Security Evaluation of DPA Countermeasures Using Dual-Rail Pre-charge Logic Style

Daisuke Suzuki and Minoru Saeki

Mitsubishi Electric Corporation, Information Technology R&D Center,
5-1-1 Ofuna Kamakura, Kanagawa, 247-8501, Japan
{Suzuki.Daisuke@bx, Saeki.Minoru@db}.MitsubishiElectric.co.jp

Abstract. In recent years, some countermeasures against Differential Power Analysis (DPA) at the logic level have been proposed. At CHES 2005 conference, Popp and Mangard proposed a new countermeasure named Masked Dual-Rail Pre-Charge Logic (MDPL) which combine dual-rail circuits with random masking to improve Wave Dynamic Differential Logic (WDDL). The proposers of MDPL claim that it can implement secure circuits using a standard CMOS cell library without special constraints for the place-and-route because the difference of loading capacitance between all pairs of complementary logic gates in MDPL can be covered up by the random masking. In this paper, we especially focus the signal transition of the MDPL gate and evaluate the DPA-resistance of MDPL in detail. Our evaluation results show that the leakage occurs in the MDPL gates as well as WDDL gates when input signals have difference of delay time even if MDPL has an effectiveness on reducing the leakage caused by the difference of loading capacitance. Furthermore, we demonstrate the problem with different input signal delays by measurements of an FPGA and show the validity of our evaluation.

1 Introduction

In recent years, some countermeasures against Differential Power Analysis (DPA) [1] at the logic level have been proposed. Since the logic level countermeasure is applied to the basic components of hardware and aims to cut off DPA leakage at its source, it indicates that we can take the versatile countermeasure independent of the algorithm.

Some problems of security and implementation are pointed out to the countermeasures at the logic level that have been already proposed. For example, Mangard pointed out that the countermeasure to implement random masking by combinational circuit [2] should leak out the secret information from the power consumption caused due to glitches [3] and actually, they found DPA leakage on the real ASIC [4]. Random Switching Logic (RSL) [5] proposed by Suzuki et al. can suppress the occurrence of glitch and make uniform the power consumption at each gate in the statistical analysis using the random number. However, RSL requires the special CMOS gates to perform effective implementing process and the special constraints of timing to assure the security. Wave

Dynamic Differential Logic (WDDL) [6], which applies the dual-rail synchronous circuit, must adopt the specialized place-and-route method to adjust the loading capacitance for implementing of the secure circuit [7]. In addition, Suzuki et al. present the fact that DPA leakage occurs when there are differences in the delay time between the input signals at the WDDL gates [5, 8].

As one of the recent research, Masked Dual-Rail Pre-Charge Logic (MDPL) [9] that improved WDDL was proposed at CHES 2005 conference. The proposers of MDPL claim that it can implement secure circuits using a standard CMOS cell library without special constraints for the place-and-route because the difference of loading capacitance between all pairs of complementary logic gates in MDPL can be covered up by the random masking.

In this paper, we especially focus the signal transition of the MDPL gate and evaluate the DPA-resistance of MDPL in detail. Our evaluation results show that the leakage occurs in the MDPL gates as well as WDDL gates when input signals have difference of delay time even if MDPL has an effectiveness on reducing the leakage caused by the difference of loading capacitance. Furthermore, we demonstrate the problem with different input signal delays by measurements of an FPGA and show the validity of our evaluation.

2 DPA Countermeasures Using Dual-Rail Circuits

2.1 Wave Dynamic Differential Logic [6]

Tiri et al. proposed WDDL applying DCVSL (Differential Cascode Voltage Switch Logic) as a countermeasure against DPA [6]. Figure 1 shows the basic components of WDDL. The WDDL circuits have the following features:

(1) WDDL gates have complementary outputs $(q, \bar{q})$.
(2) The pre-charge signal controls the pre-charge phase to transmit (0, 0) and the evaluation phase to transmit (0, 1) or (1, 0).
(3) The pre-charge operation is performed at the first step in combinational circuit and, the components to be used are limited to AND, OR, and NOT (re-wiring) operations.
(4) The number of transitions in all circuits generated during an operation cycle is constant without depending on the values of input signals.

The power consumption in the CMOS circuits is generally proportional to the number of transitions at the gates. Therefore, the WDDL circuits are effective as a countermeasure against DPA since the power consumption may become constant without depending on the values of input signals as described in the feature above.

2.2 Masked Dual-Rail Pre-charge Logic [9]

Popp et al. proposed Masked Dual-Rail Pre-charge Logic (MDPL) that the random data masking is introduced into WDDL gates [9]. Figure 2 and Figure 3

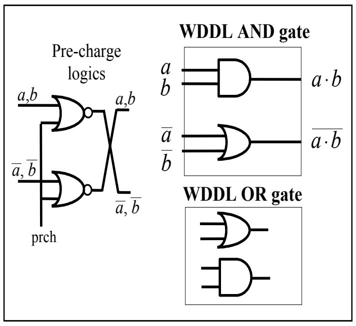

Fig. 1. Components of WDDL

show the basic components of MDPL. In addition, Table 1 shows the truth table of an MDPL AND gate. The logic AND function and OR function in the WDDL gate apply a pair of standard two-input AND gate and OR gate and on the other hand, those in the MDPL gate apply a pair of majority logic (MAJ) gates.

The architecture of cryptographic circuits using MDPL is shown in Figure 4. The signals $(a_m, b_m, \bar{a_m}, \bar{b_m})$ masked with the random data m and $\bar{m}$ and those random data are entered into the MAJ gates in the combinational circuit shown in Figure 4. Hereupon, at the MAJ gates with the three input ports (x, y, r) shown in Figure 3, the signals $(a_m, \bar{a}_m)$ and $(b_m, \bar{b}_m)$ are entered into the input ports x and y, respectively and then, the signals $(m, \bar{m})$ are entered into the input port r.

When examining the security against DPA, we assume that an attacker can predict the architecture of the combinational circuit shown in Figure 4 and the pre-masking signals $(a, b, \bar{a}, \bar{b})$ corresponding to the signals $(a_m, b_m, \bar{a_m}, \bar{b_m})$. And the random numbers m and $\bar{m}$ generated in the VLSI can be predicted only with a probability of $1/2$.

The relations between the signals are described below. In the beginning, there are following relations between the input signals.

$$a_m = a \oplus m, b_m = b \oplus m, \bar{a}_m = a \oplus \bar{m}, \bar{b}_m = b \oplus \bar{m}.$$

The output signals q_m and $\bar{q}_m$ of the MDPL AND gate are as follows:

$$\begin{aligned} q_m &= MAJ(a_m, b_m, m) = a \cdot b \oplus m, \\ \bar{q}_m &= MAJ(\bar{a}_m, \bar{b}_m, \bar{m}) = a \cdot b \oplus \bar{m}. \end{aligned}$$

As realized from Figure 3 and the above formulas of q_m and $\bar{q}_m$, the MDPL gates have the following feature, including those of WDDL gates described in Section 2.1.

- Even if the correct signal values a, b $(\bar{a}, \bar{b})$ are predictable, the random transition occurs at the MAJ gate according to the value of random data m $(\bar{m})$.

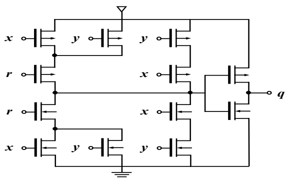

Fig. 2. MAJ gate

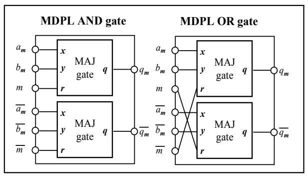

Fig. 3. Components of MDPL

Table 1. Truth table of an MDPL AND gate

a	b	a_m	b_m	m	q_m	$\bar{a}_m$	$\bar{b}_m$	$\bar{m}$	$\bar{q}_m$
0	0	0	0	0	0	1	1	1	1
0	0	1	1	1	1	0	0	0	0
0	1	0	1	0	0	1	0	1	1
0	1	1	0	1	1	0	1	0	0
1	0	1	0	0	0	0	1	1	1
1	0	0	1	1	1	1	0	0	0
1	1	1	1	0	1	0	0	1	0
1	1	0	0	1	0	1	1	0	1

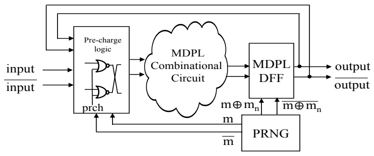

Fig. 4. Architecture of MDPL circuit

For this reason, the power consumption is made uniform even if there is a difference of the loading capacitance between each complementary logic gate. Thus, the proposers of MDPL claim that MDPL does not need the constraints on the place-and-route to adjust the loading capacitance and can improve security and implementability.

3 Security Problems of WDDL

This section states the main factor of leakage in WDDL gate based on the contents that have been already discussed on the security of WDDL.

3.1 Main Factors of the Leakage in WDDL

As the main factors of the DPA leakage in WDDL, the following two contents have been pointed out [7, 8]:

F1: Leakage caused by the difference of loading capacitance between two complementary logic gates in WDDL gate

F2: Leakage caused by the difference of delay time between the input signals of WDDL gates

We here describe the factor of the above-mentioned leakage in detail. At first, we explain the main factor of leakage in F1. The power consumption at the CMOS gate can be generally evaluated in the following formula [10]:

$$P_{\mathrm{total}} = p_{\mathrm{t}} \cdot C_{\mathrm{L}} \cdot V_{\mathrm{dd}}^2 \cdot f_{\mathrm{clk}} + p_{\mathrm{t}} \cdot I_{\mathrm{sc}} \cdot V_{\mathrm{dd}} \cdot f_{\mathrm{clk}} + I_{\mathrm{leakage}} \cdot V_{\mathrm{dd}}, \tag{1}$$

where C_{L} is the loading capacitance, f_{clk} is the clock frequency, V_{dd} is the supply voltage, p_{t} is the transition probability of the signal, I_{sc} is the direct-path short circuit current, and I_{leakage} is the leakage current. As realized from the formula (1), the power consumption at the first term is different between the gates if there is a difference of the loading capacitance between each complementary logic gate. Since the existence of transition at each complementary logic gate is determined by the values of input signals, the total power consumption differ in dependence of the signal values even if the total number of transitions is equal between the gates. For this reason, the difference of power consumption occurs in dependence of the DPA selection function.

Next, we explain the main factor of leakage in F2. As described in Section 2.1, the transition probability during an operation cycle at the WDDL gates is assured $p_t = 1$ without depending on the input signals. However, the operation timing of each complementary logic gate are generally different due to the conditions of values or delay time of input signals during an operation cycle. In other words, this means that the timing of starting the power consumption varies in dependence of the signal values during an operation cycle. Therefore, since the average power traces specified by the predictable signal values have different phases, the spike can be detected after the DPA operation.

3.2 Countermeasures against Main Factors of Leakage in WDDL

We here consider the above-mentioned two factors of the leakage from the viewpoint of implementing the logic circuit. First, we examine the leakage caused by the difference of loading capacitance in F1. The difference of loading capacitance generally arises between the gates in dependence of the number and type of gates connected to each other and the result of place-and-route. Complementary logic gates of WDDL are different in the point of logical expression (positive/negative), but their attribute (such as order and the number of connected gate) are designed to be equal. Thus, the number of gates connected to complementary logic gates of WDDL is equal basically. Therefore, the difference of loading capacitance in the WDDL circuit arises due to the difference of capacitance at the AND/OR gates themselves and the difference of place-and-route. Furthermore, when we consider the whole cryptographic circuit, a signal propagating path with transition is determined in probability depending on the values of input related signals. In a word, the leakage in F1 is a difference of power consumption that depends on the difference between the propagation probability and the loading capacitance of the signal in each path. We predict that the difference of the capacitance that depends on the place-and-route is more predominant as the factor of the leakage in F1 than the difference of capacitance at

Table 2. Factors of the leakage caused by the difference of delay time

factor	classification	difference to cause the leakage
diff(a,$\bar{a}$)	incidental	place-and-route
diff(b,$\bar{b}$)	incidental	place-and-route
diff(a,b)	inevitable (+ incidental)	logic steps (+ place-and-route)
diff($\bar{a}$,$\bar{b}$)	inevitable (+ incidental)	logic steps (+ place-and-route)

each gate such as AND/OR gate. Hereafter, we refer the leakage that depends on the place-and-route and does not depend on the logical formula as *incidental leakage*.

Next, we examine the leakage caused by the difference of delay time in F2. Suzuki et al. analyzed the existence of leakage on assumption that there is different delay time between a and b (or between $\bar{a}$ and $\bar{b}$) among four input signals of WDDL AND gate of Figure 1 [8]. We explain the propriety of this assumption below. Since the basic cryptographic components including the S-box as a representative generally have their randomness, the logical formula consists of various terms. Unless the special design is made as described in Ref. [12], the input signals at the gates have the different number of logic steps and are easy to cause differences in the delay time. On the contrary, since the number of gates connected to each complementary output of WDDL is equal as described above, the difference of place-and-route is predominant over a difference in the delay time between a and $\bar{a}$ (or b and $\bar{b}$). In fact, it is appropriate to realize that a difference in the delay time between a and b (or $\bar{a}$ and $\bar{b}$) occurs necessarily on the normal design of logic circuit. From the consideration above, it can be said that the leakage caused by the difference of delay time includes the *inevitable leakage* that occurs depending on the difference of the logical formula together with the *incidental leakage* that occurs depending on the place-and-route. Table 2 summarizes the relation of the leakage factors that correspond to the difference of delay time between each input signal (diff(): indicates difference of delay time between each argument signal).

A main factor of *incidental leakage* is the automatization of the place-and-route that is generally carried out in the VLSI design at present. Therefore, *incidental leakage* can be likely to improve with the place-and-route in the manual operation or the semi-automatic operation using the special constraints. Actually, Tiri et al. and Guilley et al. proposed "Fat Wire" [7] and "Backend Duplication" [11], respectively as a countermeasure in the place-and-route to improve the DPA-resistance.

On the other hand, there is no study of a countermeasure against the *inevitable leakage* in the dual-rail circuit so far as the authors know. The S-box design method for low power consumption proposed by Morioka et al. is recommended as one technique to reduce *inevitable leakage* [12]. In the circuit design, it generally needs high effort to adjust the delay time between the input signals at each gate.

4 Security Evaluation of MDPL

As for the main factors of leakage described in Section 3.1, we here evaluate the effectiveness of MDPL. As stated in Section 2.2, MDPL can improve in principle the leakage caused by the difference of loading capacitance in F1 of Section 3.1. Therefore, we focus the leakage caused by the difference of delay time in F2 of Section 3.1.

When examining the difference of delay time, it is first necessary to inquire the conditions of delay time between the input signals. As described in Section 3.2, differences of delay time between independent signals (e.g. a_m and b_m) are more likely to occur than those between complementary signals (e.g. a_m and $\bar{a}_m$) in the design of dual-rail circuit. In the case of the MDPL gate, we supposed that there are differences in the delay time between the signals a_m, b_m and m (or $\bar{a}_m$, $\bar{b}_m$ and $\bar{m}$). From the above matters, when assuming the single input change model and if $delay(a_m) < delay(b_m)$ ($delay()$: indicates the delay of the signal in parentheses) is satisfied, the following three delay condition (C1 - C3) cover the whole timing relations of inputs signals in the MDPL gate.

C1: $delay(a_m) < delay(b_m) < delay(m)$
C2: $delay(a_m) < delay(m) < delay(b_m)$
C3: $delay(m) < delay(a_m) < delay(b_m)$

In the case of $delay(a_m) > delay(b_m)$, the equivalent conditions C1 - C3 can be obtained by changing the DPA selection function, so that it is not necessary to distinguish the delay conditions between the data signals (a_m and b_m).

Table 3 shows the delay conditions and the timing of transition on evaluation and pre-charge phase in the MDPL AND gate. In addition, Table 3 indicates the values (a, b, m) that bring Δq_m ($\Delta \bar{q}_m$) $= 1$ under each delay condition and the transition of the input signal which brings the output transition. For example, when the values (a, b, m) is set (0, 0, 1) on evaluation phase under the delay condition C1, the transition of the output signal q_m (that is, Δq_m) occurs at a time when the transition of the input signal b_m (that is, Δb_m) occurs.

Next, we evaluate the DPA-resistance of the MDPL AND gate from Table 3. Here, the DPA selection function is a or b. The differential waveform (T_{1-0}) that the average power waveform (T_0) with the selection function "0" is subtracted from the average power waveform (T_1) with the selection function "1" is regarded as the DPA trace. Table 4 shows the evaluation result of the DPA-resistance of the MDPL AND gate. And also, Table 4 indicates the existence of leakage according to delay conditions and the spike polarity on the DPA trace T_{1-0}. As an example, we explain DPA-resistance on the evaluation phase under the delay condition C2. First, it is found that the transition Δq_m ($\Delta \bar{q}_m$) occurs together with the transitions Δm ($\Delta \bar{m}$) and Δb_m ($\Delta \bar{b}_m$) on the evaluation phase under the delay condition C2 in Table 3. Here, when the DPA selection function is a, the output transition with $a = 1$ is sure to occur with the transition Δb_m ($\Delta \bar{b}_m$), but the output transition with $a = 0$ occurs with the transitions Δm ($\Delta \bar{m}$). Note that the transition Δm ($\Delta \bar{m}$) is performed prior to Δb_m ($\Delta \bar{b}_m$) according to the delay conditions. Therefore, it is predictable that the average power waveform

Table 3. Timing of transition in an MDPL AND gate

Delay condition: C1 $\Delta a_m \rightarrow \Delta b_m \rightarrow \Delta m$ $(\Delta \bar{a}_m \rightarrow \Delta \bar{b}_m \rightarrow \Delta \bar{m})$								
phase	evaluation phase				pre-charge phase			
$a\ b\ m$	Δq_m	timing	$\Delta \bar{q}_m$	timing	Δq_m	timing	$\Delta \bar{q}_m$	timing
0 0 0	0	-	1	Δb_m	0	-	1	Δb_m
0 0 1	1	Δb_m	0	-	1	Δb_m	0	-
0 1 0	0	-	1	$\Delta \bar{m}$	0	-	1	$\Delta \bar{a}_m$
0 1 1	1	Δm	0	-	1	Δa_m	0	-
1 0 0	0	-	1	$\Delta \bar{m}$	0	-	1	$\Delta \bar{b}_m$
1 0 1	1	Δm	0	-	1	Δb_m	0	-
1 1 0	1	Δb_m	0	-	1	Δa_m	0	-
1 1 1	0	-	1	$\Delta \bar{b}_m$	0	-	1	$\Delta \bar{a}_m$

Delay condition: C2 $\Delta a_m \rightarrow \Delta m \rightarrow \Delta b_m$ $(\Delta \bar{a}_m \rightarrow \Delta \bar{m} \rightarrow \Delta \bar{b}_m)$								
phase	evaluation phase				pre-charge phase			
$a\ b\ m$	Δq_m	timing	$\Delta \bar{q}_m$	timing	Δq_m	timing	$\Delta \bar{q}_m$	timing
0 0 0	0	-	1	$\Delta \bar{m}$	0	-	1	$\Delta \bar{m}$
0 0 1	1	Δm	0	-	1	Δm	0	-
0 1 0	0	-	1	$\Delta \bar{m}$	0	-	1	$\Delta \bar{a}_m$
0 1 1	1	Δm	0	-	1	Δa_m	0	-
1 0 0	0	-	1	$\Delta \bar{b}_m$	0	-	1	$\Delta \bar{m}$
1 0 1	1	Δb_m	0	-	1	Δm	0	-
1 1 0	1	Δb_m	0	-	1	Δa_m	0	-
1 1 1	0	-	1	$\Delta \bar{b}_m$	0	-	1	$\Delta \bar{a}_m$

Delay condition: C3 $\Delta m \rightarrow \Delta a_m \rightarrow \Delta b_m$ $(\Delta \bar{m} \rightarrow \Delta \bar{a}_m \rightarrow \Delta \bar{b}_m)$								
phase	evaluation phase				pre-charge phase			
$a\ b\ m$	Δq_m	timing	$\Delta \bar{q}_m$	timing	Δq_m	timing	$\Delta \bar{q}_m$	timing
0 0 0	0	-	1	$\Delta \bar{a}_m$	0	-	1	$\Delta \bar{a}_m$
0 0 1	1	Δa_m	0	-	1	Δa_m	0	-
0 1 0	0	-	1	$\Delta \bar{a}_m$	0	-	1	$\Delta \bar{m}$
0 1 1	1	Δa_m	0	-	1	Δm	0	-
1 0 0	0	-	1	$\Delta \bar{b}_m$	0	-	1	$\Delta \bar{m}$
1 0 1	1	Δb_m	0	-	1	Δm	0	-
1 1 0	1	Δb_m	0	-	1	Δa_m	0	-
1 1 1	0	-	1	$\Delta \bar{b}_m$	0	-	1	$\Delta \bar{a}_m$

T_0 will show the peak value of power consumption prior to T_1. We here consider that detectable power waveform in an actual measurement shows the power consumption that some capacitance influence, and does not show pure power consumption at each gate. More detailed consideration is presented in Appendix A. From the abovementioned contents, the valley-type spike appears on the differential waveform T_{1-0}.

As shown in Table 4, it should be noted that the leakage occurs under any delay conditions. In short, there is no secure delay condition in MDPL on the single input change model. Therefore, in order to implement the secure logic circuits using MDPL gates, it is required to adjust differences in the delay time between the input signals.

5 Experimental Results

In this section, we show experimental results of evaluating DPA-resistance of the basic components of WDDL and MDPL implemented on FPGA. The measurement of the power consumption is done by measuring the potential difference between both ends of a 10 ohm resistance which is inserted between the power source and a power supply pin of the FPGA. Table 5 shows the evaluation environment applied this time. This evaluation aims to inspect the effectiveness of MDPL for the leakage caused by the difference of loading capacitance (see F1

Table 4. DPA-resistance of an MDPL AND gate

Delay condition	Phase	Selection function	Leakage	Spike polarity
C1	evaluation	a	No	-
		b	No	-
	pre-charge	a	No	-
		b	Yes	$\uparrow$
C2	evaluation	a	Yes	$\downarrow$
		b	No	-
	pre-charge	a	No	-
		b	Yes	$\uparrow$
C3	evaluation	a	Yes	$\downarrow$
		b	No	-
	pre-charge	a	No	-
		b	No	-

in Section 3.1) and leakage caused by the difference of delay time described in Section 4.

5.1 Implementation of Model Circuits for Evaluation

Figure 5 shows the architecture of a model circuit used for evaluation. In the circuits shown in Figure 5, we implement 32 AND operations by using each countermeasure and supply the same input signals [1]. In order to evaluate only the power consumption of each countermeasure, the model circuit is designed so that other circuit parts should not operate while the countermeasure (MDPL/WDDL) part operates. In addition, a pair of positive logic and negative logic (combinational circuits for pre-charge, WDDL AND gates, MDPL AND gates and input/output FF (Flip-Flop) circuits) in the countermeasures is integrated into two LUTs (Look-Up Tables) and FFs in the Slice that are the basic components of Xilinx FPGA. And, the random number for masking is generated by M-Sequence of degree 89, which is created by the shift register installed in the FPGA. By using above mentioned simple circuits, we experimented following two evaluations (E1 and E2):

E1: We use a variety of constraints in the place-and-route to the circuits of WDDL and MDPL respectively and compare each DPA-resistance.

E2: To satisfy each delay conditions (C1 - C3), we insert the proper delay element constructed of 4 LUTs connection in series after the pre-charge logic of MDPL and compare the obtained DPA traces with evaluation results shown as Table 4 in Section 4.

The evaluation E1 is to compare WDDL with MDPL in relation to the main factor of leakage described in F1 of Section 3.1. The evaluation E2 is to inspect

[1] This is to ease the measuring. In the case that only one AND operation is implemented, the amount of the leakage becomes 1/32 and the number of samples to obtain the same Signal-Noise ratio should become the square of 32 times.

Table 5. Evaluation environment

Design environment	
Language	Verilog-HDL
Simulator	NC-Verilog LDV5.1 QSR2
Logic synthesis	Synplify Pro 8.1
Place and Route	ISE 6.3.03i, IP update4
Measurement environment	
Target FPGA	XCV1000-6-BG560C
Oscilloscope	Tektronix TDS 7104

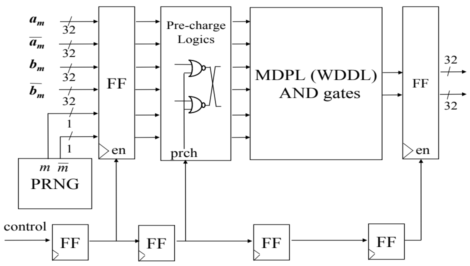

Fig. 5. Architecture of model circuit for evaluation

the leakage caused by the difference of delay time in MDPL circuits shown in Table 4.

5.2 DPA Traces of Model Circuits

First, we explain the result for the evaluation E1. Figure 6 shows the DPA trace of the WDDL AND gates. The difference of constraints is location of LUTs and Slices used for the complementary logic for the WDDL and MDPL AND gates [2]. As realized from Figure 6, the polarity and height of spike change in dependence of the constraints. Figure 8 shows the DPA traces when the same constraints in the place-and-route are used for the MDPL AND gates. It is found that the spikes are difficult to recognize in Figure 8 by comparison with Figure 6. In other words, this indicates that MDPL has effectiveness on reducing leakage caused in dependence of the place-and-route.

Here, we consider each trace under the Constraint 1 in Figure 6 and Figure 8, respectively. Figure 7 and Figure 9 show magnified views of DPA traces under the Constraint 1. From Figure 6, Constraint 1 makes the complementary gates balance more than other constraints. Nevertheless, we can confirm slight leakages from the magnified views. Since these spikes have only narrow width, we guess that these leakages occur due to slight differences of delay time.

[2] Each location is concretely specified by LOC and BEL command [13, 14].

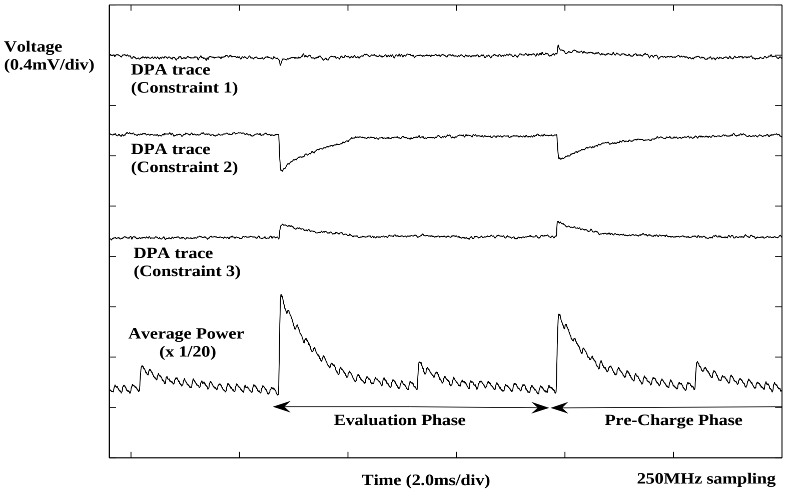

Fig. 6. DPA traces of WDDL AND gates (Evaluation E1, 200,000 samples)

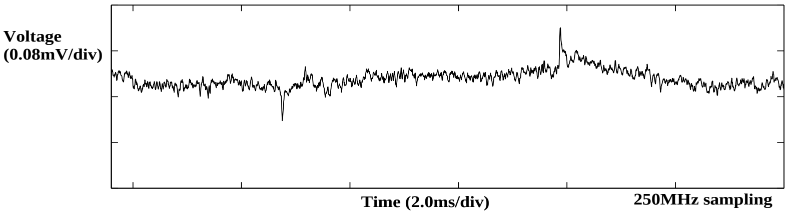

Fig. 7. Magnified view of the DPA trace with Consraint 1 in Fig.6

From the abovementioned matters, in order to make cryptographic circuits secure by using MDPL, we have to adopt the implementation method with attention on the number of logic steps of every signal and differences in the delay time between the signals, or the implementation method to adjust differences in the delay time between the input signals by use of the delay elements. Moreover, if the slight leakages caused in Figure 8 become a problem, we also have to pay attention to constraints of the place-and-route.

Next, we explain the result of evaluation E2. Figure 10 shows the DPA trace of the MDPL AND gates corresponding to Table 4. From the content shown in Figure 10, it is found that the existence and polarity of spikes to be caused in the delay conditions are in good agreement with the content of Table 4. From this fact, we can confirm the leakage caused by the difference of delay time on the FPGA.

Here, we compare the height of spikes in Figure 8 and Figure 10. Since the delay elements are not entered intentionally into the input signals on the

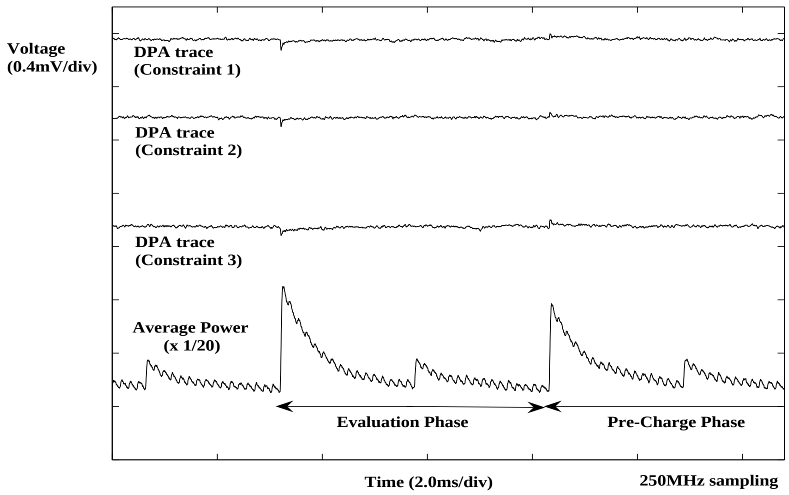

Fig. 8. DPA traces of the MDPL AND gates (Evaluation E1, 200,000 samples)

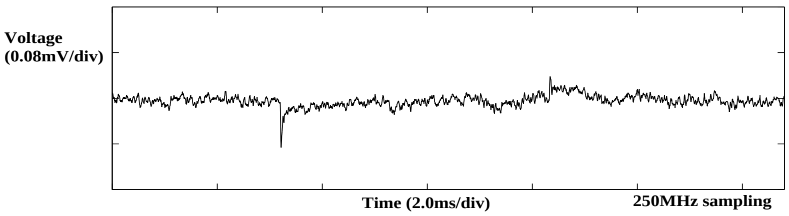

Fig. 9. Magnified view of the DPA trace with Consraint 1 in Fig.8

implementation for the evaluation E1, differences in the delay time between the input signals mainly depends on the place-and-route. Therefore, there are slight differences in the delay time between the input signals by comparison with the implementation for the evaluation E2. In short, because there is only a slight phase difference between the average power traces T_0 and T_1, the height of spikes (leakage) is also slight in Figure 8. On the contrary, as shown in Figure 10, it is found that the easily visible leakage occurs on the implementation for the evaluation E2 because there are large differences in the delay time between the input signals.

6 Conclusion

In this paper, we classified the main factors of leakage in DPA countermeasures using dual-rail circuit and especially evaluated the security of MDPL. As a result, it was found that MDPL has effectiveness on reducing the leakage caused by the

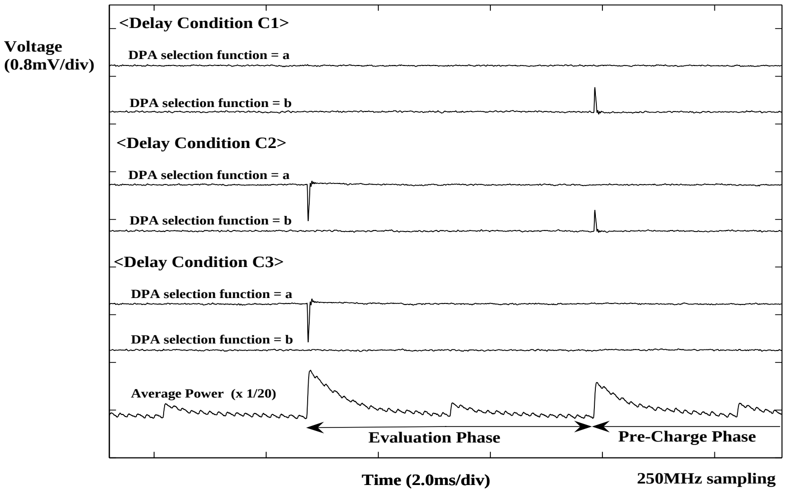

Fig. 10. DPA traces of the MDPL AND gates (Evaluation E2, 200,000 samples)

difference of loading capacitance, but it makes the leakage occur as well as the WDDL when there are differences in the delay time between the input signals. In addition, experimental results using the FPGA showed that the more differences in the delay time between the input signals increases, the more leakage volume increases. Therefore, we expect that the DPA trace from the simulation has two spikes with different polarity, respectively. On the other hand, we run the DPA by measuring the voltage at both ends of the resistance connected outside of FPGA in our experiment.

The complicated logic circuits such as the cryptographic circuit generally cause differences in the delay time between the input signals. For this reason, the designer has to adjust the delay of signals with attention when designing the combinational circuit in order to structure the secure circuit using WDDL or MDPL. On the contrary, it needs some high-advanced complicated design at the logic level to adjust such differences in the delay time between the input signals. Moreover, if we assume an attacker who has high ability and can detect small spikes in Figure 8 which is caused by the differences in the delay time between the input signal, it is very difficult to keep security of the cryptographic circuit from the attacker.

When evaluating the DPA-resistance of the whole device including the cryptographic circuit, the visibility of leakage mostly depends on the characteristics of VLSI such as noise level, the evaluation environment, and the undetermined elements such as the ability of attackers. One of the future subjects is the research about how large differences in the delay time between the input signals are to be allowed (or to be a problem) on the whole device.

References

1. P. Kocher, J. Jaffe and B. Jun, "Differential Power Analysis," *Crypto'99*, LNCS 1666, pp. 388-397, Springer-Verlag, 1999.
2. E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data," Cryptology ePrint Archive, 2003/236, 2003.
3. S. Mangard, T. Popp, and B. M. Gammel, "Side-Channel Leakage of Masked CMOS Gates," *CT-RSA 2005*, LNCS 3376, pp. 361-365, Springer-Verlag, 2005
4. S. Mangard, N. Pramstaller and E. Oswald, "Successfully Attacking Mased AES Hardware Implementation," *CHES 2005*, LNCS 3659, pp. 157-171, Springer-Verlag, 2005.
5. 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.
6. K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," In Proc. of Design Automation and Test in Europe Conference, pp. 246-251, 2004.
7. K. Tiri and I. Verbauwhede, "Place and Route for Secure Stabdard Cell Design," *CARDIS'04*, pp.143-158, 2004.
8. D. Suzuki, M. Saeki, and T. Ichikawa, "DPA Lekage Models for CMOS Logic Circuits," *CHES 2005*, LNCS 3659, pp. 366-382, Springer-Verlag, 2005.
9. T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge Logic : DPA-Resistance Without Routing Constraints," *CHES 2005*, LNCS 3659, pp. 172-186, Springer-Verlag, 2005.
10. A. P. Chandrakasan, S. Sheng, and R. W. Brodersen, "Low Power Digital CMOS Design," IEEE Journal of Solid State Circuits, Vol.27, N0.4. pp. 473-484,1992.
11. S. Guilley, P. Hoogvorst, Y. Mathieu, and R. Pacalet, "The "Backend Duplication" Method," *CHES 2005*, LNCS 3659, pp. 383-397, Springer-Verlag, 2005.
12. S. Morioka and A. Satoh, "An Optimized S-box Circuit Architecture for Low Power AES Design," *CHES 2002*, LNCS 2523, pp. 172-186, Springer-Verlag, 2002.
13. Xilinx, Inc., Data sheet "Virtex^{TM} 2.5 V Field Programmable Gate Arrays," http://direct.xilinx.com/bvdocs/publications/ds003.pdf
14. Xilinx, Inc., Software Manuals "Constraints Guide," http://www.xilinx.com/support/sw_manuals/xilinx6/download/cgd.zip

A Detectable Leakage in an Actual Measurement

In this paper, we discussed the leakage due to the difference of delay time between the input signals of the complementary gates. We consider the difference between the leakage that occurs essentially and the leakage that can be observed in our experiment.

Figure 11 shows our qualitative hypothesis of the mechanism that the leakage occurs due to the difference of delay time. Current at each complementary gate that we can observe from the simulation (such as SPICE etc.) will show the sharp trace that the current change completes in the short time as shown in the left of Figure 11.

On the other hand, we run the DPA by measuring the voltage at both ends of the resistance connected outside of FPGA in our experiment. In this case,

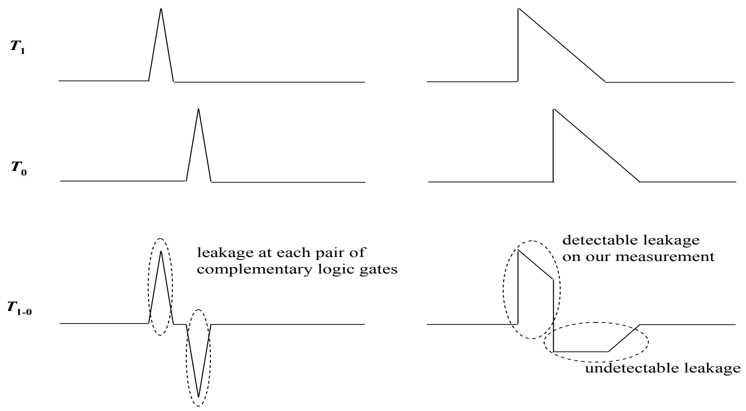

Fig. 11. Hypothesis concerning detectable leakage : from a simulation (left); and from our experiment (right)

each trace shown in this paper has the feature shown in the right of Figure 11. First, the current incereases rapidly in the vicinity of the clock edge. Afterwards, the current decreases slowly until the next clock edges. Therefore, we can expect that only the first spike sharpens, and the next spike smoothes. As a result, we can recognize only the first spike from the DPA trace. One of the causes of different results from simulation and actual measurement is various capacitance of FPGA and measuring instruments.