International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.4, April 2013 DOI:10.15693/ijaist/2013.v2i4.127-131

An energy efficient flip flop for three- phase dual – rail pre- charge logic family Using transmission gates

[1]S.Mohana chandran,[2]A. Rajaram
[1]PG Scholar, [2]Associate professer, Department of ECE,
Karpagam University, Coimbatore – 641021, Tamilnadu, India

Abstract—**This paper investigates the design of a data flip-flop compatible with the three-phase dual-rail pre-charge logic (TDPL) family using transmission gates. TDPL is a differential power analysis (DPA) resistant dual-rail logic style whose power consumption is insensitive to unbalanced load conditions, based on a three phase operation where, in order to obtain a constant energy consumption, an additional discharge phase is performed after pre-charge and evaluation. In this work, the TDPL basic gates operation is shortly summarized and the TDPL flip-flop implementation is reported. A part of an encryption algorithm is used as case a study to prove the effectiveness of the proposed circuit. Simulation results in a 180nmCMOS process show an improvement in the energy consumption.**

Index Terms—**Differential power analysis (DPA), dual-rail logic, security, sense amplifier-based logic (SABL), three-phase dual-rail pre-charge logic (TDPL).**

I. INTRODUCTION

Side channel attacks can disclose confidential data (i.e., cryptographic keys and user PINs) looking at the information leaked by the hardware implementation of cryptographic algorithms. 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].

Since the introduction of DPA, several countermeasures have been proposed in the technical literature at different levels from system to transistor-level. 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) [2], wave dynamic differential logic (WDDL) [3], dual-spacer DRP [4]), 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. 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. Semi-custom design flows supporting differential logic families have been proposed in the technical literature [5] but 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 introduces additional constraints for the routing tool. In addition, in a modern deep sub-micron technology, local process gradients cannot beneglected and they are the limiting factor for the load matching accuracy. A second technique proposed in [6]–[8] is based on a masked dualrail pre-charge logic style (MDPL) and on an improved implementation (iMDPL) where, due to the random masking at the gate level, power consumption is randomized. The iMDPL solves the problems of the MDPL due to the synchronization of the inputs but the penalty with respect MDPL is a factor of 3 and 1.5 in terms of area and power consumption, respectively.

A third solution has been reported in [9]: 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 [10]. While in [9] only a basic set of logic gates is reported, this paper is devoted to the implementation of a data flip-flop compatible with TDPL gates. The TDPL operating principle is shortly summarized in Section II where simulation results in the adopted technology are also reported for both TDPL and SABL basic gates. The flip-flop implementation details and simulation results are presented in Section III. Finally, a case study is discussed in Section IV and an extensive comparison with the corresponding SABL implementation is carried out.

II. TDPL LOGIC STYLE

In the TDPL, during a first phase (pre-charge), the output lines of ageneric logic gate are both charged 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}/or V_{ss} are taken into account. In [9], the proposed logic style has been implemented as an enhancement of the SABL logic style with a minimum increase in the required area. Therefore, as in [9], SABL cells are assumed as the benchmark for the equivalent TDPL cells in this work. For instance, a TDPL inverter is shown in Fig. 1 and the timing diagram corresponding to the circuit operation [9] is depicted in Fig.2. Notice that TDPL, like SABL, is a Domino Logic and, therefore, CMOS static inverters must be inserted between two cascaded gates. This means that the inputs to a logic gate are both low at the beginning of the evaluation phase (outputs of the driving gate are pre-charged to V_{dd} andone of them goes high when the driving gate evaluates, thus triggering the evaluation of the gate under analysis. The duration of the evaluation phase limits the length of the combinatorial paths (i.e., number of cascaded gates between two flip-flops). The three control signals are derived from a base clock and they must be routed as clock signals, keeping their skew under control. The current consumption profile of the TDPL inverter has been reported in [9], where each operation phase can be identified. A basic set of cells, obtained by changing the pull-down logic, has been designed in a 180-nm CMOS

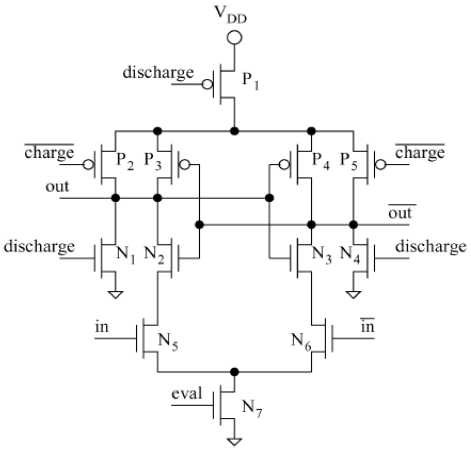

Fig.1 TDPL inverter

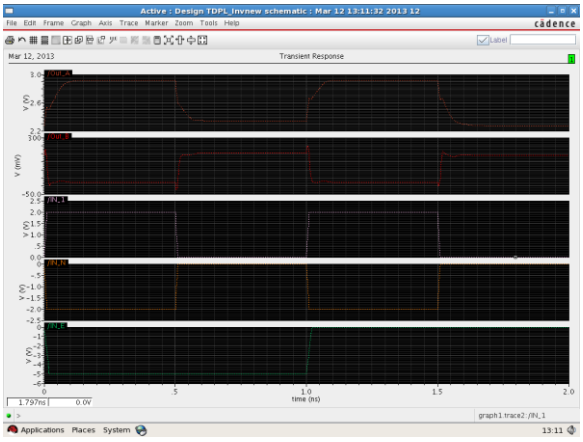

Fig.2. Timing diagram of TDPL

100 MHz operating frequency are adopted. Each transistor is designed with a widthW = 0.12 _m and the minimum gate length _ L=65 nm is assumed. Simulations are done in Spectre, using BSIM4 transistor models. In order to simulate the cells in a real operating condition, a testbench has been defined where each input to the gate under analysis is driven by a TDPL inverter and unbalanced load capacitances to C_{out} and V_{ss} 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.

As in [2], the energy per cycle is adopted as figure of merit to measure the resistance against power analysis attacks. The obtained results for the three analyzed gates (Inverter, NAND/AND and XOR/NXOR) have been compared with respect to the difference , the normalized energy deviation (NED), defined as, and the normalized standard deviation (NSD), As expected, SABL gates are sensitive to unbalanced load conditions 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 in spite of unbalanced load capacitances. As expected, almost a doubling of 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), especially if compared with what is reported for MDPL [7]. With respect to SABL, TDPL requires the routing of two additional signals. 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.

III. FLIP-FLOP IMPLEMENTATION

The implementation of a data flip-flop compatible with TDPL gates is based on the scheme shown in Fig. 3: it includes a first TDPL inverter, an intermediate circuit which drives the set/ reset inputs to a CMOS SR-latch and a second TDPL inverter on the output. Its operation is similar to the SABL flip-flop reported in [2] where the additional circuitry after the first TDPL inverter avoids the latch invalid input charge by forcing a logic-1 during both the phases of discharge and charge. In other words, the input TDPL inverter with the additional circuitry on its outputs behaves as a SABL inverter. The timing diagram shown in Fig. 4 clarifies the flip-flop operation where evaln is equal to 0 negated and charge are the discharge and charge signals referred to. Therefore, as are active when evaln = 0. With reference to Fig. 4, on the evaln enters its evaluation phase and node is set to 0. Further changes of the input data during the evaluation phase do not affect node 1 Transistors N1,N3 are closed P2, P4 are open) and the CMOS SR-latch is either set or reset depending on node 1 thus storing the input data node 2 Meanwhile, the output inverter is in the discharge and charge phases thus being insensitive to its inputs. When the input inverter enters its discharge phase raising edge), N1, and N3are open and P2, P4 are closed thus forcing the hold state of the SR-latch (Set= reset= 1). Hereafter, changes on node 1 due to the discharge/charge phase in the first invert do not affect node2 . The output inverter enters its evaluation phase thus setting q according to node 2.

IV. CASE STUDY

As a case study, the circuit shown in Fig. 5 has been simulated. It includes two 4-bit input registers (data_i, key_i), four XOR gates, the S-box s0 from the Serpent algorithm [11] and a 4-bit output register (data_o). Both the combinatorial logic and the registers have been implemented in TDPL using the proposed flip-flop, where the clock signal is applied to the eval in input in Fig. 3 and the other control signals are not shown. As a reference, the same circuit has been implemented in SABL as well. In order to take into account the unbalanced routing in a semi-custom layout, every gate output is loaded with unbalanced load capacitances to $_{Vdd}$ and V_{ss} In details, the asserted lines are loade with 4 and 1.5 fF to $_{Vdd}$ and V_{ss}, respectively, while 0.5 and 1 fF have

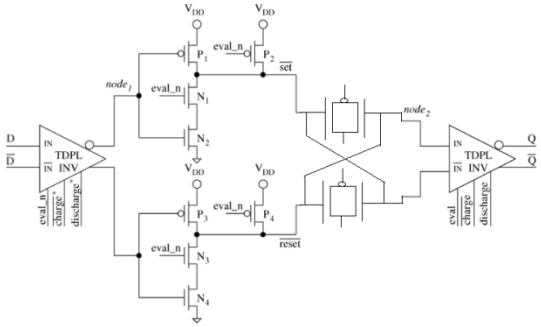

Fig.3 Combined TDPL Using Transmission Gates

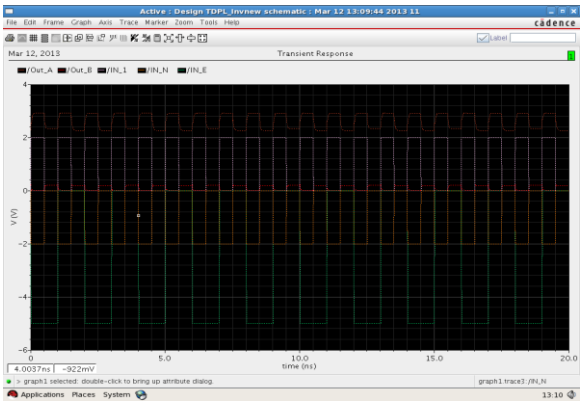

Fig.4 Output of TDPL Using Transmission Gates

been used for the negated lines. These are reasonable parasitic capacitance values for the local routing in the adopted technology. A superimposition of the power supply current traces I_{dd} for every possible transition of the input data is depicted in Figs. 3 and 4 for the SABL and the TDPL implementation respectively. In both Figure SABL: superimposition of the power supply current traces. cases, each operation phase can be identified in the supply current profile: the SABL circuit shows a data dependency during both pre-charge and evaluation (first and second peak in Fig. 4) while, in the TDPL implementation, the pre-charge current pulse is constant and a data dependency is visible during the discharge and evaluation phases (first and third peak). In addition, the TDPL circuit shows a fourth current peak due to the flip-flop operation (charging of in Fig. 3) which is also constant with respect to the input data. A histogram of the observed energies per cycle for every possible input transition is reported in Fig. 8 and it shows that TDPL guarantees a balanced energy consumption, independent of the processed data, even in presence of unbalanced interconnections. Notice that the same scale has been used for the energy per cycle. The obtained simulation results are summarized in Table I for both SABL and TDPL, where the energy consumption has been evaluated.

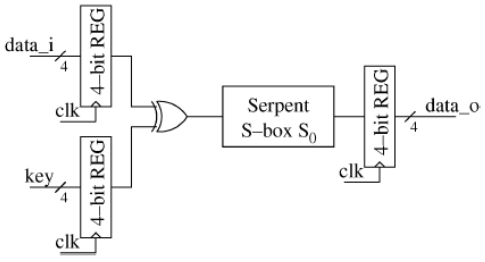

Fig. 5. Circuit used as case study.

Table -1 Comparision table of TDPL

on both the clock cycles necessary to process the input data. These results confirm that, as for the single logic gates, TDPL shows an extremely balanced energy consumption per cycle in spite of unbalanced semi-custom routing. In comparison to SABL, the simulated values for both NED and NSD are more than 10 times smaller for the TDPL implementation.

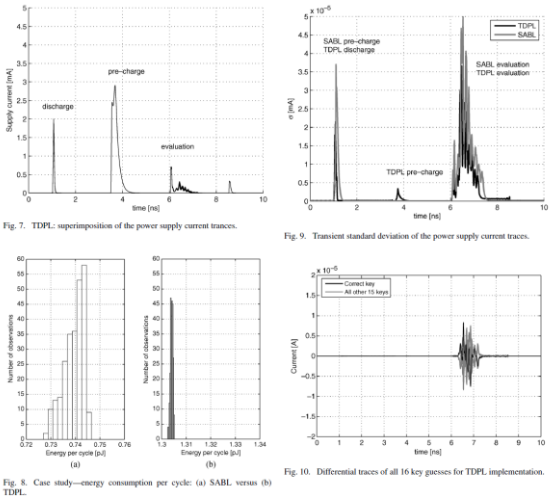

Fig. 7. TDPL: superimposition of the power supply current traces.

Fig. 9. Transient standard deviation of the power supply current traces.

Fig. 8. Case study—energy consumption per cycle: (a) SABL versus (b) TDPL.

Fig. 10. Differential traces of all 16 key guesses for TDPL implementation.

Fig. 6. a) Transient standard deviation of the power supply current traces. b) Differential traces of all 16 key guesses for TDPL implementation.

The standard deviation of the power supply current traces for both implementations is shown in Fig. 6. This figure of merit allows to better asses the DPA resistivity in case the attacker is supposed to use a measurement equipment able to discriminate each current consumption peak inside the operating cycle [12]–[14]. Notice that, in the case study under analysis, a bandwidth larger than 1 GHz would be necessary for the measurement channel, neglecting the low-pass filtering due to the parasitics of the on-chip power grid. Fig. 6 confirms that the pre-charge peak in TDPL is data-independent, as well as the fourth peak introduced by the flip-flops. Moreover, the data dependency of the remaining peaks is noticeably reduced in comparison to SABL. Finally, a complete DPA has been performed on both implementations using the 256 simulated power supply current traces for every possible transition of the input data. One of the S-box outputs is used as target bit.. The amplitude of the trace corresponding to the correct key (black line) is the highest in both cases thus resulting in a successful DPAattack (maximum peak of 8.342 and 14.88 μA, respectively). However, while for the SABL case, the trace of the correct key is clearly distinguishable(9.643 μA maximum peak for an incorrect key), for the TDPL implementation, it is only marginally higher than the other ones (7.524 μAmaximum peak for an incorrect key). From these simulation results, it follows that TDPL shows a smaller remaining leakage compared to SABL but it can be hardly evaluated if it would be sufficient for a successful attack on a real circuit, where the current traces are affected by measuring errors, noise and filtering effects. As a final remark, it is worth notice that the early propagation effect represents a further source of information leakage due to the pulldown network in both logic styles. In order to minimize this effect, the enhanced differential pull-down network (DPDN) introduced for SABL, can be applied to TDPL as well.

	1 clock cycle		**2 clock cycle**	
	Existing work	modified	Existing work	modified
Max(E)	1305.53	1307.25	1306.32	1308.50
Min(E)	1302.44	1305.00	1303.12	1306.30
Tot(E)	2.79	2.25	3.1	2.20
NSD	0.4%	0.3%	0.6%	0.4%

V. CONCLUSION

A flip-flop compatible with the DPA-resistant logic family TDPL with transmission gateshas been introduced and compared to the state of the art in the technical literature. From the performed experimental results on a case study in a 180-nm CMOS process, it follows that the proposed implementation shows a constant energy consumption even in presence of asymmetric interconnections. The simulated energy consumption per cycle shows an improvement in the energy consumption balancing in excess of 2 times with respect to the corresponding TDPL implementation without requiring any constraint on the geometry of the complementary wires. The analysis of the instantaneous current consumption profiles and a complete DPA performed on the simulated current traces confirm the improvement obtained with the proposed logic family.

REFERENCES

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in *Proc. Adv. Cryptol. (CRYPTO)*, 1999, pp. 388–397.

[2] 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. IEEE 28th Euro. Solid-State Circuit Conf. (ESSCIRC)*, 2002, pp. 403–406.

[3] K. Tiri and I. Verbauwhede, "A logic design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Autom., Test Euro. Conf. Expo. (DATE)*, 2004,
pp. 246 251.
[4] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," in *Proc. Workshop Cryptograph. Hardw. Embed. Syst. (CHES)*, 2004, pp. 282–297.
[5] 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.
[6] T. Popp and S. Mangard, "Masked dual-rail pre-charge logic: DPA-resistance without routing constraints," in *Proc. Workshop Cryptograph. Hardw. Embed. Syst. (CHES)*, 2005, pp. 172–186.
[7] T. Popp and S. Mangard, "Implementation aspects of the DPA-resistant logic style MDPL," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2006, pp. 2913–2916.
[8] T. Popp, M. Kirschbaum, T. Zefferer, and S. Mangard, "Evaluation of the masked logic style MDPL on a prototype chip," in *Proc. Workshop Cryptograph. Hardw. Embed. Syst. (CHES)*, 2007, pp. 81–94.
[9] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dualrail pre-charge logic," in *Proc.Workshop Cryptograph. Hardw. Embed. Syst. (CHES)*, 2006, pp. 232–241.
[10] E. Menendez and K. Mai, "A high-performance, low-overhead, poweranalysis- resistant, single-rail logic style," in *Proc. IEEE Int. Workshop Hardw.-Oriented Security Trust (HOST)*, 2008, pp. 33–36.