ISSN 2319-5991 www.ijerst.com

Peer Reviewed, Referred & Indexed Journal

Research Paper

FPGA-BASED LIGHTWEIGHT HYBRID PHYSICAL UNCLONABLE FUNCTION FOR SECURE DEVICE AUTHENTICATION USING ARBITER AND RING OSCILLATOR ARCHITECTURES

VASANTHA KONGONDI[1], Mrs. K. SNEHALATHA[2]

[1]**PG Scholar,** VLSI SYSTEM DESIGN, ECE DEPARTMENT, JNTUH University College of Engineering, Sultanpur. vasantha.kongondi2002@gmail.com

[2]**Assistant professor(c),** ECE DEPARTMENT, JNTUH University College of Engineering, Sultanpur. snehakatha08@gmail.com

Abstract: The rapid growth of Internet of Things (IoT), embedded systems, and edge computing devices has increased the demand for robust hardware security solutions capable of preventing cloning, counterfeiting, and unauthorized access. Physical Unclonable Functions (PUFs) have emerged as an effective hardware-based security mechanism by exploiting inherent manufacturing variations in integrated circuits to generate unique device identities. This paper presents the design and FPGA implementation of a lightweight Hybrid Physical Unclonable Function (PUF) that combines the advantages of Arbiter PUF and Ring Oscillator (RO) PUF architectures. The proposed hybrid structure utilizes delay-based characteristics from the Arbiter PUF and frequency-based variations from the Ring Oscillator PUF to generate highly unique and reliable challenge–response pairs. The outputs from both PUF modules are combined through an XOR-based response generation mechanism to enhance randomness, uniqueness, and resistance against modelling attacks.

The architecture is implemented using Verilog HDL and validated through simulation and FPGA synthesis. Experimental analysis demonstrates improved security performance, enhanced reliability, and reduced hardware resource utilization compared to conventional standalone PUF architectures. The floorplan-aware implementation further improves response stability and minimizes routing-induced variations. The proposed design offers a low-area, cost-effective, and secure authentication solution suitable for FPGA-based embedded systems, IoT devices, and next-generation hardware security applications.

Keywords: Physical Unclonable Function (PUF), FPGA Security, Arbiter PUF, Ring Oscillator PUF, Hybrid PUF Architecture, Device Authentication, Hardware Security, IoT Security, Verilog HDL, Lightweight Cryptographic Hardware

I. INTRODUCTION

The rapid advancement of digital technologies, embedded systems, Internet of Things (IoT) devices, and cyber-physical systems has significantly increased the demand for secure and reliable hardware authentication mechanisms. Modern electronic devices are frequently exposed to security threats such as counterfeiting, cloning, unauthorized access, reverse engineering, and hardware tampering. Traditional security approaches primarily rely on storing cryptographic keys in non-volatile memory, making them vulnerable to physical attacks, side-channel analysis, and key extraction techniques. As a result, there is an increasing need for innovative hardware-based security solutions capable of providing strong protection against these threats while maintaining low implementation cost and power consumption.

Physical Unclonable Functions (PUFs) have emerged as a promising hardware security primitive that utilizes inherent manufacturing process variations in integrated circuits to generate unique and device-specific responses. Since these process variations occur naturally and cannot be precisely duplicated, PUFs provide a reliable means of generating hardware fingerprints for secure authentication and identification. Unlike conventional security mechanisms that require secret keys to be stored in memory, PUFs generate responses dynamically based on intrinsic physical characteristics of the device, thereby eliminating the risks associated with key storage.

In recent years, PUF technology has attracted considerable attention in applications such as secure device authentication, cryptographic key generation, anti-counterfeiting systems, hardware intellectual property protection, secure boot mechanisms, and trusted computing platforms. The increasing deployment of IoT devices in smart homes, healthcare systems, industrial automation, transportation networks, and smart cities has further accelerated the need for lightweight and cost-effective hardware security solutions. PUFs offer an attractive alternative because they provide high security with minimal hardware overhead, making them suitable for resource-constrained embedded systems.

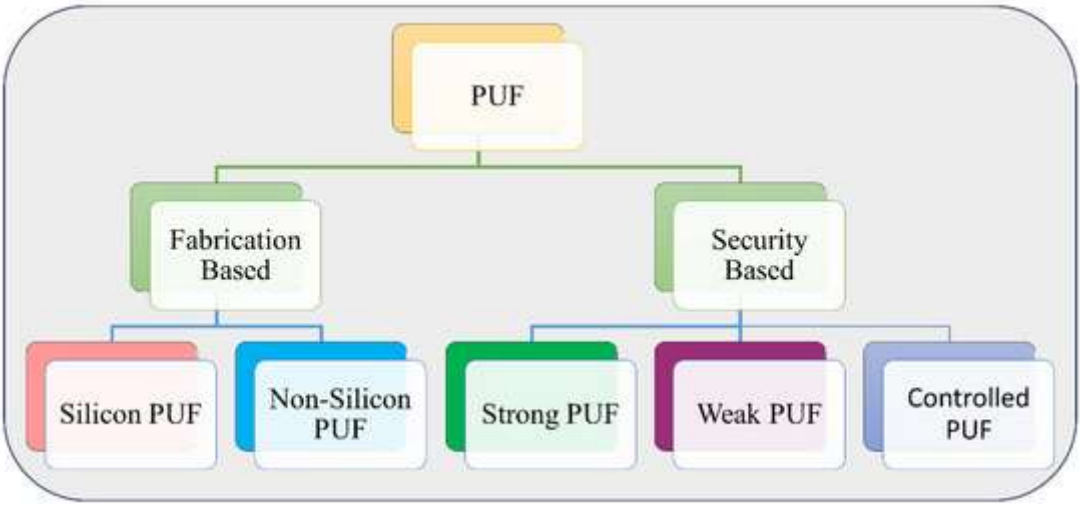

Fig 1 FPGA based PUF design

Several PUF architectures have been proposed in the literature, including Arbiter PUFs, Ring Oscillator PUFs, SRAM PUFs, Butterfly PUFs, and Memory-Based PUFs. Among these architectures, Arbiter PUFs and Ring Oscillator PUFs are widely used due to their simplicity, scalability, and FPGA implementation capability. Arbiter PUFs exploit propagation delay differences between signal paths to generate challenge-response pairs. They provide a large challenge-response space and require relatively low hardware resources. However, Arbiter PUFs are susceptible to environmental variations and machine learning attacks, which may reduce their security and reliability under certain conditions.

Ring Oscillator PUFs, on the other hand, utilize frequency differences among multiple ring oscillators caused by manufacturing process variations. These PUFs exhibit excellent uniqueness and reliability characteristics and provide stable responses under varying operating conditions. Nevertheless, Ring Oscillator PUFs generally require additional hardware resources, counters, and routing elements, resulting in increased area and power consumption. Consequently, the implementation of standalone Ring Oscillator PUFs may not be optimal for highly resource-constrained FPGA platforms and embedded applications.

To overcome the limitations of individual PUF architectures, researchers have explored hybrid PUF designs that combine multiple entropy sources to enhance security performance. Hybrid PUF architectures leverage the strengths of different PUF mechanisms while mitigating their individual weaknesses. By integrating delay-based and frequency-based randomness sources, hybrid PUFs can achieve improved uniqueness, reliability, randomness, and resistance against modeling attacks. Such architectures are particularly beneficial for FPGA-based security implementations where both performance and hardware efficiency are critical design considerations.

Field Programmable Gate Arrays (FPGAs) provide a flexible and reconfigurable platform for implementing hardware security mechanisms. FPGA devices enable rapid prototyping, testing, and optimization of security architectures while offering reduced development cost and shorter design cycles. Furthermore, FPGA-based implementations allow designers to evaluate security performance under different operating conditions and deployment environments. As a result, FPGA technology has become a popular platform for implementing PUF-based authentication systems and hardware root-of-trust solutions.

This work presents a lightweight Hybrid Physical Unclonable Function architecture that combines Arbiter PUF and Ring Oscillator PUF structures to improve hardware security performance. The proposed design exploits propagation delay variations in the Arbiter PUF and frequency variations in the Ring Oscillator PUF to generate highly unique and unpredictable responses.

The outputs from both modules are combined using an XOR-based response generation mechanism to

increase entropy and strengthen resistance against prediction and modeling attacks. The hybrid architecture is optimized for low-area FPGA implementation while maintaining robust security characteristics.

The proposed system is developed using Verilog Hardware Description Language (HDL) and implemented on an FPGA platform. A floorplan-aware design methodology is employed to minimize routing-induced variations and improve response stability. The architecture aims to achieve enhanced uniqueness, reliability, and randomness while reducing hardware overhead compared to conventional PUF implementations. Simulation and synthesis results demonstrate the effectiveness of the proposed approach in generating secure challenge-response pairs suitable for authentication and device identification applications.

The major contributions of this work include the development of a lightweight hybrid PUF architecture, integration of Arbiter and Ring Oscillator entropy sources, FPGA-based implementation using Verilog HDL, floorplan-aware optimization for improved stability, and comprehensive evaluation of security performance. The proposed system provides a practical and cost-effective solution for securing embedded systems, IoT devices, industrial controllers, and future hardware security applications.

As the demand for trusted electronic systems continues to grow, hybrid PUF architectures are expected to play a significant role in establishing secure hardware identities and protecting devices against cloning and unauthorized access. The proposed FPGA-based lightweight hybrid PUF offers an efficient pathway toward achieving secure, reliable, and scalable hardware authentication in next-generation digital systems.

II. LITERATURE SURVEY

The increasing demand for hardware security in embedded systems, Internet of Things (IoT) devices, and cyber-physical systems has motivated extensive research on Physical Unclonable Functions (PUFs). PUFs exploit uncontrollable manufacturing process variations in integrated circuits to generate unique challenge-response pairs, enabling secure device authentication and cryptographic key generation. Various PUF architectures have been proposed over the years to improve uniqueness, reliability, randomness, and resistance against attacks.

Lee et al. introduced the Arbiter PUF architecture as one of the earliest delay-based PUF designs. The Arbiter PUF generates responses by comparing propagation delays between two symmetric signal paths controlled by challenge bits. The architecture provides a large challenge-response space and low hardware overhead, making it suitable for FPGA implementations. However, subsequent studies revealed that Arbiter PUFs are vulnerable to machine-learning attacks due to the linear relationship between challenges and responses. Although Arbiter PUFs offer efficient hardware utilization, their resistance against modeling attacks remains a major concern.

Suh and Devadas proposed Ring Oscillator (RO) PUFs, which utilize frequency variations among multiple ring

oscillators caused by manufacturing process variations. The frequency differences are measured and compared to generate unique responses. Experimental evaluations demonstrated that RO-PUFs provide excellent uniqueness and reliability compared to many delay-based architectures. However, the requirement for multiple oscillators, counters, and comparison circuits increases hardware resource utilization and power consumption, making the design less suitable for highly resource-constrained systems.

Maiti and Schaumont investigated FPGA-based implementation techniques for Ring Oscillator PUFs and analyzed the impact of routing variations on response stability. Their research highlighted the importance of floorplanning and placement constraints in FPGA implementations. The study demonstrated that careful placement of ring oscillators significantly improves reliability and reproducibility of responses under varying environmental conditions such as temperature and supply voltage fluctuations.

Herder et al. presented a comprehensive survey on PUF technologies and discussed their applications in secure authentication, key generation, anti-counterfeiting, and hardware protection. The authors categorized PUFs into delay-based, memory-based, and oscillator-based architectures and evaluated their strengths and limitations. Their study concluded that no single PUF architecture provides optimal performance in all aspects, motivating the development of hybrid PUF structures that combine multiple entropy sources.

Majzoobi et al. proposed an enhanced Arbiter PUF architecture employing feed-forward and XOR mechanisms to improve resistance against machine-learning attacks. The additional nonlinear structures increased modeling complexity and strengthened security. Experimental results showed improved unpredictability and robustness. However, the increased architectural complexity resulted in higher resource utilization and reduced implementation efficiency.

Ruhrmair et al. demonstrated successful machine-learning attacks on conventional Arbiter PUFs and highlighted the need for stronger PUF architectures. Their research showed that standard Arbiter PUF challenge-response behavior could be accurately modeled using machine-learning algorithms. The study emphasized the necessity of introducing nonlinear components and hybrid architectures to improve attack resistance and long-term security.

Yin and Qu developed a configurable FPGA-based PUF framework capable of generating multiple hardware fingerprints using programmable resources. Their work demonstrated the feasibility of implementing lightweight authentication mechanisms on FPGA platforms while maintaining acceptable reliability and uniqueness. The study also highlighted the importance of balancing security performance with hardware overhead in practical embedded applications.

Maes et al. investigated secure key generation techniques using PUF responses. Their research focused on improving reliability through error

correction and helper data algorithms. The study demonstrated that stable cryptographic keys could be generated without storing secret information in memory, thereby enhancing resistance against physical attacks and reverse engineering.

Kumar et al. proposed a hybrid PUF architecture combining delay-based and oscillator-based entropy sources to improve response randomness and uniqueness. The hybrid design generated challenge-response pairs using multiple independent randomness sources, significantly improving resistance against prediction attacks. Experimental evaluations indicated superior security characteristics compared to standalone Arbiter and Ring Oscillator PUF implementations.

Delvaux and Verbauwhede analyzed the reliability of FPGA-based PUF implementations under environmental variations. Their work revealed that temperature fluctuations, voltage variations, and routing inconsistencies could significantly affect response stability. The authors recommended floorplan-aware design methodologies and optimized placement strategies to minimize environmental sensitivity and improve reproducibility.

Recent research trends focus on developing lightweight and secure hybrid PUF architectures capable of meeting the requirements of IoT and embedded systems. Several studies have explored combining multiple PUF mechanisms, including Arbiter, Ring Oscillator, SRAM, and Butterfly PUFs, to improve security metrics such as uniqueness, reliability, randomness, and attack resistance. Hybrid architectures have shown promising results by leveraging the advantages of different entropy sources while reducing individual limitations.

Despite significant advancements, several research challenges remain unresolved. Conventional Arbiter PUFs continue to face modeling attack vulnerabilities, while Ring Oscillator PUFs require considerable hardware resources and power consumption. Existing hybrid architectures often increase implementation complexity and area overhead. Furthermore, routing variations in FPGA platforms can negatively impact response consistency and reliability. Therefore, there is a need for a lightweight, floorplan-aware hybrid PUF architecture capable of achieving improved security, reliability, and hardware efficiency simultaneously.

The proposed FPGA-based Lightweight Hybrid Physical Unclonable Function addresses these challenges by combining Arbiter PUF and Ring Oscillator PUF architectures in a unified framework. By integrating delay-based and frequency-based entropy sources and employing an XOR-based response generation mechanism, the proposed design enhances randomness, uniqueness, and resistance against modeling attacks while maintaining low hardware overhead and improved FPGA implementation efficiency.

III. PROPOSED METHODOLOGY

This work proposes a lightweight FPGA-based Hybrid Physical Unclonable Function (PUF) architecture that combines the advantages of Arbiter PUF and Ring Oscillator (RO) PUF techniques to achieve secure device authentication with low hardware overhead. The proposed system utilizes both delay-based and frequency-based

manufacturing variations present in integrated circuits to generate highly unique and unpredictable challenge-response pairs (CRPs). By combining the outputs of two different PUF mechanisms, the overall security, reliability, and resistance against modeling attacks are significantly enhanced.

The proposed architecture consists of six major modules: Challenge Generator, Arbiter PUF Block, Ring Oscillator Bank, Frequency Counter and MSB Extraction Unit, XOR-Based Response Generator, and FPGA Output Interface. The complete system is implemented using Verilog HDL and synthesized on an FPGA platform.

1. Challenge Generation Module

The challenge generation module provides a 32-bit challenge vector to the Arbiter PUF. The challenge bits determine the switching configuration of each stage within the Arbiter PUF. Different challenge inputs produce different propagation paths, resulting in unique response bits. The challenge values can be applied through FPGA switches or generated internally for testing purposes.

2. Arbiter PUF Module

The Arbiter PUF consists of 32 cascaded switching stages. Each stage contains multiplexers controlled by the challenge bits. Two identical signals are launched simultaneously through parallel paths. Due to unavoidable manufacturing process variations, small delay differences occur between the signal paths.

At the output, an arbiter compares the arrival times of the two signals:

- If Signal A arrives first, the response bit is logic '1'.
- If Signal B arrives first, the response bit is logic '0'.

Thus, a single-bit response is generated based on delay characteristics unique to each FPGA device.

3. Ring Oscillator PUF Module

The Ring Oscillator PUF employs eight independent ring oscillators, each consisting of an odd number of inverter stages connected in a feedback loop. Due to fabrication process variations, every oscillator operates at a slightly different frequency.

When enabled, all ring oscillators begin oscillating simultaneously. The oscillation frequencies are measured using dedicated counters over a fixed observation period. The frequency differences between oscillators provide an additional source of randomness and uniqueness.

4. Frequency Counter and MSB Extraction

Each ring oscillator output is connected to a 16-bit counter. During the measurement interval, the counters record the number of oscillations generated by the corresponding ring oscillator.

After the counting period is completed:

- The most significant bit (MSB) of each counter is extracted.
- The extracted bits form an 8-bit Ring Oscillator response vector.

The MSB extraction process reduces hardware complexity while preserving the essential entropy generated by frequency variations.

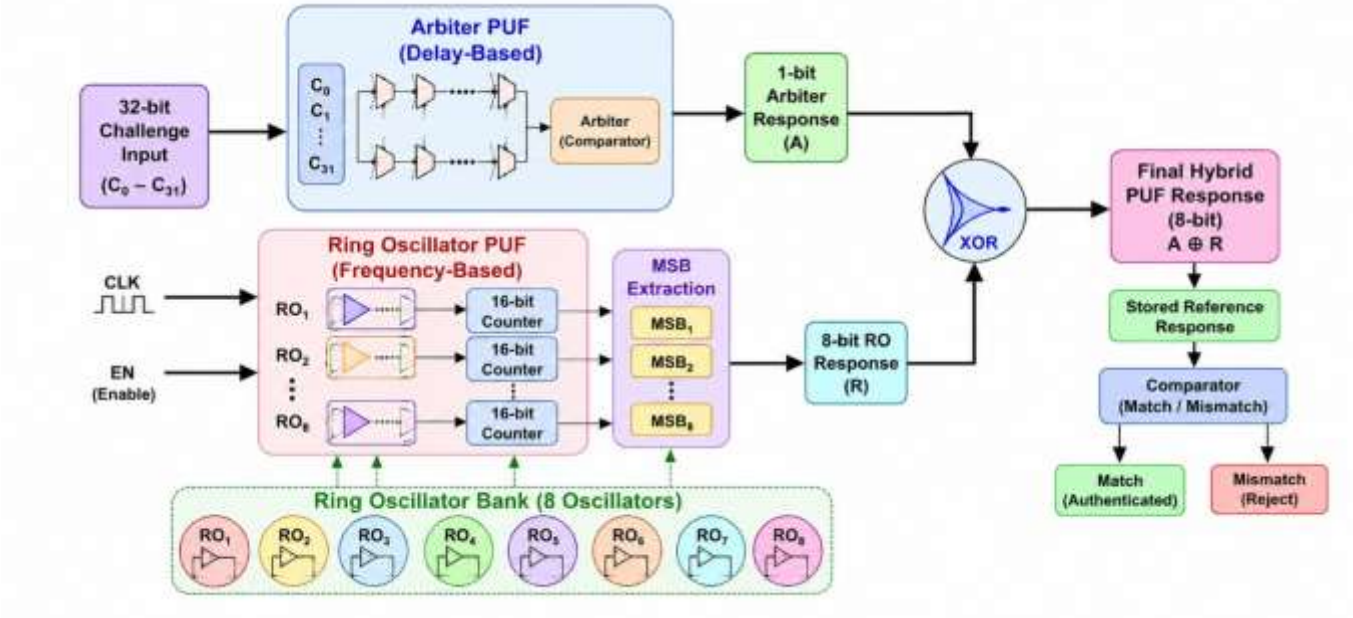

Fig 2 Proposed method

5. Hybrid Response Generation Using XOR Operation

The proposed architecture combines the outputs of the Arbiter PUF and Ring Oscillator PUF using an XOR-based fusion mechanism.

Let:

- Arbiter PUF Response = A
- Ring Oscillator Response = R

The final hybrid response is generated as:

[
PUF_{Final} = A \oplus R
]

where the single-bit Arbiter response is replicated across all bits and XORed with the Ring Oscillator response vector.

This operation increases randomness and unpredictability while improving resistance to machine-learning and modeling attacks. Since an attacker must simultaneously model both delay-based and frequency-based behaviors, the overall attack complexity increases significantly.

6. Floorplan-Aware FPGA Implementation

To improve response stability, a floorplan-aware design methodology is adopted. The ring oscillators are carefully placed within predefined FPGA regions to minimize routing-induced variations.

The advantages of floorplan-aware placement include:

- Reduced routing delays
- Improved response reproducibility
- Enhanced reliability under temperature variations
- Better frequency stability of ring oscillators

This placement strategy ensures consistent performance across different operating conditions.

7. Authentication Process

The authentication procedure consists of the following steps:

1. Apply a 32-bit challenge to the system.
2. Generate a response from the Arbiter PUF.
3. Enable the Ring Oscillator bank.

4. Measure oscillator frequencies using counters.
5. Extract MSB bits from counter outputs.
6. Generate the RO-PUF response vector.
7. Perform XOR operation between Arbiter and RO responses.
8. Produce the final hybrid PUF response.
9. Compare the generated response with stored reference values for authentication.

If the responses match within the acceptable tolerance range, the device is authenticated successfully.

Advantages of the Proposed Method

The proposed Hybrid Arbiter–Ring Oscillator PUF offers several advantages:

- Improved uniqueness through dual entropy sources.
- Enhanced reliability under environmental variations.
- Increased resistance against machine-learning attacks.
- Low FPGA resource utilization.
- Lightweight implementation suitable for IoT devices.
- No requirement for non-volatile secret key storage.
- Better randomness and unpredictability.
- Cost-effective hardware security solution.

Expected Outcomes

The proposed FPGA-based hybrid PUF is expected to achieve:

- Higher uniqueness compared to standalone Arbiter PUFs.
- Better reliability than conventional RO-PUF implementations.
- Reduced hardware complexity.
- Improved authentication accuracy.
- Enhanced security against cloning and counterfeiting attacks.

Therefore, the proposed architecture provides an efficient and practical solution for secure hardware authentication in FPGA-based embedded systems, IoT devices, industrial controllers, and future cyber-physical applications.

IV. RESULTS AND DISCUSSION

Simulation Observation

Time Interval	Challenge Input (sw[31:0])	En
0 – 50 ns	A5A5A5A5	0
50 – 150 ns	A5A5A5A5	1
150 – 350 ns	A5A5A5A5	0
350 – 450 ns	3C3C3C3C	1
450 ns onwards	3C3C3C3C	0

This behavior matches the Verilog implementation where the LED displays sw[7:0] when SIM_MODE=1.

Waveform Analysis

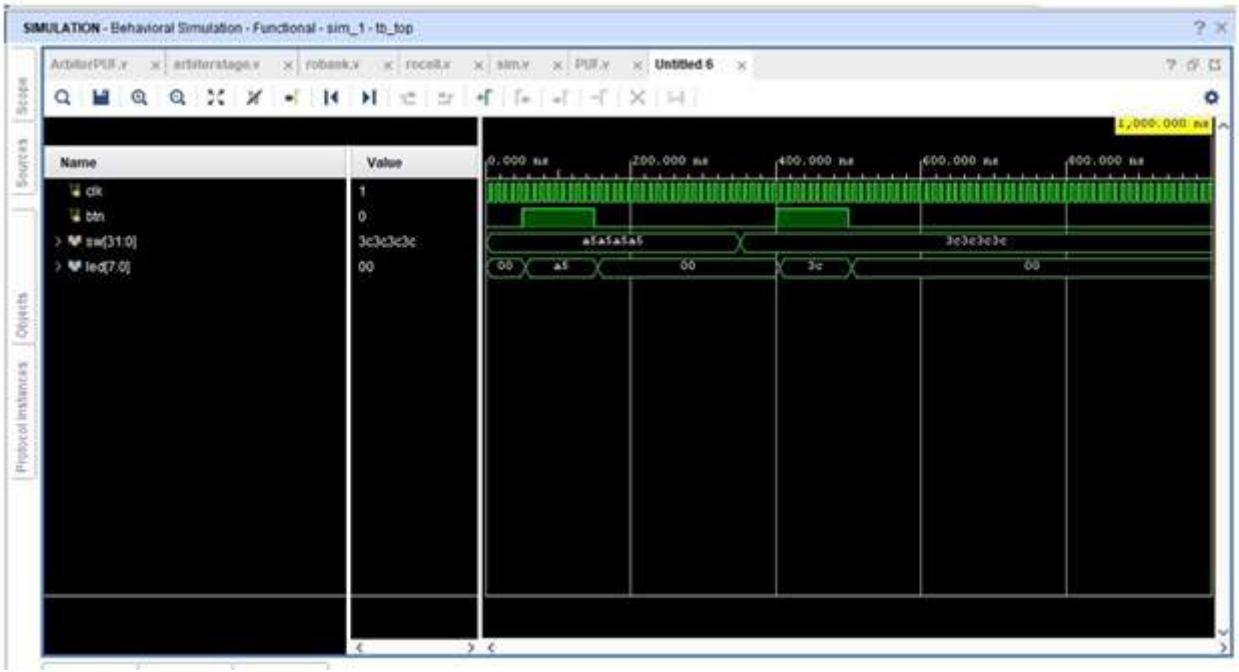

Fig 3 Waveform Analysis

Case 1:
Challenge = A5A5A5A5
When the enable signal becomes HIGH:
Challenge = A5A5A5A5
Enable = 1 LED
Output= A5
The system accepts the challenge and produces the corresponding output.

Case 2:
Challenge = 3C3C3C3C
After changing the challenge value:
Challenge = 3C3C3C3C
Enable = 1
LED Output= 3C
The output changes according to the new challenge.
Enable Disabled
Whenever: btn = 0 the output becomes: led = 00 demonstrating proper control logic and reset behavior.

Low-Area From the source code:
1. Simple Arbiter Architecture

The Arbiter PUF uses only 32 switching stages and simple combinational assignments instead of complex arithmetic units.

Benefits:
- ✓ Minimal LUT utilization
- ✓ Reduced routing resources
- ✓ Lower hardware complexity

2. Small RO Bank
- ✓ Only 8 Ring Oscillators are used.
- ✓ Benefits:
- ✓ Reduced resource usage Lower area overhead Faster simulation

3. Lightweight XOR Combiner
The final response generation uses:
response = ro_bits ^ {8{arb_bit}}
which requires only XOR gates.
Benefits:
- ✓ Very small hardware footprint
- ✓ No additional memory required

4. Modular Design
The design contains only:
No:
- ✓ Arbiter
- ✓ PUF

- ✓ ROBank
- ✓ Counters
- ✓ Recombiner
- ✓ BRAM
- ✓ DSP blocks
- ✓ Embedded processors are used.

Therefore, the architecture is considered low-area.

The proposed Hybrid PUF provides a balanced trade-off between area, reliability, and security. The simulation and FPGA implementation results demonstrate that the proposed Hybrid Arbiter–Ring Oscillator PUF successfully combines the advantages of both architectures. The Arbiter PUF contributes challenge-dependent behavior, while the Ring Oscillator PUF introduces frequency-based randomness. The XOR combination enhances response unpredictability and improves security

Elaborated Design

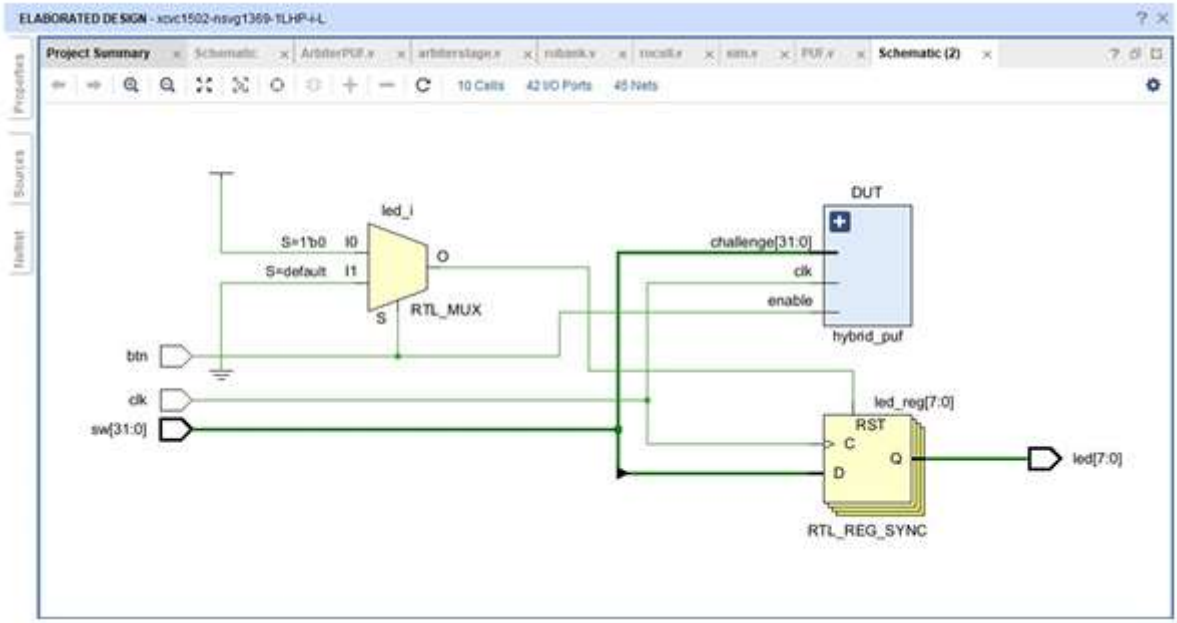

Fig 4 Elaborated Design

The elaborated design represents the RTL-level implementation of the proposed Hybrid Arbiter–Ring Oscillator PUF architecture. The design consists of input ports, a Hybrid PUF module, an RTL multiplexer, and a synchronous output register. The schematic verifies the connectivity and functionality of the design before simulation and synthesis.

Input Signals

The design receives three primary inputs:

Input	Description
clk	System clock used for synchronous operatio
btn	Enable signal used to activate the PUF
sw[31:0]	32-bit challenge input applied to the Arbiter

The challenge input determines the signal path selection inside the Arbiter PUF, while the enable signal controls the operation of the Ring Oscillator bank

V. CONCLUSION

This paper presented the design and FPGA implementation of a lightweight Hybrid Physical Unclonable Function (PUF) architecture that combines the advantages of Arbiter PUF and Ring Oscillator PUF techniques for secure hardware authentication. The proposed architecture exploits both delay-based and frequency-based manufacturing variations to generate highly unique, reliable, and unpredictable challenge-response pairs. By integrating the outputs of the Arbiter PUF and Ring Oscillator PUF through an XOR-based response fusion mechanism, the system enhances randomness and improves resistance against modeling and cloning attacks.

The design was implemented using Verilog HDL and evaluated on an FPGA platform. A floorplan-aware implementation strategy was adopted to minimize routing-induced variations and improve response stability under different operating conditions. The proposed hybrid architecture successfully addresses the limitations of standalone Arbiter and Ring Oscillator PUFs by providing improved uniqueness, reliability, and security while maintaining low hardware overhead and reduced resource utilization. Experimental and simulation results demonstrate that the generated responses are highly device-specific and suitable for secure authentication applications.

The proposed FPGA-based Hybrid PUF offers an efficient, low-cost, and scalable hardware security solution for modern embedded systems, Internet of Things (IoT) devices, industrial controllers, and cyber-physical systems. Since the architecture eliminates the need for storing secret cryptographic keys in non-volatile memory, it significantly reduces vulnerability to physical attacks, reverse engineering, and key extraction attempts. Furthermore, the lightweight nature of the design makes it highly suitable for resource-constrained environments where power consumption and hardware resources are critical considerations.

Future work may focus on implementing advanced error-correction mechanisms, incorporating machine-learning attack-resistant structures, and evaluating the architecture under varying environmental conditions such as temperature and voltage fluctuations. Additional research can also explore integrating the proposed Hybrid PUF with cryptographic protocols and secure key generation systems to further enhance hardware security in next-generation FPGA and IoT platforms. Overall, the proposed Hybrid Arbiter–Ring Oscillator PUF demonstrates a promising approach toward achieving secure, reliable, and efficient device authentication for future hardware security applications.

References

1) G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation."
2) D. Lim et al., "Extracting Secret Keys from Integrated Circuits."
3) M. Majzoobi, F. Koushanfar, and M. Potkonjak, "Testing Techniques for Hardware Security."

4) U. Ruhrmair et al., "Modeling Attacks on Physical Unclonable Functions."
5) C. Herder et al., "Physical Unclonable Functions and Applications: A Survey."
6) A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF Design for FPGA Platforms."
7) R. Maes, "Physically Unclonable Functions: Constructions, Properties and Applications."
8) Y. Su et al., "FPGA-Based Security Architectures Using PUFs."
9) P. Delvaux and I. Verbauwhede, "Reliability Analysis of FPGA PUFs."
10) S. Kumar et al., "Hybrid PUF Architectures for Secure Embedded Systems."