Advancing Hardware Security: A Review and Novel Design of Configurable Arbiter PUF with DCM-Induced Metastability for Enhanced Resource Efficiency and Unpredictability

Lukram Dhanachandra Singh[1,3], Preetisudha Meher[2]
[1]Department of Electronics and Communication Engineering, NIT Arunachal Pradesh
[2]Department of Electronics and Communication Engineering, NIT Arunachal Pradesh
[3]Department of Electrical Engineering, NIT Manipur

Abstract

As the Internet of Things (IoT) and Blockchain technologies continue to assert their dominance in the technical landscape, the demand to enhance security measures becomes foremost. In this context, Physical Unclonable Functions (PUFs) are widely used hardware security primitives that can be used to solve a wide range of security issues. To support hardware security solutions, this paper presents an extensive overview and analysis of the existing Physical Unclonable Functions (PUFs) used as True Random Number Generators (TRNGs). Recognizing the shortcomings of current PUF designs, we propose a configurable Arbiter PUF design employing Digital Clock Manager (DCM)-induced metastability as an entropy source, presenting a robust solution for evolving hardware security. To mitigate the adverse consequences of metastability, the proposed Arbiter PUF includes a Carry Chain primitive with four Flip-Flop clones. Acknowledging the constantly evolving IoT and Blockchain environment, the suggested configurable Arbiter PUF is made to satisfy the highest security standards. By exploiting the inherent variations in FPGA technology, we aim to reduce system resource and area consumption, aligning with the efficiency criteria of modern applications. The system's performance is additionally enhanced by an on-chip post-processing based on DSP. Simulation results demonstrate successful implementation on a Xilinx Basys-3 FPGA board, offering a scalable and efficient solution. The generated sequences of the proposed PUF undergo rigorous testing, including National Institute of Standards and Technology (NIST) statistical tests for uniqueness, reliability, and randomness. This holistic approach aims to improve the PUF's performance and security.

Keywords: physical unclonable function, FPGA, IoT, configurable arbiter PUF, hardware security, TRNG.

1. Introduction

In today's world, with the development of technology, people have started more depending on electric circuits. For example, online transactions, sharing data from one person to another person, electronic data transfer from one place to another place, etc. Like this, people start using electronic systems in various ways. Developing such electronic system technologies, more threat comes out rapidly. Even the IoTs and Blockchain which are also becoming an emerging technology, need better security [1],[2],[3]. So, the researchers are doing more research on hardware security to detect and prevent such threats enhancing the security. In the realm of hardware security, the invention of true random numbers is essential to withstand several types of malicious assaults. The development of Physical Unclonable Functions (PUFs) has shown promise in producing True Random Number Generators (TRNGs) [4]. PUFs make each device unique and unpredictable by taking advantage of the inherent physical variations that occur during the fabrication process of integrated circuits. A TRNG is an essential part of secure communication protocols, key generation, and cryptographic systems. TRNGs, as opposed to pseudorandom number generators (PRNGs), generate unbiased and unpredictable sequences, which is essential for ensuring the reliability of cryptographic systems. PUFs are a kind of TRNGs that have drawn interest because of their intrinsic robustness to environmental changes and modeling attacks.

Arbiter PUFs represent a popular class of PUFs, which depends on variations in time delays in digital circuits. The fundamental concept is a race condition between two paths, where the delays induced on each path determine the result. This generates a response that is unique and challenging to recreate while delivering a secure means to produce random numbers. We choose the Arbiter PUF over other PUF architectures because of its robustness against different types of attacks, simplicity of use, and ease of implementation [5].

This article presents a novel configurable Arbiter PUF architecture, inspired by the need for enhanced reliability and security in PUF-based TRNGs. We contribute an alternative perspective to the field by using the metastability triggered by Digital Clock Managers (DCM) as an entropy source. In digital systems, metastability is usually an undesirable phenomenon because it can result in unpredictable behavior and be risky. On the other hand, researchers may investigate the deliberate manipulation of metastability for the development of unique identifiers in the context of a PUF. To mitigate the potential consequences of metastability, our approach incorporates a Carry Chain primitive consisting of four Flip-Flop duplicates. This improves the overall performance by guaranteeing improved phase shift resolution adjustment at the destination. The inclusion of the on-chip post-processing method using single Digital Signal Processing (DSP) slice of FPGA also improves the TRNG's overall reliability and performance.

This work focuses on the comprehensive analysis of the proposed Arbiter PUF, covering simulation results, implementation on a Xilinx Basys-3 FPGA board, and validation through NIST randomness tests for Challenge-Response Pairs or sequences generated. Hamming Distance is used to calculate uniqueness and reliability. This paper is further divided into four sections, namely existing PUF designs and related works, the proposed methodology which explains on improvement of the existing design, and then the implementation, result analysis, and discussion. The last section will give the conclusion and discuss the outline of future directions for this study, including the use of AI and machine learning methods to improve and further optimize PUF-based TRNG performance. The knowledge gained from the review offers new opportunities to advance hardware security solutions.

2. Literature Review on existing PUF-based RNGs and related work

If we recall the background of hardware security, we found that the Codebreakers [6], written by David Kahn in 1967, was a history of cryptography from the time of ancient Egypt to the present. Its examination of the development of security led to its publication. Following that, many concepts for securing computing, information flow, operating systems, etc. were put out in the 1970s. The National Bureau of Standards created the Data Encryption Standard (DES) in 1997 and Triple DES [7] was developed in 1998, which employs the DES algorithm three times to encrypt each block. After this Triple DES, various hardware security concepts were produced. A system for verifying user identity and authorization of the point of sale or access: Personal Identification systems using authentication channels were developed by Simmons with an application of two-key cryptography [8]. After this, researchers start to focus on the identification of data devices, documents, and individuals [9]. The physical one-way function (POWF) was developed by Pappu and Recht and gives authentication protocols according to the physical characteristic function [10]. It physically converts the medium's microstructure to a fixed-length string of binary digits that are used to distribute and authenticate unique identifiers rather than depending on number theory.

In 2002, the phrase Physical Unclonable Functions (PUF) was first used in Silicon Physical Random Functions. It is a process for recognizing and authenticating individual integrated circuits (ICs). PUFs are physical structures with a distinct challenge-response behavior that is dependent on inescapable manufacturing variances. PUFs have the advantage of being unclonable, which means that not even the original maker can create a similar device or product. The ability to construct PUFs in such a way that active tampering affects the physical structure and subsequently destroys the related secret is another advantage above standard security modules. This can be viewed as a defense mechanism against invasive attacks. The concept of PUF was first proposed by Pappu in [10]. It was followed by other kinds of PUF which fall into four categories [11]: Non-electronic PUF, Analog electronic PUF, Memory-based intrinsic PUF, and Delay-based intrinsic PUF. Non-electronic PUFs mainly include Optical PUF [11], Paper PUF [12], and CD PUF [13]. Analog electronic PUFs mainly include Coating PUF [14], LC-PUF (like Coating PUFs), Threshold voltage-based PUF, and Impedance-based PUF. The Memory-Based intrinsic PUF mainly includes Static RAM PUF (SRAM PUF) [15] and Butterfly PUF [16]. The SRAM PUF consists of many memory units. The Delay-based intrinsic PUF is currently the hottest research topic.

A delay-based PUF [17] was described utilizing the look-up table and multiplexer intrinsic FPGA structure, and it was fully implemented on 28nm FPGAs with great reliability and uniqueness providing IP Protection. A comprehensive exploration of the security landscape of Physical Unclonable Functions (PUFs) is presented [18], delving into the fundamental question of PUF security and its impact on security applications and protocols. By examining the evolution of PUFs and their integration into hardware implementation research, the study offers insights into the advancements spurred by nanotechnologies and the exploration of disorder-based physical phenomena, presenting a retrospective analysis of challenges and solutions in the continuous development of PUFs. An efficient reliable PUF-Based cryptographic key generator in 65nm CMOS with an integrated self-test was described in [19] which includes Error-correcting codes (ECC) approaches providing high space, power, and delay overheads and are sensitive to information leakage when used to increase response dependability. To assess the dependability of PUF bits, a highly reliable PUF-based cryptographic key generator Secure Split Test Techniques to prevent IC piracy for IoT devices, claiming that SSTF and PUF-based SSTF (PUF-SSTF), which is appropriate for ICs intended for usage in smartphones and IoT devices, is available [20]. PUFs have been suggested for usage in IC anti-counterfeiting, device identification, and authentication [Majzoobi and Koushanfar 2011] [21], tying hardware to software platforms [Kumar et al. 2008][16], secure storing of cryptographic secrets [Yu et al. 2011] [22], keyless secure communication [Ruhrmair 2012] [23], and other applications. Another paper on PUF as an anti-counterfeiting, key distribution, and storage was published [24]. FPGA intrinsic PUFs [25] were also developed for IP protection. Reverse engineering and prevention techniques for PUFs using side channels [26] were also proposed. Similarly [27] is also about Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching. And many more kinds of research were done on PUF to solve most of the hardware security issues.

PUFs are also classified as Strong PUFs and Weak PUFs. Strong PUFs are those that have a sufficiently vast challenge space to make complete enumeration of its CRP set impossible and are the PUFs of choice in most real-world security applications. On the other hand, weak PUFs only permit the application of a limited number of challenges. Several strong PUF-based authentication protocols have been proposed in the past, such as Controlled PUFs [Gassend et al. 2002][28], Noisy PUFs [Ozturk et al. 2008][29], Logically Reconfigurable PUFs (LRPUF) [Katzenbeisser et al. 2011][30], Slender PUFs [Majzoobi et al. 2012][31], Converse PUF-based Authentication [Koc¸abas et al. 2012][32] etc. However, several serious security and usability problems with the aforementioned protocols were revealed in [Delvaux et al. 2014][33]. These protocols raise mostly the following issues: Issues with synchronization, replay attacks, impersonating tokens or servers, constrained attack models, and scalability. Another privacy-preserving authentication scheme based on SRAM PUF was recently presented in [Aysu et al. 2015][34]. However, we are unable to immediately implement this protocol since the SRAM PUF has been demonstrated to be physically unclonable [Helfmeier et al. 2013][35].

The first Si PUF [36] was confirmed on an FPGA and is known as an Arbiter PUF; where from the variation of delay between two undistinguishable symmetrical pathways, it recovers the chip signature. The arbiter PUF (A-PUF) is a popular PUF architecture because it consumes fewer hardware resources than RO-PUF and has a larger challenge-response area than memory-based PUFs.

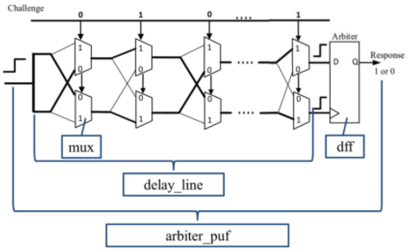


Figure 1. Conventional Arbiter PUF

The Arbiter-PUF whose architecture is shown in Figure 1, has been used as the underlying block in more elaborate PUF architectures such as the feed-forward arbiter PUF, lightweight PUF, and XOR PUF as a well-known delay-based PUF. However, the FPGA version of the conventional A-PUF has low reliability, owing to the delay flip-flop (DFF) arbiter's metastability and the FPGA's routing limitations. Scalability challenges arise because Ring Oscillator (RO) and Arbiter-based PUF cannot be implemented directly in the next generation of FPGAs.

Lightweightness, unpredictability, unclonability, and originality are desired PUF characteristics (concerning each instance) [38], [39]. So, many other PUFs such as switched-capacitor PUF, DRAM PUF, Hybrid Oscillator Arbiter PUF, Bistable ring PUF, XOR Arbiter PUF, Dual Arbiter PUF [4], and many other modifications of mentioned PUFs have been proposed [18] as designs of various pseudorandom or true random number generators.

Various research was done on these random number generators and for the application of hardware security solutions, PUF designs are used to generate pseudo-random numbers (PRNGs) and true random numbers (TRNGs) [37,41]. From time to time, they have been modified for better performances such as scalability, uniqueness, reliability, randomness, linearity, etc. [Maes et al. 2009] have presented an error-correcting circuit with a very low hardware overhead to minimize the uncertainty and vagueness of the PUF's responses and make it more resistant and safer [15]. This was done to make it reliable and to have complete entropy. A Processor-Based Strong PUFs With Aging-Based Response Tuning was proposed [40] with an algorithm that takes advantage of deliberate post-silicon aging to adjust the variation in inter- and intra-chip signatures.

In between some have worked on and proposed various ways to enhance the PUF properties like in [42] a reconfigurable arbiter PUF that replaces a 2x2 switch block with a 4X4 switch block making regular key updates possible with a long-term secret key. As the development of PUF performance is a challenging one, many researchers have concluded that dual-mode PUF has better performances than the prior ones and many designs were proposed in [43], they designed a dual-mode PUF introducing a feedback structure performing bitwise XOR of the challenge and its response and use it as input to challenge the PUF, the reconfigurable RO PUF can act as a RO PUF or a bistable ring PUF confusing the attacker. Another arbiter-PUF architecture was also put out [45], using other arbiter-PUFs to obscure part of the challenge bits. This approach hides the challenge obfuscation scheme itself while also reducing the modeling accuracy. An innovative filtering technique was used in [44] Dual Arbiter PUF design to estimate the delay difference between the signals with which they filter out faulty outputs and significantly lower the BER of the PUF.

In recent studies of entropy sources for Physical Unclonable Functions (PUFs) [49] and True Random Number Generators (TRNGs) [46], diverse techniques like jitter [47,48] and metastability have been explored. Notably, metastability has gained prevalence due to its reliability and effectiveness, prompting its frequent utilization in contemporary research endeavours [50,51]. One notable advancement involves leveraging Digital Clock Managers (DCMs) to induce metastability [52], as they offer precise control over clocking elements, ensuring a stable and consistent source of entropy. Additionally, recent innovations, such as the Dynamically Configurable PUF and Dynamic Matching Authentication Protocol, have demonstrated robust resistance against sophisticated machine learning-based attacks. Drawing inspiration from these advancements, this work proposes the design of a Configurable Arbiter PUF with DCM-induced metastability, strategically aiming to enhance resource efficiency and unpredictability while addressing hardware and power constraints.

3. Proposed Methodology

A Digital Clock Manager (DCM) is a crucial component of digital systems and Field Programmable Gate Arrays (FPGAs). It is responsible for producing stable clock signals, flexible clock domain control, and phase-locked loops (PLLs). Even while DCMs are often designed to avoid metastability, in our proposed system design, we exploit it by analyzing different configuration options with proper handling of clock management in FPGA designs.

To Reduce hardware complexity and the number of digital logics used, the proposed design strategically employs a single configurable arbiter PUF with a solitary delay line, unlike dual arbiter PUF which involve the intricate coordination of two arbiter structures and associated delay lines, which is important in resource-constrained environments like the Internet of Things and FPGA applications.

The methodology involves truncating the original APUF to generate multiple responses and XORing them to derive a 1-bit final response. This design allows for various ways to choose the branch signal. Utilizing a group of Multiplexers (MUXs), we can select different combinations, and the signals selected by the MUXs, termed configuration signals, which will be the DCM-inducing metastability. This dynamic utilization of DCM strengthens our PUF's resilience and offers a reliable source of entropy. Furthermore, the incorporation of a carry chain including four flip-flops that can easily fit into a single slice removes the requirement for routing between XOR gates and flip-flops. This improves the overall performance by guaranteeing improved phase shift resolution adjustment at the destination while also simplifying the design.

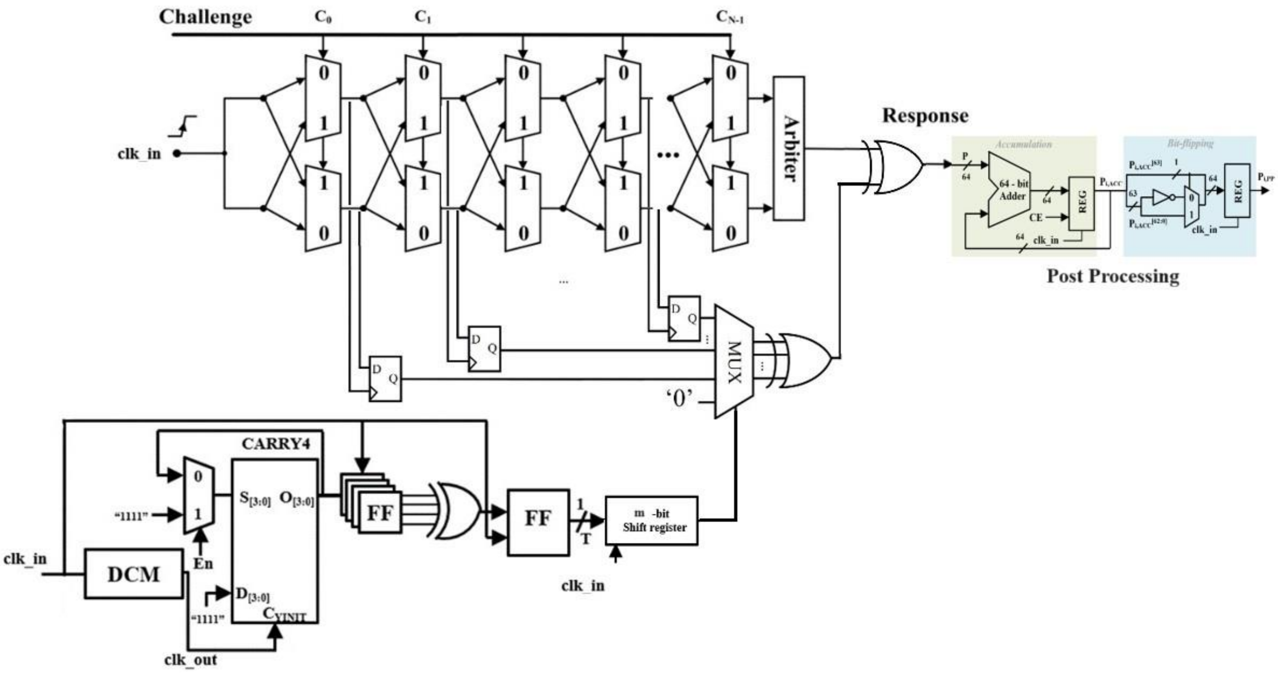


Figure 2. The architecture of the proposed configurable Arbiter PUF with post-processing

A comparable structure is created by adding a '0' signal to the MUX signal options to preserve compatibility with conventional APUF structures. Crucially, only a small amount of extra hardware—an arbiter, a MUX, and an XOR gate—is needed to add a branch. This architecture turns out to be far more resource-efficient than the conventional Arbiter PUF structure.

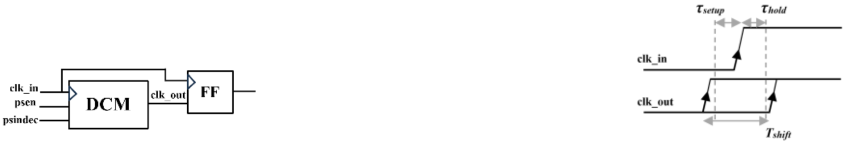


Figure 3. DCM with FF & T_{shift} in clock signal

We take advantage of the Dynamic Phase Shifting (DPS) capability to create metastability in one or more Flip-Flops (FFs). When psen is asserted high, this dynamic configuration starts and automatically modifies the DCM's phase shift. As soon as Clk_in and Clk_out get close to the FF inputs, the random sequence generation starts, breaking the FF setup/hold time constraints and pushing the FF into the metastable region.

We employ the DCM phase shift to resolve differences in routing delays caused by different routing patterns. However, the DCM's phase shift resolution might not be accurate enough. To get over this restriction, we suggest a unique application of the carry-chain primitive in FPGA slices along with a programmable feedback loop to increase unpredictability. By avoiding the metastability region, this method allows for more accurate phase shift resolution correction at the destination.

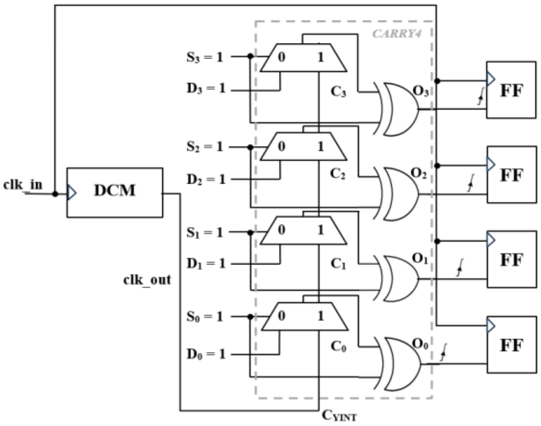


Figure 4. Carry chain with four FF copies

Routing between flip-flops and XOR gates is obviated by consolidating the CARRY4 primitive and the four flip-flops into a single slice. This consolidation greatly increases the efficiency and unpredictable nature of the system by allowing us to concentrate just on the propagation delays of multiplexers in the carry chain.

Thus, the signal generated by DCM that will induce metastability to the PUF acts as a configuration signal that will stock up to m-bits in the shift register, then this random metastable induced m-bit signal will configure the MUX, and its output will XORed with that of the arbiter PUF. Generating single-bit response at a time.

To further optimize our design, we implement on-chip post-processing, making use of an FPGA's single DSP slice. Remarkably, this addition does not compromise the bit production rate, ensuring both the speed and effectiveness of the process. Through their integration into a single arbiter PUF, we can achieve an acceptable balance between hardware efficiency and security robustness. This simplified method provides the way for a resource-efficient and scalable solution that is specifically intended to meet the demands of blockchain and Internet of Things technologies. We demonstrate a feasible way forward for hardware security solutions with our upgraded configurable Arbiter PUF design with DCM-induced metastability, which combines unique aspects to optimize resource utilization, improve phase shift resolution, and boost unpredictability.

4. Design and Hardware Implementation

The design process involves utilizing the Xilinx Vivado High-Level Synthesis tool for logic synthesis and floor planning. Subsequently, the design is implemented on a MicroBlaze System, benefitting from its connection automation that generates local memory with user-defined size and configurable caches. Various peripherals, including AXI Interconnect, MicroBlaze Debug Module, Interrupt Controller, processor System Reset, and a clock source, are integrated, and connections are established as per specific requirements.

The Artix 7 FPGA Board, Xilinx Basys 3 (XC7A35T-ICPG236C), features 5200 logic slices, each of which has four 6-input LUTs and eight flip-flops. 90 DSP slices are also there in it. Clock speeds that exceed 450MHz. There are also five clock management tiles, each of which has a phase-locked loop (PLL). On a Xilinx Basys 3 FPGA, the suggested DAPUF with DCM-based system design has been implemented. The Xilinx SDK tool is used to design an application that is implemented after the Basys-3 board is connected to a laptop. In Figure 5, the experimental setup is shown. And figure 6 presents the simulation diagram of the system.

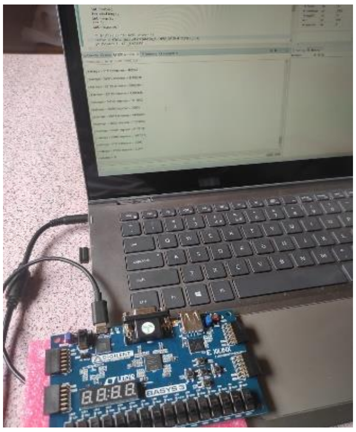


Figure 6. Experimental Set up

In the floor planning phase, a portion of the design is dedicated to the Configurable Arbiter PUF, determining the module's size as the smallest possible, as depicted in Figure 7. Manual placement of the Arbiter PUF and MicroBlaze system is conducted to define the optimal locations of these modules, as illustrated in Figure 8, along with an enlarged view. This meticulous floor planning and routing are pivotal steps, imposing constraints to minimize the FPGA's occupied area and reduce power consumption.

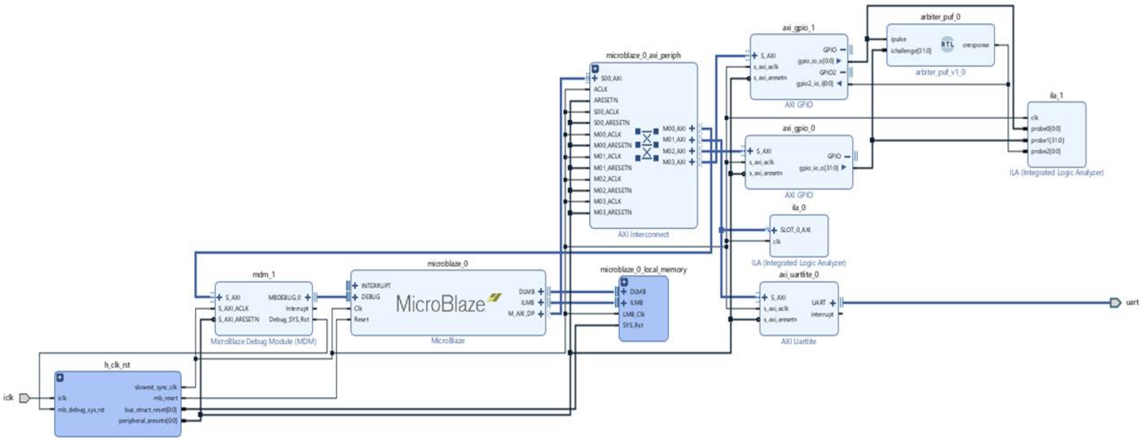


Figure 5. Simulation diagram of the entire system

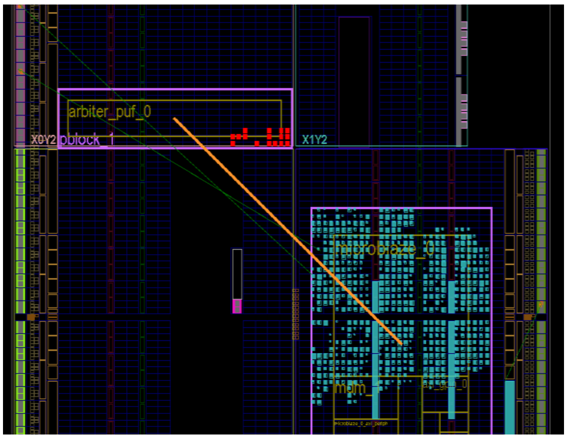


Fig. 7 Floorplanning

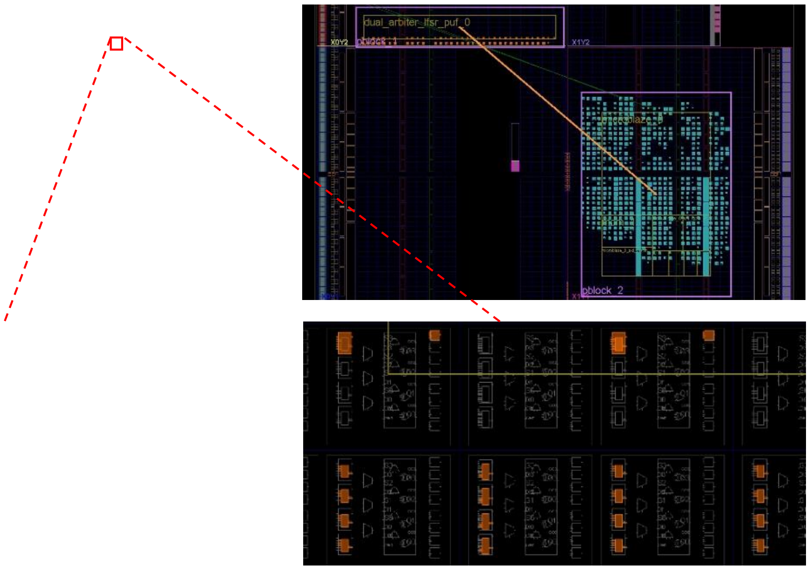


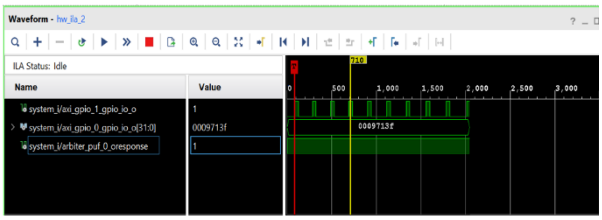
Fig. 8 Placement and its enlarged view

A thorough simulation of the complete system is carried out after it has been implemented on the FPGA board to obtain an understanding of the behavior of the metastable RO PUF. The responses are examined in a variety of settings to make sure that the system demonstrates the necessary degrees of uniqueness and randomness.

The National Institute of Standards and Technology (NIST) tests and other statistical metrics and testing methodologies are used to characterize the performance of the metastable RO PUF. These assessments guarantee that the answers exhibit a sufficient degree of originality and dependability.

5. Result Analysis

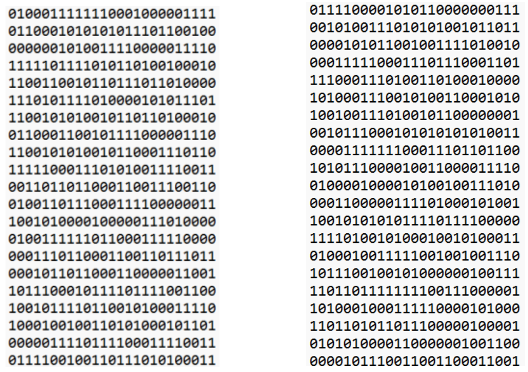
Upon loading the generated bitstream of the designed system onto the hardware via a computer, the software or application is run through the Xilinx SDK tool to produce pseudorandom sequences known as challenge-response pairs (CRPs). The inbuilt Logic Analyzer in the block design is used to view the waveforms of these CRPs, or the created pseudorandom sequences. This makes an extra oscilloscope is unnecessary and offers a practical and effective way to observe. This experimental step makes sure the system works as planned, producing pseudorandom sequences in response to predetermined challenges. The waveforms are generated as shown in Figure 9 (a part) and analyzed with the use of the Integrated Logic Analyzer, which helps validate the system's overall functionality. Figure 10 represents some samples of the generated binary sequences i.e. responses of the proposed configurable Arbiter PUF.


Waveform - hw_ila_2

ILA Status: Idle

Name	Value
system_i/axi_gpio_1_gpio_io_o	1
system_i/axi_gpio_0_gpio_io_o[31:0]	0009713f
system_i/arbiter_puf_0_oresponse	1

Fig. 9 Waveforms of CRPs recorded from ILA



```
0100011111110001000001111    0111100001010110000000111
0110001010101011101100100    0010100111010101001011011
0000001010011110000011110    0000101011001001111010010
1111101111010110100100010    0001111100011101110001101
1100110010110111011010000    1110001110100110100010000
1110101111010000101011101    1010001110010100110001010
1100101010010110110100010    1001001110100101100000001
0110001100101111000001110    0010111000101010101010011
1100101010010110001110110    0000111111100011101101100
1111100011101010011110011    1010111000010011000011110
0011011011000110011100110    0100001000010100100111010
0100110111000111100000011    0001100000111101000101001
1001010000100000111010000    1001010101011110111100000
0100111111011000111110000    1111010010100010010100011
0001110110001100110111011    0100010011111001001001110
0001011011000110000011001    1011100100101000000100111
1011100010111101111001100    1101101111111100111000001
1001011110110010100011110    1010001000111110000101000
1000100100110101000101101    1101101011011100000100001
0000011110111100011110011    0101010000110000001001100
0111100100110111010100011    0000101110011001100011001
```

Figure 10. Generated Binary Sequences as Responses

The utilization of the area by the design of the whole system is given in Figure 11. The utilization of the area by LUT is only 25% and it is 17% only for Flip Flops which are relatively less compared to other PUF-based pseudorandom generators. Area complexity of the proposed configurable arbiter PUF can be obtained from equation 1 as the proposed architecture has twice the delay line of 64 pairs of multiplexers, a flip flop for each delay line, and one XOR gate.

$$\text{Area} = 256\ (A_{\text{MUX}}) + 2\ (A_{\text{FF}}) + A_{\text{XOR}} \qquad (1)$$

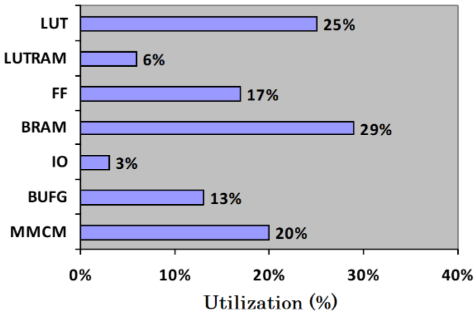
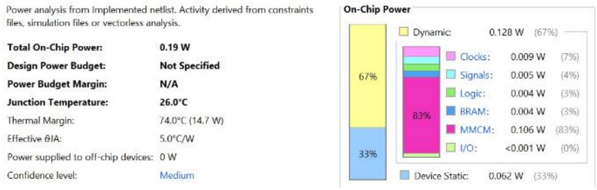


Fig. 11 The utilization of Area in FPGA

The proposed configurable arbiter PUF including DCM and post-processing unit (excluding the Microblaze system) exploits only 196 LUTs, 62 FFs, and 1 DSP i.e. less hardware area complexity thanks to FPGA technology. It also improves hardware security because it passes every NIST test.

The power analysis from the implemented netlist as provided by Xilinx vivado after the implementation and generation of the responses is found to be 0.19 W as shown below in Figure 12.



Power analysis from Implemented netlist. Activity derived from constraints files, simulation files or vectorless analysis.

Total On-Chip Power:	**0.19 W**
Design Power Budget:	**Not Specified**
Power Budget Margin:	**N/A**
Junction Temperature:	**26.0°C**
Thermal Margin:	74.0°C (14.7 W)
Effective θJA:	5.0°C/W
Power supplied to off-chip devices:	0 W
Confidence level:	Medium

On-Chip Power

Dynamic:	0.128 W	(67%)
Clocks:	0.009 W	(7%)
Signals:	0.005 W	(4%)
Logic:	0.004 W	(3%)
BRAM:	0.004 W	(3%)
MMCM:	0.106 W	(83%)
I/O:	<0.001 W	(0%)
Device Static:	0.062 W	(33%)

Fig. 12 Power Analysis

Randomness is one of the most important features to check for when identifying whether a number or sequence was generated by a generator or a PUF design. That suggests that the generated number could be easily assessed by an attacker. The National Institute of Standards and Technology created the NIST test, a statistical test battery, to assess random and pseudorandom number generators for use in cryptography applications. This test is carried out to analyze the designed generator. The NIST test employs fifteen distinct statistical tests to confirm the resulting sequence's unpredictability. Thus, we collect 10^6 bits of sequences, more than 100 times as it is required to go for the NIST test which is a standard test suite for testing the uniqueness, and randomness of the generated sequences.

Table 1. NIST test result of our proposed PUF

Statistical Tests	**Pass / Fail**	**Statistical Tests**	**Pass / Fail**
Frequency	Pass	Non-overlapping Templates	Pass
Block Frequency (m = 64)	Pass	Random Excursions (x = +1)	Pass
Cumulative sum-Forward	Pass	Approximate Entropy	Pass
Cumulative sum-Reverse	Pass	Overlapping Templates	Pass
Runs	Pass	Universal	Pass
Long Runs of Ones	Pass	Random Excursions Variant (x = -1)	Pass
Rank	Pass	Serial	Pass
DFT	Pass	Linear Complexity (M = 100)	Pass

The test result is shown in Table 1 and the proposed system passed all the NIST standard tests providing the required randomness.

6. Conclusion and Discussion

In conclusion, the presented work introduces a novel Configurable Arbiter PUF design with DCM-induced metastability, leveraging advancements in entropy sources and addressing the critical issues of hardware efficiency and unpredictability. The use of metastability induced by Digital Clock Managers demonstrates precision and reliability, aligning with recent trends in PUF and TRNG research. Compared to existing PUFs, the proposed dual arbiter PUF using LFSR (just 196 LUTs, 62 FFs, and 1 DSP) has less hardware area complexity thanks to FPGA technology. It also improves hardware security because it passes every NIST test.

Looking ahead, future research directions hold promising opportunities for enhancing the robustness of hardware security solutions. Firstly, the incorporation of Built-In Self-Test (BIST) mechanisms presents a valuable avenue. A bit-self-test (BST) arbitrary PUF high reliability and uniqueness was presented with delay detection and automatically it selected the reliable resources at a normal temperature [45]. BIST provides autonomous testing capabilities, offering advantages in diagnosing and identifying potential issues within the PUF system, ensuring continuous reliability.

Moreover, the integration of AI algorithms emerges as a transformative approach to further improve system performance. AI algorithms can play a pivotal role in error correction, post-processing, and configuration optimization. By leveraging AI knowledge, the system can adapt dynamically, enhancing its resilience against evolving threats and mitigating the impact of external factors. Several researchers have already implemented AI, Machine Learning (ML), and Deep Learning techniques on PUFs and TRNGs [54, 55]. These applications demonstrate the feasibility and efficacy of using intelligent algorithms to optimize performance, detect anomalies, and enhance the overall security of hardware systems. Further research and exploration in these directions hold the potential to shape the future landscape of hardware security with increased efficiency and robustness.

References

[1] W. Liu, L. Zhang, Z. Zhang, C. Gu, C. Wang, M. O'Neill, and F. Lombardi, "XOR-based Low-cost Reconfigurable PUFs for IoT Security," ACM Transactions on Embedded Computing Systems (TECS), vol. 18, no. 3, pp. 1-21, Apr. 2019.

[2] M. Barbareschi et al., "A PUF-based mutual authentication scheme for cloud-edges iot systems," Future Generation Computer Systems, vol. 101, pp. 246–261, 2019.

[3] L. D. Singh and P. Meher, "A Novel Approach on Advancement of Blockchain Security Solution," Advances in Intelligent Systems and Computing, pp. 449–456, 2020, doi: 10.1007/978-981-15-1451-7_48.

[4] Singh, L. D., Meher, P., & Panda, A. K. (2023). Dual Arbiter PUF with Shift Register Based TRNG on Basys-3 FPGA Board and its Performance Analysis on Uniqueness, Reliability, and Randomness. International Journal of Intelligent Systems and Applications in Engineering, 12(1s), 51 – 60. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/3394

[5] S. S. Zalivaka et al., "Reliable and modeling attack resistant authentication of arbiter puf in fpga implementation with the trinary quadruple response," IEEE Transactions on Information Forensics and Security, vol. 14, no. 4, pp. 1109–1123, 2019.

[6] David Kahn , "The Codebreakers – The Story of Secret Writing" (ISBN 0-684-83130-9), 1967.

[7] "Data Encryption Standard (FIPS PUB) 46-3", National Institute Standards and Technology, Gaithersburg, MD, 1999.

[8] G. Simmons, "A system for verifying user identity and authorization at the point-of sale or access," Cryptologia, vol. 8, no. 1, pp. 1–21, 1984.

[9] G. Simmons, "Identification of data, devices, documents and individuals," in IEEE International Carnahan Conference on Security Technology, 1991, pp. 197–218.

[10] Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. "Physical one-way functions". Science. 297 (5589): 2026–2030. 2001

[11] R. Maes, I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in Towards Hardware-Intrinsic Security, ser. Information Security and Cryptography, Springer, 2010: 3-37.

[12] P. Bulens, F. X. Standaert, J. J. Quisquater, "How to strongly link data and its medium: the paper case," IET Information Security, 2010, 4(3): 125-136.

[13] G. Hammouri, A. Dana, B. Sunar, "CDs have fingerprints too," In Proc. CHES, Lausanne, Switzerland, 2009: 348-362.

[14] P. Tuyls, G. J. Schrijen, B. Koric, et al. "Read-proof hardware from protective coatings," in Proc. CHES, Yokohama, Japan, 2006: 369-383.

[15] MAES, R., TUYLS, P., AND VERBAUWHEDE, I. 2009. Low-overhead implementation of a soft decision helper data algorithm for SRAM pufs. In Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings. 332–347.

[16] S. Kumar, J. Guajardo, R. Maes, et al., "The butterfly PUF: protecting IP on every FPGA," in Proc. HOST, Anaheim, USA, 2008: 67-70.

[17] Jiliang Zhang et,al, "Design and Implementation of a Delay-Based PUF for FPGA IP Protection," International Conference on Computer-Aided Design and Computer Graphics - 2013.

[18] C. H. Chang, Y. Zheng, and L. Zhang, "A Retrospective and a Look Forward: Fifteen Years of Physical Unclonable Function Advancement," IEEE Circuits and Systems Magazine, vol. 17, no. 3, pp. 32-62, Aug. 2017.

[19] Mudit Bhargava et, al, "An efficient reliable PUF-based cryptographic key generator in 65nm CMOS" IEEE Design, Automation & Test in Europe Conference & Exhibition (DATE).

[20] Sudeendra Kumar K, K.K. Mahapatra, et, al, "Secure Split Test Techniques to prevent IC piracy in IoT devices", VLSI Integration, Elsevier, June 2017.

[21] MAJZOOBI, M. AND KOUSHANFAR, F. 2011. Time-bounded authentication of FPGAs. IEEE Transactions on Information Forensics and Security 6, 3-2, 1123–1135.

[22] YU, M. M., M’RA¨IHI, D., SOWELL, R., AND DEVADAS, S. 2011. Lightweight and secure PUF key storage using limits of machine learning. In Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings. 358–373.

[23] RUHRMAIR, U. 2012. Simple systems as a keyless cryptographic and security primitive. In Cryptography and Security. Springer, 329–354.

[24] J. Guajardo, B. Koric, P. Tuyls, et al. “Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable function,” Information Systems Frontiers, 2009, 11(1): 19-41.

[25] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, FPGA intrinsic PUFs and their use for IP protection. Springer, 2007.

[26] S. Wei, J. B. Wendt, A. Nahapetian and M. Potkonjak, "Reverse engineering and prevention techniques for physical unclonable functions using side channels," 2014 51st ACM/EDAC/IEEE Design Automation Conference (DAC), 2014, pp. 1-6, doi: 10.1145/2593069.2593204.

[27] M. Rostami, M. Majzoobi, F. Koushanfar, D. S. Wallach and S. Devadas, "Robust and Reverse-Engineering Resilient PUF Authentication and Key-Exchange by Substring Matching," in IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 37-49, March 2014, doi: 10.1109/TETC.2014.2300635.

[28] GASSEND, B., CLARKE, D. E., VAN DIJK, M., AND DEVADAS, S. 2002. Controlled physical random functions. In 18th Annual Computer Security Applications Conference (ACSAC 2002), 9-13 December 2002, Las Vegas, NV, USA. 149–160.

[29] OZTURK, E., HAMMOURI, G., AND SUNAR, B. 2008. Towards robust low-cost authentication for pervasive devices. In Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom 2008), 17-21 March 2008, Hong Kong. 170–178.

[30] KATZENBEISSER, S., KOC¸ ABAS, U., ¨ VAN DER LEEST, V., SADEGHI, A., SCHRIJEN, G. J., AND WACHSMANN, C. 2011. Recyclable pufs: logically reconfigurable pufs. J. Cryptographic Engineering 1, 3, 177–186.

[31] MAJZOOBI, M., ROSTAMI, M., KOUSHANFAR, F., WALLACH, D. S., AND DEVADAS, S. 2012. Slender PUF protocol: A lightweight, robust, and secure authentication by substring matching. In 2012 IEEE Symposium on Security and Privacy Workshops, San Francisco, CA, USA, May 24-25, 2012. 33–44.

[32] KOCABASUPETER, A., KATZENBEISSER, S., AND SADEGHI, A. 2012. Converse puf-based authentication. In Trust and Trustworthy Computing - 5th International Conference, TRUST 2012, Vienna, Austria, June 13-15, 2012. Proceedings. 142–158.

[33] DELVAUX, J., GU, D., SCHELLEKENS, D., AND VERBAUWHEDE, I. 2014. Secure lightweight entity authentication with strong pufs: Mission impossible? In Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings. 451–475.

[34] AYSU, A., GULCAN, E., MORIYAMA, D., SCHAUMONT, P., AND YUNG, M. 2015. End-to-end design of a pufbased privacy preserving authentication protocol. In Cryptographic Hardware and Embedded Systems - CHES 2015 - 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings. 556–576.

[35] HELFMEIER, C., BOIT, C., NEDOSPASOV, D., AND SEIFERT, J.-P. 2013. Cloning physically unclonable functions. In Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on. IEEE, 1–6.

[36] B. Gassend, D. Clarke, M. van Dijk, and S. Devdas, “Silicon physical random functions,” in Proc. 9th ACM. Conf. Computer Communication security, pp. 148- 160, 2002.

[37] K. Pratihar, U. Chatterjee, M. Alam, R. S. Chakraborty and D. Mukhopadhyay, "Birds of the Same Feather Flock Together: A Dual-Mode Circuit Candidate for Strong PUF-TRNG Functionalities," in IEEE Transactions on Computers, vol. 72, no. 6, pp. 1636-1651, 1 June 2023, doi: 10.1109/TC.2022.3218986.

[38] P. Gope et al., “Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions,” IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2831–2843, 2018.

[39] M. A. Qureshi and A. Munir, “Puf-rake: A puf-based robust and lightweight authentication and key establishment protocol,” IEEE Trans. on Dependable and Secure Computing, pp. 1–1, 2021.

[40] J. Kong and F. Koushanfar, "Processor-Based Strong Physical Unclonable Functions With Aging-Based Response Tuning," in IEEE Transactions on Emerging Topics in Computing, vol. 2, no. 1, pp. 16-29, March 2014, doi: 10.1109/TETC.2013.2289385.

[41] N. Irtija, E. E. Tsiropoulou, C. Minwalla and J. Plusquellic, "True Random Number Generation with the Shift-register Reconvergent-Fanout (SiRF) PUF," 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 2022, pp. 101-104, doi: 10.1109/HOST54066.2022.9839935.

[42] E. Dubrova, "A Reconfigurable Arbiter PUF with 4 x 4 Switch Blocks," 2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL), Linz, Austria, 2018, pp. 31-37, doi: 10.1109/ISMVL.2018.00014.

[43] Qian Wang, Mingze Gao, Gang Qu, A machine Learning Attack Resistant Dual-mode PUF, GLSVLSI'18, May 23-25, 2018.

[44] Mohammad Ebrahimabadi et al, A Novel Modeling-Attack Resilient Arbiter-PUF Design, 34th International Conference on VLSI Design (VLSID) 2021 DOI: 10.1109/VLSID51830.2021.00026

[45] Zhangqing He, Wanbo Chen, Lingchao Zhang, GaoJub Chi, Qi Gao, and Lein Harn, "A Highly Reliable PUF With Improved Uniqueness in FPGA Implementation Using Bit- Self-Test", October 2, 2020

[46] Rojas-Muñoz, L.F.; Sánchez-Solano, S.; Martínez-Rodríguez, M.C.; Brox, P. True Random Number Generation Capability of a Ring Oscillator PUF for Reconfigurable Devices. Electronics 2022, 11, 4028. https://doi.org/10.3390/electronics11234028

[47] X. Wang et al., "High-Throughput Portable True Random Number Generator Based on Jitter-Latch Structure," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 2, pp. 741-750, Feb. 2021, doi: 10.1109/TCSI.2020.3037173.

[48] Li Xiang, Stanwicks Peter, Provelengios George, Tessier Russell, and Holcomb Daniel. 2023. Jitter-based adaptive true random number generation circuits for FPGAs in the cloud. ACM Transactions on Reconfigurable Technology and Systems 16, 1, (2023), 20 pages.

[49] P. S. Meka, R. Sivaraman, A. Rengarajan and S. Rajagopalan, "Metastability Influenced PUF for Cryptographic Key Generation: A FPGA Approach," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-6, doi: 10.1109/ICCCI48352.2020.9104146.

[50] Serrano, R.; Duran, C.; Sarmiento, M.; Dang, T.-K.; Hoang, T.-T.; Pham, C.-K. A Unified PUF and Crypto Core Exploiting the Metastability in Latches. Future Internet 2022, 14, 298. https://doi.org/10.3390/fi14100298

[51] F. Frustaci, F. Spagnolo, S. Perri and P. Corsonello, "A High-Speed FPGA-Based True Random Number Generator Using Metastability With Clock Managers," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 2, pp. 756-760, Feb. 2023, doi: 10.1109/TCSII.2022.3211278.

[52] A. P. Johnson, R. S. Chakraborty and D. Mukhopadyay, "An Improved DCM-Based Tunable True Random Number Generator for Xilinx FPGA," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 64, no. 4, pp. 452-456, April 2017, doi: 10.1109/TCSII.2016.2566262.

[53] Wang, Y., Wang, C., Gu, C., Cui, Y., O'Neill, M., & Liu, W. (2021). A Dynamically Configurable PUF and Dynamic Matching Authentication Protocol. IEEE Transactions on Emerging Topics in Computing (TETC). Advance online publication. https://doi.org/10.1109/TETC.2021.3072421

[54] P. H. Nguyen, D. P. Sahoo, C. Jin, K. Mahmood, U. Ruhrmair, and M. van Dijk, "The Interpose PUF: Secure PUF Design Against State-of-the-art Machine Learning Attacks," IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2019, no. 4, pp. 243-290, Aug. 2019.

[55] M. Khalafalla and C. Gebotys, "PUFs Deep Attacks: Enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs," in Proc. of 2019 Design, Automation and Test in Europe Conference and Exhibition (DATE), Florence, Italy, 2019, pp. 204-209