Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 52 (2012) 11344-11349

ISSN: 2229-712X

An efficient low power DPA resistant Delay-based Dual-Rail Pre-charge logic

Elakkiya A, M.Shobana, K.Prabharan and M.Maheshwari

Department of Electronics and Communication, J.J. College of Engineering and Technology, Trichy.

ARTICLE INFO

Article history:

Received: 25 July 2012;

Received in revised form:

30 October 2012;

Accepted: 5 November 2012;

Keywords

Cryptography,

Differential power analysis (DPA), dual-rail pre-charge logic(DRP),

Sense amplifier-based logic (SABL), wave dynamic differential logic (WDDL), security,

Three phase dual-rail pre-charge logic (TDPL).

ABSTRACT

Differential Power Analysis (DPA) has been shown to be an effective attack in cryptographic systems capable of revealing secret data by measuring power consumption. Recent DPA resistant circuits / logics incur severe penalties in terms of area and power. This paper proposes the design of a secure logic family for DPA resistant cryptographic devices. Here the power consumption is insensitive to unbalanced load conditions thus adopting a semi-custom design flow without any constraint on the routing of the complementary wires. The proposed logic is based on a novel encoding concept where the information is represented in time domain rather than in the spatial domain as in standard dual-rail logic. In this paper, a logic family exploiting the proposed concept is simulated to show power consumption independent of the processed data and routing capacitances. It also shows an optimistic improvement in the energy consumption balancing and area reduction.

Introduction

One of the biggest challenges of designers of cryptographic devices is to provide resistance against side-channel attacks. These attacks pose a serious threat to the security of implementations of cryptographic algorithms in practice, since they can disclose confidential data (i.e., cryptographic keys and user PINs) looking at the information leaked by their hardware implementation. Power analysis attacks extract secret information from an IC via measurement of the power consumption. In particular, differential power analysis (DPA), exploits the fact that digital circuits feature a power consumption profile dependent on the processed data: even small correlations between the circuit switching activity and the key material can be revealed by measuring the current consumption over repeated computations [1]–[3].

Previous Work

Since the introduction of DPA, several countermeasures have been proposed in the technical literature. System-level techniques include adding noise to the device power consumption [4], duplicating logic with complementary operations [5], active supply current filtering with power consumption compensation [6], passive filtering, battery on chip, and detachable power supply [7]. Though these countermeasures have a pure theoretical interest since, with the current state of the art, their employment is limited by technological and cost constraints.

As countermeasures that can be implemented using logic gates available in a standard-cell library, we can find random masking [8], random pre-charging [9], and random delay insertion [10]. Random masking is the most studied but, as it has been proved in [11], 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., sense amplifier-based logic (SABL) [12], wave dynamic differential logic (WDDL) [13], dual-spacer DRP [14]), 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. DRP logics are not affected by glitches but building two balanced wires requires a full-custom approach thus increasing design and maintenance costs.

Semi-custom design flows supporting differential logic families have been proposed in the technical literature. For instance, a technique for the automatic routing of balanced complementary lines has been introduced in [15]. Even if an automatic place and route could 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.

A second technique proposed in [16] 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 DRP logic, glitches are avoided and, at the same time, the complementary wires do not need to be balanced thus removing the main drawback of the dual-rail circuits. As reported in [17], a first implementation of MDPL showed a DPA leakage due to the early propagation of the input data with respect to the masking ones. The authors propose an improved implementation (iMDPL) where SR-latches are used to resynchronize the inputs thus forcing a combinatorial cell to evaluate only when all the inputs are in a valid differential state.

Tele:

E-mail addresses: elaks.ece@gmail.com

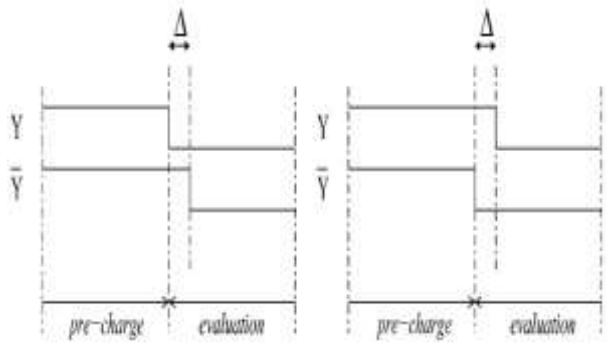

Fig. 1. Time domain data encoding. (a) Logic-1; (b) logic-0

The penalty with respect MDPL is a factor 3 and 1.5 in terms of area and power consumption, respectively.

A third solution has been reported in [18]: a logic insensitive to unbalanced routing capacitances is obtained by introducing a three-phase dual-rail pre-charge logic (TDPL) with an additional discharge phase where the output which is still high after the evaluation phase is discharged as well. Since both outputs are pre-charged to V_{DD} and discharged to V_{SS}, a TDPL gate shows a 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 has been also proposed which shows a lower overhead in terms of power consumption and area thus being suitable for embedded and mobile applications [19].

This paper proposes a novel approach to the design of a secure logic family which is based on a standard two-phase operation (pre-charge/evaluation) while being at the same time insensitive to unbalanced load conditions.

In the proposed logic family, the information is represented in the time domain by forcing a positive (logic-1) or negative (logic-0) relative delay between the differential lines. Therefore, as in TDPL, both outputs are pre-charged and discharged inside the operating cycles but, due to the chosen data encoding, a single control signal is sufficient as in a standard dual-rail logic.

Design details and simulation results on a basic set of logic gates are reported in Section III. A case study is discussed in Section IV and an extensive comparison with the corresponding SABL design is carried out. Finally, the design of a latch and a flip-flop is reported in Section V.

Proposed Logic Style

This paper proposes a delay-based dual-rail pre-charge logic (DDPL) which exploits the time domain data encoding shown in Fig. 1: during the pre-charge 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 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 and a XOR/NXOR which operate accordingly to the introduced data encoding are depicted in Fig.2. With reference to the timing diagram shown in Fig. 3, the NAND operation is the following:

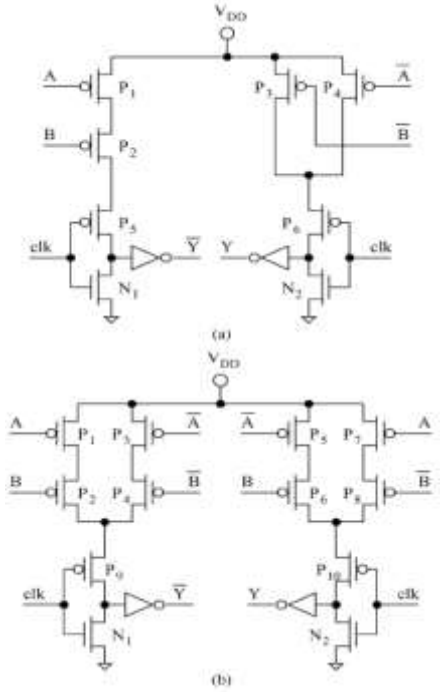

Fig. 2. (a) NAND/AND and (b) XOR/NXOR

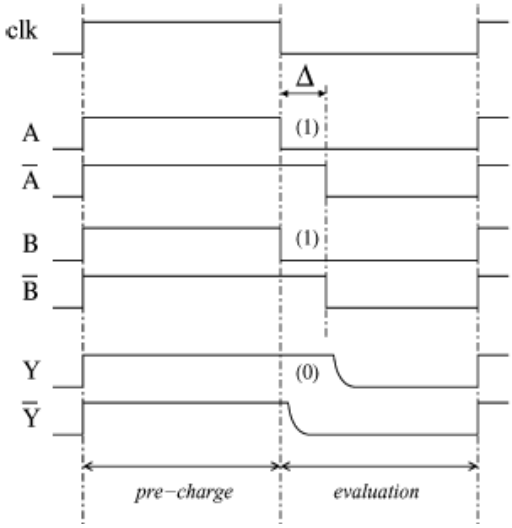

Fig. 3. Timing diagram of the DDPL NAND

1) *pre-charge:* at the beginning of each cycle , signal *clk* goes high, thus closing N_1 and N_2 and pre-charging both output lines to V_{DD}. Since during this phase the input lines are high (outputs from another DDPL gate), the pull-up logic is open.

2) *evaluation:* the new DDPL encoded input data(A,$\bar{A}$), (B, $\overline{B}$) are presented to the circuit on the falling edge of signal *clk*. Since A,B go low before $\overline{A}$, $\overline{B}$ (both inputs are logic-1's), the negated output $\overline{Y}$ is discharged before Y, thus generating a logic-0, as expected in a NAND gate.

The NAND operation for the other input combinations is similar.

In order to convert a single-rail CMOS data to the DDPL format, the converter shown in Fig. 4 is used: during the pre-charge phase (*clk* = 1), both outputs are charged to V_{DD} while, on the clock falling edge, they are discharged to V_{SS} forcing a delay Δ between them, accordingly to the single-rail input data A. If A = 1, Y = 0, and $\overline{Y}$ = 0 after a delay Δ. Conversely, for A = 0, $\overline{Y}$ = 0, and Y = 0 after a delay Δ. By construction, the CMOS-to-DDPL converter has a data independent current consumption.

In order to simulate the cells in a real operating condition, the testbenches shown in Fig. 5 have been defined where, each input to the gate under analysis is driven by the CMOS-to-DDPL converter. To simulate both balanced and unbalanced loads, a different number of CMOS inverter is used on the two outputs. The same testbench 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.

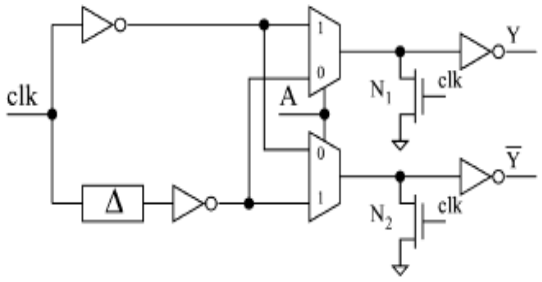

Fig. 4. CMOS-to-DDPL converter

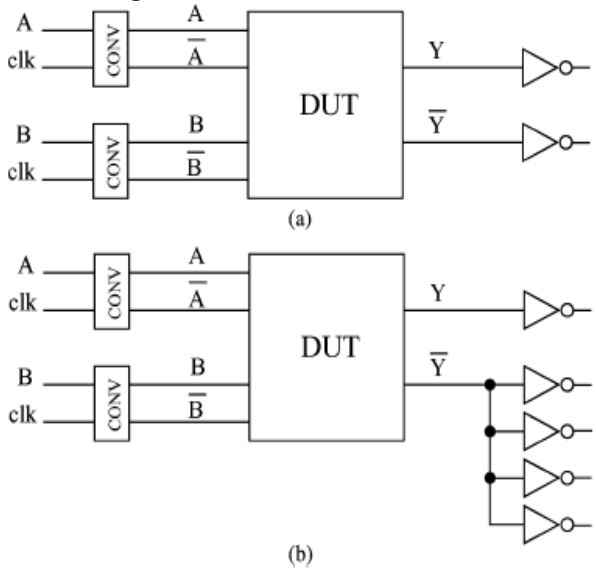

Fig. 5. Simulation testbenches: (a) balanced and (b) unbalanced loads.

For the NAND/AND gate, a superimposition of the power supply current traces $I_{DD}(t)$ for the 16 input transitions is depicted in Fig. 6 in case of unbalanced loads. In both the cells SABL and DDPL, 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 especially during pre-charge. In the DDPL cells, the pre-charge current pulse is almost constant. In the evaluation phase, two pulses are visible which correspond to the transitions at distance Δ=1 ns of the outputs lines.

Clearly, DDPL shows an advantage with respect to SABL since the two evaluation peaks at distance Δ = 1 ns must be resolved in order to detect a data dependency while, for SABL, resolving the pre-charge peak is sufficient.

In other terms, in a standard pre-charge logic like SABL, the operating frequency constraints the logic synthesis of the design and determines, at the same time, the achievable security level. On the contrary, in DDPL, the clock frequency does not fix the security since it depends on the delay Δ which must be chosen considering only the critical path t_{crit} of the design ($\Delta > t_{crit}$).

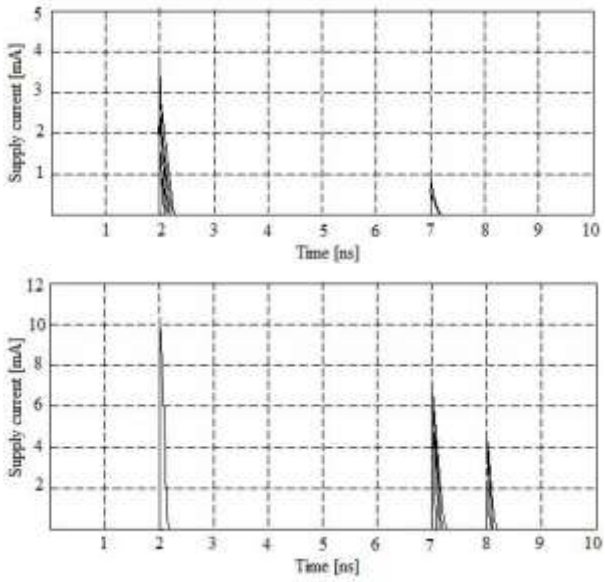

Fig. 6. NAND/AND—superimposition of the power supply current traces: (above) SABL versus (bottom) DDPL.

Table I
Simulation results of DDPL NAND and XOR gates

Parameters	Unbalanced loads		Balanced loads	
	NAND	XOR	NAND	XOR
Max (E) (pJ)	1042.5	1106	1042	1105
Min (E) (pJ)	900	920	910	920
ΔE (pJ)	142.5	186	132	185
NED	14%	17%	13%	17%
$\bar{E}$ (pJ)	974.43	1008.7	976.84	1015.6
σ_E (pJ)	43.733	51.85	35.325	55
NSD	5%	5%	4%	5%
# Transistors	12	16	12	16

Therefore, a cryptographic core in DDPL can run at a low frequency (for instance in a power constrained application) having, in spite of that, a high resistance against DPA.
As in [12], the energy per cycle

$$E = V_{DD} \bullet \int_0^T I_{DD}(t)dt \qquad (1)$$

is adopted as figure of merit to measure the resistance against power analysis attacks. The normalized energy deviation (NED) is defined as

$$NED = \frac{\max(E) - \min(E)}{\max(E)} \qquad (2)$$

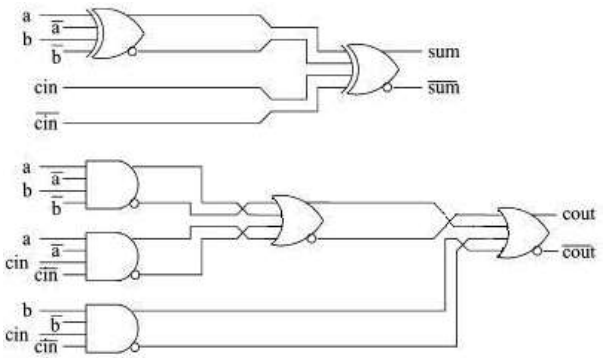

Fig. 7. DDPL full adder

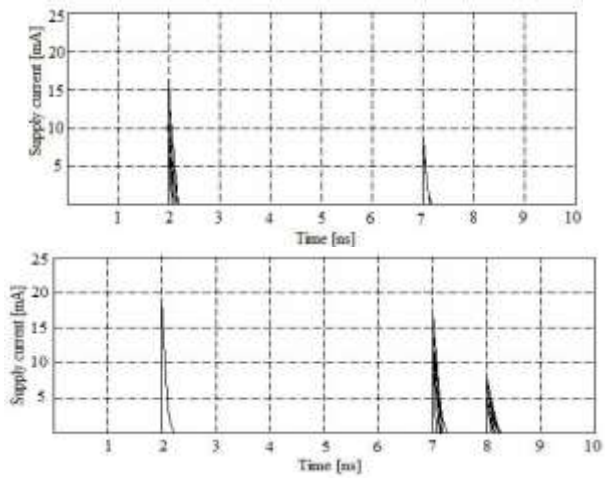

Fig. 8. FULLADDER—superimposition of the power supply current traces: (above) SABL versus (bottom) DDPL

Table II
NAND-comparison with SABL and WDDL

Parameters	Unbalanced loads			Balanced loads		
	SABL	WDDL	This work	SABL	WDDL	This work
Max (E) (pJ)	232.5	163.5	1042.5	235	143	1042
Min (E) (pJ)	75.5	20	900	86.5	20	910
ΔE (pJ)	157	143.5	142.5	148.5	123	132
NED	67.5%	87.7%	13.6%	63.19%	86%	12.66%
$\bar{E}$ (pJ)	143.156	70.28	974.43	145.37	64	976.84
σ_E (pJ)	45.43	40.59	43.733	42.85	35.9	35.325
NSD	31.73%	57.76%	4.48%	29.48%	56.1%	3.62%
# Transistors	16	20	12	16	20	12

and NSD is the normalized standard deviation

$$NSD = \frac{\sigma_E}{\bar{E}} \qquad (3)$$

The obtained results for the analyzed gates are summarized in Tables I and II. As expected, SABL gates are sensitive to unbalanced load conditions (NED > 67.5%, NSD > 31.73%) thus confirming that a balanced routing must be necessarily employed to obtain a constant energy consumption. Conversely, DDPL cells show an extremely balanced energy consumption (NED < 13.6%, NSD < 4.48%) in spite of unbalanced load capacitances (Table I).

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. In terms of silicon area (see transistor count in Table II), DDPL shows a certain improvement with respect to SABL (25% for the NAND/AND) and a relevant advantage with respect to WDDL. Compared to TDPL, lower area consumption is also expected since DDPL does not require the routing of additional control signals.

Table III
Simulation results of full adder

Parameters	Unbalanced loads		Balanced loads	
	SABL	This work	SABL	This work
Max (E) (pJ)	1386	2165	1320	2155
Min (E) (pJ)	963	1770	936	1600
ΔE (pJ)	423	395	384	555
NED	30.52%	18.24%	29.09%	25.75%
$\bar{E}$ (pJ)	1127	1956	1096	1939
σ_E (pJ)	104.5	92.59	86.51	105.4
NSD	9.3%	4.7%	7.9%	5.5%

Case Study

In order to confirm the results discussed in the previous section, a DDPL full adder designed as depicted in Fig. 7 has been tested and compared with the equivalent SABL design. It is based on XOR/NXOR and NAND/AND gates and cascaded gates are connected using a Domino logic where the static inverters are included inside the gates (see Fig. 2) and they do not cause an unbalanced energy consumption because, in each cycle, both inverters on each couple of output wires switch two times (0-1 commutation during the pre-charge phase and a 1-0 event during the evaluation).

On the contrary, in the SABL approach balanced interconnections between inverter and the following gate are necessary. As for the simulation of a single gate, balanced and unbalanced load conditions have been used on the outputs (Fig. 5).

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 Fig. 8 for both SABL and DDPL in the unbalanced case. Results summarized in Table III confirm the improvement which has been obtained with respect to SABL.

Flip Flop Design

The implementation of a data latch for the proposed logic style is based on the scheme shown in Fig. 9: the DDPL encoded data input is converted to a dual-rail CMOS format ($CONV^{-1}$) whose outputs are $\overline{set}$ / $\overline{reset}$ the inputs to a CMOS SR-latch. On the outputs, a CMOS-to-DDPL converter as in Fig. 4 is used to regenerate a DDPL data for the following combinatorial logic. A DDPL data flip-flop is obtained cascading two latches in master-slave configuration and it is shown if Fig. 10.

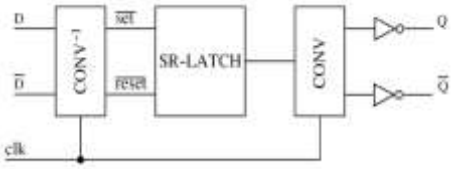

Fig. 9. DDPL latch

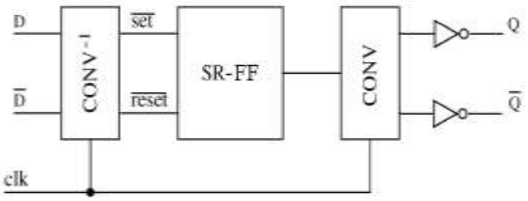

Fig. 10. DDPL Flip Flop

The input DDPL-to-CMOS converter and the corresponding timing diagrams of the DDPL latch are shown in Fig.11 (a) and (b) respectively: during the first semi-period of the clock signal *clk*, P_1 is open and the outputs $\overline{set}$ / $\overline{reset}$, are both forced high by N_1, N_4 (hold state for the SR-latch). On the clock falling edge, P_1 is closed, the outputs are released and the DDPL encoded input data ($A,\bar{A}$) is presented to the circuit. As soon as the first input line goes low, P_2 is closed and, depending on which input line goes low first, the corresponding output line goes low as well thus storing the correct logic value in the CMOS SR-latch. The cross-coupled nMOS transistors N_2, N_3 force the other output in the opposite logic state.

Since the input converter evaluation phase is driven by the input signals themselves, the proposed logic is insensitive to a skew on the clock signal *clk*, as long as it does not exceed Δ_f, where Δ_f is the final delay on the flip flop inputs.

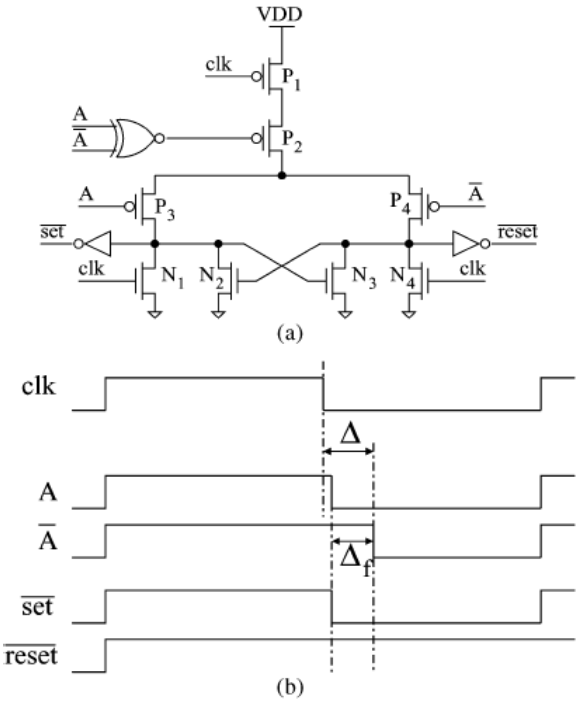

Fig. 11. DDPL-to-CMOS converter: (a)design and (b)timing diagram.

It is worth noting that NXOR gate in Fig. 11(a) switches two times in each cycle. Therefore, under the assumption that a symmetric full-custom layout is used for the internal interconnections, the DDPL flip-flop is by construction DPA resistant.

Conclusion

An efficient low power time domain data encoding based DPA-resistant dual-rail logic style that is 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. A set of combinatorial gates and a data flip-flop have been designed and simulated showing that the proposed logic family has constant energy consumption even in presence of asymmetric interconnections. The simulated energy consumption per cycle is more balanced than in the corresponding SABL gates. DDPL guarantees a level of protection against DPA similar to TDPL but it does require a single control signal. In terms of area, DDPL is comparable to SABL. The introduced time domain data encoding allows to set the DPA-resistance independently from the operating frequency by choosing the delay parameter Δ according to the expected resolution of current consumption measurements.

References

[1] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. Adv. Cryptology (CRYPTO)*, 1999, vol. 1666, Lecture Notes in Computer Science, pp. 388–397, Springer-Verlag .

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

[3] C. Clavier, J. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," in *Proc.Workshop Cryptographic Hardw. Embed. Syst. (CHES)*, 2000, vol. 1965, Lecture Notes in Computer Science, pp. 252–263, Springer-Verlag.

[4] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macii, and F.Pro, "Energy-aware design techniques for differential power analysis
protection," in *Proc. Des. Autom. Conf. (DAT)*, 2003, pp. 36–41.

[5] 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. Des., Autom. Test Eur. Conf. (DAT)*, 2003, pp. 84–89.

[6] G. B. Ratanpal, R. D. Williams, and T. N. Blalock, "An on-chip suppression countermeasure to power analysis attacks," *IEEE Trans. Depend. Secure Comput.*, vol. 1, no. 3, pp. 179–189, Jul.–Sep. 2004.

[7] A. Shamir, "Protecting smart cards from passive power analysis with detached power supplies," in *Proc. Workshop Cryptographic Hardw. Embed. Syst. (CHES)*, 2000, vol. 1965,Lecture Notes in Computer Science, pp. 71–77, Springer-Verlag.

[8] J. D. Golic and R. Menicocci,"Universal masking on logic gate level," *Electronics Lett.*, vol. 40, no. 9, pp. 526–528, Apr. 2004.

[9] M. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti, "A power consumption randomization countermeasure for DPA-resistant cryptographic processors," in *Proc. Int. Workshop Power Tim. Model., Opt. Simulation (PATMOS)*, 2004, vol. 3254, Lecture Notes in Computer Science, pp. 481–490, Springer-Verlag.

[10] M. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti, "A countermeas- ure against differential power analysis based on random delay insertion," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2005, pp. 3547–3550.

[11] S. Mangard, T. Popp, and B. M. Gammel, "Side-channel leakage of maskedCMOSgates," in *Proc. Cryptographers' Track at the RSA Conf. (CT-RSA)*, 2005, vol. 3376, Lecture Note in Computer Science, pp. 351–365, Springer-Verlag..

[12] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differentialCMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. IEEE 28th Eur. Solid-State Circuit Conf. (ESSCIRC)*, 2002, pp. 403–406.

[13] K. Tiri and I. Verbauwhede,"A logic design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Des., Autom. Test Eur. Conf. Expo. (DATE)*, 2004, pp. 246–251.

[14] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," in *Proc. Workshop Cryptographic Hardw. Embed. Syst. (CHES)*, 2004, vol. 3156, Lecture Notes in Computer Science, pp. 282–297, Springer-Verlag.

[15] K. Tiri and I. Verbauwhede, "Place and route for secure standard cell design," in *Proc. Smart Card Res. Adv. Appl. IFIP Conf. (CARDIS)*, 2004, pp. 143–158.

[16] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA- resistance without routing constraints," in *Proc.Workshop Cryptogra- phic Hardw. Embed. Syst. (CHES)*, 2005, vol. 3659, Lecture Notes in Computer Science, pp. 172–186, Springer-Verlag.

[17] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip, "in *Proc. Workshop Cryptographic Hardw. Embed. Syst. (CHES)*, 2007, vol. 4727, Lecture Notes in Computer Science, pp. 81–94, Springer-Verlag.

[18] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual--rail pre-charge logic," in *Proc. Workshop Cryptographic Hardw. Embed. Syst. (CHES)*, 2006, vol. 4249, Lecture Notes in Computer Science, pp. 232–241, Springer-Verlag.

[19] E. Menendez and K. Mai, "A high-performance, low-overhead, power analysis- resistant, single-rail logic style," in *Proc.IEEE Int. Workshop Hardw.-Oriented Security Trust (HOST)*, 2008, pp. 33–36.