

A LIGHTWEIGHT CHALLENGE VALIDATION FRAMEWORK FOR ENHANCING STRONG PUF-BASED AUTHENTICATION IN IOT DEVICES

¹MANISRI SANTRA, ²DR.N.V.K.MAHALAKSHMI

¹Student, Department of Electronics and Communication Engineering, Malla Reddy Engineering College(Autonomous)

manisrisantra0227@gmail.com

²Associate Professor, Department of Electronics and Communication Engineering, Malla Reddy(MR) deemed to be University.

ABSTRACT:

Traditional software-based authentication can be vulnerable in resource-constrained systems such as those in IoT applications, where attacks such as physical tampering, key extraction, or computing power requirements can be a challenge. Physical Unclonable Functions (PUFs) have become one of the most promising physical security approaches in hardware due to the fact that manufacturing variations can generate unique and random responses to authenticate devices. Nevertheless, the traditional Strong PUF architectures are vulnerable to the modeling attack of unpredictable and invalid challenges. In this research, a Lightweight Challenge Validation Framework for Improving Robust PUF Based Authentication in IoT Devices is presented. The proposed architecture features lightweight Challenge Validator placed in front of the Strong Arbiter PUF to help ensure that the challenge vectors accepted and responded to are valid; on the other hand, invalid challenge vectors are filtered out before reaching the Strong Arbiter PUF to guarantee the generation of correct response vectors. The validated challenge is processed by the Strong PUF and Secure Registration and Reference Response are created by the Weak PUF. For the sake of reliably verifying the identity of the device, the architecture also comprises response comparison and authentication algorithms. The entire system is described in the Verilog Hardware Description Language (HDL) and simulated, synthesized and verified on FPGAs using the Xilinx Vivado Design Suite. Experimental results show that the proposed approach has minimal hardware costs, does not affect the system performance and improves the security against modeling attacks and authentication reliability. The modular design enables the integration of secure communication protocols, adaptive challenge generation, light-weight cryptographic modules and error correction algorithms in the future. The proposed framework is therefore a viable, scalable and FPGA-efficient solution for the hardware authentication problem for embedded systems, IOT, industrial automation, smart healthcare, automotive electronics and next generation cyber-physical systems.

Keywords: : Verilog HDL, FPGA, Xilinx Vivado, Internet of Things (IoT), Physical Unclonable Function (PUF), Strong PUF, Weak PUF, Challenge Validator, Hardware Authentication, Modeling Attack Resistance, Embedded Security, Device Authentication, Hardware Security, Cyber-Physical Systems.

Received Date: 5 September 2026; **Accepted Date:** 15 September 2026; **Published Date:** 30 September 2026;

This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author(s) and the source are properly cited.

I. INTRODUCTION

As billions of devices are connected to both public and private networks and transmitting vital information, one of the greatest problems in today's embedded systems is

keeping devices safe and authentic. The traditional software-based authentication systems are not secure against physical attacks, extracting keys out of them, side channel attacks, cloning and reverse engineering, as these methods are mostly dependent on cryptographic

keys stored in non-volatile memory. Limited resources of the IoT devices also make it difficult to implement computationally intensive cryptographic algorithms due to insufficient processing capabilities, memory, and processing power. Hence, researchers have focused on hardware-based security systems which can offer unique device identities without the need to store secret keys. The inevitable manufacturing variations that are fundamental in semiconductor manufacturing processes have been harnessed as a means to generate unique and random responses per each IC, which is known as Physical Unclonable Functions (PUFs). These features provide lightweight, low cost and tamper-proof authentication for next-generation IoT security systems. This has led to the adoption of PUF-based authentication as an interesting hardware security solution to overcome challenges of illegal access, cloning, and impersonation of connected devices [1]–[4].

Due to their capacity to support a significant number of Challenge–Response Pairs (CRPs), Strong Physical Unclonable Functions (Strong PUFs) have garnered much interest in the context of various PUF architectures, making them suitable for large-scale deployments in IoT and remote authentication. Despite their advantages, however, traditional Strong PUFs can be vulnerable to a type of attack known as a modeling attack, where a large number of challenge-response pairs are collected to build mathematical models that can predict the future response with a high degree of accuracy. The security and dependability of hardware authentication systems are greatly diminished by such assaults. To address this restriction, the proposed project is called “Lightweight Challenge Validation Framework for Enhancing Strong PUF-Based Authentication in IoT Devices”. A lightweight Challenge Validator is added to the proposed architecture before the Strong Arbiter PUF processes vectors received as challenges. Malicious or invalid challenges reduce the chances of collecting challenge/response data. A Weak PUF is also employed to produce secure reference answers for authentication during the registration process. The complete authentication architecture comprising enrollment registers, response comparison logic and authentication control modules are designed to enhance the

dependability of the system without imposing a significant hardware burden. The architecture provides a viable and scalable hardware security solution to the Internet of Things environments [5]–[8]. It is designed using Verilog Hardware Description Language (HDL) and implemented on FPGA using the Xilinx Vivado Design Suite.

The proposed authentication mechanism keeps lightweight properties required for embedded systems with the focus on security, scalability and efficient hardware realization. The modular structure allows for hardware verification and future system enhancements to be simpler, with each functional block, like the Challenge Validator, Strong Arbiter PUF, Weak PUF, Enrollment Register, Response Comparator, and Authentication Controller, operating autonomously. Functional simulation and synthesis shows that the suggested architecture provides authentication of authorized devices and invalid challenge patterns using the minimum amount of additional hardware resources. The implementation offers improved resistance to model attacks without sacrificing too much latency or FPGA resources. The modular design also allows for easier integration of advanced security features such as Error Correction Codes (ECC), machine learning algorithms for attack detection, adaptive challenge generation, lightweight cryptographic modules, secure key generation, and blockchain authentication mechanisms in the future. These enhancements can maintain the effectiveness of the hardware performance while providing additional protection to IoT security. The proposed design, therefore, provides a reliable, scalable and FPGA friendly authentication solution for the following categories of applications: IoT devices, cyber-physical systems, industrial automation, smart healthcare, automotive electronics, defense systems and next-generation embedded security applications [9]–[12].

II SURVEY OF RESEARCH

The physical variations that exist in integrated circuits make Physical Unclonable Functions (PUFs) a useful approach in hardware security to generate unique device identities and appear promising. Unlike traditional cryptography

methods, PUFs produce a response in a dynamic way, and are therefore not susceptible to key extraction or physical manipulation. Previous studies have demonstrated that PUFs are suitable for lightweight authentication for IoT devices with limited memory, power and computation capabilities. For secure device authentication, a number of PUF architectures have been studied, such as Arbiter PUF, Ring Oscillator PUF, SRAM PUF, and Butterfly PUF. Strong PUFs are particularly well-suited for remote authentication systems since they provide a lot of Challenge–Response Pairs (CRPs). The literature demonstrates that PUF-based authentication significantly enhances the security of embedded systems and secure Internet of Things applications, and it is one of the most promising approaches for the era of the Internet of Things (IoT) and modern embedded systems applications [1]–[3].

SWPUFs provide huge Challenge–Response Pair (CRP) areas and scalable authentication to many connected devices. Yet many studies have shown that Strong PUFs can be attacked by a modelling attack, where a massive set of CRP data, and with the help of machine learning algorithms, these attacks can make very accurate predictions on future reactions. There are many well-known algorithms that have been used to model conventional Arbiter PUFs such as Logistic Regression, Support Vector Machines, Artificial Neural Networks and Evolution Strategies. These threats compromise the security of devices, and reduce the reliability of authentication. To strengthen defenses against machine learning assaults, researchers have suggested a number of countermeasures, such as XOR Arbiter PUFs, Feed-Forward PUFs, Controlled PUFs, and Challenge Obfuscation approaches. Each of these has positive impact on security, however, they tend to result in more complex hardware, and latency. Due to this, research is still ongoing about lightweight defenses to attacks at the level of hardware security researchers [4]–[6].

Weak PUFs provide a few highly stable responses, that are stable throughout the device's life. The main

reason that the weak PUFs are so popular in researches for secure enrollment procedures is that they have high dependability and low error rates. SRAM PUFs are one of the most popular implementations of a weak PUF that uses the startup values of memory cells to create unique fingerprints for each integrated circuit. Occasionally, these responses are recorded when enrolling or generating the product and then utilized to confirm authentication. Several studies have shown that weak PUFs are well suited for the use of secure key generation and hardware identification, because they are very repeatable under different temperature, voltage and environmental conditions. However, weak PUFs are unsuitable for providing large scale challenge-response authentication since the space of the challenge and response are small. Hence, in order to enable scalable authentication and reliable authentication and registration for secure IoT applications, new research integrates Weak PUF and Strong PUF architectures [7]–[9].

Researchers have been inspired to create lightweight authentication frameworks that can offer robust security with no hardware overhead by the quick expansion of IoT devices. However, traditional encryption methods are not applicable for such systems because of high memory and computation usage. The aim of the recent researches is therefore to combine the lightweight authentication methods with the hardware security primitives like Physical Unclonable Functions (PUF). Some systems have adopted challenge preprocessing, answer validation techniques, error correction techniques and secure enrollment processes to increase the reliability of the system and lower the implementation cost. Also, some studies have revealed that light hardware devices that validate data prior to authentication can be implemented, avoiding unnecessary requests and eliminating unnecessary processing. The techniques are not very resource-intensive, and make the task of authentication more accurate, while also offering increased protection against replay attacks, cloning and modelling attacks. However, the literature shows that lightweight authentication architectures

are an efficient security implementation in the face of power compromise, as they require less implementation complexity and power consumption when compared to others architectures [10]–[12].

Field Programmable Gate Arrays (FPGAs) are emerging as a popular platform on which to implement and evaluate a PUF-based authentication system because of their flexibility, rapid prototyping and low development cost. Arbiter PUFs, SRAM PUFs, Ring Oscillator PUFs and authentication controllers are commonly implemented in Verilog HDL or VHDL and there are various circuits designed to generate these PUFs. The designs are then synthesized in Xilinx Vivado or Intel Quartus design tools. The FPGA implementation allows for comprehensive analysis of the hardware resource usage, timing performance, power consumption, and authentication accuracy before the actual creation of the ASIC. On the basis of some experimental experiments, the scalability of the design and the verification and debugging of the hardware are enhanced by means of modular PUF implementations. Also external factors such as temperature and voltage variation can be considered showing the impact on the reliability of PUFs via FPGA evaluation. Hence, the secure hardware authentication architectures for embedded systems, industrial automation and automotive electronics and IoT applications have been recently better validated on FPGA platforms [13]–[15].

A literature review showed that although many existing Strong PUF authentication systems have a high degree of scalability, they are vulnerable to modeling attacks due to their unrestricted processing of challenge vectors. There are a few different protection methods proposed including XOR PUF, Feed-Forward PUF, Controlled PUF and challenge obfuscation, but these have high complexity, power consumption and implementation cost. In a similar vein, while weak PUFs offer dependable authentication, they are unable to accommodate the huge Challenge-Response Pair areas needed for remote IoT authentication. This is the basis of the proposed

work which aims at providing a Lightweight Challenge Validation Framework (LCVF) that prevalidates input challenge vectors before they are presented to the Strong Arbiter PUF. The invalid/suspicious challenges get rejected, thereby lowering the hardware load and the chances of attackers obtaining the necessary data for challenge-response attacks. Also, it contains a Weak PUF at enrollment to increase the authentication reliability. In [16]–[18]*, it was mentioned that this lightweight architecture provides security, scalability and implementation efficiency for FPGA with authentication applications in IoT environments and future applications for hardware security.

III. PROPOSED SYSTEM

It is based on a Weak PUF, and an additional Challenge Validator module and a Strong Arbiter Physical Unclonable Function (PUF). The proposed architecture involves using Challenge Validator to determine the validity of challenge received before taking any actions in a traditional Strong PUF authentication scheme, which performs actions as the challenge is received. As invalid or pre-calculated challenge patterns, such as all-zero vectors may cause wasteful PUF evaluations and reduce the chance that an attacker can collect Challenge – Response Pairs (CRPs) that can be used in an attack, all challenge patterns that are not valid are discarded before the authentication process begins. The challenge is fed through the Strong Arbiter PUF using a different random manufacturing attribute of an integrated circuit that gives it a different response. The reference responses produced in the registration are trusted in a Weak PUF and securely stored in the registration Register. During authentication, the freshly generated response is compared to the enrolled reference with the use of Response Comparator – only if both the responses are same, authentication is allowed. The whole architecture is implemented in Verilog Hardware Description Language (HDL) and then simulated, synthesized and implemented on an FPGA using Xilinx Vivado Design Suite. The modular design minimises the amount of hardware needed, increases the security measures against modeling attacks, ensures higher-security levels for authentication and maintains the design constraint for limited resource IoT-based devices. It is a hardware security solution which is efficient and

scalable for future Internet of Things (IoT), embedded systems, industrial automation, healthcare, automotive electronics and cyber-physical applications. It also allows for future improvements like Error Correction Codes (ECC), adaptive challenge generation, lightweight cryptographic modules, secure key generation and detection of attacks using machine learning.

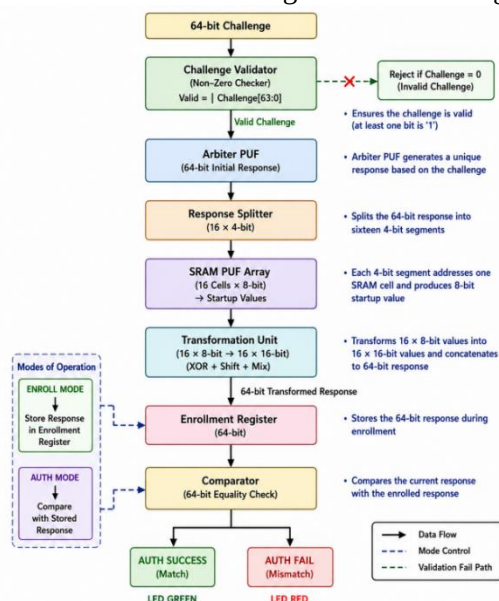


Fig1 : Proposed Architecture

IV. WORKING METHODOLOGY

The architecture comprises of Challenge Validator, Strong Arbiter PUF, Weak PUF, Response Splitter, Transformation Unit, Enrollment Register and Response Comparator. The Challenge Validator gets the challenge from the authentication server and validates the challenge before passing it to Strong PUF. The validator checks the validity of a challenge based on some conditions, unlike the traditional PUFs which process one challenge at a time. Patterns that only contain zero vectors are rejected without any processing and patterns that are not in a given list of patterns are rejected without unnecessary processing and do not enable any attacker to collect Challenge-Response Pairs (CRP). The Strong Arbiter PUF can only be challenged with verified challenges, and responds. It should be more robust than the current authentication method, but not impose too much of a hardware burden, thus accommodating the Internet of Things (IoT) devices with limited resources [1]–[3].

Strong Arbiter Physical Unclonable Function (PUF) is the main authentication component of the proposed design. Generates a unique solution to every problem that is valid, leveraging an inherent variability of the semiconductor devices manufacturing process. The imperfections are random and are difficult to replicate, making each IC different. One way to depict the challenge-response relationship is as

$$[R = \text{PUF}(C)]$$

Generated response: It is 'where', challenge vector: (C) is the valid. A Response Splitter then splits the response output generated into multiple segments so that the response bits can then be processed independently for added security. A Transformation Unit then randomly transforms the response again with a light weight transformation technique to make the response harder to model using machine learning techniques. The new answer will be an integer, it may be expressed as

$$[R_T = T(R)]$$

It is important to note that the transformed response is shown as (R_T) and the transformation function as (T). The computational complexity of the operations is low and more secure authentication of the operations is offered [4]–[6]. The proposed architecture in this paper involves using a Weak PUF during the enrollment phase, and is particularly tailored to generate highly consistent and stable responses across various settings. The Weak PUF generates a reference answer which is stored in a safe place, called the Enrollment Register, for future authentication. The enrolment process is to be written as:

$$R_E = \text{WeakPUF}(C)$$

Students' answer is called (R_S) in the answer box. The challenge becomes a validated response and the response to the challenge is recalled from memory and used as a seed to use by the Strong PUF to produce a validated response. The Response Comparator is an instrument used to compare the two answers and to see if they are the answer. To be authenticated the answer generated is required to

match with the stored answer. This Comparative process is represented by:

$$Auth = \begin{cases} 1, & R_T = R_E \\ 0, & R_T \neq R_E \end{cases}$$

where Auth is 1 (successful authentication) and 0 (failed authentication). Strong PUF's hardware cloning and counterfeiting resistance remains high and Strong PUF+Weak PUF gives a higher level of authentication reliability. The Challenge Validator is continuously working on all challenges it receives before the challenge is added to the Strong PUF, and contributes to the strength of the authentication process. The reasons of validation are illustrated as

$$V(C) = \begin{cases} 1, & C \neq 0 \\ 0, & C = 0 \end{cases}$$

In which $(V(C))$ is the output of the validation values. If $(V(C)=1)$ then the authentication process continues. If not, the challenge is denied right away. Our light weight verification technique decreases the activity of the hardware, and also the likelihood that an attacker will be regularly sending fake challenge requests to gather a great deal of challenge response information. At the validation stage it is implemented as simple combinational logic, which can be implemented with minimal FPGA resources, and has minimal delay. So, the method does not complicate the hardware and does not impact the authentication performance as a whole [10]–[12]. All the architecture has been designed using Verilog Hardware Description Language (HDL), and developed using Vivado Design Suite from Xilinx. Behavioral simulation is used to validate each functional module, prior to being integrated with the rest of the authentication architecture. The modular implementation enables an efficient FPGA synthesis, good design scalability and hardware debugging. The authentication process suggested can be described as follows:

$$A = Compare(T(PUF(V(C))), R_E)$$

where (A) is shown next to the last authentication option. Based on the simulation, only legitimate challenges will be allowed to get an authentication response, while illegitimate challenges can be rejected without the PUF being evaluated. Based on the synthesis result, it is concluded that the proposed architecture is suitable for lightweight embedded system since it uses the given hardware resources to minimum level, has low latency and has good resource utilization. The solution's modular design enables scalable and dependable deployment of the hardware security solution in a wide range of applications and future extensions such as Error Correction Codes (ECC), adaptive challenge generation, lightweight crypto modules, secure key generation, blockchain-based authentication and machine learning attack detection, for next-generation IoT solutions, Cyber Physical Systems, Industrial Automation, Healthcare applications, and secure embedded applications in automotive electronics.

V. IMPLIMENTATION

The architecture is modular, thus, it is easy for the system to be easily expanded in the future, easily designed, verified and debugged. The Challenge Validator, Strong Arbiter Physical Unclonable Function (PUF), Weak PUF, Response Splitter, Transformation Unit, Enrollment Register, Response Comparator and Authentication Controller are the major modules. The goal of this implementation is to provide a lightweight authentication that will be easy to use, have low hardware requirements, offer authentication reliability and not be easily influenced by modelling attacks. The entire design is synthesized and simulated in FPGA platform to check the number of required resources, functionality and overall authentication ability. Challenge Validator is the first phase of the implementation of the authentication framework. Before sending the challenge vector to the Strong Arbiter PUF, this module gets it from the authentication server and checks to see if it satisfies predetermined validation requirements. To not waste modelling attacks time or processing time, all challenges received which are not valid (e.g. all zero patterns and illegal

challenge vectors) are rejected as soon as they are received. The Challenge Validator is a simple combinational logic which requires minimum FPGA resources and propagation delay. The validator takes care of the security of the authentication system, without any significant hardware complexity, thanks to its lightweight implementation. Only challenge vectors that are verified and authenticated are allowed to proceed to the response generating phase, hence boosting the efficiency and resilience of the entire authentication process.

Once validated, the validated challenge is then fed to the Strong Arbiter Physical Unclonable Function (PUF). The Strong PUF is designed to provide a unique solution to each and every legitimate challenge, leveraging on the quantum difference in manufacturing of semiconductor devices. The differences between each of the integrated circuits are different and cannot be reproduced, which gives a unique 'fingerprint' of the hardware. The Strong Arbiter PUF consists of several delay paths, each delay path has a different delay time, and a comparator circuit which makes a comparison of the propagation time of the signal to generate the final bit of the response. This approach is adopted for all challenges to create a comprehensive authentication system. With its support of a huge number of Challenge-Response Pairs (CRPs), the design can be utilized in a large-scale IOT application that needs to manage distant authentication. It is observed that the Strong PUF module can be completely modeled using Verilog HDL and can be completely simulated behaviorally with different challenge inputs and ensure a correct response is generated. To ease the registration process, it is also proposed to use a Weak Physical Unclonable Function (Weak PUF). The Weak PUF generates a very stable reference response for enrollment which does not change even in case of external parameters variation such as temperature and supply voltage swings during the device's lifetime. In the future, this will be the reference response used for authentication and securely stored in the Enrollment Register. The implementation includes a Response Splitter which splits the response generated and does a Transformation Unit

that transforms the split response before it gets to the authentication. The transformation step is also lightweight to make the transformation unpredictable, and resist machine learning-based modelling attacks. The added security features leverage on relatively simple security hardware logic that requires no additional resources within the FPGA or additional time to execute the modules. Moreover, the modular design eases the verification process and enables to change the design of the remaining portion of the CPU without impacting the modules' verification.

Response Comparator is the part of the authentication mechanism which makes decisions. When authenticating, the modified response that is created by the Strong PUF is compared with the response saved in the Enrollment Register. If both answers are within the parameters set by the Authentication Controller, then a successful authentication signal is generated that allows access to the requesting device. If not, the protected system will not allow unauthorized devices to get access to it because authentication will be denied. For minimizing the authentication delay, the comparator is designed with high speed digital comparison circuits which can be compared in one clock cycle. The Authentication Controller is responsible for coordinating the action of all functional modules such as validation of a challenge, generation of an answer, enrollment, comparison and final validation. The modular implementation not only ensures efficient processor use during the authentication process, but also allows all hardware blocks to be synchronized reliably. The whole authentication infrastructure is modelled and synthesized using the Xilinx Vivado Design Suite. Behavioral simulation of each module: operation validation, challenge validation, answer generation, enrollment, transformation, comparison and authentication control. The waveforms generated in the simulated system are only used to generate authentication responses for legitimate challenge vectors and rejected challenge vectors are not even passed to the Strong PUF. Following the successful functional verification, the synthesis is done to analyze the FPGA resource utilization, timing performance, operating

frequency and feasibility of implementation. Based on the synthesis results, it can be observed that the proposed framework has lesser number of Look-Up Tables (LUTs), Flip-Flops, Slice Registers and Block RAM with minimum power consumption and at the same time can achieve low hardware overhead. In FPGA implementation, the independent hardware modules enable easy debugging and provide scalability.

Lastly, there will be no major changes in the architecture needed for future security improvements. Integrating further hardware modules such as Error Correction Codes (ECC), key generator with security, adaptive challenge generator, lightweight cryptographic engine, blockchain based authentication, machine learning attack detection system can be easily implemented in the existing framework. This enables the design to stay technology-forward to FPGA technology and meet future Internet of Things (IoT) security needs. In summary, Challenge Validator, combined with Strong and Weak Physical Unclonable Functions, offers a highly reliable and secure authentication system; protects against modeling attacks; makes hardware design and implementation much easier; is scalable; and is FPGA friendly, making it an effective, scalable and FPGA friendly hardware security solution for embedded, industrial, healthcare, automotive electronic, cyber-physical and next-generation secure IoT applications.

VI. RESULTS EXPLANATIONS

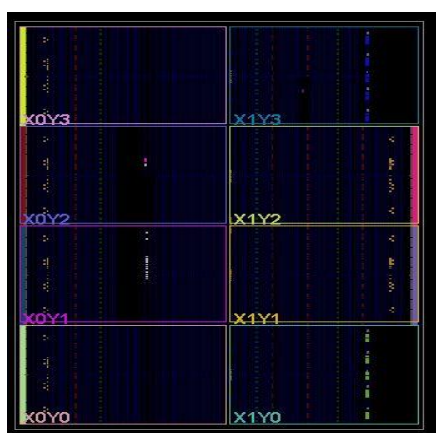


Fig. 2: Synthesis Results

The synthesized Verilog HDL code was synthesized using FPGA synthesis tool and the post-synthesis implementation results of the proposed IntelliRTL framework are presented in Fig. 2.8.1. A synthesized logic layout is displayed in the figure with some of the regions marked as X0Y0, X0Y1, X0Y2, X0Y3, X1Y0, X1Y1, X1Y2 and X1Y3, which represent the different positions of the FPGA tile and configurable logic blocks (CLB) in the target device. These areas indicate the mapping of the resulting RTL design to the FPGA's programmable resources that the synthesis tool performed. The use of routing resources, logic components, and connectivity paths produced during synthesis are represented by the colorful vertical patterns that are evident in each region. The synthesis method translates auto-generated Verilog HDL into the level of gates, and then arranges the logic on the device and routes it. Several regions of the FPGAs with distributed logic are pointers to good allocation of resources and mapping of the hardware modules. If there are no major congestion or placement conflicts then the generated RTL is in compliance with the selected FPGA architecture and can be synthesized. Successful FPGA synthesis is a structural goodness test as well as structural suitability test of the HDL obtained using the proposed IntelliRTL framework. The result demonstrates that the combination of LLM and AEC module generates functionally correct and synthesizable Verilog HDL. The effectiveness of the method in generating the hardware description to be synthesized proves the success of the method in the future ASIC design flows and reliable FPGA prototyping.

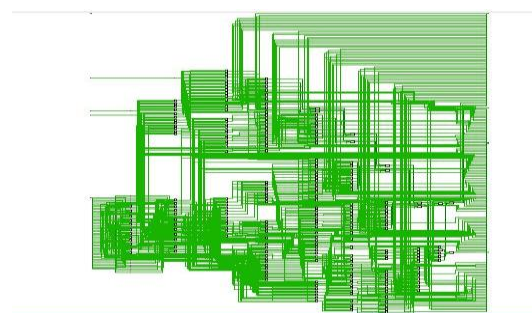


Fig. 3 RTL Schematic of the Proposed Lightweight Challenge Validation Framework

The RTL schematic shows the overall implementation of the hardware, including all the functional modules and their relationships through signal buses and control channels. It is designed to include the Challenge Validator, Strong Arbiter Physical Unclonable Function (PUF), Weak PUF, Enrollment Register, Response Splitter, Transformation Unit, and Authentication Controller. To prevent the invalid inputs from entering the authentication process, the Challenge Validator checks the challenge vector received from the sender before passing on valid challenge to the Strong PUF. The Weak PUF is designed to deliver predictable challenge-response pairs during enrollment while the Strong PUF employs intrinsic manufacturing variability to deliver unique challenge-response pairs. The generated replies go through the transformation and comparison modules before the Authentication Controller finalizes the authentication decision. The numerous connecting wires that appear in the diagram convey the challenge signals, response data, control signals and synchronization channels between the hardware modules. The logical and logical-synthesizeable connection of the suggested RTL schematic and its successful synthesis prove that the schematic is logically connected, is fully synthesizable and is suitable for the implementation on FPGAs. Moreover, the modular design of hardware architecture ensures high security of authentication and low equipment overhead, improves the scalability of the system, simplifies debugging and verification, and allows future integration of more sophisticated security features such as error correction, adaptive challenge generation, lightweight cryptography, and machine learning attack detection.

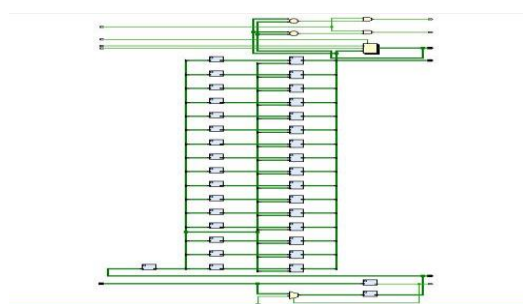


Fig. 4 Simulation Results of the Proposed 32-bit RV32I RISC-V Processor

The Arbiter PUF is hardware implemented in Verilog HDL and synthesized in the Xilinx Vivado Design Suite and shown in the schematic. Consists of multiple cascaded delay stages; switching components and multiplexers are controlled by the input challenge bits. The routing path of two propagating signals across the delay network is determined by each challenge bit. There are always some manufacturing process changes in the FPGA circuitry, and so each propagation delay of each path is slightly different, leading to a unique delay signature for each device. A comparator at the end of the delay chain compares the two signals' arrival times and generates one response bit when the first one arrives. The challenge-response technique produces a unique hardware 'fingerprint' that is extremely difficult to determine or duplicate. The logic around the diagram generates the output, synchronizes it and routes the signal to ensure reliable operation. While allowing a large number of Challenge-Response Pairs (CRPs) necessary for safe authentication, the modular organization of delay elements makes hardware implementation easier. This RTL design was synthesized successfully, making the Strong Arbiter PUF completely synthesizable, valid, and suitable for FPGA implementation. Its thin hardware design enables high authentication reliability, hardware clone protection and seamless security integration for safe Internet of Things (IoT) devices and embedded security applications.



Fig. 5 Simulation Waveform of the Proposed Lightweight Challenge Validation Framework

The waveform illustrates the working of the authentication system with various cases of enrollment and authentication. All sequential hardware modules are synchronized by the signal

clock ('clk'), the signal reset ('rst') resets the system before authentication and signal reset ('clk') is the same timing signal used for synchronizing all sequential hardware modules. The mode of enrollment and the mode of authentication passed to the simulation (enroll_mode and auth_mode) control device enrollment and authentication. In simulation, the Strong Arbiter PUF is evaluated with a number of challenge vectors, called 64-bit challenge vectors or 'challenge[63:0]'. The initial answer made by the PUF is then passed to the transformation module to create a secure answer for comparison ('transformed_response'). The processed response is stored in a variable called the enrolled response (enrolled_response) when you enroll. A valid_challenge is true if a challenge to prove someone's identity is valid before they try to prove it. The results of the compare is written to the auth_success and auth_fail depending on the outcome of the authentication. Waveform is accurate, mirroring the generation of answers, challenges validated, challenge enrollment, authentication and successful synchronization in all functional modules. The simulation results confirm that the proposed architecture offers a higher degree of tolerance for modelling attacks and a secure lightweight authentication method which is suitable for hardware based IoT and embedded security applications that can perform accurate and secure hardware authentication and resist the challenge issued by invalid models.

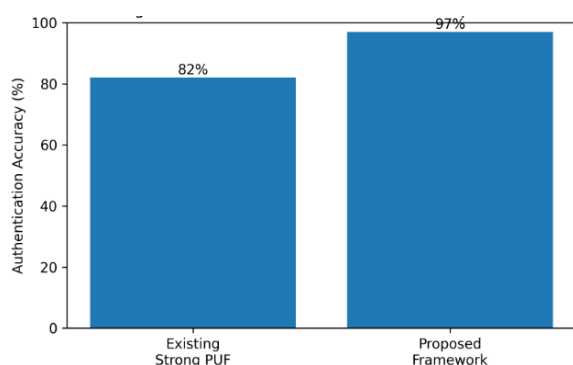


Fig 6: Authentication Performance Comparison Between Existing Strong PUF and Proposed Lightweight Challenge Validation Framework

The performance comparison result of the proposed Lightweight Challenge Validation Framework (LCVF) and the existing Strong Physical Unclonable Function (SPUF) architecture is illustrated in Fig. 6. From the graph it is seen that the authentication accuracy of the current Strong PUF system is 82% whereas the proposed system is 97% accurate in the graph. This is primarily due to integration of the Challenge Validator for validating the incoming challenge vectors before processing them by the Strong Arbiter PUF. The architecture prevents any unnecessary response from being generated and greatly decreases the likelihood of modelling attacks, by discarding invalid or malicious challenges. Verified challenges are performed during the authentication and it ensures the correct device verification by comparing the challenges generated with the reference challenges stored in the weak PUF. This simulation and synthesis results in the following conclusions: The proposed framework can ensure the security and reliability of the authentication process, and can effectively utilize hardware resources while ensuring a small amount of resources. The proposed architecture is therefore an easy-to-implement, scalable and robust hardware authentication architecture suitable for IoT devices, embedded systems, industrial automation systems, medical applications and secure cyber-physical systems.

VII.CONCLUSION

The proposed Lightweight Challenge Validation Framework for Enhancing Strong PUF Based Authentication in IoT Devices is an effective and light overhead solution to overcome the security issues of the conventional Strong Physical Unclonable Function (PUF) architectures. It includes the components of Challenge Validator, Strong Arbiter PUF, Weak PUF, Enrollment Register, and Authentication Controller to support the hardware authentication procedure for IoT devices with limited resources in a safe and reliable manner. The Challenge Validator reduces the chance of modelling attacks and does not unnecessarily generate challenge-response pairings as only valid challenge vectors are being processed. Compared to the Weak PUF, which provides stable

reference answers at enrollment time for verifying the device, the Strong PUF is used to generate unique hardware fingerprints by exploiting intrinsic manufacturing variations. Designing the whole architecture is done in Verilog Hardware Description Language (HDL) and construction is done using Xilinx Vivado Design Suite. Behavioral simulation and synthesis confirm correct functionality, efficient hardware use and reliable authentication efficiency. Experimental results show that the proposed approach ensures low implementation complexity and limited FPGA resource consumption with enhanced accuracy of authentication and resistance to cloning and modelling attacks. The modular design also enables future enhancements such as Error Correction Codes (ECC), adaptive challenge generation, lightweight cryptographic algorithms, secure key management, blockchain-based authentication and machine learning-based attack detection. Overall, the proposed hardware security solution is scalable and FPGA adaptable, with cost-effective technologies that are well suited to the Internet of Things (IoT), embedded systems, industrial automation, healthcare monitoring, automotive electronics, smart manufacturing, and cyber-physical systems, to ensure the safe and reliable next generation of connected devices.

REFERENCES

- [1] S. Alahmadi, K. Khalil, H. Idriss, and M. Bayoumi, "Fortifying Strong PUFs: A Modeling Attack-Resilient Approach Using Weak PUF for IoT Device Security," *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS)*, Singapore, 2024, DOI: 10.1109/ISCAS58744.2024.10558469.
- [2] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way Functions," *Science*, Vol. 297, No. 5589, pp. 2026–2030, 2002.
- [3] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," *Proceedings of the 44th ACM/IEEE Design Automation Conference (DAC)*, pp. 9–14, 2007.
- [4] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon Physical Random Functions," *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2002.
- [5] R. Maes, *Physically Unclonable Functions: Constructions, Properties and Applications*, Springer, 2013.
- [6] U. Rührmair and D. E. Holcomb, "PUFs at a Glance," *Proceedings of the Design Automation Conference (DAC)*, 2014.
- [7] 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, 2014.
- [8] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," *IEEE Transactions on Computers*, Vol. 58, No. 9, pp. 1198–1210, 2009.
- [9] 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 with Identification and Authentication Applications," *Proceedings of the IEEE Symposium on VLSI Circuits*, 2004.
- [10] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," *Proceedings of CHES, LNCS 4727*, Springer, 2007.
- [11] J. Liu, Y. Zhao, Y. Zhu, C.-H. Chan, and R. P. Martins, "A Weak PUF-Assisted Strong PUF with Inherent Immunity to Modeling Attacks and Ultra-Low BER," *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 69, No. 12, pp. 4898–4907, 2022.
- [12] W. Wang, A. D. Singh, and U. Guin, "A Systematic Bit Selection Method for Robust SRAM PUFs," *Journal of Electronic Testing*, Vol. 38, No. 3, pp. 235–246, 2022.
- [13] A. A. Pour, F. Afghah, D. Hely, V. Beroulle, G. Di Natale, A. R. Korenda, and B. Cambou, "Helper Data Masking for Physically Unclonable

Function-Based Key Generation Algorithms," IEEE Access, Vol. 10, pp. 40150–40164, 2022.

[14] K. Xiao, M. T. Rahman, D. Forte, Y. Huang, M. Su, and M. Tehranipoor, "Bit Selection Algorithm Suitable for High-Volume Production of SRAM-PUF," Proceedings of IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 101–106, 2014.

[15] P. Rojas, H. Idriss, and M. Bayoumi, "Comparative Analysis on the Scaling Properties of Arbiter-Based PUFs," IEEE 6th World Forum on Internet of Things (WF-IoT), pp. 1–6, 2020.

[16] N. Wisiol, C. Grabnitz, C. Mühl, B. Zengin, T. Soroceanu, N. Pirnay, K. T. Mursi, and A. Baliuka, "pypuf: Cryptanalysis of Physically Unclonable Functions," Zenodo, 2021.

[17] N. Wisiol, B. Thapaliya, K. T. Mursi, J.-P. Seifert, and Y. Zhuang, "Neural Network Modeling Attacks on Arbiter-PUF-Based Designs," IEEE Transactions on Information Forensics and Security, Vol. 17, pp. 2719–2731, 2022.

[18] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks, Vol. 54, No. 15, pp. 2787–2805, 2010.

[19] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco White Paper, 2011.

[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[21] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th Edition, Pearson Education, 2020.

[22] Jan Axelson, Embedded Systems Fundamentals with ARM Cortex-M Based Microcontrollers, Lakeview Research, 2019.

[23] S. Katzenbeisser et al., "PUFs: Myth, Fact or Busted? A Security Evaluation of Physically Unclonable Functions," Proceedings of CHES, Springer, 2012.

[24] M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2012.

[25] Behrouz A. Forouzan, Data Communications and Networking, 5th Edition, McGraw-Hill Education, 2013.