PUF Based Authentication System for IoT Nodes: A Comparative Study

Magna Mishra
National Institute of Technology
Rourkela, India
kmishra5731@gmail.com

Sudeendra Kumar K
PES University
Bangalore, India
kumar.sudeendra@gmail.com

AK Swain
National Institute of Technology
Rourkela, India
swain.ayas@gmail.com

K K Mahapatra
National Institute of Technology
Rourkela, India
kkm@nitrkl.ac.in

2022 IEEE International Symposium on Smart Electronic Systems (iSES) | 979-8-3503-9922-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISES54909.2022.00085

Abstract—Physical Unclonable Function (PUF) is an established hardware security primitive which is useful in mitigating chip counterfeiting, IP protection and cryptographic key generation. In this paper, we propose a XOR based Arbiter PUF which is an improvement to conventional arbiter PUF. A network of XOR gates is placed between the arbiter stages in conventional arbiter PUF to construct the proposed PUF. The PUF can be configured for different size of challenge response pairs (CRPs) due to its modular design. It is scalable in terms of the stages of arbitration required as well as the width of the challenge bits given as input. The designed PUF is implemented on Xilinx Artix-7 and Spartan-6 FPGAs and the standard PUF design metrices like uniqueness, reliability and uniformity are measured and comparative analysis is presented. The proposed PUF exhibits the better PUF metrics in comparison with conventional Arbiter PUF and other recently presented PUF topologies in the literature. Near field communication (NFC) based applications needs the sound authentication systems and PUF circuits are suitable for the purpose. The proof-of- concept prototype is developed for authentication in NFC systems using proposed XOR based PUF and effectiveness of proposed PUF is validated.

Keywords—Physically Unclonable Function (PUFs), Arbiter, XOR, Near Field Communication (NFC), Authentication System

I. Introduction

The growth of the semiconductor industry in the mid-1990s era led to decrease in price of silicon-based fabrication. Earlier silicon was costlier and much of the work was handled by software, but with gradual decrease and improvements in hardware design, the industry is shifting towards hardware-based designs. For instance, complicated tasks like cache maintenance and instruction scheduling were earlier done by application software in computers. Today all of these tasks are performed directly at hardware level in modern computing devices. With changing times, the metrics that are focused in system design have also shifted. Throughout the 80s, designers were focused on packing more transistors, in the 90s the focus was on improving clock speeds, in the beginning of the 21st century the focus was on making silicon cheaper and now the focus is on improving connectivity and making the systems secure [1].

A. A Glimpse on Hardware Security

One of the major difficulties in implementation of Internet of Things (IoT) in smart applications where millions of edge nodes will dynamically enter and exit the network is authentication. Researchers in industry and academia are designing solutions to above mentioned hardware security issues. Physical Unclonable Function (PUF), which is an established hardware security primitive in recent times has got applications to address the hardware security problems and cryptographic key generation. PUF circuits will come handy to design and develop the authentication and identification in large scale IoT applications.

B. Relevance of PUFs for Authentication

Designing novel PUF topologies is an attractive topic for several researchers in last one decade. The basic PUF topologies are based on ring oscillator and arbiter. Physical disorders introduced during manufacturing form the base for intrinsic PUFs [2]. Being unpredictable and unique in nature, PUFs present a unique footprint of the device. Since the footprint is related to manufacturing and defects created during manufacturing, it is virtually impossible to duplicateor clone the structure. The randomness of PUF output ensures that no two units have equal signatures for the same inputs. Itis based on the concept that no two devices can have complete physical similarity although they might be logically similar. A PUF's reliability mainly depends on the difficulty in predicting the random variation of input output pairs [3].

C. PUFs versus Cryptography

When it comes to authentication, cryptographic algorithms have been widely used for decades. But instead of relying on a key for encryption, PUFs make use of Challenge-Response Pairs (CRPs) [4]. The authentication function of a PUF is always a multiple input, multiple out algorithms. This property of PUFs eliminates the vulnerability of spoofing attacks where hardware devices /application software is tempered to forge the identity of the device. Another advantage of PUFs is their scalability according to the intent/application. PUFs and their control circuits are extremely simple as compared to complex ciphers.

The scalability of combinational PUFs increases the design complexity linearly as compared to hardware based cryptographic algorithms, which may go till $O(2^n)$. This directly translates to the latency of operation when implemented in an ASIC. In short, PUF based hardware security systems will always have lesser latency and faster authentication. This makes the use of PUFs highly advantageous in 'Real-Time' and 'Mission-Critical' systems. Sometimes complex look-up tables with one-to-many mappings for all CRPs have to be included to improve the repeatability and reliability. Since PUFs are reliant on physical parameters of the materials in the circuit, temperature, electromagnetic interference and voltage can easily affect the responses. Still researchers are interested in developing new PUF topologies to overcome the issues like improving the basic PUF metrics and associated CRP processing circuitry for targeted application. In this paper, we propose novel PUF topology, which is an improvement to a conventional arbiter PUF. In this work, we have discussed a novel XOR based PUF architecture that introduces XOR gates between MUX stages in arbiters. Furthermore, we present a thorough investigation of PUF metrics. Further, this paper is organized as follows: Section II discusses contributions made in the paper from a top view.

979-8-3503-9922-6/22/$31.00 ©2022 IEEE
DOI 10.1109/iSES54909.2022.00085

Section III describes the proposed PUF design. In Section V, PUF metrics such as uniqueness, uniformity and reliability have been evaluated and contrasted with existing PUF designs. All measurements made were conducted on the proposed work implemented on Artix-7 series FPGAs and Spartan-6 series FPGAs. Xilinx ILA debugcore was used in the synthesized netlist to collect the outputs. Section VI establishes the use case of the proposal via a controller mechanism which uses a PUF with NFC devices. The paper is concluded in section VII along with possible future scope.

II. CONTRIBUTIONS OF THE CURRENT PAPER

A. Problems addressed in the current paper

- To design an extremely lightweight and scalable combinational PUF block.
- To achieve better performance metrics along with better Power-Performance-Area optimization.
- To design a lightweight controller for validating PUF application in device level authentication.

B. Novel contributions of the current paper

- The proposed work discusses the design and implementationof a novel Arbiter PUF which uses XOR gates between Arbiter stages. It has been proven that the proposed design has better uniqueness index as compared to previous works while consuming lesser resources (Slices & LUTs).
- The XOR network proposed between two arbiter stages improves hardware obfuscation and provides better security towards side-channel attacks.
- The proposed PUF based authentication system can be leveraged for hardware security of lightweight IoT nodes/edge devices.

C. Challenges faced in solving the problems

- While design, verification, simulation and implementation of the circuit was easy on an FPGA, the performance metrics couldn't be tested in actual silicon due to long fabrication times of ASICs.
- Although a theoretical study was made on the hardware security metrics, quantitative data supporting better effectiveness in side-channel attacks couldn't be produced due to unavailability of appropriate testing environment.

III. PROPOSED ARCHITECTURE

The paper proposes a unique authentication system which secures the data transactions between two devices in a lock and key fashion. The master device behaves like a lock and the slave device that needs access to the master device behaves as a key. The proposed design as shown in Fig.1, is a XOR network-based Arbiter PUF. Arbiter PUFs produce outputs based on the principle of differential path delays [5],[6] and [7]. Multiplexers are used to create two or more parallel paths. Due to intrinsic gate delay difference between both the parallel paths, the same signal is bound to producea delta delay on arrival at the output. A latch present at the output of the network of multiplexers captures the delta delay and latches to either 0 or 1 based on which path has lower delay. In addition to the network of multiplexers, a network of XOR gates has been added to further randomize the outputs.

In each stage of the Arbiter, for each multiplexer, a XOR gate is added which XORs the output of the multiplexer and the select line and passes the signal forward to the next stage. The more the number of stages, the more is the randomization. Addition of XOR increases hardware obfuscation and randomness. The bits driving the multiplexer select lines make the "key" for the PUF. N such arbiters can be used to produce an N-bit response for an N-bit challenge for a given value of "key". If we have M stages of multiplexers in each arbiter, then the key has to be of M bits. Overall, the proposed PUF can produce $2^{(N+M)}$ unique CRPs

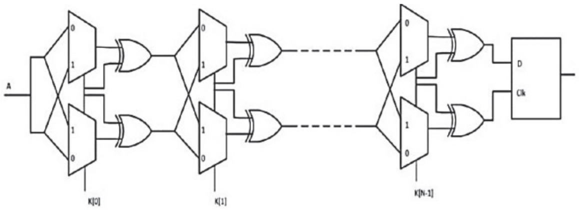

Fig. 1. Proposed PUF design

IV. EVALUATION AND COMPARISION OF PUF METRICS

There are three main evaluation metrics of a PUF as described in [8]:

Uniqueness, Uniformity and Reliability

Uniqueness of a PUF measures how well it can differentiate between a pair of chips. It is mathematically defined by using Hamming distance between a pair of chips distinct chips i and j with n-bit responses Ri and Rj for a challenge C. Uniformity defines the ratio of 0s and 1s in a PUF's response. It is mathematically described using percentage of Hamming weight of a response. Reliability of a PUF describes its ability to produce identical result when the challenge is constantly applied under varying environmental conditions such as voltage fluctuations and temperature. Ideally, reliability of a PUF circuit should be 100%.

To evaluate the proposed XOR design on the above metrics, several boards of Artix-7 series (Basys-3, Zybo, Nexys4 DDR) and Spartan 6 series (Nexys-3) were used.

A. Results

The results of evaluation for PUF metrics with 4-bit and 8-bit challenges and 4 level arbitration are as follows:

TABLE I: WITHOUT CONSIDERING KEYS AS A PART OF CRPs

Levels of Arbitration	Width of challenge bits	Slices	Uniqueness(%)	Reliability* (%)	Uniformity (%)
4	4	56	52	100	48.2
4	8	236	61	100	32.66

TABLE II: CONSIDERING KEYS AS A PART OF CRPs

Levels of Arbitration	Width of challenge bits	Slices	Uniqueness (%)	Reliability* (%)	Uniformity (%)
4	4	56	50.6	100	46.78
4	8	236	49.99	100	32.86

Variation of Hamming distance with respect to intra

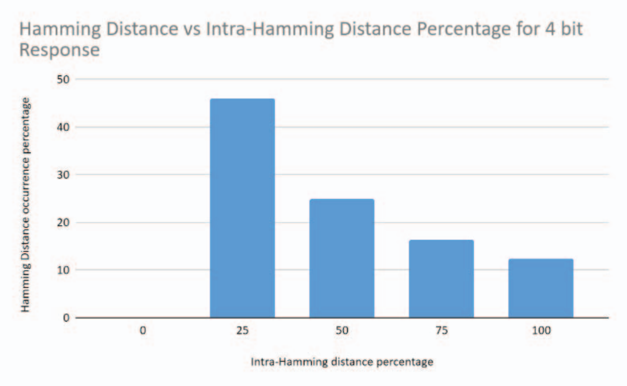

Fig. 2. Hamming Distance versus Intra Hamming Distance (in percentage) for 4-bit response and 4 levels of arbitration.

Hamming Distance have been plotted in Fig. 2 and Fig. 3. To visualize the number of unique CRPs obtained vs the number of total CRPs, Fig 4 can be referred. Considering that the key value as constant, horizontal axis represents the number of arbiter levels and the vertical axis represents the number of responses.

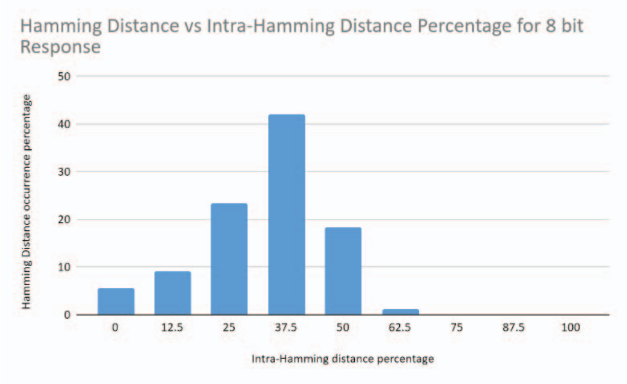

Fig. 3. Hamming Distance versus Intra Hamming Distance (in percentage) for 8-bit response and 4 levels of arbitration.

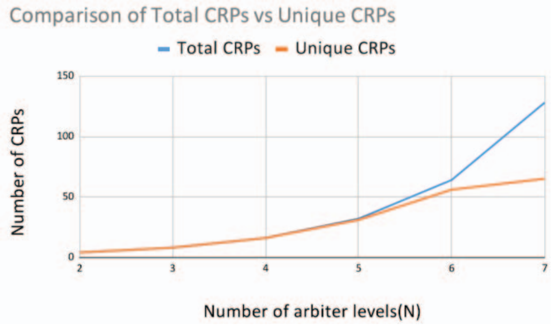

Fig. 4. Comparison of total number of CRPs and Unique CRPs for N levels of arbitration and N bit response.

B. *Comparison with Existing Work*

The proposed design of XOR PUF has been compared with existing state of the art PUFs described by [7], [9], [10] and [11]. The results have been summarized in Table III. From the comparison, it can be noted that the uniqueness of the proposed design is better than all other previous works. The uniqueness which is expected to be 50% ideally, has been met in all the use cases. The inter-class Hamming Distance is used to measure uniqueness index that averages the Hamming Distance of multiple CRPs of various chips. A uniqueness of 50% or more is considered acceptable because majority of the area of the curve Hamming Distance occurrence percentage vs Inter-Hamming distance lies within 50%. Uniformity index drops in case of 8-bit challenges since the total number of CRPs increases exponentially in comparison to the number of bits. Resources consumed is not significantly different from existing works.

III. Application

Near Field Communication (NFC) has been proposed in conjunction with authentication systems to enable wireless authentication between IoT node devices and central hub. NFC can use several frequencies, generally 13.5 MHz and 125 MHz are widely used. The use case described below employs the proposed PUF scheme in a controller, interfaced with a 2.4GHz transceiver module (ISM frequency band). The proposed system has been used to model a keyless ignition system in automobiles. Modern-day automobiles have complete electronic control systems and drive-by-wire technology. Engine ignition and control are handled by a system of microcontrollers called the Engine Control Unit (ECU).

Wireless fobs generally implement a light weight cryptography algorithm. Despite the encrypted wireless communication between the key and vehicle, many attacks have been proven to be successful at unlocking the vehicle [13]. Such types of attacks are commonly referred to as spoofing where a generic software defined radio can be used to pick up the transmission and programmed to mimic the same.

To demonstrate the working of the PUF based keyless ignition system, we consider the set-up as described below and demonstrated in Fig.5. The wireless fob key will be slave and the vehicle's ECU will be the master/host. The slave will periodically keep sending 1-byte pings in a dedicated channel using GFSK modulation.

The host will be interrupted by the transceiver module upon receiving the ping. The host would now send a challenge over the same channel. At the same time, it will also pass the same challenge to its own PUF and record the response for comparison. The slave would receive the response and pass it through its PUF. It would then send back the PUF response back to the host. The host will compare the received response with its calculated response and unlock the ECU for ignition.

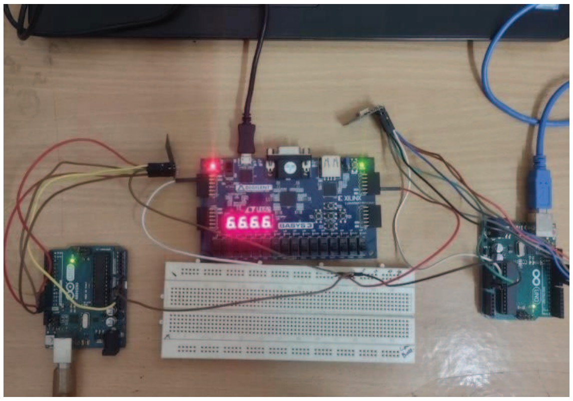

Fig. 5. Setup to validate Authentication using PUF over NFC

TABLE III. COMPARISON OF PROPOSED DESIGN WITH EXISTING PUF SCHEMES

Year	PUF architecture	Device Used	Total number of slices	Uniqueness (%)	Reliability (%)	Uniformity (%)
2022	This work (4 level arbitration, 4-bit challenge)	Artix-7 and Spartan-6	56	52	100*	48.2
2022	This work (4 level arbitration, 4-bit challenge) ^	Artix-7 and Spartan-6	56	50.6	100*	46.78
2022	This work (4 level arbitration, 8-bit challenge)	Artix-7 and Spartan-6	236	61	100*	32.66
2022	This work (4 level arbitration, 8-bit challenge) ^	Artix-7 and Spartan-6	236	49.99	100*	32.86
2022	XOR [9]	Artix-7	64	49.47	98.94	NA
2022	XOR [9]	Spartan-6	64	49.03	97.54	NA
2019	XOR-based Reconfigurable RO (XRRO) [7]	Spartan-6	NA	48.76	97.72	NA
2019	XOR -based reconfigurable bistable RO (XRBR) [7]	Spartan-6	NA	40.67	98.22	NA

2017	Pico [11]	Spartan-6 and Artix-7	128	45.6	99.2(M)
					98.74(A)
						NA

2015	Pico [10]	Spartan-6	64	49.93	93.96	NA

^ when keys are included as a part of CRP, * repeated observations, M through manual testing, A through automated testing

IV. CONCLUSION

Physical Unclonable Function circuits are important security primitives to effectively solve the security problems connected with hardware security like counterfeiting and authentication applications in IoT systems. Different topologies of PUF are presented in the past and still researchers are interested in investigating the novel PUF topologies with better metrics and associated CRP processing circuits for intended applications. In this paper, we present the novel XOR based arbiter PUF and investigated the PUF metrics on Artix-7 and Spartan-6 FPGA devices. It is observed that, the proposed XOR based arbiter PUF exhibits the satisfactory PUF metrics which are vastly acceptable for both hardware security and cryptographic applications. The metrics for the PUF yielded desirable results in case of uniqueness and uniformity, with the worst-case uniqueness being 49.99%. Comparison with recent PUF topologies is also presented in Table III. The proof-of-concept setup is developed to verify the proposed PUF topology for NFC applications. Experiment indicates that, the proposed PUF works well for authentication of IoT edge nodes.

REFERENCES

[1] Alladi, Tejasvi ”Consumer IoT: Security vulnerability case studies andsolutions.” IEEE Consumer Electronics Magazine 9.2 (2020): 17-25.

[2] Pappu RS, Recht B, Taylor J, Gershenfeld N (2002) Physical one-way functions. Science 297:2026–2030

[3] Suh, G. Edward, and Srinivas Devadas. "Physical unclonable functionsfor device authentication and secret key generation." 2007 44th ACM/IEEE Design Automation Conference. IEEE, 2007.

[4] Joshi, Shital, Saraju P. Mohanty, and Elias Kougianos. "Everything you wanted to know about PUFs." IEEE Potentials 36.6 (2017): 38-46.

[5] Nguyen, Phuong Ha ”Security analysis of arbiter PUF and its lightweight compositions under predictability test.” ACM Transactions on Design Automation of Electronic Systems (TODAES) 22.2 (2016): 1-28

[6] Zhou, Chen, Keshab K. Parhi, and Chris H. Kim. ”Secure and reliable XOR arbiter PUF design: An experimental study based on 1 trillion challenge response pair measurements.” Proceedings of the 54th Annual Design Automation Conference 2017

[7] Liu, Weiqiang ”XOR-based low-cost reconfigurable PUFs for IoT security.” ACM Transactions on Embedded Computing Systems (TECS) 18.3 (2019): 1-21.

[8] Maiti, Abhranil, Vikash Gunreddy, and Patrick Schaumont. "A systematic method to evaluate and compare the performance of physical unclonable functions." Embedded systems design with FPGAs. Springer, New York, NY, 2013. 245-267.

[9] Della Sala, Riccardo, Davide Bellizia, and Giuseppe Scotti. "A Lightweight FPGA compatible weak-PUF primitive based on XOR gates." IEEE Transactions on Circuits and Systems II: Express Briefs (2022).

[10] Gu, Chongyan and O’Neill, Maire, “Ultra-compact and robust FPGA based PUF identification generator,” in 2015 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE,May 2015, pp. 934–937

[11] C. Gu, N. Hanley, and M. O’Neill, “Improved reliability of FPGA based PUF identification generator design,” ACM Transactions on Reconfigurable Technology and Systems, vol. 10, no. 3, 2017.

[12] Labrado, Carson, and Himanshu Thapliyal. "Hardware security primitives for vehicles." *IEEE Consumer Electronics Magazine* 8, no. 6 (2019): 99-103.

[13] Chatterjee, Durba, Debdeep Mukhopadhyay, and Aritra Hazra."Formal Analysis of Physically Unclonable Functions." 2021 IFIP/IEEE 29th International Conference on Very Large ScaleIntegration (VLSI-SoC). IEEE, 2021.

[14] Yanambaka, Venkata P., Saraju P. Mohanty, Elias Kougianos, Babu K. Baniya, and Bibhudutta Rout. "Veda-PUF: A PUF based on Vedic Principles for Robust Lightweight Security for IoT." In 2021 IEEE International Symposium on Smart Electronic Systems(iSES)(Formerly iNiS), pp. 400-405. IEEE, 2021.

[15] Sahoo, Sauvagya Ranjan, K. Sudeendra Kumar, and Kamalakanta Mahapatra. "A novel current controlled configurable RO PUF with improved security metrics." *Integration* 58 (2017): 401-410.