Advanced Design for DPA Resistant Circuit by using Optimizing Differential Logic Gates

Kiran Kumar[1] K. Rajasekhar[2]
[1]M.Tech Student [2]Assistant Professor & Project Guide
[1,2]Department of Electronics & Communication Engineering
[1,2]Baba Institute of Technology & Sciences, Visakhapatnam, India

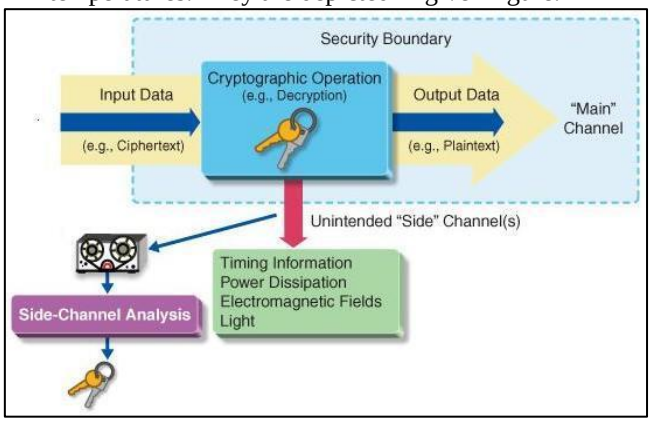
Abstract— Differential Power Analysis used in the crypto circuits may be attacked by an another/separate party, using power consumption dependence on secret message/information for hiding critical data (information).To avoid DPA and security basis differential logic styles are basically used, because of constant power dissipation. This paper is also proposed a new design methodology to improvement of pull-down logic configuration for most differential gates are secured. Previously the AND/NAND and XOR/X NOR gates in 90nm VLSI technology, using by SABL (Sense Amplifier Based Logic) for DPDN (Differential Pull down Logic). A new Proposals OR/NOR gates are used to secure/protect Differential logic gates at 90nm technology at 27oC temperature with simulate to help of Micro Wind and DSCH to eliminate charge in the pull-down differential gate and remove the memory effect.

Key words: DPA (Differential Power Analysis), Side Channel Attack, Sense Amplifier Based Logic (SABL), Differential Pull Down Network (DPDN), Dynamic and Dual-Rail Gate Logic Style, VLSI 90nm Technology, Single Switch Solution, Differential Logic Gates (AND/NAND, XOR/XNOR, OR/NOR)

I. INTRODUCTION

Now a day's security is the most important concern. Encryption is usually based on exact protected algorithms, considered to make a secret message text from a basic text, which cannot be mathematically attacked. However, the physical performance of the encryption algorithm -SCI (side-channel information) that preserves is used by an attacker to trace the important secret key. Side channel attacks (SCA"s)

1) on the hiding policy used for extracting the information through different techniques & some defaults/weaknesses which give away the chance to
2) Find out the confidential key through power utilization, instant delay, and electromagnetic emission, etc. DPA attack is based on the well-recognized information that active power utilization in a logic circuit. Thus, an attacker can acquire the top secret key by measuring the current from power supply of the cryptographic device while doing the encryption mechanism as power provide current of a hiding mechanism as it is the stage an encryption, and by analyzing the exact power traces. Side channel attacks (SCAs) [2] on cryptographic devices use definite objective data such as power utilization, instant delay, and electromagnetic emission to find out the Secret key. Side channel attack is basically attacking for side channel information, to measuring for the secret information or secret massage. Side channel attack is mainly attacked (Leaks key dependent information) Side Channel Attacks are attacks that are based on "Side Channel Information" as like delay, power dissipation, charge stored and also process variations in temperatures. They are depicted in given figure.



The Side-Channel (Leaks key dependent information)

Fig. 1: Basic Side Channel Attack

Differential power analysis (DPA) [3] is one of the common calculate for its simplicity and effectiveness. DPA attack is based on the well-recognized information that active power utilization in a cause circuit is temporary on the data individual process by the device. Thus, an attacker can acquire the top secret key by measure the power supply current of a cryptographic mechanism while it is performing an encryption, and by statistically analyze of the exact power traces. On the extra hand, circuit-level neutralizer is new common, since they are not unnatural to one unambiguous cryptographic algorithm. Previously a practical technique has been establish, designer require be troubled no more about the protection of implementations for an exact algorithm, and this construct regular propose possible. This kind of explanation fall into two categories: gate level masks circuits and balancing circuits.

SABL (Sense Amplifier Based Logic) is taken into consideration because in this style, the differential logic designs are provided with constant power supply. Some other logic styles are gate level masking, complementary circuits and DPA algorithms as depicted in the fig.2.

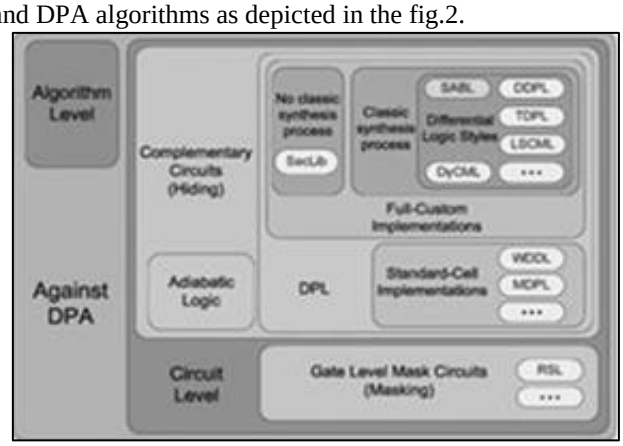


Fig. 2: Various Measures against DPA

The SABL logic style [4] when it is used with, Dynamic Current Mode Logic (DyCML) [5], Low-Swing Current Mode Logic (LSCML) [6], Three-Phased Dual-Rail Pre-charge Logic (TDPL) [7] is less attacked by DPA. SABL is a differential logic technique that has the following requirements apart from the other design styles: it has one charge event and uniform capacitance charges. SABL achieves better results because their internal structure suppresses the influence of internal capacitances better than the reduced output swing used by DyCML and LSCML.

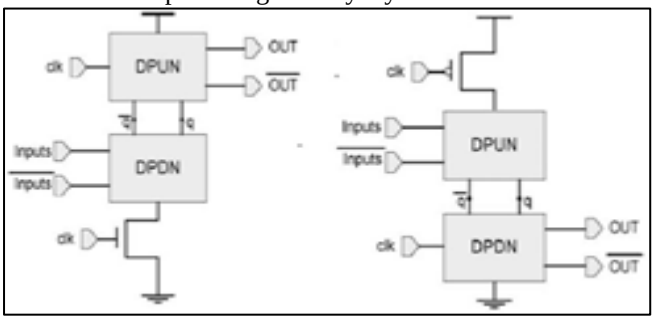


Fig. 3:

DPDN	#trns DPDN	AND/NAND		XOR/XNOR		Drawbacks
		^{E}avg	σ_e	^{E}avg	σ_e	
SABL[4]	12	1	1	1	1	Sensible to unbalanced outputs
DyCML [5]	13	1.996	126.7	1.976	≈1e8	Sensible to unbalanced outputs Reduced output swing
LSCML [6]	13	131.80	1.553	1.50	≈1e5	Sensible to unbalanced outputs Reduced output swing
TDPL[7]	14	1.333	0.80	1.40	1.28	Generation and routing of additional control signal
DDPL[8]	8	1.251	0.24	1.30	0.66	Need of level converts and present timing

Table 1: Features and Performances of Full-Custom Secure DPL Techniques

From table 1, it shows that SABL gates provide the best trade-off in hardware resources, power and security, especially if balanced outputs are provided. It is inferred from table1 that Sense Amplifier Based Logic style is preferred because it is sensible to unbalanced outputs with constant power, low energy consumption, reduced delay and difficult to attack power traces by the effect of DPA. In this, the DPDN network is considered while pull down configuration energy consumption is reduced due the effect caused by sensing amplifier.

II. SABL TECHNIQUE FOR DPA RESISTANCE IN DPDN NETWORK

The necessary circuit design of a differential DPL cell is shown in Fig.2.The DPDN in Fig. 2(a) is typically implemented with NMOS transistor coupled to the bottom locked NMOS transistor. With no loss of majority, a DPA-resistant gate can also be constructing with the logic function implement in the DPUN with PMOS transistors and a clocked PMOS transistor on. As mentioned, SABL fulfils all the necessities for DPA resistance. Fig. 3 shows the DPUN formation for SABL. SABL operates as follows

Fig.3. Dynamic and dual-rail gate logic style. (a) Using N-MOS transistors to implement the DPDN block logic function. (b) Logic function implemented with P-MOS transistors (DPUN) Differential circuits utilize their inherent symmetry to have same consumptions for "0" and "1" evaluations, as both the true and complemented outputs are generated simultaneously. Fig. 3 shows a typical scheme for a dynamic differential logic style. Such logic styles contain a differential pull-down network (DPDN) performing the logic function and a differential pull-up network (DPUN) working in alternate pre charge and evaluation phases. They provide the complementary outputs at every clock cycle with a single clock event. Way that the right and false networks were reversed among the two WDDL instances.

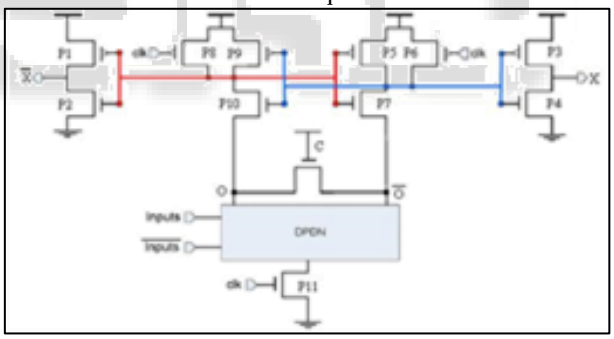


Fig. 4: SABL Logic Style

The properties of SABL that makes it resistant to DPA are :1) an existence for clocked base transistor P11 2) complete balance in DPUN, also 3) Outputs of DPDN having no connection to the gate of output inverters (P1/P2 and P3/T4). Even using a proper common method for SABL in DPUN, the DPDN must be balanced for implementing the logic regardless of input. For making an effective DPDN to counter the DPA attacks, it should be completely balanced, equal number of NMOS series transistors with equal resistance in all paths. The gate operates with a constant delay regardless of input values. Fig. 4 shows AND/NAND and XOR/XNOR for DPDN.

III. OPTIMIZATION OF DPDN (DIFFERENTIAL PULL DOWN NETWORKS)

A method for matching the charge in internal nodes in the pre charge phase. This can be achieved mostly in two main

different ways: 1) by recycling the charge and equalizing it by it sharing among the internal nodes and 2) by charging/discharging all the internal nodes to the equal final value.

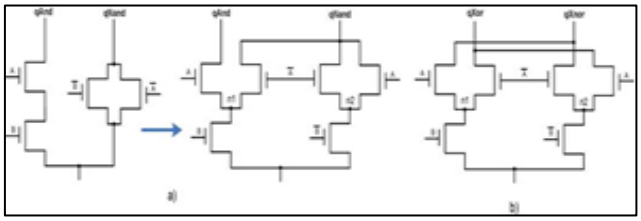


Fig. 5: Realization of an (a) NMOS AND/NAND and (b) NMOS XOR/XNOR DPDN

A. Single-Switch Solution (P)

The internal nodes in the similar level are attached together for a differential logic function for any DPDN execution a

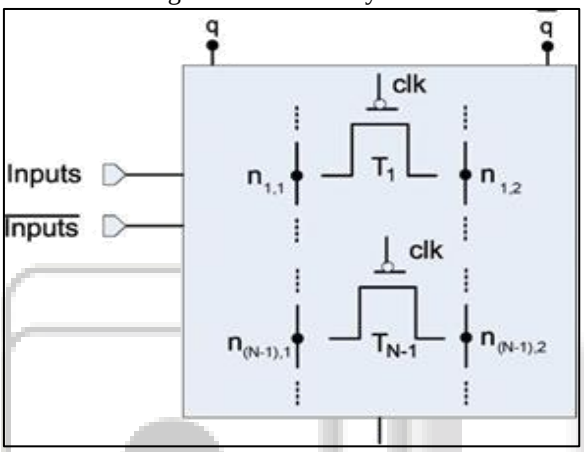


Fig. 6:

Fig.6 fo. Single-switch Solution scheme r N-depth DPDN switch which is ON during the pre-charge phase (clock=0), by making voltages equal in the same level. There is only one switch for each transistor level in the DPDN except for the first one, which gives the complementary outputs. In the SABL structure, these are interconnected with the intermediate Vdd-gated NMOS transistor that is always ON. This measure confirms accurate distribution of charge during pre-charge without any leakage of information. In SABL, only a single phase clock is needed.

B. Dual-Switch Solution (2P)

In the DPDN style the intermediate nodes are fixed to supply/ground terminals with independent switches while pre-charge, driving exactly the same voltage in all nodes. Exactly one pair of switches is required for each DPDN level except for first one, which generates the true and the complemented output. In the SABL structure, these are interconnected with the intermediate Vdd-gated NMOS transistor which are ON continuously. Thus, for an N-depth DPDN, 2(N-1) switches are required. In single-switch configuration, the only possible solution uses PMOS switches that are ON during pre-charge.

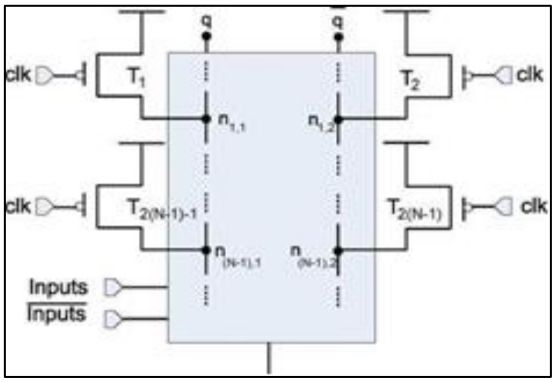


Fig. 7: Dual-switch Solution Scheme for N-Depth DPDN

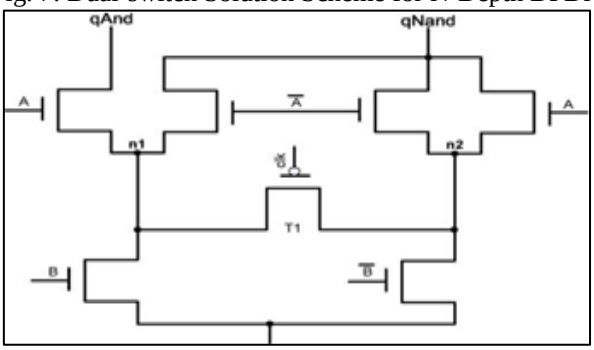


Fig. 8: AND/NAND DPDN with Single-Switch Solution

Without any leakage of information. In SABL, only a single phase clock is needed. Solution are presented respectively in Fig.10 and Fig.11.

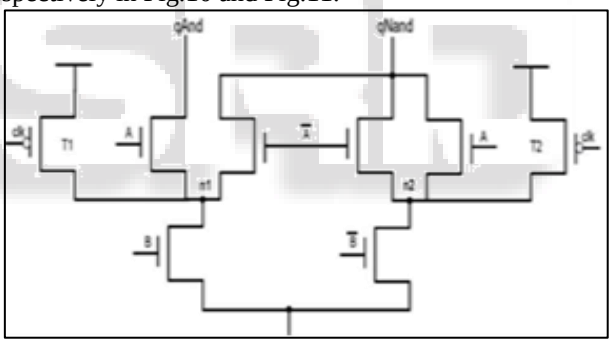


Fig. 9: AND/NAND DPDN with Dual-Switch Solution

IV. SIMULATION AND RESULTS (EXISTING SYSTEM)

The proposed technology of SABL gates is performed using AND/NAND type and XOR/XNOR type of design in sense amplifier based logic is simulated in Micro Wind Tool and Digital Schematic Editor and Simulator (DSCH) using VLSI 90 nanometer technology . It is carried out using nominal conditions, i.e., for classic transistors, Vdd and at temperature of 25^0C [9]. The inputs and outputs of the entry individual tested were passed through gates of same style having low clock frequency being 0.500GHz.The power consumption for all the possible combinations were measured. The Differential Pull down Logic (DPDN) in AND/NAND Gate for results.

Single and dual switch solution and in XOR/XNOR [10] shown below.

A. Results

The Differential Pull down Logic (DPDN) in AND/NAND Gate for single and dual switch solution is given by

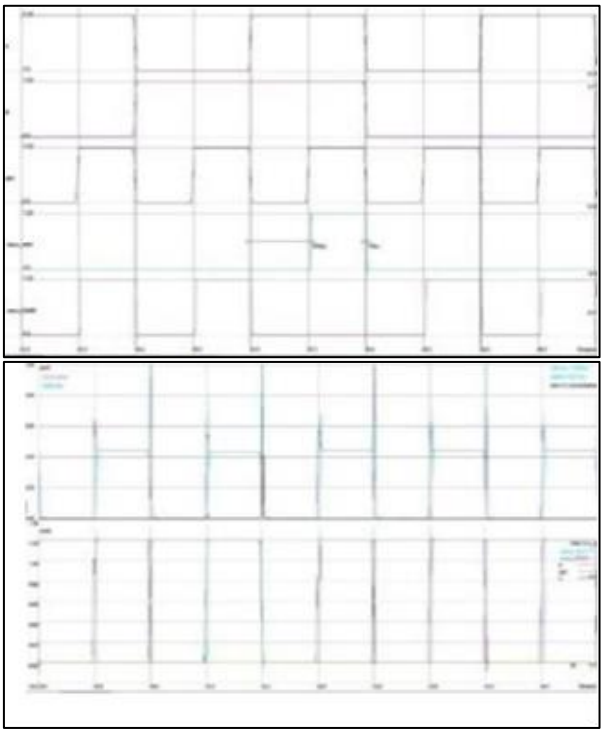


Fig. 10: AND/NAND Simulation for a and b are Single and Dual Switch Solution

SABL Style	00	01	10	11
AND (P&2P)	0.272mw	0.272mw	0.272mw	0.272mw
NAND (P&2P)	0.272mw	0.272mw	0.272mw	0.272mw

Table 2: Performance AND/NAND with Single (P) and Dual (2P) Solutions

The Differential Pull down Logic (DPDN) in OR/XNOR Gate for single switch solution is given by

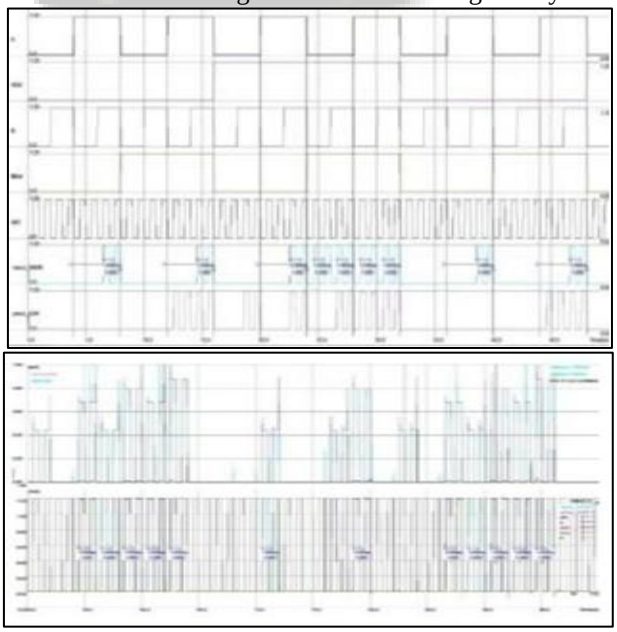


Fig. 11: XOR/XNOR Simulation for single and dual switch solution

SABL Style	00	01	10	11
NOR (P&2P)	0..202mw	0..202mw	0..202mw	0..202mw
XNOR (P&2P)	0..202mw	0..202mw	0..202mw	0..202mw

Table 3: Performance AND/NAND with Single (P) and Dual (2P) Solutions

V. IMPLEMENTATION

A new proposals OR/NOR gates are used to secure/protect differential logic gates at 90nm technology, to eliminate charge (Power is Reduced) in the pull-down of a differential gate and remove the memory effect. In Sense Amplifier Based Logic (SABL) gate in Differential Pull down Network (DPDN) circuit using by OR/NOR gates for single switch solution and dual switch solution. Because of the removing memory effort by calculating power analysis.

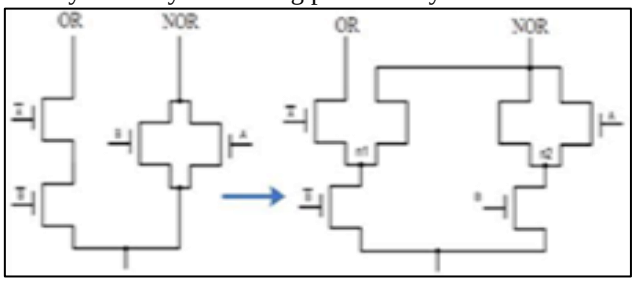


Fig. 12: Single/Dual Switch Solution for OR/NOR Gates

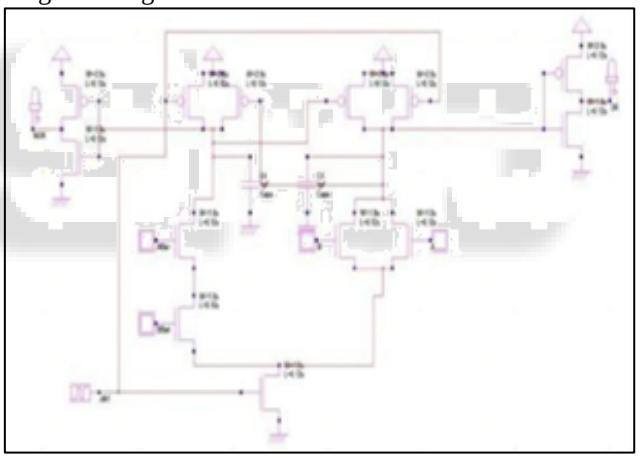


Fig. 13: SABL Style for DPDN for OR/NOR Gates

VI. RESULTS

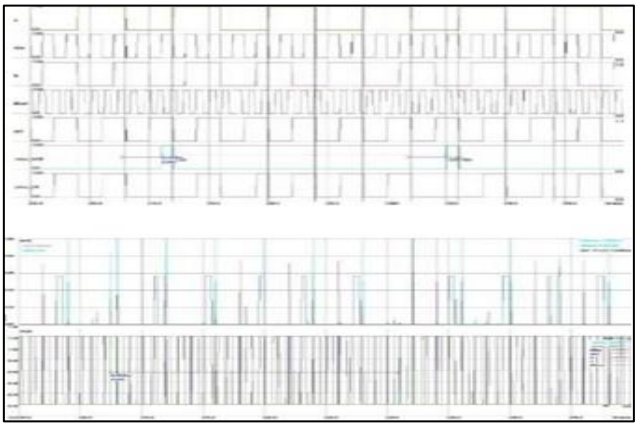


Fig. 14: XOR/XNOR Simulation for single and dual switch solution

SABL Style	00	01	10	11
OR (P&2P	0.130mw	0.130mw	0.130mw	0.130mw
NOR (P&2P)	0.130mw	0.130mw	0.130mw	0.130mw

Table 4: Performance AND/NAND with Single (P) and Dual (2P) Solutions

VII. PERFORMANCE EVALUATIONS

The simulations are performed at 25ºc temperature. The delay, energy deviation and also number of transistor are calculated for SABL style in DPDN network for single switch and dual switch solution for AND/NAND, XOR/XNOR and also OR/NOR gates to protect security bases of view is given by in this table Single switch solution is represented with 'P' and Dual switch solution is represented with '2P'.

DPDN gate in SABL style	Transistor for SABL	Total Power (mw)	Delay in (ps)	Energy consumption (fj)
AND/NAND	16	P -> 0.272 2P ->0.272	250	30.25
XOR/XNOR	15	P ->0.202 2P ->0.202	220	26.03
OR/NOR	13	P->0.130 2P ->0.130	190	22.28

Table 5: Performance Comparison of DPDN Gates

VIII. CONCLUSION

This paper implemented to provide security data transmission through Crypto circuits. The implemented method uses OR/NOR gate in pull down configuration based on SABL (Sense Amplifier Based Logic) for DPA resistant circuits. This mechanism provide eliminates the memory effect with the help of single and dual switch solution in the use of differential pull down network. So the total power is reduced due to internal effect charge used. The memory effect and energy deviation is also successfully reduced to secure/protect differential networks against DPA Resistance Circuit. The proposed results for OR/NOR gates in Differential logic gates which are provided to eliminate the internal charge stored at the pull down configuration in SABL (Sense Amplifier Based Logic). The designed methodology is implemented using CMOS technology at 90nm for complementary circuits for hiding the secret information/data. By implementing the design technique using OR/NOR gates, the number of transistors in DPDN gate in SABL style are reduced, the power consumption and the network delay are also reduced when compared with the existing methods.

REFERENCES

[1] Erica Tena-Sánchez, Javier Castro, and Antonio J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits", IEEE journal and systems (Vol.4, Issue. 2), 2014.
[2] Peter Gutmann, David Naccache, Charles C. Palmer "Side- Channel Attacks on Cryptographic Software" IEEE Journal on, (Vol.9, pp.1540-7993), (2009).
[3] P. Kocher, Jaffe, B. Jun, "Differential Power Analysis," Proc. Int. Cryptal. Conf., (pp.388-397), (1999).
[4] K.Tiri, M. Akmal, I. Verbau whede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," Proc. Eur. Solid-State Circuits Conf., (pp.403– 406), (2002).
[5] M.W.Allam, M.I.Elmasry,"Dynamic Current Mode Logic (DyCML): A New Low- power high- performance logic style," IEEE J.Solid-State Circuits, (Vol. 36, Issue. 3, pp. 550–558), (2001).
[6] Hassoune, F. Macé, D. Flandre, J.-D. Legat, "Low-swing current mode logic (LSCML): A new logic style for secure and robust smart cards against power analysis attacks," Micro electron. J., (Vol. 37, Issue.9, pp. 997–1006), (2006).
[7] M.Bucci, L.Giancane, R.Luzzi, A. Trifiletti, "Three-phase dual rail pre-charge logic," Proc. Int. Workshop Cryptography. Hardware Embed. Sys., (pp. 232–24), (2006).
[8] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Triletti, "Delay based dual-rail precharge logic," IEEE Trans. Very Large Scale (VLSI) Syst., (Vol. 19, no. 7, pp. 1147– 1153),(2011).
[9] D. Suzuki, M. Saeki, "Security evaluation of DPA countermeasures using dual-rail pre-charge logic style," in Proc. Int. Workshop Cryptograph. Hardware Embed. Syst., (pp. 255–269), (2006).
[10] L. Lin, W. Burleson, "Leakage-based differential power analysis (LDPA) on sub- 90nm CMOS crypto systems," Proc. IEEE Int. Symp Circuits Syst, (pp. 252– 255), (2008).

