A Practical DPA Countermeasure with BDD Architecture

Toru Akishita, Masanobu Katagi, Yoshikazu Miyato,
Asami Mizuno, and Kyoji Shibutani

System Technologies Laboratories, Sony Corporation,
1-7-1 Konan, Minato-ku, Tokyo 108-0075, Japan
{Toru.Akishita,Masanobu.Katagi,Yoshikazu.Miyato}@jp.sony.com,
{Asami.Mizuno,Kyoji.Shibutani}@jp.sony.com

Abstract. We propose a logic-level DPA countermeasure called Dual-rail Pre-charge circuit with Binary Decision Diagram architecture (DP-BDD). The proposed countermeasure has a dual-rail pre-charge logic style and can be implemented using CMOS standard cell libraries, which is the similar property to Wave Dynamic Differential Logic (WDDL). By using novel approaches, we can successfully reduce the early propagation effect, which is one of the main factors of DPA leakage of WDDL. DP-BDD is suited to implementation of S-boxes. In our implementations of the AES S-box, DP-BDD can reduce the maximum difference of transition timing at outputs of S-box to about 1/6.5 compared to that of WDDL without delay adjustment. Moreover, by applying simple delay adjustment to the inputs of the S-box, we can reduce it to about 1/85 of that without the adjustment. We consider DP-BDD is a practical and effective DPA countermeasure for implementation of S-boxes.

Keywords: DPA, countermeasure, dual-rail pre-charge logic, Binary Decision Diagram

1 Introduction

Differential Power Analysis (DPA) is a serious threat to cryptographic devices such as smart cards [8]. Recently, various countermeasures have been proposed to protect implementations of cryptographic algorithms against DPA at the logic level. Since the logic-level countermeasures can be adapted to basic logical gates such as an AND gate, we can apply them to implementations of any cryptographic algorithms. These logic-level countermeasures are classified into the following three groups: masking logics, dual-rail pre-charge logics, and hybrid-type logics.

Masking logics try to randomize the activity at every node in a circuit using random values in order to remove correlation between key-related intermediate values and power consumption of the circuit. Masked-AND, a type of masking logics, was proposed by Trichina [20]. It has been pointed out, however, that Masked-AND is not completely secure due to the effect of glitches [9, 14]. Recently, Random Switching Logic (RSL) was proposed by Suzuki et al. [16]. RSL

is theoretically secure under the leakage models described in [14], but possesses two disadvantages: one is that it cannot be implemented using CMOS standard cell libraries and the other is that it requires careful timing adjustment of enable signals.

A dual-rail pre-charge logic was first proposed by Tiri et al. as Sense Amplifier Based Logic (SABL) [17], where a signal is represented by two complementary wires and one of these two wires is charged and discharged in every cycle. Considering that SABL needs a special CMOS library, Tiri et al. also proposed Wave Dynamic Differential Logic (WDDL) [18] that can be implemented using CMOS standard cell libraries. WDDL is a practical countermeasure, but it cannot suppress two factors of DPA leakage. The first one is due to unbalanced load capacitance of complementary logic gates. In order to balance it, WDDL requires a custom layout for a secure design [19, 7]. The other is due to the early propagation effect. This leakage is caused when input signals of a WDDL gate have difference of delay time [14]. The input signals generally pass the different number of logic gates, and then the difference of delay time inevitably occurs. Careful delay adjustment can reduce the difference, but applying it all WDDL gates in cryptographic circuits seems to be unrealistic.

Hybrid-type logics are combined with masking logics and dual-rail pre-charge logics. At CHES 2005, Popp and Mangard proposed MDPL that combines dual-rail pre-charge circuits with random masking to improve the first disadvantage of WDDL [11]. They claimed that it can achieve secure design using a CMOS standard cell library without special layout constraint, but in the next year it was pointed out that MDPL can be still insecure when there is relatively large difference in delay time between the input signals of MDPL gates [4, 15]. In addition, the combination of masking and dual-rail was shown to be unable to provide a routing-insensitive logic style [6, 13]. At present, hybrid-type logics seem to have no advantage over dual-rail pre-charge logics.

In this paper, we propose a novel DPA countermeasure called *Dual-rail Precharge circuit with Binary Decision Diagram architecture* (DP-BDD). It is based on a Binary Decision Diagram (BDD) that is a direct acyclic graph used to represent a Boolean function. DP-BDD is composed of AND-OR gates which are included in CMOS standard cell libraries. Due to the based BDD architecture, the input signals of an AND-OR gate always pass the same number of AND-OR gates, and then the early propagation effect, which is one of the main factors of DPA leakage of WDDL, is significantly reduced.

This DPA countermeasure is suited to implementation of S-boxes. In our implementations of the AES [10] S-box, DP-BDD can reduce the maximum difference of transition timing at the outputs of the S-box to about 1/6.5 compared to that of WDDL without delay adjustment. Moreover, by applying simple delay adjustment to the inputs of the S-box, we can reduce it to about 1/85 of that without the adjustment. DP-BDD requires a custom layout to prevent the leakage caused by unbalanced load capacitance of complementary logic gates the same as WDDL, but we consider that DP-BDD is a practical and effective DPA countermeasure for implementation of S-boxes.

The rest of the paper is organized as follows: Section 2 presents WDDL and its security problem. Section 3 gives brief introduction of BDD that is the basic architecture of our method. In Section 4 we present the proposed DPA countermeasure called DP-BDD. In Section 5, we apply WDDL and DP-BDD to implementations of AES S-box and compare their effectiveness. We introduce simple delay adjustment of DP-BDD to reduce the difference of transition timing further in Section 6. Finally we draw our conclusion and discuss further work in Section 7.

2 Wave Dynamic Differential Logic (WDDL)

Tiri et al. proposed Wave Dynamic Differential Logic (WDDL) as a logic-level countermeasure of DPA [18]. WDDL has the following features:

- WDDL gates have complementary inputs and outputs.
- WDDL has the pre-charge phase to transmit $(0, 0)$ and the evaluation phase to transmit $(0, 1)$ or $(1, 0)$, and performs these phases mutually.
- WDDL can construct combinational logics by using only AND gates, OR gates, and NOT operations (signal swapping).

A value a is represented $(a, \overline{a})$ in WDDL, where $\overline{a}$ is the negation of a. An activity factor within WDDL circuits is constant independent of the input signals due to the above features. Since power consumption at CMOS gates generally depends on the transition probability of the gates, WDDL is considered to be effective as a DPA countermeasure.

However, the power consumption at CMOS gates also depends on load capacitance of the gates. If there is difference of load capacitance between complementary logic gates of WDDL, the difference of power consumption occurs. The number of gates connected to complementary logic gates of WDDL is basically equal, and then the difference of load capacitance is caused by the difference of place-and-route. The leakage due to the place-and-route is called as *incidental leakage* [15]. It can be improved by the place-and-route in the manual or semi-automatic operation using special constraints such as "Fat Wire" [19] and "Backend Duplication" [7].

Another leakage is due to the early propagation effect [14, 15]. This leakage is caused when there is the difference of delay time between the input signals of a WDDL gate. In Fig. 1, we illustrate a WDDL AND gate and its signal transitions according to the inputs (a, b). Here, we assume that the transition of a or $\overline{a}$ reaches the gate earlier than the transition of b or $\overline{b}$ both on the evaluation phase and on the pre-charge phase. The transition timing of the complementary output q or $\overline{q}$ on the evaluation phase depends on the input a. On the other hand, the transition timing of q or $\overline{q}$ on the pre-charge phase depends on the input b. Therefore, the difference of delay time between the inputs a and b may leak the values a and b. Since basic cryptographic components including S-boxes of blockciphers require complicated logic circuits, the input signals of a WDDL gate generally pass different number of logic gates. Therefore, the difference of

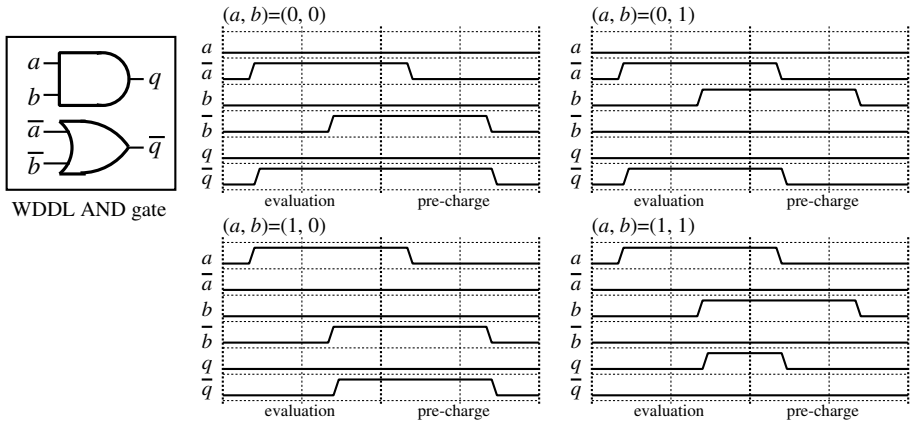

Fig. 1. The early propagation effect of a WDDL AND gate

delay time between these signals inevitably occurs. This type of leakage is called as *inevitable leakage* [15]. The leakage can be improved by adjusting delay time between the input signals, but very high effort and many constraints in the circuit design are required to adjust delay time of all WDDL gates in complicated logic circuits including S-boxes.

3 Binary Decision Diagram

A Binary Decision Diagram (BDD) is a direct acyclic graph that is used to represent a Boolean function [1], and one of most commonly used synthesis tools for logic optimization of digital systems [22]. We briefly explain a BDD according to Fig. 2. The left figure is a truth table representing the function $f(A, B, C)$ and the right figure shows a block diagram of a binary decision tree corresponding to the truth table. In the right figure, an isosceles trapezoid represents a 2-to-1 multiplexer, and we call a signal A, B, C as a *non-terminal node*, a signal $0, 1, 0, \cdots$ at the lowest part as a *terminal node*, and a signal connecting two multiplexers as an *internal node*. The outputs f in the truth table are located in regular order from the left to the right of terminal nodes.

Generally the term BDD refers to Reduced Ordered Binary Decision Diagram (ROBDD) [2]. A binary decision tree is uniquely transformed into ROBDD by merging any isomorphic subgraphs and eliminating any redundant nodes. In this paper, however, we call as BDD the block diagram in which we only merge any isomorphic subgraphs on a binary decision tree. In this BDD architecture, since the same number of multiplexers must be passed from any terminal node to the output, the difference of propagation delay dependent of inputs is relatively small.

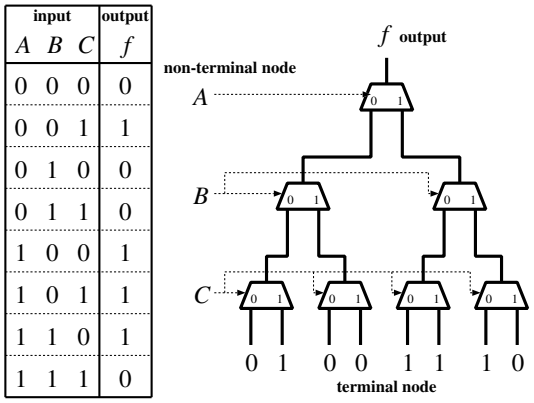

Fig. 2. A truth table and a binary decision tree

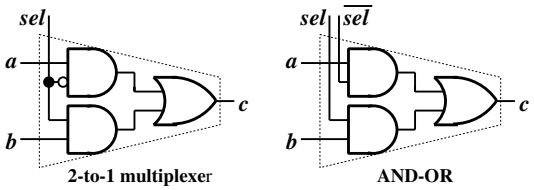

Fig. 3. A 2-to-1 multiplexer and an AND-OR gate

4 Dual-Rail Pre-Charge Circuit with Binary Decision Diagram Architecture

In this section, we propose a novel DPA countermeasure to reduce the inevitable leakage at logic level, called Dual-rail Pre-charge circuit with Binary Decision Diagram architecture (DP-BDD). It is based on BDD and constructed in the following steps.

Pre-charged AND-OR gates. We avoid the existence of glitches to control the transition probability of all signals in a BDD circuit. In order to prevent glitches, we firstly replace 2-to-1 multiplexers in BDD to 2-way 2-and 4-input AND-OR (shortly, AND-OR) gates. As shown in Fig. 3, an AND-OR gate is equivalent to a 2-to-1 multiplexer except the negation of a select signal being input. Fig. 4(a) shows a modified BDD circuit. In the figure an isosceles trapezoid represents an AND-OR gate. Non-terminal nodes $(A, \overline{A})$, $(B, \overline{B})$, or $(C, \overline{C})$ are connected to each AND-OR gate as $(sel, \overline{sel})$ in Fig. 3.

Next, we apply so-called pre-charge mechanism to the terminal nodes $(0, 1)$ and the non-terminal nodes $(A, \overline{A})$, $(B, \overline{B})$, $(C, \overline{C})$; these signals are set to 0 on the pre-charge phase and evaluate to the corresponding value on the evaluation

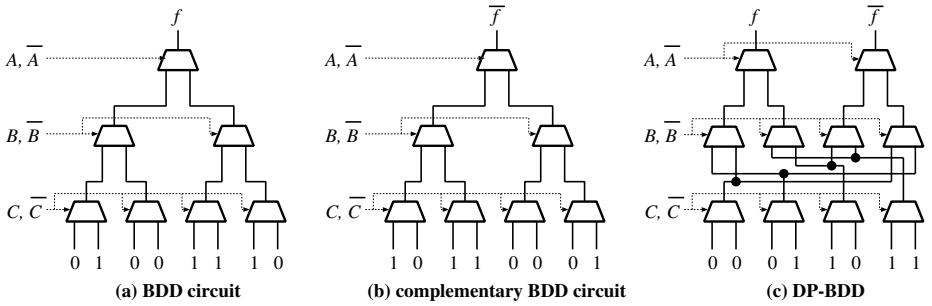

Fig. 4. Constructing DP-BDD

phase. We consider the output of an AND-OR gate at the lowest stage. On the evaluation phase, all four inputs of an AND-OR gate perform either $(0 \to 0)$ or $(0 \to 1)$, then the output also performs either $(0 \to 0)$ or $(0 \to 1)$. On the pre-charge phase, all four inputs perform either $(0 \to 0)$ or $(1 \to 0)$, then the output also performs either $(0 \to 0)$ or $(1 \to 0)$. By adapting these transitions to the inputs of AND-OR gates at the next stage, we can confirm that all internal nodes and outputs of BDD have at most one transition both on the evaluation phase and on the pre-charge phase. Therefore, we can prevent glitches in the BDD circuit.

Appending complementary circuit. Preventing glitches doesn't give any guarantee to DPA resistance because the distribution of the transition activity depends on the inputs A, B, C. In order to make it independent of the inputs, we construct the complementary BDD circuit to the original BDD circuit. It can be simply created by exchanging 0 and 1 which are input to the terminal nodes as shown in Fig. 4(b). By appending the complementary circuit to the original circuit and merging them as shown in Fig. 4(c), one of the complementary AND-OR gates perform a transition both on the evaluation phase and on the pre-charge phase. Therefore, the activity factor within the merged circuit is constant independent of the input signals. We call such a merged circuit as Dual-rail Pre-charge circuit with Binary Decision Diagram architecture (DP-BDD). [1]

We consider the inevitable leakage, which is leakage caused by the difference of delay time between the input signals of complementary AND-OR gates shown in Fig. 5. We assume that all inputs of DP-BDD, non-terminal nodes and terminal nodes, are directly connected to registers and have no propagation delay except their setup time.

[1] By inputting a random bit m and its negation $\overline{m}$ to the terminal nodes instead of 0 and 1, all internal nodes and output of DP-BDD are easily masked by m. The addition of random masking, however, does not achieve secure design without special layout constraint according to the observation in [6, 13].

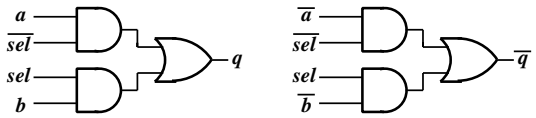

Fig. 5. Complementary AND-OR gates

The difference of delay time between input signals of AND-OR gates may lead the difference of transition timing at the output which depends on some secret information. Since signals sel and $\overline{sel}$ are directly connected to inputs of DP-BDD, the transition of sel and $\overline{sel}$ occurs soon after the transition from the pre-charge phase to the evaluation phase, and the reverse transition. On the pre-charge phase, the transition of q or $\overline{q}$ occurs at the time when the transition of sel or $\overline{sel}$ whether $sel = 0$ or 1. On the evaluation phase, if $sel = 0$, the transition of the output signal q or $\overline{q}$ occurs at the time when the transition of the input a or $\overline{a}$ occurs; if $sel = 1$, the transition of q or $\overline{q}$ occurs at the time when the transition of the input b or $\overline{b}$ occurs. Therefore, the difference of delay time between a and b (or $\overline{a}$ and $\overline{b}$) may leak the value sel on the evaluation phase. However, since the signals a and b (or $\overline{a}$ and $\overline{b}$) pass the same number of AND-OR gates, the difference of delay time between these signals is relatively small, and then detecting the inevitable leakage by DPA is more difficult.

5 Application to AES S-box

In order to protect hardware implementations of the Advanced Encryption Standard (AES) [10], the S-box is the most critical operation because it is the only non-linear operation in AES. In this section, we apply both WDDL and DP-BDD to implementations of AES S-box, and compare their effectiveness.

5.1 AES S-box based on WDDL (WDDL S-box)

There are various ways to implement the AES S-box. The most compact implementation of AES S-box is that using composite fields [12, 21, 3]. We apply WDDL to the AES S-box described in [21], whose overall amount of gates is 103 XORs + 57 ANDs, because of its relatively short critical path.

Fig. 6 shows the schematic circuit of AES S-box using composite fields. There are several operations including an isomorphic mapping, multiplications and additions over Galois field. We notice path 1 and path 2 which both are the paths to the multiplication circuit over GF(2^4). Path 1 has relatively short propagation delay because it passes only the isomorphic mapping circuit. On the other hand, path 2 has long propagation delay because it passes also the squaring, constant multiplication, addition, and inversion circuits over GF(2^4) except the isomorphic mapping circuit. Thus, since the difference of delay time between path 1 and 2 are large, we guess the inevitable leakage caused by this difference can be detected by DPA.

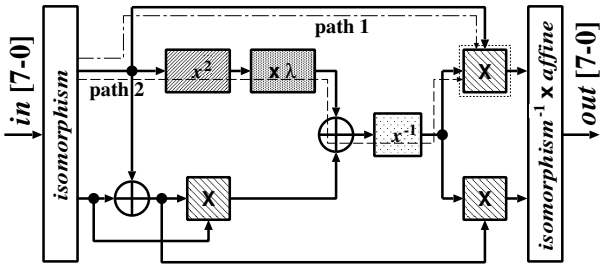

Fig. 6. AES S-box using composite fields

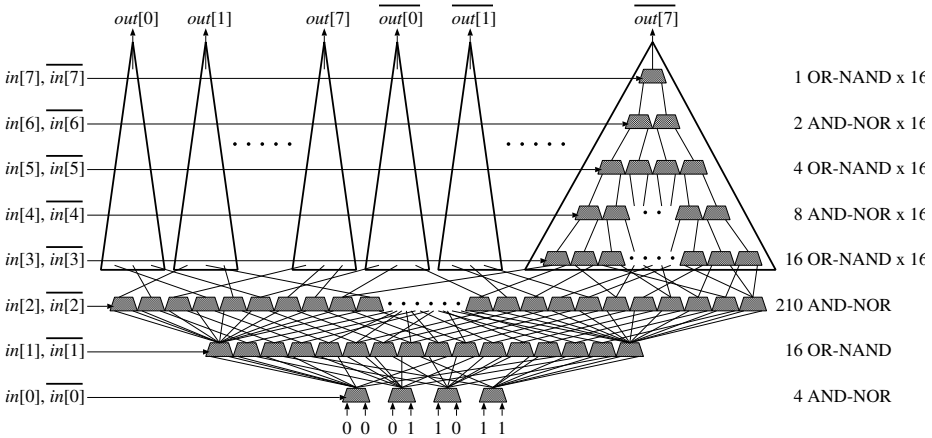

Fig. 7. AES S-box based on DP-BDD (DP-BDD S-box)

5.2 AES S-box based on DP-BDD (DP-BDD S-box)

Since the AES S-box has an 8-bit input and an 8-bit output, we firstly arrange eight binary decision trees of eight stages according to the truth tables of AES S-box. Then, AES S-box based on DP-BDD (DP-BDD S-box) can be constructed in the way described in Section 4.

Fig. 7 shows the constructed DP-BDD S-box, where $in[i]$ denotes i-th bit of the input of the S-box and $out[i]$ denotes i-th bit of the output. In CMOS a positive gate is usually constructed out of a negative gate and an inverter, and then the use of positive gates is a disadvantage in terms of gate size. In order to reduce the gate size of DP-BDD S-box, we replace AND-OR gates to AND-NOR gates at the odd stages and to OR-NAND gates at the even stages, and then the input of OR-NAND gates are pre-charged to 1 on the pre-charge phase. Its overall amount of gates is 374 AND-NORs + 352 OR-NANDs. Since any path from the terminal node 0 and 1 to two input signals of an AND-NOR/OR-NAND

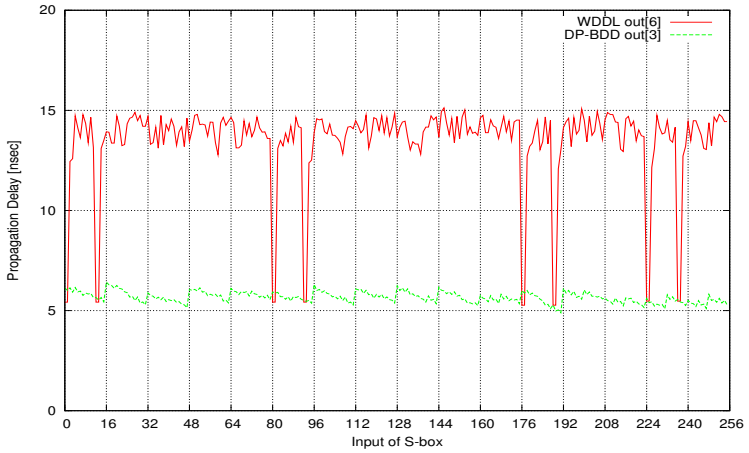

Fig. 8. Propagation delay of an output bit of WDDL S-box and DP-BDD S-box

gate passes the same number of AND-NOR/OR-NAND gates, the difference of delay time between the input signals of the gate is relatively small.

5.3 Experimental Results

We implemented both WDDL S-box and DP-BDD S-box, and performed netlist timing simulations to evaluate their effectiveness. The environment of our evaluation is as follows:

Language	Verilog-HDL
Design Library	0.18 μm CMOS standard cell library
Simulator	VCS version 2006.06
Logic Synthesis	Design Compiler version 2006.06

One gate is equivalent to a 2-way NAND and the speed is evaluated under the worst-case conditions. In the library, an AND/OR gate, an AND-OR/OR-AND gate, and an AND-NOR/OR-NAND gate are equivalent to 5/4 gates, 9/4 gates, and 7/4 gates, respectively. These simulations are based on pre-routing delay, and then free from the incidental leakage caused by the automatization of the place-and-route.

We firstly evaluate the gate counts of WDDL S-box and DP-BDD S-box. An AND gate in the AES S-box is implemented using an AND gate and an OR gate in WDDL S-box as shown in Fig. 1, while an XOR gate in the AES S-box can be implemented using an AND-OR gate and an OR-AND gate. Thus the gate count of WDDL S-box is equivalent to $103 \times 9/2 + 57 \times 5/2 = 606$ excluding buffers. On the other hand, the gate count of DP-BDD S-box is equivalent to $374 \times 7/4 + 352 \times 7/4 = 1271$ excluding buffers.

Next, we evaluate the difference of transition timing at the output of logic gates in both WDDL S-box and DP-BDD S-box. Since we guessed the largest difference will occur at the output of the S-box, we searched the output bit of S-box that has the largest difference of transition timing for all possible 256 S-box inputs; $out[6]$ (or $\overline{out[6]}$) and $out[3]$ (or $\overline{out[3]}$) are the corresponding bits of WDDL S-box and DP-BDD S-box respectively. Fig. 8 shows the propagation delay of these bits for all 256 inputs; the above line shows that of WDDL S-box and the below line shows that of DP-BDD S-box. We confirmed that the maximum difference of transition timing at the output of DP-BDD S-box (1.526 ns) is about 1/6.5 of that of WDDL S-box (9.855 ns).

6 Towards Less Difference of Transition Timing

DP-BDD reduces the difference of transition timing at the output of AND-OR gates. It is, however, desirable to reduce this difference all the more since it could be detected by DPA. We consider that the difference occurs by the accumulation of the following factors:

- difference of propagation delay between input ports of each AND-OR gate,
- difference of load capacitance between input ports of each AND-OR gate,
- difference of the number of fan-out between output signals of AND-OR gates.

In order to reduce the influence of these factors, we apply delay adjustment to inputs of DP-BDD shown in Fig. 9.

On the pre-charge phase, we don't require any delay adjustment cell because the difference of transition timing at the output of each AND-OR gate is equivalent to the difference of propagation delay between input port of the AND-OR gate.

On the evaluation phase, we insert delay cells of $delay(a)$, $delay(b)$, and $delay(c)$ to $(A, \overline{A})$, $(B, \overline{B})$, and $(C, \overline{C})$ respectively. By inserting the delay cell of $delay(c)$ to $(C, \overline{C})$, a transition of the output of AND-OR gates at stage 1 occurs at the time when a transition of C or $\overline{C}$ reaches their input ports. Next, we set $delay(b)$ that satisfies $delay(b) - delay(c)$ is larger than the propagation delay from any input ports of AND-OR gates at stage 1 to any input ports of AND-OR gates at stage 2. That indicates that a transition of the output of AND-OR gates at stage 2 occurs at the time when a transition of B or $\overline{B}$ reaches their input ports. Similarly, we set $delay(a)$ that satisfies $delay(a) - delay(b)$ is larger than the propagation delay from any input ports of AND-OR gates at stage 2 to any input ports of AND-OR gates at stage 3. Therefore, we can reduce the difference of transition timing at the outputs of all AND-OR gates to the difference of propagation delay between input port of the AND-OR gate also on the evaluation stage. It is very easy to satisfy these delay conditions because we have only to make the difference of delay between any two adjacent bits of the input sufficiently large.

By switching the input signals without delay and those with delay using AND gates, we can successfully reduce the difference of transition timing at all signals

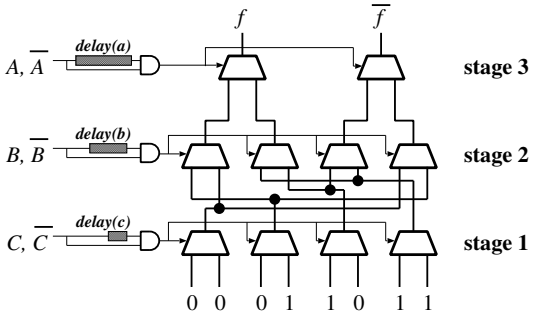

Fig. 9. Delay adjustment for DP-BDD

in DP-BDD in both the pre-charge stage and the evaluation stage. We confirmed that this delay adjustment reduced the maximum difference of transition timing in DP-BDD S-box to 0.018 ns (about 1/85 of that without delay adjustment), which is just the difference of propagation delay between the input ports *sel* and $\overline{sel}$ of an OR-NAND gate.

7 Conclusion

In this paper we presented the logic-level DPA countermeasure called DP-BDD. DP-BDD has a dual-rail logic style and can be implemented using CMOS standard cell libraries. Our experimental results showed that DP-BDD can significantly reduce the difference of transition timing at the outputs of AES S-box compared to WDDL. We consider that DP-BDD is a practical and effective DPA countermeasure for implementations of S-boxes.

At CHES 2006, Homma et al. presented high-resolution waveform matching based on a Phase-Only Correlation (POC) techniques and its application to DPA [5]. They claimed that the POC-based techniques can evaluate the displacement between signal waveforms with higher resolution than the sampling resolution. One of further works we need to carry out is how large difference of the delay time between the input signals leads to DPA leakage in real devices using such techniques.

References

1. S.B. Akers, "Binary Decision Diagram", *IEEE Trans. on Computers*, Vol.C-27, No.6, pp.509-516, 1978.
2. R.E. Bryant, "Graph-Based Algorithm for Boolean Function Manipulation", *IEEE Trans. on Computers*, Vol.C-35, No.8, pp.677-691, 1986.
3. D. Canright, "A Very Compact S-Box for AES", *CHES 2005*, LNCS 3659, pp.441-455, Springer-Verlag, 2005.

4. Z. Chen and Y. Zhou, "Dual-Rail Random Switching Logic: A Countermeasure to Reduce Side Channel Leakage", *CHES 2006*, LNCS 4249, pp.242-254, Springer-Verlag, 2006.
5. N. Homma, S. Nagashima, Y. Imai, T. Aoki, and A. Satoh, "High-Resolution Side-Channel Attack Using Phase-Based Waveform Matching", *CHES 2006*, LNCS 4249, pp.187-200, Springer-Verlag, 2006.
6. B. Gierlichs, "DPA-Resistance Without Routing Constraints?", *CHES 2007*, LNCS 4727, pp.107-120, Springer-Verlag 2007.
7. S. Guilley, P. Hoogvorst, Y. Mathieu, and R. Pacalet, "The "Backend Duplication" Method", *CHES 2005*, LNCS 3659, pp.383-397, Springer-Verlag, 2005.
8. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", *Crypto '99*, LNCS 1666, pp.388-397, Springer-Verlag, 1999.
9. S. Mangard, T. Popp, and B.M. Gammel, "Side-Channel Leakage of Masked CMOS Gates", *CT-RSA 2005*, LNCS 3376, pp.351-365, Springer-Verlag, 2005.
10. National Institute of Standard and Technology (NIST), "Advanced Encryption Standard (AES)", FIPS Publication 197, 2001.
11. T. Popp and S. Mangard, "Masked Dual-Rail Pre-Charge Logic: DPA-Resistant without Routing Constraints", *CHES 2005*, LNCS 3659, pp.172-186, Springer-Verlag, 2005.
12. A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A Compact Rijndael Hardware Architecture with S-box Optimization", *ASIACRYPT 2001*, LNCS 2248, pp.239-254, Springer-Verlag, 2001.
13. P. Schaumont and K. Tiri, "Masking and Dual-Rail Logic Don't Add Up", *CHES 2007*, LNCS 4727, pp.95-106, Springer-Verlag, 2007.
14. D. Suzuki, M. Saeki, and T. Ichikawa, "DPA Leakage Models for CMOS Logic Circuits", *CHES 2005*, LNCS 3659, pp.366-382, Springer-Verlag, 2005.
15. D. Suzuki and M. Saeki, "Security Evaluations of DPA Countermeasures Using Dual-Rail Pre-Charge Logic Style", *CHES 2006*, LNCS 4249, pp.255-269, Springer-Verlag, 2006.
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 Transactions 90-A(1), pp.160-168, 2007.
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", *ESSCIRC 2002*, pp.403-406, 2002.
18. K. Tiri and I. Verbauwhede, "A Logic Level Design Methodology for A Secure DPA Resistant ASIC or FPGA Implementation", *DATE 2004*, pp.246-251, 2004.
19. K. Tiri and I. Verbauwhede, "Place and Route for Secure Standard Cell Design", *CARDIS 2004*, pp.143-158, 2004.
20. E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data", IACR Cryptology ePrint Archive 2003/236, 2003. http://eprint.iacr.org/2003/236
21. J. Wolkerstorfer, E. Oswald, and M. Lamberger, "An ASIC Implementation of the AES S-boxes", *CT-RSA 2002*, LNCS 2271, pp.67-78, Springer-Verlag, 2002.
22. C. Yang, M. Ciesielski, V. Singhel, "BDS: A BDD Based Logic Optimization System", *Proc. of the 37th ACM/IEEE DAC 2000*, pp. 92-97, 2000.