A NEW IMPROVED MCML LOGIC FOR DPA RESISTANT CIRCUITS

A. K. Tripathy[1]

A. Prathiba[2] and V.S. Kanchana Bhaaskaran[3]

[1,2,3]School of Electronics Engineering
VIT University Chennai, India

ABSTRACT

Security of electronic data remains the major concern. The art of encryption to secure the data can be achieved in various levels of abstraction. The choice of the logic style in implementing the security algorithms has greater significance, and it can enhance the ability of providing better resistance to side channel attacks. The static CMOS logic style is proved to be prone to side channel power attacks. The exploration of CMOS current mode logic style for resistance against these side channel attacks is discussed in this paper. Various characteristics of the current mode logic styles, which make it suitable for making DPA resistant circuits are explored. A new methodology of biasing the sleep transistors of (MOS current mode logic) MCML families is proposed. It uses pass gate transistors for power-gating the circuits. The power variations of the proposed circuits are compared against the standard CMOS counterparts. Logic gates such as XOR, NAND and AND gate structures of MCML families and static CMOS are designed and compared for the ability of side channel resistance. A distributed arrangement of sleep transistors for reducing the static power dissipation in the logic gates is also proposed, designed and analyzed. All the logic gates in MCML and CMOS were implemented using standard 180 nm CMOS technology employing Cadence® EDA tools.

KEYWORDS

Side Channel Attack, DPA Resistance, Current Mode Logic, Cryptography

1. INTRODUCTION

Recently, an unprecedented growth of electronic products and the relevant security issues have come to the fore. The influence of electronics in pervasive computing needs confidentiality of the electronically processed and transmitted data. As of today, large volumes of data are being stored, processed and communicated through various electronic gadgets. The protection of data in such electronic devices poses a serious concern for both the system designers and developers, and as well for the clients.

Almost in all the digital applications, the static CMOS design of logic style has been used for the hardware implementation. This is due to the reason that CMOS has been proved robust with presumed negligible static power dissipation. Despite these characteristics, the deep submicron technology finds the use of CMOS curtailed due to its ever-increasing static power dissipation, vulnerability to side channel attacks through the power traces, and saturating high speed performance characteristics. The MOS current mode logic proves highly beneficial in such situations. In other words, the MCML is found to be more beneficial than the standard CMOS. In addition to its high speed operation which is necessary for high performance applications, it also

DOI : 10.5121/vlsic.2013.4505

has lower switching noise than its counterpart [1] [2]. These advantages make the MCML an ideal choice for circuits used in differential power attack resistant cryptographic circuits [3] [5] [6].

It may be pointed out that though the MCML gates enjoy high robustness and better speed performance characteristics, they require larger number of gates leading to increased silicon area. Furthermore, the constant current consumption of the gates makes it unsuitable for low speed applications [2].

In this paper, the MCML logic family is used for implementing the crypto-processors for providing enhanced security of electronic data. It makes use of the current mode scheme to reduce the dynamic power, realized by reduced voltage swing employed by MCML. Furthermore, the power-delay product of the circuit reduces due to enhanced delay performance achieved by proper sizing of the sleep transistor [1] [4]. The sleep transistors are used for power gating, and it eliminates the static power dissipation associated with current mode logic circuits. Through these factors, the paper validates the power gated MCML gates that achieve higher performance at low voltage and low-power operation.

This paper is organized as follows. The next section gives a brief overview of the different power attacks. Section III describes the operation of conventional MCML circuits with their advantages and disadvantages projected. The architecture of the proposed MCML circuit and its operation is also delved into in this section. Section IV describes the implementation procedure of MCML logic. The simulation results are analyzed against comparison with CMOS equivalent structures. Section V concludes.

2. POWER ANALYSIS

The instantaneous power consumption of any hardware cryptographic device is generally recorded through the power traces. The attacker performs analysis on this data and recovers the hidden information. The hidden information can be either a secret key used in a cryptographic algorithm implemented in hardware, or a PIN of any smart card. The concealed information can also be the intermediate data information. In the power analysis, the attacker attempts measuring and correlating the instantaneous power consumed by the circuit, the corresponding data under processing, or the nature of process that is being accomplished in the device at any time.

Power analysis is classified into two types, namely, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). Generally, these attacks are noninvasive. The SPA attacks recover the secret keys from direct measurement of the individual power consumption at any time. They are proved to be most effective when there is leakage of large amount of sensitive data such as the power trace. On the other hand, the DPA attacks use statistical methods to extract the information from a series of power consumption measurements taken over a certain period of time [3].

Almost all the recent cryptographic devices are implemented using semiconductor logic gates. These logic gates are constructed out of transistors. Electrons flow through these transistors causing currents and dissipating power across the loads. To measure the power consumption of the circuit, a resistor of a small value is inserted in series with the power or ground pins. The difference in voltage across the resistor divided by the resistance value gives the amount of current flowing through it. Such techniques of extracting secret information make any electronic circuit vulnerable to attacks.

3. MCML OVERVIEW

The most important property of the MCML gates that make them useful for designing DPA resistant circuits is the fact that the amount of current drawn from the power supply is independent on the switching activity. Furthermore, the MCML circuits provide true differential operation, incurs low switching noise, low voltage swing and low power dissipation at high frequencies. Due to these reasons, the MCML gates have been preferred for use in many IC applications.

3.1. MCML overview

The operating principle of a basic MCML cell is shown in Figure 1.

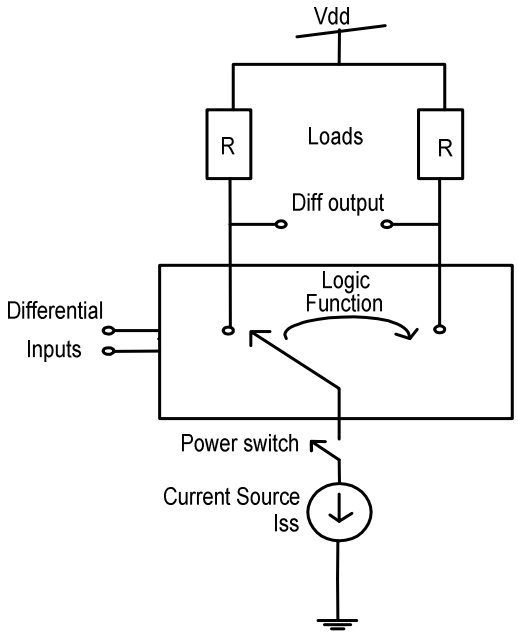

Figure 1. A Basic MCML logic circuit

The MCML cell consists of four main blocks, namely, the logic functional block, current source, power switch, and the load. The logic function is implemented using a differential pair of NMOS transistors. Depending on the complexity of the function levels, the NMOS transistors need to be stacked one upon the other to implement the logic function. The current source will provide a constant tail current I_{ss}. This current will be switched by the logic function to one of the output branch, which will eventually reach voltage level ($V_{dd} - I_{ss}R_D$), which corresponds to logic '0' due to the entire current flowing through the load resistor. The other output will stay at logic '1'. The operation is elaborated in the next section. The power switch is used to cut the current to the transistors during *sleep* mode, which will force both the outputs to logic '1', since there will be no current in the output branch.

For a typical MCML circuit, the design parameters include the total power dissipation, circuit delay, voltage swing and voltage gain. These parameters can be controlled by the variables such as bias current, differential pull-down network transistor sizes, the current source transistor size and the current source bias voltage [4]. The simplest MCML gate is the buffer or inverter with just one differential pair as shown in Figure 2.

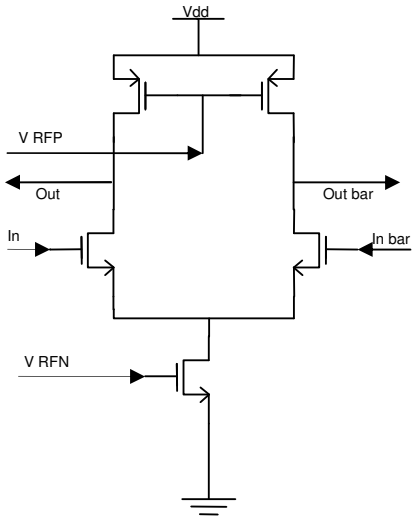

Figure 2. MCML Inverter/Buffer

3.2. Operation

This MCML logic works on *current steering* approach, where a constant bias current is routed to one of the branches depending upon the logic function being implemented[1][4]. The branch to which the current is steered results in a low output voltage and the branch to which the current is not steered results in a high output voltage. The MCML inverter shown in the Figure 2 uses 4 MOS transistors configured as two PMOS and two NMOS devices and an individual NMOS device acting as a current source. The circuit realizes current to voltage conversion. The PMOS device can operate in the triode region or as a resistor, when the inverter operates with $V_{SG} = V_{dd}$ and $V_{SD} < V_{SG}$. The current I_{ss} will be divided between the two NMOS transistors as i_{D1} and i_{D2}. From the circuit analysis, it can be found that the current i_D flowing through the transistor is given by the following equations:

$$i_D(v_i) = \begin{cases} 0 & \text{if } v_i < \sqrt{\dfrac{2I_{ss}}{\mu_n C_{ox}}} \\ \dfrac{I_{SS}}{2} + \dfrac{v_i}{2}\sqrt{\mu_n C_{ox}\dfrac{W_n}{L_n} I_{SS} - \left(\mu_n C_{ox}\dfrac{W_n}{L_n}\dfrac{v_i}{2}\right)^2} & \text{if } |v_i| < \sqrt{\dfrac{2I_{ss}}{\mu_n C_{ox}\dfrac{W_n}{L_n}}} \\ I_{ss} & \text{if } v_i > \sqrt{\dfrac{2I_{ss}}{\mu_n C_{ox}\dfrac{W_n}{L_n}}} \end{cases} \quad (1)$$

Here, v_i denotes the differential input voltage v_{i1} - v_{i2}, W_n and L_n are the effective NMOS transistor channel width and length respectively, C_{ox} is the oxide capacitance per area and μ_n denotes the NMOS carrier mobility. The output voltage transfer characteristics of this inverter can be calculated on identifying the equivalent resistance R_d of the PMOS. The differential voltage v_o of the structure is expressed as

$$v_o = v_{o1} - v_{o2} = -R_D(i_{D1} - i_{D2}) \quad (2)$$

On evaluation of the above equation and substituting the values of current in Equation 2, the voltage equations of MCML at different input conditions are given by

$$V_o(vi) = \begin{cases} R_D I_{ss} & if\ vi < \sqrt{\frac{2I_{ss}}{\mu_n C_{ox}\frac{W_n}{L_n}}} \\ -v_i R_D I_{ss}\sqrt{\mu_n C_{OX}\frac{W_n}{L_n}I_{ss} - \left(\mu_n C_{OX}\frac{W_n}{L_n}\frac{v_i}{2}\right)^2} & if\ |vi| \le \sqrt{\frac{2I_{ss}}{\mu_n C_{ox}\frac{W_n}{L_n}}} \\ -R_D I_{ss} & if\ vi > \sqrt{\frac{2I_{ss}}{\mu_n C_{ox}\frac{W_n}{L_n}}} \end{cases} \quad (3)$$

This transfer characteristic so obtained is pictured in Figure 3. As can be noted, the tail current of PMOS and NMOS transistors will identify the limits of the V_{SWING}. In order to keep the NMOS transistors out of the triode region, $R_D I_{SS}$ must be kept low enough. This is achieved when the gate-drain voltage V_{GD} is kept lower than the threshold $V_{T,n}$. This also imposes an upper bound on $R_D I_{SS}$. Hence, for the logic swing, the gate to drain voltage is given by

$$V_{GD} = V_{DD} - [V_{DD} - R_D I_{SS}] = R_D I_{SS} \le V_{T,n} \quad (4)$$

The load capacitance of the MCML gates is charged and discharged by the same amount of voltage swing. Hence, this makes it possible to operate at higher speeds due to faster charging and discharging processes. In CMOS logic, during the switching transition of any logic, the transistor switches between saturation and cutoff regions. However, note that due to the differential pair of transistors at the input, the transistors are never fully off in MCML. This inherently reduces the switching noise, since a constant amount of current is always drawn from the circuit irrespective of the input.

The propagation delay of the MCML gate is related to the voltage swing by the relation

$$\tau = C\Delta V/I$$

where C is the load capacitance of the gate
ΔV is the output swing of the logic gate.
I is the tail current

The above equation indicates that with increase in voltage swing, the propagation delay also increases and the circuit tends to operate at a slower speed. Hence, in order to operate at higher speeds, the voltage swing is either reduced or the tail current is increased. In the proposed design, the voltage swing is limited at 220 mV.

3.3. Power Gating

Despite all the advantages of MCML gates, the primary impediment in their use is the static power dissipation. Due to the current source, there remains always a leakage power, even when no inputs are applied. This causes an unwanted increase in the power utilization which is not detrimental to the efficiency of circuit. This static power dissipation thus poses a serious issue to the designers, especially for low power devices, where the power dissipation remains the main concern. The possible answer to this problem is the *power gating*. It can be the most effective method of reducing the stand-by leakage power [2]. In the power gating technique, special type of transistors called as *sleep* transistors, designed with high threshold voltage value are deployed in the design. They tend to cut-off the power supplies to certain parts, where the circuit is not in

operation. The sleep transistors are placed in series with the circuit. A sleep transistor can be either a PMOS or an NMOS transistor. The PMOS sleep transistor is called the *header switch* and it controls the V_{DD} supply to certain parts of the circuit. On the other hand, the NMOS sleep transistor is called the *footer switch* and it controls the V_{SS} node connectivity.

In this design of the MCML gates, the implementation of the sleep transistors as footers using NMOS is shown in the Figure 2. However, introducing a sleep transistor in each and every cell will increase the area of the design and the sensitivity to PVT variation will increase. Hence, for a larger design, it is proposed to implement the distributed sleep transistor approach. The sleep transistor is connected between the permanent power supply and the virtual supply network [7]. The main advantage of the distributed implementation is that the area overhead becomes significantly smaller, the circuit becomes less sensitive to the PVT variation, and furthermore, less IR drop results, as compared to the cell based implementation.

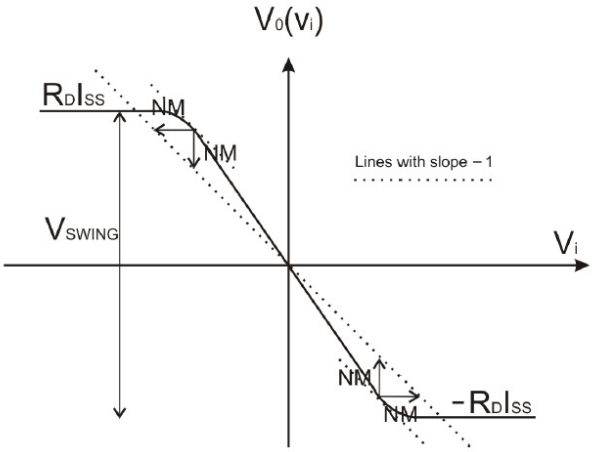

Figure 3. Transfer Characteristics of MCML inverter

4. IMPLEMENTATION & RESULTS

All the basic MCML gates such as AND, NAND, Inverter, Buffer, XOR, XNOR, OR, NOR and D-flip flop were designed and optimized to achieve lower voltage swing. Cadence® EDA tool has been employed for simulation and synthesis for all the architectures using 180nm industry standard technology libraries. Figures 4 and 5 depict the MCML XOR gate, which is widely used in encryption algorithms of cryptography. Figure 4 shows a 2 input XOR gate which uses 4 differential NMOS transistors used as inputs, and a separate NMOS which is connected to the supply for balancing the current network. The current is steered to produce the XOR logic function, when the corresponding inputs are applied. Figure 5 shows a 3-input XOR gate based on the same architecture. In Figure 6, NAND gate is typically implemented in MCML. Figure 7 shows the sleep transistors biased by a pair of pass transistor logic structure, in which the gate voltage is fed by a pair of differential inputs. The pass transistors operate when any one of the input is *high*, and will connect V_{DD} to the sleep transistor, which will in turn set the path for the current source to operate. Hence, the circuit will operate only when the inputs are applied. When an input is not applied, the pass transistors will not conduct, the output will be in high impedance state, and it will not drive the sleep transistors any further. Thus, the circuit will remain *cutoff* without any leakage power dissipation. This reduces the effort of making a multi-threshold transistor, or any other power gating technique for that matter, which will necessitate an additional power supply. In these circuits, the width of the NMOS differential transistors is kept

at 2.2um and the current source NMOS is fixed at a width of 3.2 um for allowing large current to flow through the branch. The sizing of the transistors has been done focusing on maintaining a gain of value more than *2*. The *gain* parameter directly depends on the width of the transistor. Hence, increasing the width will increase the gain, albeit at the cost of increased delay[9]. Hence, an optimum value of the *aspect ratio* is identified to provide the maximum gain and a minimum delay. In the proposed design, the gain was kept at an optimal value of 2.2.

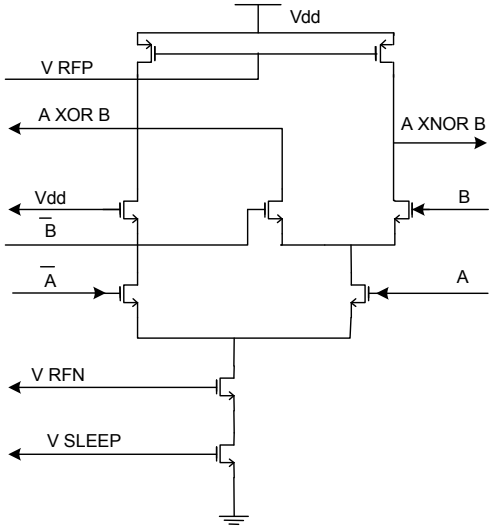

Figure 4. A MCML 2 input XOR/XNOR gate

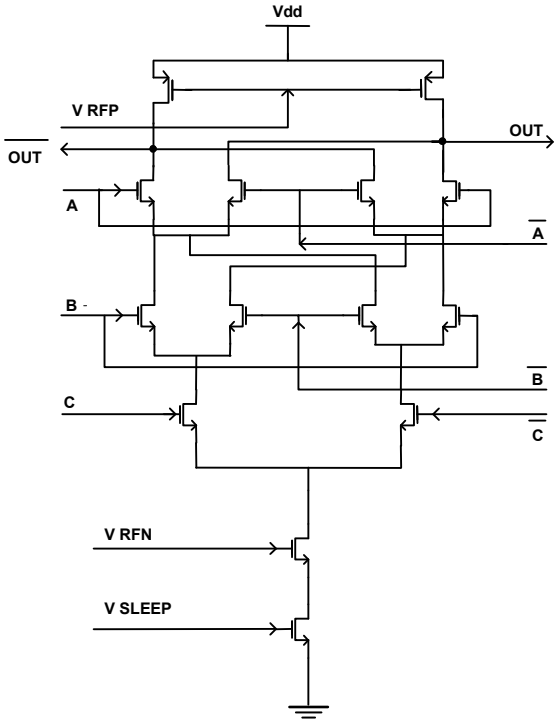

Figure 5. A MCML 3 input XOR/XNOR gate

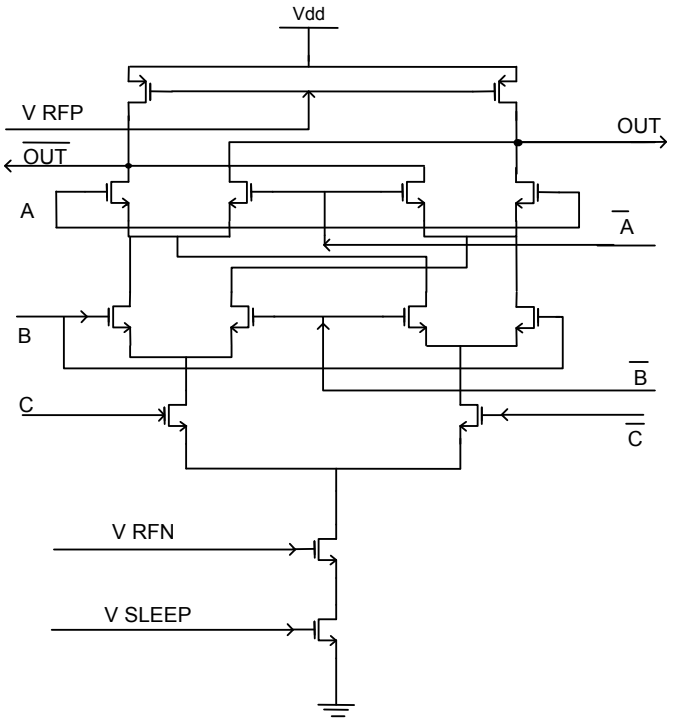

Figure 6. MCML 3 input AND/NAND gate

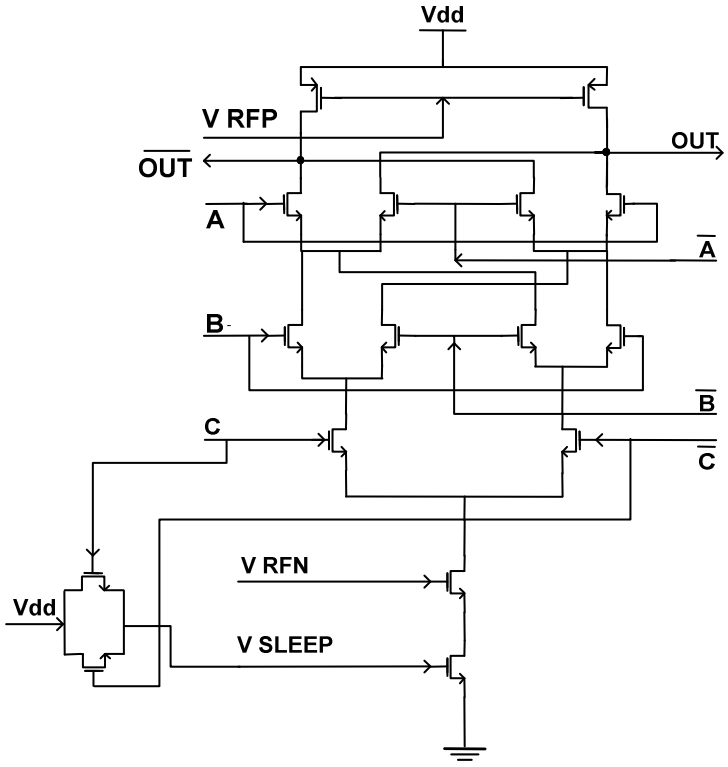

Figure 7. Biasing the sleep transistor with pass gate logic

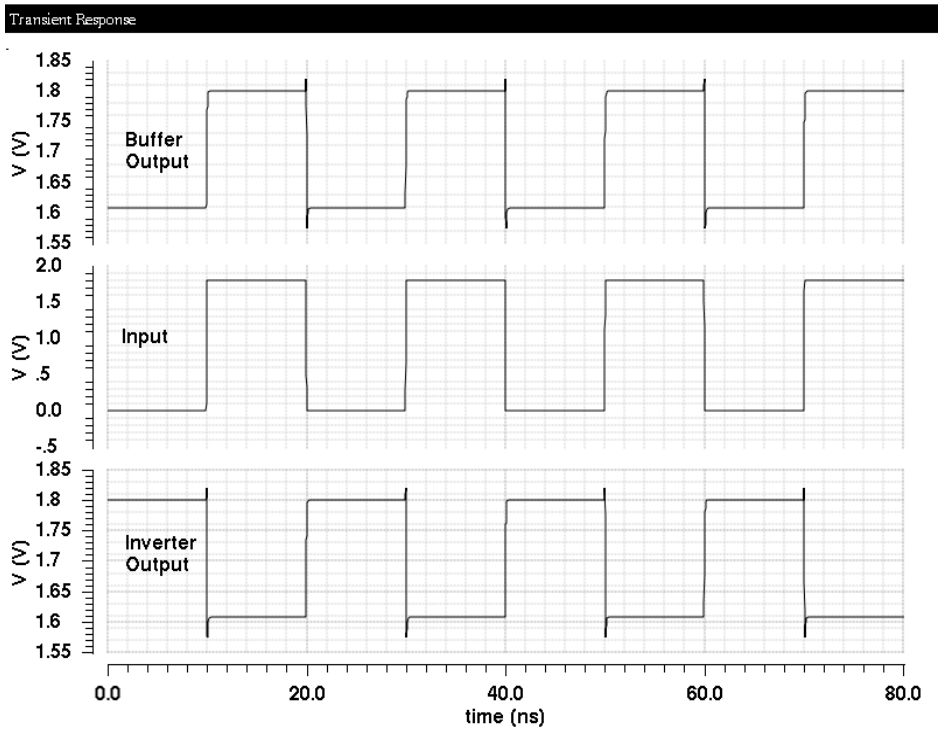

Figure 8. Transient response of MCML Inverter/Buffer

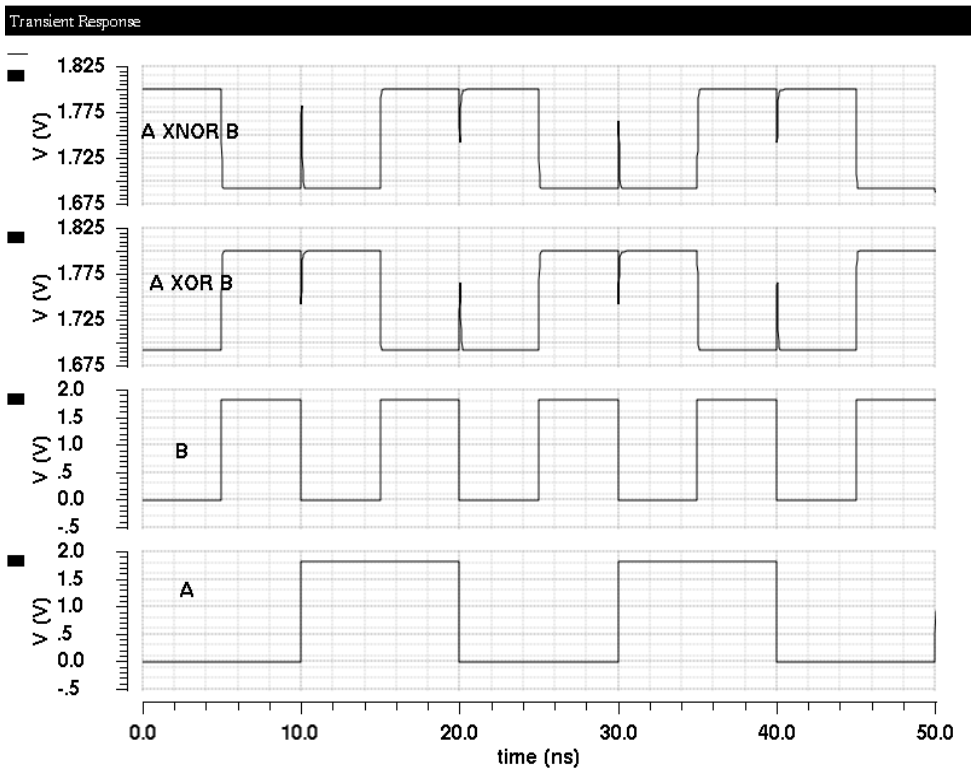

Figure 9. Transient response of MCML XOR/XNOR gate

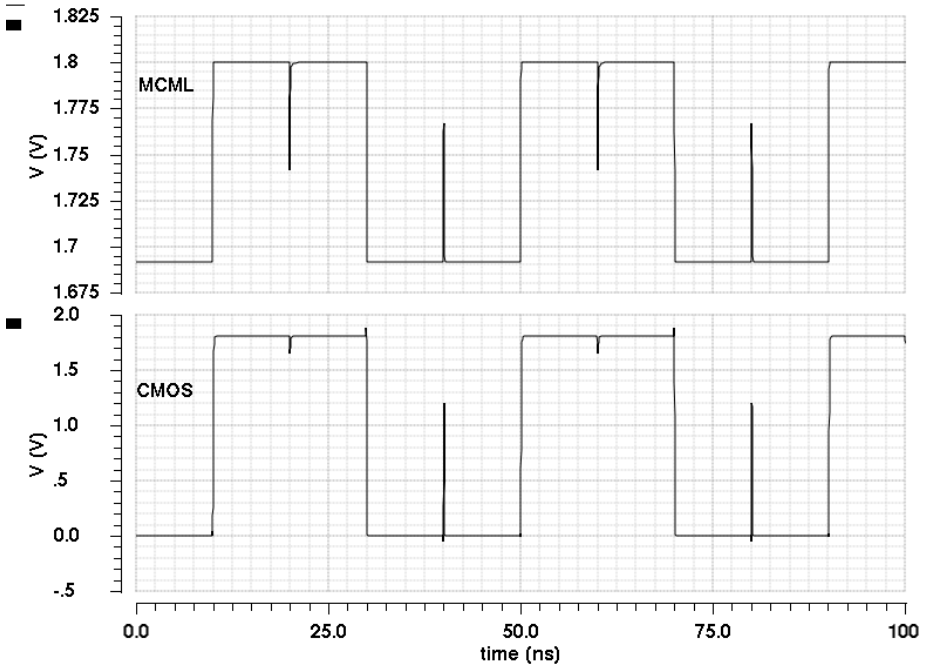

Figure 10. Voltage swing of CMOS and MCML XOR gate.

Figure 8 produces the transient response of the inverter shown in Figure 2. The graph confirms the voltage swing of the gates to be *220mV*. Figure 9 depicts the response excitation of the two input MCML XOR gate. Figure 10 shows the comparison between the voltage swing of the XOR gate designed with CMOS and MCML logic. The swing of the CMOS gate is V_{dd} , where as the swing of the MCML gate is given by $I_{DD}R_s$. In this design, the swing voltage was set to 220 mV. This swing can further be reduced by decreasing the aspect ratio of the pull down differential transistors. Simulation of MCML and CMOS XOR counterparts were performed for justifiable comparison based on the parameters, namely, current, voltage and power fluctuation. The current of MCML gate was traced to be constant, totally independent of the input variations. Furthermore, the voltage swing was observed to be very negligible in MCML gate. Figure 11 shows the comparison of power dissipation of a CMOS XOR gate as well as a MCML XOR gate, for all input transitions. As can be observed from the transients, the power of the CMOS gate shows significant changes, whenever the input changes. However, the variation in MCML gates is negligibly small. This characteristic features of the two types of gates can be represented by the equations given below, which depict the power variations of MCML and CMOS counterparts.

$$P_{CMOS} = CV_{dd}{}^2 f \tag{5}$$

$$P_{MCML} = V_{dd} I \tag{6}$$

The NMOS current source was designed to provide a constant current supply for all possible input combinations. The resistance offered by the current source is given by

$$R_{st} = \frac{L_{st}}{W_{st}} \times \frac{1}{\mu_n C_{ox}(V_{dd} - V_{T,n})} \tag{7}$$

Hence, in order to maximize the resistance R_{st}, the width W_{st} of the device was reduced to 1.2um, while the length L_{st} was fixed at 0.18um. The voltage swing V_{dd} depends on I_{ss}. Hence, to limit the voltage swing to 800mV, the I_{ss} was set to *1.2mA*.The voltage swing of all the basic gates were

calculated and the values are shown in Table I for comparison. The voltage swing of CMOS gates is seen to be constant at *1.8V,* while that of the MCML gates is very less. It can further be reduced by changing the gate to source voltage of the resistive PMOS. A similar comparison was made for a 2-input XOR gate for all the possible input combinations using a bit sequence. The values of power dissipation were recorded and were compared with that of the CMOS as shown in Table II. The power consumption was measured, *before* and *after* connecting the sleep transistor. For an MCML XOR gate, the power dissipation without introducing the sleep transistor was found to be *39.8mW*. With the NMOS sleep transistor connected as the power gating footer, the power dissipation was found less, to a value as low as *11.86nW*.

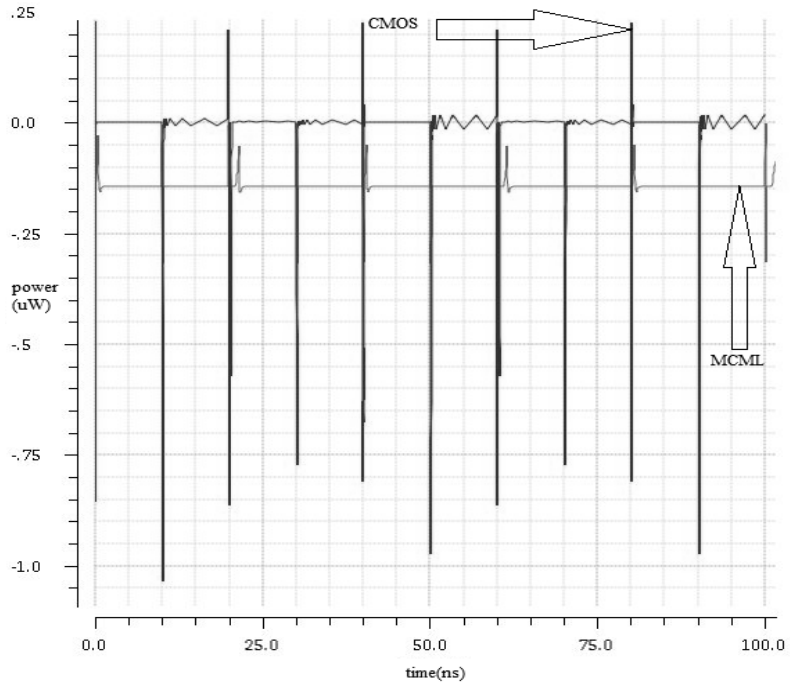

Figure 11. Power comparison of CMOS & MCML XOR gate

The MCML logic can be useful for implementing the cryptographic primitive operations, such as XOR, since it has DPA resistance which is the absolute necessity in cryptographic hardwares.

Table 1. Voltage swing for various gates using MCML and CMOS families

Logic Gates	**Inverter**	**NAND**	**XOR**	**OR**
CMOS	1.8V	1.8V	1.8V	1.8V
MCML	280mV	230mV	220mV	240mV

Table 2 Power dissipation Of MCML and CMOS XOR gate for various input transitions.

Logic transitions	CMOS (uW)	MCML (uW)
00-01	1.29	0.12
00-10	1.43	0.13
00-11	1.78	0.12
01-10	1.45	0.17
01-00	0.78	0.14
01-11	1.62	0.12
10-00	1.65	0.12
10-01	0.96	0.13
10-11	1.42	0.13
11-00	0.98	0.12
11-01	0.87	0.12
11-10	1.3	0.14

5. CONCLUSIONS

In this paper, various functional traits of current mode logic that makes them suitable for DPA resistant circuits are explored. A new methodology has been proposed for biasing the sleep transistors using pass gate transistors. Extensive simulations are carried out to validate and prove the efficacy of MCML over CMOS counterparts. The benefits of this MCML logic is the flexibility in fixing a low voltage swing, minimum delay and higher gain by proper sizing of the transistors, which is more cumbersome in CMOS logic gates counterparts. The constant current and negligible power variations for different input transitions, make it useful in the design of cryptography related circuits and systems. As the technology gets scaled down, the MCML can prove to be a better choice for DPA resistant circuits. The circuit structure also realizes negligible leakage power. Hence, the MCML logic will prove to be the best choice in designing DPA circuits in future.

REFERENCES

[1] Hassan, Mohab Anis, Mohamed Elmasry, “MOS Current Mode Circuits Analysis & Design”, *IEEE transactions on Very Large Scale Integration (VLSI) Systems*, Vol. 13, No. 8, August 2005, Pp. 885-98.

[2] Cevrero. A. et. al., “Power-Gated MOS Current Mode Logic (PG-MCML): a Power Aware DPA-Resistant Standard Cell Library”, *Design Automation Conference (DAC), 48th ACM/EDAC/IEEE 2011*, Pp. 1014-19.

[3] Minoru Saeki et. al., "A Design Methodology for a DPA-Resistant cryptographic LSI with RSL Techniques", Cryptographic Hardware and Embedded Systems - CHES 2009, Lecture Notes in Computer Science Volume 5747, 2009, Pp. 189-204.

[4] M. Sumathi, Kartheek, “Performance and analysis of CML logic gates and latches”, IEEE *International Symposium on Microwave, Antenna, Propagation and EMC Technology for wireless communication, 2007*, Pp.1428-32.

[5] F. Regazzoni. et. al., “A simulation-Based methodology for evaluating the DPA-Resistance of cryptographic functional units with application to CMOS and MCML technologies”, *International Conference IC-SAMOS*, 2007, Pp. 209–214.

[6] Jun Wu. et. al., "Measurement and Evaluation of Power Analysis Attacks on Asynchronous S-Box", *IEEE Transactions on Instrumentation and Measurement*, Vol. 61, 2012, Pp. 2765–75.

[7] Changbo Long and Lei He, "Distributed sleep transistor network for power reduction", *Proceedings of IEEE/ACM Design Automation Conference*, 2003, Pp. 181–86.

[8] M. W. Allam and M.I. Elmasry, "Dynamic current mode logic (DyCML): A new low-power high-performance logic style" *IEEE Journal of Solid-State Circuits*, 2001, Pp. 550–58.

[9] M. Yamashina and H. Yamada, (1992) "An MOS current mode logic (MCML) circuit for low-power sub-GHz processors", *IEICE Transactions on Electronics*, Vol. 75, No. 10, Pp. 1181–1187.

[10] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis", Wiener, M.J. (ed.) CRYPTO LNCS, Vol. 1666, Pp. 388-397, 1999, Springer.

[11] K. Tiri and I. Verbauwhede (2004), "A Logic Level Design Methodology for a Secure DPA resistant ASIC or FPGA Implementation", *Proceedings of the conference on Design, automation and test in Europe* – Vol. 1, DATE-04, Pp. 246-51.