Title	Counteracting differential power analysis: Hiding encrypted data from circuit cells
Author(s)	Chong, Kwen-Siong; Ne, Kyaw Zwa Lwin; Ho, Weng-Geng; Liu, Nan; Akbar, Ali H.; Gwee, Bah-Hwee; Chang, Joseph Sylvester
Citation	Chong, K.-S., Ne, K. Z. L., Ho, W.-G., Liu, N., Akbar, A. H., Gwee, B.-H., et al. (2015). Counteracting differential power analysis: Hiding encrypted data from circuit cells. 2015 IEEE International Conference on Electron Devices and Solid-State Circuits (EDSSC), 15506250-.
Date	2015
URL	http://hdl.handle.net/10220/41564
Rights	© 2015 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at: [http://dx.doi.org/10.1109/EDSSC.2015.7285109].

Counteracting Differential Power Analysis: Hiding Encrypted Data from Circuit Cells

Kwen-Siong Chong*, K.Z.L. Ne, Weng-Geng Ho, Nan Liu, Ali Akbar, Bah-Hwee Gwee, & Joseph. S. Chang
School of EEE, Nanyang Technological University, Singapore
*KSChong@ntu.edu.sg

***Abstract*—We propose a balanced Pre-Charge Static Logic (PCSL) circuit style for asynchronous systems, and compare it against other reported circuit styles to counteract differential power analysis (DPA). Our study shows that all these circuit styles (including our balanced PCSL) dissipate different energy due to data-dependency, and hence balancing the energy of circuits embodying these circuit styles remains challenging. However, in view of low circuit overheads and asynchronous operations (with noise generation), our balanced PCSL is still competitive in terms of DPA-resistance, requiring 3.5× less power traces than its NULL convention logic counterpart.**

I. INTRODUCTION

Trusted digital microchips embedded in electronics systems are highly critical for defense/security applications, and to some extent, increasingly for ubiquitous electronics including Internet-of-Things. Although confidential data (within microchips) are often encrypted, microchips could still be losing 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 amazingly simple to get the encrypted data deciphered. To counteract DPA, the general preventive ideas are based on the "masking" and "hiding" approaches [1]. The masking approach aims to mask the relationship/correlation between the encryption/decryption operations and their ensuing power dissipation, and conversely, the hiding approach aims to hide the same through breaking the link between data and power traces. The ultimate aim is to make DPA difficult, e.g. untraceable and/or with infinite time.

In this paper, we mainly focus on the hiding approach by investigating various state-of-the-art circuit styles to counteract DPA. Our investigation pertains to DPA countermeasures based on dual-rail logic for hiding/modulating/balancing the power information in terms of amplitude or time or both. The circuit styles of interest include sense amplifier-based logic (SABL) [2], wave dynamic differential logic (WDDL) [3], three-phase dual-rail pre-charge logic (TDPL) [4], dual-rail random switching logic (DRSL) [5], masked dual-rail pre-charged logic (MDPL) [6], improved MDPL (iMDPL) [7], and asynchronous dual-rail cells such as variants based on delay-insensitive-minterm-synthesis (DIMS) [8] and NULL convention logic (NCL) [9], [10]. By using AND/NAND dual-rail cells for illustration, Fig. 1 depicts various reported circuit styles for counteracting DPA. Of these circuit styles, both synchronous and asynchronous operation modalities are considered. Although the synchronous operation modality is advantageous for its simple implementation, the asynchronous operation modality could be even more advantageous [8], [11]-[13] for moderating both the time and amplitude of power

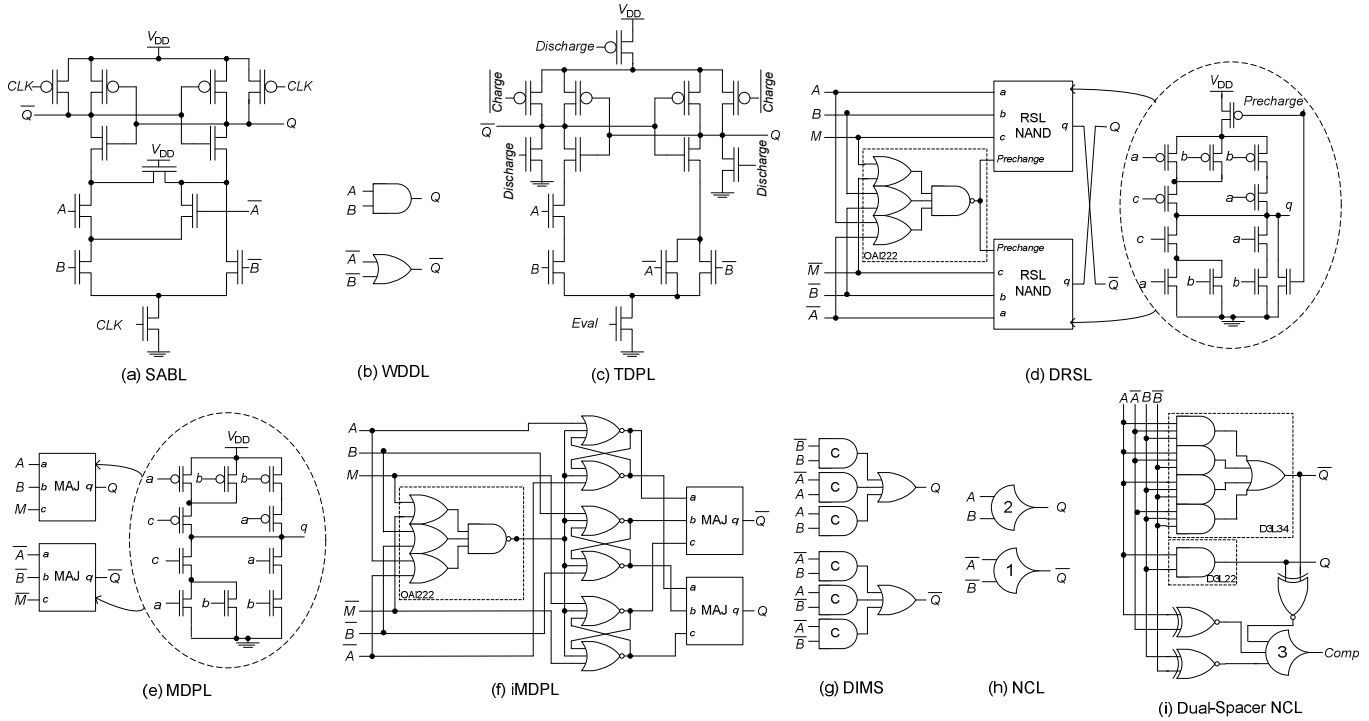

Fig. 1: AND/NAND dual-rail cells based on reported dual-rail logic styles for DPA: (a) sense amplifier-based logic, (b) wave dynamic differential logic, (c) three-phase dual-rail pre-charge logic, (d) dual-rail random switching logic, (e) masked dual-rail pre-charge logic (MDPL), (f) improved MDPL, (g) asynchronous delay-insensitive-minterm-synthesis, (h) asynchronous NULL convention logic (NCL), and (i) asynchronous dual-spacer NCL

traces, hence possibly enhancing the DPA-resistance.

We further propose to adopt our Pre-Charge Static Logic (PCSL) [11], coined as balanced PCSL here, to counteract DPA. Our proposed balanced PCSL cell is designed to mitigate the data-dependency [8] by balancing the charging/discharging paths, hence making the power dissipation of various data operations less noticeable. By merely comparing basic AND/NAND cells @ 65nm CMOS, our comparison shows that our balanced PCSL is more competitive in view of its hardware simplicity and its asynchronous operation for possible time/amplitude moderation for increased DPA-resistance.

In view of the similar hardware simplicity and possible asynchronous operation for the reported NCL and our proposed balanced PCSL, we further construct a Substitute-box (S-Box) based on these two circuit styles. We further consider the time moderation applied to the balanced PCSL S-Box by using its inherent handshake request signal. Our simulation shows that the S-Box embodying our balanced PCSL with time moderation features better DPA-resistance.

II. Proposed Balanced PCSL

Fig. 2 depicts the AND/NAND cell embodying our balanced PCSL. Particularly, the balancing is achieved by inserting dummy transistors (labelled with asterisks *) to balance the charging/discharging paths. Although the concept of such dummy transistor insertion is not new, the application of PCSL can make the overall digital circuit embodying PCSL less noticeable for power variations. Our balanced PCSL cells can be applied in a synchronous or an asynchronous pipeline. The former synchronous pipeline is the standard approach where the clocked-based registers are used. The latter asynchronous pipeline is realized similarly based on that using asynchronous handshake protocol [11]. The self-timed asynchronous operation is tolerant to process-voltage-temperature variations [11], [12], further enabling DPA countermeasures to modulate the power dissipation in both time and amplitude. The further added advantage of asynchronous operation is that dynamic voltage scaling (DVS) can be easily applied [11].

III. Simulations on Basic Cells

We first investigate the basic circuit styles for their varied very power characteristics. Table I tabulates several characteristics of the reported and proposed circuit styles

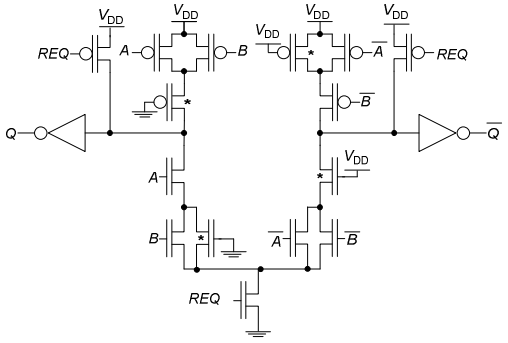

Fig. 2: An AND/NAND cell based on our balanced Pre-Charge Static Logic

whose transistor netlists (@ 65nm CMOS) are extracted (with parasitic estimation) for simulations. Based on our observations, we remark the followings.

First, from high speed and small area viewpoints, WDDL and SABL are respectively the best. Second, from the energy dissipation viewpoint, SABL and the balanced PCSL are the leading candidates. Third, from energy variation viewpoint (including by using the merits of Normalized Energy Derivation (NED) and Normalized Standard Deviation (NSD)), all these circuit styles experience varying degrees of energy difference (per operation). These energy variations indicate that balancing energy dissipation due to data-dependency remains challenging [8], [14]. Viewed differently, dual-rail logic could not be effective to mitigate leakages (due to data-dependency), and additional treatments (e.g. parasitic capacitance balancing, transistor sizing, the mode of operation) could still be required. Nonetheless, taking into consideration of circuit overheads and energy variations, SABL, WDDL and the proposed balanced PCSL are competitive. Lastly, another way to enhance DPA-resistance is through the time and power moderation [13] where the asynchronous operation could be advantageous. The circuit styles based on the asynchronous designs (e.g. DIMS, NCL and the proposed PCSL) are hence suitable. This is different from the circuit styles based on the synchronous designs which do not inherently enjoy such time and power moderation (unless large overheads are incurred).

IV. Time Moderation for Balanced PCSL Circuits

In view of the Section III, and considering the hardware simplicity and possible asynchronous operation, we design a 32-bit S-Box based on the reported NCL and our balanced

Table I. The comparison of AND/NAND dual-rail cells based on various circuit styles (simulations are conducted @ V_{DD} = 1.2V)

	Operation Modality	DPA-resistance in Time	DPA-resistance via DVS	Average Delay (ps)	Normalized Trans. Width[#]	Max. Energy (fJ)	Min. Energy (fJ)	NED (%)	NSD (%)
SABL [2]	Synchronous	Limited	Limited	64	24	3.25	3.00	7.7	3.3
WDDL [3]	Synchronous	Limited	Limited	38	30	4.04	3.48	13.9	6.1
TDPL [4]	Synchronous	Limited	Limited	55	28	5.81	1.68	71.1	37.1
DRSL [5]	Synchronous	Limited	Limited	152	90	9.52	7.18	24.6	8.1
MDPL [6]	Synchronous	Limited	Limited	41	46	3.91	2.90	25.8	11.5
iMDPL [7]	Synchronous	Limited	Limited	240	214	29.80	27.22	8.7	2.6
DIMS [8]	Asynchronous	Good	Good	125	216	12.02	9.94	17.3	6.8
NCL [9]	Asynchronous	Good	Good	44	43	5.14	3.38	34.2	17.3
Dual-Spacer NCL [10]	Asynchronous	Good	Good	55	279	44.89	7.92	82.4	58.8
Proposed Balanced PCSL	Asynchronous	Good	Good	58	39	3.52	3.12	11.4	4.9

[#] The number of transistor width are normalized with respect to a transistor having a minimum transistor width of 120nm @ 65nm CMOS

PCSL. In this paper, we only consider the time moderation.

Fig. 3 depicts the block diagram of the S-Box. In Fig. 3, we only show the single-rail signals where the inputs are *Plaintext* and *Key*, and the output is *Ciphertext*. To obtain the dual-rail netlist, a single-rail netlist is first obtained through a Verilog synthesis. Thereafter, the single-rail netlist is converted to a dual-rail NCL netlist and a PCSL netlist. The handshake signal *REQ* is required for the S-Box embodying the balanced PCSL cells. We further consider another version of the balanced PCSL S-Box by introducing a delay line (i.e. oval shape) to introduce delay noise (see later). Put simply, we have a version of balanced PCSL S-Box without noise generation, and another version with noise generation. The NCL and balanced PCSL netlists are designed @ 65nm CMOS process.

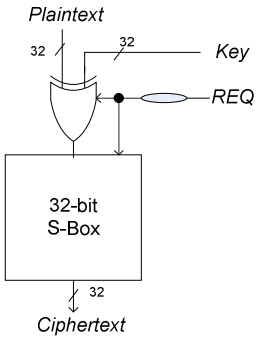

Fig. 3: The block diagram of the S-box (with XOR inputs)

Figs. 4 (a) and (b) depict the input/output patterns for the NCL S-Box and balanced PCSL S-Box circuits respectively. For simplicity in our investigation, we set the inputs (*Plaintext, Key* and *REQ*) to be updated at the same time (for every operation). Since the balanced PCSL S-Box circuit has *REQ*, as mentioned earlier, we can leverage such signal to generate a random noise in time, i.e. uncertain timing of 20ps to 100ps in the shaded shape. In view of this noise generation, the empty operation (i.e. empty operation) can be moderated in time – this helps to prevent leakages. For the balanced PCSL S-Box circuit without noise generation, the uncertain timing is reduced where all the balanced PCSL cells are reset simultaneously. For completeness, should further DPA-enhancement be considered, noises (in time) can be similarly introduced to the input signals (to both the NCL and PCSL S-Box circuits). Nonetheless, we exclude such analysis here.

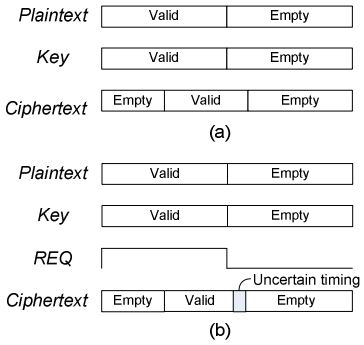

Fig. 4: The input/output for the S-Box circuits: (a) NCL and (b) balanced PCSL

We simulate 500 power traces @ Nanosim for the NCL S-Box circuit and PCSL S-Box circuits with and without noise generation. Our objective here is to attempt to make a successful attack on these circuit styles for comparison, so we consider the following simplified setups. First, in Nanosim, we setup the simulation accuracy to Level 4, appropriate for digital cell characterization. Second, we remove all the parasitic estimation – it would otherwise take very long time for power simulations and for DPA attacks/evaluations. Third, the power traces are sampled at least 20ps time step. Fourth, to reduce interface noises (i.e. to reduce the signal-to-noise ratio), we only change 1 byte data (out of 4 bytes) per operation since the attack is based on byte by byte. Fifth, we use the Hamming Weight model for DPA.

Figs. 5 (a) to (c) respectively depict the 10 power traces for the NCL S-Box circuit, the balanced PCSL S-Box circuits without and with noise generation. The first 6ns is for valid operation, and the following 6ns is for reset (empty) operation. From Fig. 5 (a), we observe that the data dependency affects the power dissipation of the NCL S-Box in both the valid and empty operations. From Fig. 5 (b), we observe less data dependency that affects the power dissipation of the balanced PCSL S-Box. Nonetheless, the amplitude of current is high during the empty operation because all the balanced PSCL cells are reset simultaneously. From Fig. 5 (c), we can observe that time noise is introduced in the empty operation.

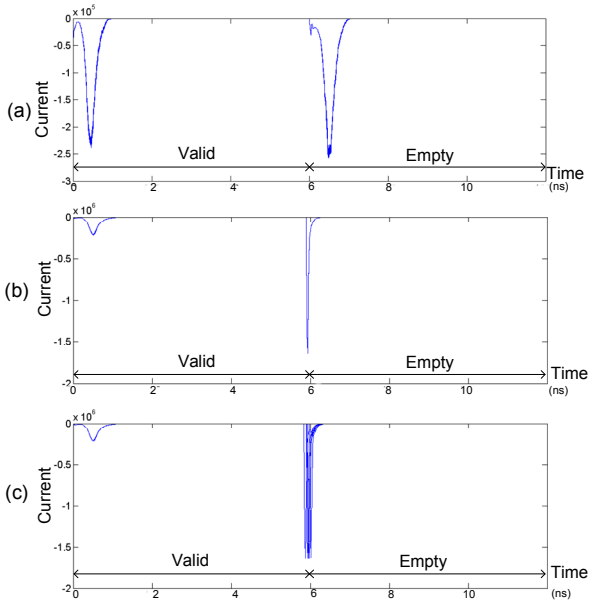

Fig. 5: The power traces of S-Box: (a) NCL, (b) Balanced PCSL without noise, and (c) Balanced PCSL with noise

Fig. 6 (a) – (c) respectively depict the DPA (versus time) of the correct key (key=35) on the NCL S-Box circuit, the balanced PCSL S-Box circuits without and with noise generation. All these S-Box circuits were successfully attacked based on the 500 power traces. From Figs. 6 (a) and (c), we observe that leakages mainly happen during the empty operations where the correlation is rather high. Put simply, the Hamming Weight power model still can predict reasonably well for the empty operation in these S-Box circuits. As expected, from Fig. 6 (c), we observe that the time noise introduced to the empty operation of the balanced PCSL S-Box reduces the leakage information.

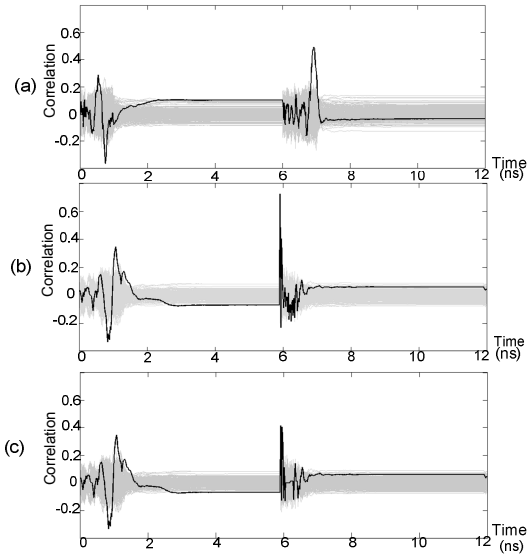

Fig. 6: The DPA of S-Box circuits (where the correct key is bold): (a) NCL, (b) balanced PCSL without noise, and (c) balanced PCSL with noise

Figs. 7 (a) – (c) further respectively depict the relationship between the correlation and the number of power traces for the NCL S-Box circuit, the balanced PCSL S-Box circuits without and with noise generation. From Fig. 7, we observe that the NCL S-Box circuit requires at least 64 power traces to break the key. Due to the leakage in the empty, the balanced PCSL S-Box circuit without noise generation requires only 21 power traces to do the same. However, the balanced PCSL S-Box circuit with noise generation requires more power traces, i.e. 225, to do the same. Viewed differently, the noise generation is effective, and can easily be applied to the asynchronous circuits (including our balanced PCSL cells).

V. Conclusions and Future Work

We have proposed a dual-rail balanced PCSL cell style for counteracting DPA. We have studied and compared various dual-rail cells, and considered that balancing of these dual-rail cells (including our balanced PCSL) remains challenging. Nonetheless, by leveraging on the asynchronous operation with noise generation, we have shown that our balanced PCSL remains competitive in terms of DPA-resistance (i.e. 3.5× less power traces than NCL). Our future work includes a further investigation on the time-cum-amplitude moderation through voltage scaling for circuits embodying our balanced PCSL.

Acknowledgments

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 kind support in funding this research.

References

[1] S. Mangard *et al*, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*, Springer, 2007.

[2] K. Tiri *et al*, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," *ESSCIRC*, 2002.

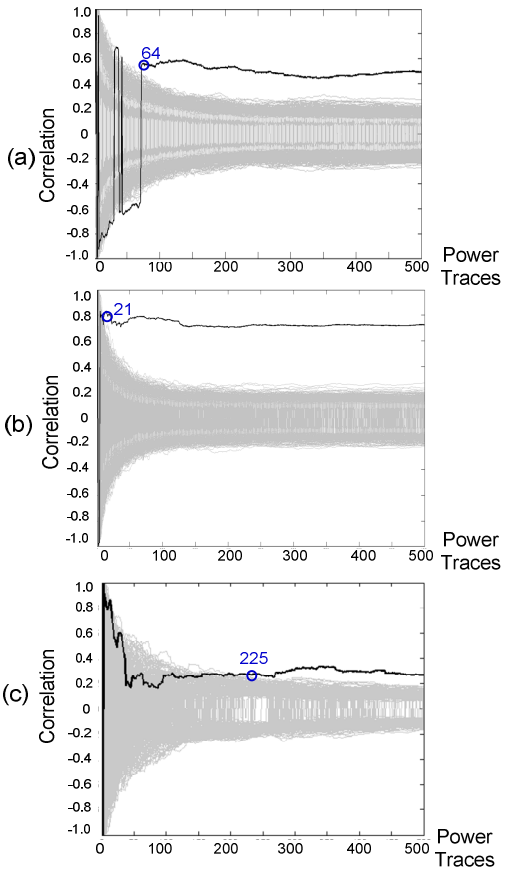

Fig. 7: The correlation vs power traces (where the correct key is bold): (a) NCL, (b) Balanced PCSL without noise, and (c) Balanced PCSL with noise

[3] D. D. Hwang *et al*, "AES-based security coprocessor IC in 0.18um CMOS with resistance to differential power analysis side-channel attacks," *IEEE JSSC*, v41, pp. 781-791, Apr. 2006.

[4] M. Bucci *et al*, "Three-phase dual-rail pre-charge logic," *CHES*, 2006.

[5] Z. Chen *et al*, "Dual-rail switching logic: A countermeasure to reduce side channel leakage," *CHES*, 2006.

[6] T. Popp *et al*, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," *CHES*, 2005.

[7] T. Popp *et al*, "Evaluation of the masked logic style MDPL on a prototype chip," *CHES*, 2007.

[8] S. Moore *et al*, "Balaced self-checking asynchronous logic for smart card application ," *J. Microprocess. Microsyst.*, v27, pp.421-420, 2003.

[9] S. Kotipali *et al*, "Asynchronous Advanced Encryption Standard Hardware with Random Noise Injection for Improved Side-Channel Attack resistance," *J. Electrical Comp. Engineering*, 2014.

[10] W. Cilio *et al*, "Side-channel attack mitigation using dual-spacer dual-rail delay-insensitive logic (D^3L)," *SECON*, 2010.

[11] T. Lin *et al*, "An ultra-low power asynchronous-logic in-situ self-adaptive VDD system for wireless sensor network," *IEEE JSSC*, v48, pp. 573-586, Feb. 2013.

[12] K.-L. Chang *et al*, "Synchronous-logic and asynchronous-logic 8051 microcontroller cores for realizing the internet of things: a comparative study on dynamic voltage scaling and variation effects," *IEEE JETCAS*, v3, pp. 23–34, Mar. 2013.

[13] C. Sui *et al*, "Random dynmaic voltage scaling design to enhace security of NCL S-box," *IEEE MWSCAS*, 2011.

[14] K. J. Kulikowski *et al*, "Delay Insensitive encoding and power analysis: a balancing act," *IEEE ASYNC*, 2005.