International Journal of Computer Science and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

Power Efficient for DPA Resistat Flip Flop Using TDPL Inverter in Reverse Logic

Nandhini M[1*], Muralidharan V[2] and Varatharaj M[3]

[1]*Electronics and Communication Engineering, Anna University, Coimbatore, India,*

www.ijcseonline.org

Received: 17/03/2014 Revised: 28/03/2014 Accepted: 27/04/2014 Published: 30/04/2014

***Abstract*—** To design a data flip-flop consistent with the three-phase dual-rail pre-charge logic (TDPL) family. 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 and also reduce the power dissipation replacing the discharge and evaluation phase by pull up and pull down networks using Reverse Logic. A part of an encryption algorithm is used as case a study to prove the effectiveness of the proposed circuit. Simulation results in a 65 nm CMOS process show an improvement in the energy consumption and power consumption.

***Keywords*—** Differential Power Analysis (DPA), Dual-Rail Logic, Security, Reverse Logic, 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. 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 neglected and they are the limiting factor for the Load matching accuracy.

A second technique proposed in [6]–[8] is based on a masked dual rail 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]: 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_{SS} and discharged to V_{DD} a TDPL gate shows constant energy consumption over its operating cycle and this method having large power dissipation. The main drawback of this solution is the additional area for the routing of the three control signals.

A Reverse Logic using TDPL has been also proposed which shows a lower overhead in terms of power consumption and power dissipation will be reduced using this logic, area thus being suitable for embedded and mobile applications. This paper is devoted to the implementation of a data flip-flop compatible with TDPL inverter using Reverse Logic.

II. TDPL INVERTER IN REVERSE LOGIC

In this section the Three Phase Dual Rail Logic consist of three phases, a first phase is pre-charge phase, the output lines of a logic gate are both charged to Supply voltage (V_{DD}), then second phase is evaluation phase the proper line is discharged to ground (V_{SS}) corresponding to the input data a new output data are generated in the inverter. Finally,

Corresponding Author: *Nandhini M*
Electronics and Communication Engineering, Anna University, Coimbatore, India.

during the Third phase i.e. discharge phase, the remaining line are discharged too in the inverter.

A TDPL inverter shows constant power consumption over its operating cycle depends upon the input data, even if presence of unbalanced capacitive loads to Supply voltage and/or ground are taken into account .To reduce the power dissipation replacing the discharge and evaluation phase by pull up and pull down networks to the discharge and evaluation phase.

The TDPL inverter in reverse logic is shown in Figure. 1 and the timing diagram of corresponding circuit operation are shown in Figure. 2. The TDPL inverter is having Domino Logic and Reverse Logic. CMOS static inverters must be inserted between two cascaded gates. At the beginning of the stage both the input of logic gate is low in the evaluation phase and the output of the driving gate are pre-charged to source .When one of the driving gate evaluated the output is goes to high. Input of the control signals are given from the clock signal.

In Three Phase Dual Rail Pre-charge Logic inverter in reverse logic when the input is given to the circuit in (charge phase) charge=0 in this condition P1, P2, P5 transistors are turned ON. This network is called pull up network. In (evaluation phase) eval=1 in this condition N7, N6, N5 transistors are turned ON. This network is called pull down network. In (Discharge phase) Discharge=1 in this condition N1, N4 transistors are turned ON .This transistors are required the additional pull down network for turned ON the circuit. The output of the TDPL inverter is out=0 and out= 1.

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 65-nm CMOS process A 1.8 V supply voltage and a 50 MHz operating frequency are adopted. Each transistor is designed with a width W= 22u and the minimum gate length L= 2u is assumed. Simulations are done in Tanner, using T-Spices models.

Three Phase Dual Rail Logic inverter using Reverse Logic shows the balanced power consumption in spite of unbalanced load capacitances and also reduces the power dissipation.

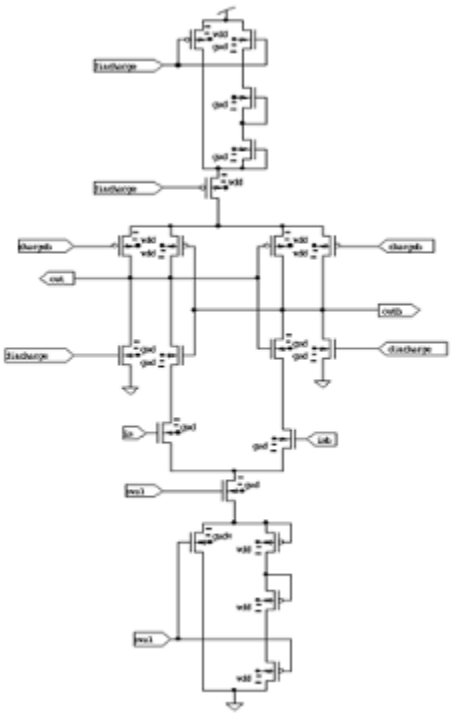

Figure.1.TDPL inverter in reverse logic

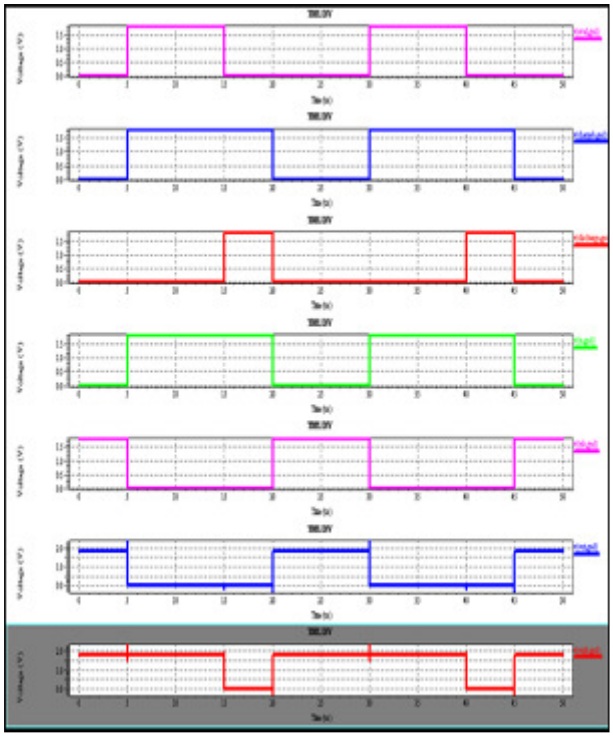

Figure.2.Waveform of TDPL inverter in reverse logic

III. FLIP FLOP IMPLEMENTATION

In this section implementation of a data flip-flop consistent with TDPL gates is based on the scheme shown in Figure. 3 shows the schematic representation of Three Phase Dual Rail Pre-charge logic Flip flop implementation. The timing

diagram shown in Figure.4 .In a TDPL Flip Flop, the Data input is given to the TDPL inverter and the output of the TPDL inverter is given to the two nodes. Consider the first Part of the TDPL inverter inputs are Charge (0), discharge (0), eval_n(1) and Data input is D(0) and D , the output of the TDPL inverter is inverted and given to the Node1.In Node 1 the P1 transistor is turned OFF and N2 transistor is turned ON with ground potential .Then N1 transistor is turned ON and P2 (set) transistor is turned OFF because the input of inverter. The output of the transistor is given to the NAND gate. Consider the second part of the TDPL inverter inputs are Charge (0), discharge (0), eval_n(1) and Data input is D and D (1), the output of the TDPL inverter is inverted and given to the Node1.In Node 1 the P3 transistor is turned OFF and N4 transistor is turned ON with ground potential .Then N3 transistor is turned ON and P4 (reset) transistor is turned OFF because the input of inverter. Further changes in the input data during evaluation phase is do not affect the Node1. The output of the transistor is given to the NAND gate .Assume the NAND gate previous input as (0 or 1). The output of the NAND gate is given to the Node 2, i.e. output of the NAND gate is given to the TDPL inverter. The output of the inverter goes to the evaluation phase according to the Node2.The TDPL inverter will invert the output value of the NAND Gate and produce the output values. Output will be maintained same as the input. These circuits maintain the constant power consumption and also reduce the power dissipation.

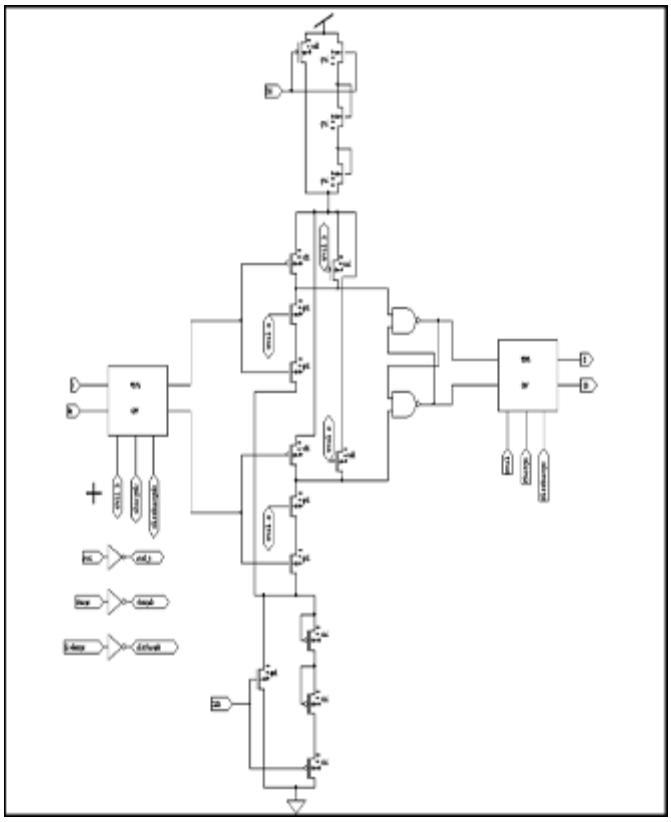

Figure .3.TDPL flip-flop implementation

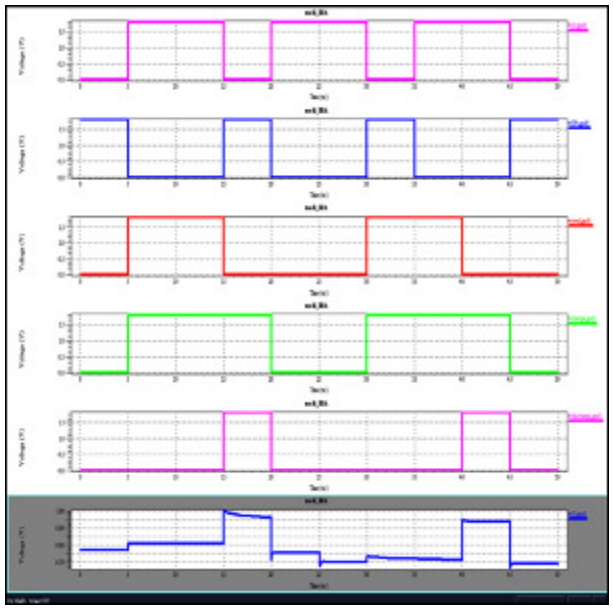

Figure.4.Waveform of Flip-flop implementation

IV. SIMULATION OUTPUT AND CASE STUDY

As a case study, the circuit shown in Figure. 5 have 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 CLK is applied to the eval input in Figure.5 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 V_{DD} and V_{SS}. In details, the asserted lines are loaded with 4 and 1.5 fF to V_{DD} and V_{SS}, respectively, while 0.5 and 1 fF have been used for the negated lines. These are reasonable parasitic capacitance values for the local routing in the adopted technology.

The simulated values for both Maximum power and Minimum power are more than 10 times smaller for the TDPL implementation. The Average power is calculated. This figure of merit allows to better assessing 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 parasitic of the on-chip power grid. The pre-charge peak in TDPL is data-independent, as well as the fourth peak introduced by the flip-flops. Finally, a complete DPA has been performed on both implementations using the 256 simulated power supply current traces I_{DD} (t) for every possible transition of the input data. One of the S-box outputs is used as target bit. The amplitude of the Upper trace corresponding to the Input

Data and Lower trace corresponding to the Output Data (black line) is the highest in both cases thus resulting in a successful DPA attack (maximum peak of 8.342 and 14.88 Micro Amps 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 [15] represents a further source of information leakage due to the pull down network in both logic styles respectively).

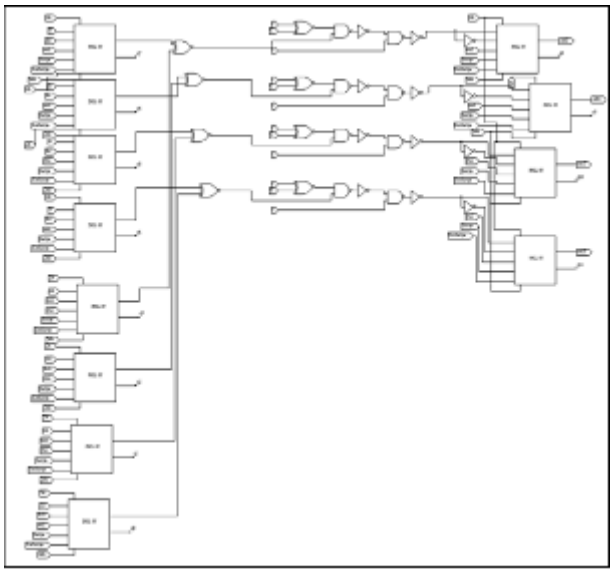

Figure.5.Circuit used as a case study

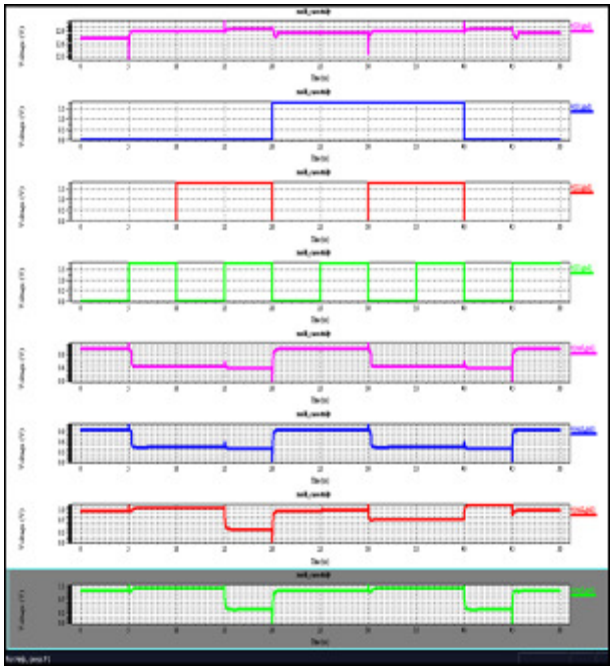

Figure.6.Waveform of case study

However, while for the SABL case, the trace of the correct key is clearly distinguishable (9.643 Micro Amps maximum peak for an incorrect key), for the TDPL implementation, it is only marginally higher than the other ones (7.524 Micro Amps maximum peak for an incorrect key). In order to minimize this effect, the enhanced differential pull-down network (DPDN) introduced for SABL [16], can be applied to TDPL as well.

V. CONCLUSION

A flip-flop consistent with the DPA-resistant logic family TPDL has been introduced and compared to the power analysis. From the performed experimental results on a case study in a 65-nm CMOS process with 1.8V and 50MHZ operating frequency, it follows that the proposed implementation shows constant power consumption and also reduce the power dissipation.

ACKNOWLEDGMENT

The research for this paper was carried was carried out as a part of master's desertion of Nandhini M and the same feels extremely indebted to Asst. Prof. Muralidharan for his guidance and commitment throughout the project and for the much needed crucial assistance provided by Prof.Varatharaj.

REFERENCES

[1] Marco Bucci, Luca Giancane, Raimondo Luzzi, and Alessandro Trifiletti (2012) introduced, the "a flip-flop for the dpa resistant three-phase dual-rail pre-charge logic family", in proc. ieee int. on very large scale integration system pp. 2128–2132.

[2] P.Kocher, J. Jaffe, And B. Jun, "Differential Power Analysis," In Proc.Adv. Cryptol. (Crypto), 1999, Pp. 388–397.

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

[4] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Improving the security of dual-rail circuits," in Proc. Workshop Cryptograph. Hardw.Embed cards," in Proc. IEEE 28th Euro.Solid-State Circuit Conf. (ESSCIRC), 2002, pp. 403–406.

[5] 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.. Syst. (CHES), 2004, pp. 282–297.

[6] 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.

[7] 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.

[8] T.PoppandS.Mangard,"ImplementationaspectsoftheDPA-resistantlogic style MDPL," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS),2006, pp. 2913–2916.

[9] 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.

[10] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-railpre chargelogic,"in Proc.Workshop Cryptograph.Hardw Embed.Syst. (CHES), 2006, pp. 232–241.

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

[12] R. Anderson, E. Biham, and L. Knudsen, "Serpent: A Proposal for theAdvanced Encryption Standard," NIST AES proposal, 1998. [Online].Available:http://www.cl.cam.ac.uk/ftp/users/ria14/serpent.pdf

[13] F. Regazzoni, T. Eisenbarth, A. Poschmann, J. Großschädl, F.Gurkaynak, M. Macchetti, Z. Toprak, L. Pozzi, C. Paar, Y. Leblebici,and P. Ienne, "Evaluating resistance of MCML technology to poweranalysis attacks using a simulation-based methodology," Trans. Computation. Sci. IV, vol. 5430, pp. 230–243, 2009.

[14] K. J. Kulikowski, M. Su, A. Smirnov, A. Taubin, M. G. Karpovsky,and D. MacDonald, "Delay insensitive encoding and power analysis:A balancing act," in Proc. 11th IEEE Int. Symp. Asynch. Circuits Syst.(ASYNC), 2005, pp. 116–125.

[15] K. J. Lin, S. C. Fang, S. H. Yang, and C. C. Lo, "Overcoming glitches and dissipation timing skews in design of DPA-resistant cryptographic hardware," in Proc. Conf. Exhib. Design, Autom. Test Euro. (DATE),2007, pp. 1–6.

[16] K. J. Kulikowski, M. G. Karpovsky, and A. Taubin, "Power attacks on secure hardware based on early propagation of data," in Proc. 12th IEEE Int. On-Line Test. Symp., 2006, pp. 131–138.

[17] K. Tiri and I. Verbauwhede, "Design method for constant power con-sumption of differential logic circuits," in Proc. Conf. Exhib. Design,Autom., Test Euro. (DATE), 2005, pp. 628–633.

AUTHORS PROFILE

NANDHINI M, Graduated with B.E in Electrical and Electronics Engineering degree from Ranganathan Engineering College, Coimbatore India 2012 and is currently perusing M.E Applied Electronics from Christ the King Engineering College, Coimbatore [TN], India.

MURALIDHARAN V, Graduated with B.E in Electronics and Communication Engineering degree from Graduated with B.E in Electronics and Communication Engineering degree from Maharaja Prithvi Engineering College, Coimbatore India in 2010, and M.E VLSI from Ramakrishna College of Engineering Coimbatore [TN], India in 2012 and Currently working in Christ the King Engineering College, Coimbatore [TN], India.

VARATHARAJ M, Graduated with B.E in Electrical and Electronics Engineering degree from Coimbatore institute of Technology India in 2005, and M.E Applied Electronics From Bannari Amman Institute of Technology [TN], India in 2007, Currently perusing Ph.D from Anna University [TN], India.