RESEARCH ARTICLE OPEN ACCESS

Analysis of Leakage Power Attacks on DPA Resistant Logic Styles: A Survey

S. Shiney Immaculate[1], K. Manoharan[2] Ph.D
Research Scholar ME[1], Assistant Professor[2]
ECE Department, SVS College of Engineering
Coimbatore
Tamil Nadu - India

ABSTRACT
This paper discusses a general model of differential power analysis (DPA) attacks to static logic circuits.IC's are vulnerable to side channel attacks .The attacker can gain information by monitoring the power consumption leaked by the switching behavior of digital complementary metal-oxide-semiconductor (CMOS) gates. In this paper, various aspects related to Leakage Power Analysis (LPA) attacks to cryptographic circuits are presented. These attacks aim at recovering the secret key of a cryptographic core from the measurements of its static (leakage) power. This method employs a comparison of different anti-DPA logic styles whose logic operates with power consumption independent of both logic values and sequence of data. This paper examines the noise characteristics of the power signals and effectiveness of LPA attacks on process variations are taken into an account.
Keywords:- Cryptography, differential power analysis, leakage power analysis, side channel attack, delay based dual - rail precharge logic (DDPL).

I. INTRODUCTION

In the nanometer regime, the power contribution due to leakage is increasing faster than the dynamic power at each technology node; hence chip power consumption is no longer dominated by the dynamic power [10]. In fact, for a typical 65 nm CMOS chip, leakage power is in the order of half the total power consumption, and it is expected to be an even greater fraction in future technologies . Under these conditions, the leakage power can be easily measured in the same way as the dynamic power is measured in traditional Power Analysis attacks. One Side Channel Attack in particular, namely the Differential Power Analysis (DPA), is of great concern [6]. Side channel attacks can reveal confidential data exploiting the information leaked by the hardware implementation of cryptographic algorithms. [11],[12],[13].

The logic styles to make devices resistant against SCA attacks are dual-rail pre-charge (DRP) logic styles that consume an equal amount of power and its power consumption is constant or independent of the processed data. In a dual-rail precharge (DRP) logic style (e.g., sense amplifier-based logic (SABL) ,wave dynamic differential logic (WDDL), dual-spacer DRP), signals are spatially encoded as two complementary wires and power consumption is constant under the assumption that the differential outputs of each gate drive the same capacitive load.

The first approach is SABL [8] it achieves the goal by switching the output independently of the input value sequence and by having a constant load capacitance equal to all internal nodes combined with one of the balanced output loads. A second approach is based on a design of a dual-rail pre-charge logic family whose power consumption is insensitive to unbalanced load conditions thus allowing adopting a semi-custom design flow (automatic place & route) without any constraint on the routing of the complementary wires. Wave Dynamic Differential Logic (WDDL) is an example of a state-of-the-art DPA-resistant logic style that can be implemented with a standard CMOS cell library [14], [15]. It consists of pre-processing input data in order to obtain masked signals which are a function of original data and a random internally-generated mask. Attacker can only correlate masked data and power consumption but he/she cannot extract information about original data. The Masked dual-rail pre-charge logic style (MDPL) [1] where, due to the random masking at the gate level, power consumption is randomized [7]. MDPL is a dual-rail pre-charge logic, where glitches are avoided but, at the same time, the complementary wires do not need to be balanced thus removing the main drawback of the dual-rail circuits.

A third solution is an logic insensitive to unbalanced routing capacitances is obtained by introducing a three-phase dual-rail precharge logic (TDPL) [2]with an additional discharge phase where the output which is still high after the evaluation phase is discharged as well. Since both outputs are precharged to and discharged to, a TDPL gate shows constant energy consumption over its operating cycle.

The main drawback of this solution is the additional area for the routing of the three control signals. A single-ended version of TDPL shows a lower overhead in terms of power consumption and area thus being suitable for embedded and mobile applications. This paper proposes the design for a secure logic family which is based on a standard two-phase operation (precharge/evaluation) while being at the same time insensitive to unbalanced load conditions. The fourth technique is a delay-based dual-rail precharge logic (DDPL) [3] which exploits the time domain data encoding. During the precharge phase both differential lines are charged to V_{DD} and, in the evaluation phase, are both discharged to V_{SS}. The information is encoded in the order with which the lines are discharged. For a logic-1, the negated line is discharged after a delay with respect to the asserted one. Conversely, for a logic-0, the negated line is discharged first. Since over the operating cycles both lines are charged and discharged once, the total current consumption is data-independent. Countermeasures to DPA attacks of logic gates are reported in Section II. The comparison of all the techniques CMOS, MDDL, SABL, WDDL, DDPL is reported in Section III respectively.

II. COUNTERMEASURES TO DPA ATTACKS

A.SABL Technique

Sense Amplifier Based Logic is a logic style that uses a fixed amount of charge for every transition, including the degenerated events in which a gate does not change state. In each and every cycle, a SABL gate charges a total capacitance with a constant value [8].

SABL is based on 2 principles. First, it is a dynamic and differential logic style and therefore has exactly one switching event per cycle and this event is independent of the input value and sequence. Since a differential logic family uses the true and the false illustrate the in and output signals, and a dynamic logic family alternates precharge and evaluation phases, both outputs are precharged to 1 in the precharge phase and exactly 1 of the 2 outputs evaluates to 0 in the evaluation phase. Second, during a switching event, it ensures that the load capacitance has a constant value. SABL completely controls the portion of the load capacitance that is due to the logic gate. The intrinsic capacitances at the differential in and output signals are symmetric and additionally it discharges and charges the entire internal node capacitances through a special pull down network.

B. WDDL Technique

The Wave Dynamic Differential Logic (WDDL) is a promising countermeasure to protect cryptographic devices from Differential Power Attacks (DPA). But the key challenge is to maintain symmetry between dual networks, so as to obtain equal propagation delays and power consumption on differential signals.

1) Precharge wave generation

Contrary to SDDL gates, WDDL gates do not precharge simultaneously. The precharged 0's ripple through the combinatorial logic. Instead of a precharge signal that resets the logic, there is a precharge wave that just creates a Dynamic Logic without a big load on the precharge control signal [7]. The gates are precharged without distributing the signal to each individual gate.Another advantage is that during the precharge phase,WDDL has a lower peak supply current. As a result problem for signal integrity, is lowered. There are 2 ways to launch the precharge wave. The first method is to insert a precharge operator at the start of every combinatorial logic tree, i.e. the inputs of the encryption module and the outputs of the registers. The second method is preferred than the double clock frequency for the same data rate: the entire compound register is reset in every cycle.

C. Three-Phase Dual-Rail Pre-charge Logic

A three-phase dual-rail pre-charge logic (TDPL) where, during the first phase (pre-charge), the output lines of a generic logic gate are both charged to *VDD*, then (second phase - evaluation) the proper line is discharged to *VSS* according to the input data, thus generating a new output data[2]. Finally, during the last phase (discharge), the other line is discharged too. As a consequence, since both wires are pre-charged to *VDD* and discharged to *VSS*, a TDPL logic gate shows constant energy consumption over its operating cycle (independent of the input data), even if unbalanced capacitive loads to *VDD* and/or *VSS* are taken into account. The TDPL approach can be implemented as an enhancement of the SABL logic style [8] with a minimum increase in the required area. Therefore, throughout this paper, SABL cells are assumed as the benchmark for the equivalent TDPL cells. An inverter is shown in Figure 1, where two additional pull-down NMOS transistors (*N*1, *N*4) and a PMOS switch (*P*1) have been added to the SABL inverter in order to implement the discharge phase

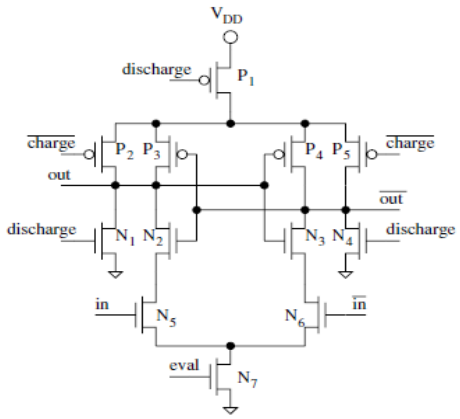

Fig .1.TDPL inverter

D. Delay-Based Dual-Rail Precharge Logic

Delay-based dual-rail precharge logic (DDPL) which exploits the time domain data encoding shown in Fig. 1: during the precharge phase both differential lines are charged to V_{DD} and, in the evaluation phase, are both discharged to V_{SS} [3]. The information is encoded in the order with which the lines are discharged. For a logic-1, the negated line is discharged after a delay Δ with respect to the asserted one. Conversely, for a logic-0, the negated line is discharged first. Since over the operating cycles both lines are charged and discharged once, the total current consumption is data-independent.

A two-input NAND/AND which operate accordingly to the introduced data encoding are depicted in Fig.2 (a).

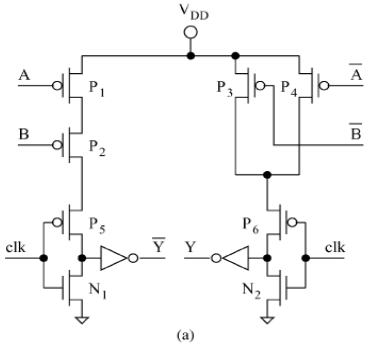

Fig.2(a).NAND/AND

Precharge phase: at the beginning of each cycle, signal goes high, thus closing and and precharging both output lines V_{DD} . Since during this phase the input lines are high (outputs from another DDPL gate), the pull-uplogic is open.

Evaluation phase: the new DDPL encoded input data (A, A′), (B, B') are presented to the circuit on the falling edge of signal. Since A, B, go low before (A ', B') (both inputs are logic-1's), the negated output (Y') is discharged before Y thus generating a logic-0, as expected in a NAND gate.

III. COMPARISON OF CMOS, MDDL, SABL, WDDL, DDPL

Here elaborated the static current traces by adding a Gaussian noise in order to take into account the on-chip noise. By using measurements to disclosure (MTD) approach the on-chip noise accounts also for all the other logic blocks which are instantiated on the chip and contribute to the overall static current consumption, but their power consumption is not correlated with the key. The LPA procedure was repeated increasing the noise standard deviation step by step. Using a maximum capacity of the attack equal to 100000 measurements [4],[5] .

By using 100000 measurements and averaging the noisy traces in order to reduce the noise for each plaintext, the correct key was disclosed up to a SNR almost equal to nearly -40dB [8],[9].

In Table I $\rho_{correct}$ is the value of the correlation coefficient of the correct key guess for 100000 measurements, which is a good estimation of the correlation when an unbounded attack is mounted (i.e., the value of the correlation coefficients calculated).

TABLE I. Actual security metrics for the DPL crypto-cores (SNR=-20 dB)

	MTD	$\rho_{correct}$	max $[\rho_{wrong}]$	G(N→ ∞)
CMOS	3072	0.529	0.431	1.227
WDDL	5440	0.578	0.479	1.207
MDPL	16880	0.545	0.489	1.115
SABL	3656	0.391	0.201	1.945

DDPL	>100000	0.009	0.516	~0

When the number of traces is high enough to obtain the convergence towards an asymptotical value. Instead$\max[\rho_{wrong}]$is the maximum asymptotical value calculated among all the wrong keys. The asymptotical gain G is calculated as the ratio between$\rho_{correct}$ and max $[\rho_{wrong}]$ and gives an estimation of the leakage resistance of an implementation.

TABLE II. Simulation results for the three basic gates with SABL and TDPL

	INV		**NAND/ AND**		**XOR/ NXOR**	
	SABL	**TDPL**	**SABL**	**TDPL**	**SABL**	**TDPL**
max(E)[fJ]	52.3	65.6	56.3	68.3	58.4	69.5
min(E)[fJ]	31.1	65.3	35.2	66.4	39.4	68.0
NED (%)	40	0.4	37.5	2.7	32.6	2.1
$\bar{E}$ **[fJ]**	41.7	65.5	50.5	67.3	48.9	68.7
σ_E **[fJ]**	10.9	0.1	8.0	0.6	8.5	0.4
NS D (%)	26.1	0.2	15.9	0.9	17.4	0.6

The energy per cycle

$$E = VDD \cdot \int_0^T IDD(t)dt \qquad (1)$$

is adopted as figure of merit to measure the resistance against power analysis attacks. The obtained results for the three analyzed gates are summarized in Table II, where the normalized energy deviation (NED) is defined as (max (*E*) −min (*E*))/ max (*E*) and NSD is the normalized standard deviation *σE/E*. As expected, SABL gates are sensible to unbalanced load conditions (NED>30%, NSD>15%) thus confirming that a balanced routing must be necessary employed to obtain a constant energy consumption. Vice versa, TDPL cells show an extremely balanced energy consumption (NED<3%, NSD<1%) in spite of unbalanced load capacitances.

From Table II, it follows that, as expected, an increase in the mean energy per cycle must be taken into account since both output lines are discharged in each cycle. On the contrary, the penalty in terms of silicon area is minimal (16% for the NAND/AND in Figure 3), especially if compared with what is reported for MDPL [1]. With respect to SABL, TDPL requires the routing of an additional signal (*discharge*). However, if at least four metal layers are available for signal routing, an increase in silicon area is not expected, especially in regular structures such as data-paths. Notice that MDPL is affected by a similar drawback due to the routing of the random data for masking. As expected, SABL and WDDL gates are sensitive to unbalanced load conditions (21.7%, 8.4%) thus confirming that a balanced routing must be necessary employed to obtain a constant energy consumption. Conversely, DDPL cells show extremely balanced energy consumption (0.7%, 0.2%) in spite of unbalanced load capacitances.

From Table III, it follows that, as expected, an increase in the mean energy per cycle must be taken into account since both output lines are discharged in each cycle. In terms of silicon area (see transistor count in Table III, DDPL [3],[16] shows a certain improvement with respect to SABL (25% for the NAND/AND) and a relevant advantage with respect to WDDL (60%). Compared to TDPL, lower area consumption is also expected since DDPL does not require the routing of additional control signals.

TABLE III.NAND-Comparison with SABL, WDDL and DDPL

	Balanced loads			**Unbalanced loads**		
	SABL	**WDDL**	**DDPL**	**SABL**	**WDDL**	**DDPL**
max(E)[fJ]	3 .121	8.613	3.756	4.615	10.24	5.375
min(E)[fJ]	2.958	7.983	3.720	2.958	8.014	5.337
ΔE[fJ]	0.163	0.630	0.036	1.657	2.223	0.038
NED	5.2%	7.3%	1%	35.9%	21.7%	0.7%
$\bar{E}$ **[fJ]**	2.989	8.261	3.739	4,195	9.491	5.358
σ_E **[fJ]**	0.041	0.176	0.010	0.699	0.801	0.011
NSD	1.4%	2.1%	0.3%	16.7%	8.4%	0.2%
TRANSISTORS	16	30	12	16	30	12

Therefore, a cryptographic core in DDPL can run at a low frequency having, in spite of that, a high resistance against DPA.

IV. CONCLUSION

A novel DPA-resistant dual-rail logic style based on a time domain data encoding and suitable to be used in a semi-custom design flow has been introduced and compared to the state of the art in the technical literature. The simulated energy consumption per cycle is up to 50 times more balanced than in the corresponding SABL gates without requiring any constraint on the geometry of the complementary wires. DDPL guarantees a level of protection against DPA similar to TDPL but it does require a single control signal as in a standard dual-rail precharge logic. In terms of area, DDPL is comparable to SABL and 60% smaller than WDDL. The introduced time domain data encoding allows setting the DPA-resistance independently from the operating frequency by choosing the delay parameter Δaccording to the expected resolution of current consumption measurements. Therefore the logic family DDPL has constant energy consumption even in presence of asymmetric interconnections and thus increasing the effectiveness of LPA attacks.

REFERENCES

[1]. T. Popp and S. Mangard, "Masked Dual-Rail Pre-charge logic:DPA resistance without routing constraints," in *Proc. CHES'05*, Scotland, UK, Sep. 2005, vol. 3659, pp. 172–186.

[2]. M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-Phase Dual- Rail Pre-Charge logic," in *Proc. Cryptographic Hardware and Embedded Syst.—CHES 2006, 8th Int. Workshop, Lecture Notes in Computer Sci. Springer*, Yokohama, Japan, Oct. 10–13, 2006.

[3]. M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay- Based Dual-Rail precharge logic," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 7, pp. 1147–1153, 2011.

[4]. M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: Well-defined procedure and first experimental results," in *Proc. Int. Conf. Microelectron. (ICM)*, 2009, pp. 46–49.

[5]. M. Djukanovic, L. Giancane, G. Scotti, and A. Trifiletti, "Impact of process variations on LPA attacks effectiveness," in *Proc. Int. Conf. Computer Elect. Eng. (ICCEE09)*, 2009, pp. 102–106.

[6]. M. Alioto, M. Poli, and S. Rocchi, "A general power model of differential power analysis attacks to static logic circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 18, no. 5, pp. 711–724,May 2010.

[7]. H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, and W. Zhang, "Masking the energy behavior of des encryption," in *Proc. IEEE Design, Automation Test Europe Conf. Exhibition— DATE*, 2003, pp. 84–89.Conf. (DAC), 2009, pp. 238–243.

[8]. M. Alioto,M. Poli, and S. Rocchi, "Differential power analysis attacks to precharged busses: a General analysis for symmetric-key cryptographic algorithms," *IEEE Trans. Dependable Secure Comput.*, vol. 7, no. 3, pp. 226–239, Sep. 2010.

[9]. J. Giorgetti, G. Scotti, A. Simonetti, and A. Trifiletti, analysis of data dependence of leakage current in CMOS cryptographic hardware," in *Proc. Great Lake Symp. VLSI (GSLVLSI 2007)*, Stresa, Italy, Mar. 11, 2007, p. 78.

[10]. L. Giancane, M. Jovanovich, G. Scotti, and A. Trifiletti, "Leakage power analysis of cryptographic devices implemented in nanometer CMOS technologies," in *Proc. Konferencija 9-a 07: Konferencija za Elektroniku, Telekomunikacije, Racunarstvo, Automatiku i Nuklearnu Tehniku, Herceg Novi (Montenegro)*, Jun. 2007, pp. 355–367.

[11]. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smartcard security under the threat of power analysis attacks," *IEEE Trans. Comput.*, vol. 51, no. 5, pp. 541–552, 2002.

[12]. S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York, NY, USA: Springer- Verlag, 2007.

[13]. K. Tiri and I. Verbauwhede, "Simulation models for side-channel information leaks," in *Proc. 42ndDesign Automation Conference (DAC)*, 2005, pp. 228–233.

[14]. K. Tiri and I. Verbauwhede, "A logic level design methodology for a secureDPAresistant ASIC or FPGA implementation," in *Proc.Design, Automation Test Eur. Conf. Expo. (DATE '04)*, 2004, pp. 246–251.

[15]. K. Tiri and I. Verbauwhede, "A digital design flow for secure integrated circuits," *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.*, vol. 25, no. 7, pp. 1197–1208, 2006.

[16]. Massimo Alioto, Simone Bongiovanni, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti, "Effectiveness of Leakage Power Analysis Attacks on DPA-Resistant Logic Styles Under Process Variations" IEEE transactions on circuits and systems—i: regular papers, vol. 61, no. 2, february 2014