Title	Security analysis of asynchronous-logic QDI cell approach for differential power analysis attack(Main Article)
Author(s)	Ho, Weng-Geng; Pammu, Ali Akbar; Liu, Nan; Ne, Kyaw Zwa Lwin; Chong, Kwen-Siong; Gwee, Bah Hwee
Citation	Ho, W.-G., Pammu, A. A., Liu, N., Ne, K. Z. L., Chong, K.-S., & Gwee, B. H. (2016). Security analysis of asynchronous-logic QDI cell approach for differential power analysis attack. 2016 International Symposium on Integrated Circuits (ISIC).
Date	2016
URL	http://hdl.handle.net/10220/42164
Rights	

Security Analysis of Asynchronous-Logic QDI Cell Approach for Differential Power Analysis Attack

Weng-Geng Ho*, Ali Akbar Pammu, Nan Liu, Kyaw Zwa Lwin Ne, Kwen-Siong Chong and Bah-Hwee Gwee
School of Electrical and Eletronic Engineering,
Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798
Email: *wgho@ntu.edu.sg

***Abstract*—We report a security analysis of the asynchronous-logic (async) quasi-delay-insensitive (QDI) Weak-Conditioned Half-Buffer (WCHB) cell approach against the side-channel differential power analysis (DPA) attack. When compared to the synchronous-logic (sync) standard cell approach, the WCHB cell approach is more power-balanced during the logic switching due to the unique features as follows. First, the WCHB cell approach embodies dual-rail data-encoding scheme, featuring more balanced power dissipation for different output transitions. Second, the WCHB cell approach embodies a power-constant input detector that validate the input-completeness, featuring more balanced power dissipation for different input combination. Based on 65nm CMOS process, the standard and WCHB cell approaches are simulated for 7 library cells, and compared in terms of the normalized energy deviation (NED) and normalized standard deviation (NSD). Nonetheless, the WCHB cell approach features 62% lower NED and 69% lower NSD than the standard cell approach.**

I. Introduction

Trusted digital microchips embedded in electronics systems are highly critical for defense/security applications and ubiquitous electronics including Internet-of-Things. Although confidential data are often encrypted, microchips could lose the security due to various forms of attack, including side channel attacks (SCAs) [1]. Particularly, differential power analysis (DPA) [1] is one form of SCAs, and is surprisingly effective and efficient to decipher the encrypted data. To counteract DPA, the general preventive methods are "masking" and "hiding" approaches [2]. The masking approach aims to mask the correlation between the encryption/decryption operations and their ensuing power dissipation through introducing confusion in the encryption/decryption algorithm part. On the other hand, the hiding approach aims to hide the correlation through breaking the link between data and power traces. The ultimate aim is to make DPA difficult, e.g. untraceable or traceable with infinite time [3].

Of the hiding approaches, power-balanced logic switching [4] is probably the most effective method to break the link between the data and power traces, making the DPA untraceable. This means that during the logic switching, the library cell that performs evaluation/reset operation makes little difference in power dissipation for two scenarios, i.e. different output transitions and different input combination. There are four possible output transitions, 0-to-0, 0-to-1, 1-to-1 and 1-to-0. In the conventional synchronous-logic (sync) standard cell approach [5], 0-to-0 and 1-to-1 output transitions do not switch the output logic, differentiating them (in power dissipation) from the switched 0-to-1 and 1-to-0 output transitions. Further, the power dissipated in the sync standard cell approach is also sensitive to the input combination. In a 2-input cell, there are four possible input combination, 00, 01, 10, 11, which dissipate different power from each other during the evaluation/reset operation. This is because the standard cell approach directly evaluates the input data and latch it to the output.

In view of these, an asynchronous-logic (async) quasi-delay-insensitive (QDI) handshake protocol [6] with dual-rail data-encoding [7] is a preferable choice as it switches the output twice, from empty to valid state (evaluation), and from valid to empty state (reset) in every operation cycle regardless of the possible output transitions. Now, the difference in power dissipation is lesser for various output transitions. Besides the power-balanced output transitions, async QDI handshake protocol also requires additional power overhead input detector circuit to validate the input-completeness [8]. Now, the difference in power dissipation is lesser for various input combination. Thus, both the dual-rail data-encoding and input-completeness validation are useful in balancing the power dissipation. To realize the power-balanced output transitions and power-balanced input combination, the async QDI Weak-Conditioned Half-Buffer (WCHB) cell approach [9] is a potential good candidate due to its unique features, as elaborated in next paragraph.

In this paper, we report a security analysis of the async QDI WCHB cell approach, and benchmark it against the sync standard cell approach. There are two unique features in the WCHB cell approach. First, it operates in dual-rail data-encoding, which switches the output empty-valid-empty alternately. Thus for different output transitions, the power dissipation is less different – more power-balanced than the standard cell approach with single-rail data-encoding. Second, the WCHB cell approach embodies the input detector, where a constant power is dissipated to validate the input-completeness. Thus for different input combination, the power dissipation is less different – more power-balanced than the standard cell approach with non-input-complete feature. Based on the 65nm CMOS process, the WCHB cell approach is simulated in 7 library cells, e.g. 2-input AND, 2-input OR, 2-input XOR, 3-input AND, 3-input OR, 3-input AO and 3-input OA, and benchmarked against the standard cell approach. On average, the WCHB cell approach features 62% and 69% lower normalized energy deviation (NED) and normalized standard deviation (NSD) respectively than the standard cell approach.

This paper is organized as follows. Section II presents the security analysis and comparison of the various cell approaches. Section III presents the simulation results of the WCHB cell approach under different output transitions and input combination. Finally, conclusions are drawn in Section IV.

II. Security Analysis and Comparison

A. Review of Cell Approaches

We now review the sync standard cell approach and the async QDI WCHB cell approach. For fair comparison, both the cell approaches have the same gate-level pipeline data-path, where every gate embeds individual latch for data propagation. Nonetheless, their cell structure, interface signals and operation modalities are different from each other.

Fig. 1 depicts the standard latched AND cell, comprising a standard AND cell and a standard D-type flip-flop cell. The standard latched AND cell propagates 2-input data *A* and *B* to output *Q*, latched by the clock signal *CLK*. The data are propagated in single-rail data-encoding, in which the data wires carry the logic values information, i.e. logic '0' and logic '1'. The standard latched AND cell is typically a clock-based sync approach, switching the output logic depends on the input values and the *CLK*.

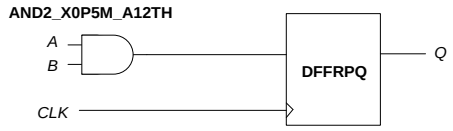

Fig. 1: Standard Latched AND Cell

Fig. 2 depicts the async QDI WCHB AND/NAND cell, comprising a functional block, a latch and an output completion detection (OCD). The functional block consists of the combination of C-Muller cells and an OR cell to validate the input-completeness [10], i.e. input detector and to perform evaluate/reset operation. The latch consists of C-Muller cells to latch and maintain the output state. The OCD is a NOR cell to perform completion detection after every evaluate/reset operation.

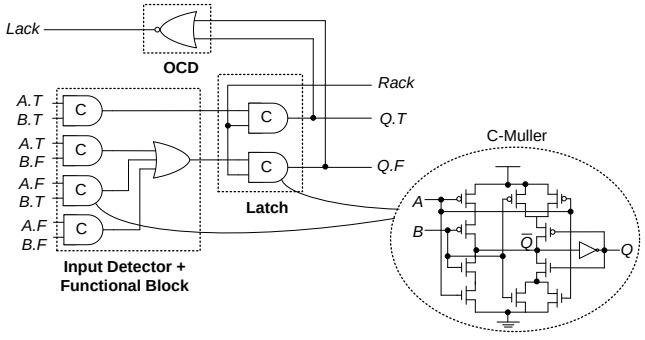

Fig. 2: WCHB AND/NAND Cell

The WCHB AND/NAND cell propagates 2-input data *A.T*/*A.F* and *B.T*/*B.F* to output *Q.T*/*Q.F* in dual-rail data-encoding, latched by the handshake signal *Rack* from the succeeding pipeline. Now, the data wires not only carry the logic values information, but also the validity of the signals. When both *A.T* and *A.F* is '0', the input *A* is empty. When either *A.T* or *A.F* is '1', the input *A* is valid. During the valid state, input *A* is logic '1' if *A.T* = 1 and is logic '0' if *A.F* = 1. When all the inputs and *Rack* arrive, the WCHB AND/NAND cell evaluates the dual-rail AND logic function, as expressed in equation (1).

$$\begin{aligned} Q.T &= A.T \cdot B.T \\ Q.F &= A.T \cdot B.F + A.F \cdot B.T + A.F \cdot B.F \end{aligned} \quad (1)$$

B. Comparison of Cell Structure

We now describe the comparison of the cell structure for sync standard cell approach and the async QDI WCHB cell approach, as tabulated in Table I. As seen, both the cell approaches feature the same gate-level static logic implementation for speed-efficient data propagation. Every gate embeds an individual latch, i.e. flip-flop cell and C-Muller cell in the standard and WCHB cell approaches respectively. To latch the data propagation, there is a control signal, i.e. *CLK* clock signal and *Rack* handshake signal in the standard and WCHB cell approaches respectively.

TABLE I
STRUCTURE OF VARIOUS CELL APPROACHES

	Standard	WCHB
Data-Path Logic Implementation	Gate-Level Static Logic	
Latch Type	Flip-Flop Cell	C-Muller Cell
Latch Control Signals	*CLK*	*Rack*
Design Methodology	Synchronous Clock-based	Async QDI Handshake
Data-Encoding	Single-Rail	Dual-Rail
Signal Validity	Non-Input-Complete	Input-Complete
Different Output Transitions	Less Power-Balanced	More Power-Balanced
Different Input Combination	Less Power-Balanced	More Power-Balanced

In terms of design methodology, the WCHB cell approach is the async QDI handshake protocol featuring dual-rail data-encoding. The WCHB cell approach run evaluate/reset operation alternately to continuously propagate empty/valid data. In the dual-rail encoding, the use of two wires for indicating the signal validity will balance the power dissipation for different output transitions. For instance, for both the output transitions 0-to-1 and 0-to-0, the WCHB cell has to switch the data valid-empty-valid similarly, making lesser difference in power dissipation. Whereas in the single-rail standard cell approach, there is no data switching for the output transition 0-to-0. Thus, the power dissipation for the output transitions 1-to-0 and 0-to-0 can be easily differentiated.

In the input-complete feature, the use of input detector circuit which constitute to the overall power dissipation, will balance the power dissipation for different input combination. For instance, the input detector circuit in the WCHB cell approach has similar switching regardless of the input combination, making lesser difference in power dissipation. Whereas in the non-input-complete standard cell approach, there is no input detector and the power dissipation is solely constituted from the logic evaluation. Thus, the power dissipation for different input combination can be easily differentiated.

C. Comparison of Cell Timing

We now analyze the timing for the sync standard cell approach and the async QDI WCHB cell approach. Fig. 4 (a) depicts the timing diagram of the standard cell approach from cycle 1 to cycle 6 in different output (*Q*) transitions and input (*AB*) combination. As seen, from cycle 1 to 3 where *Q* transition is 0-to-0, there is no *Q* switching for *AB* combination 00, 01, 10. In cycle 4 where *Q* transition is 0-to-1, *Q* is switched to 1 for *AB* combination 11. In cycle 5 where *Q* transition is 1-to-1, *Q* remains at 1, i.e. no *Q* switching for *AB* combination 11. In cycle 6 where *Q* transition is 1-to-0, *Q* is switched to 0 for *AB* combination 10. In short, *Q* is only switched where *Q* transitions are 0-to-1 and 1-to-0, dissipating relatively higher power than the *Q* transitions 1-to-1 and 0-to-0, i.e. less power-balanced.

Fig. 4 (b) depicts the timing diagram of the WCHB cell approach, which operates in the async QDI handshake protocol. In contrast to the standard cell approach in Fig. 4 (a), the handshake *Rack* signal is used for data propagation, and the input/output (*A.T·B.T* and *Q.T*) signals are designed in dual-rail data-encoding. As seen, in every cycle from cycle 1 to 6, *A.T·B.T* and *Q.T* must be reset to the empty state first. After *Rack* is triggered and *A.T·B.T* arrives, *Q.T* is evaluated to either logic 0 (V0) or logic 1 (V1) in the valid state. In every cycle, there is *Q.T* switching between the empty and valid states regardless of the different *Q.T* transitions and *A.T·B.T* combination, i.e. more power-balanced.

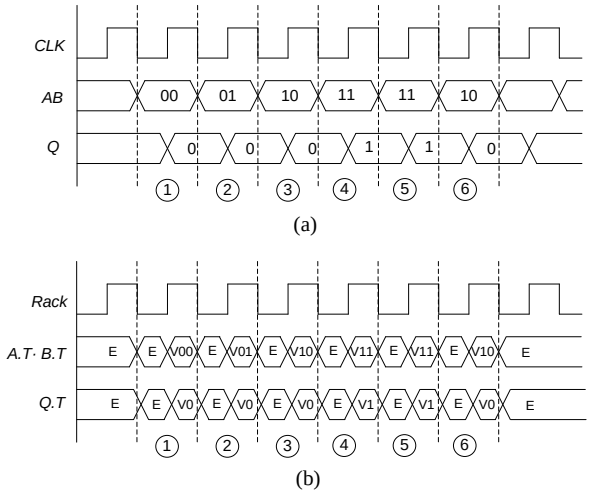

Fig. 4: Timing Diagrams (a) Standard Cell Approach and (b) WCHB Cell Approach

III. Simulation Results

Based on 65nm CMOS process technology, the async QDI WCHB cell approach is benchmarked against the sync standard cell approach. Using 2-input AND cells for demonstration, we compare the power dissipation of various cell approaches for different output transitions and different input combination. Table II tabulates the power dissipation @100MHz input rate for output transitions 0-to-0, 0-to-1, 1-to-1 and 1-to-0, under input combination 00, 01, 10 and 11. The cycle 1 to cycle 6 can be referred to the timing diagrams in Fig. 4 for various scenarios.

From the Table II, we remark the following. First, the standard cell approach has ~60% different power dissipation (min: 0.42µW, max: 1.01µW) for 0-to-0/1-to-0 output transition, and ~30% different power dissipation (min: 1.15µW, max: 1.6µW) for 0-to-1/1-to-1 output transition although the input combination is the same. Whereas in the WCHB cell approach, there is no power difference for the above cases. Second, for different input combination, the WCHB cell approach dissipates ~23% power difference (min: 2.38µW, max: 3.1µW). In contrast, the standard cell approach dissipates ~74% power difference (min: 0.42µW, max: 1.6µW).

TABLE II
POWER DISSIPATION @100MHZ INPUT RATE FOR AND CELLS BASED ON STANDARD AND WCHB CELL APPROACHES

	Power Dissipation (µW)							
Output Tran.	0-to-0			0-to-1	1-to-1	1-to-0		
Input Comb.	00	01	10	11	11	00	01	10
Cycle	1	2	3	4	5	-	-	6
Standard	0.42	0.43	0.46	1.6	1.15	0.97	0.98	1.01
WCHB	2.68	3.1	2.9	2.38	2.38	2.68	3.1	2.9

We further complete the simulation results for various library cells based on the standard and WCHB cell approaches, as tabulated in Table III. We obtain the transistor count, max energy dissipation (E) per-cycle, min E per-cycle from the simulation, and calculate the normalized energy deviation (NED) and normalized standard deviation (NSD). The NED and NSD range from the value 0 to 1. Equation (2) generalizes the NED, which represents the variation of E per-cycle. The lower NED means the lower variation of E per-cycle, lowering the chance of power information leaking for DPA attack. Equation (3) generalizes the NSD, which represents the variation of standard deviation of E per-cycle. The collected data of E per-cycle forms the normal distribution, and the smaller NSD shows the lower standard deviation of the data, lowering the chance for DPA attack.

$$\text{NED} = \frac{\text{Max E per-cycle} - \text{Min E per-cycle}}{\text{Max E per-cycle}} \quad (2)$$

$$\text{NSD} = \frac{\text{Standard Deviation}}{\text{Mean}} \quad (3)$$

TABLE III
NED AND NSD FOR VARIOUS LIBRARY CELLS BASED ON STANDARD AND WCHB CELL APPROACHES

	Transistor Count		Max E per-cycle ($\times 10^{-14}$J)		Min E per-cycle ($\times 10^{-14}$J)		NED		NSD	
Library Cells	STD	WCHB	STD	WCHB	STD	WCHB	STD	WCHB	STD	WCHB
2-input AND	38	88	1.60	3.10	0.42	2.38	0.74	0.23	0.44	0.10
2-input OR	38	88	1.56	3.33	0.42	1.99	0.73	0.40	0.30	0.18
2-input XOR	42	92	1.68	2.98	0.42	2.53	0.75	0.15	0.33	0.06
3-input AND	40	144	1.64	4.88	0.42	3.34	0.74	0.32	0.42	0.10
3-input OR	40	144	1.65	5.05	0.42	2.87	0.75	0.43	0.24	0.14
3-input AO	44	144	1.59	4.93	0.42	3.58	0.74	0.27	0.35	0.10
3-input OA	44	144	1.61	4.62	0.42	3.79	0.74	0.18	0.42	0.06
Average	41	121	1.61	4.13	0.42	2.93	0.74	0.28	0.36	0.11

From Table III, the WCHB cell approach has 3× more transistor count than the standard cell approach due to the async QDI features that include the dual-rail data-encoding and input-completeness validation. Although the standard cell approach has the lower transistor count due to the simpler single-rail data-encoding and the non-input-complete feature, there is a large difference between the max E per-cycle and min E per-cycle. This causes the NED and NSD of the standard cell approach are as high as 0.74 and 0.36 respectively. Whereas in the WCHB cell approach that operates in async QDI dual-rail protocol, the NED and NSD are much lower, 0.28 and 0.11 respectively. In short, the WCHB cell approach features the 62% lower NED (0.28 vis-à-vis 0.74), and 69% lower NSD (0.11 vis-à-vis 0.36) than the standard cell approach.

IV. CONCLUSIONS

We have reported the security analysis of the async QDI WCHB cell approach, and benchmarked it against the sync standard cell approach for DPA attack. The WCHB cell approach has the power-balanced feature for different output transitions and different input combination. The power-balanced feature is due to the dual-rail data-encoding and input-completeness in the async QDI handshake protocol. By means of 7 library cells, the WCHB cell approach features, on average, 62% lower NED and 69% lower NSD than the standard cell approach.

ACKNOWLEDGEMENT

This research work was supported by Agency for Science, Technology and Research (A*STAR), Singapore, under SERC 2013 Public Sector Research Funding, Grant No: SERC1321202098. The authors thank A*STAR for the support in funding this research.

REFERENCES

[1] P. Kocher, J. Jaffe and B. Jun, "Differential power analysis," Proc. *CRYPTO*, pp. 388-397, 1999.

[2] S. Mangard, E. Oswald and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2007.

[3] K.-S. Chong, K. Z. L. Ne, W.-G. Ho, N. Liu, A. Akbar, B.-H. Gwee and J. S. Chang, "Counteracting differential power analysis: Hiding encrypted data from circuit cells," Proc. *IEEE EDSSC*, pp. 297-300, Jun. 2015.

[4] 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," Proc. *IEEE ESSCIRC*, pp. 403-406, Sep. 2002.

[5] J. M. Rabaey, A. Chandrakasan and B. Nikolic, *Digital Integrated Circuits: A Design Perspective*, Prentice-Hall, 2003.

[6] A. J. Martin, and M. Nystrom, "Asynchronous techniques for system on-chip designs," *IEEE Proc.*, vol. 94, no. 6, pp 1089–1120, Jun. 2006.

[7] K. J. Kulikowski, *et. al.*, "Delay Insensitive encoding and power analysis: a balancing act," Proc. *IEEE ASYNC*, pp. 116-125, May 2005.

[8] P. A. Beerel, R. O. Ozdag and M. Ferretti, *A Designer's Guide to Asynchronous VLSI.*, Cambridge University Press, 2010.

[9] Y. Thonnart, E. Beigne and P. Vivet, "A pseudo-synchronous implementation flow for WCHB QDI asynchronous circuits," Proc. *IEEE ASYNC*, pp 73-80, May 2012.

[10] K.-S. Chong, W.-G. Ho, T. Lin, B.-H. Gwee and J. S. Chang, "Sense Amplifier Half-Buffer (SAHB): a low-power high-performance async QDI cell template," *IEEE TVLSI*, vol. PP, no. 99, pp 1-14, Jul. 2016.