A Power-Balanced Sequential Element for the Delay-based Dual-Rail Precharge Logic Style

Simone Bongiovanni, Mauro Olivieri, Giuseppe Scotti, and Alessandro Trifiletti

***Abstract*—Delay-based Dual-rail Pre-charge Logic (DDPL) is a logic style introduced with the aim of hiding power consumption in cryptographic circuits when a Power Analysis (PA) attack is mounted. Its particular data encoding allows to make the adsorbed current constant for each data input combination, irrespective of capacitive load conditions. The purpose is to break the link between dynamic power and data statistics and preventing power analysis. In this work we present a novel implementation of a dynamic differential master-slave flip-flop which is compatible with the DDPL data encoding. Efforts were made in order to design a completely dynamic master-slave architecture which does not require a conversion of the signals from dynamic to static domain. Moreover we show that the area occupied is also reduced due to a compact differential layout. Simulations performed using a 65nm-CMOS process showed that the proposed circuit exhibits good performance in terms of NED (Normalized Energy Deviation) and CV (Coefficient of Variation) of the current samples as required in transistor level countermeasures against power analysis, and it outperforms other previously published DPA-resistant flip-flops in the real case of unbalanced load conditions.**

***Index Terms*—Cryptography, Delay-based Dual-rail Pre-charge Logic (DDPL), Dynamic Flip-Flop, Dual-rail Precharge Logic, Power Analysis (PA), Power-Balanced Circuits, Sense Amplifier-Based Logic (SABL), VLSI design.**

I. Introduction

A side-channel attack is an attempt to recover confidential data, such as the secret key of a cryptographic algorithm, by exploiting the information leaked by the hardware implementation during the execution of the algorithm [1]. For this reason side-channel attacks represent a critical issue for cryptographic applications where a high level of security is required. Power analysis is a side-channel attack methodology which exploits the dependence of the dynamic power consumption of the hardware implementation on the switching activity and on the state of internal gates: both the switching activity and the input state of internal gates correlate to the processed data. Many techniques have been introduced to promote power analysis attacks, such as Differential Power Analysis (DPA) [2] and Correlation Power Analysis (CPA) [3], template attacks [4], collision attacks [5], Mutual Information Analysis (MIA) [6], and more recently Leakage Power Analysis (LPA) [7].

S. Bongiovanni, M. Olivieri, G. Scotti and A. Trifiletti are with the Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni (DIET) of the University "La Sapienza".

Several countermeasures at each abstraction level have been proposed in the literature [8] [9] [10]. Hiding (i.e. making constant) and masking (i.e. randomizing) dynamic power consumption are the most important ways for de-correlating power consumption and internal data. For this purpose novel logic families, namely the Dual-rail Pre-charge Logic (DPL) styles, were implemented either at cell or transistor level. Whereas the former led to the design of novel standard cell based logic styles for both FPGA and ASIC, the latter are adoptable only for ASIC. Each DPL logic family is based on a specific data encoding implemented through dynamic differential circuit architectures.

One of the most important issues in the design of DPLs for cryptographic applications is the implementation of a compatible memory element for a specific data encoding. First of all it is necessary to define some metrics for describing and comparing dynamic latches and flip-flops. Conventional timing metrics such as delay, setup and hold time are useful but not sufficient for this purpose [11] [12]. For instance, area is an important requirement because cryptographic modules must be as small as possible for running in embedded systems (e.g. smart cards), therefore an architecture with a differential and compact layout should be preferred. Power consumption is also critical because smart card power budget should be minimized. Yet, the standard deviation of the average power over a clock cycle should be as low as possible in order to meet the constraints for which a DPL has been designed (i.e. a constant power consumption). This has the side effect of implying the maximum power consumption for each input data combination. In addition, the design of each DPL circuit cannot neglect the need of balancing the internal nodes to avoid capacitive mismatches between differential lines [13], and of controlling the early evaluation effect, which refers to the different propagation times between signals [14]. Both represent well-known information leakage factors in all DPLs.

In DPLs a flip-flop is typically arranged in two differential master-slave stages of cascaded latches. In this architecture the clock frequency is doubled for achieving the same throughput as conventional CMOS [15]. The drawbacks are an increased power consumption and a complex structure, which are both justified by a higher level of immunity against power analysis attacks. In addition the setup and hold time of the latches must be appropriately evaluated.

Copyright © 2013 by Department of Microelectronics & Computer Science, Lodz University of Technology

Wave Differential Dynamic Logic (WDDL) [16] is one of the first gate-level countermeasures against power analysis compatible also with FPGA implementation. A WDDL cell is based on single-rail cells available in existing standard-cell libraries. Combinational cells are composed of two CMOS gates, one for each rail, which implement positive monotonic Boolean functions. This ensures the presence of one transition during a clock cycle for each data input. A combinational gate [16] is composed of a SR-latch at the output which aims at synchronizing the differential output signals after the evaluation. A WDDL flip-flop [17] is composed of two CMOS flip-flops on each rail which work simultaneously. Only sequential gates are connected to the clock signal, precharging and evaluating at the same time. The differential signals propagates along the combinational path, producing a wave. WDDL suffers both from time and capacitive mismatches due to the difficulty of balancing the internal gates. Several improvements have been presented for solving these drawbacks, both at logic [18] and layout level [19] [20].

Sense Amplifier Based Logic (SABL) [21] is a full custom DPL style. In SABL combinational and sequential gates are both implemented with a sense amplifier cell whose aim is to keep the charge during the whole evaluation period through a positive feedback. The first implementation of SABL flip-flop (SAFF) [22] was a master-slave configuration in which a SABL inverter is the master device and a static Set-Reset (SR) latch is the slave device. In this implementation the differential capacitances at the output of the latches exhibit different charging and discharging times. More specifically if the SAFF flip-flop stores the same value for two or more consecutive cycles, the latch will not switch and will maintain its state: consequently, there is no dynamic power consumption in the static latch and the flip-flop is vulnerable to power analysis. In [23] the authors proposed a fully dynamic master-slave configuration which solves this problem. Even if the dynamic master-slave implementation of the SABL flip-flop is effective to equalize the power consumption, nevertheless it suffers from the common drawback of SABL gates which exhibit a power consumption dramatically dependent on the capacitive load mismatches on differential pairs. This dependence forces the designer to manually route each differential line in order to guarantee a perfect balance of the capacitances.

An original solution for solving this problem is the Three-phase Dual-rail Pre-charge Logic (TDPL) [24]. This logic style is obtained by introducing an additional discharge phase on the output line which is still high after the evaluation. For this reason it is insensitive to unbalanced routing capacitances. Since both outputs are pre-charged to V_{DD} and discharged to 0, a TDPL gate shows a constant energy consumption over its operating cycle. A master-slave flip-flop similar to SAFF has been also proposed for TDPL style [25]. However the main drawback of TDPL is the additional area required for routing three control signals which represents a serious constraint for the layout.

Delay-based Dual-rail Pre-charge Logic (DDPL) has been presented as an improvement of TDPL [26]. It is based on a time domain data encoding and, as in TDPL, both outputs are charged and discharged once within the operating cycle, leading to a constant power consumption even if unbalanced capacitive loads are taken into account. In addition, and differently from TDPL, DDPL requires a single clock signal. For these reasons DDPL is suitable to be used in a semi-custom design as a standard dual-rail logic. In [26], the authors presented a DDPL SR-latch-based flip-flop which has been used to build a cryptographic hardware implementation as a case study. It is composed of two cascaded DDPL latches, which are in turn composed of three stages: the first stage is a converter; the second stage is a static Set-Reset latch which executes the sampling of the data; the third stage is a converter which resets the complementary lines into the DDPL domain. Similarly to the SAFF and the TDPL flip-flop, in the DDPL SR-latch-based flip-flop the conversion of a dynamic signal into the static CMOS domain is not the best choice for guaranteeing a constant power consumption. Moreover this implementation results in a large number of required transistors with a high power consumption.

The aim of this paper is to present a novel flip-flop compatible with DDPL, which overcomes the limitation of the above mentioned DPL flip-flops. We will show that our proposed implementation requires less area and a lower power consumption than the DDPL SR-latch-based flip-flop presented in [26], and at the same time the standard deviation of the distribution energy per each cycle is lower with respect to the WDDL and SABL configurations, thanks to the effectiveness of the DDPL data encoding.

II. The Delay-Based Data Encoding

DDPL data encoding differs from the Return to Zero (RTZ) protocol adopted in other DPLs, such as WDDL and SABL. RTZ logic families exhibit only a signal transition on one of the differential rails, whereas the other remains at the precharge value; DDPL is also precharged, but both signals of a differential pair are forced to V_{DD} during the evaluation phase. Specifically, the delay-based data encoding is characterized by two asynchronous evaluation sub-phases after the rising edge of the clock (evaluation phase), and the differential signals propagate asynchronously along a combinational path with an output delay time which depends on the propagation time of the logic. Thus the data encoding is not executed in the voltage domain, but in the time domain, and the information is encoded according to the order as the lines are charged.

Each DDPL cell has a differential complementary pair $(A, \overline{A})$, where A is defined as the asserted signal and $\overline{A}$ is the non-asserted. Fig. 1 shows the two possible logic values for a delay-based differential pair.

During the pre-charge phase the differential lines are set to 0 V and, in the evaluation phase, they are both charged to V_{DD} after the clock rising edge. For a logic-0 (Fig. 1a), the first line to be charged is $\overline{A}$. Conversely, for a logic-1 (Fig. 1b), the first line to be charged is A.

Since both lines are charged and discharged once over each operating cycle, the switching activity is always equal to 1 on each differential line for both input data. Moreover the capacitive mismatches between the complementary lines do not affect the balanced distribution of the current because each capacitance is always charged and discharged once during a clock cycle, unlike RTZ-based logics in which only one capacitance is charged and discharged in a cycle. Therefore the delay-based data encoding aims at equalizing the dynamic power consumption over a cycle irrespective of input data.

For understanding the working principle of a DDPL cell, a basic DDPL NOT/BUFFER gate is shown in Fig. 2 and the timing diagram of the processed signals in Fig. 3 for the case of logic-1.

The circuit is a DDPL n-type gate. We refer as n-type (p-type) to a dynamic circuit topology in which the evaluation network is the pull-down (pull-up). In a DDPL n-type circuit all complementary lines are forced to V_{DD} during the pre-charge phase. Moreover the gate is a Domino-type logic and the complementary outputs are pre-charged to 0.

Note that the output inverters exhibit no data dependence because in each clock cycle they perform the same transitions ($0\rightarrow1$ and $1\rightarrow0$ on complementary outputs).

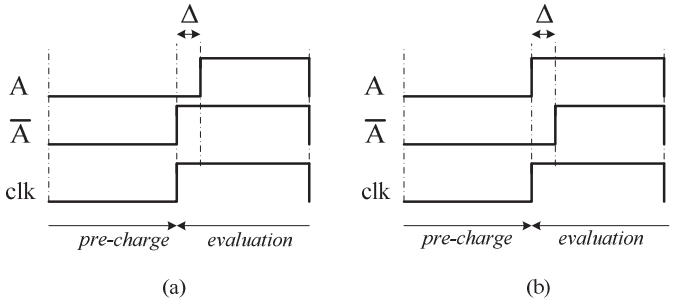

Fig. 1. Time domain data encoding. (a) Logic-0. (b) Logic-1.

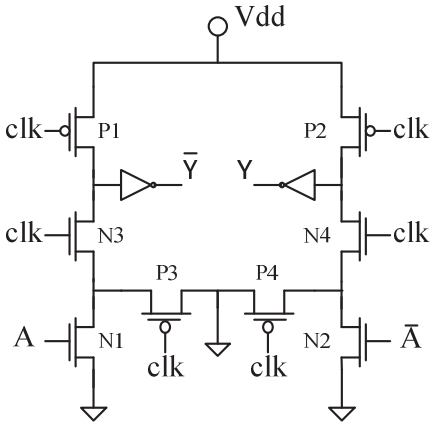

Fig. 2. A DDPL NOT/BUFFER gate

With reference to the timing diagram shown in Fig. 3 for a logic-1, the DDPL data operation is the following:

1) pre-charge: at the beginning of each cycle, *clk* is low and P1 and P2 are closed, pre-charging both output lines to 0. Since during this phase the input lines are low (outputs from another DDPL gate), the pull-down logic is open.

2) evaluation: the DDPL encoded input data $(A, \overline{A}) = (1,0)$ are presented to the circuit after the rising edge of signal *clk*. Since A goes high before $\overline{A}$, the output Y is charged after $\overline{Y}$, thus $(Y, \overline{Y}) = (0,1)$.

As demonstrated [26], in DDPL the clock frequency does not fix the security since it depends on the delay Δ between DDPL complementary lines; on the contrary in a RTZ logic the operating frequency constraints the logic synthesis of the design and determines, at the same time, the achievable security level.

In addition, DDPL is insensitive to unbalanced routing capacitances due to the presence of a pre-charge and an evaluation phase on both complementary lines, irrespective of input data. This ensures a constant energy consumption even if unbalanced capacitive loads are taken into account.

Note that for a DDPL gate, in general the input delay Δ_i is mapped into a different output delay Δ_o , namely $\Delta_i \neq \Delta_o$, because the propagation times of the evaluation differential paths and the differential load are different [27].

In [27], the authors state that if the evaluation network is adequately designed, it is possible to equalize the propagation times of the differential paths and produce an output delay Δ_o which is always lower than the input delay Δ_i . This way, by fixing a delay time Δ at the beginning of a combinational path, the value of Δ_o at the output of each cell cannot exceed the original value Δ.

In next section we describe the circuitry of the DDPL sequential circuit. The flip-flop samples the differential pair during the delay time Δ_i and regenerates a one-clock-cycle-delayed replica of the delay-based differential signals, with an output delay time Δ_o just equal to the original value Δ.

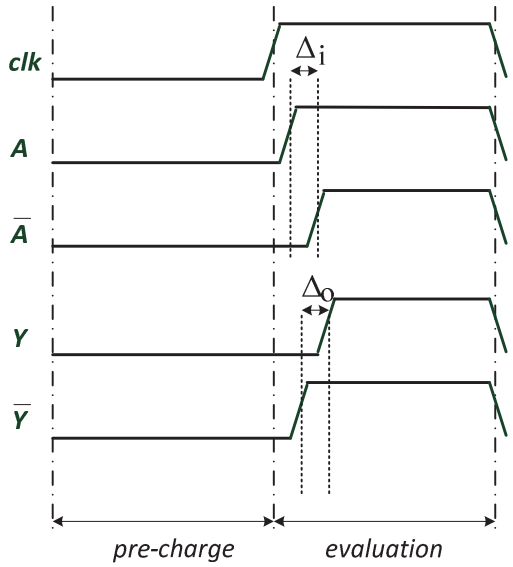

Fig. 3. Time diagram of the DDPL NOT/BUFFER signals (case of logic-1).

III. Architecture of the DDPL Master-Slave Flip-Flop

One important property of delay-based logic families is that two independent half circuits can be identified in a gate, which are activated in turn according to the arrival times of the delayed dual-rail signals. The block diagram of the proposed master-slave flip-flop is presented in Fig. 4. It is composed of three latches and two inverting delay blocks Δt on both paths.

In Fig. 5 the timing diagram of the input/output signals is shown. Signal *IN* represents the input data of the DDPL circuit encoded as a single-rail signal, which is converted in the delayed dual-rail pair $(D, \overline{D})$ by a converter at the input of the whole DDPL circuit (not shown). The signals $(D, \overline{D})$ are then regenerated after a clock cycle, as in other dynamic flip-flops.

The single blocks of the flip-flop and the role of the voltage V_{bias} will be described and explained in more detail in the following sections.

A. The input converter

The first stage is a converter, which is a self-timed pulse clock latch. The circuit is shown in Fig. 6. Basically it makes the conversion from the delay-based data encoding to the RTZ protocol. Similarly to the DDPL combinational gates, the architecture of the cell is differential and it is composed of two independent halves. The working principle of one half circuit is shown in Fig. 7: when *clk* is low, P1 is closed, the input capacitance of the inverter at internal node *v* is pre-charged, and the output line is forced to 0.

The input of the cell is a DDPL p-type signal pair which is sampled by the transmission gate N3-P3. The output of the CMOS XOR gate, which is implemented with a balanced differential architecture, is a pulse clock which drives the transmission gate: when *clkb* is high, which is possible only during the dynamic period Δ in which A and $\overline{A}$ are different from each other during the evaluation phase, N3-P3 (N4-P4) is closed and the datum is sampled. Only one of the two differential paths activates through the transmission gates. The capacitance C is discharged at the arrival of the first signal, and the output goes to V_{DD}, whereas C keeps its charge for the whole evaluation phase for the delayed signal.

The converter works like a dynamic latch in which the information is sampled by a transmission gate and the charge is hold on a capacitance for an half period. The timing diagram of the signals is shown in Fig. 8. It is worth noting that the static XOR gate is symmetric (i.e. it switches twice in each cycle), and it does not consume static power (Fig. 9).

B. The master latch

The cascaded master-slave latches in Fig. 4 work similarly as in the master-slave sense amplifier flip-flop [16]. However the gates are designed in a DDPL-like architecture and do not require a feedback on the output node as in conventional sense-amplifier logics. The p-type master latch shown in Fig. 10 takes as input a pair of RTZ signals sampled at the falling edge of the clock by the pass-transistor P3 (Fig. 11). This way the charge on the input capacitance C is stored for the following half period, in which the input converter and the slave latch are in precharge. The output of the latch is a pair of RTZ signals, as described in Fig. 12 where the time diagram of the processed data is shown.

C. The slave latch

The n-type slave latch shown in Fig. 13 has the aim of converting the RTZ signal into the DDPL domain: it takes as input the RTZ data and the clock signal, internally generates the Δ-delayed clock signal *clkd* through a Δ-block element, and produces the DDPL outputs by selecting them like a multiplexer. Note that the Δ-block element in Fig. 13 can be implemented with some cascaded CMOS inverters [26].

As described in the next section, an efficient low area implementation uses a current starved inverter in which the delay is controlled through a static voltage. This allows to obtain a fixed stable delay Δ avoiding a remarkable number of cascaded inverters.

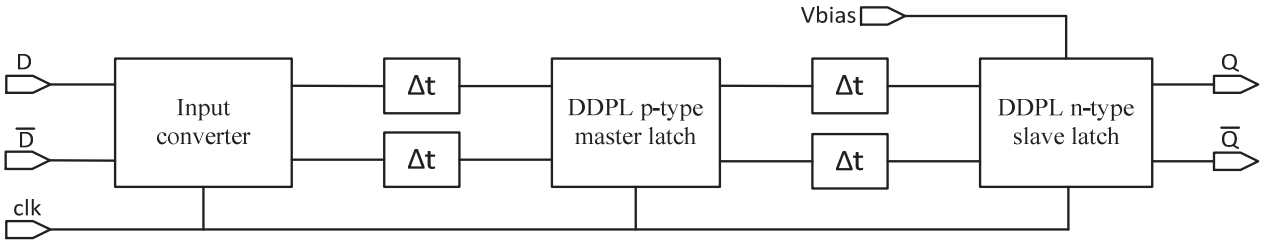

Fig. 4. Block scheme of the DDPL master-slave flip-flop.

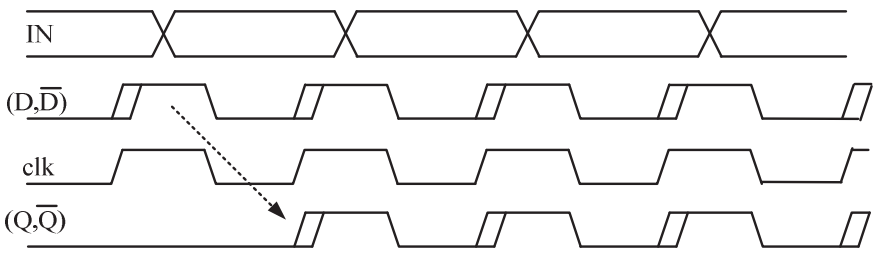

Fig. 5. Timing diagram of the signal processed in the DDPL master-slave flip-flop.

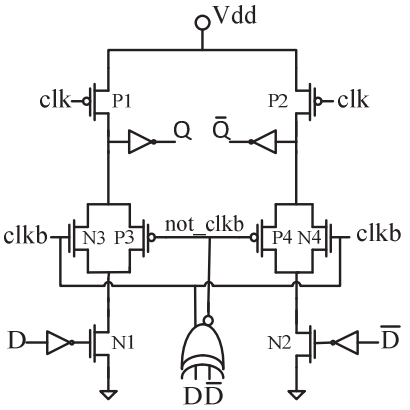

Fig. 6. DDPL-to-SABL converter.

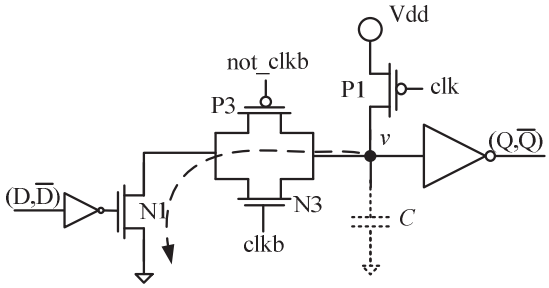

Fig. 7. Working principle of a differential half circuit of the converter.

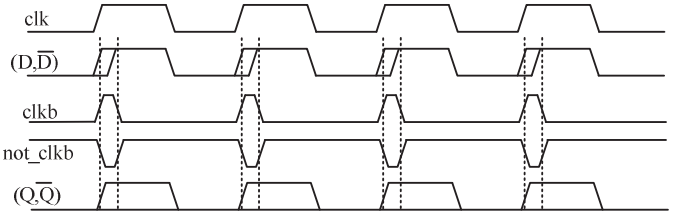

Fig. 8. Time diagram of the signals elaborated by the converter.

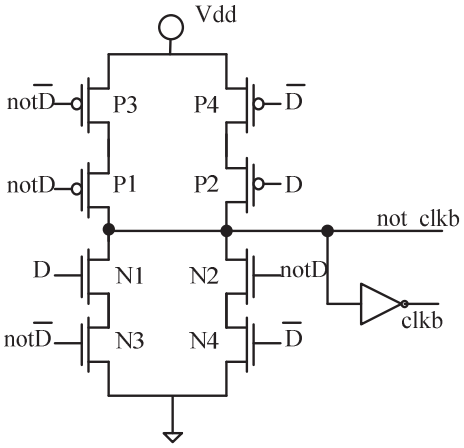

Fig. 9. Scheme of the differential XOR for the generation of the clock pulse.

This solution requires the routing of only a static voltage which represents an improvement with respect to TDPL style where a dynamic signal must be routed.

In Fig. 14 and in Fig. 15 the working principle of one half circuit of the slave latch and the time diagram of the signals are shown, respectively.

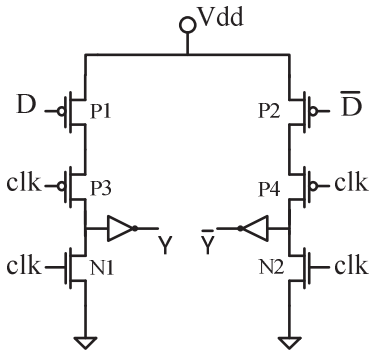

Fig. 10. DDPL p-type master latch.

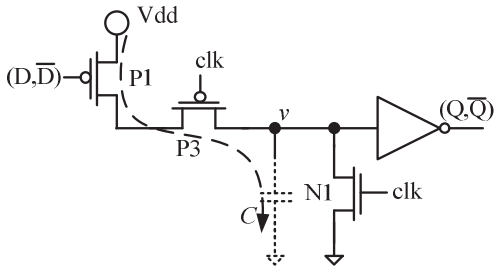

Fig. 11. Working principle of a differential half circuit of the master latch.

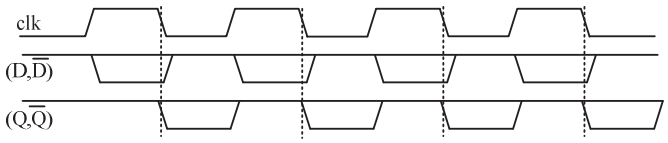

Fig. 12. Timing diagram of the signals elaborated by the master latch.

The task of the Δt blocks in Fig. 4 is to fix the hold time at the input of the latches by increasing the pre-charge phase duration of SABL signals [23]. They are implemented with an odd number of stages of cascaded CMOS inverters which aim at inverting the signals and adding a sufficient delay time. For our design three inverters are sufficient for meeting the requirement on the minimum hold time. Note that for circuits in which the clock skew is critical, the blocks Δt can be also replaced by current starved inverters and the static voltage required for generating *clkd* inside the Δ-blocks can be also routed for the blocks Δt. This helps to prevent early evaluation errors due to clock skews effects, which in the dynamic circuits can be critical, with no area overhead.

D. The delay element Δ

An important issue for the DDPL circuits is the implementation of the fixed delay Δ in the converter of Fig. 13 for the regeneration of the DDPL data encoding. A straightforward solution to implement this delay at circuit level is using a chain of inverter stages, but this solution is not area efficient, even for generating a Δ in the order of few hundreds of picoseconds. For instance, to obtain a Δ equal to 500ps, about 15 inverter stages would be required for a single flip-flop in a 65nm CMOS process, but it does not represent an optimized and low area solution.

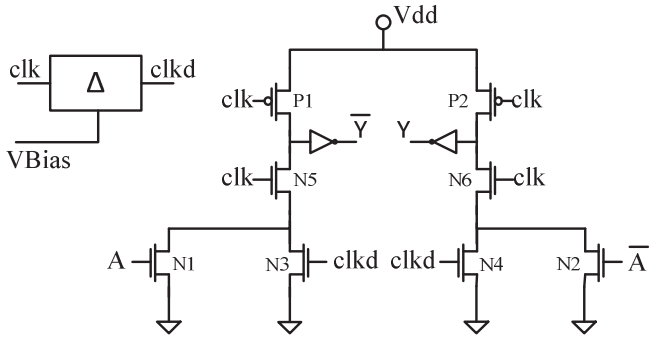

Fig. 13. RTZ-to-DDPL converter working as a n-type slave latch.

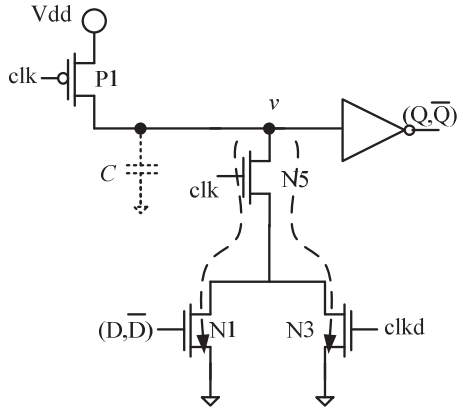

Fig. 14. Working principle of a differential half circuit of the slave latch.

An analysis of different circuit solutions to implement a constant delay at circuit level using CMOS technology is reported in [28]. Among the reported circuits, we selected the topology shown in Fig. 16 which is very simple and area efficient.

The circuit shown in Fig. 16 is composed of three blocks, where the first and third blocks are standard CMOS inverters, whereas the second one is a current starved inverter. This topology has been adopted because alternating a current starved inverter with basic inverters lowers the sensitivity of the delay to temperature and supply voltage variations, as reported in [29].

Note that the routing of a static voltage line Vbias can be adopted for controlling the delay of the current starved inverters. The routing of such static voltage signal can be avoided by generating Vbias locally (using two diode-connected MOS transistors), or by setting Vbias = 0 and sizing P2 appropriately (in this case a non-minimum gate length has to be used for P2).

Finally it has to be pointed out that if one wants to delay only the falling edge of the signals, transistor N2 in Fig. 16 is redundant and can be removed.

Since the output lines of the DDPL flip-flop exhibit a delay with respect to each other which is just equal to the original Δ, the proposed memory element works like a dynamic flip-flop (with a delay equal to one clock-period) in which the DDPL data integrity is regenerated at the output with the same speed penalty as in the other dynamic flip-flop with respect to a static implementation.

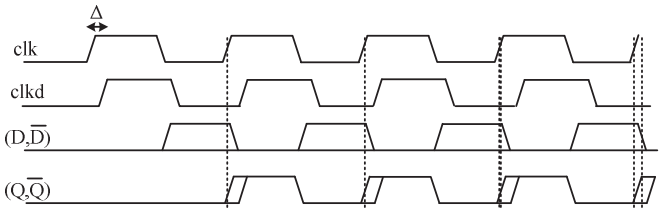

Fig. 15. Timing diagram of the signals elaborated by the slave latch.

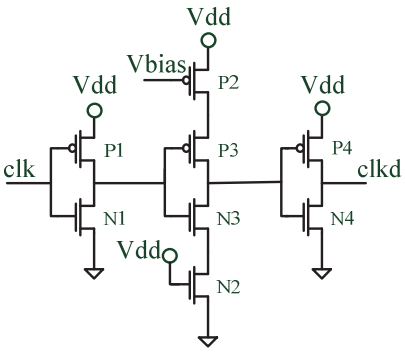

Fig. 16. Implementation of a delay element line based on a current starved inverter for the DDPL flip-flop.

The critical path of a DDPL logic is set by the number of combinational gates between two flip-flops as it happens in a standard non-time-encoded logic. This issue will be analysed in the next section.

IV. Timing Requirements and Area Overhead

A. Area and parasitics distribution

The fully differential architecture of the proposed flip-flop can be exploited to perform a very compact and symmetric layout, in order to have a very good balance of the parasitic capacitances and an equalized propagation of the signals on each internal differential pair. In particular the latter represents a critical issue for the internal section of the flip-flop, where RTZ signals are processed, and a differential and symmetric topology is required so that the routing does not introduce any capacitive mismatch.

A post layout analysis confirms a perfect balance between capacitances on the internal differential wires. The output complementary lines are the only ones that are expected to be mismatched due to the automatic routing, but this is not a limiting factor because output signals are encoded in the DDPL domain.

The layout (Fig. 19) was designed with Virtuoso XL Layout Editor by using the layout views of the BSIM4 low power standard-V_T (SVTLP) transistor models available in the STMicroelectronics 65nm-CMOS library. Three levels of metallization layers have been used for the interconnections. The design occupies an active area of about 61μm^2, that can be also reduced by further optimization, and.

B. Timing parameters

In this section the timing parameters of the master-slave DDPL flip-flop are discussed. In order for a DDPL circuit to work, an accurate timing analysis of the logic must be taken into account. Basically, DDPL is a synchronous dynamic

logic, however with an asynchronous evaluation phase which is strongly dependent on the propagation times of the dual-rail signals along the combinational logic units.

Combinational logics between the flip-flops differ according to the implemented functions of the logic gates, as shown in Fig. 17. In figure Δ_i represents the delay time between the differential signals processed by the flip-flop after propagating along the combinational logic *i* (*i* = 1, 2, ...). Each logic circuit is composed of two independent differential halves which have different propagation times, called T1 and T2 for the combinational logic 1 (T1' and T2' for the combinational logic 2). Therefore the actual delay time Δ_i at the input of a flip-flop is different from Δ.

Following the analysis reported in [27], the combinational circuits are designed in order to guarantee that Δ_i is always less than Δ. Thus the value of Δ_i for each combinational logic must be within the interval $I = [\Delta_{su}, \Delta]$, where Δ_{su} is the setup time of the flip-flop, whereas Δ is the original time delay which is chosen for guaranteeing a certain level of security of the logic.

The proposed flip-flop samples a datum during the delay time Δ_i at the rising edge of the clock, and regenerates it at the rising edge of the clock of the next cycle similarly to other DPL flip-flops. The delay time Δ_o of the delay-based dual-rail pair at the output of the flip-flop is just the original delay Δ. Namely the DDPL sequential element regenerates the data encoding, provided that the delay Δ_i is greater than Δ_{su}.

The setup time of the flip-flop defines the noise margin of a DDPL circuit and represents the minimum delay time Δ_i which allows flip-flop to correctly sample a delay-based pair.

Note that the flip-flop regenerates the delay-based signals at the rising edge of the clock in the subsequent cycle, therefore the propagation time is measured as the time between the rising edge of the clock signal and the rising edge of the regenerated signal (i.e. the first one of the delay-based pair) during the following clock cycle.

The hold time of the flip-flop is just the actual delay time Δ_i of the signals at the input of the flip-flop itself.

In order to measure the above defined timing parameters of the flip-flop, the testbench shown in Fig. 18 has been designed. The cells are placed side-by-side in order to consider also the parasitic capacitances of the CMOS-to-DDPL converter and the DDPL NOT/BUFF gate. The parasitic extraction of the layout leads to a mismatch factor equal to 1.8 (C_{L1} = 1.64 fF, C_{L2} = 2.9 fF). C_{L1} And C_{L2} model the total capacitances of the differential dual-rail wires due both to the parasitic and the cross-coupling effects. In the simulations we used a 1V supply voltage and a 10 MHz operating frequency, which is typical for cryptographic applications. The falling/rising edges of the clock and the data inputs were set to 20ps; the buffers were chosen from the above mentioned library. A dynamic delay Δ = 500ps for DDPL signals has also been adopted. Simulations were done in Cadence Spectre, using BSIM4 SVTLP transistor models with nominal process corners (Temp = 25°C).

With the above parameters, the setup time was estimated 85 ps. This values poses a limit on the maximum number of stages of a combinational logic before the flip-flop. The propagation time was estimated in about 130 ps. The proposed architecture also exhibits a good robustness to clock skews thanks to the internally generated self-timed pulse clock.

V. Power-Balance of the DDPL Flip-Flop

In this section we assess the power balancing ability of the DDPL flip-flop when a mismatch of the load capacitances is considered. A comparison will be executed among CMOS, WDDL, SABL, TDPL, and DDPL. As case study, a 4-bit register has been built for each of the logic styles under test. Before showing the results of the simulations, some metrics for comparing the performances of the flip-flops are recalled.

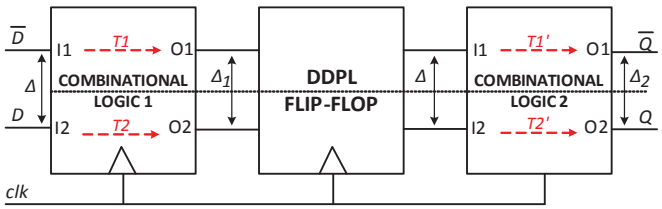

Fig. 17. Variation of the delay Δ along combinational logics.

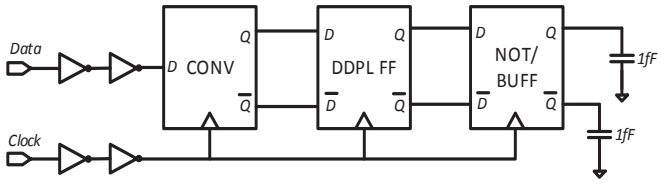

Fig. 18. Testbench for post layout simulations of the DDPL flip-flop.

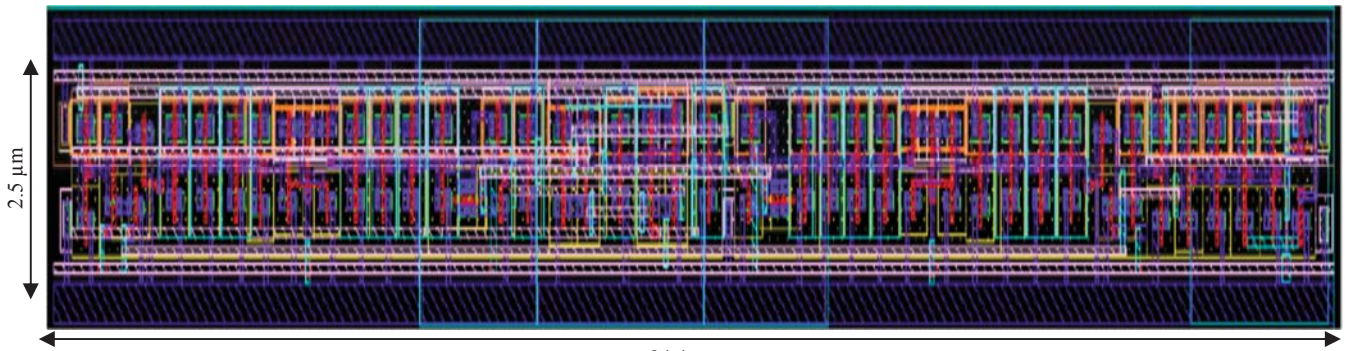

Fig. 19. Layout of the DDPL master-slave flip-flop.

A. Power-balancing metrics

The purpose of the DPLs is to break the physical link between the dynamic power consumption and the processed data. Thus, a DPL cell must charge/discharge the capacitive load with the same fixed amount of charge over a cycle. This way the current adsorbed from the power supply is almost constant for each input data, and this prevents any leakage source on power consumption. Similarly to the combinational gates, sequential elements implemented for DPL styles must balance the instantaneous current without requiring too large area and average power.

For this reason the power-balancing ability of the flip-flops is compared using the Normalized Energy Deviation (NED) and Normalized Standard Deviation (NSD). Energy per cycle, NED and NSD are calculated as [16]:

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

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

$$NSD = \frac{\sigma_E}{E_{AV}}. \tag{3}$$

E_{AV} and σ_E are the average and the standard deviation of the distribution of the energies per cycle respectively, calculated for a number *N* of inputs where all possible data transitions are considered. The energy per cycle has been calculated measuring the adsorbed current $I_{DD}(t)$ on the V_{DD} pin and integrating it in a clock cycle.

Practical hardware implementations are typically characterized by the presence of a low pass filter on the power supply line, therefore NED and NSD are useful for determining if a DPL cell is able to balance the current consumption in a clock cycle or not. The slower are NED and NSD, the better is the power-balancing ability of the gate.

However these metrics give information on the average current adsorbed in a clock cycle, but they do not give information on how much each time sample of the instantaneous current trace is scattered according to the data transitions.

Specifically, even in presence of a low energy deviation, few current samples could exhibit a dependence on data which could be exploited by DPA/CPA attacks for extracting information on processed data. This is an important issue which must be adequately addressed for designing power-balanced dynamic sequential elements for counteracting power analysis attacks.

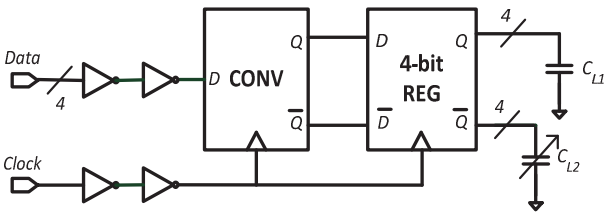

Fig. 20. Testbench for the simulation of the DPL 4-bit registers.

Even if each node of a dual-rail precharge combinational logic is well balanced and no leakage is detectable through a power analysis, registers represent an important information leakage source, and in a power-balanced circuit the number of leaking samples must be reduced as much as possible.

For this purpose a good statistical gauge for assessing the dependence of the instantaneous adsorbed current on the input pattern [30] is the coefficient of variation CV which represents a normalized measure of the dispersion of the set of current samples.

CV is calculated as the ratio between the standard deviation and the mean of the set of the current samples at each time instant. In the case under consideration, the larger is the coefficient of variation at a certain time sample, the larger is the dependence of the current on the input values.

Stated that some leakage is expected, a well power-balanced sequential element exhibits low NED and NSD, and the shortest possible time interval of high CV. This way the side-channel due to the power consumption can be reduced.

B. Testbench and simulation parameters

The testbench for the simulations is defined in Fig. 20. Each DPL register requires a specific conversion of the one-rail input signal according to its data encoding, whereas the differential output load is represented by some capacitances which have been increased up step-by-step in the simulations. As reported in Table I, the capacitance C_{L1} is fixed at 2fF for the asserted lines, whereas C_{L2} has been changed in the range 2fF to 10fF with a step size equal to 2fF for the non-asserted lines, so to simulate different levels of mismatch. The Mismatch Factor (MF) is defined as the ratio of C_{L2} and C_{L1}.

A 1V supply voltage and a 10 MHz operating frequency are used. In order to simulate the cells in a real operating condition, the falling/rising edges of the clock and the data inputs were set to 20ps, and in the design all signals were driven by buffers from the above mentioned library. A dynamic delay Δ_i = 500ps for DDPL input signals has also been adopted. Simulations were done in Cadence Spectre, using BSIM4 SVTLP transistor models with nominal process corners (Temp = 25°C).

TABLE I.
CAPACITIVE LOAD AND MISMATCH FACTOR FOR PARAMETRIC SIMULATIONS OF THE REGISTERS.

C_{L1} [fF]	C_{L2} [fF]	MF = C_{L2}/C_{L1}
2	2	1 (no)
2	4	2 (low)
2	6	3 (moderate)
2	8	4 (high)
2	10	5 (extreme)

C. Comparison to other flip-flops for DPLs

Input data were chosen in order to consider all possible transitions inside the logics. The results (i.e. the time samples representing the current adsorbed for each clock cycle under unbalanced load conditions) are reported in Fig. 21 to Fig. 26, where the superimposition of the current traces in a clock cycle is depicted for each of the registers under analysis. The traces were sampled with a time period equal to 1ps, which for a clock cycle corresponding to 100ns leads to 10^5 time samples.

A CMOS register designed with standard flip-flops (with minimum fan-out) from the library SVTLPCORE65 of the STMicroelectronics 65nm CMOS design kit has been adopted as benchmark for the simulations.

The electrical schemes of the flip-flops under test were extracted from the literature.

In order to have a fair comparison, all transistors have been designed with minimum sizes (L = 65nm, W = 135nm) so to guarantee at the same time the lowest occupation of area and the correct working of the logic. All the Domino inverters in the flip-flops and the XOR gate in the DDPL flip-flops have been sized using the values for the minimum fan-out found in the above mentioned technology library.

In Fig. 27 to Fig. 32 the curves of the coefficient of variation as a function of the time samples are shown. The figures capture the normalized variance of the current traces for each time sample. As expected, the standard CMOS register exhibits an high unbalance for the whole evaluation phase. For what concerns the DPL flip-flops, figures refer to the case of a moderate mismatch occurring on the differential output capacitances (MF = 3), which is a reasonable value for the interconnection wires resulting from an automatic routing.

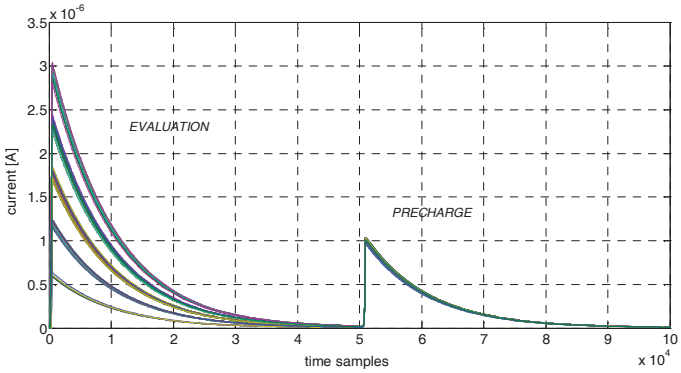

Fig. 21. Superimposition of the current traces for all possible input data in a CMOS 4-bit register (MF = 3).

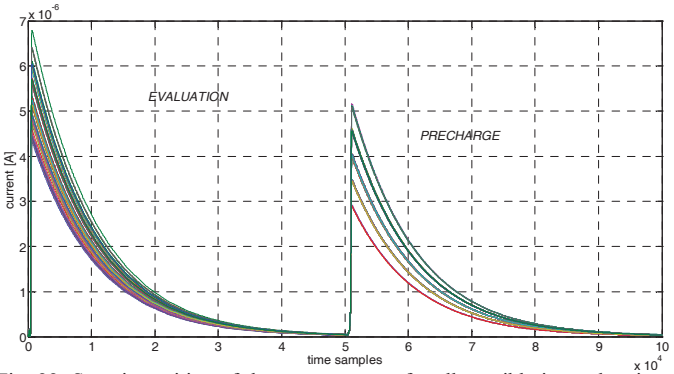

Fig. 22. Superimposition of the current traces for all possible input data in a WDDL 4-bit register (MF = 3).

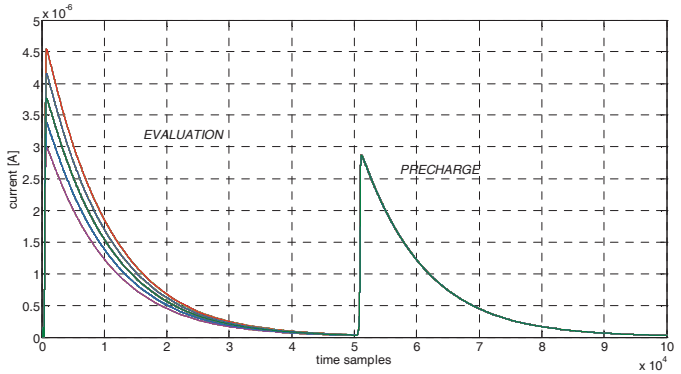

Fig. 23. Superimposition of the current traces for all possible input data in a SABL 4-bit register (MF = 3).

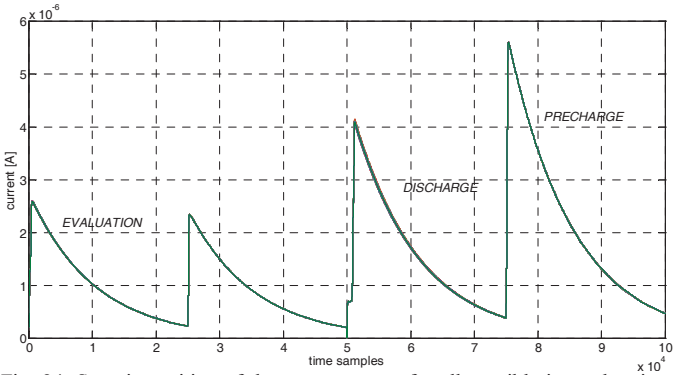

Fig. 24. Superimposition of the current traces for all possible input data in a TDPL 4-bit register (MF = 3).

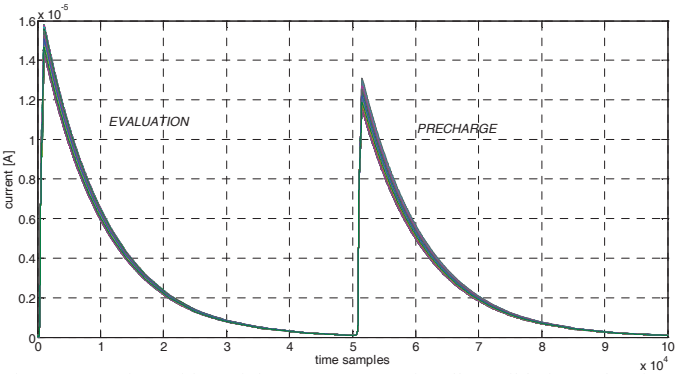

Fig. 25. Superimposition of the current traces for all possible input data in a DDPL 4-bit register implemented with SR-latch-based flip-flops (MF = 3).

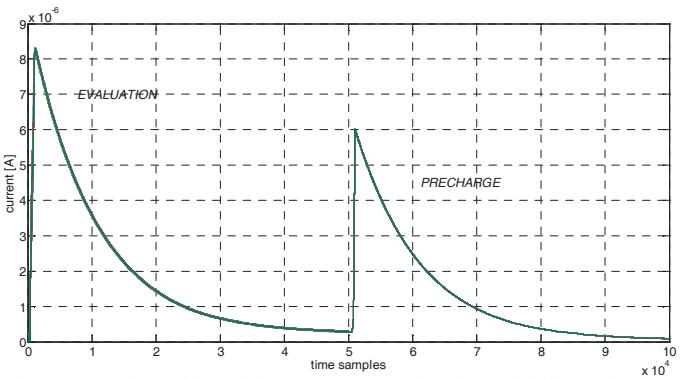

Fig. 26. Superimposition of the current traces for all possible input data in a DDPL 4-bit register implemented with master-slave flip-flops (MF = 3).

The coefficient of variation grows according to the increase of the MF of the differential capacitances during the evaluation phase for WDDL and SABL flip-flops, amounting to high values already for a low MF. For the WDDL register an increase also occurs during the precharge phase.

Instead the variance of the current traces is very low in TDPL and DDPL flip-flops for the whole clock cycle. For these logic styles the CV remains almost constant regardless of variations of the mismatch factor. This confirms that TDPL and DDPL exhibit an exceptional power-balance even in presence of an extreme capacitive mismatch.

The peak in the amplitude of CV is a transient effect which depends on the commutation of the clock and is not data-dependent, therefore it can be neglected.

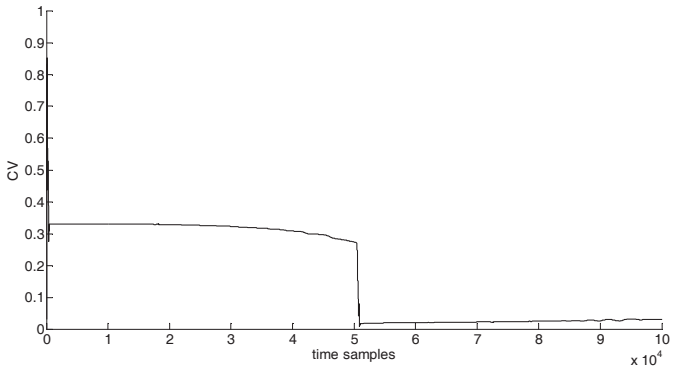

Fig. 27. Coefficient of Variation (CV) for the CMOS 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

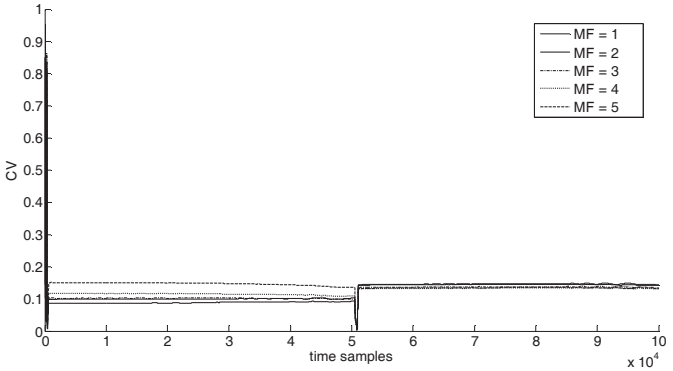

Fig. 28. Coefficient of Variation (CV) for the WDDL 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

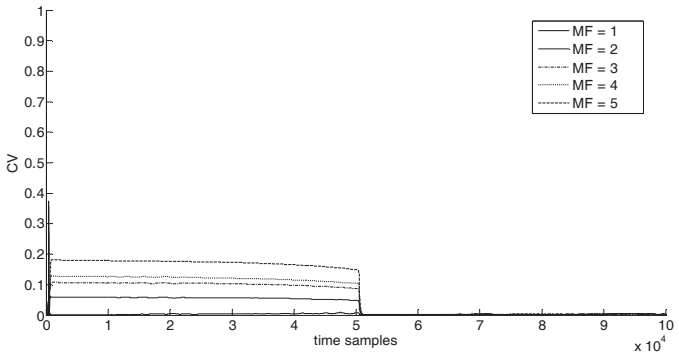

Fig. 29. Coefficient of Variation (CV) for the SABL 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

Actually the DDPL flip-flop exhibits a residual information leakage which could be detectable in a time period just equal to the value of Δ_i, as shown in Fig. 33. During this time window a slight data-dependence of the current still remains, and the amplitude of the CV curve depends on the mismatch factor. As stated in previous section, the time period Δ_i does not exceed the original Δ. In simulations it is equal to 500ps, and in current technologies it is in the order of some hundreds of picoseconds (but always higher than the setup time).

For capturing these leakage points, a resolution higher than 2GSamples/s is required. This sampling rate can be reached using oscilloscopes with an high bandwidth, which typically are not adopted in an actual low cost measurement setup for power analysis attacks [26].

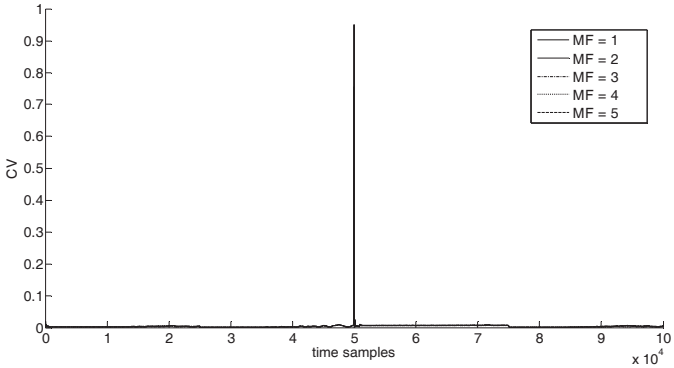

Fig. 30. Coefficient of Variation (CV) for the TDPL 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

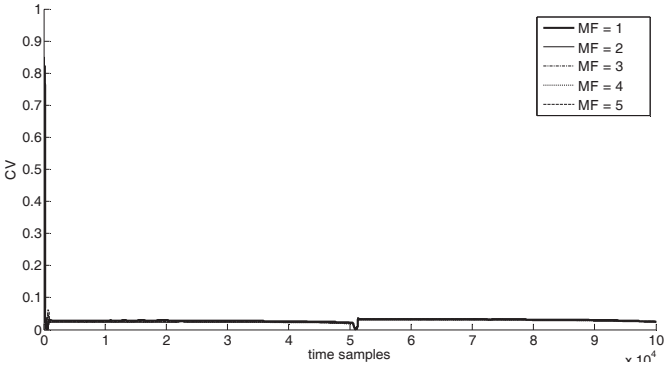

Fig. 31. Coefficient of Variation (CV) for the SR-latch-based DDPL 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

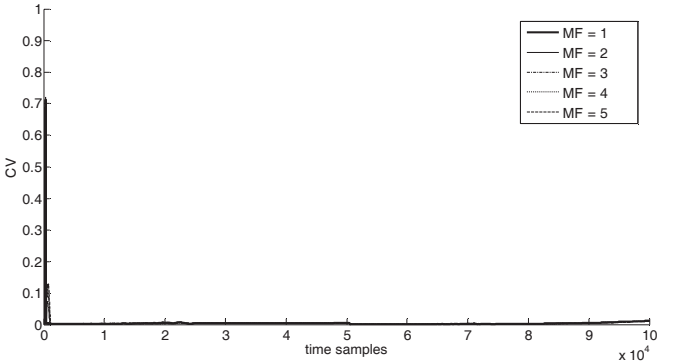

Fig. 32. Coefficient of Variation (CV) for the master-slave DDPL 4-bit register as a function of the time samples in a clock cycle under different mismatch factors.

Instead for the DPL implementations based on the RTZ protocol, the state of the flip-flop is kept by a feedback structure (i.e. SR or sense amplifier latch), and this leads to a strong dependence of the current traces on the processed data, causing the enlargement of the duration of high CV amplitudes. In these circuits the leakage is distributed in a time window comparable to the clock period and easily detectable.

The dynamic working principle of the proposed flip-flop allows to exploit the benefits of the delay-based data encoding, in which data are processed in a time period that is long enough for sampling the delay-based dual-rail signals, but at the same time too short for detecting the state of the latch. Therefore the side-channel is restricted and hidden from a practical power analysis attack, unlike the RTZ-based circuits in which the data-dependence is extended for a longer time period.

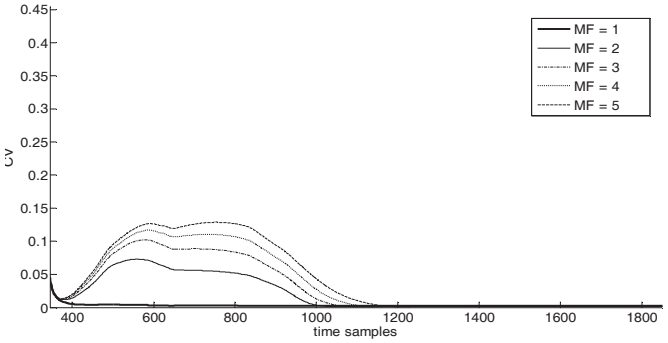

Fig. 33. Screenshot of the Coefficient of Variation for the master-slave DDPL 4-bit register around the delay time Δ under different mismatch factors.

TABLE II.
POWER-BALANCING METRICS FOR THE CMOS 4-BIT REGISTER.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
-	60.95	21.98	29.705	0.320

TABLE III.
POWER-BALANCING METRICS FOR THE WDDL 4-BIT REGISTER.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
1	39.48	12.10	88.933	0.101
2	37.45	10.93	91.074	0.090
3	39.31	10.66	95.407	0.102
4	34.76	11.03	99.260	0.115
5	42.05	12.27	102.301	0.147

TABLE IV.
POWER-BALANCING METRICS FOR THE SABL 4-BIT REGISTER.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
1	0.21	0.04	61.436	0.004
2	11.50	3.25	66.220	0.056
3	20.72	6.10	69.722	0.101
4	28.04	7.51	74.105	0.120
5	34.18	10.92	76.799	0.170

In Table II to Table VII the values of the measured power-balancing metrics for the registers under test are reported for different mismatch factors. The average correlation coefficient CV_{AV} represents the mean of the correlation coefficient during the evaluation phase, where the data-dependence is stronger.

In Fig. 34 the distribution of the average currents I_{AV} is depicted for a number of clock cycles (i.e. 100) in the case of mismatch factor equal to 3. The figure shows a very low variance around the mean for the TDPL and DDPL master-slave configurations, which are almost superimposed. Finally, in Table VIII the performances of the DPL flip-flops are summarized for the case of a moderate mismatch factor.

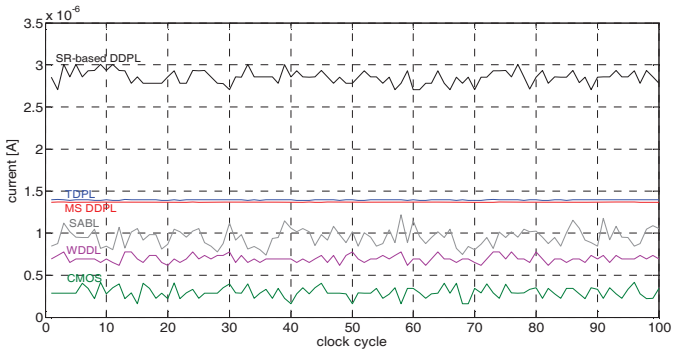

Fig. 34. A comparison of the distribution of the average current for 100 clock cycles for the DPL flip-flops under test (MF = 3).

TABLE V.
POWER-BALANCING METRICS FOR THE TDPL 4-BIT REGISTER.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
1	0.98	0.18	123.428	0.003
2	0.81	0.19	131.586	0.002
3	0.77	0.18	139.438	0.002
4	0.63	0.13	147.405	0.002
5	0.68	0.15	155.309	0.002

TABLE VI.
POWER-BALANCING METRICS FOR THE SR DDPL 4-BIT REGISTER.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
1	10.77	2.97	268.461	0.028
2	10.39	2.54	278.126	0.023
3	10.10	2.77	285.391	0.025
4	9.91	2.60	293.290	0.024
5	9.65	2.69	301.288	0.024

TABLE VII.
POWER-BALANCING METRICS FOR THE MS DDPL FLIP-FLOP.

MF	NED [%]	NSD [%]	E_{AV} [fJ]	CV_{AV}
1	0.74	0.15	120.911	0.004
2	0.59	0.13	128.950	0.005
3	0.62	0.13	136.881	0.004
4	0.53	0.12	144.844	0.005
5	0.45	0.11	152.782	0.006

TABLE VIII.
PERFORMANCES OF THE DPL FLIP-FLOPS IN TERMS OF OCCUPIED AREA AND AVERAGE ENERGY UNDER A MODERATE OUTPUT MISMATCH (MF = 3).

	# MOS	Area [um^2]	Area increase	NED [%]	E_{AV} [fJ]
WDDL [17]	66	52	x 2.7	39.31	95.407
SABL [23]	44	39	x 2.1	20.72	69.722
TDPL [25]	58	52	x 2.7	0.77	139.438
DDPL [26]	126	113	x 5.9	10.10	285.391
DDPL (this paper)	66	61	x 3.2	0.62	136.881

The proposed DDPL flip-flop improves the previously published implementation in terms of area overhead (which has been measured with respect to the area of the CMOS flip-flop used as benchmark) and power-balance. The DDPL flip-flop overcomes also SABL and WDDL in terms of NED, NSD and CV_{AV}, which are extremely slow (< 1%) and comparable to TDPL. Obviously, an area penalty must be taken into account for enhancing the power-balance of the circuit.

Moreover, as the unbalances of the internal wires were not considered in simulations, the performances of the proposed flip-flop are underestimated with respect to the TDPL implementation, where the routing of the differential wires is constrained by the presence of the SR slave latch, which may introduce time or capacitive mismatches, and of an additional dynamic signal.

VI. CONCLUSION AND FUTURE WORK

In this paper a flip-flop for the Delay-based Dual-rail Precharge Logic style has been proposed and compared to the state of the art in the technical literature. The circuit is based on a dynamic differential architecture with a highly symmetric layout, which allows to balance all internal complementary interconnections so to prevent any capacitive and time mismatch on the differential signals.

The performance of the circuit has been validated through post-layout simulations. A 4-bit register has been implemented in a 65nm-CMOS process. Simulation results show that the proposed implementation exhibits a constant energy consumption in presence of asymmetric load conditions. With respect to WDDL and SABL flip-flops, the simulated energy consumption per cycle of the DDPL flip-flop shows an improvement in the energy distribution balancing in excess of 10 times for a low mismatch and 20 times for a moderate mismatch, with a reduced area and power overhead. This confirms that WDDL and SABL are very sensitive to mismatches occurring on the capacitances of the output wires, and can be used for designing power-balanced circuits for cryptographic applications only if the layout of the interconnections wires is perfectly balance, which is hard to guarantee in current sub-micron technologies.

The novel DDPL architecture also overcomes the previous published implementation. Even if the latter is insensitive to the variation of the mismatch factor, it does not exhibit an optimized power-balance because of the presence of an unfair SR-latch which forces a dynamic-to-static conversion of the signals. Moreover the area overhead is almost halved with respect to the previous implementation, thanks to the minor number of transistors and to the highly differential architecture.

The performances of the proposed DDPL master-slave flip-flop are comparable to the TDPL flip-flop, both in terms of area occupation (~60 μm^2) and energy-balance (NED < 1%). However TDPL style has the drawback of requiring the routing of an additional dynamic control signal for synchronizing the elaboration phases, and this poses a constraint on the layout of the whole circuit. Moreover DDPL is an improvement of TDP because the delay-based circuits requires only a static voltage as input for the delay elements of the flip-flops, which can be routed as a global signal and is not critical for the balance of the capacitances at the internal nodes, under the perspective of a reduced compact layout. A DDPL circuit requires an adequate timing analysis, but this is must be accounted also for the other DPL logic styles and does not represent a drawback.

By using the proposed flip-flop, power-balanced circuits can be designed with delay-based logics, adopting a single clock signal and without requiring any constraint on the geometry of the complementary wires. Power-balanced logic help to break the link between the data and the instantaneous power consumption directly at physical level and can be adopted for designing secure cryptographic hardware.

Future research will focus on the implementation of a cryptographic hardware module in DDPL in which the proposed flip-flop will be adopted and on which Power Analysis attacks will be mounted in order to test the effectiveness of the circuit in a real attack scenario.

REFERENCES

[1] P. C. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems”, in Proc. of *CRYPTO ’96* (LNCS), Santa Barbara, CA, USA, 1996, vol. 1109, pp. 104-113.

[2] P. C. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, in Proc. of *CRYPTO ’99* (LNCS), Santa Barbara, CA, USA, 1999, vol. 1666, pp. 388-397.

[3] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a leakage model”, in Proc. of *CHES 2004* (LNCS), Berlin, Germany, 2004, vol. 3156, pp. 16-29.

[4] S. Chari, J. Rao, and P. Rohatgi, “Template Attacks”, in Proc. of *CHES 2002* (LNCS), San Francisco, CA, USA, 2002, vol. 2523, pp. 13-28.

[5] K. Schramm, G. Leander, P. Felke, and C. Paar, “A collision-attack on AES: combining side-channel and differential attack”, in Proc. of *CHES 2004* (LNCS), Berling, Germany, 2004, vol. 3156, pp. 163-175.

[6] B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel. “Mutual information analysis”, in Proc. of *CHES 2008* (LNCS), Washington, CA, USA, 2008, vol. 5154, pp 426-442.

[7] M.Alioto, L. Giancane, G. Scotti, and A. Trifiletti, “Leakage Power Analysis attacks: a novel class of attacks to nanometer cryptographic circuits”, *IEEE Trans. on Circuits and Systems I*, vol. 57, no. 2, pp. 355-367, Feb. 2010.

[8] J. D. Golic, and R. Menicocci, “Universal masking on logic gate level”, *Electronics Lett*., vol. 40, no. 9, no.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. of *PATMOS 2004* (LNCS), Isle of Santorini, Greece, vol. 3254, pp. 481-490, Sept. 2004.

[10] M. Bucci, M. Guglielmo, R. Luzzi, and A. Trifiletti, "A countermeasure against differential power analysis based on random delay insertion", in Proc. of *ISCAS 2005*, vol.4, pp. 3547–3550, May 2005.

[11] J. M. Rabaey, A. P. Chandrakasan, and B. Nikolic. *Digital Integrated Circuits: a Design Perspective*, 3rd ed., Prentice Hall electronics and VLSI series, Pearson Education, 2003.

[12] V. Stojanovic, and V. G. Oklobdzija, "Comparative analysis of master-slave latches and flip-flops for high-performance and low-power systems", *IEEE Journal of Solid-State Circuits*, vol. 34, no. 4, pp. 536-548, Apr. 1999.

[13] K. Tiri, and I. Verbauwhede, "Place and route for secure standard cell design", in Proc. of *CARDIS 2004*, Toulouse, France, 2004, pp. 143–158.

[14] D. Suzuki, and M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic styles", in Proc of CHES 2006 (LNCS), Yokohama, Japan, 2006, vol. 4249, pp. 255-269.

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

[16] K. Tiri and I. Verbauwhede, "A logic design methodology for a secure DPA resistant ASIC or FPGA implementation", in Proc. of DATE 2004, Paris, France, 2004, pp. 246–251.

[17] A. Moradi, T. Eisenbarth, A. Poschmann, and C. Paar, "Power Analysis of single-rail storage elements as used in MDPL", in Proc. of ICISC 2009 (LNCS), Seoul, Korea, 2010, vol. 5984, pp. 146-160.

[18] R. P. McEvoy, C. C. Murphy, W. P. Marnane, and M. Tunstall, "Isolated WDDL: A hiding countermeasure for Differential Power Analysis on FPGAs", *ACM Trans. On Reconfigurable Technol. And Syst.*, vol. 2, no. 1, pp 1-23, Mar. 2009.

[19] P. Yu, and P. Schaumont, "Secure FPGA circuits using controlled placement and routing", in Proc of *CODES+ISSS '07*, New York, NY, USA: ACM, 2007, pp 45-50.

[20] K. Baddam, and M. Zwolinski, "Divided backend duplication methodology for balanced dual-rail routing", in Proc. of *CHES 2008* (LNCS), Washington, DC, USA, 2008, vol. 5154, pp. 396-410.

[21] 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", in Proc of ESSCIRC 2002, Florence, Italy, 2002, pp.403-406.

[22] M. Matsui, H. Hara, Y. Uetani, K. Lee-Sup, T. Nagamatsu, Y. Watanabe, A. Chiba, K. Matsuda, and T. Sakurai, "A 200 MHz 13 mm 22-DDCT macrocell using sense-amplifier pipeline flip-flop scheme", *IEEE Journal of Solid-State Circuits*, vol. 29, no. 12, pp. 1482-1491, Dec. 1994.

[23] B. Nikolic, V. G. Oklobdzija, V. Stojanovic, W. Jia, J. K.S. Chiu, and M. M..T. Leung, "Improved Sense-Amplifier-Based Flip-Flop: Design and Measurements", *IEEE Journal of Solid-State Circuits*, vol. 35, no 6, pp. 878-884, Jun. 2000.

[24] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic", in Proc. of *CHES 2006* (LNCS), Yokohama, Japan, 2006, pp. 232-241.

[25] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "A flip-flop for the DPA resistant three-phase dual-rail precharge logic family", *IEEE Trans. on VLSI Systems*, vol. 20, no. 11, pp. 2128-2132, Nov. 2012.

[26] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic", *IEEE Trans. on VLSI Systems*, vol. 19, no. 7, pp. 1147-1153, July 2011.

[27] S. Bongiovanni, G. Scotti, and A. Trifiletti, "Security evaluation and optimization of the delay-based dual-rail precharge logic in presence of early evaluation of data", presented at the 11th Int. Conf. on Security and Cryptography (SECrypt 2013), Reykjavik, Iceland, July 29-31, 2013.

[28] G. S. Jovanović, and M. Stojčev, "Linear Current Starved Delay Element", in Proc. of *ICEST 2005*.

[29] G. S. Jovanović. M. Stojčev, and Z. Stamenković, "A CMOS Voltage Controlled Ring Oscillator with Improved frequency Stability", *in Scientific Publications of the State University of Novi Pazar, Series A: Applied Mathematics, Informatics and Mechanics*, vol. 2, pp. 1-9, 2010.

[30] B. Halak, J. P. Murphy, and A. Yakovlev, "Power Balanced Circuits for Leakage-Power-Attacks Resilient Design", IACR Cryptology ePrint Archive 2013: 48 , Jan. 2013. [Online]. Available: http://eprint.iacr.org/2013/048.pdf.

Simone Bongiovanni was born in Rome, in 1983. He received the Bachelor's degree in electronic engineering and the Master of Science degree (summa cum laude) in electronic systems for telecommunications from Università di Roma "La Sapienza," Rome (Italy), in 2007 and 2010 respectively. He discussed a thesis on the study of the hardware security of smart cards for mobile payments applications, and collaborating with the Communications Department of the Ministry of Economic Development of Italy and the "Ugo Bordoni" Foundation. In 2011 he joined to the R&D division of the company "General Impianti" of the Loccioni Group in Jesi (Italy), where he worked as junior researcher engineer. He is currently attending a Ph.D. course at the Dipartimento di Ingegneria dell'Informazione, Elettronica e Telecomunicazioni of the university "La Sapienza". His research interests include the analysis and design of techniques for secure IC's devices for cryptographic applications, with a particular focus on power analysis attacks, and the design of digital integrated circuits.

Mauro Olivieri (M'98) received the Master (Laurea) degree in electronic engineering "cum laude," in 1991 and the Doctorate degree in electronic and computer engineering in 1994 from the University of Genoa, Genoa, Italy, where he was an Assistant Professor from 1995 to 1998. In 1998, he joined Sapienza University, Rome, Italy, where he is currently an Associate Professor, teaching digital electronics and VLSI system architectures. His current research interests include digital system-on-chip design, microprocessor core design, and digital nanoCMOS circuits.
He authored more than 100 research papers and a textbook in three volumes. He is a Reviewer for several IEEE Transactions and is in the technical program committee of the IEEE DATE Conference. He is an Evaluator for the Joint Technology Initiative of the European Commission on Nanoelectronics (ENIAC Joint Undertaking).

Giuseppe Scotti was born in Cagliari in 1975. He received the Master and Ph.D. degree in Electronic Engineering from the University of Rome "La Sapienza" in 1999 and 2003 respectively. He is currently Assistant Professor in the scientific field "Elettronica" (ING-INF/01) in the Department DIET at the same University.
From 2003 to 2010 he was Professor of Digital Electronics at "La Sapienza" University, and since 2006 he teaches a course in Theory of Electronic Circuits at "La Sapienza" University.
From 2004 to 2006 he participated in the European project SCARD (Side Channel Attacks Resistant Design), and from 2007 to 2009 he was involved in the European Integrated Project SHAPES (Scalable Software Hardware Application Platform for Embedded Systems).
His research activity was mainly concerned with integrated circuits design and focused on design methodologies able to guarantee robustness with respect to parameter variations in both analog circuits (radio frequency and microwave applications) and digital VLSI circuits. In the context of analog design his research activity was concerned with circuit topologies for the realization of analog functions using low-voltage ultra-short channel CMOS technology and with the development of current mode building blocks. He has been also involved in research/design activities held in collaboration between "La Sapienza" University and some industrial partners which led, between 2000 and 2012, to the implementation of 12 ASICs.
He has coauthored more than 100 publications in international journals and conferences and is the co-inventor of 2 international patents.
He conducts peer reviews for IEEE (IEEE TCAS, TCAS, TVLSI), Wiley and Elsevier journals.

Alessandro Trifiletti was born in Rome, Italy, in 1959. He received the Laurea degree in electronic engineering from the Università di Roma "La Sapienza," Rome, Italy. In 1991, he joined the Dipartimento di Ingegneria Elettronica, Università di Roma "La Sapienza," as a Research Assistantwhere he is currently an Associate Professor.
His research interests include high speed circuit design techniques and III-V device modeling.