Secure CMOS Logic Through Logic Encryption

Aalolika Roy Chowdhury
Department of EEE
Ahsanullah University of Science and Technology
Dhaka,Bangladesh

Tonima Rani Ghosh
Department of EEE
Ahsanullah University of science and Technology)
Dhaka,Bangladesh

Raihan Ahmed
Department of EEE
Ahsanullah University of Science and Technology
Dhaka,Bangladesh

Md. Idrak Efaz
Department of EEE
Ahsanullah University of Science and Technology
Dhaka,Bangladesh

Sumaia Akter Ritu
Department of EEE
Ahsanullah University of Science and Technology
Dhaka,Bangladesh

Designed and laid out

***Abstract*—In the present world, the semiconductor industry is growing rapidly where hardware security is the primary concern to prevent piracy. Many fabless companies send their ICs to the foundries that have advanced fabrication capabilities. But there comes a risk of IP piracy, reverse engineering, overproduction and malicious tampering of IC for Trojan insertion as the IC design flow is known to the attackers. An efficient method to protect hardware is logic encryption where the original functionality is accessible by the authorized persons only. In our proposed circuits, a novel transistor-level method logic encryption for CMOS gates is ensured along with power, cost, performance, and reliability optimizations. We designed secure OR, AND, NOR, NAND, XOR and XNOR circuits where the correct output depends on the logic level of key. Faulty outputs will be provided by the encrypted circuits during the application of an incorrect key pattern.**

I. Background

When the chips enter in the supply chain of IC, they can be attacked by the hackers through reverse engineering to access the design or specific secrets from a design. Annually 4 billion dollars is lost in the semiconductor industry due to these problems. So, the IP vendors have to face difficulties to save the intellectual properties from piracy, overproduction and reverse engineering. Many logic encryption techniques have been applied by the researchers to protect hardware from piracy but those methods increase some circuit parameters like area, power, delay, and energy. In our circuits, these disadvantages were eliminated. Area, power, delay, and energy are reduced by an average of 42.94%, 37.37%, 26.79%, and 50.96% respectively in the proposed encrypted key gates. Moreover, other logic encryption methods have a constant output like as logic high (1) or logic low (0) whereas our proposed gates don't provide any continuous or constant output which helps to prevent piracy. Without the correct key, the attacker will not be able to access the circuit netlist by reverse engineering because a Trojan will not be inserted into the netlist's internal node.

II. Design Representation

A. Secure OR Gate

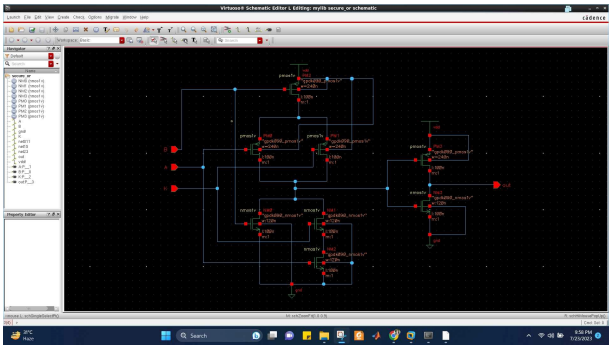

Fig. 1. Schematic of Secure OR Gate

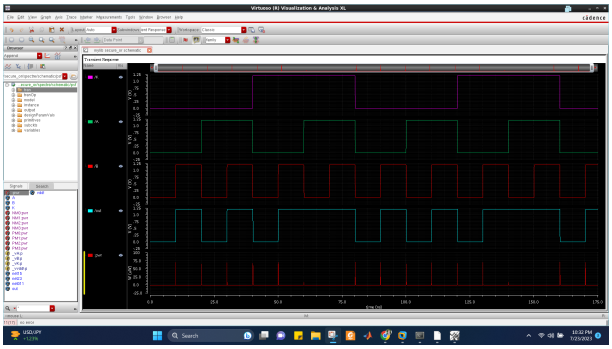

Fig. 2. Waveform of Secure OR Gate

K	A	B	OR
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Fig. 3. Secure OR Gate Truth Table

From the schematic diagram of OR gate, we get the output function to be, OR = AK + B When the logic level of K is 1, we get the output as OR = A + B, which is the expected output of OR gate. Whereas, if K = 0, the output will not provide the expected values of OR gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of OR gate will not be found.

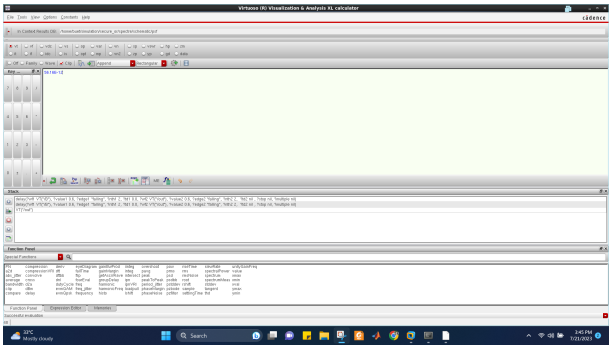

Fig. 4. Secure OR gate Propagation Delay

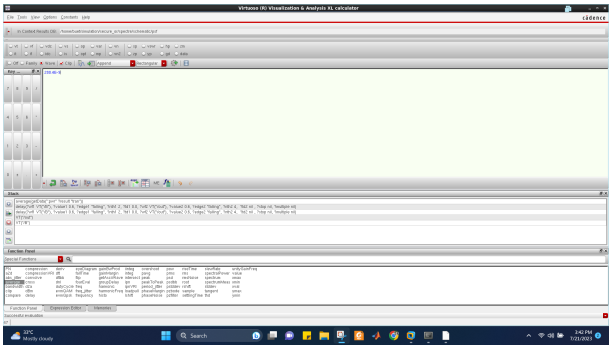

Fig. 5. Secure OR gate Average Power

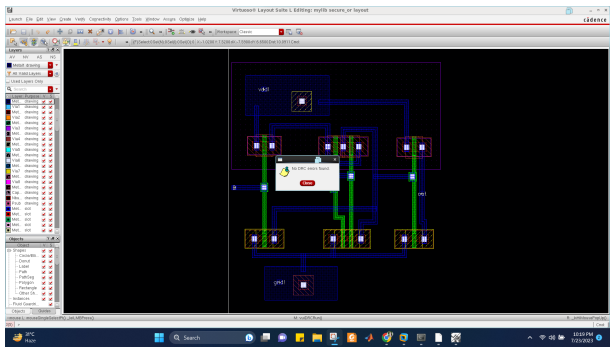

Fig. 6. Secure OR Layout DRC

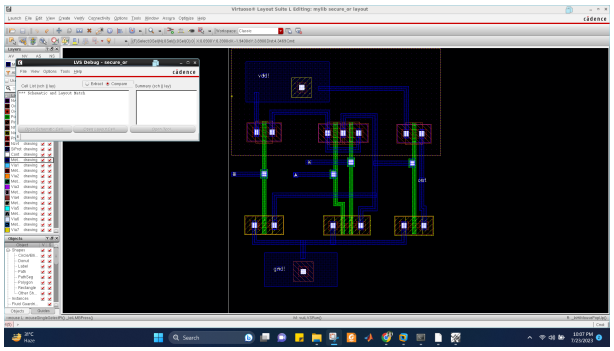

Fig. 7. Secure OR Layout LVS

B. Secure AND Gate

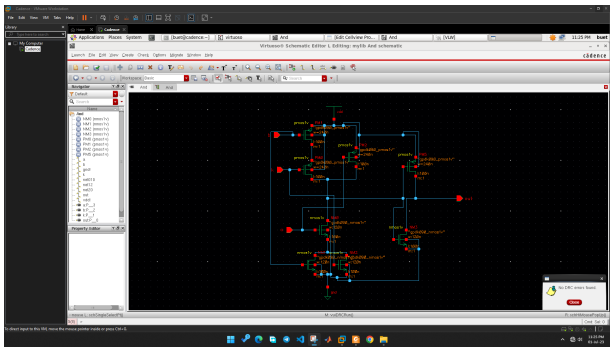

Fig. 8. Schematic of Secure AND Gate

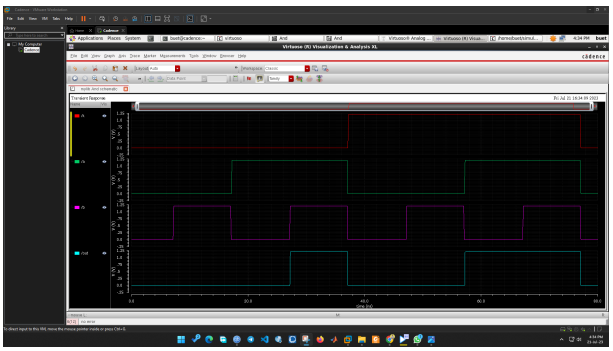

Fig. 9. Waveform of Secure AND Gate

K	A	B	AND
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

Fig. 10. Secure AND Gate Truth Table

Here, from the schematic diagram of AND gate, we get the output function to be, AND = A(B+K). When the logic level of K is 0, we get the output as AND = A.B , which is the expected output of AND gate. Whereas, if K = 1, the output will not provide the expected values of AND gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of AND gate will not be found.

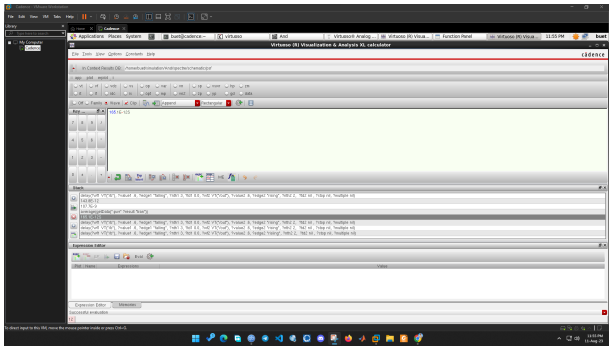

Fig. 11. Secure AND gate Propagation Delay

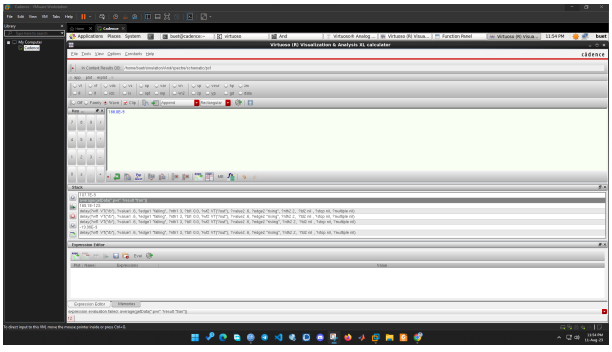

Fig. 12. Secure AND gate Average Power

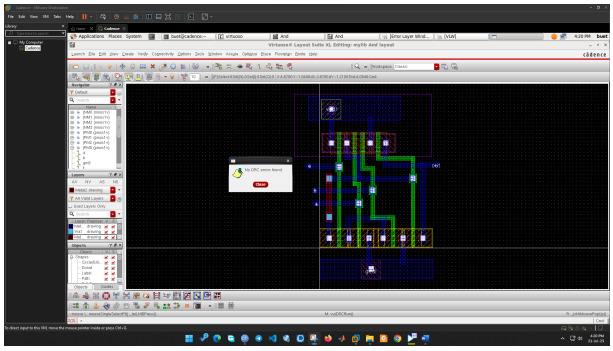

Fig. 13. Secure AND Layout DRC

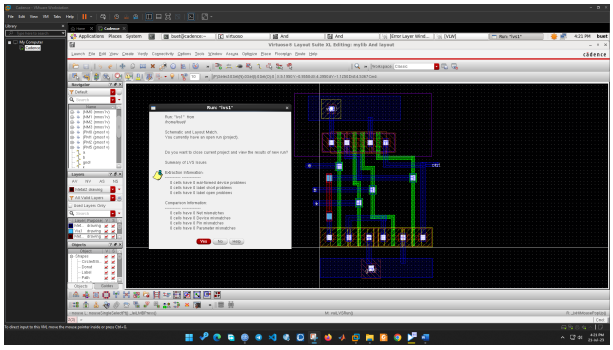

Fig. 14. Secure AND Layout LVS

C. Secure NOR Gate

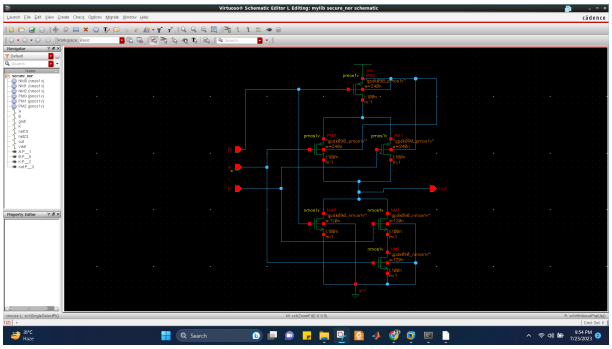

Fig. 15. Schamatic of Secure NOR Gate

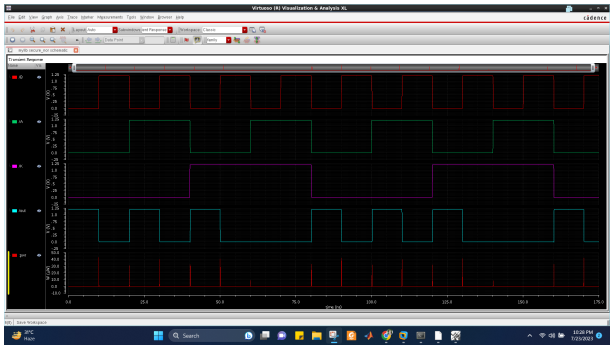

Fig. 16. Waveform of Secure NOR Gate

K	A	B	NOR
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	0

Fig. 17. Secure NOR Gate Truth Table

From the schematic diagram of NOR gate, we get the output function to be, NOR=(AK+B)' When the logic level of K is 1, we get the output as NOR gate, which is the expected output of NOR gate. Whereas, if K = 0, the output will not provide the expected values of NOR gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of NOR gate will not be found.

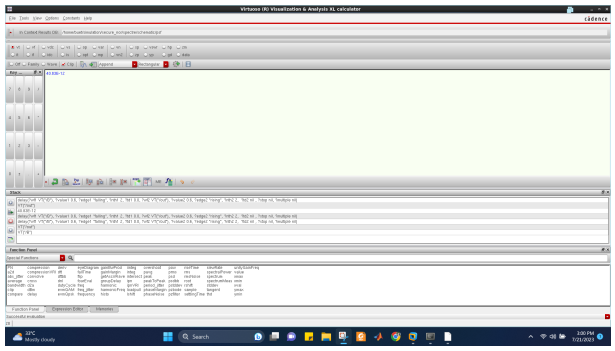

Fig. 18. Secure NOR gate Propagation Delay

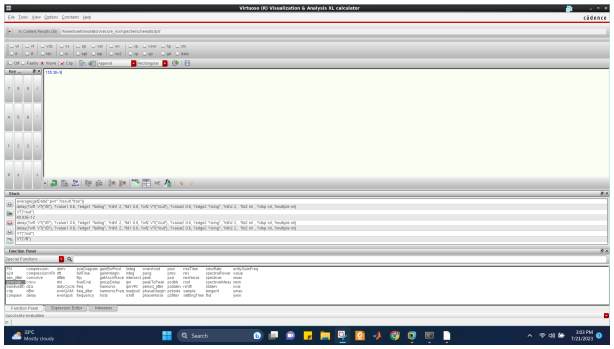

Fig. 19. Secure NOR gate Average Power

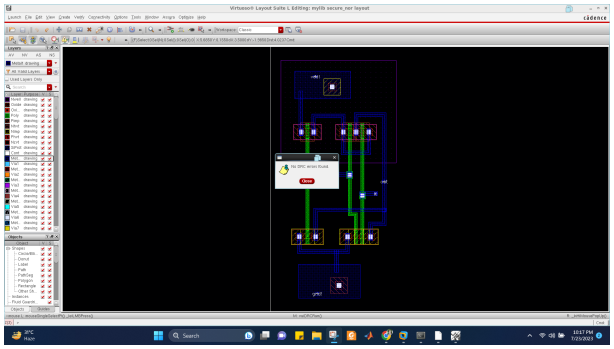

Fig. 20. Secure NOR Layout DRC

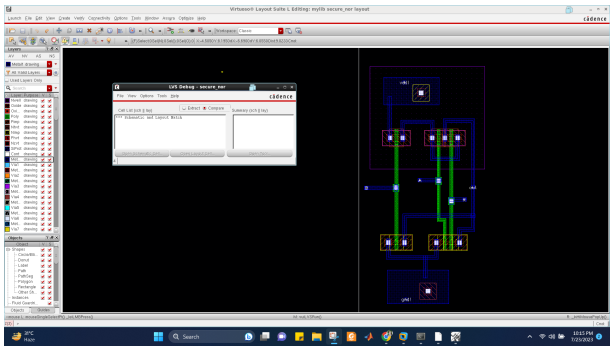

Fig. 21. Secure NOR Layout LVS

D. Secure NAND Gate

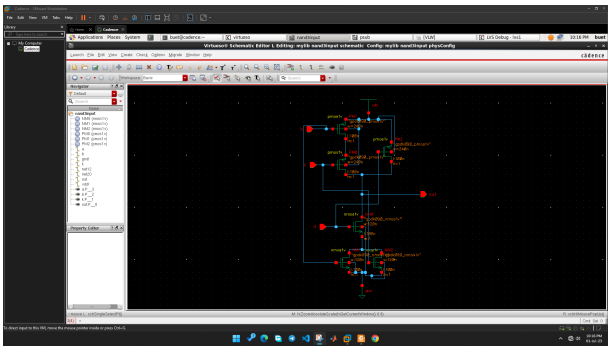

Fig. 22. Schamatic of Secure NAND Gate

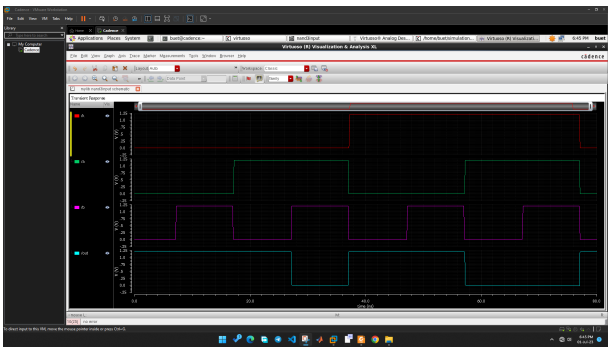

Fig. 23. Waveform of Secure NAND Gate

K	A	B	NAND
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Fig. 24. Secure NAND Gate Truth Table

When the logic level of K is 0, we get the output as Nand gate, which is the expected output of Nand gate. Whereas, if K = 1, the output will not provide the expected values of NAND gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of Nand gate will not be found.

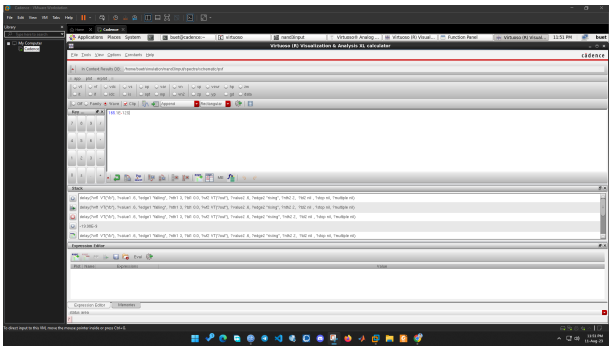

Fig. 25. Secure NAND gate Propagation Delay

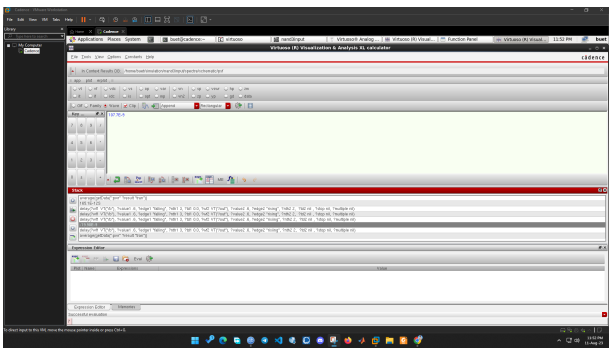

Fig. 26. Secure NAND gate Average Power

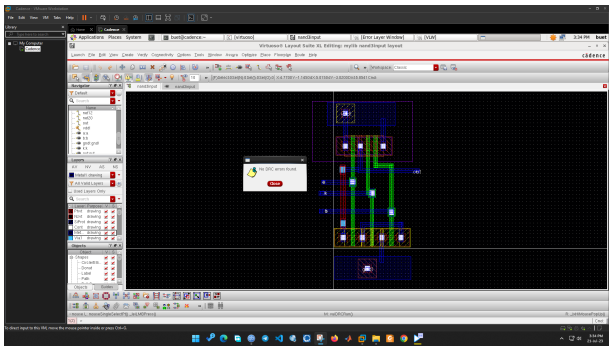

Fig. 27. Secure NAND Layout DRC

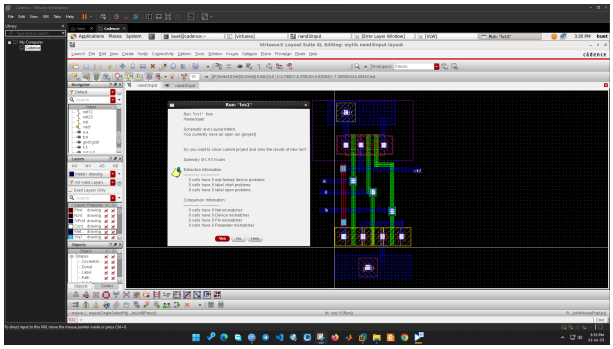

Fig. 28. Secure NAND Layout LVS

E. Secure XOR Gate

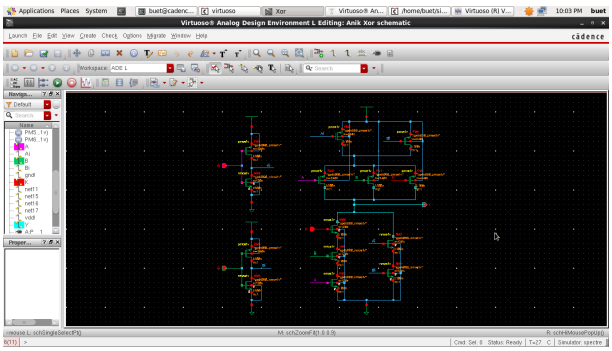

Fig. 29. Schamatic of Secure XOR Gate

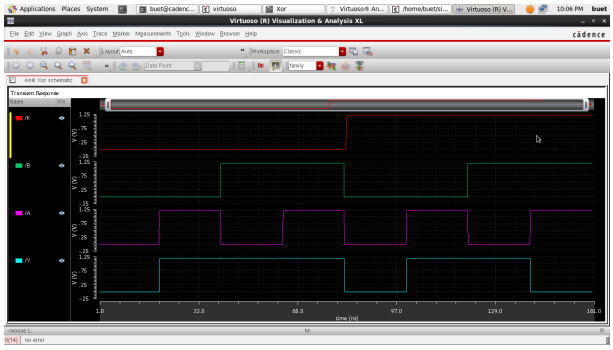

Fig. 30. Waveform of Secure XOR Gate

K	A	B	XOR
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

Fig. 31. Secure XOR Gate Truth Table

When the logic level of K is 1, we get the output as XOR gate, which is the expected output of XOR gate. Whereas, if K = 0, the output will not provide the expected values of XOR gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of XOR gate will not be found.

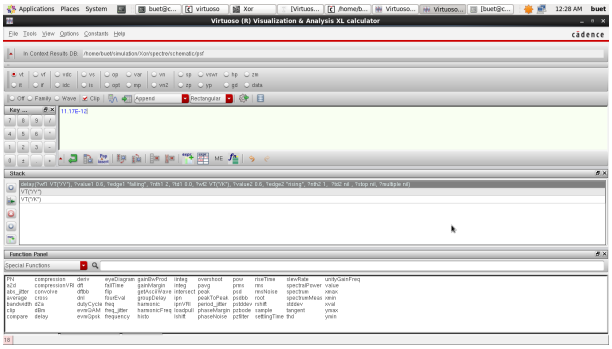

Fig. 32. Secure XOR gate Propagation Delay

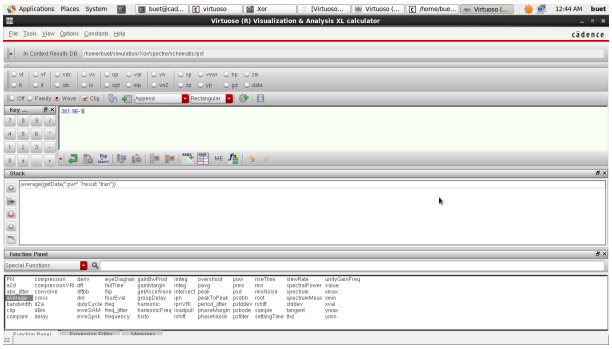

Fig. 33. Secure XOR gate Average Power

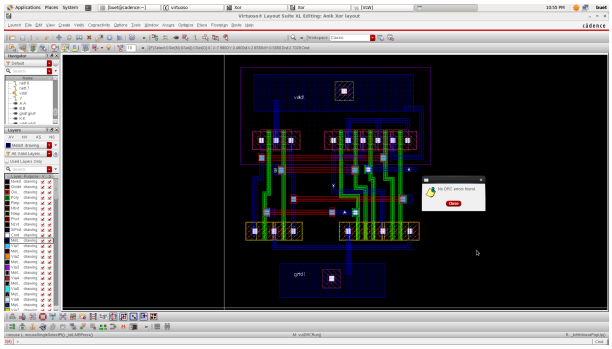

Fig. 34. Secure XOR Layout DRC

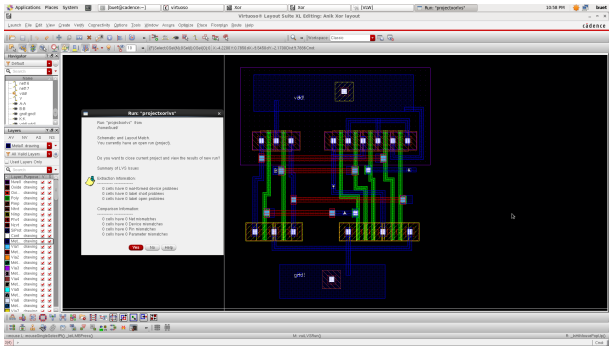

Fig. 35. Secure XOR Layout LVS

F. Secure XNOR Gate

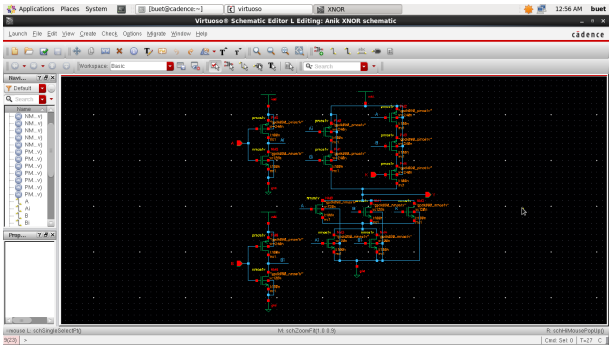

Fig. 36. Schamatic of Secure XNOR Gate

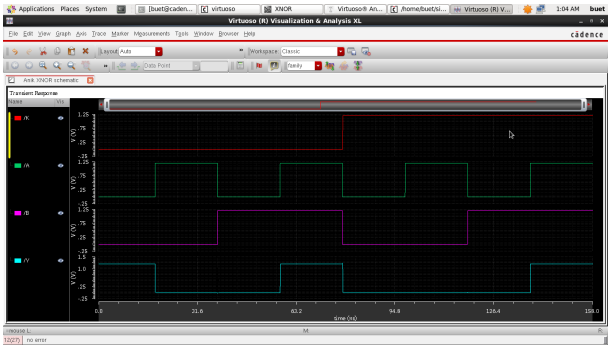

Fig. 37. Waveform of Secure XNOR Gate

K	A	B	XNOR
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

Fig. 38. Secure XNOR Gate Truth Table

When the logic level of K is 0, we get the output as XNOR gate, which is the expected output of XNOR gate. Whereas, if K = 1, the output will not provide the expected values of XNOR gate. In this way, the privacy of this gate is ensured as without the particular value of K, the accurate result of XNOR gate will not be found.

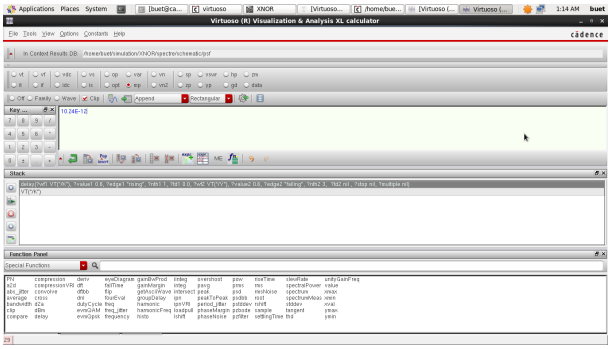

Fig. 39. Secure XNOR gate Propagation Delay

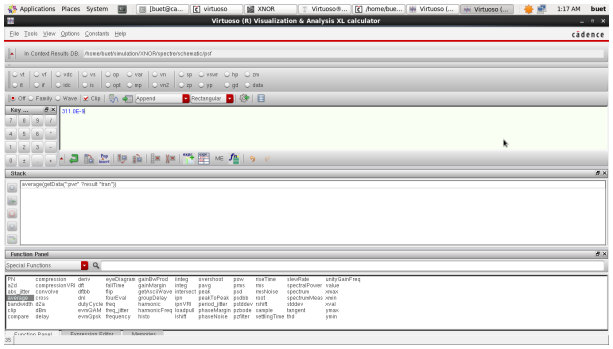

Fig. 40. Secure XNOR gate Average Power

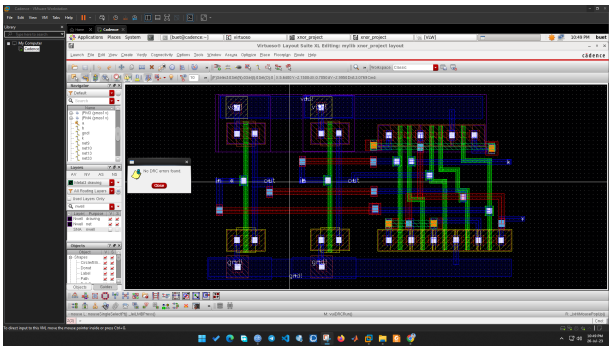

Fig. 41. Secure XNOR Layout DRC

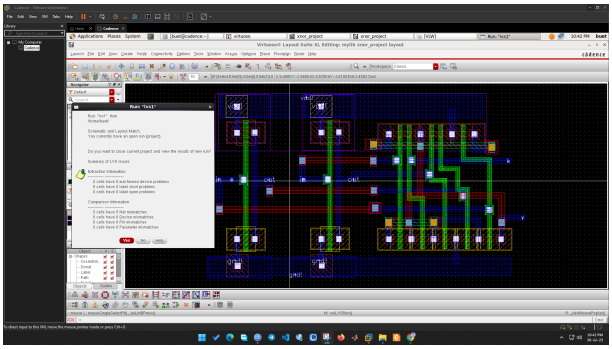

Fig. 42. Secure XNOR Layout LVS

III. DATA REPRESENTATION

Key	Inputs		Outputs					
K	A	B	AND	OR	XOR	NAND	NOR	XNOR
0	0	0	0	0	0	1	1	1
0	0	1	0	1	1	1	0	0
0	1	0	0	0	1	1	1	0
0	1	1	1	1	1	0	0	1
1	0	0	0	0	0	1	1	0
1	0	1	0	1	1	1	0	0
1	1	0	1	1	1	0	0	0
1	1	1	1	1	0	0	0	1

Fig. 43. Combined Truth Table

Gate no	Propagation delay	Average Power	Power delay Product	Cell area	No. transistors	No. of DRC	No. LVS Mismatches
NAND	143.8E-12	107.7E-9	1.587E-17	9.6288 micrometer	6	0	0
AND	165.1E-12	188.0E-9	3.103E-17	19.516 micrometer	8	0	0
NOR	40.83E-12	155.3E-9	6.341E-18	31.014 micrometer	6	0	0
OR	56.16E-12	280.4E-9	1.574E-17	36.636 micrometer	8	0	0
XOR	11.17E-12	361.9E-9	4.042E-18	37.0821 micrometer	14	0	0
XNOR	10.24E-12	311.0E-9	3.184E-18	33.7800 micrometer	14	0	0

Fig. 44. Comparison Table

IV. Future Aspects

Day by day, the necessity of hardware security is increasing because of the rise in intellectual property piracy. Therefore, the significance of logic encryption to protect circuits as well as specific secrets of design is increasing rapidly. Though, the proposed methodology for logic encryption is executed here for some simple logic gates (OR, AND, NOR, NAND, XOR, XNOR) designed with CMOS, it can be used for various complex circuits for maintaining the privacy along with efficient designing of circuits.

V. Conclusion

In this project, a new topology for CMOS gates at the transistor level is designed regarding the necessity of hardware security. The gates have an efficient structure to prevent intellectual property piracy, IC counterfeiting and reverse engineering. It was also observed that the proposed circuits reduce the area, delay, save power and energy compared to the existing methodologies of logic encryption. Thus, a trade-off between circuit performance for security purpose and design efficiency is ensured.

References

[1] Chandra, S.S., Kannan, R.J., Balaji, B.S. et al. Efficient esign and analysis of secure CMOS logic through logic encryption. Sci Rep 13, 1145 (2023). https://doi.org/10.1038/s41598-023-28007-2