Center for Embedded Computer Systems
University of California, Irvine

A Standard Cell-Based DPA Attack Countermeasure using Homogeneous Dual-Rail Logic (HDRL)

Kazuyuki Tanimura and Nikil Dutt

Center for Embedded Computer Systems
University of California, Irvine
Irvine, CA 92697-2625, USA

{ktanimur},{dutt}@uci.edu

CECS Technical Report <12-01>
January 25, 2012

A Standard Cell-Based DPA Attack Countermeasure using Homogeneous Dual-Rail Logic (HDRL)

Kazuyuki Tanimura, *Non Member, IEEE,* and Nikil D. Dutt, *Fellow, IEEE*

***Abstract*—DPA (Differential Power Analysis) attacks statistically find the correlation between power consumption and secret data in crypto-hardware. WDDL (Wave Dynamic Differential Logic) is a standard cell-based countermeasure for DPA and guarantees a 100% switching factor to shield the power information. However, our experiments observe that WDDL fails to compensate the power imbalance. This paper proposes Homogeneous Dual-Rail Logic (HDRL), a standard cell DPA attack countermeasure that theoretically guarantees fully balanced power consumption and significantly improves DPA attack resistivity. Our experimental results on the AES S-Box circuit show that HDRL successfully prevents DPA attacks in all cases. In addition, HDRL achieves such higher security with only 100.0% energy overhead while WDDL incurs 231.7% energy overhead. Also, HDRL requires the same area overhead as WDDL. HDRL's better resistivity and lower energy overhead make it a promising countermeasure for standard cell based embedded crypto-applications such as smart cards.**

I. Introduction

Side-channel attacks are a substantive security threat for crypto-hardware systems. Kocher et al. [1] proposed DPA (Differential Power Analysis) attack that is one of the most difficult side-channel attacks to prevent. A number of transistor through register-transfer level countermeasures have been proposed [2]–[22] with varying DPA attack resistivity. In particular, WDDL (Wave Dynamic Differential Logic) [7]–[12] has been well researched since it requires only standard cells, which reduces design cost and time compared to full-custom ASIC countermeasures. WDDL incurs over 2x area and energy overheads due to pairing a complementary cell with every cell in the original circuit. Despite sacrificing such overheads, WDDL is still vulnerable to DPA attacks.

This paper proposes Homogeneous Dual-Rail Logic (HDRL) that guarantees fully balanced power consumption of standard cells. Experimental results on an AES S-Box circuit exemplar demonstrate HDRL provides higher DPA attack resistivity in all instances with much lower energy (100.0% vs. 231.7%) overhead and similar area overhead compared with traditional WDDL. Since HDRL is a standard cell countermeasure, HDRL is a promising approach, where design cost and time are critical.

II. DPA Attack Model Formulation

Fig. 1 shows the 128-bit AES circuit with 16 S-Boxes [23]. Note this paper evaluates HDRL using the AES circuit; however, HDRL is also applicable to any other crypto-hardware. `PlainText`, `CipherText`, and `ScheduledKey` of Fig. 1 are 128-bit vectors of plain text, cipher text, and scheduled key (consists of 16 sub 8-bit secret `Keys`), respectively. It takes 10 Rounds (cycles) until the valid `CipherText` is out. According to Morioka et al. [24], S-Boxes consume 75% of energy in an AES circuit. Thus, S-Boxes are the easiest targets for adversaries to conduct DPA attacks. Fig. 2 shows the DPA attack model for evaluating a single AES S-Box [19], [22], [25], [26]. In Fig. 2, adversaries attempt to uncover `Key` (the sub 8-bit secret key of `ScheduledKey` in Fig. 1), and they measure `VSS` current of the circuit.

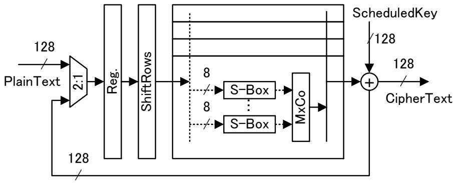

Fig. 1. AES Data Path

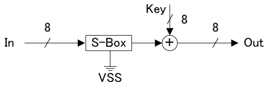

Fig. 2. DPA Attack Model on AES S-Box

The following is the DPA attack procedure. Adversaries observe the `Out` and `VSS` current of Fig. 2 as many times as possible. By collecting a number of data, DPA can statistically find the correlation between `Key` and `VSS` (even if `VSS` is noisy data). Adversaries group the observed `VSS` into either G_0 or G_1 referring to a selection function D in Eq. (1). D returns an 8-bit value [25].

$$D = Sbox^{-1}(c \oplus k_{est.}) \tag{1}$$

c, $k_{est.}$, and $Sbox^{-1}$ are 8-bit cipher text, estimated 8-bit sub secret key, and inverse AES S-Box function, respectively. Moreover, c is an element of `CipherText` and equivalent to `Out` in Fig. 2. The returned D value equals to `In` in Fig. 2 iff $k_{est.}$ =`Key`.

Let A_0 and A_1 be the average `VSS` current in G_0 and G_1.

$$\begin{align} 0 \le \quad & t \quad < \text{clock period} \tag{2} \\ A_0(t) \quad & = \quad \frac{1}{|G_0|} \sum_{D(c,k_{est.}) \in G_0} p_c(t) \tag{3} \\ A_1(t) \quad & = \quad \frac{1}{|G_1|} \sum_{D(c,k_{est.}) \in G_1} p_c(t) \tag{4} \end{align}$$

, where t is the time `VSS` current is sampled. $p_c(t)$ is the measured `VSS` current with respect to cipher text c at time t. Every $p_c(t)$ has to belong to either G_0 or G_1. $|G_0|$ and $|G_1|$ are the number of $p_c(t)$ in the group.

There are two well-known grouping methods for making G_0 or G_1. One refers to the ith bit of the 8-bit D value. In this method, $p_c(t)$ is grouped into

$$\left.\begin{array}{l} G_0 \text{ when } D[i] = 0 \\ G_1 \text{ when } D[i] = 1 \end{array}\right\} \tag{5}$$

The other grouping refers to Hamming weight of the D [27]. In this method, $p_c(t)$ is grouped into

$$\left.\begin{array}{l} G_0 \text{ when } 0 \le \text{Hamming weight of} D < 4 \\ G_1 \text{ when } 4 < \text{Hamming weight of} D \le 8 \end{array}\right\} \tag{6}$$

When $k_{est.}$ $\neq$`Key`, the absolute difference between A_0 and A_1 is expected to be close to zero. In contrast, when $k_{est.}$ =`Key`, the absolute differential power between A_0 and A_1 is expected to become the largest amongst all $2^8 = 256$ candidates of 8-bit $k_{est.}$. This largest differential power is denoted as DP and formulated as follows.

$$DP = \arg\max_t |A_0(t) - A_1(t)| \tag{7}$$

Ideal countermeasures have the same differential power (i.e., $DP \approx 0$) for all $k_{est.}$ candidates so that adversaries lose the reasoning for $k_{est.}$ =`Key`.

DPA is much faster than brute-force attacks. The DPA search space is $2^8 \times 16$ (128-bit AES uses 16 S-Boxes) whereas there are 2^{128} possible candidates of 128-bit `ScheduledKey`. This paper focuses on the first order DPA formulated above to compare HDRL to WDDL rather than higher order DPA.

K. Tanimura and N. D. Dutt are with the Department of Computer Science, University of California, Irvine, Irvine, CA 92697 USA e-mail: {ktanimur},{dutt}@uci.edu

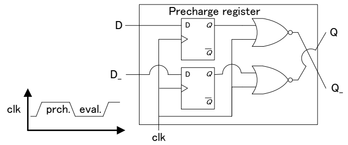

Fig. 3. WDDL Pre-charge Timing and Generation

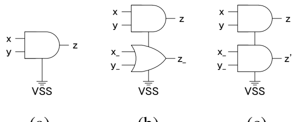

Fig. 4. (a) Normal (b) WDDL (c) HDRL AND

III. Related Work

A number of countermeasures against DPA attacks have been researched [2]–[22]. Randomization countermeasures [2]–[6], [19]–[21] mask intermediate results and agitate power information. These countermeasures make it difficult to perform DPA but do not guarantee to obscure the power information despite sacrificing performance.

Power balancing is another approach for mitigating DPA. Transistor level countermeasures [13]–[18] can level the DP imbalance. However, the full-custom ASIC solution requires prohibitively expensive design cost and time.

WDDL [7]–[12] is a dual-rail pre-charge logic that requires only standard cells and is applicable to traditional CAD flow. WDDL couples a complementary cell to every original cell and guarantees at least one of the cells switches every cycle. E.g., AND cells are paired with OR cells. However, this approach incurs over 2x area and energy overheads; nonetheless, WDDL does not suppress DP well as shown in the next section.

Fig. 3 shows the timing of WDDL pre-charge step and generation [11]. When the clk is 1, the pre-charge wave of 0 traverses the combinational circuit connected to the pre-charge register in Fig. 3. Therefore, all meaningful switchings start from 0, and one of the primary or complementary cells switches at the evaluation time (when the clk is 0). As a result, a 100% switching factor is guaranteed.

The most recent work by Tanimura et al. [22] examined the selective insertion of complementary cells that maintains WDDL level attack resistivity while simultaneously lowering the area and energy overheads. Although this approach incurs lower overheads, it still leaks the power information, just as WDDL does.

IV. Homogeneous Dual-Rail Logic

Homogeneous Dual-Rail Logic (HDRL) wisely combines VSS current waves and suppresses the DP curves. Theoretically, HDRL is able to force DP to be 0 with the hypothesis that the inputs to a cell are hardly distinguishable by observing its VSS. HDRL does not require the pre-charge step and there is no delay overhead. One can implement HDRL using the same cells for both the primary and complementary cells.

A. HDRL AND Exemplar

Fig. 4 (a), (b), and (c) show how to organize Normal, WDDL, and HDRL AND cells, as exemplars. The Normal AND cell has two inputs: x and y, and the WDDL and HDRL AND cells have four inputs: x, x_, y, and y_. x_ and y_ are negations of inputs x and y, respectively. The complementary cell of WDDL is an OR cell. In contrast, the complementary cell of HDRL is the same as the primary (AND) cell. All Fig. 4 (a), (b), and (c) have VSS, and the primary and complementary cells of Fig. 4 (b) and (c) share the same VSS. Note that HDRL does not always have to take negation of primary inputs. The detailed input value conditions to the complementary cells will be presented in the next subsection (Proposition 1).

TABLE I shows the tools we use throughout this paper to validate our approach. The target hardware design files are described in Verilog gate-level netlists. NanoSim measures the VSS current, and the time resolution is 10ps. The VDD is 1.2V.

TABLE I
Experimental Tools

Current Measurement Tool	Synopsys NanoSim C-2009.06
Plotting Tool	Synopsys CosmosScope C-2009.06-SP1
Standard Cell Library	Synopsys SAED_EDK 90nm

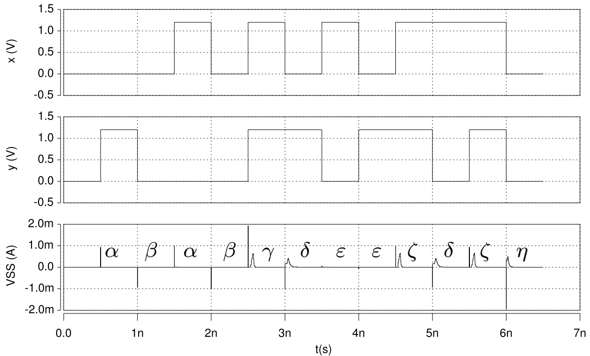

Fig. 5. VSS Current of an AND Cell

Fig. 5 shows VSS current of the Normal AND of Fig. 4 (a). The top two charts are the voltages of x and y. These inputs are comprised of all xy switching combinations. The bottom chart represents the VSS current. Fig. 5 shows that the VSS current flows only when inputs are switching, which is a feature of CMOS. Furthermore, we can label and categorize the each VSS current shape. For example, there are approximately the same VSS current shapes at 0.5ns and 1.5ns, and let us label them α. α is defined as the VSS current when either x or y is switching from 0 to 1; i.e., {(x:0→0, y:0→1) or (x:0→1, y:0→0)}. Note that the c-load difference of the inputs, x and y, are ignorably small due to the symmetry of the AND cell inputs (equally drive two n- and p-mos transistors).

Let us define all the VSS current wave labels as follows.

$$\begin{array}{lll} \alpha & \text{when} & \{(\mathtt{x}:0 \rightarrow 0, \mathtt{y}:0 \rightarrow 1), (\mathtt{x}:0 \rightarrow 1, \mathtt{y}:0 \rightarrow 0)\} \end{array} \quad (8)$$

$$\begin{array}{lll} \beta & \text{when} & \{(\mathtt{x}:0 \rightarrow 0, \mathtt{y}:1 \rightarrow 0), (\mathtt{x}:1 \rightarrow 0, \mathtt{y}:0 \rightarrow 0)\} \end{array} \quad (9)$$

$$\begin{array}{lll} \gamma & \text{when} & \{(\mathtt{x}:0 \rightarrow 1, \mathtt{y}:0 \rightarrow 1)\} \end{array} \quad (10)$$

$$\begin{array}{lll} \delta & \text{when} & \{(\mathtt{x}:1 \rightarrow 1, \mathtt{y}:1 \rightarrow 0), (\mathtt{x}:1 \rightarrow 0, \mathtt{y}:1 \rightarrow 1)\} \end{array} \quad (11)$$

$$\begin{array}{lll} \varepsilon & \text{when} & \{(\mathtt{x}:0 \rightarrow 1, \mathtt{y}:1 \rightarrow 0), (\mathtt{x}:1 \rightarrow 0, \mathtt{y}:0 \rightarrow 1)\} \end{array} \quad (12)$$

$$\begin{array}{lll} \zeta & \text{when} & \{(\mathtt{x}:1 \rightarrow 1, \mathtt{y}:0 \rightarrow 1), (\mathtt{x}:0 \rightarrow 1, \mathtt{y}:1 \rightarrow 1)\} \end{array} \quad (13)$$

$$\begin{array}{lll} \eta & \text{when} & \{(\mathtt{x}:1 \rightarrow 0, \mathtt{y}:1 \rightarrow 0)\} \end{array} \quad (14)$$

Based on Eqs. (3) and (4), the DP curve of the AND cell is calculated as follows (grouping (x:0,1→0) and (x:0,1→1) VSS current waves into G_0 and G_1, respectively).

$$A_{\mathtt{x}=0} = 1/6(\alpha+\beta+\beta+\delta+\varepsilon+\eta) \quad (15)$$

$$A_{\mathtt{x}=1} = 1/6(\alpha+\gamma+\varepsilon+\zeta+\delta+\zeta) \quad (16)$$

$$\begin{aligned} DP &= |A_{\mathtt{x}=0} - A_{\mathtt{x}=1}| \\ &= 1/6\,|(2\beta+\eta)-(\gamma+2\zeta)| \neq 0 \end{aligned} \quad (17)$$

As Eq. (17) shows, the DP is not equal to zero. This is also true even if we change grouping by x with grouping by y.

Fig. 6 shows the VSS current of the complementary (OR) cell in WDDL AND (Fig. 4 (b)). The input vector and labeling method is the same as Eqs. (8)–(14); however all the current labels have ‘ mark, and $\alpha \neq \alpha$‘.

Fig. 7 shows VSS current of the WDDL AND in Fig. 4 (b). The top four charts are the voltages of x, x_, y, and y_. The bottom chart represents the VSS current. Since WDDL requires all input vectors to be 0 at the pre-charge step, the transitions of x, x_, y, and y_ start always from 0. Hence, there are only four cases of input switching combinations:

$$\{(\mathtt{x}:0 \rightarrow 0, \mathtt{x\_}:0 \rightarrow 1, \mathtt{y}:0 \rightarrow 0, \mathtt{y\_}:0 \rightarrow 1)\} \quad (18)$$

$$\{(\mathtt{x}:0 \rightarrow 0, \mathtt{x\_}:0 \rightarrow 1, \mathtt{y}:0 \rightarrow 1, \mathtt{y\_}:0 \rightarrow 0)\} \quad (19)$$

$$\{(\mathtt{x}:0 \rightarrow 1, \mathtt{x\_}:0 \rightarrow 0, \mathtt{y}:0 \rightarrow 0, \mathtt{y\_}:0 \rightarrow 1)\} \quad (20)$$

$$\{(\mathtt{x}:0 \rightarrow 1, \mathtt{x\_}:0 \rightarrow 0, \mathtt{y}:0 \rightarrow 1, \mathtt{y\_}:0 \rightarrow 0)\} \quad (21)$$

All the VSS current waves are defined as combinations of AND cell labels and OR cell labels. The VSS current waves of Eqs. (18)–(21) correspond to the following four equations.

$$\gamma\text{‘} = 0 + \gamma\text{‘} \quad (22)$$

$$\alpha\text{“} = \alpha + \alpha\text{‘} \quad (23)$$

$$\alpha\text{“} = \alpha + \alpha\text{‘} \quad (24)$$

$$\gamma = \gamma + 0 \quad (25)$$

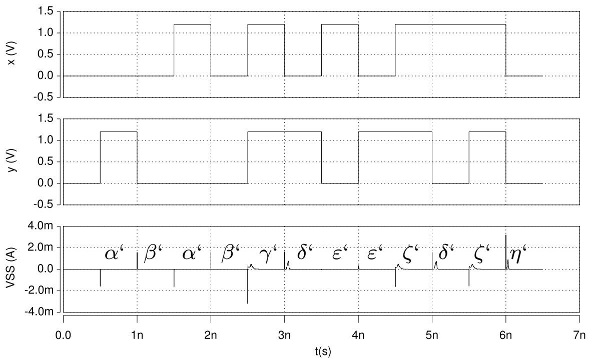

Fig. 6. VSS Current of an OR Cell

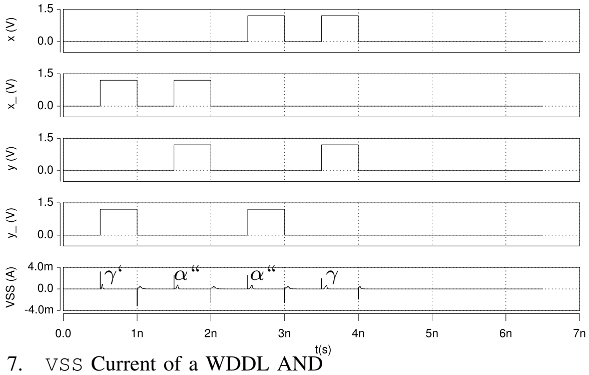

Fig. 7. VSS Current of a WDDL AND

Again, let us calculate the DP curve of the WDDL AND.

$$\begin{aligned} A_{\mathrm{x}=0} &= 1/2(\alpha\text{“} + \gamma\text{‘}) && (26)\\ A_{\mathrm{x}=1} &= 1/2(\alpha\text{“} + \gamma) && (27)\\ DP &= |A_{\mathrm{x}=0} - A_{\mathrm{x}=1}| \\ &= 1/2\,|\gamma\text{‘} - \gamma| \neq 0 && (28) \end{aligned}$$

As Eq. (28) shows, the DP of WDDL is not equal to zero, either.

Let us label all the VSS current waves of the complementary cell in HDRL(Fig. 4 (c)) using $'$ mark. Since we use the same cell for the both primary and complementary cells for HDRL, it is obvious that

$$\alpha = \alpha',\ \beta = \beta',\ \gamma = \gamma',\ \delta = \delta',\ \varepsilon = \varepsilon',\ \zeta = \zeta',\ \eta = \eta' \qquad (29)$$

These equations result in the VSS current waves of HDRL to be defined as combinations of two AND cell labels:

$$\begin{aligned} \alpha'' &= \alpha + \delta' && (30)\\ \beta'' &= \beta + \zeta' && (31)\\ \gamma'' &= \gamma + \eta' && (32)\\ \delta'' &= \delta + \alpha' = \alpha + \delta' = \alpha'' && (33)\\ \varepsilon'' &= \varepsilon + \varepsilon' && (34)\\ \zeta'' &= \zeta + \beta' = \beta + \zeta' = \beta'' && (35)\\ \eta'' &= \eta + \gamma' = \gamma + \eta' = \gamma'' && (36) \end{aligned}$$

Fig. 8 shows VSS current of the HDRL AND in Fig. 4 (c). The top four charts are the voltages of x, x_, y, and y_. The bottom chart represents the VSS current. As Fig. 8 and Eqs. (33), (35), and (36) show, δ'', ζ'', and η'' are interchangeable with α'', β'', and γ'', respectively. Accordingly, the DP curve of the HDRL AND cell become theoretically zero as follows.

$$\begin{aligned} A_{\mathrm{x}=0} &= 1/6(\alpha'' + \beta'' + \beta'' + \delta'' + \varepsilon'' + \eta'') && (37)\\ A_{\mathrm{x}=1} &= 1/6(\alpha'' + \gamma'' + \varepsilon'' + \zeta'' + \delta'' + \zeta'') && (38)\\ DP &= |A_{\mathrm{x}=0} - A_{\mathrm{x}=1}| \\ &= 1/6\left|(2\beta'' + \eta'') - (\gamma'' + 2\zeta'')\right| \\ &= 1/6\left|(2\beta'' + \eta'') - (\eta'' + 2\beta'')\right| = 0 && (39) \end{aligned}$$

The reason why all switching for HDRL are positive is complementing positive current flows are larger than equal to negative flows. Additionally, we are measuring the VSS current. Ideally, VSS should not flow negative current.

We assume evenly distributed conditions between $A_{\mathrm{x}=0}$ and $A_{\mathrm{x}=1}$. If $A_{\mathrm{x}=0}$ and $A_{\mathrm{x}=1}$ do not have evenly distributed conditions, the DP would become false positive/negative sign for all the $k_{est.}$ candidates. For example, if the number of sample power data for $A_{\mathrm{x}=0}$ is too small compared to that of $A_{\mathrm{x}=1}$, $A_{\mathrm{x}=0}$ could be too imprecise on average or distorted by noise from the environment that affects the quality of DP. Therefore, an evenly distributed condition is, in fact, the best condition for the adversaries. Note that our focus is on the first order DPA (i.e. x:0→0 and x:1→0 are treated as x:0, and we cannot distinguish them).

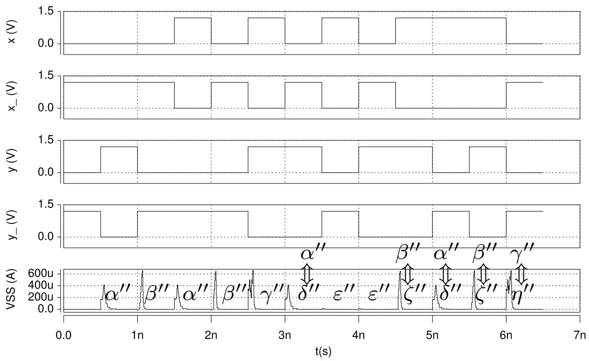

Fig. 8. VSS Current of a HDRL AND

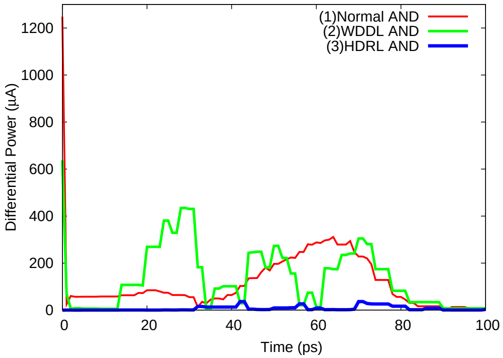

Fig. 9. Comparison of Differential Power Curves between (1) Normal AND (Eq. (17)), (2) WDDL AND (Eq. (28)), (3) HDRL AND (Eq. (39))

Adversaries may intentionally select inputs that causes undistributed conditions between $A_{\mathrm{x}=0}$ and $A_{\mathrm{x}=1}$ and use the intermediate power shape for more simple attacks such as SPA (Simple Power Analysis). In this case, the power shapes of both WDDL and HDRL are dependent on inputs. For example, WDDL consumes γ‘ for (x:0→0, y:0→0), and γ for (x:0→1, y:0→1). There is no guarantee that these two input produces the same power shape.

We cannot directly (theoretically) compare the resistivity of WDDL and HDRL against SPA attacks until we experiment on actual FPGAs/ASICs since the success rate of SPA largely depends on the noise of the environment. In DPA theory, the noise is canceled out so that DPA is considered as a more practical attacking method compared to SPA. We focus on the theoretical analysis of HDRL against DPA attacks in this paper. Further analysis of SPA attacks on HDRL might be an interesting future work.

Switching current of a specific cell can be significant in WDDL. In the manuscript, Figs. 7 and 8 show the switching current of WDDL and HDRL AND, respectively. In Fig. 7, the peak of current reaches $3.3mA$. In contrast, Fig. 8 shows that the peak of current is only $700\mu A$. As those figures show, the switching current of a specific WDDL cell could be more significant than a HDRL cell

Fig. 9 is the simulation result of Eqs. (17), (28), and (39). HDRL AND cell (Eq. (39)) is virtually flat zero (not exactly zero due to the slight c-load difference between x and y), whereas both Normal and WDDL AND cells (Eqs. (17) and (28)) are far from the horizontal axis. We also observed similar results for other cells. The peak of Normal AND is $1248\mu A$ as opposed that of WDDL AND is $637\mu A$. The peak of WDDL AND and Normal AND is at time 0 in Fig. 9 (close enough

TABLE II

TRUTH TABLE OF w AND w_

w			w_		
0	→	0	1	→	1
0	→	1	1	→	0
1	→	0	0	→	1
1	→	1	0	→	0

to time 0), the peak of WDDL AND is smaller than that of Normal AND.

This exemplar shows HDRL suppresses DP better than WDDL. WDDL works well only on the assumption that the primary and complementary cells have an equal amount of VSS current flowing through them, which is not true with most standard cell libraries. HDRL overcomes this problem and, in fact, requires smaller amount of energy overhead (shown in the experimental results).

The zero DP means the input vectors are independent from the DP of the circuit. In contrast, the non-zero DP means there is a dependency between the input and power consumption. In the later case, DPA theoretically would find the dependency of input data on power consumption eventually with adequate power sampling data.

In fact, there are slight dependencies between input vectors and the DP for wrong $k_{est.}$, but DPA considers this small dependencies as zero (because the DP for the correct Key becomes notably high without countermeasures). HDRL does not guarantee that the DP is zero for wrong $k_{est.}$ keys. HDRL guarantees the zero DP only for the correct Key. Therefore, there may be small dependencies between the input and power consumption for wrong $k_{est.}$ keys.

Besides, in crypto-hardware, the surrounding circuit (e.g. there are >=16 S-Boxes in AES) consumes power at the same time. Even though the real inputs become independent from the DP (zero DP) with the HDRL technique, the surrounding power consumption make the FALSE DP.

From the adversaries' point of view, they cannot tell whether it is the real DP (input dependent) or false DP (input independent but looks like dependent) from the amount of the DP. The purpose of having zero DP consumption is to delete the dependency of inputs on power consumption, not for changing the key ranks even though the rank of correct Key becomes lower as a corresponding result. What we can achieve with HDRL is to make the DP independent from the inputs. The drawback of WDDL is it cannot guarantee the zero DP, meaning the dependency is still there.

B. Generalized HDRL

Beyond a single AND gate example, we will show that HDRL still theoretically guarantees fully balanced power consumption for arbitrary combinational circuit. The following Propositions 1–3 guarantee that one can simply duplicate an original circuit so as to make a complementary circuit of HDRL.

Proposition 1: The sufficient conditions that w_ is the input of the corresponding complementary cell to a primary cell with an input w are that Pr(w=1)=Pr(w_=1) , where Pr stands for probability, and w and w_ have **neither** concurrent {(w:0→1, w_:0→1) **nor** (w:1→0, w_:1→0)} switches.

Proof: Suppose a HDRL AND such as Fig. 4 (c) whose inputs satisfy Proposition 1 but $DP \neq 0$. This supposition contradicts Eq. (39). Thus, Proposition 1 is true. ■

Note negations of primary circuit inputs satisfy Proposition 1. TABLE II shows the truth table of w and w_ that covers all possible combinations of switching for HDRL. In TABLE II, w_ is a negation of w. Since w and w_ are Pr(w=1)=Pr(w_=1) and have neither concurrent {(w:0→1, w_:0→1) **nor** (w:1→0, w_:1→0)} switches, w and w_ satisfy the Proposition 1. The reason why we used negations of primary circuit inputs is that they are easily generated. HDRL complementary circuit inputs do not have to be negations of primary circuit inputs, but have to satisfy Proposition 1.

TABLE III

TRUTH TABLE OF HDRL AND, OR, AND NOT CELL

x	y	AND(x,y)	OR(x,y)	NOT(x)	x′	y′	AND(x′,y′)	OR(x′,y′)	NOT(x′)
0→0	0→0	0 →0	0 →0	1 →1	1→1	1→1	1 →1	1 →1	0 →0
0→0	0→1	0 →0	0 →1	1 →1	1→1	1→0	1 →0	1 →1	0 →0
0→0	1→0	0 →0	1 →0	1 →1	1→1	0→1	0 →1	1 →1	0 →0
0→0	1→1	0 →0	1 →1	1 →1	1→1	0→0	0 →0	1 →1	0 →0
0→1	0→0	0 →0	0 →1	1 →0	1→0	1→1	1 →0	1 →1	0 →1
0→1	0→1	0 →1	0 →1	1 →0	1→0	1→0	1 →0	1 →0	0 →1
0→1	1→0	0 →0	1 →1	1 →0	1→0	0→1	0 →0	1 →1	0 →1
0→1	1→1	0 →1	1 →1	1 →0	1→0	0→0	0 →0	1 →0	0 →1
1→0	0→0	0 →0	1 →0	0 →1	0→1	1→1	0 →1	1 →1	1 →0
1→0	0→1	0 →0	1 →1	0 →1	0→1	1→0	0 →0	1 →1	1 →0
1→0	1→0	1 →0	1 →0	0 →1	0→1	0→1	0 →1	0 →1	1 →0
1→0	1→1	1 →0	1 →1	0 →1	0→1	0→0	0 →0	0 →1	1 →0
1→1	0→0	0 →0	1 →1	0 →0	0→0	1→1	0 →0	1 →1	1 →1
1→1	0→1	0 →1	1 →1	0 →0	0→0	1→0	0 →0	1 →0	1 →1
1→1	1→0	1 →0	1 →1	0 →0	0→0	0→1	0 →0	0 →1	1 →1
1→1	1→1	1 →1	1 →1	0 →0	0→0	0→0	0 →0	0 →0	1 →1

Proposition 2: The primary and complementary outputs from a HDRL cell satisfy Proposition 1 if the inputs of the HDRL cell also satisfy Proposition 1.

Proof: AND, OR, and NOT cells satisfy Proposition 2 by definition. Thus, Proposition 2 is true for all logic cells. ■

TABLE III shows the truth table of HDRL AND, OR, and NOT cell. {x′ y′} are the negations of {x y}. Thus, the combinations of {x y} and {x′ y′} satisfy Proposition 1. Indeed, TABLE III shows that the output combinations of {AND(x,y) OR(x,y) NOT(x)} and {AND(x′,y′) OR(x′,y′) NOT(x′)} also satisfy Proposition 1. Thus, the descendant of HDRL cells become also HDRL cells. Even though we feed negation of primary inputs into the complementary cells, the outputs from the complementary cells are not negation of primary inputs, but descendant cells still work as HDRL.

Proposition 3: A chain of cells works as a complementary circuit if this circuit is a duplication of the primary circuit, and if the inputs of these circuits satisfy Proposition 1.

Proof: Since Propositions 1 and 2 are true, Proposition 3 is true. ■

Since all combinational logic can be converted into logic that comprise only AND, OR, NOT cells, any combination of those cells becomes a complementary circuit. Therefore, Propositions 1–3 guarantee that one can simply duplicate an original circuit so as to make a complementary circuit. Refer to the Appendix for further examples of how HDRL works with multiple cells.

C. HDRL Design Flow

In HDRL, one can duplicate the original circuit, and the duplicated circuit works as complementary cells(by sharing the same VSS, VDD). First, we take an original circuit and conduct place and route. Second, we duplicate the design and put it next to the original circuit. By feeding negation of the input data to the duplicated circuit from outside, the duplicated circuit works as complementary cells. This method also duplicates the wire delay and capacitance that brings even better power balancing. Furthermore, complementary cells are isolated from original cells so that there is no delay overhead.

WDDL may slow down the clock speed up to 2x in order to wait for the entire circuit to be pre-charged to 0. HDRL, in contrast, does not require such a pre-charge step. Moreover, WDDL forbids the use of Inverter cells [10], and it may require the modification of the original circuit and additional delay penalty. HDRL does not have such restrictions, and a designer does not have to modify the original circuit at all.

Once the wire delay is duplicated, HDRL can complement glitches without the pre-charge stage. We explain this with the following example.

Assume the signal to the input y delays $\Delta T_{x:0\rightarrow1,y:1\rightarrow0}$ compared to x in Fig. 4 (c) when (x:0→1, y:1→0) because of different signal arrival times. At this moment, a glitch that has $\Delta T_{x:0\rightarrow1,y:1\rightarrow0}$ width comes out from the output z.

Following the definition of Eq. (12), let ε_g be the label for the power consumption curve of the original AND gate for this switching including the whole glitching period. At this time,

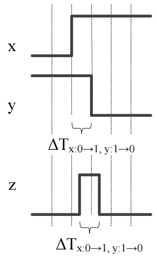
x
y
$\Delta T_{x:0\rightarrow1,\ y:1\rightarrow0}$
z
$\Delta T_{x:0\rightarrow1,\ y:1\rightarrow0}$

Fig. 10. Glitch Example for an AND Gate

the signal to the input y_ (to the complementary AND gate) also delays $\Delta T_{x:0\rightarrow 1,y:1\rightarrow 0}$ compared to x_ due to the HDRL circuit duplication. Again, let ε'_g be the label for the power consumption curve of the complementary AND gate for this switching with the glitch, following the definition of Eq. (12).

Similar to Eq. (34), which is one of the HDRL gate power shape definitions let $\varepsilon''_g = \varepsilon_g + \varepsilon'_g$ be the label for the power consumption curve of the HDRL (original + complementary) AND gate for this switching with the glitch. Replacing ε'' with ε''_g in Eqs. (37) and (38) calculates the differential power with this glitch, and the differential power still becomes zero as before. And, the new equations are

$$\begin{aligned} A_{\mathrm{x}=0} &= 1/6(\alpha'' + \beta'' + \beta'' + \delta'' + \varepsilon''_g + \eta'') && (40)\\ A_{\mathrm{x}=1} &= 1/6(\alpha'' + \gamma'' + \varepsilon''_g + \zeta'' + \delta'' + \zeta'') && (41)\\ DP &= |A_{\mathrm{x}=0} - A_{\mathrm{x}=1}| \\ &= 1/6\left|(2\beta'' + \eta'') - (\gamma'' + 2\zeta'')\right| \\ &= 1/6\left|(2\beta'' + \eta'') - (\eta'' + 2\beta'')\right| = 0 && (42) \end{aligned}$$

Note that this differential power equation becomes zero even if we add more or different glitch cases.

From this observation, glitches occurred in the original circuit are complemented with those occurred in the complementary circuit with large number of probing samples. Therefore, as long as the complementary circuit has the same placement and routing as the original circuit, HDRL can overall complement glitches.

Note that since we are targeting ASIC designs in this paper (experiments are based on a standard cell library) and an AES S-box requires only 150-200 gates (without countermeasures), it is possible to get the same wire length for both original and complementary circuit.

The actual wiring delay is not included in the design used for the experiments; however, the NanoSim (fast-SPICE) and the standard library contains the gate delay information that simulates glitches caused by the different number of gates that the signal has passed through. Therefore, the experimental (simulation) results shown in this paper do cover the cases with glitches, which demonstrate that HDRL indeed does complement glitches. Even though the wire delay is taken into account, the zero differential power will be maintained considering the above discussion.

Thus, HDRL is able to complement the glitches without the pre-charge step as long as the both original and complementary circuit have the same glitch characteristics (this should be true since the complementary circuit is the duplication of the original circuit in HDRL). On the contrary, WDDL has different glitch characteristics in the original and complementary circuit, since WDDL uses different cells for the complementary circuit from the original circuit. In HDRL, glitches will be complemented in the same manner that the regular power signatures are complemented.

Different glitching may still occur in the added complementary circuit in HDRL due to the process variations. However the same thing also could happen to WDDL, and the impact of process variations to HDRL is another interesting research topic; however, we focus on the theoretical analysis of HDRL in this paper.

We can consider two methods to feed negated inputs. The first method is use QN (negation of output Q) output from a D flip-flop. Since D flip-flop has symmetric structure on Q and QN, the timing of Q and QN are supposed to be the same. The other solution is use different flip-flops for original circuit and complementary circuit. Only for the first time, we need to feed the negated inputs from input pins to the flip-flops. After a AES round, the result of original circuit will be stored in the flip-flops in the original circuit, and the result of the complementary circuit will be stored in the flip-flops in the complementary circuit. In this way, both the original circuit and complementary circuit can keep the balanced load and wire delay.

TABLE IV
RANKS OF CORRECT Key = 0X13 WITH 4096 INPUTS

	Eq. (5)								Eq. (6)
	i=0	i=1	i=2	i=3	i=4	i=5	i=6	i=7	
Normal	94	1	120	76	4	16	1	1	1
WDDL	26	1	47	161	15	232	1	112	3
HDRL	**141**	**9**	**148**	**213**	**232**	**230**	**109**	**165**	**158**

TABLE V
RANKS OF CORRECT Key = 0X13 WITH 16384 INPUTS

	Eq. (5)								Eq. (6)
	i=0	i=1	i=2	i=3	i=4	i=5	i=6	i=7	
Normal	15	1	1	1	1	1	1	1	1
WDDL	1	1	103	129	6	218	1	256	2
HDRL	**208**	**114**	**237**	**145**	**170**	**13**	**205**	**185**	**172**

V. EXPERIMENTAL RESULTS

A. Experimental Setup

This section evaluates the DPA attack resistivity of AES S-Boxes. There are three target S-Box designs: "Normal" without countermeasures, "WDDL" pairing each cell with a different complementary cell, and "HDRL" pairing each cell with a same complementary cell. The same tool and setup are used as the previous section. The differential power on each gate may cancel out. Therefore, we conducted experiments using S-Boxes.

B. Comparison in DPA Attack Resistivity

We measured the VSS current of all 16 S-Boxes in the AES circuit of Round 10 (the last cycle) since CipherText at Round 10 is visible from outside of the circuit. We collected 4096 and 16384 VSS current samples to observe how the ranks of the correct Key vary. Those inputs are randomly generated 128-bit numbers and injected from PlainText of Fig. 1. Key is fixed at **0x13**.

TABLEs IV and V summarize the ranks of the correct Key amongst all $k_{est.}$ for all the groupings with 4096 and 16384 inputs, respectively, for attacking one of the 16 S-Boxes. The higher (smaller) rank, the larger DP. The rank of the correct Key hints the adversaries which $k_{est.}$ they should attempt. If the rank of the $k_{est.}$ is always 1 (or constantly ranked at a particular position), there is a higher chance that the $k_{est.}$ is the correct Key by the definition of DPA. Comparison between TABLEs IV and V show that the ranks of HDRL vary. For example, the rank of the grouping i=1 becomes higher when there are 4096 inputs than 16384 inputs. In contrast, the rank of the grouping i=5 becomes lower. Hence, adversaries are unable to confidently assume that what $k_{est.}$ (highly or lowly ranked) is the correct Key. The ranks of WDDL with the groupings i=1,6 are the same even though the number of input changes. In such cases, adversaries have more confidence that they only need to check the highest ranked $k_{est.}$ to find the correct Key. Accordingly, HDRL is more secure than WDDL.

In order to show that HDRL functions well for another key, we conducted the same experiment with correct Key = **0x7F** and attacked a different S-Box from the previous experiment. TABLEs VI and VII shows the ranks of correct Key, and the ranks of correct HDRL Key are more divergent than that of WDDL (the correct key of i=0 in both 4096 and 16384

TABLE VI
RANKS OF CORRECT Key = 0X7F WITH 4096 INPUTS

	Eq. (5)								Eq. (6)
	i=0	i=1	i=2	i=3	i=4	i=5	i=6	i=7	
Normal	46	1	24	96	11	13	67	1	1
WDDL	1	128	214	250	5	172	108	180	142
HDRL	**254**	**15**	**84**	**14**	**252**	**104**	**190**	**49**	**25**

TABLE VII
RANKS OF CORRECT Key = 0X7F WITH 16384 INPUTS

	Eq. (5)								Eq. (6)
	i=0	i=1	i=2	i=3	i=4	i=5	i=6	i=7	
Normal	1	1	1	1	1	1	1	1	1
WDDL	1	1	25	243	4	209	66	122	4
HDRL	**199**	**85**	**89**	**73**	**255**	**252**	**112**	**232**	**224**

cases for WDDL is ranked 1). Thus, the security advantage of HDRL is still the same for the different key, and we observed similar results for other keys as well.

C. Comparison in Overheads

TABLE VIII is the comparison in area and energy consumption, and it shows that HDRL can be implemented incurring significantly smaller energy overhead than WDDL. The power overhead of the WDDL complementary cells alone is 65.85% (not 100%) since the complementary cells are not switching while the primary cells are switching. However, since WDDL requires the pre-charge steps causing twice switching frequency, the total energy overhead becomes $165.85 \times 2 - 100 = 231.7\%$. In contrast, HDRL requires only 100% energy overhead. Since WDDL uses different cells for the complementary circuit from the original circuit, the area and energy might slightly vary for different examples; however, the result of HDRL is not dependent on the example. The area overheads of HDRL and WDDL are almost the same. Note HDRL has no delay overhead since it does not modify the original circuit.

In summary, our experimental results demonstrate that HDRL successfully repels the DPA attacks and achieves higher security with smaller energy overhead compared to WDDL. HDRL gives hardware designers more advantages in energy and design cost (easy to incorporate) with no delay overhead.

VI. CONCLUSIONS

This paper proposed HDRL for DPA attack resistive secure hardware design. Using the AES S-Box circuit as an exemplar, we observed that HDRL successfully repelled DPA attacks with 100% energy overhead while WDDL incurs 231.7% energy overhead. In addition, HDRL requires no delay overhead and similar area overhead as WDDL. HDRL is a promising approach applicable to any standard cell-based crypto-LSI.

APPENDIX

TABLE IX shows the truth table of two HDRL AND cells circuit depicted in Fig. 11. The right most column in the TABLE IX represents the power consumption of the HDRL AND cells denoted as (3) and (4) in Fig. 11. Similar to Eqs. (37), and (38),

$$\begin{aligned} A_{\mathtt{x}=0} &= 1/6(6\alpha + 6\alpha' + 8\beta + 4\beta' + 3\gamma' \\ &\quad +2\delta + 2\delta' + 2\varepsilon + 4\varepsilon' + 4\zeta' + 2\eta + \eta') \qquad (43) \\ A_{\mathtt{x}=1} &= 1/6(6\alpha + 6\alpha' + 4\beta + 8\beta' + 3\gamma \\ &\quad +2\delta + 2\delta' + 4\varepsilon + 2\varepsilon' + 4\zeta + \eta + 2\eta') \qquad (44) \end{aligned}$$

Based on Eqs. (29), and (39),

$$\begin{aligned} DP &= |A_{\mathtt{x}=0} - A_{\mathtt{x}=1}| \\ &= 0 \qquad (45) \end{aligned}$$

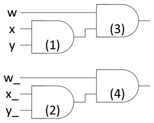

Fig. 11. Two HDRL AND Cells Circuit Exemplar

TABLE VIII
COMPARISON IN AREA AND ENERGY CONSUMPTION

	Area	Energy
Normal	100.0%	100.0%
WDDL	200.3%	331.7%
HDRL	200.0%	200.0%

*Normalized by the Normal S-Box

TABLE IX
TRUTH TABLE OF TWO HDRL AND CELLS CIRCUIT

x	y	AND(x,y)	w	x_	y_	AND(x_,y_)	w_	(3) + (4) Power Consumption
0→0	0→0	0→0	0→0	1→1	1→1	1→1	1→1	$0 + 0$
0→0	0→0	0→0	0→1	1→1	1→1	1→1	1→0	$\alpha + \delta'$
0→0	0→0	0→0	1→0	1→1	1→1	1→1	0→1	$\beta + \zeta'$
0→0	0→0	0→0	1→1	1→1	1→1	1→1	0→0	$0 + 0$
0→0	0→1	0→0	0→0	1→1	1→0	1→0	1→1	$0 + \delta'$
0→0	0→1	0→0	0→1	1→1	1→0	1→0	1→0	$\alpha + \eta'$
0→0	0→1	0→0	1→0	1→1	1→0	1→0	0→1	$\beta + \varepsilon'$
0→0	0→1	0→0	1→1	1→1	1→0	1→0	0→0	$0 + \beta'$
0→0	1→0	0→0	0→0	1→1	0→1	0→1	1→1	$0 + \zeta'$
0→0	1→0	0→0	0→1	1→1	0→1	0→1	1→0	$\alpha + \varepsilon'$
0→0	1→0	0→0	1→0	1→1	0→1	0→1	0→1	$\beta + \gamma'$
0→0	1→0	0→0	1→1	1→1	0→1	0→1	0→0	$0 + \alpha'$
0→0	1→1	0→0	0→0	1→1	0→0	0→0	1→1	$0 + 0$
0→0	1→1	0→0	0→1	1→1	0→0	0→0	1→0	$\alpha + \beta'$
0→0	1→1	0→0	1→0	1→1	0→0	0→0	0→1	$\beta + \alpha'$
0→0	1→1	0→0	1→1	1→1	0→0	0→0	0→0	$0 + 0$
0→1	0→0	0→0	0→0	1→0	1→1	1→0	1→1	$0 + \delta'$
0→1	0→0	0→0	0→1	1→0	1→1	1→0	1→0	$\alpha + \eta'$
0→1	0→0	0→0	1→0	1→0	1→1	1→0	0→1	$\beta + \varepsilon'$
0→1	0→0	0→0	1→1	1→0	1→1	1→0	0→0	$0 + \beta'$
0→1	0→1	0→1	0→0	1→0	1→0	1→0	1→1	$\alpha + \delta'$
0→1	0→1	0→1	0→1	1→0	1→0	1→0	1→0	$\gamma + \eta'$
0→1	0→1	0→1	1→0	1→0	1→0	1→0	0→1	$\varepsilon + \varepsilon'$
0→1	0→1	0→1	1→1	1→0	1→0	1→0	0→0	$\zeta + \beta'$
0→1	1→0	0→0	0→0	1→0	0→1	0→0	1→1	$0 + 0$
0→1	1→0	0→0	0→1	1→0	0→1	0→0	1→0	$\alpha + \beta'$
0→1	1→0	0→0	1→0	1→0	0→1	0→0	0→1	$\beta + \alpha'$
0→1	1→0	0→0	1→1	1→0	0→1	0→0	0→0	$0 + 0$
0→1	1→1	0→1	0→0	1→0	0→0	0→0	1→1	$\alpha + 0$
0→1	1→1	0→1	0→1	1→0	0→0	0→0	1→0	$\gamma + \beta'$
0→1	1→1	0→1	1→0	1→0	0→0	0→0	0→1	$\varepsilon + \alpha'$
0→1	1→1	0→1	1→1	1→0	0→0	0→0	0→0	$\zeta + 0$
1→0	0→0	0→0	0→0	0→1	1→1	0→1	1→1	$0 + \zeta'$
1→0	0→0	0→0	0→1	0→1	1→1	0→1	1→0	$\alpha + \varepsilon'$
1→0	0→0	0→0	1→0	0→1	1→1	0→1	0→1	$\beta + \gamma'$
1→0	0→0	0→0	1→1	0→1	1→1	0→1	0→0	$0 + \alpha'$
1→0	0→1	0→0	0→0	0→1	1→0	0→0	1→1	$0 + 0$
1→0	0→1	0→0	0→1	0→1	1→0	0→0	1→0	$\alpha + \beta'$
1→0	0→1	0→0	1→0	0→1	1→0	0→0	0→1	$\beta + \alpha'$
1→0	0→1	0→0	1→1	0→1	1→0	0→0	0→0	$0 + 0$
1→0	1→0	1→0	0→0	0→1	0→1	0→1	1→1	$\beta + \zeta'$
1→0	1→0	1→0	0→1	0→1	0→1	0→1	1→0	$\varepsilon + \varepsilon'$
1→0	1→0	1→0	1→0	0→1	0→1	0→1	0→1	$\eta + \gamma'$
1→0	1→0	1→0	1→1	0→1	0→1	0→1	0→0	$\delta + \alpha'$
1→0	1→1	1→0	0→0	0→1	0→0	0→0	1→1	$\beta + 0$
1→0	1→1	1→0	0→1	0→1	0→0	0→0	1→0	$\varepsilon + \beta'$
1→0	1→1	1→0	1→0	0→1	0→0	0→0	0→1	$\eta + \alpha'$
1→0	1→1	1→0	1→1	0→1	0→0	0→0	0→0	$\delta + 0$
1→1	0→0	0→0	0→0	0→0	1→1	0→0	1→1	$0 + 0$
1→1	0→0	0→0	0→1	0→0	1→1	0→0	1→0	$\alpha + \beta'$
1→1	0→0	0→0	1→0	0→0	1→1	0→0	0→1	$\beta + \alpha'$
1→1	0→0	0→0	1→1	0→0	1→1	0→0	0→0	$0 + 0$
1→1	0→1	0→1	0→0	0→0	1→0	0→0	1→1	$\alpha + 0$
1→1	0→1	0→1	0→1	0→0	1→0	0→0	1→0	$\gamma + \beta'$
1→1	0→1	0→1	1→0	0→0	1→0	0→0	0→1	$\varepsilon + \alpha'$
1→1	0→1	0→1	1→1	0→0	1→0	0→0	0→0	$\zeta + 0$
1→1	1→0	1→0	0→0	0→0	0→1	0→0	1→1	$\beta + 0$
1→1	1→0	1→0	0→1	0→0	0→1	0→0	1→0	$\varepsilon + \beta'$
1→1	1→0	1→0	1→0	0→0	0→1	0→0	0→1	$\eta + \alpha'$
1→1	1→0	1→0	1→1	0→0	0→1	0→0	0→0	$\delta + 0$
1→1	1→1	1→1	0→0	0→0	0→0	0→0	1→1	$0 + 0$
1→1	1→1	1→1	0→1	0→0	0→0	0→0	1→0	$\zeta + \beta'$
1→1	1→1	1→1	1→0	0→0	0→0	0→0	0→1	$\delta + \alpha'$
1→1	1→1	1→1	1→1	0→0	0→0	0→0	0→0	$0 + 0$

Thus, the DP is still zero for multiple cells. From this observation, HDRL with more than one cell (larger functional blocks) indeed complements DP, and this result supports the Proposition 2.

For more intuitive explanation, scan the AND(x,y) column from the top and the AND(x_,y_) column from the bottom in TABLE IX. The sequences of AND(x,y) from the top and AND(x_,y_) from the bottom are the same. Similarly, scan the w and w_ columns from the top and bottom, respectively. The sequences of those columns are the same, too. From this observation, it follows that the probabilities of signal transitions for the original and complementary circuits are the same assuming large number of plain text inputs by adversaries. Therefore, the zero DP is true for other larger circuits.

ACKNOWLEDGMENT

The authors thank Dr. Morioka, NEC Lab. for his courtesy in providing the composite field AES S-Box Verilog code. This work is supported by the Yoshida Scholarship Foundation.

REFERENCES

[1] P. C. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proc. CRYPTO*, 1999, pp. 388–397.

[2] J. Ambrose, R. Ragel, and S. Parameswaran, “Rijid: Random code injection to mask power analysis based side channel attacks,” in *Proc. DAC*, Jun. 2007, pp. 489–492.

[3] J. D. Golic and C. Tymen, “Multiplicative masking and power analysis of AES,” in *Proc. CHES*, 2003, pp. 198–212.

[4] M.-L. Akkar and C. Giraud, “An implementation of DES and AES, secure against some attacks,” in *Proc. CHES*, 2001, pp. 309–318.

[5] C. Gebotys, “A table masking countermeasure for low-energy secure embedded systems,” *IEEE Trans. VLSI Syst.*, vol. 14, no. 7, pp. 740–753, Jul. 2006.

[6] J.-S. Coron and L. Goubin, “On boolean and arithmetic masking against differential power analysis,” in *Proc. CHES*, 2000, pp. 231–237.

[7] K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, “A side-channel leakage free coprocessor IC in 0.18um CMOS for embedded AES-based cryptographic and biometric processing,” in *Proc. DAC*, Jun. 2005, pp. 222–227.

[8] ——, “Prototype ic with wddl and differential routing - DPA resistance assessment,” in *Proc. CHES*, 2005, pp. 354–365.

[9] I. Verbauwhede, K. Tiri, D. Hwang, and P. Schaumonr, “Circuits and design techniques for secure ICs resistant to side-channel attacks,” in *Proc. ICICDT*, 2006, pp. 1–4.

[10] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation,” in *Proc. DATE*, vol. 1, Feb. 2004, pp. 246–251 Vol.1.

[11] ——, “A digital design flow for secure integrated circuits,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 25, no. 7, pp. 1197–1208, Jul. 2006.

[12] ——, “A vlsi design flow for secure side-channel attack resistant ICs,” in *Proc. DATE*, vol. 3, Mar. 2005, pp. 58–63.

[13] ——, “Design method for constant power consumption of differential logic circuits,” in *Proc. DATE*, 2005, pp. 628–633.

[14] ——, “Securing encryption algorithms against DPA at the logic level: Next generation smart card technology,” in *Proc. CHES*, 2003, pp. 125–136.

[15] ——, “Charge recycling sense amplifier based logic: securing low power security ICs against DPA,” in *Proc. ESSCIRC*, Sept. 2004, pp. 179–182.

[16] 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 *Proc. ESSCIRC*, Sept. 2002, pp. 403–406.

[17] M. Khatir, A. Moradi, A. Ejlali, M. T. M. Shalmani, and M. Salmasizadeh, “A secure and low-energy logic style using charge recovery approach,” in *Proc. ISLPED*, 2008, pp. 259–264.

[18] S. Guilley, P. Hoogvorst, Y. Mathieu, R. Pacalet, and J. Provost, “CMOS structures suitable for secured hardware,” in *Proc. DATE*, 2004, pp. 1414–1415.

[19] P. Schaumont and K. Tiri, “Masking and dual-rail logic don’t add up,” in *Proc. CHES*, 2007, pp. 95–106.

[20] T. Popp and S. Mangard, “Masked dual-rail pre-charge logic: DPA-resistance without routing constraints,” in *Proc. CHES*, 2005, pp. 172–186.

[21] M. Saeki, D. Suzuki, K. Shimizu, and A. Satoh, “A design methodology for a DPA-resistant cryptographic LSI with RSL techniques,” in *Proc. CHES*, 2009, pp. 189–204.

[22] K. Tanimura and N. Dutt, “ExCCel: Exploration of complementary cells for efficient DPA attack resistivity,” in *HOST*, Jun. 2010, pp. 52–55.

[23] T. Sugawara, N. Homma, T. Aoki, and A. Satoh, “Differential power analysis of AES ASIC implementations with various S-box circuits,” in *Proc. ECCTD*, Aug. 2009, pp. 395–398.

[24] S. Morioka and A. Satoh, “An optimized S-Box circuit architecture for low power AES design,” in *Proc. CHES*, 2002, pp. 172–186.

[25] P. Yu and P. Schaumont, “Secure FPGA circuits using controlled placement and routing,” in *Proc. CODES+ISSS*, 2007, pp. 45–50.

[26] A. K. Zadeh and C. H. Gebotys, “Side channel aware leakage management in nanoscale cryptosystem-on-chip (coc),” in *Proc. ISQED*, 2009, pp. 230–235.

[27] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Investigations of power analysis attacks on smartcards,” in *Proc. USENIX Workshop on Smartcard Technology*, 1999, p. 17.