ISSN No:-2456-2165

A Fault Analysis Perspective of Logic Encryption in Memristor Based Combinational Circuits Using Key Gates

Dr.K.Paramasivam
Professor, Department of EEE
Kumaraguru College of Technology
Coimbatore,India

N.Nithya
Full Time Research scholar, Department of EEE
Kumaraguru College of Technology
Coimbatore,India

Abstract:- In this paper, a logic locking technique for memristor based combinational circuits using key gates is proposed. The key gates are XOR/XNOR gates with additional inputs referred as keys, which ensures the circuit to provide correct output only for specific input key. The logic encryption with key gates prevents IC's from camouflaging and overproduction outside foundries. The conventional theories of hardware security, were not concerned about area on chip. In our proposed logic, memristors with very few transistors are used for combinational logic design instead of completely relying on transistor only implementations. The Memristor Ratioed Logic (MRL) is used for designing combinational logic circuits. The SPICE simulations are done using 180um technology with LTSPICE tool and the results shows the total delay of 0.21ns with average power consumption of 647.83µW.

Keywords:- *Memristor, Linear Ion Drift model, Logic encryption, Key-gates, MRL.*

I. INTRODUCTION

The increase in the on-demand of low power, low area on chip and faster electronic circuits becomes the motivating force for the semiconductor industry to design and develop smaller IC's with complex functionalities. The fabrication of IC's with complex functionalities requires advanced and mixed fabrication facility. The globalization of IC industry facilitates the designers to outsource the designs which leads to the vulnerability in hardware security like reverse engineering, IP Piracy, counterfeiting and hardware trojans. Logic encryption or logic locking [1] is a popular technique for preventing IP piracy and illegal overproduction outside the foundry. The major goal of logic encryption is as follows:

- Locking - is defined as a logical request to ensure correct operation of the circuit following only the application of specific keys.
- Obfuscation – is defined as a request in terms of structure to ensure that correct circuit can't be decrypted by the analysis of overall structure (reverse engineering).

In this paper, memristor, a nanodevice is used for the implementation of adder circuits which results in the reduction of chip area, low power consumption and less delay. Memristor Ratioed Logic [2] style is used for the implementation of AND/OR gates and the remaining logic gates are designed with the combination of transistor and memristor. The full adder is encrypted using XOR key gates with two keys.

II. LITERATURE SURVEY

Memristor, a nanodevice, abbreviated as memory resistor, was first postulated by Prof.L. Chua in 1971. It establishes the relation between charge and flux, in which the logic value is stored in the form of resistance. A physical device using titanium di oxide was invented by a team of experts in HP Laboratories in 2008. The practical memristor of size 3nm X 3nm with operating frequency was invented in the year 2010. The design of memristor based digital IC's results in the miniaturization of chip area. Memristor finds applications in neuromorphic computing, digital IC design, image processing and pattern recognition.

Section 3 introduces the linear ion drift model used for modeling the memristor. Section 4 highlights the advantages of using Memristor Ratioed Logic. Section 5 demonstrates the logic encryption in memristor based adders and section 6 and 7 portrays the results, discussions and conclusions.

III. MEMRISTOR MODEL

In this paper, the linear ion drift model [3] is proposed for the design of memristor based combinational circuits. This model is depicted with two resistors connected in series. One resistor indicates dopants in high concentration region which results in high conductance and the other resistor indicates dopants in low concentration region resulting in low conductance. This model assumes to have uniform field and all the ions with equal average ion mobility.

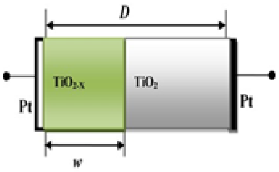

Fig 1a:- Structure of memristor

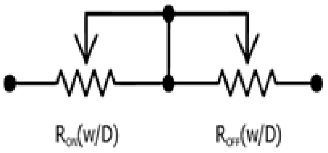

Fig 1b:- Equivalent model of linear ion drift model memristor

The proposed model is an ideal model which exhibits a linear relationship between state derivative and stimuli. It is based on the assumption that vacancies have the freedom to move through the total length of the device and it is suitable for low power applications.

$$\boldsymbol{V(t) = R(t).i(t)} \quad \textbf{(1)}$$

$$\boldsymbol{R(t) = \frac{RonW(t)}{D} + Roff\left(1 - \frac{W(t)}{D}\right)} \quad \textbf{(2)}$$

Ron indicates the resistance when x(t) → D
Roff indicates the resistance when x(t) → 0

This model exhibits the dynamic movement of state variable x(t) within the limits 0≤ w≤ D.

$$\boldsymbol{\frac{dW(t)}{dt} = \frac{\mu vRon}{D}\, i(t)} \quad \textbf{(3)}$$

It predicts inverse relationship between switching time T0 and applied voltage V0.

$$\boldsymbol{V0 = \frac{1}{T0}} \quad \textbf{(4)}$$

IV. MEMRISTOR RATIOED LOGIC

MRL logic style uses two memristors for designing AND/OR gates. The complementary logic gates and special gates are designed with the association of CMOS inverter. The CMOS inverter provides compatibility and restoration of signal level. The AND and OR gates are implemented with two memristors connected serially with common output node.

when current flows in one of the terminals of AND gate, the resistance increases resulting an output of logic 0 for all the three input combinations (00,01,10) except for input combination 11.Similarly, when current flows in one of the terminals of OR gate, the resistance decreases resulting an output of logic 1 for all the three input combinations (01,10,11) except for input combination 00. The expressions of the output voltages of OR and AND gates are as follows:

$$\boldsymbol{V_{out,or} = \frac{R_{off}}{R_{off}+R_{on}} V_{high} \approx V_{high}} \quad \textbf{(5)}$$

$$\boldsymbol{V_{out,and} = \frac{R_{on}}{R_{off}+R_{on}} V_{high} \approx 0} \quad \textbf{(6)}$$

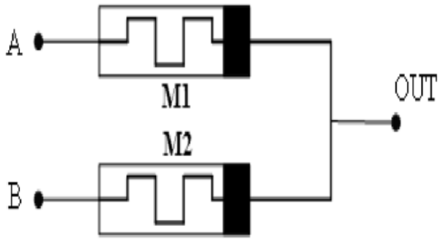

Fig 2a:- MRL based AND gate

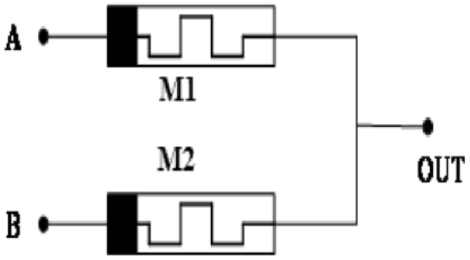

Fig 2b:- MRL based OR gate

Special gates like XOR and XNOR are designed using both CMOS inverters and memristors. The proposed XOR [4] gate is designed using 6 Memristors and 1 CMOS inverters with two transistors. The logic equation for XOR gate is OUT= (A+B).(A.B)'

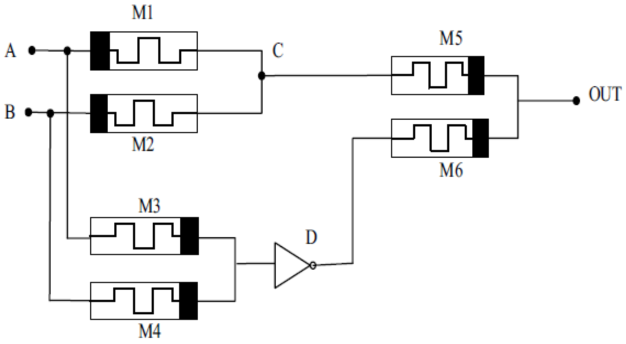

Fig 3:- MRL based XOR gate

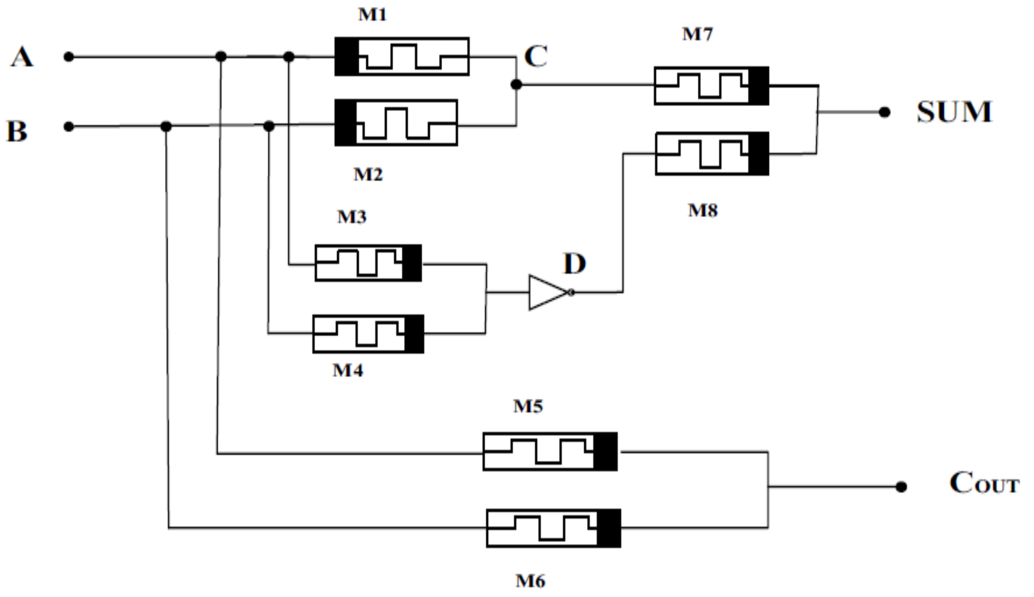

Fig 4:- MRL based half adder

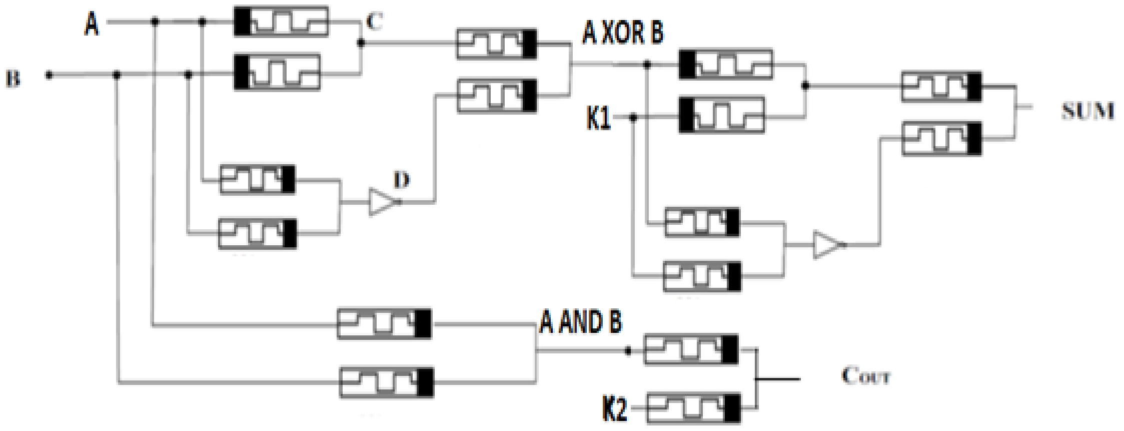

Fig 5:- Logically encrypted half adder

V. PROPOSED LOGIC OF ENCRYPTED ADDER CIRCUITS

This paper presents logically encrypted half adder and full adder circuits with set of input keys K* = {K1, K2} without change in their functionality. The XOR gate is used as key gate [5] . Memristor based AND and OR gates are used for the detection of dominant faults, stuck at '0' and stuck at '1' faults. The exact output is obtained only if the key values given are correct.

In half adder circuit, the sum output is encrypted using XOR gate with key input K1 = 0. The carry output is encrypted using AND gate with key input K2=1 for detection of faults. For an AND gate, if one of the inputs is 1, the value of other input variable is propagated as output. For an XOR gate, if key K1=0, the original value of the second input is propagated whereas if key K1=1, the complemented value is propagated as the output. The truth table of various set of key values and its outputs are shown below:

K1	K2	A	B	SUM	COUT
0	0	0	0	0	0
0	0	0	1	1	0
0	0	1	0	1	0
0	0	1	1	0	0
0	1	0	0	0	0
0	1	0	1	1	0
0	1	1	0	1	0
0	1	1	1	0	1
1	0	0	0	1	0
1	0	0	1	0	0
1	0	1	0	0	0
1	0	1	1	1	0
1	1	0	0	1	0
1	1	0	1	0	0
1	1	1	0	0	0
1	1	1	1	1	1

Table 1:- Truth Table of Logically Encrypted Half Adder

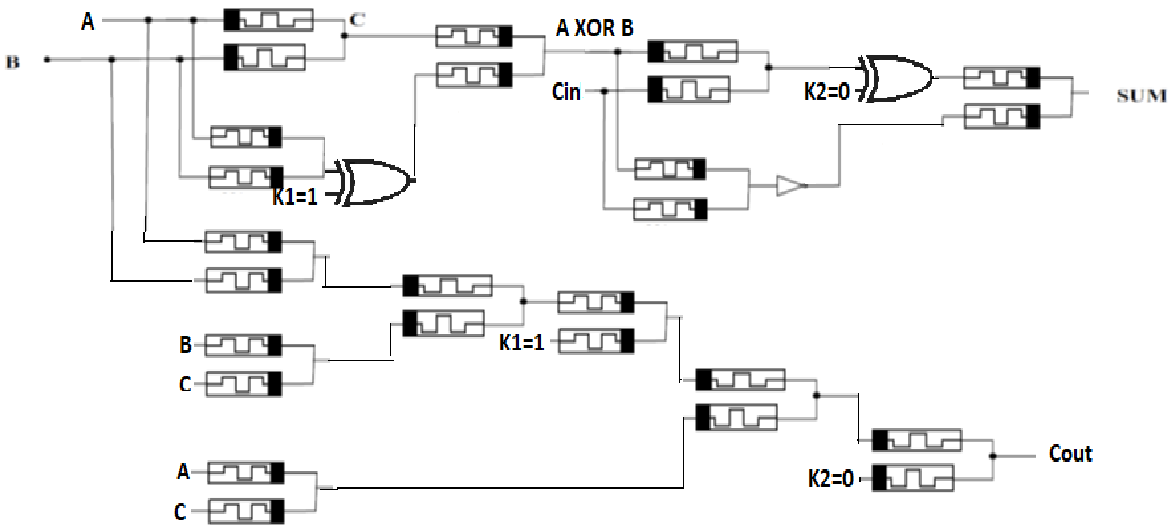

Fig 6:- Logically encrypted Full adder

K1	K2	A	B	Cin	Sum	Cout
0	1	0	0	0	1	1
0	1	0	0	1	0	1
0	1	0	1	0	1	1
0	1	0	1	1	0	1
0	1	1	0	0	1	1
0	1	1	0	1	0	1
0	1	1	1	0	0	1
0	1	1	1	1	0	1
1	0	0	0	0	0	0
1	0	0	0	1	1	0
1	0	0	1	0	1	0
1	0	0	1	1	0	1
1	0	1	0	0	1	0
1	0	1	0	1	0	1
1	0	1	1	0	0	1
1	0	1	1	1	1	1

Table 2:- Truth Table of Logically Encrypted Full Adder

In full adder sum circuit, the XOR gate is inserted instead of inverter with key K1=1 to ensure the propagation of correct ouput for the equation (A.B)’. Another XOR gate is inserted with key K2=0, for encrypting maximum output values except for B=Cin=1. In carry circuit, an AND gate with key input K1 = 1 and an OR gate with key K2 = 0 is implemented for the encryption of all the input sets except B= Cin= 1. This problem can be overcomed by the inclusion of XOR gate with K1=1 at the output of product of B and C. The reason behind this problem of not encrypting this two input sets is reduction in area and prevention of reverse engineering. The schematic diagram and truth table for logically encrypted full adder is as follows:

VI. RESULTS AND DISCUSSION

The SPICE simulations of the proposed circuit are done using LTSPICE tool. The linear ion drift model is designed with the parameters Ron = 1 kΩ, Roff = 100 kΩ. The maximum value of Ron/Roff ratio results in the proper switching of logic states. The voltages are Vt = 2 V and Vdd = 1.8 V. The results are tabulated as follows:

Parameters	**CMOS full adder**	**Memristor based full adder**	**Logically encrypted memristor based full adder**
Total Number of transistors required	34	24 Memristors and 4 transistors	40 memristors 6 transistors
Rise time delay	98.6ps	76.8ps	0.12ns
Fall time delay	63.2ps	54.2ps	89.4ps
Total delay	161.8ps	131ps	0.21ns
Power Consumption	142.6uW	73.61uW	647.83uW

Table 3:- Performance Comparison of Different Logic Full Adders

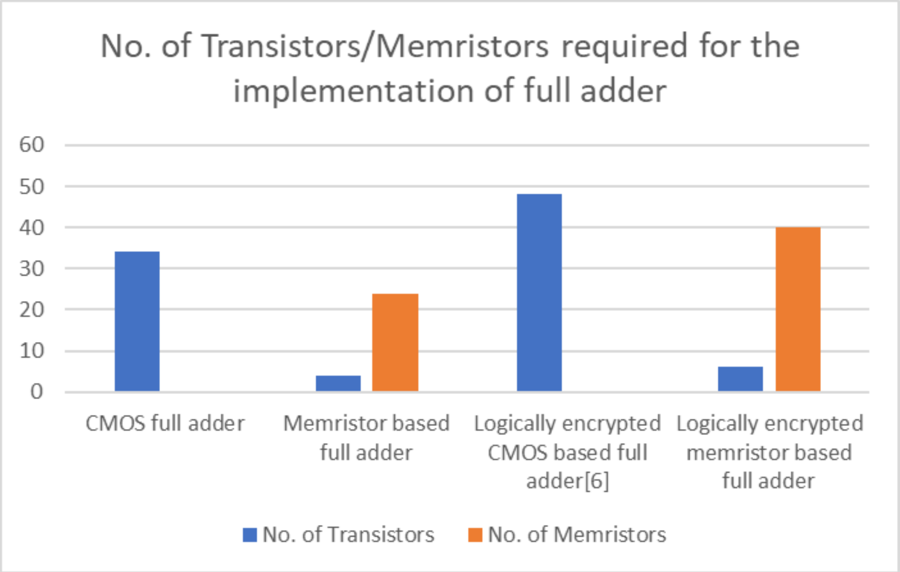

Fig 7:- Comparison of the required number of transistors for various logic full adders

VII. CONCLUSION

This paper highlights the application of memristor in hardware security with reduced chip area and power consumption. Even though, linear ion model is closely related to the definition of memristor, it has bottleneck in terms of accuracy in par with physical memristive devices. This can be overcome by the application of suitable windows [7]. The logically encrypted combinational circuits shown in this paper are designed for fault coverage with total delay of 0.21ns and average power consumption of 647.83µW which is less when compared to the CMOS based logically encrypted adder which is in several milliwatts. Reverse engineering problem is avoided as the output is not completely encrypted.

REFERENCES

[1]. J. Zhang, ―A practical logic obfuscation technique for hardware security, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 3, pp. 1193–1197, 2016.

[2]. S. Kvatinsky, N. Wald, G. Satat, A. Kolodny, U. C. Weiser, and E. G. Friedman, "MRL -Memristor Ratioed Logic," Int. Work. Cell. Nanoscale Networks their Appl., no. August, 2012.

[3]. D.B. Strukov, G.S. Snider, D.R. Stewart, R.S. Williams, "The missing memristor found". Nature 453(7191), 80–83 (2008).

[4]. Muhammad Khalid,Sana Mukhtar,MohammadJawaid, Siddiqu Sumair. Faisal Ahmed, "Memristor Based Full Adder Circuit for Better Performance", Transactions on Electrical and Electronic Materials ,2019.

[5]. Vijaypal Singh Rathor, Bharat Garg, and G K Sharma " A Novel Low Complexity Logic Encryption Technique for Design-for-Trust", in IEEE Transactions on emerging topics in Computing,2018.

[6]. K. Juretus and I. Savidis, "Reducing logic encryption overhead through gate level key insertion", in IEEE International Symposium on Circuits and Systems (ISCAS), Pp 1714-1717, 2016.

[7]. N.Nithya and K.Paramasivam, "A Comprehensive Study on the Characteristics, Complex Materials and Applications of Memristor", Complex Materials and Applications of Memristor",IEEE conference ICACCS, Mar.2020.