IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 12, December 2024| DOI: 10.15680/IJIRCCE.2024.1212001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Study on FPGA Implementation of Physical Unclonable Functions (PUFs)

Sai Kumar Marri, Anjan K

Student Researcher, Department of Electrical Engineering, UTD, USA

ABSTRACT: Physical Unclonable Functions (PUFs) are emerging as a critical hardware security primitive, leveraging the inherent and irreproducible manufacturing variations of integrated circuits (ICs) to generate unique, device-specific responses. By mapping input challenges to output responses based on physical characteristics, PUFs provide a lightweight and cost-effective solution for secure authentication, key generation, and intellectual property protection. Unlike traditional cryptographic approaches, PUFs do not require secure memory to store keys, relying instead on the physical unpredictability of the hardware. PUFs are categorized into two main types: strong PUFs, which support many challenge-response pairs for authentication, and weak PUFs, optimized for generating cryptographic keys [1]. Prominent architecture includes Arbiter PUFs, Ring Oscillator PUFs, SRAM PUFs, and Butterfly PUFs, each tailored to specific application needs and hardware environments. Among these, Ring Oscillator PUFs are particularly notable for their ease of implementation and resilience against environmental variations, making them ideal for use in FPGAs and IoT devices. Despite their advantages, PUFs face challenges in reliability and resistance to attacks, including modeling and side-channel threats. Current research focuses on enhancing security by designing machine learning-resistant PUFs, improving error correction mechanisms, and exploring quantum and nanotechnology-enhanced architectures. Furthermore, the integration of PUFs in resource-constrained devices such as IoT nodes necessitates lightweight and energy-efficient designs. The evolving landscape of PUFs highlights their potential to address emerging security concerns in diverse domains, including cryptographic protocols, secure key management, and device authentication. By combining low cost, high security, and scalability, PUFs represent a promising direction in the development of secure hardware solutions. Continued advancements in PUF technology will pave the way for their broader adoption in critical applications requiring robust and tamper-resistant security mechanisms.

KEYWORDS: Physical Unclonable Functions (PUFs), Hardware Security, Delay-based PUFs, FPGA Implementations, Ring Oscillator PUFs

I. INTRODUCTION

In the era of ubiquitous computing and interconnected devices, security has become a critical concern across domains such as the Internet of Things (IoT), mobile communications, and cloud-based applications. Ensuring secure authentication, reliable key storage, and intellectual property protection are foundational requirements for modern systems. Traditional security solutions often rely on non-volatile memory to store cryptographic keys or secrets, necessitating additional hardware and power, which increases cost, complexity, and susceptibility to physical attacks. Physical Unclonable Functions (PUFs) have emerged as a promising alternative, offering lightweight, hardware-based security without the need for dedicated secure memory. PUFs exploit the inherent and uncontrollable variations introduced during the semiconductor manufacturing process [2]. These variations, which occur even among identically designed integrated circuits (ICs), are effectively impossible to replicate. A PUF functions as a unique "fingerprint" for a device, mapping specific input challenges to output responses determined by the physical properties of the device's circuitry. This unique mapping, which is highly stable and repeatable under normal conditions, makes PUFs well-suited for applications such as secure device authentication, cryptographic key generation, and secure data storage [3].

PUFs are broadly categorized into strong PUFs and weak PUFs. Strong PUFs support a large number of unique challenge-response pairs (CRPs) and are primarily used for authentication tasks. Weak PUFs, on the other hand, are designed to generate a smaller set of highly stable responses, often utilized for cryptographic key derivation and storage. Common PUF architectures include Arbiter PUFs, Ring Oscillator PUFs, SRAM PUFs, and Butterfly PUFs, each leveraging distinct physical mechanisms to produce their outputs [4].

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

While PUFs offer several advantages, including unclonability, low cost, and resistance to certain types of attacks, they are not without challenges. Environmental factors such as temperature and voltage variations can introduce noise into PUF responses, potentially reducing reliability. Furthermore, certain PUF architectures are vulnerable to modeling attacks, where adversaries use machine learning to predict responses based on observed challenge-response pairs. These challenges have spurred extensive research into improving the robustness, security, and scalability of PUF designs. One of the most widely studied architectures, the Ring Oscillator PUF (RO-PUF), demonstrates a balance between ease of implementation and robust performance [5]. By leveraging frequency variations among identically designed ring oscillators, RO-PUFs achieve high levels of uniqueness and reliability, making them ideal for deployment in resource-constrained environments such as FPGAs and IoT devices. Other architectures, like SRAM PUFs, are particularly attractive for key generation applications due to their highly stable responses [6].

Recent advancements in PUF research include the development of machine learning-resistant designs, enhanced error correction mechanisms, and the exploration of novel materials and technologies, such as nanotechnology and quantum mechanics, to further improve security and reliability [9]. Additionally, researchers are investigating the integration of PUFs into new applications, including public-key cryptography, blockchain-based systems, and secure hardware for artificial intelligence. PUFs also hold promise in addressing the unique security challenges of the IoT landscape, where devices are often deployed in untrusted environments with limited computational and energy resources. Lightweight and efficient PUF designs can enable secure communication and authentication for IoT devices without significantly impacting performance or battery life. This introduction provides an overview of the significance, fundamental concepts, and ongoing developments in the field of Physical Unclonable Functions [7]. As PUF technology matures, it is poised to become a cornerstone of hardware-based security, addressing the growing demand for efficient, scalable, and tamper-resistant solutions in an increasingly connected world. The subsequent sections of this paper delve deeper into the architecture, functionality, applications, and challenges associated with PUFs, highlighting their potential to transform secure computing paradigms[8].

Physical Unclonable Functions (PUFs) are generally used for authentication and secret key storage without the requirement of any expensive additional hardware .This is possible, because instead of storing secrets in digital memory, PUFs extract a secret from the physical characteristics of the integrated circuit. A PUF is based on the idea that even though the mask and manufacturing process is the same among different ICs, each IC is slightly different due to normal manufacturing variability [10]. Apart from manufacturing variability that defines the secret, one cannot manufacture two identical chips, even with full knowledge of the chip's design. PUF architectures exploit manufacturing variability in multiple ways. In addition to gate delays, architectures also use other factors like the power on state of SRAM, threshold voltages, and many other physical characteristics to obtain the secret. We have implemented three PUF's which are described below:

•Arbiter PUF
•Butterfly PUF
•Ring Oscillator PUF

II. BUTTER-FLY PUF

The Butterfly Physical Unclonable Function (PUF) is a delay-based PUF architecture designed to emulate the behavior of SRAM PUFs but with a different operational mechanism. Unlike SRAM PUFs, which rely on the random power-on state of memory cells, the Butterfly PUF exploits the inherent delay variations in cross-coupled latches. The Butterfly PUF consists of two cross-coupled latches connected in a feedback loop. When initialized, the system is forced into an unstable state using a control signal called an "excite signal," which holds one latch in preset and the other in clear mode. Upon releasing the excite signal, the circuit resolves into a stable state determined by delay mismatches in the feedback paths. These delay mismatches are introduced by manufacturing variations, making the output state unique to each device. The final state of the latches determines the binary response of the PUF. Multiple challenge-response pairs can be generated by varying the excitation conditions. The Butterfly PUF is often considered an alternative to SRAM PUFs for applications requiring lightweight security primitives, especially in reconfigurable hardware. However, its reliance on delay symmetry makes its implementation less robust compared to architecture like Ring Oscillator PUFs[11].

© 2024 IJIRCCE | Volume 12, Issue 12, December 2024| DOI: 10.15680/IJIRCCE.2024.1212001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

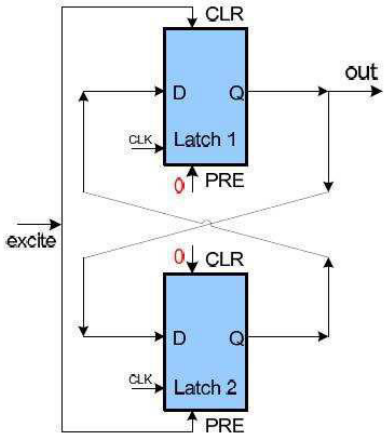

Figure 1: Butter-fly PUF

A. Design

We have used Spartan 3E board to implement our design. The input is a 16-bit challenge, and the output is an 8-bit response. We have used 8 PUF circuits to study the inter-PUF variations. Each PUF circuit consists of 16 cross-coupled latches; upon the challenge request, the cross-coupled latch is excited and samples the output after one clock cycle (latches will be in stable states by one clock cycle). These output bits are processed with the input bits (simple hash function) to generate the challenge response. PUF is converted into a MACRO, and the instance is repeated 8 times.

B. Design Summary

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	97	1,920	5%
Number of 4 input LUTs	162	1,920	8%
Number of occupied Slices	118	960	12%
Number of Slices containing only related logic	118	118	100%
Number of Slices containing unrelated logic	0	118	0%
Total Number of 4 input LUTs	206	1,920	10%
Number used as logic	162		
Number used as a route-thru	44		
Number of bonded IOBs	11	83	13%
Number of RAMB16s	2	4	50%
Number of BUFGMUXs	2	24	8%
Average Fanout of Non-Clock Nets	3.03		

Figure 2: Butter-fly PUF Device Utilization

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Hamming Distance Computation

INPUT	RESPONSE PUF-0	RESPONSE PUF-1	RESPONSE PUF-2	RESPONSE PUF-3	RESPONSE PUF-4	RESPONSE PUF-5	RESPONSE PUF-6	RESPONSE PUF-7
50FC	EA	C6	C0	5A	01	09	6A	7D
51FC	1F	41	46	C7	94	9C	67	E8
51F8	1B	45	42	CB	30	98	63	EC
41F8	0B	55	52	D3	20	88	73	FC
41E8	1B	45	42	C3	30	98	63	EC
61E8	3B	65	62	E3	10	E8	43	CC
50FC	1E	42	47	C6	35	DD	46	E9
51FC	1F	41	46	C7	34	CC	47	E8
51F8	1B	47	42	C3	30	88	43	EC
41F8	0B	47	52	D3	00	88	53	FC
41E8	1B	5F	42	C3	10	98	43	EC
61E8	3B	77	62	E3	30	B8	43	CC

Figure 3: Butter-fly PUF Hamming distance

Inter-Hamming distance = 50%

C6-1100 0110 – 37.5%
C0-1100 0000 – 37.5%
5A-0101 1010 – 37.5%
01-0000 0001 – 75%
09-0000 1001 – 62.5%
6A-0110 1010 – 37.5%
7D-0111 1101 – 62.5%

Average = (37.5+37.5+37.5+75+62.5+37.5+62.5)/7 = 350/7 = 50%

Intra-Hamming distance = 8.33%

EA-1110 1010 1E-0001 1110 – 50%
1F-0001 1111 1F-0001 1111 – 0%
1B-0001 1011 1B-0001 1011 – 0%
0B-0000 1011 0B-0000 1011 – 0%
1B-0001 0000 1B-0001 0000 – 0%
3B-0011 1011 3B-0011 1011 – 0%

Average = (50+0+0+0+0+0)/6 = 50/6 = 8.33%

Hamming Weights = 40%

		Hamming Weight	Percentage
EA	1110 1010	6/8	75%
1F	0001 1111	1/8	12.5%
1B	0001 1011	1/8	12.5%
0B	0000 1011	4/8	50%
1B	0001 0000	4/8	50%
3B	0011 1011	4/8	50%

Average: (200/5) = 40%

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. ARBITER PUF

The Arbiter Physical Unclonable Function (PUF) is a delay-based PUF architecture that relies on the difference in propagation delays between two identical signal paths to generate unique responses. This architecture is particularly suited for device authentication and secure key generation due to its simplicity and scalability [13].

The Arbiter PUF consists of two parallel signal paths, each made up of multiple switching stages (e.g., multiplexers or XOR gates). These stages are configured identically but experience slight variations in delay due to manufacturing process variations. A "challenge" input determines the switching configuration of each stage, creating unique signal propagation paths. A rising edge signal is injected into both paths, and the time it takes for the signal to propagate through each path is measured. At the end of the paths, an arbiter (typically a D-type flip-flop) determines which signal arrives first, outputting a binary response (0 or 1) [12].

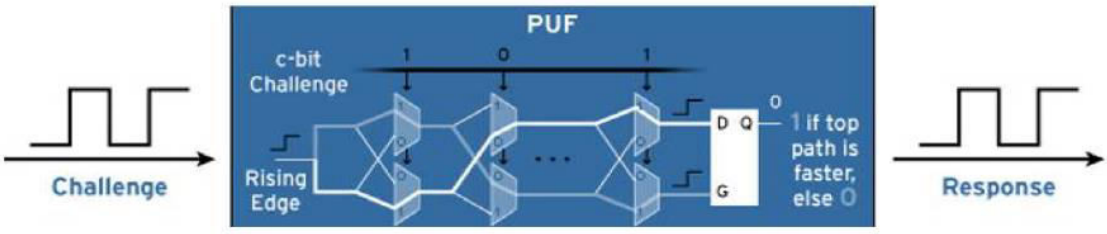

Figure 4: Arbiter PUF

A. Design:

We have used Spartan 3E board to implement our design. The input is a 16-bit challenge, and the output is an 8-bit response. We have used 8 PUF circuits to give the response. Each PUF circuit consists of 8 sub-PUF circuits, which in turn consist of 32 multiplexers and a D-flipflop at the end. The selection line of each multiplexer contributes a one-bit challenge, and the output of each sub-PUF yields a one-bit response. The D-flipflop at the end is positive-edge triggered, which is used to collect the delays from the multiplexers.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

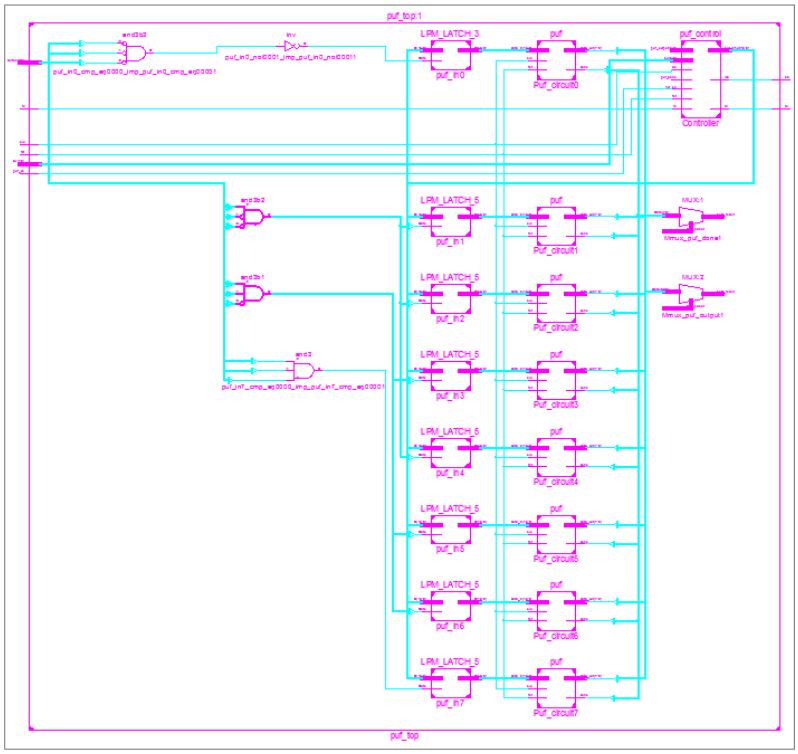

Figure 5: Arbiter PUF schematic

B. Description Summary

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	97	1,920	5%
Number of 4 input LUTs	162	1,920	8%
Number of occupied Slices	118	960	12%
Number of Slices containing only related logic	118	118	100%
Number of Slices containing unrelated logic	0	118	0%
Total Number of 4 input LUTs	206	1,920	10%
Number used as logic	162		
Number used as a route-thru	44		
Number of bonded IOBs	11	83	13%
Number of RAMB16s	2	4	50%
Number of BUFGMUXs	2	24	8%
Average Fanout of Non-Clock Nets	3.03		

Figure 6: Arbiter PUF Device Utilization

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Arbiter PUF Hamming distance computation

INPUT	52-23	72-59	60-32	79-3	20-65	59-62
RESPONSE PUF - 0	22	22	22	22	22	22
RESPONSE PUF - 1	88	88	88	88	88	88
RESPONSE PUF - 2	0	0	0	0	0	0
RESPONSE PUF - 3	50	50	50	50	50	50
RESPONSE PUF - 4	96	96	96	96	96	96
RESPONSE PUF - 5	20	20	20	20	20	20
RESPONSE PUF - 6	18	18	18	18	18	18
RESPONSE PUF - 7	13	13	13	13	13	13

Figure 7: Arbiter PUF hamming distance

Inter Hamming Distance:
22-0010 0010 – 50%
88-1000 1000 – 25%
00-0000 0000 – 50%
50-0101 0000 – 50%
96-1001 0110 – 12.5%
20-0010 0000 – 50%
18-0001 1000 – 37.5%

Average-Inter Hamming Distance = (50+25+50+50+12.5+50+37.5)/7 = 275/7 = 39.285%
Intra Hamming Distance = 0%
Hamming Weight = 0%

IV. RING OSCILLATOR PUF

Ring oscillator PUF consists of identical inverter chains that toggle at a frequency depending on the signal path delays. Each PUF will have a unique delay because of the process manufacturing variations, so the frequency of each inverter chain will be different. This PUF is more reliable for FPGA based designs because its functionality doesn't require symmetrical structure which is difficult to achieve in the FPGA architectures.

The Ring Oscillator (RO) PUF is a delay-based PUF architecture that exploits frequency variations in identically designed ring oscillators (ROs) to generate unique, device-specific responses. It is widely regarded for its ease of implementation and robustness, particularly in environments like FPGAs and IoT devices. Composed of multiple identical ROs, each consisting of an odd number of inverters connected in a loop. A counter measures the frequency of oscillation for each RO. When an RO is activated, its oscillation frequency depends on the delay of its components, which varies due to manufacturing process variations. The output response is derived by comparing the frequencies of two ROs. For instance, if RO1 oscillates faster than RO2, the response bit is 1; otherwise, it is 0. RO PUFs are used for device authentication, cryptographic key generation, and secure hardware applications. Their simplicity, scalability, and robustness make them particularly suitable for resource-constrained devices in IoT and embedded systems [16].

© 2024 IJIRCCE | Volume 12, Issue 12, December 2024| DOI: 10.15680/IJIRCCE.2024.1212001

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

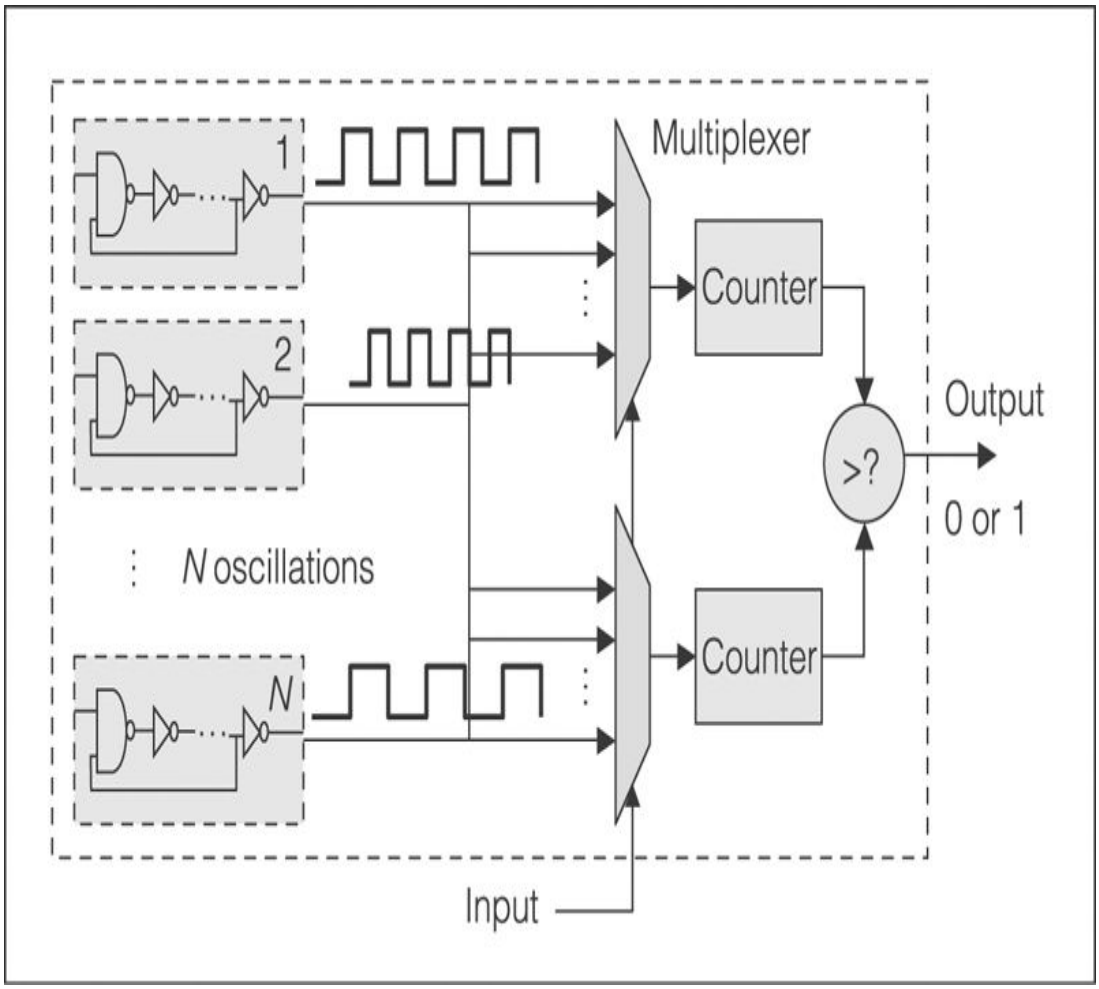

Figure 8: Ring Oscillator PUF

A. Design

We have used Spartan 3E board to implement our design. The input is a 16-bit challenge, and the output is an 8-bit response .We have used 8 PUF circuits to study the inter-PUF variations. Each PUF circuit contains 16 inverter chains, 2 MUX to select the two of the inverter chain outputs based on the challenge request, counters, and comparator to compare the counter values. When a challenge request is given, based on the request one inverter chain is fixed, and the other inverter chain is varied upon different hashing combinations of the request. For each operation, the counter values are sampled after a certain time and compared. The comparator output is sampled into one of the response bits. Each inverter chain is converted to a MACRO and instantiated in the design.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

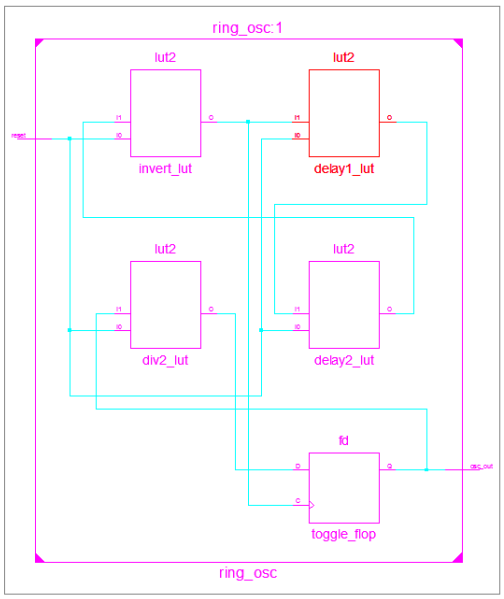

Figure 9: Ring Oscillator Schematic

B. Design Summary

Device Utilization Summary			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Flip Flops	97	1,920	5%
Number of 4 input LUTs	162	1,920	8%
Number of occupied Slices	118	960	12%
Number of Slices containing only related logic	118	118	100%
Number of Slices containing unrelated logic	0	118	0%
Total Number of 4 input LUTs	206	1,920	10%
Number used as logic	162		
Number used as a route-thru	44		
Number of bonded IOBs	11	83	13%
Number of RAMB16s	2	4	50%
Number of BUFGMUXs	2	24	8%
Average Fanout of Non-Clock Nets	3.03		

Figure 10: Ring Oscillator PUF Device Utilization

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Ring Oscillator PUF Hamming distance computation

INPUT	RESPONSE PUF-0	RESPONSE PUF-1	RESPONSE PUF-2	RESPONSE PUF-3	RESPONSE PUF-4	RESPONSE PUF-5	RESPONSE PUF-6	RESPONSE PUF-7
50FC	00	00	00	08	00	00	00	00
51FC	00	00	00	01	00	00	00	00
51F8	00	00	20	08	00	00	00	00
41F8	00	00	00	00	04	00	00	00
41E8	00	00	BE	22	00	00	00	00
61E8	00	00	00	10	00	00	00	00
50FC	00	20	80	00	00	00	00	00
51FC	00	00	00	09	00	00	00	00
51F8	00	00	40	00	00	00	00	00
41F8	00	20	84	20	00	00	00	00
41E8	00	00	00	10	00	00	00	00
61E8	00	00	00	00	00	00	00	00

Figure 11: Ring Oscillator PUF Hamming Distance computation

Inter-Hamming distance - 7.14%
20- 0010 0000 – 12.5%
40-0100 0000 – 12.5%
09-0000 1001 – 25%
00-0000 0000 – 0%
00-0000 0000 – 0%
00-0000 0000 – 0%
00-0000 0000 – 0%
Average = (50/7) = 7.14%

Intra-Hamming distance – 10.41%
08-0000 1000 00-0000 0000 – 12.5%
01-0000 0001 00-0000 0000 – 12.5%
08-0000 1000 09-0000 1001 – 25%
00-0000 0000 00-0000 0000 – 0%
22-0010 0010 20-0010 0000 – 12.5%
10-0001 0000 10-0001 0000 – 0%
Average : (12.5+12.5+25+0+12.5+0+0)/6 =62.5/6 =10.41%

Hamming weight – 25%
01-0000 0001 – 2/8 – 25%
08-0000 1000 – 2/8 – 25%
00-0000 0000 – 1/8 – 12.5%
22-0010 0010 – 2/8 – 25%
10-0001 0000 – 3/8 – 37.5%
Average: -- 125/5 = 25%

V. CONCLUSION

The implementation of Physical Unclonable Functions (PUFs) on Field-Programmable Gate Arrays (FPGAs) represents a promising approach to achieving lightweight and hardware-integrated security. FPGA-based PUFs leverage the inherent process variations in their programmable fabric to generate unique and unclonable device

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

fingerprints, making them ideal for applications in authentication, cryptographic key generation, and intellectual property protection. Several PUF architectures, such as Ring Oscillator PUFs, Arbiter PUFs, and Butterfly PUFs, have been successfully implemented on FPGAs, each offering unique trade-offs in terms of reliability, security, and resource utilization. The flexibility of FPGA platforms allows for the rapid prototyping and evaluation of these designs, enabling researchers and engineers to assess their performance under varying environmental conditions, such as temperature and supply voltage variations [14].

While FPGA implementations of PUFs demonstrate significant potential, challenges remain. The susceptibility of some PUF architectures to environmental noise and aging effects necessitates the use of error correction mechanisms to ensure stable responses. Additionally, advanced machine learning attacks pose a threat to the security of FPGA-based PUFs, especially for architectures like Arbiter PUFs. Addressing these vulnerabilities requires the exploration of robust designs, enhanced challenge-response generation, and integration with cryptographic primitives. Despite these challenges, FPGA-based PUFs hold significant advantages, including their low cost, scalability, and suitability for resource-constrained environments such as IoT devices. As the demand for secure hardware solutions grows, ongoing research into improving the robustness and attack resistance of FPGA PUFs is expected to pave the way for their widespread adoption in critical security applications [15].

In conclusion, the implementation of PUFs on FPGAs offers a compelling combination of flexibility, efficiency, and security, making it a cornerstone for advancing hardware security solutions in a variety of domains.

REFERENCES

1.S. Morozov, A. Maiti, and P. Schaumont, "A Comparative Analysis of Delay-Based PUF Implementations on FPGA," Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010.
2.A. Maiti, J. Casarona, L. McHale, and P. Schaumont, "A Large Scale Characterization of RO-PUF," Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2010.
3.C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, August 2014.
4.M. Potkonjak and V. Goudar, "Public Physical Unclonable Functions," Proceedings of the IEEE, vol. 102, no. 8, pp. 1142-1156, August 2014.
5.G. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," Proceedings of the Design Automation Conference (DAC), 2007.
6.B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Controlled Physical Random Functions," Proceedings of the 18th Annual Computer Security Applications Conference, 2002.
7.R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," Science, vol. 297, no. 5589, pp. 2026-2030, 2002.
8.J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications," Proceedings of the IEEE VLSI Circuits Symposium, 2004.
9.R. Kumar, N. Karimi, and K. Sasan, "PUF Exploiting Delay-based Architectures: Challenges and Strategies," IEEE Transactions on Circuits and Systems I, 2021.
10.D. Lim, "Extracting Secret Keys from Integrated Circuits," Master's Thesis, Massachusetts Institute of Technology (MIT), 2004.
11.A. Maiti and P. Schaumont, "Improved Ring Oscillator PUF: An FPGA-Friendly Secure Primitive," Journal of Cryptology, vol. 24, pp. 375–397, 2011.
12.U. Ruhrmair, J. Solter, and F. Sehnke, "PUF Modeling Attacks on Arbiter PUFs and the Xor Arbiter PUF," Proceedings of the Conference on Cryptographic Hardware and Embedded Systems (CHES), 2010.
13.J. Guajardo, S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2007.
14.Sai Kumar Marri, N. Muthiah. "Obscure Hardware Trojan Design in 8051 Micro-controller". International Journal of Modern Engineering Research 14. 06(2024): 43-49.
15.P. Tuyls and L. Batina, "RFID-Tags for Anti-Counterfeiting," Proceedings of the Conference on Topics in Cryptology (CT-RSA), 2006.
16.B. Gassend, "Physical Random Functions," Master's Thesis, Massachusetts Institute of Technology (MIT), 2003.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details