A CHARGE RECYCLING THREE-PHASE DUAL-RAIL PRE-CHARGE LOGIC BASED FLIP-FLOP

Kothagudem Mounika, S. Rajendar, R. Naresh

Department of Electronics and Communication Engineering,
Vardhaman College of Engineering, Hyderabad, India.

ABSTRACT

Providing resistance against side channel attacks especially differential power analysis (DPA) attacks, which aim at disclosing the secret key of cryptographic algorithm is one of the biggest challenges of designers of cryptographic devices. In this paper design of novel data flip-flop compatible with three-phase dual-rail logic (TDPL), called Charge recycling TDPL flip-flop is investigated. The new flip-flop uses inverters that uses the charge recycling technique where charge stored on high output node during evaluation phase is used to partially charge the low output node in subsequent pre-charge phases. As a result less charge comes from the power supply thus lowering the power consumption. Simulation results in Cadence Virtuoso 45 nm CMOS process show improvement in power consumption in inverter up to 60% while CRTDPL flip-flop consumes around 50% less power compared to TDPL flip-flop.

KEYWORDS

Side Channel attacks, Differential Power Analysis (DPA), Sense Amplifier Based Logic (SABL), Three-Phase Dual-rail Pre-charge logic (TDPL) Charge recycling TDPL

1. INTRODUCTION

Security of cryptographic devices is very important now-a-days mainly in devices like smart cards. But their security depends on the security of cryptographic algorithm and the secret key. However there are some methods that break the security by attacking the physical implementation of the cryptographic device.

Side channel attacks are considered as a threat for cryptographic hardware. These attacks are accelerated by just observing the respective target. These observational results yield the secret key. Differential Power Analysis (DPA) [1]-[4] takes the advantage of the fact that power consumption of digital circuits depends on the data being processed. That is even if a small relationship between the switching activity and the data being processed is known the secret key is disclosed. So just by observing the variations in the power consumption the secret key is revealed.

Many measures have been introduced to defeat DPA since they are introduced. Dual-Rail Pre-charge Logic (DPL) is a counter-measure which aims at making the circuit switching activity constant and independent of the data being processed. There are various counter-measures at different levels of abstraction. Masking is one approach at algorithmic level [5]-[6]

At the circuit level the approach is quite different. That is if the side channel information is prevented from being created then there is no way for the information to be leaked. This is done

DOI : 10.5121/vlsic.2014.5605

by making the power consumption constant without varying. Sense Amplifier Based logic (SABL) is one such logic [2].

Another solution has been proposed in [6]-[7]: A Three Phase Dual rail pre-charge logic where an additional third a phase called Discharge phase in addition to the existing Pre-charge and Evaluation phases is introduced to discharge the output that is high even after the evaluation phase.

This paper proposes a novel approach which shows lower overhead in terms of power consumption. The novel approach uses the concept of charge recycling. However the early propagation leakage [8]-[10] is a leakage in CRTDPL as in SABL and TDPL because of pull down network but enhanced pull down network introduced for SABL [9] can be used to CRTDPL also. The new charge recycling three-phase dual-rail pre-charge logic inverter (CRTDPL) operation is summarized in section 2. The flip-flop implementation is presented in section 3 Section 4 contains simulation results. Comparison results and Voltage and temperature variations are carried out in section 4. Finally conclusion is presented in section 5.

2. CHARGE RECYCLING THREE-PHASE DUAL-RAIL PRE-CHARGE LOGIC INVERTER (CRTDPL)

Charge recycling TDPL (CRTDPL) like SABL and TDPL is Domino logic, so CMOS inverters must be inserted between two cascaded gates to avoid glitches when NMOS-NMOS and NMOS-PMOS devices are cascaded. By doing this inputs to the logic gate at the evaluation phase beginning are low and also the outputs driving the gate are pre-charged to V_{DD} and one output goes high when one evaluates.

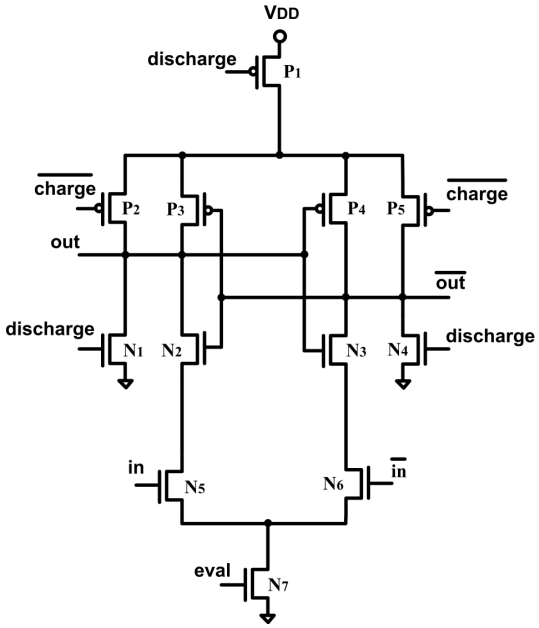


Figure 1. TDPL inverter

CRTDPL is proposed as the enhancement to TDPL logic style with decrease in the number of transistors and power consumption. TDPL inverter and CRTDPL inverter are shown in figures 1 and 2 respectively. The timing diagram of Charge recycling TDPL is shown in figure 3. The CRTDPL retains the three phase operation of TDPL [7]. It has three clock signals pre-charge, evaluate and discharge. The two inverters differ in one point. The two PMOS transistors that pre-

charge the output nodes are replaced by only one PMOS transistor between the output nodes of the CRTDPL.

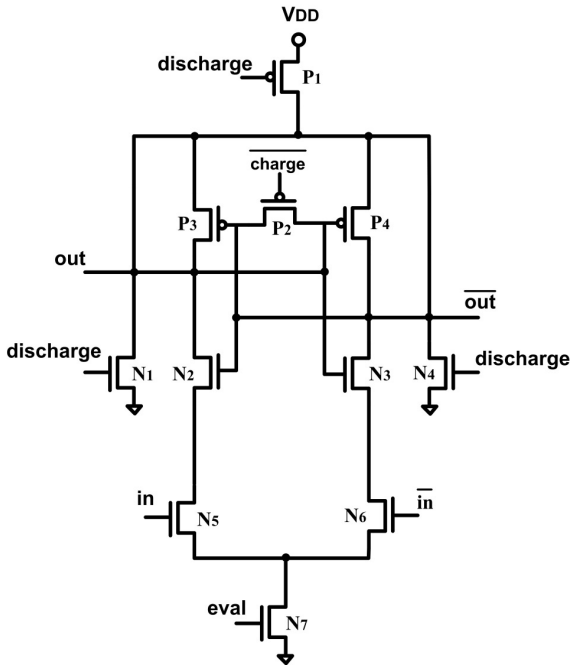


Figure 2. Charge recycling TDPL

CRTDPL consumes less power because of charge recycling. During the evaluation phase the charge is stored at one of the output nodes of the inverter. This charge is used to charge the other output node in the subsequent pre-charge phases. As a result less charge comes from the power supply, thus low power consumption profile is exhibited by CRTDPL inverter.

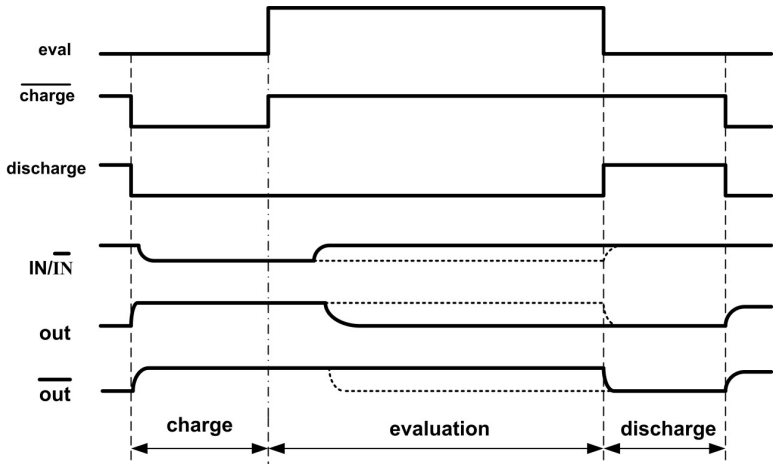


Figure 3. Timing diagram of CRTDPL inverter

3. FLIP-FLOP IMPLEMENTATION

The implementation of flip-flop that is compatible with CRTDPL gates is shown in the Figure. 4, the timing diagram is shown in figure. 5

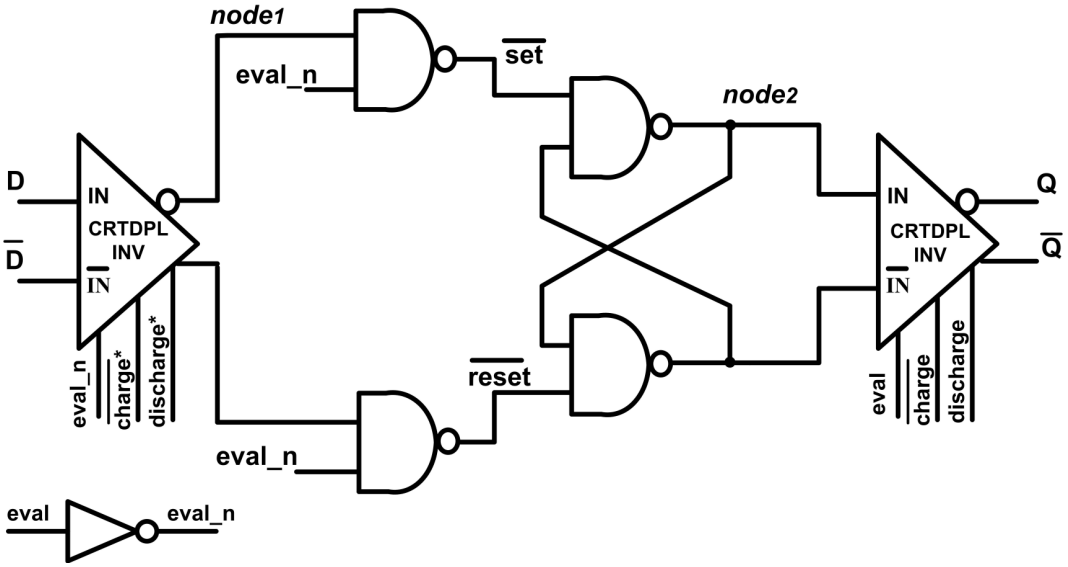


Figure 4. Charge Recycling TDPL flip-Flop Using CRTDPL Inverters

With reference to figure 4 the CRTDPL Flip-Flop uses two CRTDPL inverters and an intermediary circuit (NAND gates), which drives the output of the first inverter to the SR latch that holds the output between them. When one inverter is in evaluation phase the other inverter is in discharge or pre-charge phase. The intermediate circuit prevents the SR latch from entering into invalid state when set-bar and reset-bar are 0.

The flip-flop uses two inverters which are having the evaluate clock signal inverted. The flip-flop's operation is similar to the TDPL flip-flop presented in [7] but the only difference is the way the intermediary circuit is designed. The intermediary circuit that drives the input inverter outputs to the SR latch in [7] is replaced by a NAND gate that performs same operation of intermediary circuit. By doing this the power consumption of the flip-flop is reduced.

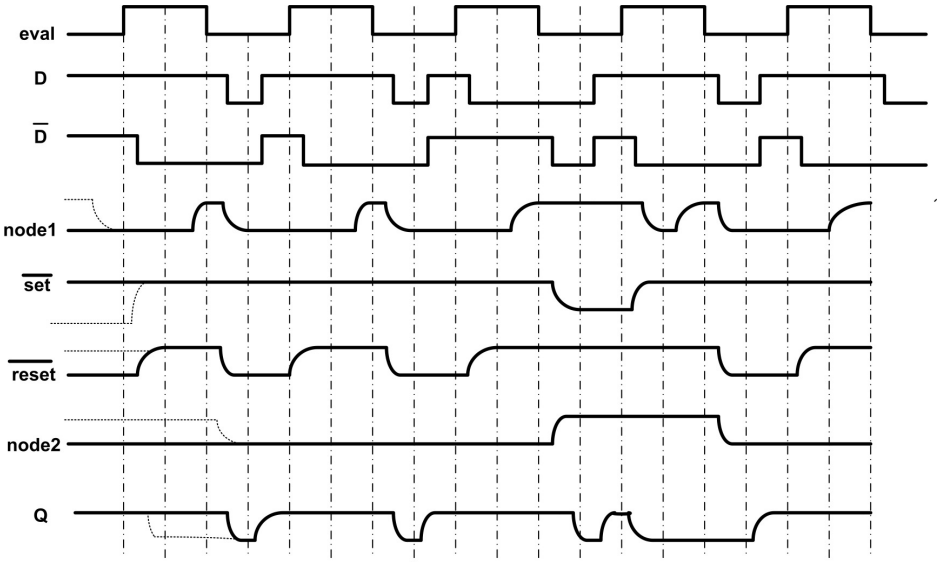


Figure 5. CRTDPL flip-flop timing diagram

4. SIMULATION RESULTS

4.1 Simulation Environment

All the circuits have been simulated using Cadence Virtuoso tool using 45nm technology. Both CRTDPL inverter and TDPL inverter and also TDPL flip-flop and CRTDPL flip-flop are simulated on same input patterns.

4.2 Simulation Comparison

In this section proposed design CRTDPL is compared with the existing TDPL family. Table 1 shows comparison results of CRTDPL and TDPL inverters and Flip-Flops in 45nm technology. It shows that CRTDPL consumes low power compared to TDPL. Figure 6 shows the histogram of the CRTDPL and TDPL inverter and flip-flop in 45nm technology. Simulation results show improvement in power consumption in inverter up to 60% while CRTDPL flip-flop consumes 49% less power compared to TDPL flip-flop. Table 2 shows the power consumption variation of CRTDPL inverter and flip-flop for various supply voltages ranging from 0.4 to 1.2V. From the table it is clear that the power consumption increases as supply voltage increases.

Table 1. Comparison results of TDPL and CRTDPL inverter and Flip-Flop

Designs	**Power (µW)**	
	TDPL	**CRTDPL**
Inverter	5.63	2.25
Flip-Flop	19.20	9.78

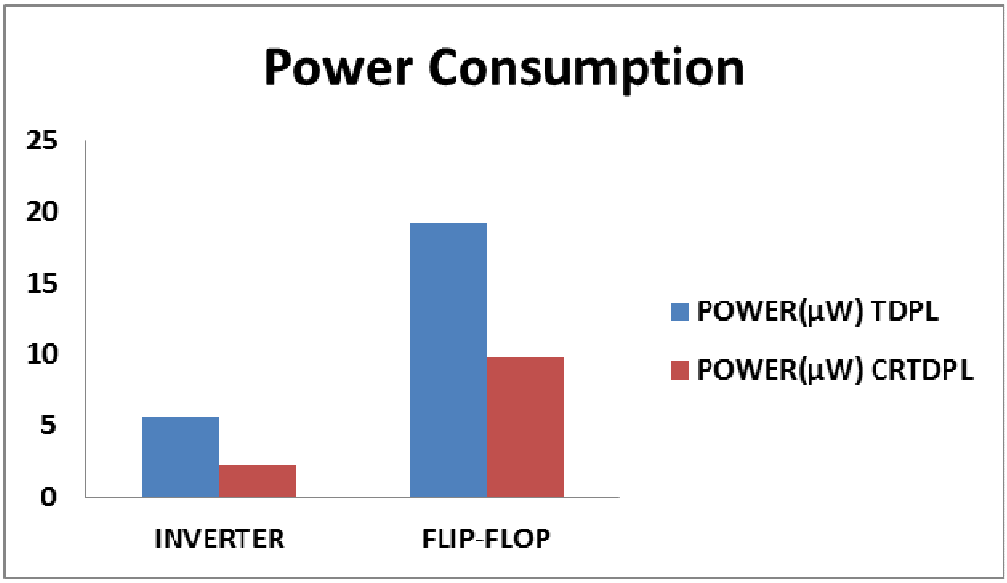


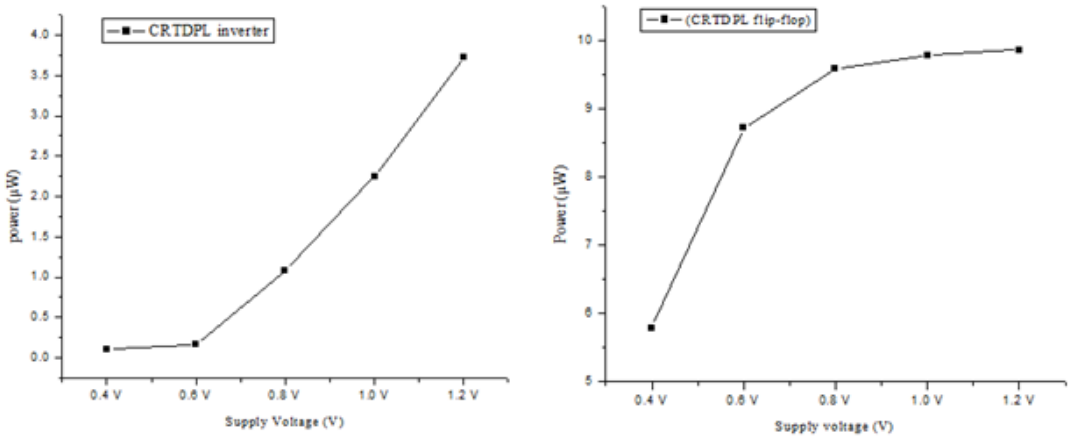
Figure 6. Comparison of Power consumption of CRTDPL, TDPL inverter and flip-flop

Table 2. Power consumption variation of CRTDPL inverter and flip-flop for various supply voltages

Supply Voltage	**POWER(µW)**	
	CRTDPL INVERTER	**CRTDPL FLIP-FLOP**
0.4 V	0.11	5.79
0.6 V	0.17	8.72
0.8 V	1.08	9.59
1.0 V	2.25	9.78
1.2 V	3.72	9.87

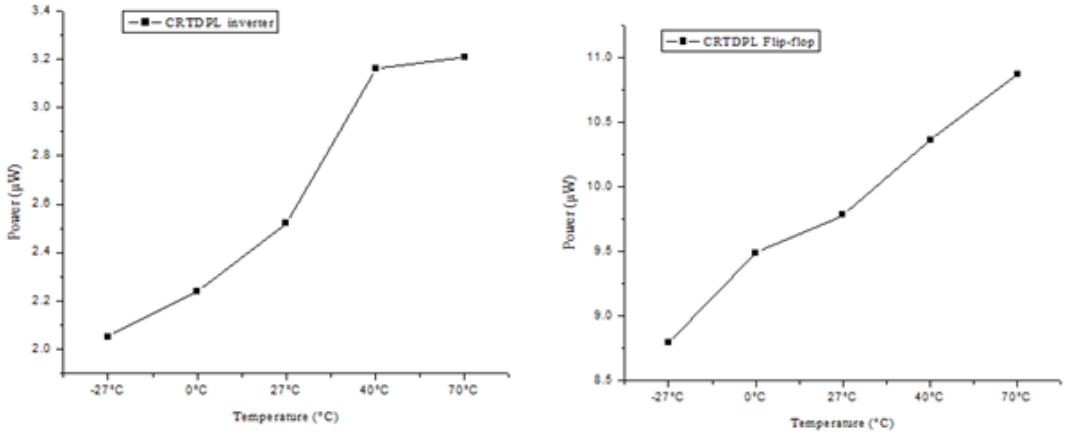
Table 3. Power consumption variation of CRTDPL inverter and flip-flop for various temperatures

Temperature	**POWER(µW)**	
	CRTDPL INVERTER	**CRTDPL FLIP-FLOP**
-27°C	2.05	8.79
0°C	2.24	9.49
27°C	2.52	9.78
40°C	3.16	10.36
70°C	3.21	10.87



a) b)

Figure 7. a) Power consumption versus supply voltage of CRTDPL inverter
b) Power consumption versus supply voltage of CRTDPL flip-flop



a) b)

Figure 8. a) Power consumption versus temperature of CRTDPL inverter
b) Power consumption versus temperature of CRTDPL flip-flop

Table 2 shows the power consumption variation of CRTDPL inverter and flip-flop for various temperatures ranging from -27^0C to 70^0C. From the table it is clear that the power consumption increases as temperature increases. Figure 8 shows the various graphs representing power consumption variation with various temperatures and supply voltages.

5. CONCLUSIONS

A charge recycling TDPL inverter that shows resistance to DPA attacks is introduced and using the CRTDPL inverter a flip-flop is designed and compared to the existing TDPL flip-flop. From the experimental results in 45 nm CMOS process it follows that the proposed implementation of CRTDPL inverter 60% power efficient compared to TDPL inverter. The CRTDPL flip-flop consumes around 50% lower power than that of TDPL flip-flop. Also the variation of power consumption with various temperatures and supply voltages is carried out.

REFERENCES

[1] P. Kocher, J. Jaffe & B. Jun, (1999) “Differential Power Analysis,” Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology, pp 388-397

[2] K. Tiri & I. Verbauwhede “A logic design methodology for secure DPA resistant ASIC or FPGA implementation”, in proc. Design, Autom., Test Euro. Conf. Expo. (DATE), pp246-251.

[3] K. Tiri, M. Akmal & I. Verbauwhede, (2002) “A dynamic and differential CMOS logic with signal independent power analysis on smart cards,” in proc. IEEE 28th Euro. Solid-State circuit Conf. (ESSIRC), pp403-406.

[4] D. Slokov, J. Murphy, A. Yakovlev, (2004), “Improving the security of dual-rail circuits", in proceedings Workshop Cryptograph, Hardware. Embedded. System (CHES) pp281-287.

[5] T.Popp, M. Kirschbaum, T. Zefferer & S. Mangard, (2007) “Evaluation of masked logic style MPDL on prototype chip,” in proc.Workshop Cryptograph. Hardware. Embed. Syst. (CHES), pp81-94.

[6] N. Pramstaqller, E. Oswald, S. Mangard, F. K. Gurkaynak, and S. Haene (2004), “ A masked AES AISIC Implementation”, in Austrochip,pp77-82

[7] M. Bucci, l. Giancane, R. Luzzi & A. Trifiletti, (2006) “Three-phase dual-rail pre-charge logic,” in Proc.Workshop Cryptograph. Hardw. Embed. Syst. (CHES), pp232-241.

[8] Marco Bucci, Luca Giancane, Raimondo Luzzi & Alessandro Trifiletti , (2012) “ A flip-flop for DPA resistant three-phase dual-rail pre-charge logic family,” in Proc. IEEE VLSI Syst.,Vol.20, No.11, pp2128-2132.

[9] K. J. Kulikowski, M. G. Karpovsky, & A. Taubin, (2006) "Power attacks on secure hardware based on early propagation of data," in proc. 12th IEEE Int. On-Line. Symp. (DATE), pp131-138.

[10] K. Tiri & I. Verbauwhede, (2005) "Design method for constant power consumption of differential logic circuits," in Proc. Conf. Exhib. Design, Autom. Test Euro., pp. 628-633.

AUTHORS

Kothagudem Mounika received her Bachelor's Degree from Jawaharlal Nehru Technological University, Hyderabad. She is currently pursuing her Master's Degree at Vardhaman College of Engineering, Hyderabad under JNTU, Hyderabad. Her research interests include Low Power Design Techniques.

S. Rajendar received his Bachelor's Degree and Master's Degree from Jawaharlal Nehru Technological University, Hyderabad, India. He is currently pursuing his Ph.D from JNTU, Hyderabad. At present he is working as Associate Professor in the department of Electronics and Communication Engineering at Vardhaman College of Engineering, Hyderabad, India. He is having 11 years of teaching experience. He is a member of IEEE, ISTE, SAISE, IAENG, UACEE, and IACSIT. He has more than 20 research publications in national and international conferences and journals to his credit. He has authored two books Electronic Devices and Electronic Devices and Circuits. His research interests include High-performance VLSI circuit design, Interconnect Modelling and Analysis.

Naresh R received his Bachelor's Degree and Master's Degree from Jawaharlal Nehru Technological University, Hyderabad, India. His research interests include Low Power and high performance Design Techniques.