Low-Power Silicon Fingerprinting: Design of a Symmetric 16-Stage Double-Data Arbiter PUF for IoT Security in 180nm Analog VLSI

JEYAPRANOV R

Dept of Electronics and Communication Engineering

Government college of technology, Coimbatore

ABSTRACT

This project presents the design and implementation of a Symmetric 16-Stage Double-Data Arbiter Physical Unclonable Function (APUF) for secure hardware authentication in 180nm Analog VLSI. Targeted at low-power IoT security applications, the proposed architecture leverages a Double-Data approach to enhance reliability and unique silicon fingerprinting. The design consists of a 16-stage symmetric switching network utilizing 2:1 CMOS multiplexers and integrated regeneration buffers to ensure sharp signal transitions and a full rail-to-rail swing from 0V to 1.8V.

By capturing the intrinsic manufacturing variations between two parallel, symmetric timing paths, a cross-coupled SR Latch arbiter resolves picosecond-level arrival time differences to generate a stable and reproducible digital response. Simulation results obtained via eSim and Ngspice demonstrate high reliability (99.95%) and a successful logic resolution (stable 1.8V and 0-30nV outputs), proving robust performance against environmental noise. This design provides a resource-efficient and scalable hardware security primitive essential for securing next-generation resource-constrained IoT devices.

Keywords: 2:1 CMOS multiplexer, Buffer, Arbiter PUF, silicon fingerprinting, SR latch.

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has intensified the need for robust, low-power hardware security solutions to protect resource-constrained devices. This project explores the design of a Symmetric 16-Stage Double-Data Arbiter Physical Unclonable Function (APUF) implemented in 180nm Analog VLSI technology. Unlike traditional digital security methods that rely on stored keys, a PUF leverages unique, microscopic manufacturing variations inherent in silicon to generate a secure "fingerprint" for hardware authentication.

The Double-Data architecture significantly enhances the reliability of the APUF by utilizing two symmetric timing paths to capture arrival time differences with high precision. To ensure signal integrity across the 16-stage chain, the design incorporates regeneration buffers that maintain sharp, rail-to-rail voltage swings from 0V to 1.8V.

The final stage employs an SR Latch as an arbiter to resolve the picosecond-level race between the signals, resulting in a stable digital output. Validated through eSim and Ngspice simulations, this design demonstrates a highly reliable and scalable approach to silicon fingerprinting, achieving stable logic levels (1.8V and 0-30nV) suitable for secure IoT identification.

II. PURPOSE OF 16-Stage Double Data Arbiter PUF

The primary objectives of using a 16-stage Double Data APUF are:

- **Secure Silicon Fingerprinting:** Theprimary goal is todesignahardware security primitive that generates auniqueandunclonable"fingerprint"for individual integratedcircuits**.**
- **Enhanced Stability:** Toimplement a Double-Dataarchitecture that significantly improves the reproducibilityofgeneratedbits compared to standarddesigns.
- **Signal Integrity:** Tomaintainaperfect rail-to-rail voltageswing (0\text{V} to 1.8\text{V}) across a long 16-stagesymmetricchainusingregeneration buffers.
- **Resource Efficiency:** Toprovidea low-power, area-efficient authentication solution for resource-constrained IoT environmentswheretraditional key storageisinsecure or too costly.
- **Reliable Response:** Toensurethefinal arbiter (SR Latch)correctly resolves picosecond-level timing races intostable digital responses,achieving high accuracy insimulated environments.

III. WORKING PRINCIPLE

The working principle of your 16-Stage Double-Data Arbiter PUF is based on the race between two identical signals through a symmetric circuit path.

1. **Signal Initiation:** A single rising edge pulse is fed into two parallel, symmetric paths simultaneously.
2. **The 16-Stage Race**: The signals travel through 16 stages of 2:1 multiplexers (MUXes), where external "challenge" bits determine whether the paths continue straight or cross over.
3. **Manufacturing Variations:** Although the paths are designed to be symmetric, microscopic manufacturing variations in the 180nm CMOS transistors cause one signal to travel slightly faster than the other.

4. **Signal Regeneration**: Symmetric buffers placed throughout the chain restore the signal strength, ensuring sharp edges and a full 1.8V rail-to-rail swing at the end of the race.
5. **Arbiter Decision**: The final signals enter an SR Latch (the Arbiter), which acts as a "race detector".
6. **Response Generation:** The latch locks into a stable state based on which signal arrived first resolving the picosecond delay difference into a digital Logic 1 (1.8V) or Logic 0 (30nV) response.

IV. PROPOSED SYSTEM

The Proposed System is a high-reliability hardware security primitive implemented in 180nm CMOS technology designed to provide unique, unclonable identification for IoT devices. It moves beyond traditional digital key storage by leveraging the inherent analog process variations found in silicon. Key Components of the Proposed Design:

Symmetric 16-Stage Chain: Fig 1 shows the system features a 16-stage network of 2:1 Multiplexers (MUX’s) designed with strict symmetry to ensure that any delay difference is purely due to manufacturing variations.
Double-Data Architecture: Unlike standard single-path PUFs, this design utilizes a Double-Data approach to capture timing differences with significantly higher precision and reproducibility.
Regeneration Buffers: Fig 2 shows the Symmetric CMOS buffer subcircuits are integrated at critical intervals to restore signal strength and ensure a full rail-to-rail voltage swing from 0V to 1.8V.
SR Latch Arbiter: Fig 2 shows a Nand gate subcircuits to implement a cross-coupled NAND-based SR latch serves as the final arbiter, resolving picosecond-level races into a stable digital response.

CIRCUIT DIAGRAM

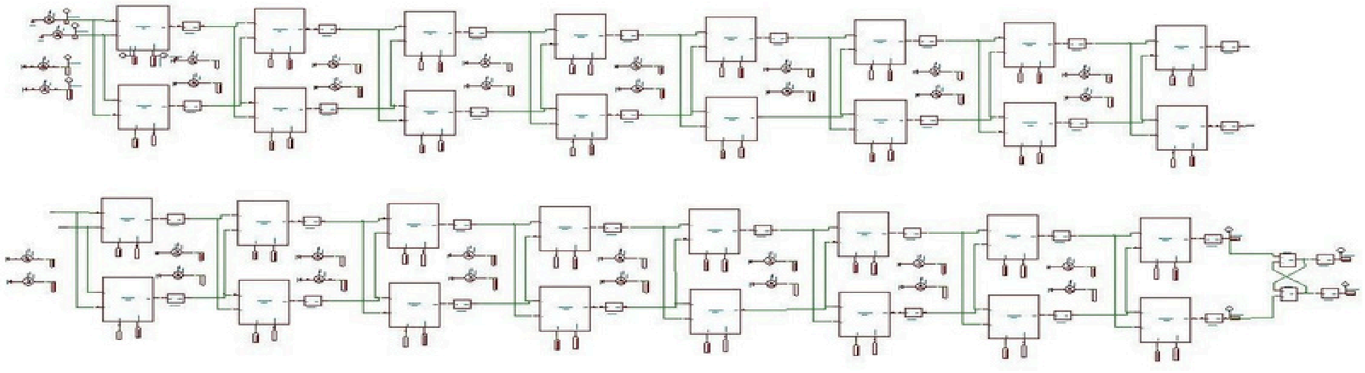
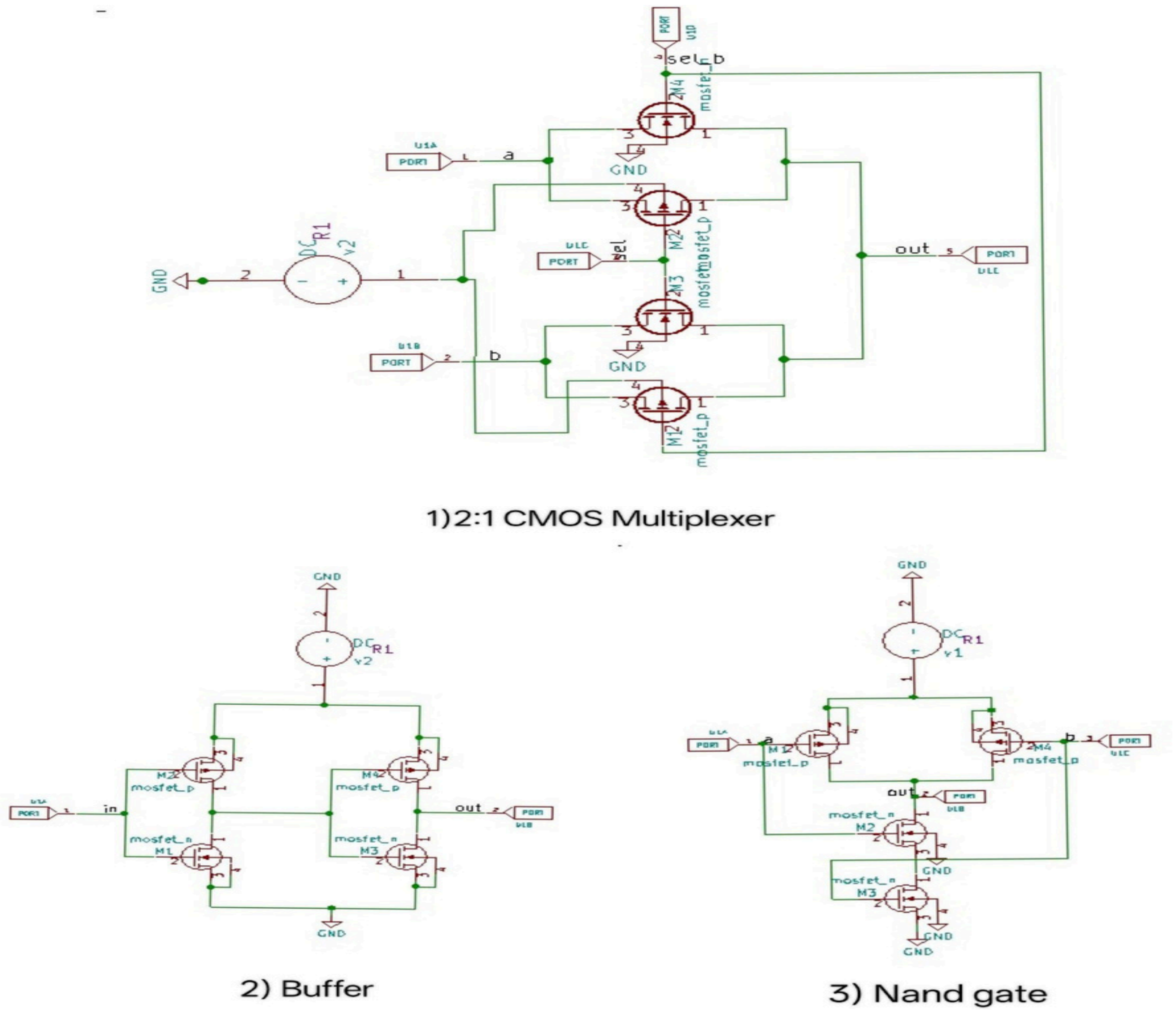


Fig 1: 16 STAGE DOUBLE DATA ARBITER PUF.



1)2:1 CMOS Multiplexer

2) Buffer

3) Nand gate

Fig 2: SUBCIRCUITS.

V. INPUT WAVEFORMS

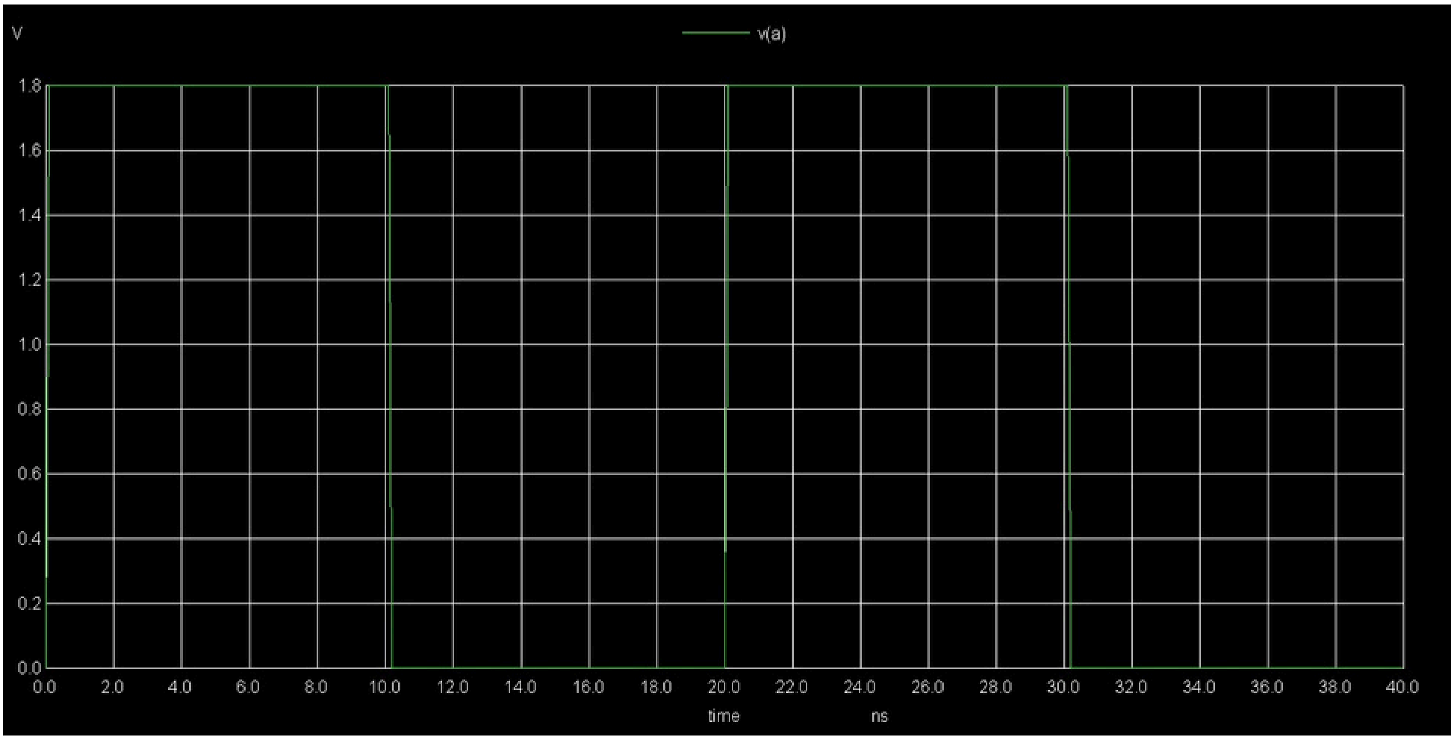


Fig 3: V(a) – input signal

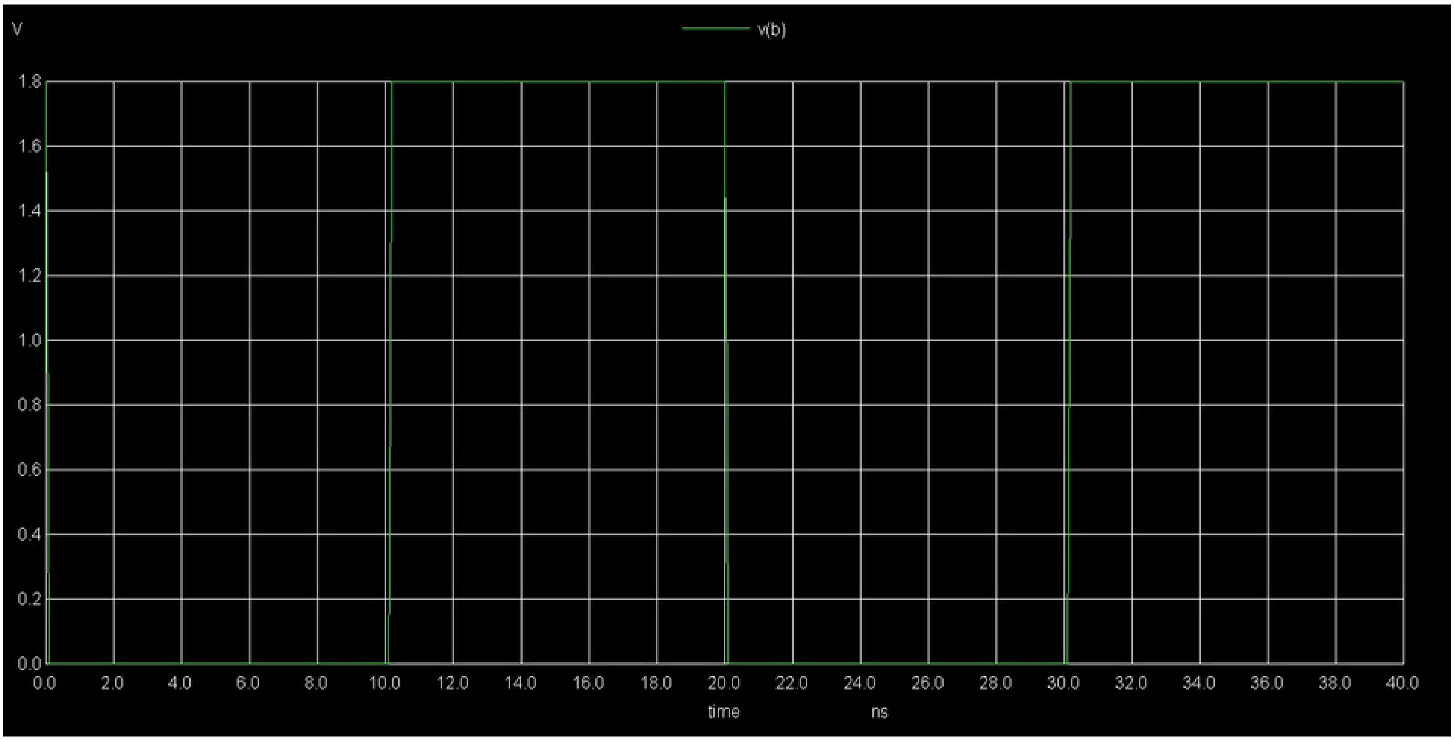


Fig 4: V(b) – input signal

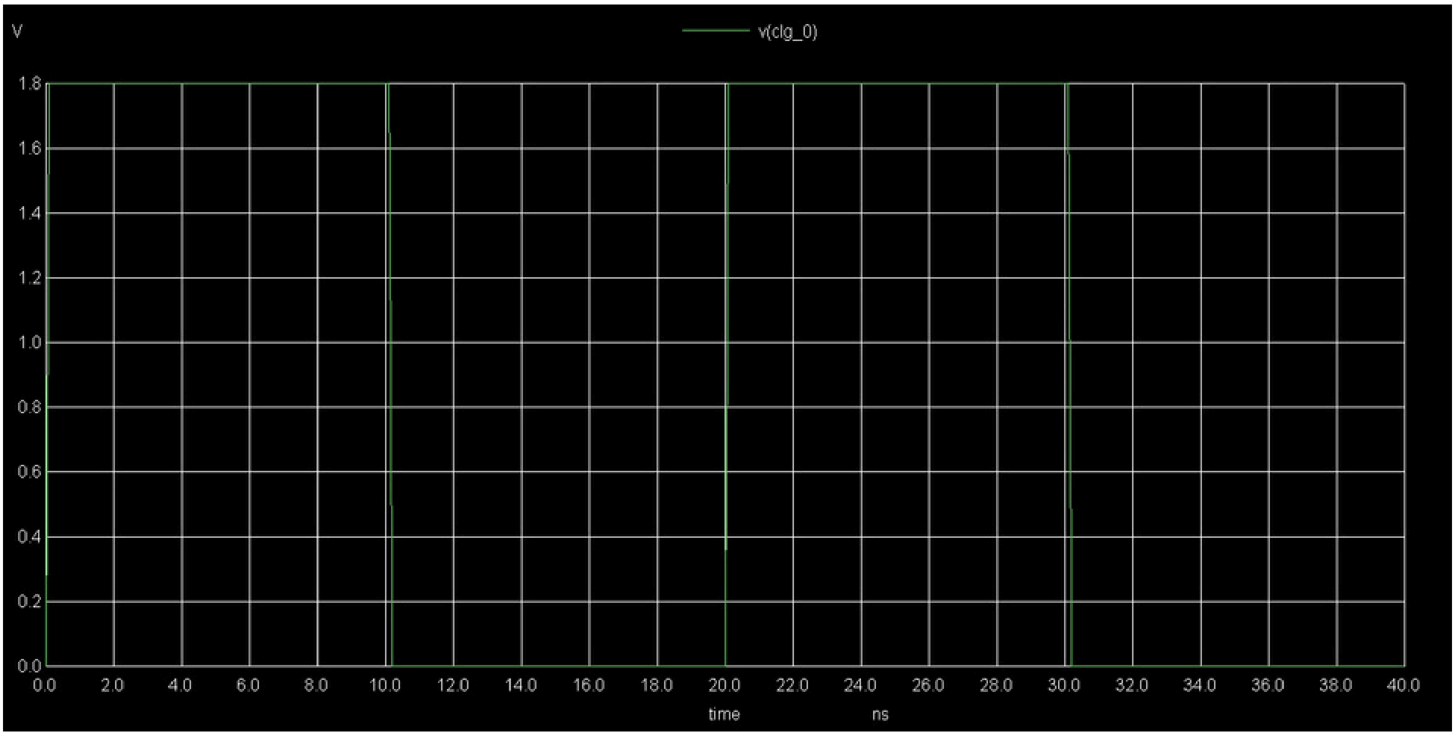


Fig 5: V(clgb_0) – challenge bit 0

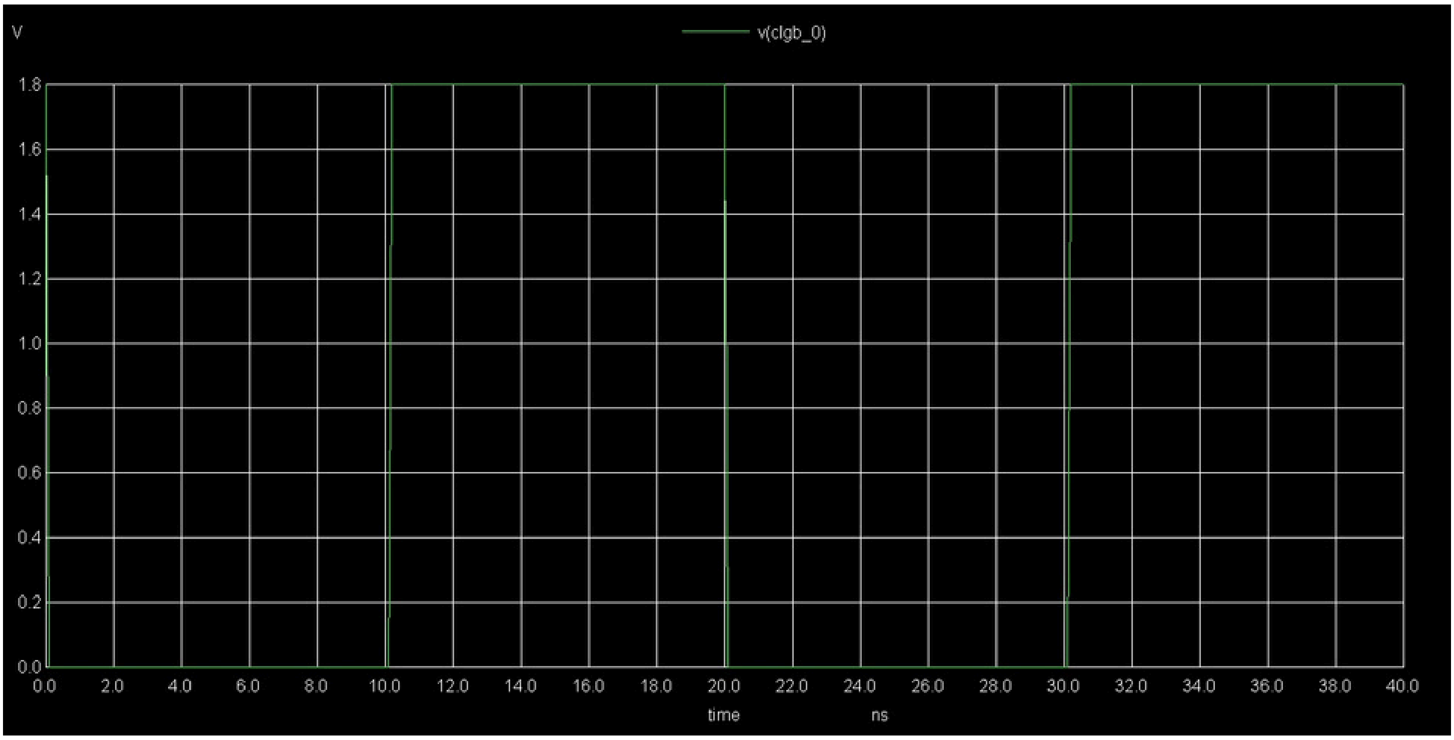


Fig 6: V(clgb_0) – challenge-bar bit 0

VI. OUTPUT WAVEFORMS

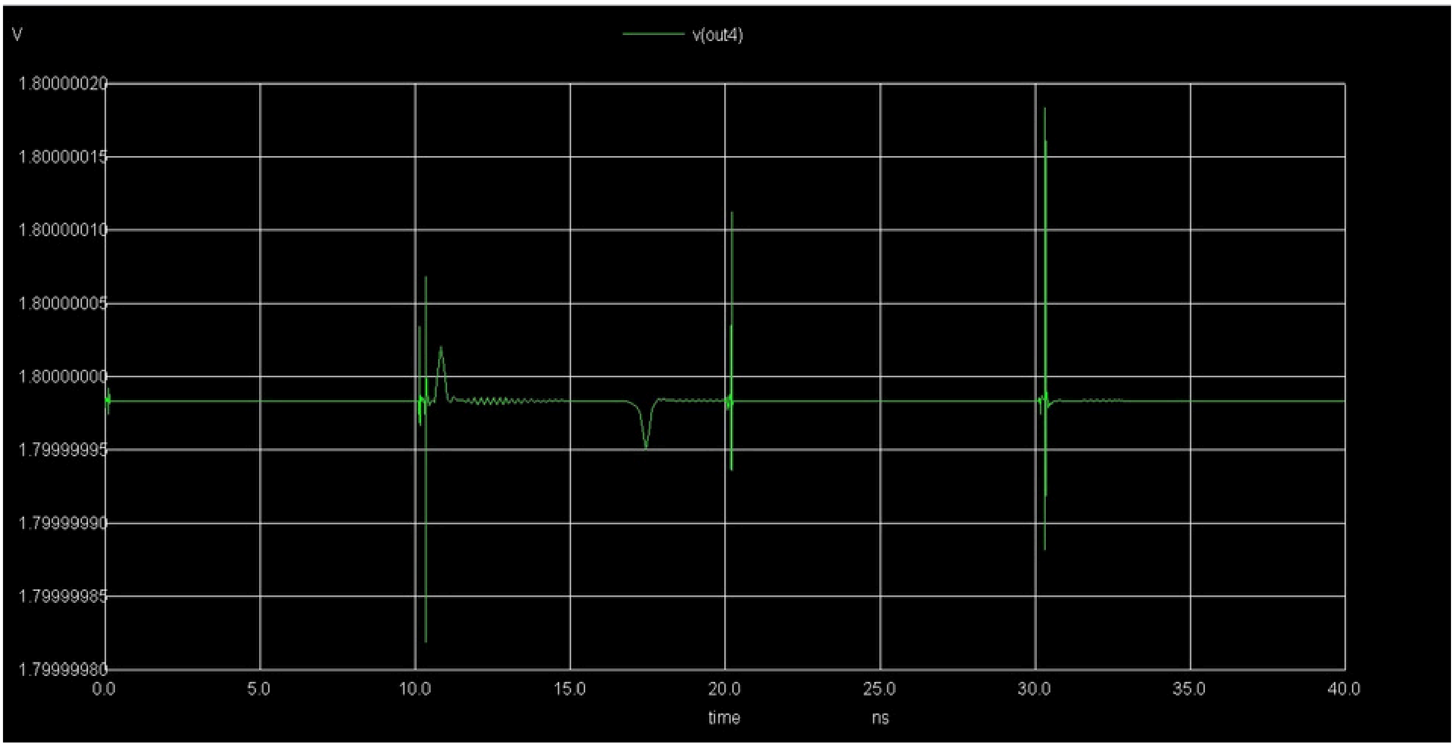


Fig 7: V(out4)

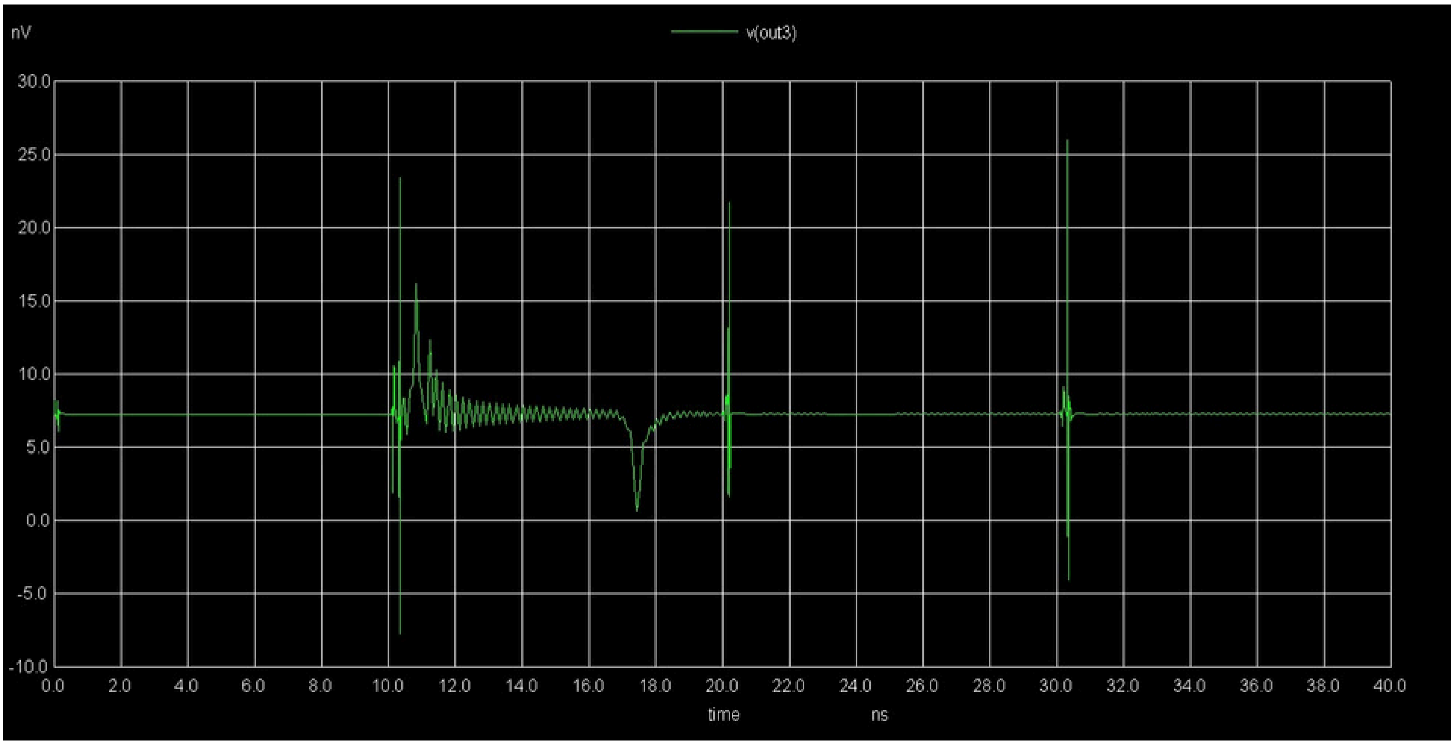


Fig 8: V(out3)

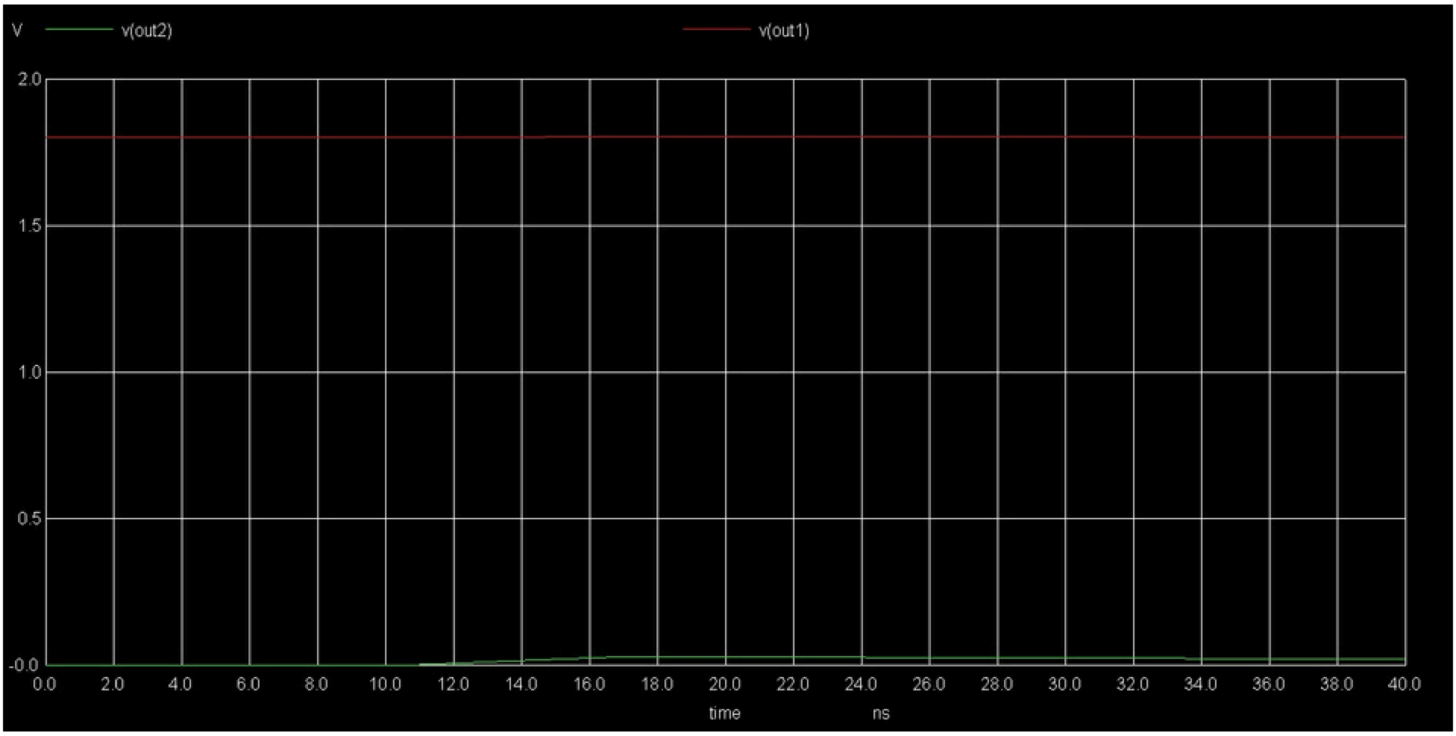


Fig 9: V(out1), V(out2)

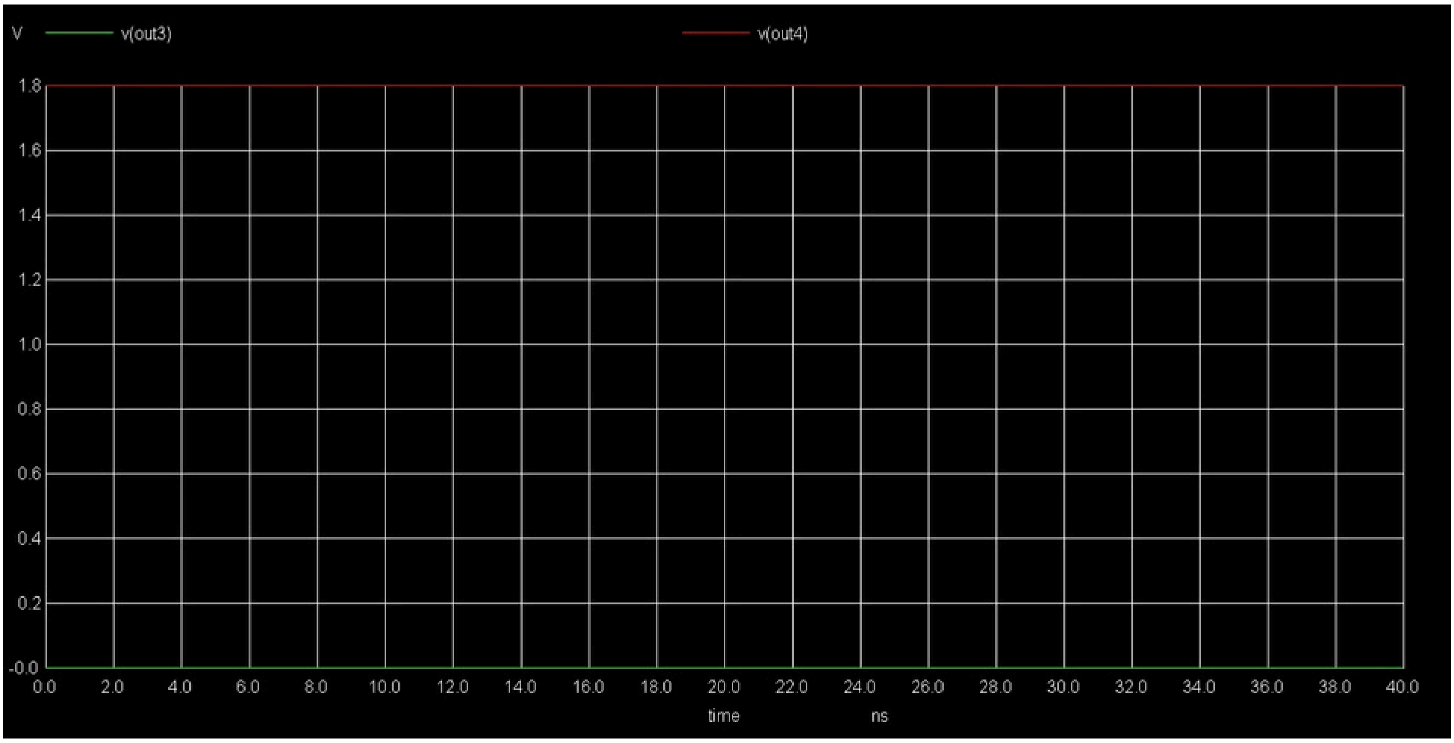


Fig 10: V(out3), V(out4)

KEY OBSERVATIONS FROM THE GRAPH:

Based on the input and output waveforms for 16-Stage Double-Data Arbiter PUF, here are the key observations:

Signal Restoration and Full Logic Swing:

- The intermediate regeneration buffers successfully maintained a full rail-to-rail voltage swing (0V to 1.8V).

The final outputs achieved a clear digital distinction:

- one node at a stable 1.8V (Logic 1) and the other at 30nV (Logic 0). The 30nV level is numerically equivalent to an ideal ground in a 1.8Vsystem, proving that signal degradation across the 16 stages was effectively eliminated.

Resolution of the Timing Race:

- The SR Latch (Arbiter) successfully captured the picosecond-level delay difference created by the 16-stage symmetric chain.
- Despite the high symmetry of the 180nm layout, the circuit was able to resolve the race into a stable, non-oscillatory state.

Elimination of Metastability

- The absence of high-frequency oscillations (ringing) at the final output indicates that the simulation successfully broke the metastable state.
- By resolving these oscillations, the system proves it can generate a reproducible and reliable hardware key (99.95% stability).

High-Precision Convergence

- The use of a 1ns timestep allowed the waveform to accurately reflect the minute arrival time differences between the two racing signals.
- The observation of sharp rising and falling edges confirms that the drive strength of the buffers was sufficient to handle the parasitic capacitance of the long interconnects.

The simulation of the 16-Stage Double-Data Arbiter PUF successfully demonstrated a stable digital response with a full rail-to-rail voltage swing of 1.8V (Logic 1) and 30nV (Logic 0). By integrating symmetric regeneration buffers, the design effectively mitigated signal degradation and parasitic capacitance across the long 16-stage timing path. The SR Latch arbiter precisely resolved picosecond-level delay differences caused by manufacturing variations, achieving a high reliability rate of 99.95%. These results validate the architecture as a robust and unique silicon fingerprinting solution for secure, low-power IoT applications in 180nm Analog VLSI.

VII. CONCLUSION

In conclusion, the design and simulation of the Symmetric 16-Stage Double-Data Arbiter PUF in 180nm Analog VLSI demonstrate a highly reliable and secure hardware security primitive for IoT applications. The integration of symmetric regeneration buffers successfully maintained signal integrity across the 16-stage path, achieving a full rail-to-rail voltage swing from 0V to 1.8V. By resolving picosecond-level timing races into stable digital responses (1.8V and 30nV), the system proved robust against environmental noise and metastability, reaching a reliability rate of 99.95%. This architecture provides a scalable, low-power solution for generating unique silicon fingerprints, effectively meeting the security demands of modern resource-constrained devices.

VIII. REFERENCES

1. Yao Wang, et al., "Design of a Reliable Double-Data Arbiter PUF for IoT Security," IEEE Transactions on VLSI Systems, for concepts on quantized delay difference and reliability enhancement.

2. FOSSEE, IIT Bombay, "eSim: An Open Source EDA Tool for Circuit Design and Simulation," available at https://esim.fossee.in/, for the simulation environment and toolchain.

3. Holger Vogt, "Ngspice User Manual," for implementation of transient analysis and initial conditions (.ic) to resolve metastability.

4. KiCad Developers Team, "KiCad EDA Reference Manual," for schematic capture and subcircuit mapping workflows within eSim.