A 4.447 mW at 100 MHz and 49.62% Uniqueness XNOR–XOR RO PUF ASIC Using 180-nm CMOS Process for IoT Security Applications

Chua-Chin Wang, *Senior Member, IEEE*, Pradyumna Vellanki, Jian-Jie Chen, and Ralph B. Gerard Sangalang, *Senior Member, IEEE*

***Abstract*—Physical unclonable functions (PUFs) are increasingly recognized as a key technology for enhancing hardware and the Internet of Things (IoT) security. The IoT devices are often plagued by weak security measures, making them susceptible to various external threats. To address these vulnerabilities, robust and reliable security solutions are critical. This study introduces a highly reliable and low-power PUF application-specific integrated circuit (ASIC) design specifically designed for the IoT security applications. Initially, the proposed design is deployed on a Xilinx ZYNQ 7000 field-programmable gate array (FPGA) board operating at 100 MHz and later designed and fabricated using the Cadence Innovus in the 180-nm CMOS process on silicon. This work presents and evaluates a novel XNOR–XOR ring oscillator (RO) PUF with a configurable frequency. The design's performance is analyzed using statistical metrics, including reliability, uniqueness, and uniformity. The XNOR–XOR RO PUF ASIC demonstrates max reliability of 91.92%, a uniqueness of 49.62%, and a uniformity of 50.19% on silicon.**

***Index Terms*—Application-specific integrated circuit (ASIC), Internet of Things (IoT), physical unclonable functions (PUFs), reliability, uniformity, uniqueness, XNOR–XOR ring oscillator (RO) PUF.**

I. Introduction

THE Internet of Things (IoT) and mobile devices are revolutionizing the way we interact with technology, connecting billions of devices into a dynamic ecosystem. However, this interconnectedness introduces significant security challenges, as devices often operate in untrusted environments where adversaries may have physical access. Robust, efficient security solutions tailored to resource-constrained devices are essential.

Conventional methods rely on nonvolatile memory [e.g., read-only memory (ROM), electrically erasable programmable read-only (EEPROM), or battery-backed static random access memory (SRAM)] to store authentication keys [1]. While effective, these methods are costly in terms of power consumption, design complexity, and manufacturing. They are also vulnerable to invasive and noninvasive attacks, requiring additional tamper-prevention hardware that increases cost and energy consumption [2].

A promising alternative physical unclonable functions (PUFs) address these limitations by embedding security directly into the hardware, deriving unique identifiers ("fingerprints") from inherent manufacturing variations in integrated circuits (ICs). These variations result in unique and unclonable responses to input challenges, offering several key advantages.

1) *Cost and Power Efficiency:* PUFs use simple digital circuits that require less power and area compared to traditional nonvolatile and volatile memory solutions.
2) *Increased Security:* The secret exists only when the device is powered on, complicating physical attacks. Any tampering alters the physical characteristics, invalidating the derived secret.
3) *Scalability:* PUFs eliminate the need for additional expensive cryptographic hardware, such as secure hash algorithms or encryption modules.

PUFs provide a foundation for secure key storage, strong authentication, and anticounterfeiting. They enable hardware-based security that is resistant to reverse engineering and duplication [3], [4]. For example, PUFs can generate unique device keys for authentication protocols, enhancing trust across devices while reducing reliance on vulnerable software-based repositories.

PUFs can be enhanced by integrating with technologies like machine learning (ML), further strengthening security systems, as illustrated in Fig. 1. By leveraging hardware-based randomness, PUFs offer scalable, efficient, and cost-effective solutions to the growing security needs of IoT and mobile devices.

The Internet of Underwater Things (IoUT) is an emerging communication ecosystem developed for connecting underwater objects in maritime and underwater environments

Received 13 February 2025; revised 12 April 2025; accepted 19 April 2025. This work was supported in part by the National Science and Technology Council (NSTC) of Taiwan under Grant 113-2218-E-110-010, Grant 112-2221-E-110-063-MY3, Grant 112-2218-E-110-005, and Grant 113-2923-E-110-001. *(Corresponding author: Chua-Chin Wang.)*

Chua-Chin Wang is with the Department of Electrical Engineering, National Sun Yat-sen University (NSYSU), Kaohsiung 80424, Taiwan, also with the Institute of Undersea Technology and the Institute of Integrated Circuit Design, National Sun Yat-sen University, Kaohsiung 80424, Taiwan, also with the Department of Electronics and Communication Engineering, Presidency University, Bengaluru 560064, India, also with the Department of Electronics and Communication Engineering, SRM Institute of Science and Technology, Chennai 603203, India, and also with the Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai 600062, India (e-mail: ccwang@ee.nsysu.edu.tw).

Pradyumna Vellanki and Jian-Jie Chen are with the Department of Electrical Engineering, National Sun Yat-sen University, Kaohsiung 80424, Taiwan (e-mail: pradyumna@vlsi.ee.nsysu.edu.tw; ko7569647@vlsi.ee.nsysu.edu.tw).

Ralph Gerard B. Sangalang is with the Department of Electronics Engineering and the Electronic Systems Research Center, Batangas State University, The National Engineering University, Alangilan, Batangas City 4200, Philippines (e-mail: ralphgerard.sangalang@g.batstate-u.edu.ph).

Digital Object Identifier 10.1109/TVLSI.2025.3563386

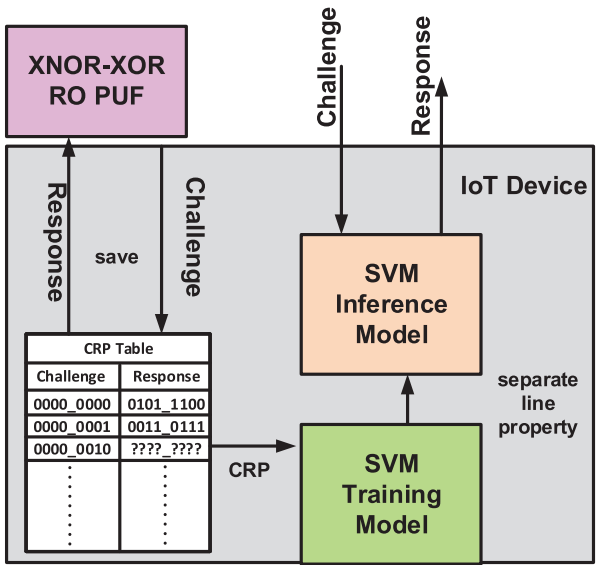

Fig. 1. PUF with ML.

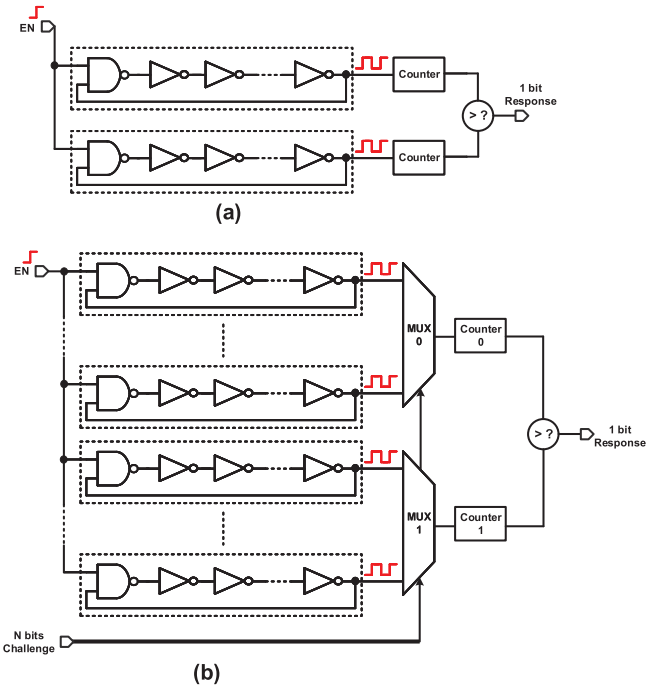

Fig. 2. Conventional RO PUF (a) without challenge code and (b) with N-bit challenge [9].

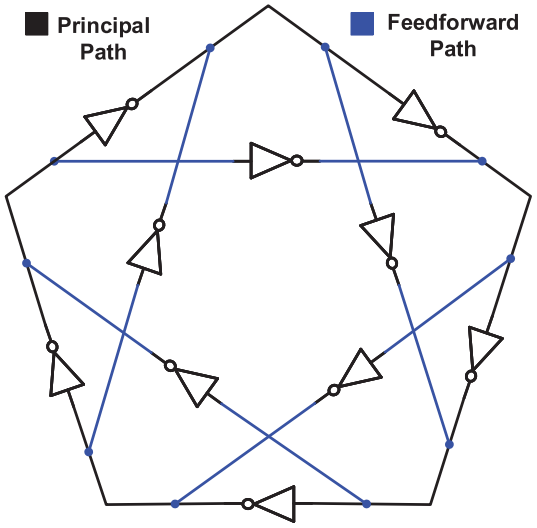

Fig. 3. Five-stage feedforward RO PUF [10].

[5]. Remotely operated vehicles (ROVs) and autonomous underwater vehicles (AUVs) are used to explore, analyze, and interact with marine environments. These vehicles rely on IoT-enabled sensors and real-time data exchange to enhance navigation, mapping, and environmental monitoring. However, secure communication is crucial, especially in security-sensitive applications such as underwater surveillance and defense-related operations. PUFs can play a key role in enhancing security by generating unique, tamper-resistant cryptographic keys. By leveraging hardware-based randomness, PUFs enable secure authentication and prevent cyber threats, ensuring reliable and protected data transmission between AUVs and surface stations or other underwater vehicles. Integrating PUFs into AUVs strengthens IoT-based maritime security, mitigating risks such as data interception and spoofing attacks [6].

This article introduces a novel ring oscillator (RO) PUF architecture that combines XNOR and XOR gates, allowing external input control over the oscillation frequency. The architecture has been first simulated, implemented on a field-programmable gate array (FPGA), and fabricated as an IC on silicon, following a typical procedure of physical design using the Taiwan Semiconductor Manufacturing Company (TSMC) 180-nm CMOS process, followed by measurements to evaluate its functionality and performance. This article is organized into the following sections.

1) *Section II:* This section reviews existing RO PUF designs and related prior work.
2) *Section III:* The details of the new PUF architecture are presented, including its design principles and features.
3) *Section IV:* This section presents the experimental setup, including the FPGA implementation, IC measurement, and statistical analysis of both outcomes. The evaluation focuses on key performance metrics such as uniqueness, reliability, and uniformity to assess the effectiveness of the proposed XNOR–XOR RO PUF in both FPGA and application-specific IC (ASIC).
4) *Section V:* This section presents the conclusions drawn from the research findings.

II. Related Works

Numerous PUFs have been proposed and successfully implemented, broadly classified into memory-based and delay-based PUFs. SRAM PUFs [7], a memory-based type, rely on SRAM startup behavior but produce limited challenge-response pairs (CRPs), making them ideal for identification rather than authentication. Delay-based PUFs, such as arbiter PUF (APUF) and RO PUF, offer more CRPs. An n-stage

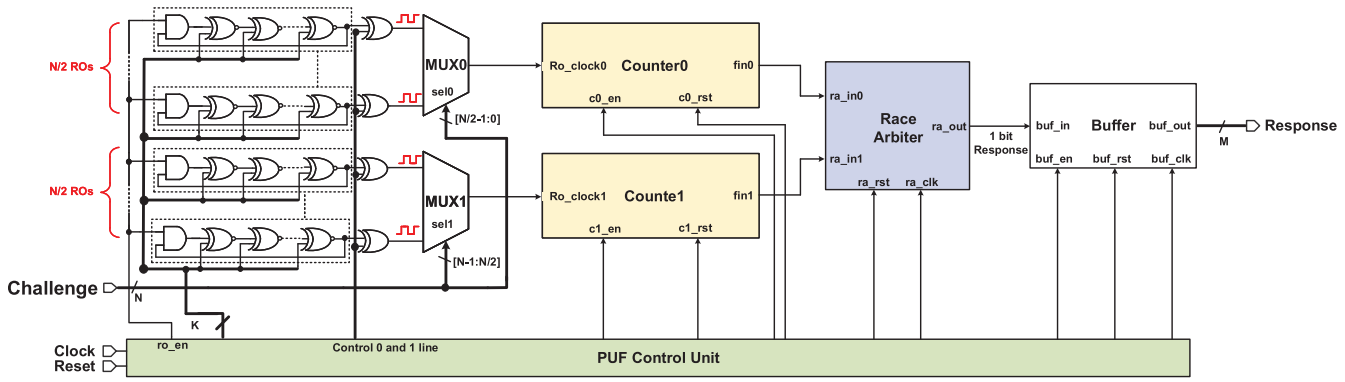

Fig. 4. Proposed XNOR–XOR RO PUF architecture.

APUF [8] uses n pairs of multiplexers (MUXs) to route signals based on challenge bits, with an arbiter measuring delay differences to generate responses. It provides many CRPs in a compact design but has low uniqueness, which can limit their robustness against certain attacks. On the other hand, RO PUFs are known for their superior uniqueness and resilience. By comparing the oscillation frequencies of ROs, these PUFs generate responses that are highly device-specific and harder to predict. As a result, RO PUFs are often preferred in applications requiring strong authentication.

A 1-bit RO PUF, as illustrated in Fig. 2(a), provides a compelling example. This design features two ROs that function as clock sources for subsequent blocks, specifically the counters. Though the ROs are designed with an identical number of odd inverter stages, their output frequencies differ due to inherent process variations in the individual devices. An arbiter is then used to compare the frequencies, selecting the faster RO and generating a response bit as the output. A MUX is integrated between the ROs and counters to enhance the design by enabling the use of a greater number of unique frequencies [9]. The challenge bits serve as selection inputs for the MUXs, allowing the system to dynamically choose between ROs based on the given challenge code. Once the challenge code is received, the counters are activated for a fixed duration. The values from the counters are then forwarded to the arbiter, which compares them to determine the final output, as shown in Fig. 2(b). This approach improves flexibility and increases the entropy of the PUF.

A feedforward RO-based PUF is proposed in [10], with an example of a five-stage feedforward RO (indicated in blue color), as illustrated in Fig. 3. Compared to conventional RO PUFs, this design achieves a higher frequency and primarily relies on the strength of the feedforward mechanism. The feedforward path also increases variations in the RO frequency, enhancing the randomness of the output.

However, implementing this design on an FPGA introduces several challenges. First, the shared paths between the principal path (indicated in black color) and the feedforward path can lead to synthesis errors. Second, the feedforward path inverters bypass two inverters in the primary path, which may result in logic errors and oscillation failures. These issues could compromise the reliability and security of the system.

In this work, the XNOR–XOR RO PUF architecture uses a modified control method. An XNOR gate is introduced as the oscillator, while additional control signal lines are incorporated to enable different oscillation frequencies.

III. Proposed XNOR–XOR Ro PUF

The architecture of the proposed XNOR–XOR RO PUF is depicted in Fig. 4. It consists of several key components that work together to achieve its functionality.

1) XNOR–XOR *ROs and MUXs (MUX0 and MUX1):* A set of N oscillators designed to produce varying frequencies based on their configurations, where N is the number of challenge bits.
   When a challenge is given, the MUXs select two frequencies that act as clock signals for the counters, triggering the counting process.
2) *Counters (Counter0 and Counter1):* These counters record the oscillation cycles of the chosen ROs.
3) *Race Arbiter:* It compares the output from the two oscillators to generate a response.
4) *Buffer:* The buffer collects and stores a series of 0 or 1 response values, ensuring controlled data handling and synchronization with the system's operations.
5) *PUF Control Unit:* It oversees the system's operations, ensuring smooth coordination between all components.

The overall operation of the XNOR–XOR RO PUF is shown using the flowchart in Fig. 5. This structured and modular design enhances the reliability and performance of the PUF, making it an effective solution for securing IoT devices.

A. XNOR–XOR RO and Multiplexers (MUX0 and MUX1)

The schematic of an individual RO is illustrated in Fig. 6. It incorporates XNOR gates that can function as either inverters or buffers, depending on the configuration of inputs S_0–S_n (as shown in Fig. 6). This configuration directly influences the oscillator's output frequency. An XOR gate is positioned at the end of the RO to ensure an odd number of stages, satisfying the Barkhausen criterion, which guarantees sustained oscillations [11]. When a challenge is provided, it serves as the selection lines for the MUXs, which choose two distinct frequencies and pass them as inputs to the counters. These outputs from

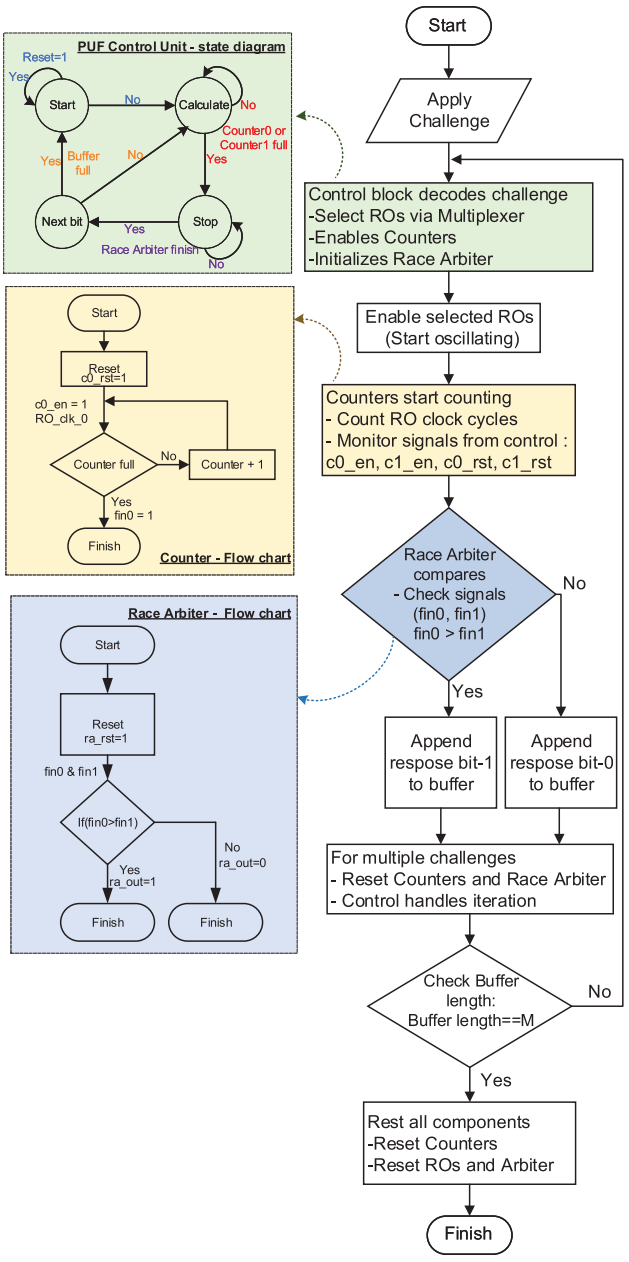

Fig. 5. Flowchart of the proposed XNOR–XOR RO PUF.

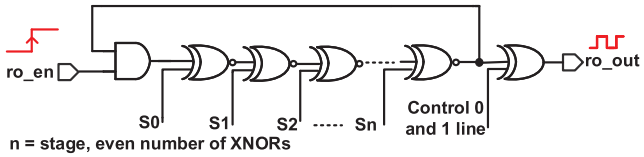

Fig. 6. XNOR–XOR RO.

the MUXs serve as clock signals for the counters, initiating the counting process.

B. Counters (Counter0 and Counter1)

Counter0 and Counter1 have the same architecture, with Counter0 used here as an example. The control flow of Counter0 is illustrated in Fig. 5 (box with yellow background).

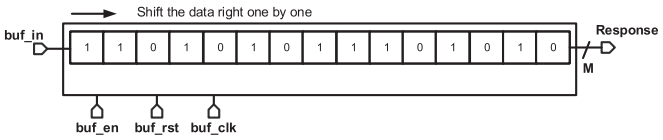

Fig. 7. Buffer register.

When the enable signal c0_en is set to 1, Counter0 begins operation. Its input frequency signal, Ro_clock0, originates from the output of the XNOR–XOR RO selected by MUX0. Each RO operates at a unique frequency, leading to distinct counting results in Counter0 and Counter1. At the end of a counting cycle, the reset signal c0_rst resets Counter0 to zero. When one of the counters reaches a predetermined value, the fin0 signal is triggered and outputs a 1 to the Race Arbiter, enabling it to compare the timing and speeds of the fin0 and fin1 signals. This mechanism plays a critical role in distinguishing the challenge-response behavior of the PUF.

C. Race Arbiter

The control flow of the Race Arbiter is depicted in Fig. 5 (box with blue background). Upon receiving the fin0 and fin1 signals from the counters, the Race Arbiter initiates a speed comparison if either fin0 or fin1 is set to 1. If fin0 reaches its target before fin1, the Race Arbiter outputs a 1-bit result of 1 on ra_out. Conversely, if fin1 reaches its target first, the output ra_out is set to 0. This comparison determines the relative speed of the two counters and forms the basis for the PUF's response generation.

D. Buffer Register

The Buffer's circuit architecture is depicted in Fig. 7. It accumulates a sequence of response values, either 0 or 1, until the designed register reaches its specified length. The control circuit manages the buffer's operations through signals buf_en, buf_rst, and buf_clk, which determine its activation, initial reset, and input frequency clock, respectively. This configuration ensures synchronized data collection and storage within the PUF system.

E. PUF Control Unit

The state diagram for the PUF control unit is shown in Fig. 5 (box with green background). The control unit of the proposed XNOR–XOR RO PUF is designed as a finite state machine (FSM) to coordinate the operation of all submodules involved in the challenge-response process. The major benefit of an FSM ASIC is that it consumes much less power compared with conventional CPU-based controllers. At the start of the process, a reset signal is activated to initialize the states of the counters, Race Arbiter, and buffer to zero.

When a challenge is given, the state machine activates, enabling the subcircuits. The XNOR–XOR RO and counters are then activated, and the scrambled challenge is fed into the MUX to select two XNOR–XOR ROs to connect to the counters. Due to variations in the frequencies of the selected

ROs, the counters will operate at different rates. When one of the counters reaches a specified value, it outputs a signal ("1") to the Race Arbiter for a speed comparison.

The result of the comparison is then sent to the buffer, which is activated to store the result. Afterward, the states of the counters and the Race Arbiter are reset to zero, repeating the process in a loop. An external counter is incorporated to determine the number of iterations needed to fill the buffer to its required length. Once the process is complete, the counters, Race Arbiter, and other subcircuits return to their initial states.

The control unit FSM progresses through the following states.

1) *Start State:* The purpose of this state is to ensure a consistent starting condition for all modules.
   a) If Reset = 1, the FSM remains in the start state. All internal components including the counters, Race Arbiter, and buffer are reset to their initial states.
   b) If Reset = 0, the FSM transitions to the calculate state by receiving the challenge and configuring the system accordingly.
2) *Calculate State:* The purpose of this state is to activate the ROs and initiate the frequency-based counting using counters.
   a) If neither counter (Counter0 or Counter1) reaches a predefined threshold, the FSM stays in this state.
   b) Once either counter reaches the predefined threshold, the FSM transitions to the stop state.
3) *Stop State:* The purpose of this state is to evaluate the speed of oscillators and generate a 1-bit response.
   a) Upon threshold completion by one counter (signaled by fin0 or fin1), the Race Arbiter is triggered and it determines which counter finished first.
   b) If fin0 arrives first, then the response bit is "1." If fin1 arrives first, then the response bit is "0." Once the response bit is generated by the Race Arbiter, the FSM moves to the next state.
4) *Next Bit State:* The purpose of this state is to store the computed response bit.
   a) The 1-bit output from the Race Arbiter is written into the buffer.
   b) If the buffer is not filled with the full response, the FSM loops back to the calculate state to continue processing the next bit. If the buffer is filled with the full response, the FSM transitions back to the start state for a new challenge.

IV. Experimental Setup and Results

To evaluate the PUF output quality, it is important to evaluate its statistical properties [8], [12].

1) *Uniqueness:* It quantifies the diversity in responses generated by various FPGA boards programmed with a PUF or by different PUF chips when subjected to the same set of challenges. If R_i and R_j denote the n-bit responses from the ith and jth FPGA board programmed with PUF or PUF chips, respectively, for the same challenge, then the uniqueness ($\mathrm{HD}_{\mathrm{inter}}$) is calculated as the average inter-Hamming distance (inter-HD) among C devices. This can be expressed using the following equation:

$$\mathrm{HD}_{\mathrm{inter}} = \frac{2}{C(C-1)} \sum_{i=1}^{C-1} \sum_{j=i+1}^{C} \frac{\mathrm{HD}\left(R_i, R_j\right)}{n} \times 100\%. \quad (1)$$

2) *Reliability:* It evaluates how consistently a PUF design can reproduce the same response under varying operating conditions, such as changes in ambient temperature or supply voltage, over time for a given challenge. For the ith FPGA board programmed with PUF or PUF chip, the average intra-Hamming distance (intra-HD) is calculated using (2). In this case, R_i represents the reference response of the ith device, R_i, r is the rth sample of response, and x denotes the number of responses generated for the same set of challenges. The overall reliability is determined by subtracting the intra-HD percentage from 100% by the following equation:

$$\mathrm{HD}_{\mathrm{intra}} = \frac{1}{m} \sum_{t=1}^{m} \frac{\mathrm{HD}\left(R_i, R_{i,r}\right)}{x} \times 100\% \quad (2)$$

$$\mathrm{Reliability} = 100\% - \mathrm{HD}_{\mathrm{intra}}. \quad (3)$$

3) *Uniformity:* The uniformity metric determines how uniform the proportion of 0's and 1's is in the PUF response and is calculated by the following equation. x denotes the number of responses generated for the same set of challenges

$$U = \frac{1}{x} \sum_{k=1}^{x} R[k] \times 100\%. \quad (4)$$

A. FPGA Implementation and Analysis

The proposed XNOR–XOR RO PUF is first implemented on a Xilinx ZYNQ 7000 FPGA board (using 28-nm technology), as shown in Fig. 8. As discussed earlier, the output of the FPGA-based XNOR–XOR RO PUF is analyzed statistically using (1)–(4) to evaluate critical parameters such as uniqueness, reliability, and uniformity. The experimental results are further processed and analyzed using MATLAB based on these equations.

1) *Uniqueness Analysis:* To evaluate the uniqueness of the XNOR–XOR RO PUF on FPGA boards under identical environmental conditions and the same set of challenges, (1) is utilized. The following parameters are considered: $C = 60$, whereas we used five FPGA boards and 12 arrangements of the same design to ensure a fair comparison.
   The calculated average inter-HD for the XNOR–XOR RO PUF is 49.90%, indicating strong uniqueness properties. The histogram illustrating the uniqueness distribution of PUF responses is presented in Fig. 9.
2) *Reliability Analysis:* To assess the reliability of the XNOR–XOR RO PUF under varying environmental conditions (e.g., changes in supply voltage and temperature) while keeping the challenge input constant, (2) and (3) are applied. The following experimental parameters are considered: $x = 3000$ and $m = 10$.

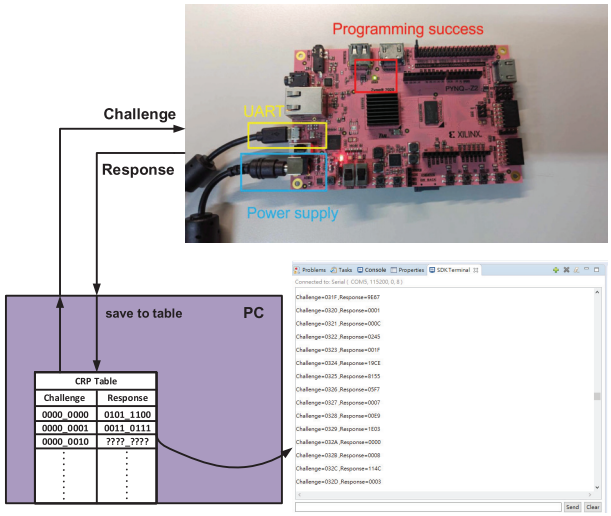

Fig. 8. Experiment conducted with FPGA.

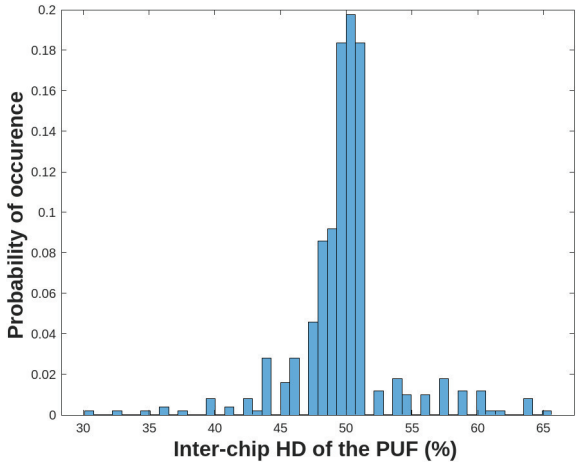

Fig. 9. Inter-HD histogram, mean of 49.90%.

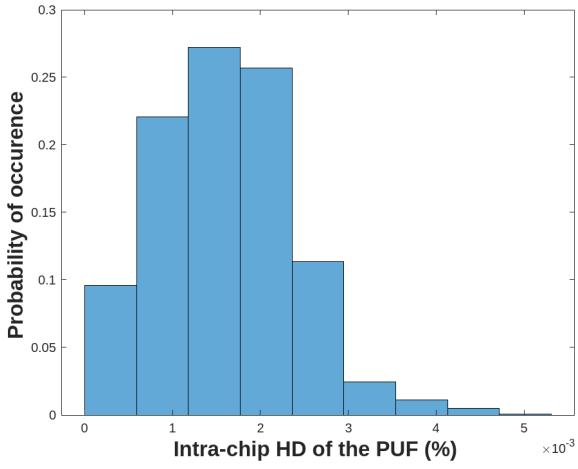

Fig. 10. Intra-HD histogram, mean of 0.14% and reliability = 99.86%.

The computed intra-HD has a central tendency of 0.14%, corresponding to a reliability of 99.86%. The histogram of intra-HD values is illustrated in Fig. 10.

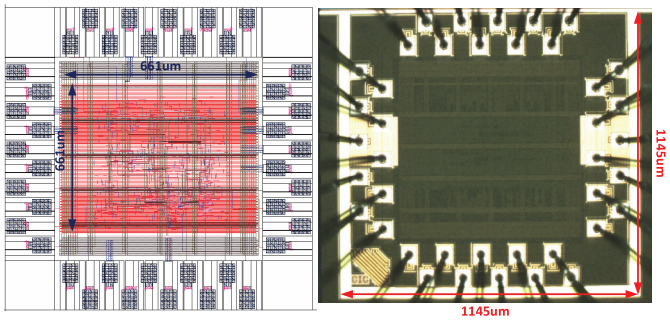

Fig. 11. Layout and die photograph of the proposed PUF ASIC.

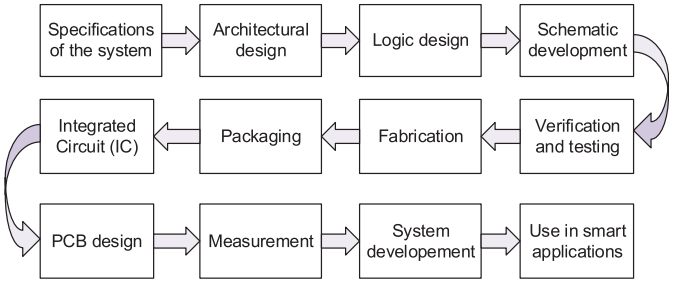

Fig. 12. Chain of semiconductor production for ICs, from design to application [13].

TABLE I

EXPERIMENTAL RESULTS USING THE XILINX ZYNQ XC7Z020 FPGA

	Uniqueness	Reliability	Uniformity
RO PUF	49.94%	94.53%	48.73%
NOR PUF	50.51%	92.13%	47.17%
XOR PUF	53.33%	96.47%	48.80%
XNOR PUF	48.08%	98.07%	73.07%
XNOR-XOR RO PUF	49.90%	99.86%	67.30%

TABLE II

POWER CONSUMPTION AT VARIOUS PVT CORNERS

S.No.	PVT Corner	Power (mW)
1	TT, VDD, 25°C	3.09
2	FF, VDD+10%, 25°C	4.33
3	FS, VDD-10%, 50°C	4.64
4	SF, VDD+10%, 0°C	2.16
5	SS, VDD, 75°C	5.56

3) *Uniformity Analysis:* The average uniformity of the XNOR–XOR RO PUF during the experiment is computed using (4), resulting in a measured value of 67.3%, where $x = 3000$.

Table I provides a summary of the experiments conducted on various PUFs using the same FPGA boards. The results indicate that the proposed XNOR–XOR RO PUF demonstrates the highest reliability, achieving an average of 99.86%. Its uniqueness value is only 0.04% lower compared to the conventional RO PUF.

Fig. 9 presents a histogram illustrating the uniqueness of the PUF responses obtained during the experiments. The calculated average inter-HD for the proposed XNOR–XOR RO PUF is 49.90%. Similarly, Fig. 10 shows a histogram of

TABLE III
PERFORMANCE COMPARISON WITH PREVIOUS FPGA-BASED PUF

	IEEE Access [14]	ICET [15]	ISCAS [16]	MICPRO [17]	Ours	
Year	2020	2021	2022	2024	2025	
Design	HC-RO	XOR RO	ERRO	Novel CRO-PUF	XNOR-XOR RO	
FPGA/ASIC	Artix-7	Virtex-6	Spartan-7	Artix-7	ZYNQ 7000	ASIC
Process (nm)	28	28	28	-	28	180
VDD (V)	1	1	1	-	1	1.8
No. of RO	32	256	64	64	512	256
Frequency (MHz)	∼	100	100	∼	100	100
Power (mW)	∼	∼	∼	206	8 @ 100 MHz	4.447 @ 100 MHz
Normalized Power	∼	∼	∼	∼	4	1.372
Uniqueness (%)	46.76	48.438	49.998	50.01	49.90	49.62
Reliability (%)	98.22	98.326	98.61	98.33	99.86	91.927
Uniformity (%)	50.36	∼	∼	49.45	67.30	50.19

Normalized Power = Power / [(No. of ROs / No. of ROs in ASIC) × VDD × VDD]

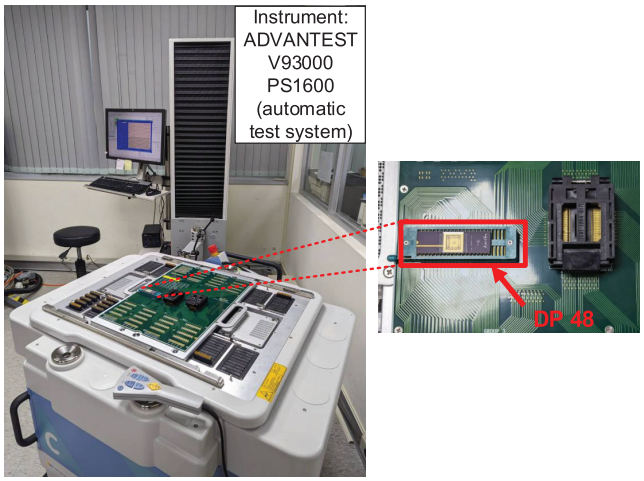

Fig. 13. Measurement setup.

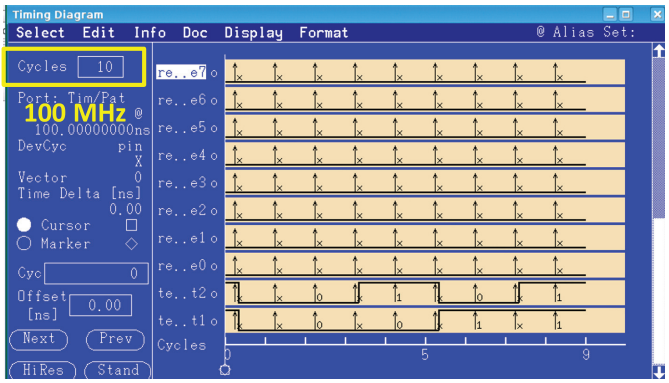

Fig. 14. Timing waveform of selected DFFs.

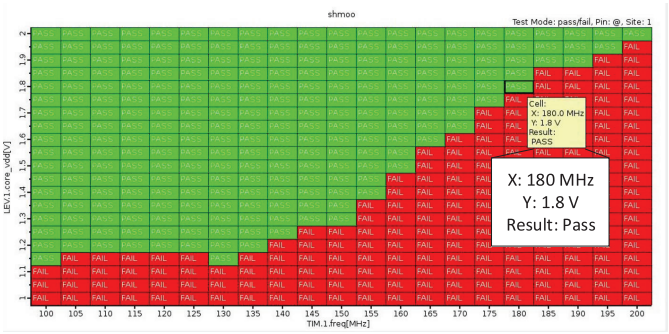

Fig. 15. Shmoo plot.

the intra-HD, with a computed central tendency of 0.14%, corresponding to a reliability of 99.86%. At 100-MHz clock frequency and 4.023-ns slack time, it consumed 8 mW of power.

B. ASIC Fabrication and Measurement

Notably, the FPGA experiment is meant to prove the predicted function of the proposed PUF design. However, it consumes too much power, which is not possible in IoT or IoUT applications. Thus, we realized the PUF using ASIC approach. The proposed design is fabricated as an ASIC on silicon, following a typical procedure of physical design using the Cadence Innovu TSMC 180-nm CMOS process. The fabricated IC occupies an area of 1145 × 1145 μm and the core area is 661 × 661 μm. The layout and die photograph of the IC are depicted in Fig. 11. A high-level overview of the semiconductor production chain for ICs, from design to application, is presented in Fig. 12. In postlayout simulations, the power consumption at various process, voltage, and temperature (PVT) corners is shown in Table II and the response time of the PUF for an 8-bit response at 100 MHz is 1.1 μs.

1) Measurement Setup and Initial Validation: The IC is tested using the ADVANTEST V93000 PS1600 automatic test system, with the measurement setup shown in Fig. 13. The initial validation of the PUF device is performed by testing the D-flip-flop (DFF) under Shmoo analysis across a range of supply voltages and frequencies. Fig. 14 presents the timing waveform, while Fig. 15 demonstrates that the device functions correctly at a 1.8-V supply voltage and supports operation up to 180 MHz.

2) Statistical Analysis of the Fabricated XNOR–XOR RO PUF: As discussed previously, the output of the fabricated XNOR–XOR RO PUF is statistically analyzed using (1)–(4) to evaluate key performance metrics, including uniqueness, reliability, and uniformity. These metrics are computed based on the experimental data collected during IC testing and are further processed and analyzed using MATLAB for com-

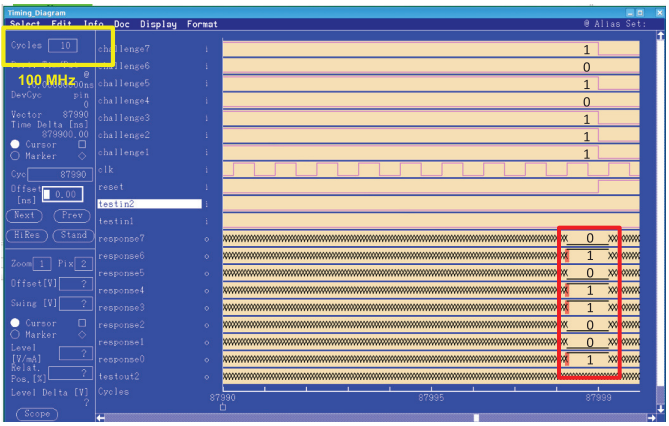

Fig. 16. 11111111 response generated by PUF to the given challenge 11010110.

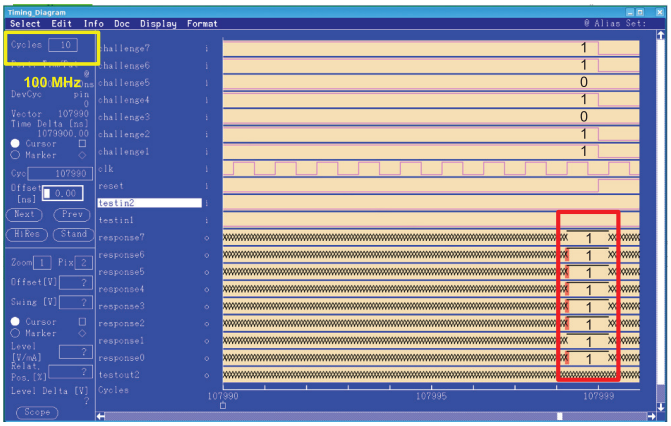

Fig. 17. 01011100 response generated by PUF to the given challenge 11110001.

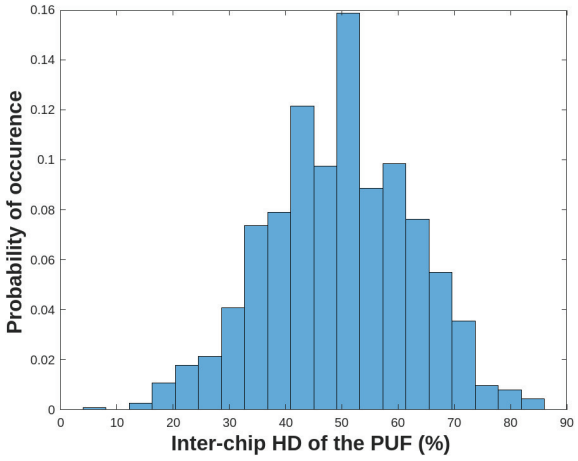

Fig. 18. Inter-HD histogram, mean = 49.62%.

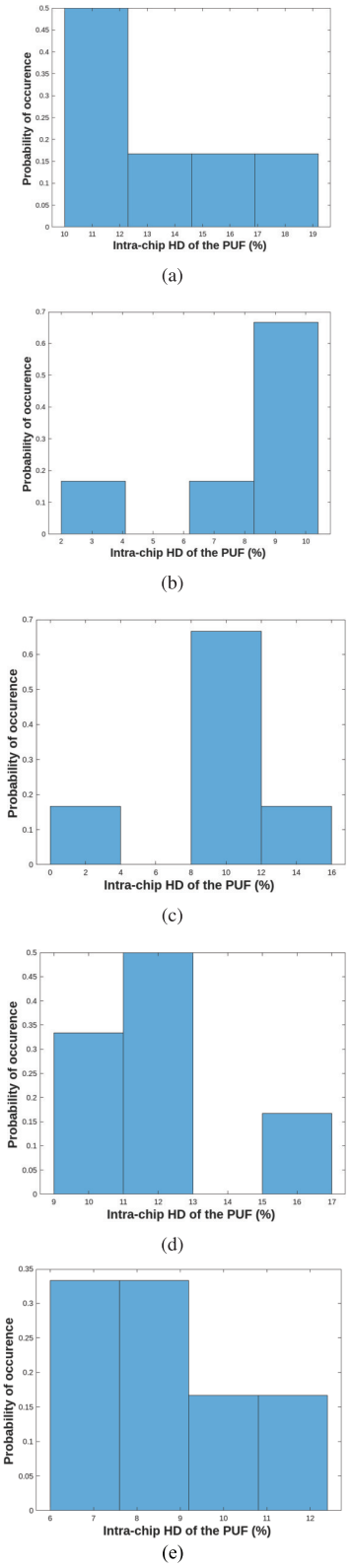

Fig. 19. Five chips measurement intra-HD histogram. (a) Chip1, 13.0371%. (b) Chip2, 8.0729%. (c) Chip3, 9.5866%. (d) Chip4, 12.3861%. (e) Chip5, 8.8216%.

prehensive evaluation. The output waveforms corresponding to different challenge inputs are shown in Figs. 16 and 17. Specifically, when the challenge 11010110 is applied to the XNOR–XOR RO PUF, it generates the response 11111111. Similarly, when the challenge 11110001 is given to the XNOR–XOR RO PUF, it produces the response 01011100.

1) *Uniqueness Analysis:* The uniqueness of the XNOR–XOR RO PUF, when fabricated as an IC and tested under identical environmental conditions using the same challenge, is analyzed using (1). For this evaluation, the

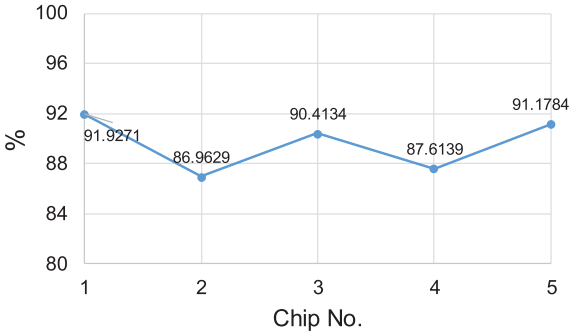

Fig. 20. Reliability of five chips in %.

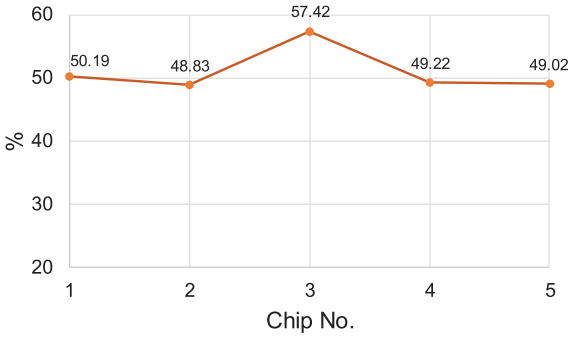

Fig. 21. Uniformity of five chips in %.

following parameters are considered: $C = 48$ and $n = 1$, with five ICs. The histogram in Fig. 18 illustrates the uniqueness distribution of the PUF responses. The calculated average inter-HD for the fabricated XNOR–XOR RO PUF is 49.62%, indicating a well-balanced response distribution.

2) *Reliability Analysis:* To assess the reliability of the XNOR–XOR RO PUF under varying external conditions while maintaining a consistent challenge input, (2) and (3) are applied. The evaluation considers the following parameter: $x = 256$. The histograms in Fig. 19 present the intra-HD distribution across the five fabricated chips, demonstrating a measured reliability range of 86.9%–92%, as shown in Fig. 20.
3) *Uniformity Analysis:* The average uniformity of the five XNOR–XOR RO PUF chips is computed using (4). The evaluation considers the following parameter: $x = 256$. The measured uniformity values range between 50% and 57.42%, aligning with theoretical expectations for a strong PUF design, with results illustrated in Fig. 21.

The power consumption of five fabricated ICs was analyzed, with measured values ranging from 4.427 to 4.458 mW, as depicted in Fig. 22. Experimental validation on both FPGA and ASIC platforms confirms that the buffer contributes to a stable and accurate response output, even under varying operational conditions. The control unit, implemented as an FSM, effectively coordinates the operation of all submodules by managing state transitions, enabling signals, and ensuring proper sequencing for accurate and synchronized PUF response generation. Though the ASIC version shows slightly

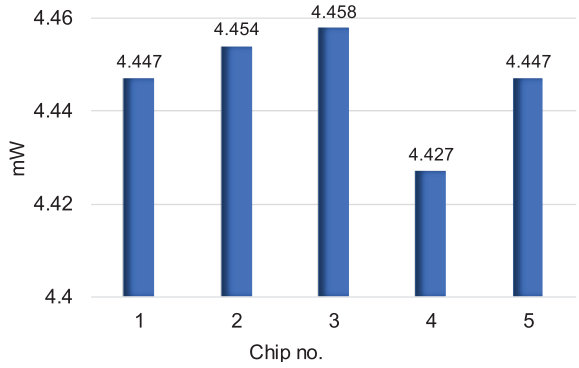

Fig. 22. Power consumption of five chips.

lower reliability than the FPGA, this is expected due to fewer ROs and sensitivity to fabrication conditions. Importantly, the ASIC offers a low-power solution with near-perfect output balance and strong uniqueness, making it a practical and secure choice for hardware-based authentication in IoT, IoUT, and embedded systems. Table III presents the state-of-the-art comparison between FPGA and ASIC with previous works.

V. Conclusion

The proposed XNOR–XOR RO PUF is verified using statistical metrics such as reliability, uniqueness, and uniformity. Initially, the design was deployed on a Xilinx ZYNQ 7000 FPGA board (28 nm) operating at 100 MHz. Statistical analysis using MATLAB showed impressive results, with reliability and uniqueness measured at 99.86% and 49.90%, respectively, and an average uniformity of 67.30%.

Furthermore, the design was implemented on silicon using Cadence Innovus in a 180-nm physical design. This work presents the first on-silicon implementation of an XNOR–XOR RO PUF, marking a significant milestone in PUF technology. The fabricated IC demonstrates high reliability (86.9%–92%), near-ideal uniqueness (49.62%), reasonable uniformity (50%–57.42%), and most important of all, very low power 4.447 mW at 1.8-V, 100-MHz, 180-nm CMOS node.

Acknowledgment

TSRI in NARL is recognized for the substantial EDA assistance provided.

References

[1] S. Elgendy and E. Y. Tawfik, "Impact of physical design on PUF behavior: A statistical study," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021, pp. 1–5.
[2] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
[3] C.-H. Chang, Y. Zheng, and L. Zhang, "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," *IEEE Circuits Syst. Mag.*, vol. 17, no. 3, pp. 32–62, 3rd Quart., 2017.
[4] M. A. Usmani, S. Keshavarz, E. Matthews, L. Shannon, R. Tessier, and D. E. Holcomb, "Efficient PUF-based key generation in FPGAs using per-device configuration," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 2, pp. 364–375, Feb. 2019.
[5] M. Jahanbakht, W. Xiang, L. Hanzo, and M. R. Azghadi, "Internet of underwater things and big marine data analytics—A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 2, pp. 904–956, 2nd Quart., 2021.

[6] B. R. Chandavarkar and A. V. Gadagkar, "Mitigating localization and neighbour spoofing attacks in underwater sensor networks," in *Proc. 11th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2020, pp. 1–5.
[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*. Berlin, Germany: Springer, 2007, pp. 63–80.
[8] E. Elmitwalli, K. Ni, and S. Köse, "Machine learning attack resistant area-efficient reconfigurable ising-PUF," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 4, pp. 526–538, Apr. 2022.
[9] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Design Autom. Conf.*, Jun. 2007, pp. 9–14.
[10] T.-K. Dang, R. Serrano, T.-T. Hoang, and C.-K. Pham, "A novel ring oscillator PUF for FPGA based on feedforward ring oscillators," in *Proc. 19th Int. SoC Design Conf. (ISOCC)*, Oct. 2022, pp. 87–88.
[11] B. Razavi, *Design of Analog CMOS Integrated Circuits*, 2nd ed., New York, NY, USA: McGraw-Hill, 2017.
[12] N. N. Anandakumar, M. S. Hashmi, and M. Tehranipoor, "FPGA-based physical unclonable functions: A comprehensive overview of theory and architectures," *Integration*, vol. 81, pp. 175–194, Nov. 2021.
[13] A. Shamsoshoara, A. Korenda, F. Afghah, and S. Zeadally, "A survey on physical unclonable function (PUF)-based security solutions for Internet of Things," *Comput. Netw.*, vol. 183, Dec. 2020, Art. no. 107593.
[14] D. Deng, S. Hou, Z. Wang, and Y. Guo, "Configurable ring oscillator PUF using hybrid logic gates," *IEEE Access*, vol. 8, pp. 161427–161437, 2020.
[15] L. Yao, H. Liang, Z. Huang, C. Jiang, M. Yi, and Y. Lu, "A lightweight configurable XOR RO-PUF design based on Xilinx FPGA," in *Proc. IEEE 4th Int. Conf. Electron. Technol. (ICET)*, Chengdu, China, May 2021, pp. 83–88.
[16] D. Rizk, R. Rizk, F. Rizk, and A. Kumar, "An economic uniqueness-improved reliable reconfigurable RO PUF for IoT security," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Austin, TX, USA, May 2022, pp. 1680–1684.
[17] H. Kareem and D. Dunaev, "A novel low hardware configurable ring oscillator (CRO) PUF for lightweight security applications," *Microprocessors Microsyst.*, vol. 104, Feb. 2024, Art. no. 104989.

Chua-Chin Wang (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from Stony Brook University, The State University of New York (SUNY) at Stony Brook, Stony Brook, NY, USA, in 1992.

He has been a Full Professor with the Department of Electrical Engineering, National Sun Yat-sen University (NSYSU), Kaohsiung, Taiwan, since 1998, where he was the CEO of the Operation Center of Industry-University Cooperation, from 2012 to 2014, held the position of Vice President at the Office of Industrial Collaboration and Continuing Education Affairs, from 2014 to 2015, was designated as the Dean of the College of Engineering, from 2014 to 2017, served as the Director of the Underwater Vehicle Research and Development Center, from 2018 to 2024, and is currently the Vice President of the Office of Research and Development. His research interests include memory and logic circuit design, communication circuit design, biomedical circuits, and interfacing I/O circuits.

Dr. Wang was bestowed with the Distinguished Engineering Professor designation by Chinese Institute of Engineers and the Fellow designation by IET, and received the Outstanding Research Award from NSYSU in 2012. His accomplishments earned him the ASE Chair Professor designation in 2013. He was honored by the IEEE Tainan Section with the Outstanding Technical Achievement Award in 2018. He held the position of Associate Editor of IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS from 2010 to 2013 and IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS from 2010 to 2011. He was the General Chair of the 2012 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS). He was designated as the Distinguished Lecturer at the IEEE CASS from 2019 to 2021.

Pradyumna Vellanki was born in India in 1993. She received the B.Tech. and M.Tech. degrees from Jawaharlal Nehru Technological University Kakinada (JNTUK), Kakinada, India, in 2015 and 2017, respectively. She is currently working toward the Ph.D. degree in electrical engineering at the National Sun Yat-sen University, Kaohsiung, Taiwan.

She was an Assistant Professor with the A.K.R.G. College of Engineering and Technology, Nallajerla, India, from November 2017 to August 2019. She then served as an Assistant Professor with the Sri Vasavi Engineering College, Tadepalligudem, India, from August 2019 to September 2021, followed by a similar role at the Sasi Institute of Technology & Engineering, Tadepalligudem, from October 2021 to August 2023. Her research interests include data converters, gate drivers, and IC design.

Jian-Jie Chen is currently working toward the M.S. degree in electrical engineering at the National Sun Yat-sen University, Kaohsiung, Taiwan.

Ralph Gerard B. Sangalang (Senior Member, IEEE) received the B.S. degree in electronics and communications engineering and the M.S. degree in electronics engineering from Batangas State University, The National Engineering University, Batangas City, Philippines, in 2009 and 2019, respectively, and the joint Ph.D. degree in electrical engineering and electronics engineering from the National Sun Yat-sen University, Kaohsiung, Taiwan, and Batangas State University, The National Engineering University, in 2023 and 2024, respectively.

He is currently an Assistant Professor and the Head of the Electronic Systems Research Center and the Program Chair of the Electronics Engineering Graduate Programs, Batangas State University, The National Engineering University, where he is also in charge of the Master of Science, the Master of Engineering, and the Doctor of Philosophy in the field of electronics engineering. His research interests include memory design, AI circuits, digital systems, control systems, computational modeling, fractional circuits, research security, fractional systems, and engineering education.

Dr. Sangalang received the Yeh Kung-Chie Memorial Scholarship Award at NSYSU in 2023. He was the Program Chair of B.S. Electronics Engineering from 2017 to 2021 and the Interim Program Chair of B.S. Biomedical Engineering. He was also the Student Outcome Committee Chair of the College of Engineering, Architecture and Fine Arts, from 2014 to 2021. He is the Governor of the Institute of Electronics Engineers of the Philippines—Batangas Chapter for 2025 and has been serving in different positions in the organization since 2014. He is also the Vice President of the Technical of the Mechatronics and Robotics Society of the Philippines—Batangas Chapter. He has served as a reviewer for IEEE International Symposium on Circuits and Systems (ISCAS), IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS), IEEE Symposium on Computer Applications and Industrial Electronics (ISCAIE), IEEE International Symposium on Biomedical Imaging (ISBI), Circuits, Systems, and Signal Processing (CSSP), *International Journal of Engineering* (IJE), *Kybernetika*, and *International Journal of Computing and Digital Systems* (IJCDS).