IEICE Electronics Express, Vol.9, No.6, 458–463

A proper security analysis method for CMOS cryptographic circuits

Yoshio Takahashi[1,2a)] **and Tsutomu Matsumoto**[2b)]

[1] *NTT DATA Corporation, Research and Development Headquarters, Toyosu Center Bldg. Annex, 3–3–9 Toyosu, Koto-ku, Tokyo 135–8671, Japan*

[2] *Graduate School of Environment and Information Sciences, Yokohama National University, 79–7 Tokiwadai, Hodogaya-ku, Yokohama 240–8501, Japan*

a) *takahashiysd@nttdata.co.jp*

b) *tsutomu@ynu.ac.jp*

Abstract: Differential Power Analysis (DPA) aims at revealing secret keys in cryptographic devices by analyzing their power consumption as side-channel information. Although power consumption models based on transition probability were used to evaluate a DPA-resistance in previous studies, the adequacy of this model has not been confirmed enough. In this paper, we show two experiments about information of power consumption precisely, and show that Random Switching Logic which is one of the DPA-countermeasures is in reality not secure against DPA.

Keywords: cryptography, side channel attack, Differential Power Analysis, CMOS circuit, power analysis model, security evaluation

Classification: Integrated circuits

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *CRYPTO '99, LNCS 1666*, pp. 388–397, Springer, Aug. 1999.

[2] T. Ishihara and H. Yasuura, "On Accuracy of Switch Level Power Estimation for CMOS LSI Circuits," *IPSJ*, vol. 95, no. 54, pp. 23–30, 1995.

[3] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks - Revealing the Secrets of Smart Cards*, Springer, 2007, ISBN-13:978-0387308579.

[4] 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. Fundamentals*, vol. E90-A, no. 1, pp. 160–168, 2007.

[5] K. J. Kulikowski, M. G. Karpovsky, and A. Taubin, "Power Attacks on Secure Hardware Based on Early Propagation of Data," *12th IEEE International On-Line Testing Symposium*, pp. 131–138, July 2006.

[6] D. Suzuki, M. Saeki, and T. Ichikawa, "Countermeasure against DPA Considering Transition Probabilities," *IEICE Technical Report*, vol. 104, no. 200, ISEC2004-59, pp. 127–134, 2004.

[7] TOSHIBA, "CMOS Digital Integrated Circuit TC4001BP, TC4001BF, TC4001BFN, TC4001BFT," data sheet, Oct. 2007.

[8] Linear Technology, Design Simulation and Device Models' page, last visit Jan. 2012. [Online] http://www.linear.com/designtools/software/

DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012

1 Introduction

In recent years, countermeasures against Differential Power Analysis (DPA), an advanced form of side-channel attack introduced in [1], have been recognized as indispensable for cryptographic devices. Further, constructing power analysis models has been an effective method for analyzing the security of the DPA countermeasures for CMOS cryptographic circuits.

Before the introduction of DPA, power consumption was considered a basic parameter in the design of power supplies, heat radiators, etc. The predominant factor affecting power consumption is the charge-discharge current for load capacitance [2]. This current can be easily estimated from the product of the load capacitance and the transition probability at each gate. This calculation model, called Convenient Model, reduces the estimation time. The use of an analog circuit simulator allows for accurate power analysis but results in large time consumption for large-scale integrated circuits. After the introduction of DPA, the correlation between CMOS power consumption and the transition probability has been used to reveal the secret keys of cryptographic circuits. Thus, Convenient Model has been used to evaluate DPA resistance [3].

The data for DPA are recorded as waveforms ("power traces") by an oscilloscope and used to monitor the time-series behavior of a power-supply line, but the information extracted from power traces is not the total power consumption alone. Hence, we focus on the relationship between the delay time of a logic gate and the number of charging and discharging paths. If differences in the delay time can be extracted from power traces, the DPA attack might be successful. Although some DPA countermeasures e.g., Random Switching Logic (RSL) [4], have security proofs in Convenient Model, reconsideration of the security analysis using power traces shall be necessary. Our analysis points out a new fact: the RSL is not secure against DPA.

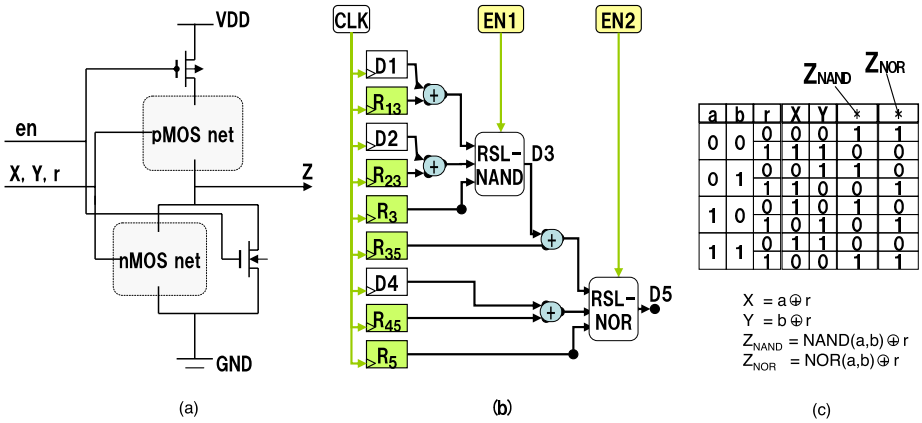
2 Previous work

2.1 Differential power analysis

DPA is to reveal the cryptographic secret keys through statistical analysis with many pairs of plaintexts (or cipher texts) and the corresponding power traces. The attacker creates a binary-output function SF using a candidate partial key and plaintexts to predict the input signal of a logic gate in the device. Using this function, called the selection function, the attacker divides the power traces into two groups: W_0 for SF $= 0$ and W_1 for SF $= 1$. Then the attacker calculates the mean $\overline{W_i} = \mathrm{mean}(W_i)$ and the difference between the means $dW = \overline{W_1} - \overline{W_0}$ (DPA trace). The peak of the DPA trace indicates the accuracy of the SF-based prediction, so that the attacker knows if the candidate key is appropriate. Refer to [1] for details.

Since one of the reasons for DPA is the dependence of the transition probability on the input signal values, the adopted countermeasures should break this dependency. Then, the peak of the DPA trace with the right candidate would become zero, and the attack fails.

DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012



a	b	r	X	Y	*	*
0	0	0	0	0	1	1
		1	1	1	0	0
0	1	0	0	1	1	0
		1	1	0	0	1
1	0	0	1	0	1	0
		1	0	1	0	1
1	1	0	1	1	0	0
		1	0	0	1	1

Fig. 1. (a) General form of RSL gate, (b) Applied RSL, (c) Truth table for RSL-NAND and RSL-NOR.

2.2 Random Switching Logic (RSL)

RSL is a DPA countermeasure based on data masking with random numbers: logic gates are replaced by the RSL gates which are specially manufactured CMOS circuits of general form shown in Fig. 1 (a). The input signals X, Y and the output signal Z are masked by a random number r. Let a, b and $c = \mathrm{F}(a, b)$ be the corresponding premasked value, namely, $X = a \oplus r$, $Y = b \oplus r$, and $Z = c \oplus r = F(a, b) \oplus r$. The signal en suppresses the occurrence of glitches and hazards to prevent the early propagation effect [5]. While en is 1 (disable), Z is fixed at 0. After the input signals are fixed, en becomes 0 (enable), and the RSL-gate output becomes valid. Thus, the RSL gate consumes power when en changes and Z transition occurs. Fig. 1 (b) shows an example RSL circuit with 'RSL-NAND' and 'RSL-NOR'. Each RSL gate is operated independently with a different masking random number (R_3 and R_5). For details, refer to [4].

The first report on RSL [6] was published in 2004. Then, signal en was mentioned in the lastest paper [4] published in 2007. To the best of our knowledge, no other update in RSL has been reported up to the present.

2.3 Security analysis of RSL against DPA

The security proof of RSL against DPA has been shown using the *Leakage Model* [4], which is a DPA trace formulation in Convenient Model. The *Leakage Model* consists of a complicated expression with many parameters related to signal delay. However, the DPA trace for RSL with maskinig by signal en is simplified as follows. Let P_1 and P_0 be the powers for the transition and no-transition cases, respectively. Then, the power consumption at the RSL gate is expressed as $P_Z = P_{\mathrm{F}(a,b)\oplus r}$ because Z determines the power of the RSL gate. Let $\overline{W_i}$ be the mean of the powers corresponding to the case $a = i,\ i \in \{0, 1\}$:

$$\overline{W_i} = \frac{\sum_{b\in\{0,1\},r\in\{0,1\}} P_{\mathrm{F}(i,b)\oplus r}}{4} = \frac{P_1 + P_0}{2}.$$

Hence, $\overline{W_1} = \overline{W_0}$. The DPA trace $dW = \overline{W_1} - \overline{W_0} = 0$, indicating that RSL is robust to DPA in Convenient Model.

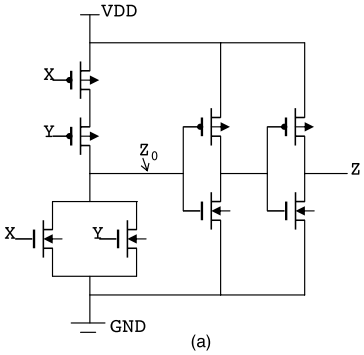
DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012

3 Experimental results

3.1 Oscilloscope observation: CMOS NOR

The target device was a real CMOS integrated circuit, TC4001BP (Quad 2-Input Positive NOR gate with buffers, [7]) (Fig. 2 (a)). VDD was connected to a 3.3-V voltage source. GND was connected to a ground voltage. The logic values '1' and '0' are represented by the voltages at VDD and GND, respectively. Input signals X, Y were driven at each event, as shown in Fig. 2 (b). Power traces were measured by a digital oscilloscope at the resistor (15 Ω) inserted in the GND line. To eliminate the effect of driving the input signals, power traces are expressed as the difference between the traces for e1 and es1 (Figs. 2 (d) and 2 (e)).

The dispersion of the delay times for Z:1 → 0 is relatively large (Fig. 2 (c)). Because there are two paths for discharging the load capacitance of Z_0 (Fig. 2 (a)), the delay times for Z:1 → 0 depend on the input combination. However, since there is only one charging path, the delay time dispersion for Z:0 → 1 is small. Then, the time of Z transition can be detected from these power traces (Figs. 2 (d) and 2 (e)). For example, the power traces of e1 and e2 show a peak at about 100 ns and 75 ns, respectively, which correspond to the delay times of Z (Fig. 2 (c)).

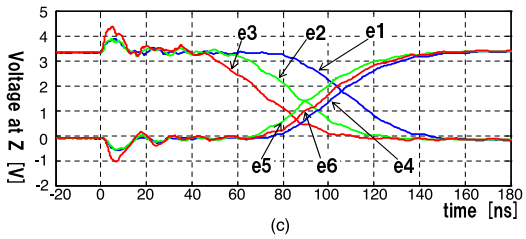


(a)

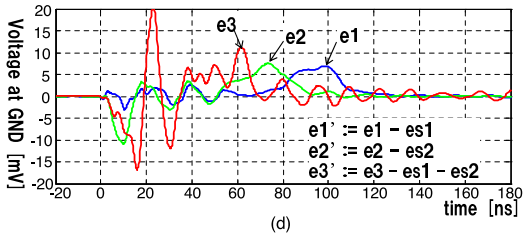
Event	Input signal	Output
e1	X: 0 hold, Y: 0 → 1	Z: 1 → 0
e2	X: 0 → 1, Y: 0 hold	Z: 1 → 0
e3	X: 0 → 1, Y: 0 → 1	Z: 1 → 0
e4	X: 0 hold, Y: 1 → 0	Z: 0 → 1
e5	X: 1 → 0, Y: 0 hold	Z: 0 → 1
e6	X: 1 → 0, Y: 1 → 0	Z: 0 → 1
es1	X: 1 hold, Y: 0 → 1	Z: 0 hold
es2	X: 0 → 1, Y: 1 hold	Z: 0 hold
es4	X: 1 hold, Y: 1 → 0	Z: 0 hold
es5	X: 1 → 0, Y: 1 hold	Z: 0 hold

By "S: i → j," we denote the transition where the logic value of signal S changes from i to j.

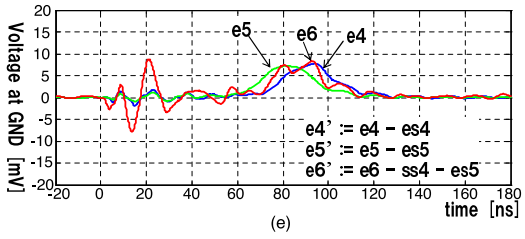
(b)



(c)



(d)



(e)

Fig. 2. (a) NOR gate circuit, (b) Input signal definition for each event, (c) Waveforms of voltage of Z, (d) Power traces of e1, e2, e3, (e) Power traces of e4, e5, e6.

DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012

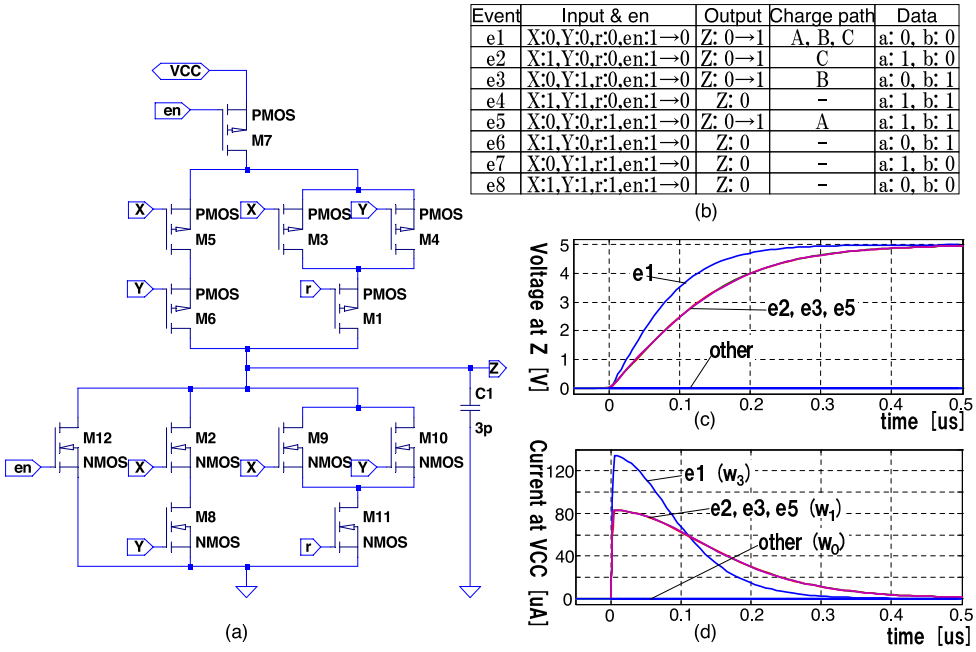


Fig. 3. (a) RSL-NAND circuit, (b) Input signal definition for each event, (c) Waveforms of voltage of Z for each event, (d) Power traces of each event.

3.2 Spice simulation: RSL-NAND

The RSL-gate power trace was analyzed by LTspice IV [8], an analog circuit simulator from Liner Technology. The target circuit RSL-NAND [4] is shown in Fig. 3 (a). The capacitor C1 (3 pF) was inserted in the output Z as the load capacitance. The voltage at VCC was set to 5 V. The default parameters were used for pMOS and nMOS. Signals X, Y, r, and en were driven, as shown in Fig. 3 (b). The charging current flowed from VCC to C1 via three paths:

$$\begin{aligned} \text{path} \quad \text{A}: \quad & VCC - M7 - M5 - M6 - C1; \\ \text{path} \quad \text{B}: \quad & VCC - M7 - M3 - M1 - C1; \\ \text{path} \quad \text{C}: \quad & VCC - M7 - M4 - M1 - C1. \end{aligned}$$

The waveform of e1 is easily distinguishable from that of the other events (Figs. 3 (c) and 3 (d)) because there are three charging paths for e1 (A, B, and C), while there is only one (A, B, or C) or no path for the others, as shown in Fig. 3 (b).

3.3 CMOS and RSL results

The electrical (dis)charging time constant differs with the number of (dis) charging paths; hence, the current peak and transition time for the subsequent gates changed. This fluctuation of the delay time was detected as shown in Fig. 2 (d).

DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012

4 Security analysis of RSL with power traces

Analysis of the RSL security against DPA must be reconsidered with power traces. The power traces of RSL-NAND are shown as the waveforms of VCC (Fig. 3 (d)) and classified into three types: w_3, power trace of e1; w_1, power trace of e2, e3, and e5; w_0, power trace of other events. The events for which $a = 1$ are e2, e4, e5, and e7 (Fig. 3 (b)), and those for which $a = 0$ are e1, e3, e6, and e8. Hence, the RSL DPA trace dW_{RSL} is

$$dW_{\mathrm{RSL}} = \frac{w_1 + w_0 + w_1 + w_0}{4} - \frac{w_3 + w_1 + w_0 + w_0}{4} = \frac{w_1 - w_3}{4}.$$

Here, $w_1 \neq w_3$, and consequently, $dW_{\mathrm{RSL}} \neq 0$, implying that DPA may succeed in attacking RSL-NAND.

To examine the effect of RSL, r is fixed at 0, i.e., the RSL function is disabled, and the DPA trace is

$$dW_{\mathrm{RSLoff}} = \frac{w_1 + w_0}{2} - \frac{w_3 + w_1}{2} = \frac{w_0 - w_3}{2}.$$

The peak values of w_3 and w_1 are 135 μA and 83 μA, respectively (Fig. 3 (g)). The peak of $dW_{\mathrm{RSL}} = (w_1 - w_3)/4 = -13\,\mu\mathrm{A}$, and that of $dW_{\mathrm{RSLoff}} = (w_0 - w_3)/2 = -67\,\mu\mathrm{A}$. With RSL, a fivefold decrease in the peak of the DPA trace (non-zero peak) is observed.

5 Conclusion

A proper security analysis method for DPA countermeasures such as RSL has been proposed. Despite the security proof against DPA in Convenient Model, the attack can be successful because the presence of different (dis)charge paths changes the power trace shape and output delay. This has been confirmed by the measurements on CMOS NOR and RSL-NAND simulation. The results show that Convenient Model alone is not always sufficient for power analysis for security proof. The DPA resistance of CMOS circuits should be evaluated by properly including power traces in the model.

DOI: 10.1587/elex.9.458
Received January 11, 2012
Accepted February 20, 2012
Published March 25, 2012