Mesopotamian journal of Cybersecurity
Vol.4,No.2, **pp**. 88–105
DOI: https://doi.org/10.58496/MJCS/2024/009; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Review Article

Memristive-Based Physical Unclonable Function Design of Authentication Architectures: A Systematic Review

Hussien Tho-Al-Fuqar Al-Ani [1,*], Israa Badr Al-Mashhadani [2]

[1] *Department of Computer, Collage of Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq*

[2] *Department of Computer, Collage of Engineering, Al-Nahrain University, Jadriya, Baghdad, Iraq*

ARTICLE INFO

Article History

Received 18 May 2024
Accepted 19 Jul 2024
Published 02 Aug 2024

Keywords

Hardware Security

Physically Unclonable Function (PUF)

Memristor (M)

Ring Oscillator-PUF (RO-PUF)

Field Programmable Gate Arrays (FPGA)

ABSTRACT

Physically unclonable functions (PUFs) are advanced physical security measures that offer fundamental, unclonable appraisals of physical objects, providing an effective defense against hardware vulnerability breaches. They function as unique digital hardware fingerprints. This study discusses previous methods adopted for improving hardware security via PUF technology, with a specific focus on PUF circuits implemented on FPGA boards. Hardware security is assumed to be enhanced by adding a memristor to the ring oscillator PUF circuit and implementing these authentication architectures on FPGA boards. Additionally, this study explores methods for improving the main performance metrics for FPGA-based memristive-ring oscillator PUFs, including uniqueness, uniformity, and reliability. The study was founded on many scientific studies selected according to specific criteria. This study aims to assess and contrast these studies to achieve substantial enhancements in the security of devices on the basis of the obtained results. Upon comparing the findings, it was revealed that the proposed techniques, which provide flexibility and adaptability in dealing with memristive-PUF circuits to improve security services, displayed a distinct enhancement in security performance compared with other research that did not include any references to memristors. As an essential part of the authentication architecture, performance metrics involving memristor technology are verified in this study, with a uniqueness of 48.57%, uniformity of 51.43%, and bit-aliasing of 51.43%. These outcomes demonstrate the validation of memristor-based physical unclonable functions (M-PUF) against encryption and verification within a certified key exchange and tests.

1. INTRODUCTION

As modelling, reverse engineering, and data extraction from integrated circuits (ICs) have increased, hardware security has become crucial [1], [2]. To address the need for distinctive integrated circuits that are resilient to reverse engineering, PUF technology provides a suitable solution to various security challenges [2]. Physically unclonable functions (PUFs) leverage the system's diverse physical properties, making them difficult to replicate even with a thorough understanding of the architecture. PUFs utilise the system's various physical characteristics, making duplication challenging despite a deep comprehension of the design [3].

The PUF is classified into two basic types for adoption in electronic circuits: strong and weak. Each type of classification has a specific application, which informs the selection of the hardware security type. The ring oscillator PUF is considered the most widely used type of weak PUF, with a finite number of challenge-response pairs (CRPs), whereas the arbiter serves as an example of a strong PUF with a vast number of CRPs [4], [5].

In this work, the ring oscillator-PUF (RO-PUF) is identified as a weak category of PUF, characterised by the challenge and its response [6]. Despite attempts to mimic it, the main feature of a PUF is that variations in gate delays lead to variations in how a particular challenge is approached. As forecasting or gathering data on these variations becomes more significant, the challenge and its response increase [7][8]. A ring oscillator serves as the regulator for the PUF, presenting it as a critical component in this design [9]. To mitigate this component, several FPGA devices are simulated to assess the encryption

*Corresponding author. Email: st.compe.hussien.t.jamil@ced.nahrainuniv.edu.iq

quality, while memristors that meet certain requirements and technological attributes that contribute to exploring the extent of constructing electrical circuits with robust security capabilities are also incorporated [10].

This paper discusses previous studies conducted in the field of hardware security within modern technologies currently in deployment. One of these technologies is physically unclonable functions (PUFs); additionally, the study discusses memristor technology and its significance in conjunction with PUF circuits. Compared with cryptography, this work explores the proposed memristive-based physical unclonable function (M-PUF) across several distinct FPGA chips. It examines situations, including authenticating protocols, and allows key exchanges to establish a unique, reliable, irreversible, and unpredictable outcome. Using Xilinx ISE edition 14.7, the M-RO-PUF structure is implemented on several FPGA devices via Verilog (HDL) as the test language.

2. Memristive-Based Physical Unclonable Function (M-PUF)

This section covers PUF technology and its applications in device security features. These circuits can be categorised as either weak or strong PUF circuits, with each category containing several types of PUF circuits. It will also focus on the most common types of PUFs, including the ring oscillator PUF (RO-PUF) and the arbiter PUF (A-PUF), which are commonly employed circuits in earlier studies. Furthermore, memristor technology will be explained in general, and its mechanism of use will be explored from both practical and theoretical perspectives.

2.1 Physical Unclonable Function (PUF)

PUF technology is an alternative to expensive, nonvolatile memory and is used to generate the private keys needed for cryptography and device authentication procedures [11]. A distinguishing feature of the fundamental structure is which, in a particular challenge, produces a response result relying on a characteristic of a complex physical structure that is difficult to replicate. PUFs often depend on unique physical differences that naturally occur during semiconductor manufacturing [4].

PUF is utilised to generate secret keys for cryptographic processes. It provides a distinct set of output bits for each secret input set or challenge. An input, known as a challenge, is sent to the PUF, which then generates an output known as a response. An imposed challenge and the response it receives together make up a challenge–response pair (CRP) [12]. Throughout their entire existence and in various environmental settings, CRPs should function consistently. Every chip should have a different set of CRPs. Responses to identical challenges should differ across ICs [1], as illustrated in Figure 1.

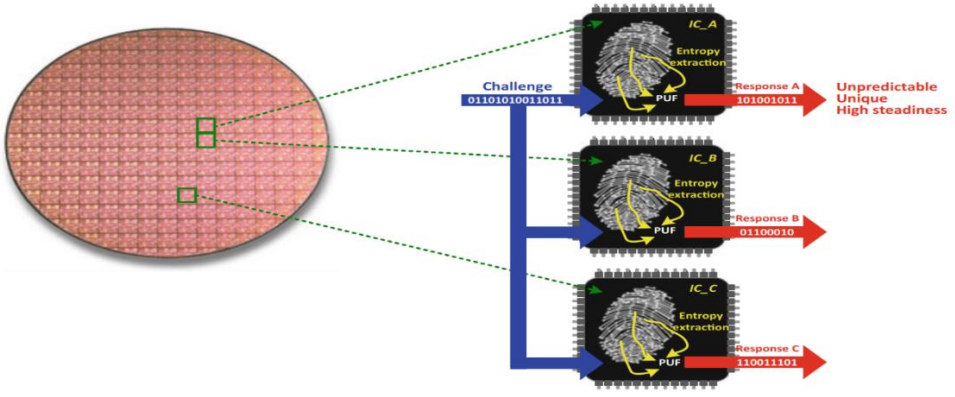

Fig. 1. CRPs apply to several ICs [13].

2.1.1 Ring Oscillator PUF (RO-PUF)

A ring oscillator PUF was designed as an FPGA-friendly PUF architecture, comparing oscillation periods contrastingly to single-path latency. However, compared with the arbiter PUF (A-PUF) in the same region, the RO-PUF yields significantly fewer response bits. With respect to authentication times, longer service lifetimes are correlated with more response bits, or CRPs [5]. This specific type of latency variation is adapted by the delay-based PUF found in the hardware's interconnects, which measures the frequency fluctuations of connected ring oscillators to generate diverse response patterns.

For every RO, there is an even number of inverters and one NAND gate, as illustrated in Figure 2. Two different ROs are chosen for the m-bit challenge via multiplexers. The selected ROs begin to oscillate and drive the next counter when the signal that enables oscillation increases, determining the number of oscillation cycles. The ROs can simultaneously stop functioning by pulling down the RO EN [14].

After a time period of t, also known as the measuring period, the comparator compares the count values of both counters. Despite the structural similarity of all ROs, manufacturing variances cause their frequencies to vary. Therefore, if it is assumed that the fastest RO is at the top, the comparator generates a response bit of 1; otherwise, it generates a response bit of 0 [5]. The output of applying n different challenges in the same manner can yield an n-bit response.

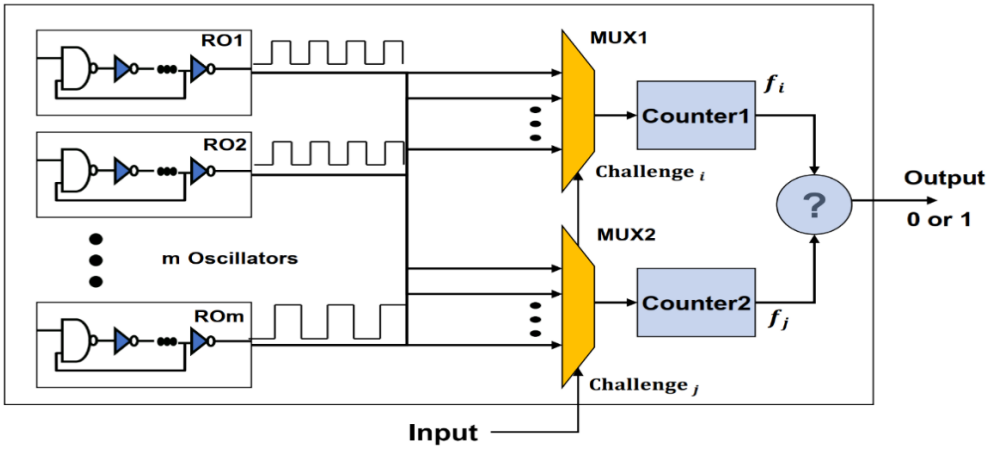

Fig. 2. Ring Oscillator PUF (RO-PUF) [15].

2.1.2 Arbiter PUF (A-PUF)

The first silicon PUF that deploys an arbitrator to compare the times of two identical paths is called the arbitrator PUF (A-PUF). Achieving symmetrical paths to ensure strong uniqueness is challenging, particularly in the context of field-programmable gate arrays (FPGAs), to alleviate the tension associated with routing [5].

The A-PUF is divided into k stages, each of which has 2-input multiplexers, as shown in Figure 3. The first-stage input receives a signal to generate a response bit; the challenge is used to ascertain the signal path to the subsequent step. Every multiplexer path (top and bottom paths) is concurrently and parallelly raced by the two electrical signals. An arbiter, which can be implemented by a latch, is used after the APUF design to identify whether the top or bottom signal comes first and outputs a logic ‘0’ or ‘1’, respectively.

A rising signal is simultaneously applied to the two pairs to assess the output for a given input. Next, the signals rapidly flow through the pairs of top and bottom selectors. Finally, the arbitrator determines which signal is faster. The responses are ‘0’ in all other cases and ‘1’ in the event that the top two selector pairs arrive at the arbiter first [6].

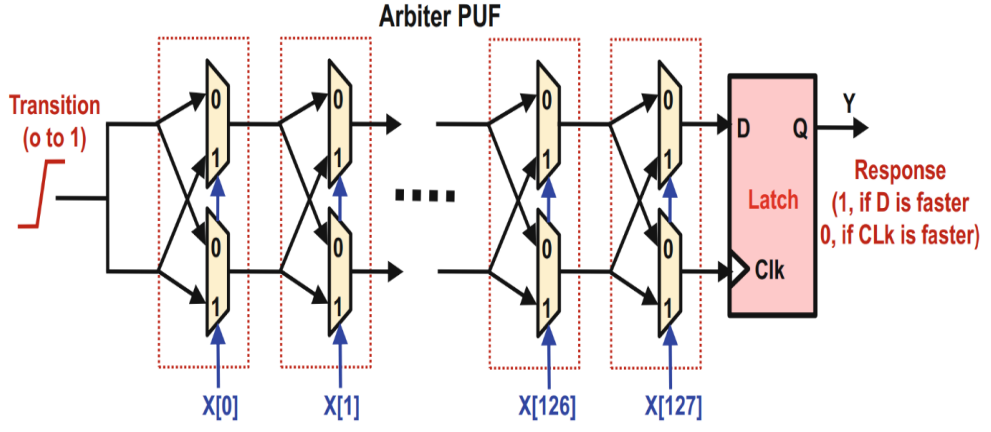

Fig. 3. The 128-bit challenge inputs the arbiter PUF [16].

2.2 Memristor

In addition to resistors, capacitors, and inductors, the fourth passive element is a two-terminal nonlinear resistor known as a memristor. Chua proposed memristors in 1971, which serve as the fourth essential circuit component [17], as illustrated in Figure 4. In mathematics, the relationship between the charge q and the flux φ is represented by the formula M=dq/dφ for the memristor.

Memristors have been suggested as potential successors to conventional memory, such as flash memory and DRAM, in next-generation nonvolatile memory. The Hewlett-Packard (HP) group experimentally demonstrated the first memristive device in 2008 [18] as an electrical resistance component that has the ability to maintain an internal resistive state on the basis of the voltage and current supplied in the past. Three standard operations are defined for the majority of memristive devices: formation, which is the device's initialisation procedure; return, which shifts the resistance of the memristor from a higher resistance state (HRS) to a lower resistance state (LRS); and setup, which alters the resistance of the memristor between the HRS and the LRS. Memristor-based logic gates and neuromorphic computing are two other areas in which memristors are progressively being employed [7]. Currently, memristors are employed for various purposes, with hardware security being one of the most significant applications [19].

Owing to the memory-like qualities of memristors and their ability to alter resistance, PUF designs incorporate this device to provide even greater diversity. Furthermore, the technology used to manufacture memristors is fairly consistent with the standards employed in CMOS production today. Unlike unidirectional MOSFETs, memristors are bidirectional devices; thus, it has been hypothesised that memristor-based PUFs are more resilient to model-building assaults than exclusively CMOS-based PUFs are. In efforts to enhance PUF performance, research has been conducted on incorporating memristors into various PUF types [20].

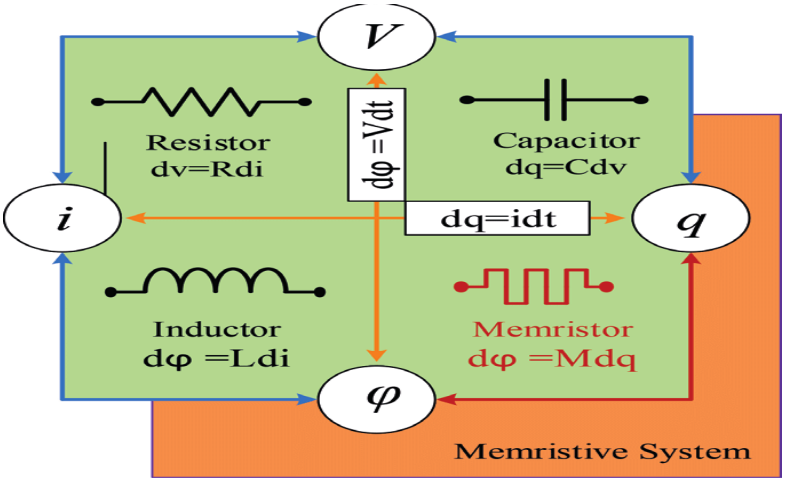

Fig. 4. Fourth passive element [21].

3. RESEARCH METHOD

The systematic literature review utilised in this paper aims to investigate pertinent research regarding memristor-based physical unclonable function design in authentication architectures. This paper provides comprehensive answers to research questions covering the field of study.

3.1 Research Questions

RQ1: What outcomes did the researchers obtain when deploying the RO-PUF on the FPGA?

RQ2: Can the proposed architecture improve device security compared with previous architectures?

RQ3: What is the purpose of implementing the M-ROPUF authentication architecture?

3.2 Searching Strategy

A systematic literature search was conducted to identify the most important recent studies in the field of hardware security, which discuss previous methods aimed at improving device security via physical unclonable function (PUF) technology and memristor technology. The research papers were selected according to specific criteria, which included recent studies in this field. These studies were chosen from the years 2017–2024 (as illustrated in Table 1).

TABLE 1. NUMBER OF PAPERS PER DATABASE

Search Engines	Number of Papers
Crossref	2724
Google Scholar	568
Semantic Scholar	358
Scopus	39
Total Number	3689

The collection of sources was processed sequentially via basic keywords related to the search, as shown in Table 2, through the utilisation of search engines.

TABLE 2. KEYWORDS AND STRINGS

Search Engines	Search Keyword
Crossref	"PUF" OR "Memristor" "FPGA" OR "Memristor" "Ring Oscillator PUF" OR "Arbiter PUF" "Memristor-based PUF" OR "FPGA" "PUF" AND "Memristor" "FPGA" AND "PUF"
Google Scholar	
Semantic Scholar	
Scopus	

3.3 Inclusion/Exclusion Criteria

The criteria adopted by this research were selected according to a specific mechanism that included studies conducted in the field of authentication architectures for memristor-based physically unclonable functions (M-PUF). The exclusion and inclusion mechanisms were based (as illustrated in Figure 5) on the extent to which the content of these studies and the study under consideration are comparable.

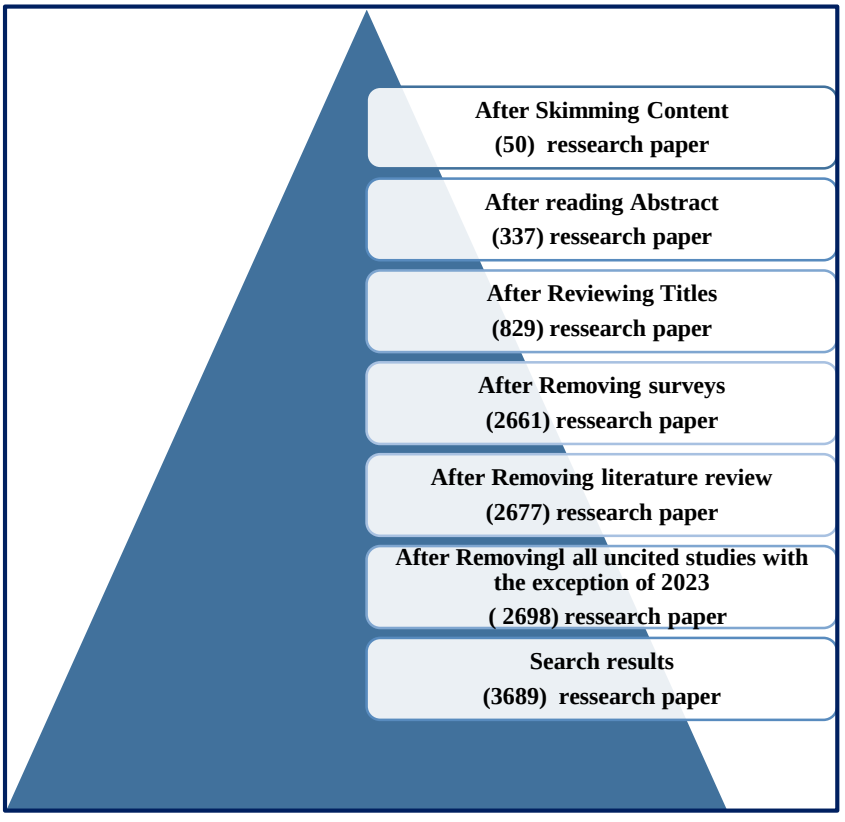

Fig. 5. Illustration of the inclusion/exclusion criteria.

The following requirements had to be met for the research articles or papers to be chosen:

- Research related to physically unclonable functions (PUF).
- Research related to memristor-based physical unclonable functions (PUF).
- Research related to hardware security and field-programmable gate arrays (FPGA).

Papers were rejected if any of the following requirements were not met:

- Research fundamentals do not include physically unclonable functions (PUF).
- They cover only a portion of the research and ignore the remainder of the study.
- Studies that fall outside of the area of our research.

3.4 Paper Selection Criteria

Considering the conducted studies, only 52 research papers were selected using the previously stated study methodology. These papers were selected using predefined established criteria, which are based on the quality and efficiency of the research as well as the publication outcomes. Regarding the methods used for their selection, the following digital libraries (as depicted in Table 3) were chosen for this systematic literature review.

TABLE 3. DIGITAL LIBRARY AND PAPERS

Digital Library	Number of Paper
IEEE Xplore	22
Springer Link	5
ScienceDirect	3
ResearchGate	2
TechRxiv	2
MDPI	2
IET	2
Mesopotamian Academic Press	4
University of Victoria Libraries	1
Wiley Online Library	1
SPIE digital library	1
IntechOpen	1
IOPscience	1
J-STAGE	1
ICTACT	1
IJEECS	1
IIETA	1
BEEI	1
Total	52

The papers above were selected on the basis of recent studies from 2017–2024. Figure 6 presents the distribution of the selected papers by year.

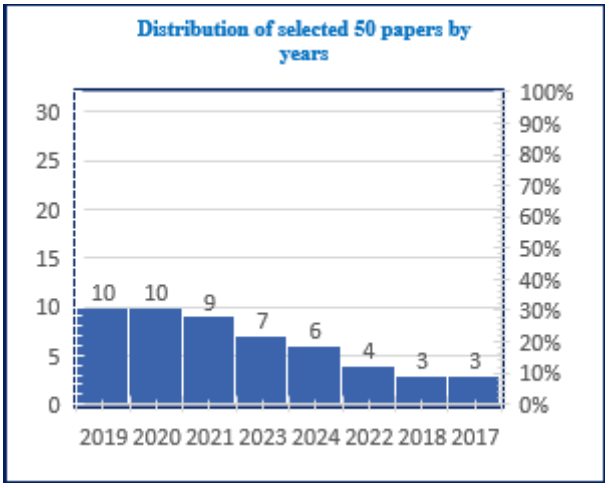

Fig. 6. Distribution of papers by year.

This selection process in the systematic literature review, as depicted in Figure 7, adhered to a specific mechanism with defined criteria that relied on selecting reliable digital libraries and their affiliated journals to guide study selection.

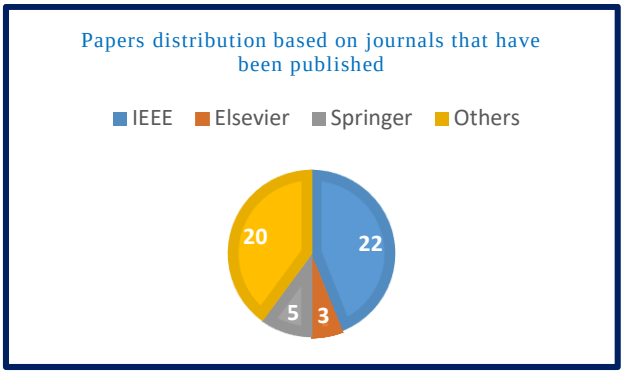

Fig. 7. Distribution of papers by publisher.

Figure 8 shows the types of papers included in this systematic literature review, along with their respective quantities, which vary across articles, conference papers, books, and theses.

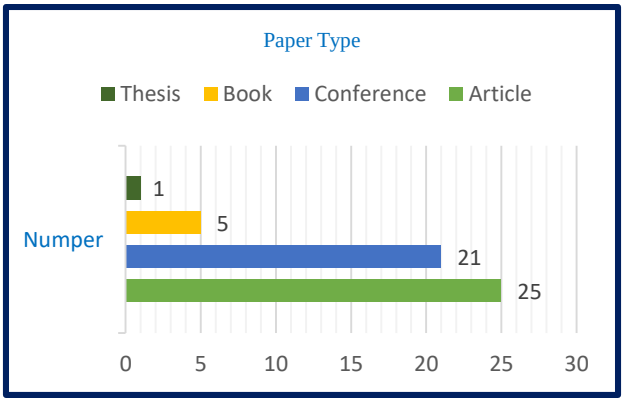

Fig. 8. Paper type.

4. RELATED WORK

It is important to consider the valuable information contained in scientific research that can enhance efficiency, performance, and effectiveness. The selected research is directly related, or as closely related as possible, to the field of study as a scientific reference. This reference can be relied upon to make comparisons between the results extracted from these references by identifying the tools used in this study and those references to avoid weaknesses that could affect the preparation of this study.

4.1 Related Survey

This section elucidates the research that is relevant to the area of investigation, which focuses on PUF circuits with memristor technology. The summary is as follows:

4.1.1 Memristive Physical Unclonable Functions (M-PUFs)

In 2023, Al-Khaboori and Al-Mashhadani [19] analysed various memristive PUF design strategies that have been proposed in the literature. Next, they provided specific performance evaluation results for several memristive PUF designs achieved through manufacturing and simulation techniques and compared these results. Ultimately, the majority of the circuits were assessed via simulation, whereas a small number were assessed via fabrication because of the costly nature of the fabrication process. Memristors are anticipated to be marketed and used in next-generation hardware security. However, they have not yet been released commercially and are still in the prototype stage. Researchers are exploring M-PUF apps for various purposes, such as storage, secret key generation, device identification, and authentication. M-PUF leverages the unique properties of memristors, including their nanoscalability, bidirectionality, nonvolatility, model complexity, and nonlinearity, to enhance PUF performance measures such as bit aliasing, uniformity, dependability, and uniqueness. The nonvolatility of memristors makes PUFs extremely vulnerable to variations in the manufacturing process. As a result, various uses of M-PUFs, including memory applications as well as safety features such as chip authentication, identification, and generated keys, will produce distinct outcomes for each input. Additionally, it is anticipated that the size of the M-PUF circuit will increase with the actual marketing of memristor devices. Notably, the simulation approach produced better outcomes than did the manufacturing process, as the fabrication process placed more emphasis on the operation's success rather than its actual performance. The outcomes also demonstrate the resistance of M-PUFs against machine learning, side-channel, modelling, and fault-injection attacks.

4.1.2 Configurations of Memristor-Based APUF (M-APUF)

In 2019, Teo et al. [20] advised adjusting the settings of the memristor-based arbiter PUF (APUF) to improve variations. This adjustment is aimed at enhancing the PUF's uniformity, reducing bit-aliasing, enhancing uniqueness, and increasing resilience against support vector machine (SVM) attacks. Another objective is to increase the difficulty or duration required for a competitor to reproduce the schematic of the circuit. Two setups exist for achieving these goals: (1) adjusting the memristor count in each transistor and (2) changing the count of challenge bits and response bits. The outcomes demonstrate outstanding performance as well as robust defenses against SVM assaults. The results are also valid for other combinations. With this CMOS technology, the memristor-based A-PUF performs effectively in emulation under all conditions. If the SVM accuracy in prediction is limited to 52.3% and their uniqueness, bit-aliasing, and uniformity values for the two CMOS technologies are nearly 50%, this indicates strong PUF performance. In summary, the settings apply to memristor-based A-PUF hardware security device implementation.

4.1.3 Ring Oscillator Physically Unclonable Function (M-ROPUF)

In 2019, Teo et al. [22] proposed two main changes to the RO-PUF. First, memristors are added to the inverting units of the RO. These memristors have a smaller footprint and consume less power than other CMOS components do, which explains their inclusion. Additionally, the memristors satisfy the requirements for CMOS manufacturing. The process for developing PUFs for response is the subject of the second modification. In contrast to traditional RO-PUF designs, which yield one response bit for each pair of ROs, the suggested memristor-based RO-PUF produces a single multibit response for each series of RO pairs. With a minimal amount of circuit overhead, this approach can dramatically improve the CRP set list, as illustrated in Figure 9.

In terms of bit-aliasing, uniqueness, and uniformity, the results indicate that the proposed memristor-based RO-PUF method results in very little response bias. Furthermore, the memristor method suggested for the RO-PUF is not well predicted by the support vector machine (SVM), rendering it resistant to SVM attacks. In summary, the proposed memristor-based RO-PUF offers a simple yet dependable PUF design. Further experiments, including modelling attacks with various machine learning techniques, randomness tests such as NIST verification, and assessments of voltage and temperature reliability, are planned for future research to validate and evaluate the proposed memristor-based RO-PUF. For security considerations, the RO-PUF may ultimately be manufactured and utilised as a real physical component.

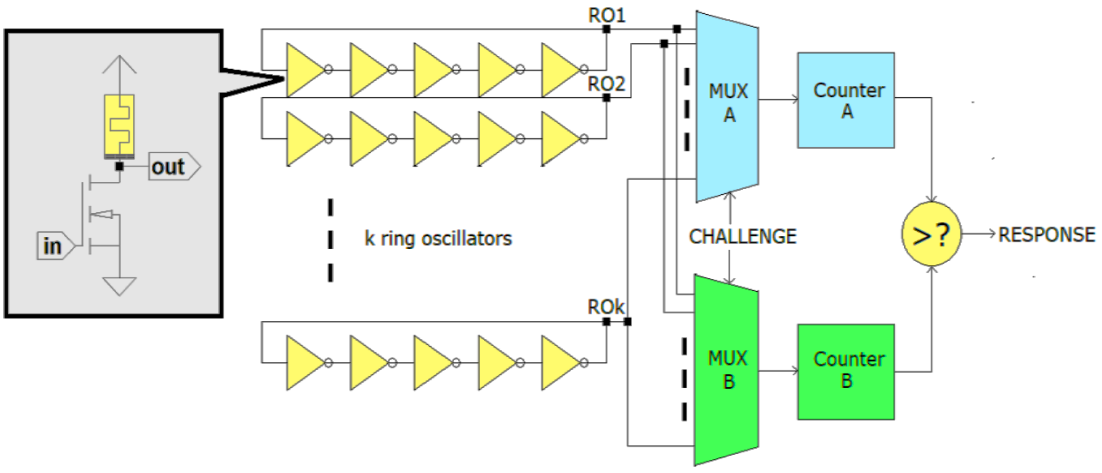

Fig. 9. Proposed memristor-based ROPUF [22].

4.1.4 A Ring Oscillator Physical Unclonable Function (RO-PUF)

In 2024, Liu et al. [23] proposed an architecture that was applied to several FPGAs, specifically Kintex-7, where the challenge was activated as an 8-bit input to obtain a 32-bit output from this system as a response. This system is implemented by inputting the challenge signal to the host computer via the UART port, as illustrated in Figure 10. Next, an analysis of the outputs extracted from the RO-PUF circuit is performed to measure the performance metric, which includes the basic metrics of uniformity, uniqueness, and reliability. The experimental results show that the proposed RO-PUF has 47.30% uniformity, 97.07% reliability, and 47.46% uniqueness. According to these results, the proposed method can be considered a promising solution in the areas of secret key generation as well as internet Protocol security protection, in addition to other areas within the scope of security.

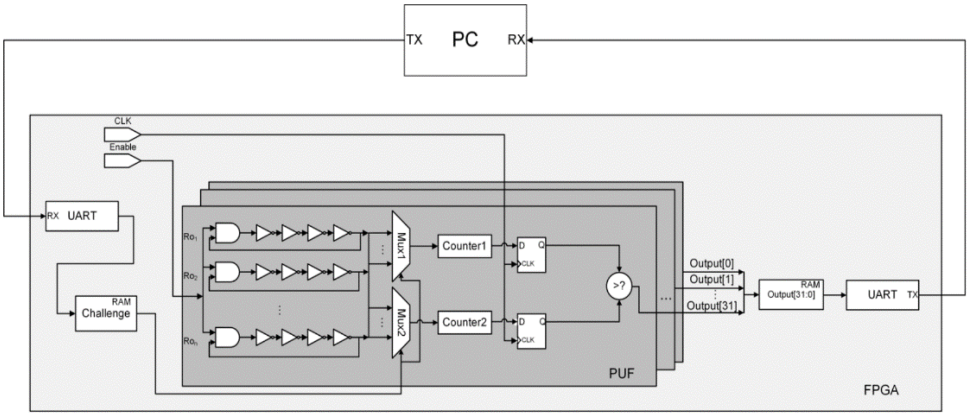

Fig. 10. Testing of the proposed RO-PUF [23].

4.2 Classification and Comparison of Related Works in this Field

In this section, previous studies in the field of hardware security were examined, focusing on a specific basis in terms of the implemented structure and based on PUF circuits as its basic application principle. Additionally, studies conducted on various FPGA devices were considered. Some of these studies applied memristor technology to PUF circuits. This section was organised to classify previous research on the basis of the structure and architecture aimed at improving hardware security. These studies have been classified into two main tables—Table 4 and Table 6—each complementing the other.

Table 4 delineates the classification of research in terms of the structure and tools employed on the basis of the implementation methods of PUF circuits, particularly the ring oscillator PUF (RO-PUF) and arbiter PUF (A-PUF) circuits. These circuits are implemented on various FPGA devices. In some instances, ring oscillator PUF circuits were used alongside FPGA hardware, as seen in [1], [3]–[5], [12], [14], [15], [23], [24], [25], [28], [30], [31], [33]–[35], [43]–[47], [49], and [50]. Additionally, other studies investigate different aspects of the implementation mechanisms. One of which is designing an integrated PUF circuit using IDEALY RO-PUF to generate secret keys, as in [36]. Moreover, the PUF design takes advantage

of D-Latches' metastability characteristics and the delay differential between two ostensibly similar signal channels when there is an incomplete reset source. The outcomes of the design are detailed in [11]. Another aspect is the use of RO-PUF with programmable delay lines (PDLs), which are run by FPGA devices. The PUF modifies the look-up table (LUT) propagation path via the PDL, which modifies the RO output. For a given RO-PUF design and challenge, several responses arise on the basis of the result of the altered RO [26]. The RO circuit was also developed in [32] of the Boosted Configurable Ring Oscillator PUF (BC-PUF) with an area-efficient CROPUF variation appropriate for Internet of Things devices with limited resources. Furthermore, BC-PUF utilises an absorbent method for transitional responses to maximise the use of CMOS delay setups. Additionally, BC-PUF reduces the possibility of modelling attacks via machine learning (ML) [51]. Another method that minimises switching activity, emphasises interstage delays and shrinks the RO set is an effective way to lower area overhead as well as power consumption [29]. Another study investigated the advantages and disadvantages of PUF technology concerning speed, slow response, and the extent to which it can be attacked externally through modelling attacks and other methods. The study concluded that memory-based PUF technology generates output faster, as outlined in reference [9].

In other studies, arbiter PUF circuits were utilised with FPGA hardware, as noted in [6], [40], and [41]. Additionally, in further research, the incorporation of memristor technology was explored to increase the security efficiency of these circuits. The memristor's significance lies in its ability to regulate the current entering these circuits and eliminate the need for frequency regulation processes. Moreover, the memristor possesses other features that contribute to its potential in this context. Table 4 also presents studies conducted on memristors as a technology that aids in enhancing the efficiency of PUF circuits when utilised alongside them, as demonstrated in [7], [19], [38], and [39]. The author of [20] elucidated the use of a memristor with an arbiter PUF circuit to verify the efficiency of the circuit's performance and enhance hardware security. Additionally, the extent of improvement in hardware security was assessed, as demonstrated in [22]. Several studies have aimed for significant improvements and addressing potential future challenges, as demonstrated in [27], [37], [42] and [48]. Additionally, to integrate with embedded systems, a simpler RO-PUF is designed as a parametrizable IP component with an included common AXI4-Lite interface design. The modular device's RO bank's position and size may be selected before the analysis and execution phase, as outlined in reference [14].

TABLE 4. CLASSIFICATION OF RESEARCH ACCORDING TO STRUCTURE

Reference	Year	Structure	PUF Circuits	Number Of Stage	Challenge Response Pairs (CRPs)		Implementation Devices	
					Challenge	Response	Memristor	FPGA
[1]	2020	Delay- based RO PUF	RO PUF	256 ROs	16-bits	1-bit	-	✓
[3]	2019	RO PUF With Enhanced CRPs	RO PUF	256 ROs	16-bits	28-bits	-	✓
[4]	2023	XOR all ROs outputs	RO PUF	32 ROs	m-bit	n-bit	-	✓
[5]	2020	Hybrid configurable RO (HC-RO)	HC-RO	16, 32, 64 HC-RO	m-bit	n-bit	-	✓
[6]	2019	Multi-line APUF	APUF	64 stages	64-bits	12-bits	-	✓
[7]	2019	Memristor-based PUFs and TRNGs	PUFs	N stages	m-bit	n-bit	✓	-
[11]	2021	Delay Difference PUF (DD-PUF)	DD-PUF	N stages	m-bit	128-bit	-	✓
[12]	2020	Internet of Things (IoT) with the PUF	RO PUF	512 ROs	16-bits	256 bits	-	✓
[14]	2021	Configurable RO-PUF for Embedded Systems	RO PUF	5 ROs	16-bits	256 bits	-	✓
[15]	2021	configurable-based ring oscillator PUFs (CF-ROPUFs)	RO PUF	16 ROs	10-bits	256-bits	-	✓
[19]	2023	MEMRISTIVE PUF (MPUF)	PUFs	N stages	m-bit	n-bit	✓	-
[20]	2019	memristor-based APUF	APUF	N stages	8, 16, and 32 bits	4 & 8 bits	✓	-

[22]	2019	memristor-based ROPUF	RO PUF	8 ROs	98 bits	28-bits	✓	-
[23]	2024	ring oscillator-based PUF	RO PUF	15 ROs	8-bits	32-bits	-	✓
[24]	2020	ring oscillator-based PUF	RO PUF	10 ROs	m-bit	45 bits	-	✓
[25]	2023	robust architecture configurable (RAC) RO-PUF	RO PUF	16 ROs	11-bit	2024 bits	-	✓
[26]	2024	Programmable Delay Lines PDL-based RO-PUF	RO PUF	32 ROs	m-bit	n-bit	-	✓
[27]	2020	RO-PUF Designs in FPGA	RO PUF	128 ROs	6-byte	n-bit	-	✓
[28]	2019	Implementation RO-PUF in FPGA	RO PUF	N ROs	m-bit	n-bit	-	✓
[29]	2024	Configurable Ring Oscillator (CRO) PUF	RO PUF	N ROs	32-bit	1K	-	-
[30]	2020	Delay-based RO PUF on FPGA	RO PUF	256 ROs	8-bit	8-bit	-	✓
[31]	2019	FPGAs-based RO PUF and derive a random number	RO PUF	N ROs	m-bit	n-bit	-	✓
[32]	2024	Boosted Configurable Ring Oscillator PUF (BC-PUF)	RO PUF	8, 128 or 256 ROs	32-bit	16-bit	-	✓
[33]	2021	configurable RO-PUF based on FPGA	RO PUF	7 ROs	m-bit	n-bit	-	✓
[34]	2022	FPGA-based Ring Oscillator PUFs	RO PUF	16 ROs	8-bit	32-bit	-	✓
[35]	2019	FPGA-based RO PUF	RO PUF	16 ROs	16-bit	8-bit	-	✓
[36]	2024	IDELAY-based PUF technology	RO PUF	N ROs	m-bit	255-bit	-	✓
[37]	2023	Configuration Updates for Remote FPGAs	APUF	8 stages	8-bit	32-bit	-	✓
[38]	2021	Various memristor-based PUFs	pulse width-based memristive-PUF (pm-PUF)	-	m-bit	n-bit	✓	-
			Selected Bit-line Current PUF (SBC-PUF)	-	m-bit	n-bit	✓	-
			Total Bit-line Current PUF (TBC-PUF)	-	m-bit	n-bit	✓	-
			Multi-Array PUF (MA-PUF)	-	m-bit	n-bit	✓	-
[39]	2021	memristive polimino PUF based on symmetric functions.	polimino PUF	-	m-bit	n-bit	✓	-
[40]	2022	design of Hybrid PUF	Arbiter PUF & Butterfly PUF	N stages	8-bit	n-bit	-	✓
[41]	2022	implementation of XOR APUF on FPGAs	XOR APUF	3 stages	64-bit	64 bit	-	✓
[42]	2020	Reliable and Lightweight PUF-based Key Generation	PUF	-	m-bit	n-bit	-	✓
[43]	2020	Configurable RO PUF Based on FPGA	XOR RO-PUF	128 stages	m-bit	n-bit	-	✓
[44]	2021	FPGA-based RO PUF	RO PUF	N ROs	m-bit	n-bit	-	✓

[45]	2021	Configurable XOR RO-PUF Design Based on Xilinx FPGA	XOR RO-PUF	128 XOR ROs	m-bit	128-bit	-	✓
[46]	2018	implementation Of A Hybrid RO PUF	hybrid PUF	64 ROs	5-bit	64 bit	-	✓
[47]	2022	modified RS-LPUF and RO-PUF through the incorporation of the TMV scheme and coarse PDL techniques	RO-PUF (Ring oscillator-based PUF)	32 ROs	8-bit	256-bit	-	
			RS-LPUF (RS Latch-based PUF)	32 RS latches	8-bit	256-bit		✓
[48]	2018	PUF-Based Key Generation in FPGAs	Per-Device PUF	N stages	m-bit	100-bit	-	✓
[49]	2019	In-depth Analysis Of Measurement Data Extracted From Xilinx Zynq-7000 Fpgas	RO PUF	3800 ROs	m-bit	n-bit	-	✓
[50]	2019	FPGA Based Robust Random Number Generator	RO PUF	32 ROs	8 bit	255 bit	-	✓

Moreover, Table 6 shows the results obtained from those studies, which were based on performance metrics used to determine the efficiency of security in held studies. It presents the performance analysis obtained through the simulation process. The mechanisms employed in earlier research are clarified in Table 6, which indicates the significant improvement in terms of performance and security, which may vary from one study to another because of the methods and tools utilised. Generally, there are specific standards used to measure the security efficiency of hardware, which determine the extent of improvement. By examining the results extracted from the system built according to the previously defined structure, these performance metrics include uniqueness, uniformity, bit-aliasing, reliability, randomness, and average frequency. These metrics are deployed to test the performance efficiency of hardware security and measure the extent of improvement in the security system. The table also displays the different types of FPGA hardware used, which vary according to the nature of the studies conducted, illustrating the variety of FPGAs utilised. To clarify the common PUF performance metrics mentioned in Table 6, which are used in the proposed study, the equations are briefly explained below.

1) Uniqueness: This determines the degree of uniqueness among the chips. A high value for uniqueness is associated with significant process variation. Fifty percent (50%) uniqueness is the value of an ideal PUF.

$$Uniqueness. = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(Ri, Rj)}{n} \times 100\% \quad (1)$$

2) Uniformity: This is an indicator of the degree of randomness in the CRP. Before an answer has 50% of its total ‘0’s and ‘1’s, it cannot be considered random.

$$Uniformity(i) = \frac{1}{n} * HW(Ri) \times 100\% \quad (2)$$

3) Reliability: At 100%, the PUF should respond consistently regardless of the amount of noise and interference from its surroundings.

$$Hdintra(i) = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(Ri, R'i, y)}{n} \times 100\% \quad (3)$$

$$Reliability = 100\% - HDintra\ (i) \quad (4)$$

4) Bit-aliasing: Bit-aliasing finds the commonalities in the answers provided by PUFs. When bit-aliasing occurs, different ICs can produce comparable outcomes. The bit-aliasing of the l-th bit in an n-bit response is its average Hamming weight over several k devices. Fifty percent (50%) is the optimal value.

$$Bit - Aliasing = \frac{1}{k} * \sum_{i=1}^{k} ri, l \times 100\% \quad (5)$$

5) Randomness: PUFs should ideally have a randomness rate of 50%. Randomness is defined as the percentage of PUFs that will yield a response of '0' or '1'.

$$Randomness = \sum_{i=1}^{N} \frac{Ri}{N} \times 100\% \quad (6)$$

Table 5 lists all the parameters mentioned in the previous equations through which the performance metrics of device security are measured.

TABLE 5. EQUATIONS AND PARAMETERS

Parameters	Definitions	Parameters	Definitions
k	Number of PUF chips using	HW	Hamming Weight: the n-bit PUF identifier
i	The chip (i)	Hdintra	The average inter-chip hamming distance among the *k* devices
j	The chip (j)	x	The number of response samples
HD	Hamming distance: the response obtained from a group of chips	y	The y-th sample of response
Ri	Response n-bit obtained from the chip (i)	R'i,y	The y-th sample of R′i
Rj	Response n-bit obtained from the chip (j)	ri,l	The l−th binary bit of an n−bit response from a chip i
n	The bit-length	N	The total number of n−bit challenge

TABLE 6. PUF PERFORMANCE METRICS ANALYSIS

Reference	Year	Hardware	Uniqueness (50%)	Uniformity (50%)	Bit-aliasing (50%)	Reliability (100%)	Randomness (100%)	Average Frequency
[1]	2020	FPGA Spartan–3E (XC2C256)	47.5%	≈ 51.23%	-	-	-	103.89MHz
		FPGA Spartan–3E (XC2C256)	45.5%	≈ 43.67%	-	-	-	101.71MHz
[3]	2019	FPGA Spartan 3E (XC3S500E)	-	47%	-	-	-	102.23 MHz
		FPGA Spartan 6E (XC6SLX9)	-	48%	-	-	-	104 MHz
[5]	2020	50 FPGAs	46.76%	50.36%	-	-	-	-
[6]	2019	FPGA Virtex-5 (XC5VLX110T)	46.53%	-	-	99.88%	49.77%	-
[11]	2021	FPGA Artix-7	49.48%	-	-	98.33%	-	-
		FPGA Spartan- 6	49.28%	-	-	98.37%	-	-
[12]	2020	FPGA Cyclone 5 Intel Chip	48.18%	-	-	100%	46.62%	-
[15]	2021	30 FPGAs Spartan-3E	-	-	-	98.5%	93.3%	-
[20]	2019	Memristor 180nm at 1.8V No. of memristor per transistor 3	49.995%	50.310%	50.344%	-	-	-
		Memristor 130 nm at 1.2V No. of memristor per transistor 5	49.215%	54.560%	54.763%	-	-	-
[22]	2019	Memristor 180 nm at 1.8V	48.57%	51.43%	51.43%	-	-	-
		Memristor 130 nm at 1.2V	51.36%	49.49%	48.81%	-	-	-
[23]	2024	4 Kintex-7	47.46%	47.30%	-	97.07%	-	-

[25]	2023	FPGA	49.78 %	49.42 %	-	97.72 %	98.34 %	-
[29]	2024	application-specific integrated circuit (ASIC)	45.5%	49.42%	-	9.95%	-	-
[30]	2020	FPGA Spartan 7	46.436%	-	-	99.68%	-	-
[31]	2019	54 FPGAs devices (24 Nexys-4 DDR, 10 Basys-3 and 20 Zybo)	49.90%	-	-	99.70%	-	-
[32]	2024	50 FPGAs (13 Nexys A7, 13 Nexys, 4 DDR, and 27 Nexys)	42%	50.2%	-	3.925%	-	-
[33]	2021	FPGA Spartan series	49.13%	-	-	98.87%	-	-
[34]	2022	5 FPGAs Arty A7	49.84%	49.06%	-	98.36%	-	-
[35]	2019	3 FPGAs Virtex-6 (ML605)	47.57%	48.96%	-	-	-	-
[36]	2024	FPGA ZYNQ PSoC xc7z010clg400-1	49.63%	59.38%	-	98.23%	-	-
[38]	2021	Memristor (TBC-PUF)	50.1%	51.8%	51.2%	-	-	-
		Memristor (SBC-PUF)	50.0%	48.1%	49.0%	-	-	-
		Memristor (MA-PUF)	50.6%	52.5%	51.2%	-	-	-
[41]	2022	25 FPGAs Artix-7	48:69%	50:73%	-	99:41%	-	-
[43]	2020	FPGA Artix-7 BASYS3	49.44%	-	-	98.12%	-	-
[45]	2021	16 FPGAs Virtex-6	48.438%	-	-	Under voltage 1.758% Under temperature 1.674%	-	-
[46]	2018	FPGA Altera 6	65.4%.	-	-	-	-	-
[47]	2022	10 FPGAs Artix-7 (XC7A100T) Only PDL (RO-PUF)	48.91%.	49.55%	49.55%	97.91%	-	-
		10 FPGAs Artix-7 (XC7A100T) both PDL and TMV (RO-PUF)	48.91%	49.62%	49.62%	99.39%	-	-
		10 FPGAs Artix-7 (XC7A100T) Only PDL (RS-LPUF)	49.47%	51.02%	51.02%	98.29%	-	-
		10 FPGAs Artix-7 (XC7A100T) both PDL and TMV (RS-LPUF)	49.47%	50.68%	50.68%	99.46%	-	-
[48]	2018	FPGAs ZYNQ-7000	46.25%	-	-	2.37%	-	-
[50]	2019	34 FPGAs devices (24 Nexys-4 DDR and 10 Basys-3 FPGA)	49.83%	-	-	99.35%	-	-

The classification of different design approaches of memristive PUFs that were investigated in the previous section is summarised in Tables 4 and 6, which contain detailed information on the proposed models, including the model type and the implementation process type if it is simulated or implemented. The increase in the size of the memristor circuit appears to be the cause of the growth in the size of the M-PUF circuits, and it is expected that the number of challenge-response bits will increase when the real implementation of memristor PUFs occurs. Table 6 compares the performance metric results obtained via the simulation process and the implementation process. The results demonstrated that uniqueness and uniformity are almost at the 50% optimum value, depending on the FPGA model and source of fabrication. Comparing different results of performance metrics obtained by different FPGA models. The highest value of the uniformity metric is equal to ≈ 51.23%, which was obtained from [1], whereas the memristor (MA-PUF) uniformity metric is equal to ≈ 52.5%, which was obtained

from [38]. The highest value of the uniqueness metric using FPGA Altera 6 is equal to the 65.4% obtained from the simulated design [46], whereas using a memristor of size 130 nm at a 1.2 V uniformity metric is equal to the 51.36% obtained from [22]. The highest value of the bit-aliasing metric using Memristor 130 nm at 1.2 V No. of memristor per transistor 5 is equal to the 54.763% obtained from [20], and the highest value of the reliability metric using FPGA Virtex-5 (XC5VLX110T) is equal to the 99.88% obtained from the design in [6].

5. DISCUSSION

This systematic review was conducted to highlight previously employed mechanisms that led to significant improvements in the field of hardware security, particularly within the domain of physical unclonable function (PUF) security. The methods employed varied due to differing viewpoints in terms of dealing with this technology. This research encompasses several approaches to architecture, some of which focus on PUF circuits, specifically the ring oscillator PUF (RO-PUF) and the arbiter PUF (A-PUF). After completing the design process for this circuit, the simulation or implementation process was conducted on several field-programmable gate arrays (FPGAs) to measure the performance metrics, as described in [1], [3], [5], [6], [23], [25], [26], [29], [32], [36], and [41].

Other studies have improved the architecture through the use of memristor technology with PUF circuits, showing noticeable improvements over previous techniques, as outlined in references [20], [22], [38]. The performance metrics were achieved in [20], with a uniqueness of 49.215%, uniformity of 54.560%, and bit-aliasing of 54.763%. Modifying the settings of the memristor-based APUF to increase variances is suggested. This enhancement improves the functionality of the PUF in terms of bit-aliasing, uniqueness, and uniformity while also increasing its resilience against support vector machine (SVM) attacks. Additionally, the objective is to prolong the time it takes for an attacker to replicate the circuit design. In another study [22], the performance metrics reached a uniqueness of 48.57%, uniformity of 51.43%, and bit-aliasing of 51.43%. A single series of RO pairs in the suggested memristor-based ROPUF produces a single multibit response. The range of a CRP set can be significantly increased via this technique without incurring significant circuit loss. The results demonstrate that the suggested memristor-based ROPUF possesses minimal response bias in the areas of uniqueness, uniformity, and bit-aliasing. Furthermore, the nature of the suggested memristor-based RO-PUF cannot be accurately modelled by SVM, rendering it immune to SVM threats [52]. Additionally, memristor technology was used in [38], which achieved high-security results for hardware, with performance metrics for uniqueness at 50.6%, uniformity at 52.5%, and bit-aliasing at 51.2%. Unlike CMOS-based PUFs, PUFs with a crossbar array architecture offer the advantages of a smaller device footprint and lower power consumption. Therefore, various memristor-based PUFs equipped with robust defenses against machine learning assaults are expected to be excellent choices for PUF-secure hardware systems.

The results indicate that the use of memristors improved the results. This is attributed to their properties that can create stability for the architecture being utilised. Thus, one of the most important research priorities is to focus on memristor technology and its mechanisms for use in the security field. This will enable the development of security devices with high capabilities and protection. Therefore, it is recommended that this memristor technology be implemented in various PUF circuits, which leads to the establishment of a strong, robust security system that is resistant to reverse engineering and has very high performance efficiency from both security and practical aspects, leading to significant improvements in hardware security.

6. CONCLUSION

A physical unclonable function (PUF) hardware, which does not require nonvolatile memory to extract differences across implementations and produce unique secret keys, is considered a potential security primitive in hardware security. The ring oscillator PUF (RO-PUF) is a simple tool that takes advantage of the frequency difference between two physically identical ring oscillators. However, if several reliable output bits are needed, many ROs need to be built. This research explores various possibilities encountered during the construction of a ring oscillator-PUF (RO-PUF) implemented on an FPGA. It provides alternative solutions for each identified issue. Additionally, the study explores methods to enhance the uniqueness, uniformity, and reliability of the three key performance indicators for the ring oscillator-PUF (RO-PUF) system on the basis of FPGA simulations. The analysis was generated via a large number of scientific studies that met specific criteria for inclusion. To significantly increase the security of devices on the basis of the findings of these investigations, the goal is to assess and compare these studies. Some studies have indicated that incorporating memristor technology into PUF circuits is a suggested technique for enhancing security services in this field by providing flexibility and adaptability in dealing with PUF circuits, as evidenced by the comparison of the results, which depicted a discernible improvement in security performance compared with similar research that did not involve memristors. Owing to the practical and theoretical properties of memristors and their positive effects, such as nonvolatile memory and circuit current control to maintain frequency uniformity in circuits, as for future research plans, the proposed architecture of the RO-PUF based on a memristor can be manufactured as a fingerprint device that provides a highly efficient security service and is also subject to further tests

and experiments to work in various surrounding conditions in terms of temperature and environmental factors so that it can provide a security system that is resistant to reverse engineering, which limits security breaches.

Conflicts of interest

The paper explicitly states that there are no conflicts of interest to disclose.

Funding

The acknowledgments section of the paper does not mention any financial support from institutions or sponsors.

Acknowledgement

The author acknowledges the support and resources provided by the institution in facilitating the execution of this study.

References

[1] M. Latha, A. Bazil Raj, and L. Abhikshit, "Design and Implementation of a Secure Physical Unclonable Function in FPGA," Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020, pp. 1083–1089, 2020, doi: 10.1109/ICIRCA48905.2020.9183101.

[2] H. Omotunde and M. Ahmed, "A comprehensive review of security measures in database systems: Assessing authentication, access control, and beyond," Mesopotamian Journal of Cyber Security, vol. 2023, pp. 115–133, 2023.

[3] S. Batabyal and A. Bazil Raj, "Design of A Ring Oscillator Based PUF with Enhanced Challenge Response Pair and Improved Reliability," 2019 4th IEEE International Conference on Recent Trends on Electronics, Information, Communication and Technology, RTEICT 2019 - Proceedings, pp. 1370–1374, 2019, doi: 10.1109/RTEICT46194.2019.9016894.

[4] B. Vivek, A. Arulmurugan, S. Maheswaran, S. Dhamodharan, A. Dharunash, and N. Gowtham, "Design and Implementation of Physical Unclonable Function in Field Programmable Gate Array," Proceedings of the 8th International Conference on Communication and Electronics Systems, ICCES 2023, pp. 152–158, 2023, doi: 10.1109/ICCES57224.2023.10192681.

[5] 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, doi: 10.1109/ACCESS.2020.3021205.

[6] J. Wen, M. Huang, Z. Chen, L. Zhu, S. Chen, and B. Li, "A Multi-Line Arbiter PUF with Improved Reliability and Uniqueness," 2019 IEEE 4th International Conference on Signal and Image Processing, ICSIP 2019, pp. 641–648, 2019, doi: 10.1109/SIPROCESS.2019.8868889.

[7] Y. Pang, B. Gao, B. Lin, H. Qian, and H. Wu, "Memristors for hardware security applications," Adv. Electron. Mater., vol. 5, no. 9, pp. 1–17, 2019, doi: 10.1002/aelm.201800872.

[8] R. Al-Amri, D. Hamood, and A. Farhan, "Theoretical background of cryptography," Mesopotamian Journal of Cyber Security, vol. 2023, pp. 7–15, 2023, doi: 10.58496/mjcs/2023/002.

[9] H. Ning, F. Farha, A. Ullah, and L. Mao, "Physical unclonable function: Architectures, applications and challenges for dependable security," IET Circuits, Devices and Systems, vol. 14, no. 4, pp. 407–424, 2020, doi: 10.1049/iet-cds.2019.0175.

[10] H. Abunahla and B. Mohammad, Memristor Technology: Synthesis and Modeling for Sensing and Security Applications, Springer International Publishing: Cham, Switzerland, 2018.

[11] R. Della Sala, D. Bellizia, and G. Scotti, "A novel ultra-compact fpga puf: The dd-puf," Cryptography, vol. 5, no. 3, 2021, doi: 10.3390/cryptography5030023.

[12] M. K. Ahmed, V. P. Yanambaka, A. Abdelgawad, and K. Yelamarthi, "Physical Unclonable Function Based Hardware Security for Resource Constraint IoT Devices," IEEE World Forum on Internet of Things, WF-IoT 2020 - Symposium Proceedings, pp. 8–9, 2020, doi: 10.1109/WF-IoT48130.2020.9221357.

[13] L. Bossuet and L. Torres, "Foundations of hardware IP protection," 2017, doi: 10.1007/978-3-319-50380-6.

[14] M. C. Martínez-Rodríguez, E. Camacho-Ruiz, P. Brox, and S. Sánchez-Solano, "A configurable ro-puf for securing embedded systems implemented on programmable devices," Electronics (Switzerland), vol. 10, no. 16, 2021, doi: 10.3390/electronics10161957.

[15] F. Amsaad et al., "Enhancing the performance of lightweight configurable PUF for robust IoT hardware-assisted security," IEEE Access, vol. 9, pp. 136792–136810, 2021, doi: 10.1109/ACCESS.2021.3117240.

[16] D. Das, B. Chatterjee, and S. Sen, "Security of analog, mixed-signal, and RF devices," In Emerging Topics in Hardware Security, Tehranipoor, M., Eds. Springer, Cham., 2021, doi.org/10.1007/978-3-030-64448-2_15.

[17] O. Krestinskaya, A. Irmanova, and A. James, "Memristors: Properties, models, materials," Springer International Publishing, vol. 14, 2020. doi: 10.1007/978-3-030-14524-8_2.

[18] I. Al-Mashhadani and S. Hadjiloucas, "Linearized Bond Graph of Hodgkin-Huxley Memristor Neuron Model," 15th International Workshop on Cellular Nanoscale Networks and their Applications, Dresden, Germany, CNNA 2016, pp. 1–2, 2016.

[19] N. Al-Khaboori and I. Al-Mashhadani, "Memristive physical unclonable functions: The state-of-the-art technology," International Journal of Safety and Security Engineering, vol. 13, no. 2, pp. 349–358, 2023.

[20] J. Teo, N. Hashim, A. Ghazali, and F. Hamid, "Configurations of memristor-based APUF for improved performance," Bulletin of Electrical Engineering and Informatics, vol. 8, no. 1, pp. 74–82, 2019, doi: 10.11591/eei.v8i1.1401.

[21] A. Yesil, F. Gül, and Y. Babacan, "Emulator circuits and resistive switching parameters of memristor," Memristor and Memristive Neural Networks, no. April, 2018, doi: 10.5772/intechopen.71903.

[22] J. Teo, N. Hashim, A. Ghazali, and F. Hamid, "Ring oscillator physically unclonable function using sequential ring oscillator pairs for more challenge-response-pairs," Indonesian Journal of Electrical Engineering and Computer Science, vol. 13, no. 3, pp. 892–901, 2019, doi: 10.11591/ijeecs.v13.i3.pp892-901.

[23] Z. Liu, W. Li, S. Li, and W. Wang, "A ring oscillator based physical unclonable function for hardware security on FPGA platform," vol. 13090, no. Iccais 2023, pp. 1–6, 2024, doi: 10.1117/12.3025809.

[24] M. Masoumi and A. Dehghan, "Design and implementation of a ring oscillator-based physically unclonable function on field programmable gate array to enhance electronic security," International Journal of Electronic Security and Digital Forensics, vol. 12, no. 3, pp. 243–261, 2020, doi: 10.1504/IJESDF.2020.108295.

[25] H. Kareem and D. Dunaev, "A robust architecture of ring oscillator PUF: Enhancing cryptographic security with configurability," Microelectronics J., vol. 143, no. July 2023, p. 106022, 2023, doi: 10.1016/j.mejo.2023.106022.

[26] J. Park, H. Yang, D. Lee, and H. Yoo, "Physical Unclonable Function Using Programmable Delay Lines," 2024 Int. Conf. Electron. Information, Commun. ICEIC 2024, 2024, doi: 10.1109/ICEIC61013.2024.10457091.

[27] E. Avaroğlu, "The implementation of ring oscillator based PUF designs in Field Programmable Gate Arrays using of different challenge," Physica. A.: Statistical Mechanics and its Applications, vol. 546, no. xxxx, p. 124291, 2020, doi: 10.1016/j.physa.2020.124291.

[28] R. Pramudita, S. Ramadhan, F. Hariadi, and A. Ahmad, "Implementation ring oscillator physical unclonable function (PUF) in FPGA," 2018 International Symposium on Electronics and Smart Devices, 2018, doi: 10.1109/ISESD.2018.8605475.

[29] E. Abulibdeh, H. Saleh, B. Mohammad, M. Al-qutayri, and A. Veeran, "Area and Power Efficient Implementation of Configurable Ring Oscillator PUF," 2024, doi: 10.36227/techrxiv.171207533.30573247/v1.

[30] A. Aguirre, M. Hall, T. Lim, J. Trinh, W. Yan, and F. Tehranipoor, "A systematic approach for internal entropy boosting in delay-based RO PUF on an FPGA," Midwest Symposium on Circuits and Systems, vol. 2020-Augus, pp. 623–626, 2020, doi: 10.1109/MWSCAS48704.2020.9184468.

[31] A. Chauhan, V. Sahula, and A. Mandal, "Novel randomized placement for FPGA based robust ROPUF with improved uniqueness," Journal of Electronic Testing: Theory and Applications (JETTA), vol. 35, no. 5, pp. 581–601, 2019, doi: 10.1007/s10836-019-05829-5.

[32] E. Abulibdeh, H. Saleh, B. Mohammad, M. Al-qutayri, and P. Santikellur, "Boosted PUF : Boosting Efficiency and Resilience in Configurable RO PUF for IoT Devices," 2024, doi: 10.36227/techrxiv.171172842.27972652/v1.

[33] K. Li, Y. Meng, J. Li, S. Wang, and J. Yang, "Research and design of a high-security configurable RO-PUF based on FPGA," Procedia. Comput. Sci., vol. 183, no. 2018, pp. 40–45, 2021, doi: 10.1016/j.procs.2021.02.028.

[34] H. Kareem and D. Dunaev, "Xilinx FPGA-based Ring Oscillator PUFs: Design Challenges and Solutions," 2022 11th Mediterranean Conference on Embedded Computing, MECO 2022, pp. 1–5, 2022, doi: 10.1109/MECO55406.2022.9797077.

[35] K. Zhou, H. Liang, Y. Jiang, Z. Huang, C. Jiang, and Y. Lu, "FPGA-based RO PUF with low overhead and high stability," Electron. Lett., vol. 55, no. 9, pp. 510–513, 2019, doi: 10.1049/el.2019.0451.

[36] Z. Mao, B. Li, L. Peng, and Y. Li, "Design and implementation of IDELAY-RO PUF in Xilinx ZYNQ PSoCs," IEICE Electron. Express, vol. 21, no. 6, pp. 1–6, 2024, doi: 10.1587/elex.21.20240013.

[37] F. Salem, "Authentication of Configuration Updates for Remote Field Programmable Gate Arrays with the use of Physical Unclonable Function," University of Victoria, 2023.

[38] W. Sun, J. Lee, D. Kim, and Y. Choi, "A Hardware Security Architecture : PUFs(Physical Unclonable Functions) using memristor," TENSYMP 2021 - 2021 IEEE Region 10 Symposium, pp. 1–4, 2021, doi: 10.1109/TENSYMP52854.2021.9550970.

[39] S. Basu, M. Kule, and H. Rahaman, "Symmetric Function Based Memristive Polimino PUF with Enhanced Security," Proceedings - 2020 6th IEEE International Symposium on Smart Electronic Systems, iSES 2020, pp. 143–146, 2020, doi: 10.1109/iSES50453.2020.00040.

[40] K. Devika and R. Bhakthavatchalu, "FPGA implementation of programmable Hybrid PUF using Butterfly and Arbiter PUF concepts," J. Phys. Conf. Ser., vol. 2312, no. 1, pp. 0–7, 2022, doi: 10.1088/1742-6596/2312/1/012033.

[41] N. Anandakumar, M. Hashmi, and M. Chaudhary, "Implementation of efficient XOR Arbiter PUF on FPGA with enhanced uniqueness and security," IEEE Access, vol. 10, no. December, pp. 129832–129842, 2022, doi: 10.1109/ACCESS.2022.3228635.

[42] J. Kim, H. Jo, K. Jo, S. Cho, J. Chung, and J. Yang, "Reliable and Lightweight PUF-based Key Generation using Various Index Voting Architecture," Proceedings of the 2020 Design, Automation and Test in Europe Conference and Exhibition, DATE 2020, pp. 352–357, 2020, doi: 10.23919/DATE48585.2020.9116519.

[43] Z. Wei, Y. Cui, Y. Chen, C. Wang, C. Gu, and W. Liu, "Transformer PUF : A Highly Flexible Configurable RO PUF Based on FPGA," IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation, vol. 2020-Octob, pp. 20–25, 2020, doi: 10.1109/SiPS50750.2020.9195259.

[44] V. Tran, Q. Trinh, and V. Hoang, "Stabilizing On-chip Secure Key Generation Using RO-PUF," International Conference on ICT Convergence, vol. 2021-Octob, pp. 805–809, 2021, doi: 10.1109/ICTC52510.2021.9621147.

[45] L. Yao, H. Liang, Z. Huang, C. Jiang, M. Yi, and Y. Lu, "A Lightweight Configurable XOR RO-PUF Design Based on Xilinx FPGA," 2021 IEEE 4th International Conference on Electronics Technology, ICET 2021, no. 62027815, pp. 83–88, 2021, doi: 10.1109/ICET51757.2021.9451016.

[46] N. Sivasankari and A. Muthukumar, “Implementation of a hybrid ring oscillator physical unclonable,” vol. 1680, no. July, pp. 602–607, 2018, doi: 10.21917/ijme.2018.0104.

[47] N. Anandakumar, M. Hashmi, and S. Sanadhya, “Design and analysis of FPGA-based PUFs with enhanced performance for hardware-oriented security,” ACM J. Emerg. Technol. Comput. Syst., vol. 18, no. 4, 2022, doi: 10.1145/3517813.

[48] M. Usmani, S. Keshavarz, E. Matthews, L. Shannon, R. Tessier, and D. 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, 2019, doi: 10.1109/TVLSI.2018.2877438.

[49] A. Herkle, H. Mandry, J. Becker, and M. Ortmanns, “In-Depth Analysis and Enhancements of RO-PUFs with a Partial Reconfiguration Framework on Xilinx Zynq-7000 SoC FPGAs,” Proceedings of the 2019 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2019, pp. 238–247, 2019, doi: 10.1109/HST.2019.8740832.

[50] A. Chauhan, V. Sahula, and A. Mandal, “Novel Randomized & Biased Placement for FPGA Based Robust Random Number Generator with Enhanced Uniqueness,” Proceedings - 32nd International Conference on VLSI Design, VLSID 2019 - Held concurrently with 18th International Conference on Embedded Systems, ES 2019, pp. 353–358, 2019, doi: 10.1109/VLSID.2019.00079.

[51] M. Sheela, D. Hemanand, and V. Reddy, “Cyber Security System Based on Machine Learning Using Logistic Decision Support Vector,” Mesopotamian J. CyberSecurity, vol. 2023, pp. 64–71, 2023, doi: 10.58496/MJCS/2023/011.

[52] A. Ketab, and N. El Abbadi, “LipPrint : Using Lip Movements as a Silent Password,” Mesopotamian J. CyberSecurity, vol. 4, no. 2, pp. 74–87, 2024, doi: 10.58496/MJCS/2024/008.