Three-Phase Dual-Rail Pre-charge Logic

Marco Bucci[1], Luca Giancane[2],
Raimondo Luzzi[1], and Alessandro Trifiletti[2]

[1] Infineon Technologies AG
[2] University of Rome "La Sapienza"
{marco.bucci, raimondo.luzzi}@infineon.com
{giancane, trifiletti}@die.mail.uniroma1.it

Abstract. This paper investigates the 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. The proposed logic is based on a three phase operation where, in order to obtain a constant energy consumption over the operating cycle, an additional discharge phase is performed after pre-charge and evaluation. In this work, the proposed concept has been implemented as an enhancement of the SABL logic with a limited increase in circuit complexity. Implementation details and simulation results are reported which show a power consumption independent of the sequence of processed data and load capacitances. An improvement in the energy consumption balancing up to 100 times with respect to SABL has been obtained.

Keywords: DPA, dual-rail logic, SABL, security.

1 Introduction

Side channel attacks can reveal confidential data (i.e. cryptographic keys and user PIN's) exploiting the information leaked by the hardware implementation of cryptographic algorithms. In particular, power analysis attacks, simple and differential, are based on the fact that logic operations feature a power consumption profile dependent on the processed data: with simple statistical analyses of a sufficient number of power traces, the correlation between the circuit switching activity and the key material can be revealed [1,2,3,4].

In the recent years, a wide spectrum of countermeasures against differential power analysis (DPA) have been proposed in the technical literature. In a classification which takes into account the involved abstraction level during the design flow, three classes can be defined: system-level, gate-level and transistor-level countermeasures.

System-level techniques include adding noise to the device power consumption [5], duplicating logics with complementary operations [6], active supply current filtering with power consumption compensation [7], passive filtering, battery on chip and detachable power supply [8]. Notice that some of the mentioned countermeasures have a pure theoretical interest since, with the current

L. Goubin and M. Matsui (Eds.): CHES 2006, LNCS 4249, pp. 232–241, 2006.

state of the art, their employment to design tamper resistant cryptographic devices (e.g. chipcard microcontrollers) is limited by technological and cost constraints.

As gate-level countermeasures, techniques that can be implemented using logic gates available in a standard-cell library are intended, e.g. random masking [9], random pre-charging [10], state transitions and Hamming weight balancing, random delay insertion [11]. Random masking is the most studied but, as it has been recently proved [12,13], implementations in an automatic synthesis flow starting from a HDL description, can be still attacked exploiting glitches generated in the combinatorial networks when the random masks are applied.

Finally, the transistor-level approach is based on the adoption of a logic style whose power consumption is constant or independent of the processed data. In a dual-rail pre-charge (DRP) logic style (e.g. SABL [14], WDDL [15], Dual-Spacer DRP[16]), signals are encoded as two complementary wires and power consumption is constant under the hypothesis that the differential outputs of each gate drive the same capacitive load. Dual-rail pre-charge logics are not affected by glitches but building two balanced wires requires a full-custom approach thus increasing design and maintenance costs.

Recently, semi-custom design flows with support differential logic families have been proposed in the technical literature. An approach based on a technique for the automatic routing of balanced complementary lines is reported in [17]. Even if an automatic place and route could sensibly reduce design time and increase the portability, the proposed balanced routing technique does not take into account the dependence of the capacitive load on a line on the logic state of the adjacent wires and, furthermore, introduces additional constraints for the routing tool thus limiting its efficiency and, likely, causing an area overhead especially if only few metal layers are available for the inter-cell routing (as it is the case in a chipcard where the top layers are reserved for shielding). Moreover, in a modern deep sub-micron technology, intra-chip process gradients cannot be neglected and they are the limiting factor for the load matching accuracy.

A second approach proposed in [18] is based on a masked dual-rail pre-charge logic style (MDPL) where, due to the random masking at the gate level, power consumption is randomized. Moreover, since MDPL is a dual-rail pre-charge logic, 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. On the other hand, the authors report in [19] a significant penalty in terms of area and, above all, power consumption with respect to a CMOS implementation.

This paper proposes a further approach to the design of a dual-rail pre-charge logic family which is insensitive to unbalanced load conditions thus allowing adopting a semi-custom design flow (automatic place & route) without additional constraints on the routing of the complementary wires.

The proposed concept is based on a three phase operation where an additional discharge phase is performed after the pre-charge/evaluation steps typical of any dynamic logic style. Although the concept is general, it can be implemented as an improvement of the SABL logic with a limited increase in circuit complexity.

Implementation details and simulation results on a basic set of logic gates are reported in Section 2. A more complex case study is discussed in Section 3 and an extensive comparison with the corresponding SABL implementation is carried out.

2 The Proposed Logic Style

This paper proposes 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 V_{DD}, then (second phase - evaluation) the proper line is discharged to V_{SS} according to the input data, thus generating a new output data. Finally, during the last phase (discharge), the other line is discharged too. As a consequence, since both wires are pre-charged to V_{DD} and discharged to V_{SS}, a TDPL logic gate shows a constant energy consumption over its operating cycle (independent of the input data), even if unbalanced capacitive loads to V_{DD} and/or V_{SS} are taken into account.

The proposed approach can be implemented as an enhancement of the SABL logic style 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.

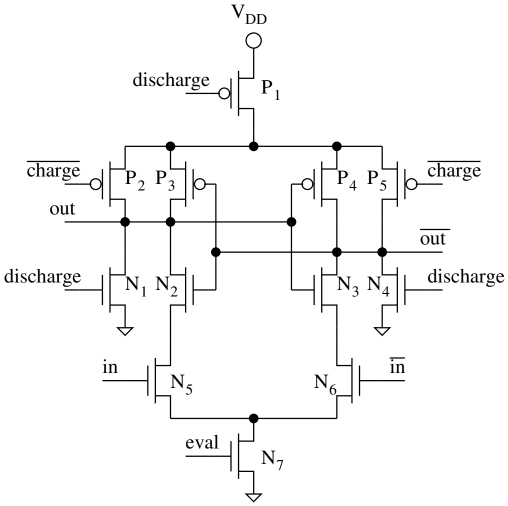

Fig. 1. TDPL inverter

With reference to the timing diagram shown in Figure 2, the circuit operation is the following:

1. charge: at the beginning of each cycle, signal *discharge* goes low, thus closing P1. Signal $\overline{charge}$ goes low too and both output lines are pre-charged to V_{DD}.
2. evaluation: during the charge phase new input data (in, $\overline{in}$) are presented to the circuit. On the raising edge of signal *eval*, N_7 is closed thus discharging one of the output lines according to the input data.
3. discharge: at the end of each operating cycle, input *discharge* is activated in order to pull down (through the additional pull-down transistors N_1, N_4) the output line which has not been discharged during the evaluation phase.

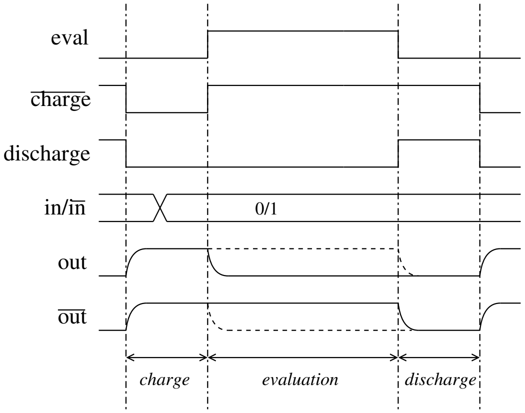

Fig. 2. Timing diagram of the TDPL inverter

More complex gates are obtained changing the pull-down logic. As an example, a 2-input NAND/AND and a XOR/NXOR are depicted in Figure 3.

This basic set of cells has been designed in a $0.12\mu m$ CMOS process from Infineon Technologies. A $1.5V$ supply voltage and a $200MHz$ operating frequency are adopted. Each transistor is designed with a width $W = 0.68\mu m$ and the minimum gate length $L = 0.12\mu m$ is assumed. Simulations are done in Spectre, using BSIM3v3 transistor models.

Table 1. Capacitive loads

	to V_{DD}	to V_{SS}
from *out*	$C_{out}^{VDD} = 8fF$	$C_{out}^{VSS} = 4fF$
from $\overline{out}$	$C_{\overline{out}}^{VDD} = 1fF$	$C_{\overline{out}}^{VSS} = 3fF$

In order to simulate the cells in a real operating condition, the testbench shown in Figure 4 has been defined where, each input to the gate under analysis is driven by a TDPL inverter and unbalanced load capacitances to V_{DD} (C_{out}^{VDD}, $C_{\overline{out}}^{VDD}$) and V_{SS} (C_{out}^{VSS}, $C_{\overline{out}}^{VSS}$) are assumed on the output lines (out, $\overline{out}$).

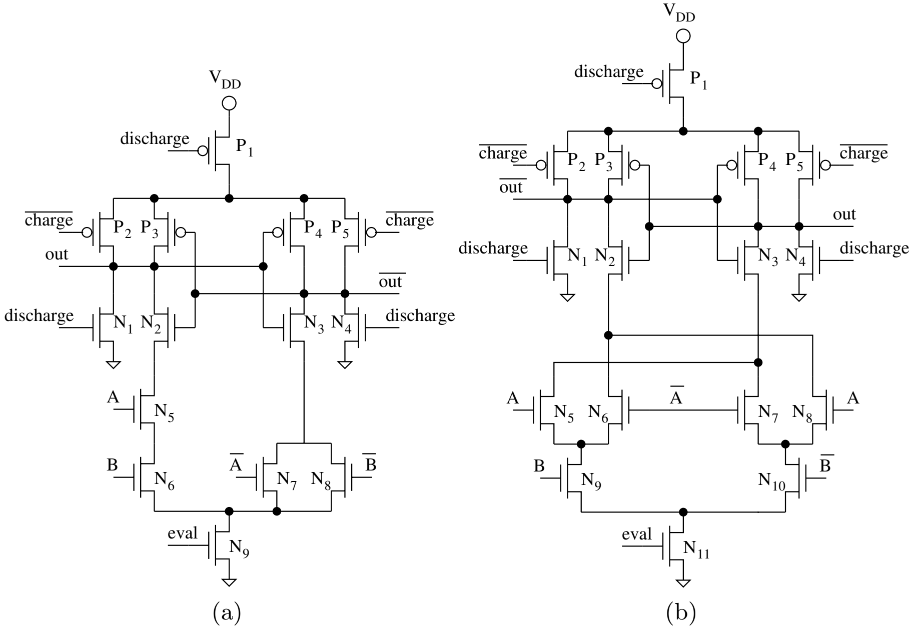

Fig. 3. NAND/AND (a) and XOR/NXOR (b)

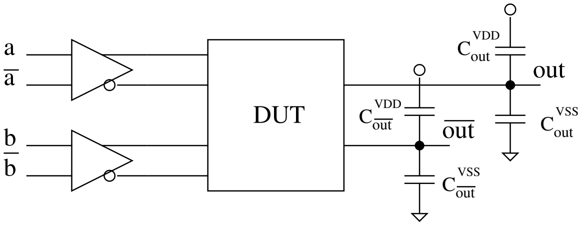

Fig. 4. Simulation testbench

Typical values for the parasitic interconnection capacitances in a standard-cell semi-custom layout are used (Table 1). The same testbench, with SABL inverters on the inputs, has been used to simulate the corresponding SABL cells. In both cases, only the current consumption of the gate under analysis is taken into account and every input data transition is simulated.

For the NAND/AND gate, a superimposition of the power supply current traces $I_{DD}(t)$ for the 16 input transitions is depicted in Figure 5. Both in the SABL and the TDPL cell, each operation phase can be clearly identified in the supply current profile. Notice that, in unbalanced load conditions, SABL cells show a data dependent current consumption during both pre-charge and evaluation. In the TDPL cells, the pre-charge current pulse is constant while a data dependency is visible in the evaluation and discharge phases.

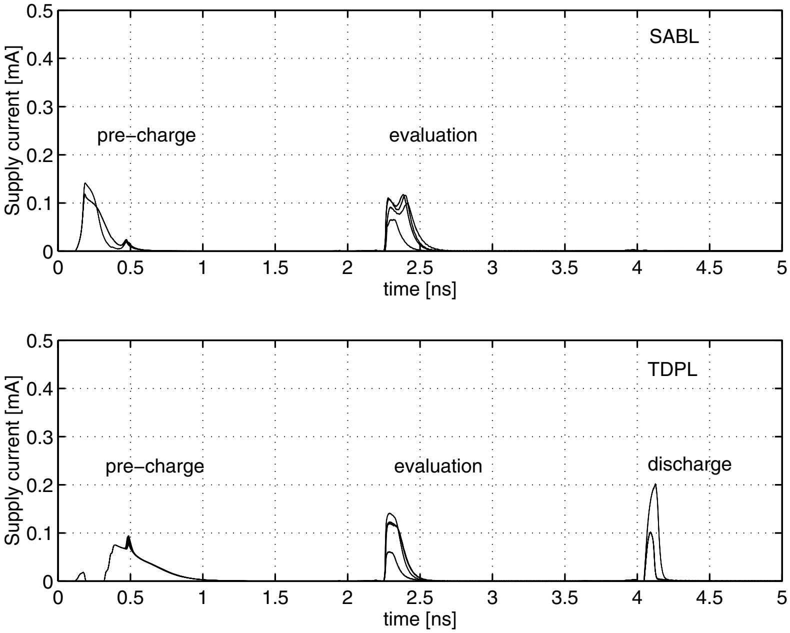

Fig. 5. NAND/AND - superimposition of the power supply current traces: SABL (above) vs. TDPL (bottom)

As in [14], the energy per cycle $E = V_{DD} \cdot \int_0^T I_{DD}(t)dt$ 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 2, where the normalized energy deviation (NED) is defined as $(\max(E) - \min(E))/\max(E)$ and NSD is the normalized standard deviation $\sigma_E/\overline{E}$. 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.

Table 2. Simulation results for the three basic gates

	INV		NAND/AND		XOR/NXOR	
	SABL[14]	This work	SABL[14]	This work	SABL[14]	This work
$\max(E)$[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	40.4%	0.4%	37.5%	2.7%	32.6%	2.1%
$\overline{E}$[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
NSD	26.1%	0.2%	15.9%	0.9%	17.4%	0.6%

From Table 2, 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 [19]. 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.

3 A Case Study

In order to confirm the results discussed in the previous section, a TDPL full adder designed as depicted in Figure 6 has been tested and compared with the

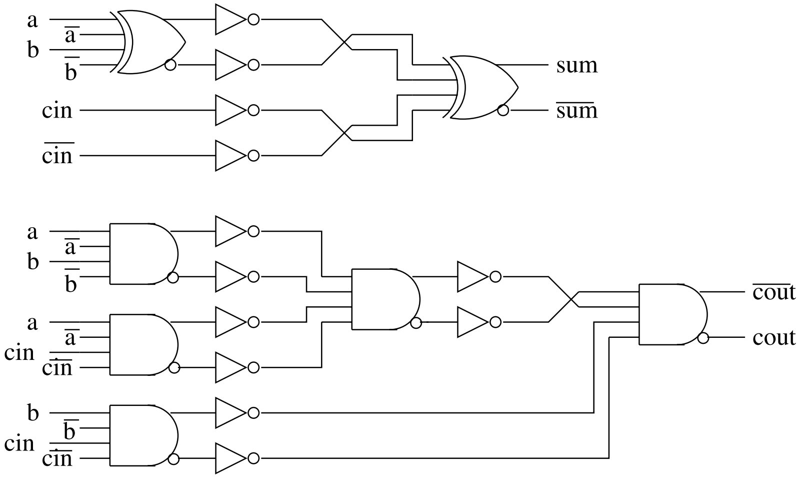

Fig. 6. TDPL full adder

Table 3. Simulation results for the FULLADDER

	FULLADDER	
	SABL[14]	This work
max(E)[fJ]	447.0	609.6
min(E)[fJ]	360.1	604.1
NED	19.4%	0.9%
$\overline{E}$[fJ]	405.6	606.8
σ_E[fJ]	22.1	1.3
NSD	5.4%	0.2%

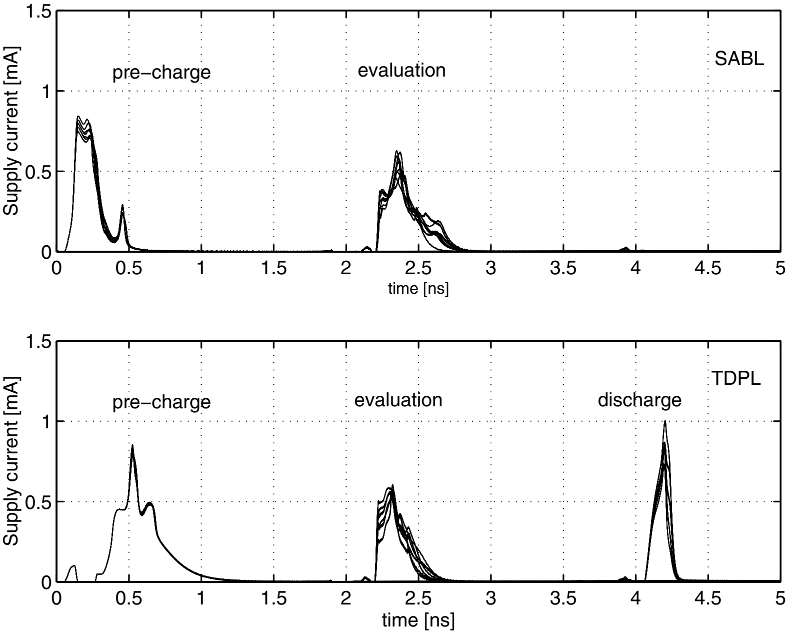

Fig. 7. FULLADDER- superimposition of the power supply current traces: SABL (above) vs. TDPL (bottom)

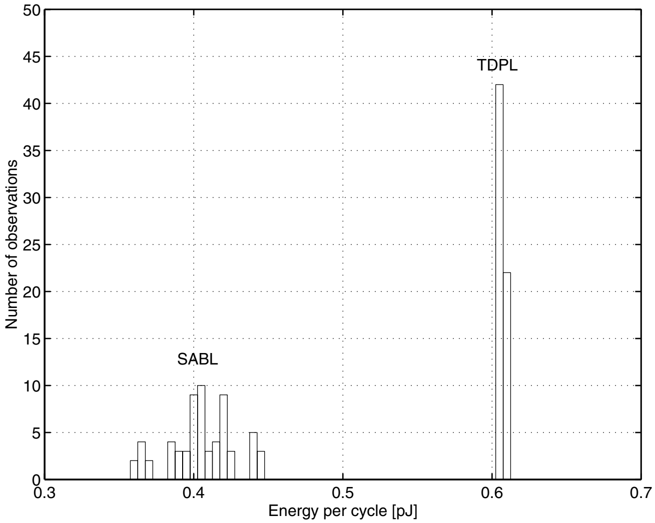

Fig. 8. FULLADDER - energy consumption per cycle: SABL vs. TDPL

equivalent SABL design. An implementation based on XOR/NXOR and NAND/ AND gates is employed and cascaded gates are connected using a Domino logic. The static inverters between two gates do not cause an unbalanced energy consumption because, in each cycle, both inverters on each couple of output wires switch two times (1-0 commutation during the pre-charge phase and a 0-1 event during either the evaluation or the discharge phase). On the contrary, in the SABL approach balanced interconnections between inverter and the following gate are necessary.

As done for the simulation of a single gate, unbalanced capacitances (Table 1) have been used on the output of each SABL/TDPL gate in order to model the routing parasitic capacitances. A superimposition of the power supply current traces $I_{DD}(t)$ for the 64 possible transitions of the 3-bit input $\{A, B, C_{in}\}$ is depicted in Figure 7 for both the SABL and the TDPL implementation.

A histogram of the observed energies per cycle reported in Figure 8 shows that TDPL guarantees a balanced energy consumption, independent of the processed data, even in presence of unbalanced interconnections. Results summarized in Table 3 confirm the improvement which has been obtained with respect to SABL.

4 Conclusions and Future Work

A novel DPA-resistant dual-rail logic style 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. Experimental results confirm that the proposed logic family shows a constant energy consumption even in presence of asymmetric interconnections. The simulated energy consumption per cycle is up to 100 times more balanced than in the corresponding SABL gates without requiring any constraint on the geometry of the complementary wires. At the same time, the penalty in terms of mean power consumption and silicon area is smaller than in the MDPL style thus representing a valid alternative approach in all the cases where the design and characterization of a new digital library can be afforded.

Further work on a TDPL storage element is planned. Actually, even if TDPL is compatible with SABL flip-flops, a memory element which supports the three phase operation allows to fully exploit the advantages of TDPL.

References

1. P. Kocher, J. Jaffe and B. Jun, *Differential power analysis*, Proc. Advances in Cryptology (CRYPTO '99), Lecture Notes in Computer Science, vol. 1666, Springer-Verlag, pp. 388-397, 1999.
2. T. S. Messerges, E. A. Dabbish and R. H. Sloan, *Examining Smart-Card Security under the Threat of Power Analysis Attacks*, IEEE Trans. Computers, vol. 51, no. 5, pp. 541-552, May 2002.
3. J. Coron, *Resistance Against Differential Power Analysis for Elliptic Curve Cryptosystems*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '99), Lecture Notes in Computer Science, vol. 1717, Springer-Verlag, pp. 292-302, 1999.
4. C. Clavier, J. Coron and N. Dabbous, *Differential Power Analysis in the Presence of Hardware Countermeasures*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '00), Lecture Notes in Computer Science, vol. 1965, Springer-Verlag, pp. 252-263, 2000.

5. L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, F. Pro, *Energy-aware design techniques for differential power analysis protection*, Proc. Design Automation Conf. (DAT '03), pp. 36-41, 2003.
6. H. Saputra, N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. Brooks, S. Kim, and W. Zhang, *Masking the energy behavior of DES encryption*, Proc. Design, Automation and Test in Europe Conf. (DAT '03), pp. 84-89, 2003.
7. G. B. Ratanpal, R. D. Williams and T. N. Blalock, *An On-Chip Suppression Countermeasure to Power Analysis Attacks*, IEEE Trans. Dependable and Secure Computing, vol. 1, no. 3, pp. 179-189, July-Sept. 2004.
8. A. Shamir, *Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '00), Lecture Notes in Computer Science, vol. 1965, Springer-Verlag, pp. 71-77, 2000.
9. J. Dj. Golic and R. Menicocci, *Universal Masking on Logic Gate Level*, Electronics Lett., vol. 40, no. 9, April 2004.
10. M. Bucci, M. Guglielmo, R. Luzzi and A. Trifiletti, *A Power Consumption Randomization Countermeasure for DPA-Resistant Cryptographic Processors*, Proc. Int.l Workshop on Power and Timing Modeling, Optimization and Simulation (PATMOS '04), Lecture Notes in Computer Science, vol. 3254, Springer-Verlag, pp. 481-490, 2004.
11. M. Bucci, M. Guglielmo, R. Luzzi and A. Trifiletti, *A Countermeasure against Differential Power Analysis based on Random Delay Insertion*, Proc. IEEE Int.l Symp. Circuits and Systems (ISCAS '05), pp. 3547-3550, 2005.
12. S. Mangard, T. Popp and B. M. Gammel, *Side-Channel Leakage of Masked CMOS Gates*, Proc. Cryptographers' Track at the RSA Conference (CT-RSA '05), Lecture Note in Computer Science, vol. 3376, Springer-Verlag, pp. 351-365, 2005.
13. S. Mangard, N. Pramstaller and E. Oswald, *Successfully Attacking Masked AES Hardware Implementations*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 157-171, 2005.
14. 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 28th European Solid-State Circuit Conf. (ESSCIRC '02), 2002.
15. K. Tiri and I. Verbauwhede, *A Logic Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation*, Proc. Design, Automation and Test in Europe Conference and Exposition (DATE '04), pp. 246-251, 2004.
16. D. Sokolov, J. Murphy, A. Bystrov and A. Yakovlev, *Improving the Security of Dual-Rail Circuits*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '04), Lecture Notes in Computer Science, vol. 3156, Springer-Verlag, pp. 282-297, 2004.
17. K. Tiri and I. Verbauwhede, *Place and route for secure standard cell design*, Proc. Smart Card Research and Advanced Application IFIP Conf. (CARDIS '04), 2004.
18. T. Popp and S. Mangard, *Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints*, Proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES '05), Lecture Notes in Computer Science, vol. 3659, Springer-Verlag, pp. 172-186, 2005.
19. T. Popp and S. Mangard, *Implementation Aspects of the DPA-Resistant Logic Style MDPL*, to appear in Proc. IEEE Int.l Symp. Circuits and Systems (ISCAS '06).