PUF-Based Authentication for the Security of IoT Devices

Ahmed Oun
Department of Electrical & Computer
Engineering and Computer Science
Ohio Northern University, Ada, Ohio 45810
a-oun@onu.edu

Mohammed Niamat
Department of Electrical Engineering and
Computer Science
University of Toledo, Toledo, Ohio 43606
Mohammed. Niamat@utoledo.edu

***Abstract*— The Internet of Things (IoT) has become in demand nowadays as many embedded devices are connected to the internet to collect a vast amount of data for processing. A substantial amount of this data between IoT devices is confidential information; therefore, attacks on IoT devices are growing, causing challenges to the security of the IoT devices. Physical Unclonable Functions (PUFs) are proposed as a powerful and lightweight solution to secure IoT devices. PUFs authenticate and generate secure cryptographic keys using manufacturing process variations to protect IoT devices from different attacks; this unique identity is based on physical characteristics. Device authentication is an essential task in IoT. In this paper, we propose a lightweight XOR-ROPUF based authentication scheme for the security of IoT systems. The proposed management scheme carries out the authentication between the verification authority and the IoT devices to ensure data congeniality and integrity, and thus reduces the risk of cyber attacks.**

Keywords*— *Hardware Security, FPGA, PUFs, Authentication, Internet of Things.

I. Introduction

The need for communication amongst connected devices has led to an increase in demand for the Internet of Things (IoT). IoT has developed as an expanded network where millions of devices are connected to the internet to transfer helpful information [1]. IoT refers to the appearance of the network of physical objects that have internet infrastructure, connectivity, and information transfer between these objects and other internet systems to achieve tasks without human interaction [2]. From the most straightforward consumer-based applications such as smartphones and smart homes to complex industry solutions, like the smart power grid and medical devices, the Internet of Things (IoT) is everywhere and constantly improving how consumers work, as shown in Fig. 1. IoT devices are becoming widely used in emerging applications such as edge computing, smart and connected cities, medical devices, smart power grids, and intelligent autonomous systems. IoT technology is presumed to be used in various ways and strongly impacts different applications such as personal health monitoring devices, the smart home, and smartphones by providing interconnection and information exchange. They also connect an increasing number of dynamic global information networks consisting of Internet-connected objects, making the IoT a complex growing system [3]. These applications are increasingly integrated into insecure physical environments making the necessary authentication scheme challenging for security in IoT networks and leading to many challenges, like security, privacy, authentications, etc., and need to be protected from the new cyber and physical system attacks [4]. Hardware security is one of the significant challenges in IoT due to the likelihood of these devices communicating in an unsecured system, thus providing an adversary to gain access to the system. Therefore, there is a need to develop a hardware security solution to trust IoT networks [5].

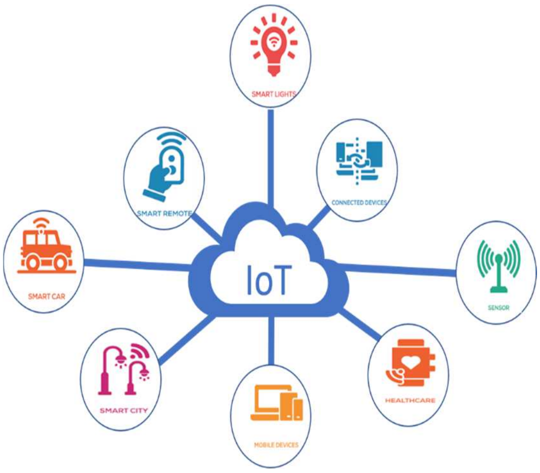


Fig. 1. The overall picture of Internet of Things Devices.

II. Background

A. *Physical Unclonable Functions on the Internet of Things*

The life process of IoT devices affects different parties and facilities, and thus, various security threats impact these devices. IoT-based threats have endangered IoT devices' security, operability, reliability, and expansive applications [6]. An adversary can steal design information during manufacturing at an untrusted foundry, and these attacks may lead to leaking secret information from an IoT-based and intelligent electronic device. Security of the Internet of Things (IoT) is one of the current primary challenges in developing our life and future manufacturing systems. They face complex challenges to secure devices against cyber-attacks. Network authentication is highly required as IoT is growing, and it is essential to have an effective device authentication mechanism

2023 IEEE International Conference on Electro Information Technology (eIT) | 978-1-6654-9376-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/EIT57321.2023.10187363

978-1-6654-9376-5/23/$31.00 ©2023 IEEE

to identify the trusted device [7]. Because of the increasing demand for IoT devices, these devices must be inexpensive and challenge the implementation of security functions. Authentication is considered to be the first obstacle to securing IoT systems against various types of attacks. Therefore, using physically unclonable functions (PUF) could solve many IoT security requirements at an acceptable cost [8]. PUFs are low-cost, hardware security primitive for intelligent and energy-constrained IoT devices. Research for IoT authentications and encryption schemes has proposed the use of PUFs as a low cost solution [9]. Therefore, IoT and smart devices will need to find robust solutions for the IoT devices' security to protect communication over the internet and reduce the new security attacks. Physical Unclonable Functions (PUFs) have been proposed as a lightweight, cost-efficient solution. Implementing a PUF circuit in reconfigurable hardware like a Field Programmable Gate Array (FPGA) ensures secure authentication for IoT devices [10].

B. *PUF-Based Threats on IoT Devices*

Attacks on Internet of Things (IoT) devices are increasing rapidly; therefore, there are many potential threats for IoT devices that use PUFs for authentication. Possible definitive attacks include reading out private keys from memory, and communication attacks [11]. The main new threat on the PUF-based security system is for an attacker to obtain the ability to provide the correct response for a given challenge. Modeling attacks are an example of the emerging attacks that aim to replicate the behavior of PUF's challenge and response for cloning the secret keys generated by a PUF design[12]. Modeling attacks against PUF-based schemes for IoT devices authentication are classified into different categories:

1) *Machine Learning (ML) attacks*

Researchers have found that PUFs are vulnerable to various machine learning modeling attacks; therefore, ML attacks are considered one of the most successful attacks to clone the behavior of PUF design. Several machine learning-based modeling attacks have been analyzed to mimic the behavior of the PUFs [13]. The efficiency of these algorithms can be determined by the complexity of the different PUF designs [14].

2) *Man in the Middle Attack*

In this type of attack, an adversary can extract and record the data packets on the communication network between a server and a device and prevent and store exchanged CRPs [15]. Therefore, after obtaining a set of CRPs, a PUF can be modeled using machine learning.

3) *Side-channel hardware-based attacks*

Side-channel attacks use various parameters such as current leakage, voltage variations, and power consumption to establish an attack against semiconductor integrated circuits (IC) and internet of things (IoT) devices [16]. These attacks take advantage of the side challenge parameters to model a robust PUF design.

III. Device Authentication in IoT using Delay-based PUF

Device authentication is one of the essential tasks in IoT. The authentication scheme in IoT devices guarantees a more secure and efficiently interoperable alternative to IoT systems. Nevertheless, the remarkable number of smart devices makes it challenging to secure their authenticated and certified whenever connected to the IoT system. Most existing IoT systems are secured through authentication, ensuring connected IoT devices can access the resource. Here we focus on the authentication of users and devices in IoT using the Physical Unclonable Function (PUF) to enable IoT systems to handle authentic and verified devices.

A. *Implementation of XOR-ROPUF Design*

PUF is a robust security mechanism that recognizes a hardware fingerprint, and it provides a unique hardware key depending on the specific device properties. PUFs are commonly used for authentication and secure communication, which fits appropriately into the resource demands of IoT devices. A probable solution can be provided using PUF to generate a unique response for each device due to manufacturing variation. The proposed XOR-ROPUF enhances entropy, allowing the design to generate challenge-response pairs for secure and trusted IoT applications that require robust and lightweight secret and cryptographic key generation. Our lightweight PUF design is a low-cost and efficient hardware security design intended to generate low-cost secret keys for IoT security, including IoT robust authentication. The design of the PUF has been proposed earlier in our work [12]. The design is implemented on Xilinx Artix 7 FPGAs installed on the Diligent Nexys 4 board. Fig. 2 represents the implemented XOR-ROPUF, the responses generated from the PUF are fed back to the challenge generator. An XOR network takes the challenges from the challenge generator and combines the response to generate a new challenge. The PUF design takes a 16-bit challenge and generates a 16-bit response.

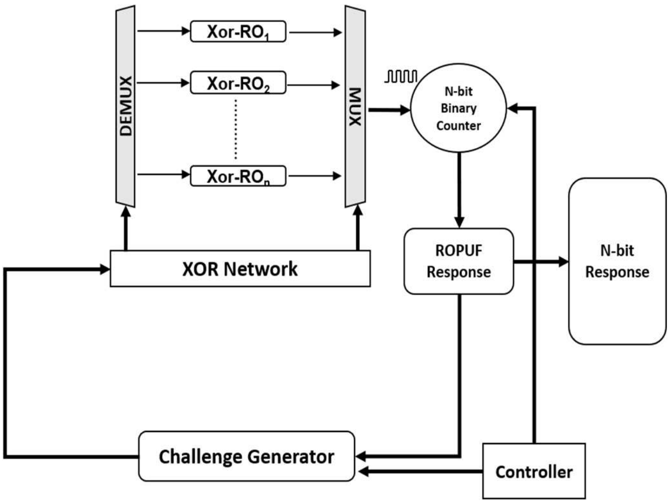


Fig. 2. XOR-ROPUF Design.

B. Proposed PUF-Based Authentication Scheme

The device authentication scheme is proposed for IoT applications using a lightweight XOR-ROPUF. The main objective of using the PUF model is to carry out the authentication between the verifier (verification authority) and prover (IoT Device). This scheme presents a suitable technique for authentication using a model of the PUF that provides a compact solution for the authentication of IoT systems. Fig. 3 shows the proposed scheme between the IoT devices and the authentication server to ensure data congeniality and integrity. The proposed PUF-based IoT device authentication scheme reduces the risk of authentication vulnerability. The proposed technique can be performed by storing and updating challenge and response pairs through communication with the IoT devices to be authenticated.

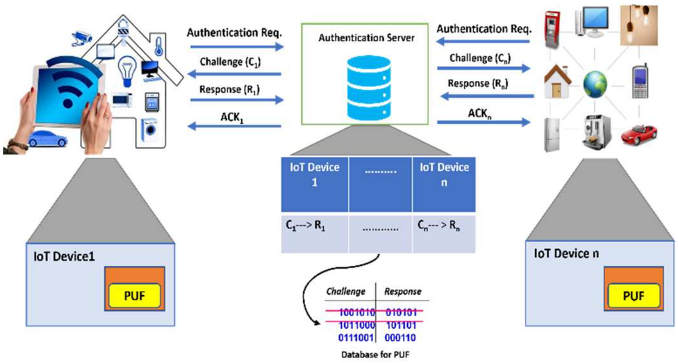
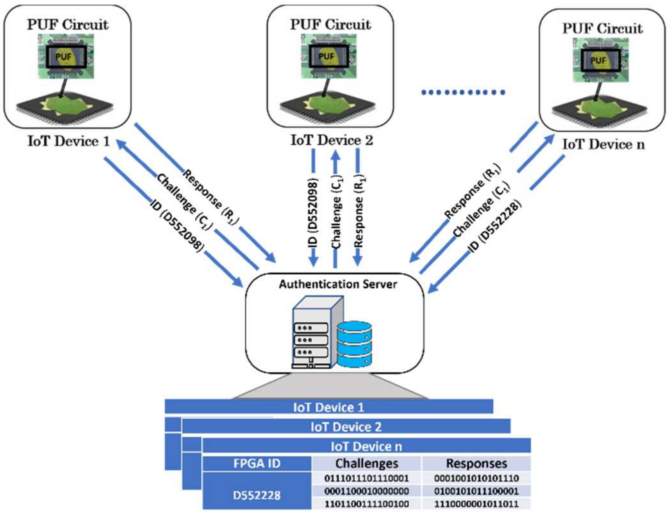


Fig. 3. PUF-based IoT Device Authentication scheme.

The PUF-based scheme eliminates some drawbacks because it is a low-cost device authentication solution to identify the trusted hardware. It secures communication among the devices using a lightweight system. IoT device identity can be verified through verification authority to establish trust in an IoT device. The PUF-based authentication scheme consists of a two-step process: enrollment and verification, which ensures the authentication.

- The first phase of the authentication process is Enrollment: During the enrollment phase, the IoT device embedding the PUF is directly connected to the server (verification authority). The authentication server sends challenges, and the IoT device embedding the PUF circuit sends back the responses. The authentication server stores all challenge and response pairs in a secure database by taking and performing each entity. During the enrollment phase, the IDs of all entities are recorded in the database by the verifier. Then the device can be deployed. Fig. 4 shows how the PUF chip is enrolled individually with the authentication server. The challenge-response pairs (CRPs) are collected and stored during enrollment. The authentication server has a database that stores all challenges for each PUF. The server sends one challenge (Ci) to each PUF and records the response (Ri) generated from each PUF in the database.



FPGA ID	Challenges	Responses
D552228	0111011101110001	0001001010101110
	0001100010000000	0100101011100001
	1101100111100100	1110000001011011

Fig. 4. Enrollment phase of PUF in Authentication scheme.

- The second phase is Verification: During the verification phase, the IoT device needs to be authenticated by the verification authority. Each IoT device is being identified by its unique ID. The server receives the entity's ID, sends an arbitrary PUF challenge to the IoT device, and checks against the previously registered value in its database. The authentication scheme to authenticate the IoT devices is explained in Fig. 5.

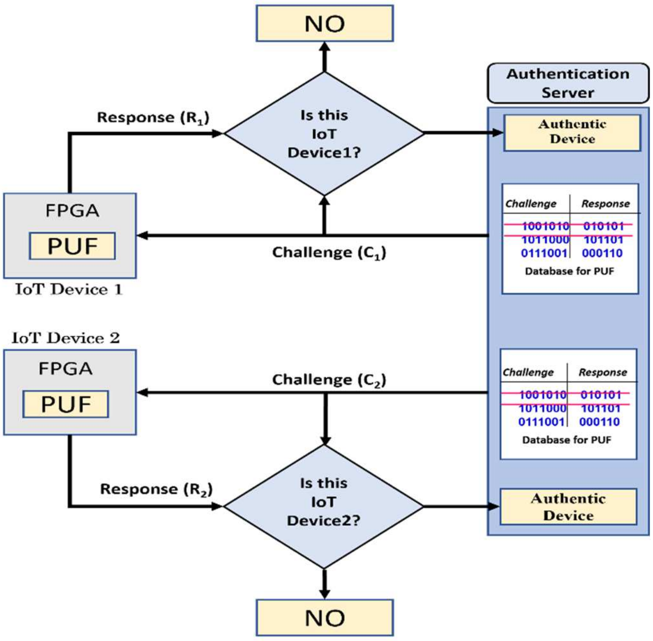


Fig. 5. PUF based Device Verification phase.

The CRPs obtained from different Artix 7 FPGAs are listed in Table I. The IoT device is authenticated if the measured response matches the stored response in the verification authority database. Only if the two values match can the verification authority conclude that the IoT device is authentic.

TABLE I. CHALLENGE- RESPONSE PAIRS FOR DIFFERENT FPGAS

IoT Device	FPGA ID	Challenges	Responses
1	D552098	0111011101110001 0001100010000000 1101100111100100	1000000000110101 0001110011001101 1100000100110110
2	D552320	0111011101110001 0001100010000000 1101100111100100	1010111000000010 0010010010001010 1100001001110101
3	D552224	0111011101110001 0001100010000000 1101100111100100	1010011001010001 1101011001001001 0011111010001010
………..	…………	………………..	………………………
n	D552228	0111011101110001 0001100010000000 1101100111100100	0001001010101110 0100101011100001 1110000001011011

Our proposed PUF based device authentication scheme is well suited for IoT devices with good reliability. The different parameters (Uniformity, Uniqueness, Bit aliasing, Reliability) for the XOR-ROPUF have been measured and are shown in Table II. However, ten different Artix-7 FPGAs are used for data acquisition for calculating the parameters. For comparing the data with other similar designs, PUF metrics from other designs are included in Table II. The performance of the PUF with quantified parameters and results show that our proposed device authentication scheme is suited for hardware security.

TABLE II. ROPUF PARAMETERS (PERFORMANCE METRICS FOR PUFS)

Design	Uniformity	Uniqueness	Bit-Aliasing	Reliability
XOR- ROPUF	50.76%	49.40%	48.35%	99.8%
Inverter ROPUF [17]	47.02%	45.15%	47.20%	98.0%
ROPUF [18]	50.56%	47.24%	50.56%	99.14%
APUF [18]	55.69%	7.20%	19.57%	99.76%

The hardware implementation of the XOR-ROPUF leverages the inherent physical characteristics of the FPGA to secure, reliable, and trusted IoT applications. The proposed secured PUF based scheme eliminates some drawbacks of traditional approaches and explains how PUFs can be used to build low-cost authentication schemes. The proposed PUF-based security enhancement scheme addresses the need for a high-security IoT network.

IV. CONCLUSION

An authentication scheme is proposed for the security of IoT systems using a lightweight XOR-ROPUF. The proposed management scheme carries out the authentication between the verification authority, the authentication server, and the IoT devices to ensure data congeniality and integrity. The proposed XOR-ROPUF based scheme is a low-cost device authentication solution to identify the trustworthiness of the devices. It secures the communication exchange amongst the devices using a lightweight system, and reduces the risk of authentication vulnerability.

REFERENCES

[1] Evans, Dave. "The internet of things: How the next evolution of the internet is changing everything." CISCO white paper 1.2011 (2011): 1-11.

[2] Al-Fuqaha, Ala, et al. "Internet of things: A survey on enabling technologies, protocols, and applications." IEEE communications surveys & tutorials 17.4 (2015): 2347-2376.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for Smart Cities," IEEE Internet of Things Journal, vol. 1, pp. 22-32, 2014.

[4] P. Gope and B. Sikdar, ``Lightweight and privacy-preserving two-factor authentication scheme for IoT devices,'' IEEE Internet Things J., vol. 6, no. 1, pp. 580_589, Feb. 2019.

[5] A. Sengupta and S. Kundu, ``Guest editorial securing IoT hardware: Threat models and reliable, low-power design solutions,'' IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 25, no. 12, pp. 3265_3267, Dec. 2017.

[6] C. Dong, G. He, X. Liu, Y. Yang, and W. Guo, ``A multi-layer hardware Trojan protection framework for IoT chips,'' IEEE Access, vol. 7, pp. 23628_23639, 2019.

[7] Babaei, Armin, and Gregor Schiele. "Spatial reconfigurable physical unclonable functions for the Internet of Things." International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage. Springer, Cham, 2017.

[8] X. Xin, J. Kaps, and K. Gaj, ``A configurable ring-oscillator-based PUF for Xilinx FPGAs,'' in Proc. 14th Euromicro Conf. Digit. Syst. Design, Oulu, Finland, 2011, pp. 651_657.

[9] B. Zhao, P. Zhao, and P. Fan, ``EPUF: A lightweight double identity verification in IoT,'' Tsinghua Sci. Technol., vol. 25, no. 5, pp. 625_635, Oct. 2020.

[10] Mukhopadhyay, Debdeep. "PUFs as promising tools for security in internet of things." IEEE Design & Test 33.3 (2016): 103-115.

[11] Wallgren, Linus, Shahid Raza, and Thiemo Voigt. "Routing attacks and countermeasures in the RPL-based internet of things." International Journal of Distributed Sensor Networks 9.8 (2013): 794326.

[12] Hazari, Noor Ahmad, Ahmed Oun, and Mohammed Niamat. "Machine Learning Vulnerability Analysis of FPGA-based Ring Oscillator PUFs and Counter Measures." ACM Journal on Emerging Technologies in Computing Systems (JETC) 17.3 (2021): 1-20.

[13] A. Oun and M. Niamat, "Design of a Delay-Based FPGA PUF Resistant to Machine Learning Attacks," 2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS), 2021, pp. 865-868, doi: 10.1109/MWSCAS47672.2021.9531815.

[14] A. Oun, N. A. Hazari and M. Y. Niamat, "Analysis of Swarm Intelligence Based ANN Algorithms for Attacking PUFs," in IEEE Access, vol. 9, pp. 121743-121758, 2021, doi: 10.1109/ACCESS.2021.3109235.

[15] Halak, Basel, Mark Zwolinski, and M. Syafiq Mispan. "Overview of PUF-based hardware security solutions for the Internet of Things." 2016 IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS). IEEE, 2016.

[16] S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.-P. Seifert, C. Boit, and H.-W. Hubers, ``Photonic side-channel analysis of arbiter PUFs,'' J. Cryptol., vol. 30, no. 2, pp. 550_571, 2017.

[17] Mustapa Muslim, Mohammed Y. Niamat, Atul Prasad Deb Nath, and Mansoor Alam. "Hardware-oriented authentication for advanced metering infrastructure." IEEE Transactions on Smart Grid 9, no. 2 (2016): 1261-1270.

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