \left[\mathrm{m}', \ldots, \mathrm{m}'\right]\right) + \\ &\quad\ \mathrm{HD}\left(\overline{\mathrm{Q}}^{(\mathrm{t})}, \overline{\mathrm{Q}}^{(\mathrm{t}+1)} \oplus \left[\mathrm{m}', \ldots, \mathrm{m}'\right]\right) \\ &= 2 \cdot \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t}+1)} \oplus \left[\mathrm{m}', \ldots, \mathrm{m}'\right]\right) \end{aligned} \tag{12}$$

The proposed modification prevents sampling-phase leakage, 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 the target of the attack. As illustrated in the previous section, during the sampling phase HW of the masked input signals, $\mathit{Leak}_{\textcircled{\scriptsize S}} = \mathrm{HW}(\mathrm{D_{m_n}})$, is leaking. In fact, we are looking for a technique to discover a relation between the unmasked values D and HW of the masked values. Table 1 shows all possible values of HW of an 8-bit masked input, $\mathrm{D_{m_n}}$. As shown in the fourth column, the average of HWs, $\mu(\mathrm{HW}\left(\mathrm{D_{m_n}}\right))$, is always 4. In other words, the mask bit switches the flip-flop's content between two complementary states where sum of HWs is always 8. However, the difference between HWs when the mask bit is 0 or 1, $|\mathrm{HW}\left(\mathrm{D_0}\right) - \mathrm{HW}\left(\mathrm{D_1}\right)|$, takes certain values depending on HW of D. Indeed, there is a relation between the unmasked value, D, and the difference between HWs. This difference is given in the last column of Table 1. We call it *Difference of Hamming Weights* ($\mathrm{DHW}\left(\mathrm{D}\right) = |\#\mathrm{ofBits} - 2 \cdot \mathrm{HW}\left(\mathrm{D}\right)|$) and later will use it 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 $\mathrm{HW}(\mathrm{D_{m_n}})$ for an unknown mask bit $\mathrm{m_n}$ to the average of HWs $\mu(\mathrm{HW}(\mathrm{D_{m_n}}))$ is the same independent of the mask bit $\mathrm{m_n}$. Hence,

$$|\mu(\mathrm{HW}(\mathrm{D_{m_n}})) - \mathrm{HW}(\mathrm{D_0})| = |\mu(\mathrm{HW}(\mathrm{D_{m_n}})) - \mathrm{HW}(\mathrm{D_1})| = \frac{1}{2}\mathrm{DHW}(\mathrm{D})$$

We can not directly predict the leakage of a masked flip-flop, but by subtracting the average power consumption and taking the absolute value $\mu(\mathit{Leak}_{\textcircled{\scriptsize S}}) = \mu(\mathrm{HW}(\mathrm{D_{m_n}}))$ from the individual power consumption

$$|\mathit{Leak}_{\textcircled{\scriptsize S}} - \mu(\mathit{Leak}_{\textcircled{\scriptsize S}})| = |\mathrm{HW}(\mathrm{D_{m_n}}) - \mu(\mathrm{HW}(\mathrm{D_{m_n}}))| = \frac{1}{2}\mathrm{DHW}(\mathrm{D})$$

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

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

$\mathrm{HW}(\mathrm{D})$	$\mathrm{HW}(\mathrm{D}_{\mathrm{m_n}})$		$\mu(\mathrm{HW}(\mathrm{D}_{\mathrm{m_n}}))$	$\mathrm{DHW}(\mathrm{D}) =$ $\mid \mathrm{HW}(\mathrm{D}_0) - \mathrm{HW}(\mathrm{D}_1) \mid =$ $\mid 8 - 2 \cdot \mathrm{HW}(\mathrm{D}) \mid$
	$\mathrm{m_n} = 0$	$\mathrm{m_n} = 1$		
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

Algorithm 1 The attack algorithm (for a single point of measurements)

```
$\mu = \frac{\sum_{i=1}^{z} p_i}{z}$ ; $p_i$ : $i^{\mathrm{th}}$ measured power value, $z$: # of measurements
for all measured power values $p_i, 1 \leq i \leq z$ do
    $\widehat{p_i} = |p_i - \mu|$
end for
Perform a CPA on $\widehat{P} = \{\widehat{p_i}; 1 \leq i \leq z\}$ using leakage model $\mathrm{DHW}(\cdot)$
```

the preprocessed power traces. For clarity, a pseudocode overview of the attack is given in Algorithm 1.

The illustrated leakage model, $\mathrm{DHW}(\cdot)$, fits the sampling phase leakage of the masked flip-flops, $Leak_{\circledS}$. Also, it can be applied to the hold phase leakage, $Leak_{\textcircled{H}}$, by replacing HW with HD in Table 1. In fact, the table is the same for HD, just the notation will be changed, i.e., *Difference of Hamming Distances* is

$$\mathrm{DHD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t+1})}\right) = \left|\#\mathrm{ofBits} - 2 \cdot \mathrm{HD}\left(\mathrm{Q}^{(\mathrm{t})}, \mathrm{Q}^{(\mathrm{t+1})}\right)\right|.$$

In comparison with Zero-Offset second order DPA [21], which similarly does a preprocessing step on power traces before running straight DPA, the preprocessing of our attack shows a similar time complexity of $O(z \cdot t)$, where each power trace consists of t points. On the other hand, since in masked precharged logic styles the mask bit is represented by two precharged complementary signals, the information of the mask bit, which is essentially required to perform a second-order DPA attack, is not leaking (without considering the difference between the unbalanced capacitances). Consequently, not only a classical DPA is not possible, but also a Zero-Offset 2DPA could not recover the secrets without knowing the layout details, i.e., knowledge about the loading imbalances. Our simulation results (which are not presented here) confirmed these issues. In fact, the preprocessing step of our proposed attack tries to remove the effect of single mask bit by folding the power values from an estimated mean value. Thus, from

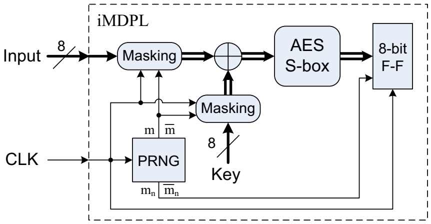


Fig. 1. Block diagram of the attacked device

this point of view, our proposed attack can be considered as a second-order DPA attack.

However, the preprocessing step is similar to the one suggested in [13], i.e., estimation of and folding around the empirical mean value per sampled time instant. Note that in their attack the preprocessing step takes place to classify the power values based on the estimated mask bit due to the leakage caused by the loading imbalances of a combinational circuit, then a CPA (or even DPA) attack using a normal HW model is performed. However, in our proposed attack after the same preprocessing step the newly proposed DHW or DHD model is used in a CPA attack to defeat the effect of the single-bit mask. Moreover, since their attack has been verified using weighted toggle count model to simulate the power consumption of a post placed-and-routed combinational circuit, they did not consider the power consumption and the leakage of the flips-flops. As a result, the principles of the attack presented in [13] and our proposed one are not the same. Further, the applicability of their attack in practice has been discussed in [10].

In fact, our leakage models, DHW and DHD, are adapted to the fact that although the masked circuits are DRP circuits, the flip-flops are only single-rail. In the next section the simulation results of attacks performed using our leakage models are presented.

4 Simulation Results

In order to evaluate the efficiency of the proposed attack, we analyzed the circuit shown in Fig. 1. It consists of an 8-bit key addition and an AES S-box followed by an 8-bit flip-flop. The circuit is implemented using iMDPL cells. 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 did not put any capacitances manually at the gate outputs.

First, we take a look at the leakage of the sampling phase $Leak_{\textcircled{S}}$. As described in Sect. 2.3, this leakage is caused by the toggling of inputs of the flip-flops

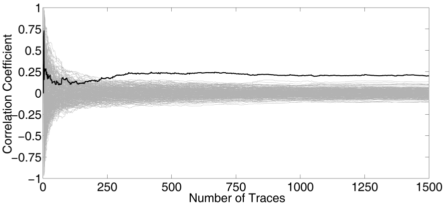


Fig. 2. Correlation coefficient of the key hypotheses vs. the number of traces using the sampling phase leakage model

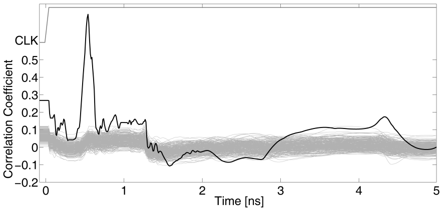


Fig. 3. Correlation coefficient of the key hypotheses using the hold phase leakage model

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. 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. 2.

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 $Leak_{\textcircled{\scriptsize H}}$ coincides with the positive clock edge (beginning of the precharge 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. 3 shows the correlation coefficient of the key hypotheses for the different points of power traces using 1 500 measurements. Obviously, the maximum correlation for the correct key guess appears directly after the rising edge of the clock signal.

We limited the attack results to the iMDPL circuits since the structure (and, hence, 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 [9] (just using hold-phase leakage). All attacks led to the same results as shown for the iMDPL.

5 Practical Issues

Since our proposed leakage model and hence our attack is a second-order attack, we compare the sensitivity to noise of our proposed attack to that of a corresponding first-order attack.

[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 [8].

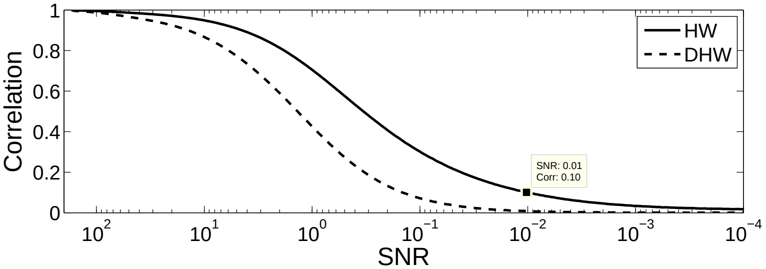


Fig. 4. Comparison of DHW model (of a single-bit masked ciruit) and HW model (of the corresponding unmasked circuit), correlation of the predictions and measurements over SNR

We consider a set of $1,000,000$ random bytes assuming a HW leakage with additive white Gaussian noise featuring zero mean and a specified standard deviation. To model the effect of noise to the attack, we determine the correlation between HWs and noisy HWs (i.e., HW+noise as the simulated noisy measurement) for different noise standard deviations (and hence different SNRs). As usual for a hamming weight model, each bit has an equal contribution to the power consumption.

It should be noted that in order to make simulation and calculations closer to real measurements, noisy HW values are rounded to decimal values restricted to a byte since most of the measurement tools (i.e., digital oscilloscopes) use 8-bit analogue to digital converters and hence real measured power values are stepwise to 256 steps. In order to compare the noise effect on our proposed DHW-based attack, the same scenario is repeated for the masked circuit by masking the input bytes (by a random mask bit for each byte) before extracting the HW and adding noise. When analyzing the generated data, the new preprocessing step is performed according to the scheme presented by Algorithm 1. A comparison between these two experiments over their signal to noise ratio, SNR $=$ var(signal)/var(noise), is depicted in Fig. 4. As expected, correlation between the predictions and measurements is decreased for low SNRs. However, the correlation for the DHW model (single-bit masked circuit) decreases more rapidly than that of HW model (unprotected circuit). It means, our proposed attack is more sensitive to noise than a straightforward CPA.

To investigate the applicability of our proposed attack in the presence of noise, we performed another experiment where additionally to the previous case an 8-bit key XOR followed by an AES Sbox is taken into account (similar to the circuit in Fig. 1). First, a first-order CPA attack using HW model of an unmasked circuit is performed for all possible values of the secret key (256 cases). The success rate of this attack is obtained for different signal to noise ratios[3]. Then, the same scenario is repeated for the single-bit masked circuit. This means, our

[3] Success rate is computed as a ratio of the number of successful attacks over the number of all cases.

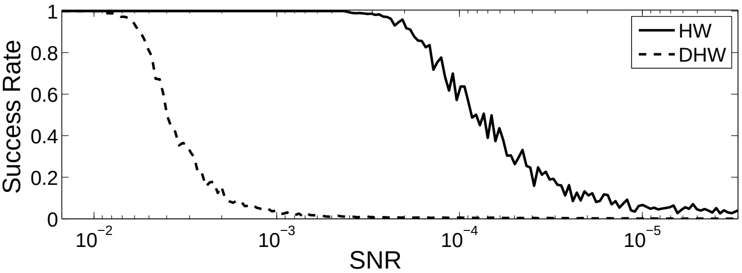


Fig. 5. Comparison of HW and DHW attacks, success rate over SNR

proposed attack using DHW model (Algorithm 1) is performed for all possible secret keys, and success rates are computed for different signal to noise ratios. Fig. 5 depicts a comparison of success rates over SNR, threshold of SNR for a 100% success rate in our proposed attack is higher than that of a straightforward CPA. In other words, our proposed attack on a single-bit masked circuit stops succeeding earlier than a first-order CPA on a corresponding unprotected circuit with an increasig SNR. Mapping the SNR threshold of DHW attack, i.e., 0.01, to the diagrams of Fig. 4 clarifies maximum correlation, i.e., 0.01, which can be achieved by a successful DHW attack at the threshold point. At the same SNR, maximum correlation for a successful first order CPA attack is around 0.1. It means, DHW attack works on a single-bit masked circuit if correlation between predictions and measurements of the same unprotected circuit (i.e., when mask bit generator is off and mask bit is always 0) is greater than 0.1.

Note that these observations are for $1,000,000$ measurements. The SNR threshold for a successful DHW attack and hence minimum required correlation value for the unprotected circuit are increased by deducting the number of measurements, e.g., we got 0.1 and 0.3 as SNR threshold and minimum required correlation respectively using $10,000$ measurements. Also, it should be noted that in our simulations we have supposed that the leakages are linearly related to predictions (HW), which does not hold precisely in practice. Moreover, in our proposed attack (and in our simulation as well) we have taken all of single-bit masked registers into account. In other words, all the masked registers in the architecture which are triggered at the same time must be considered in the attack. Otherwise, the DHW/DHD model does not fit to the folded measurements.

6 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.

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 masked flip-flops. Using DHW and DHD as power model for a classical CPA attack on pre-processed power traces 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 most of the 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. 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.
2. 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.
3. B. Gierlichs. DPA-Resistance Without Routing Constraints? In *CHES 2007*, volume 4727 of *LNCS*, pages 107–120. Springer, 2007.
4. 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.
5. P. C. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *CRYPTO 1999*, volume 1666 of *LNCS*, pages 388–397. Springer, 1999.
6. S. Mangard, E. Oswald, and T. Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, 2007.
7. 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.
8. 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.
9. 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.
10. T. Popp, M. Kirschbaum, and S. Mangard. Practical Attacks on Masked Hardware. In *CT-RSA 2009*, LNCS. Springer, 2009. to appear.
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. DPA Leakage Models for CMOS Logic Circuits. In *CHES 2005*, volume 3659 of *LNCS*, pages 366–382. Springer, 2005.
16. D. Suzuki, M. Saeki, and T. Ichikawa. Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, E90-A(1):160–168, 2007. Also available at `http://eprint.iacr.org/2004/346`.
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.
21. J. Waddle and D. Wagner. Towards Efficient Second-Order Power Analysis. In *CHES 2004*, volume 3156 of *LNCS*, pages 1–15. Springer, 2004.

Appendix I - Schematics of Flip-Flops

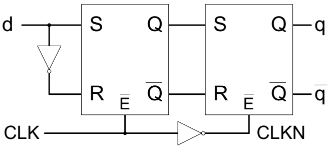


Fig. 6. Typical block diagram of an edge-sensitive flip-flop

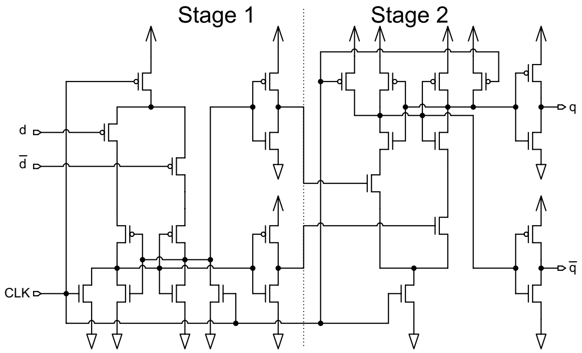
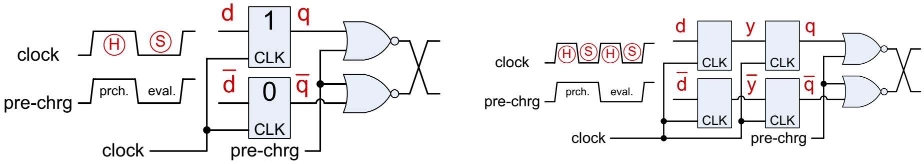


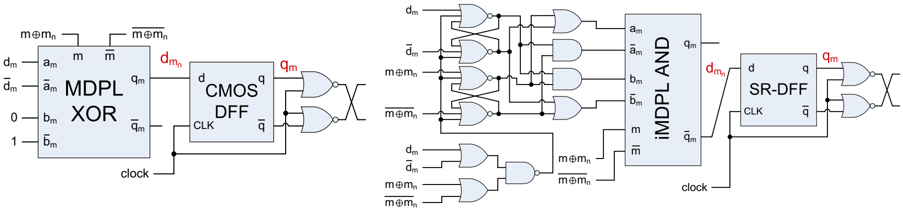
Fig. 7. SABL-DFF



(a) SDDL FF

(b) M-S DDL FF

Fig. 8. WDDL flip-flops



(a)

(b)

Fig. 9. (a) MDPL-DFF and (b) iMDPL-DFF