FDPUF: Frequency-Domain PUF for Robust Authentication of Edge Devices

Shubhra Deb Paul, *Member, IEEE*, Aritra Dasgupta, *Member, IEEE* and Swarup Bhunia, *Fellow, IEEE*

***Abstract*—Counterfeiting, overproduction, and cloning of integrated circuits (ICs) and associated hardware have emerged as major security concerns in the modern globalized microelectronics supply chain. One way to combat these issues effectively is to deploy hardware authentication techniques that utilize physical unclonable functions (PUFs). PUFs utilize intrinsic variations in hardware that occur during the manufacturing and fabrication process to generate device-specific fingerprints or immutable signatures that cannot be replicated by counterfeits and clones. However, unavoidable factors like environmental noise and harmonics can significantly deteriorate the quality of the PUF signature. Besides, conventional PUF solutions are generally not amenable to in-field authentication of hardware, which has emerged as a critical need for Internet of Things (IoT) edge devices to detect physical attacks on them. In this paper, we introduce frequency-domain PUF or FDPUF, a novel PUF that analyzes time-domain current waveforms in the frequency domain to create high-quality authentication signatures that are suitable for in-field authentication. FDPUF decomposes electrical signals into their spectral coefficients, filters out unnecessary low-energy components, reconstructs the waveforms, and generates high-quality digital fingerprints for device authentication purposes. Compared to existing authentication mechanisms, the higher quality of the signatures through frequency-domain analysis makes the proposed FDPUF more suitable for protecting the integrity of the edge computing hardware. We perform experimental measurements on FPGA and analyze FDPUF properties using the NIST test suite to demonstrate that the FDPUF provides better uniqueness and robustness than its time-domain counterpart while being attractive for in-field authentication.**

***Index Terms*—Hardware Authentication, PUF, FPGA, NIST, DCT, Wiener filter, Counterfeiting, Frequency-Domain.**

I. Introduction

Counterfeiting is an international criminal industry that spans the whole spectrum of all manufactured products. With the recent shift of the global semiconductor industry from a vertical business model to a horizontal model and a shorter time-to-market strategy, the fabless manufacturers share their design with untrusted offshore fabrication facilities or foundries. Additionally, the integration companies acquire Intellectual Properties (IPs) from untrusted vendors. For these reasons, counterfeit electronics have become an increasingly concerning security matter in the hardware industry. Other forms of hardware attacks include in-field alterations/tampering and hardware Trojans. The combination of these attacks can lead to product failures, cause a loss in revenue for businesses, and bring economic disaster that impacts national and public security. In this scenario, physical unclonable function (PUF) based authentication techniques can play a critical role in mitigating hardware counterfeiting and cloning.

Physical unclonable functions or PUFs are complex structures that exploit the manufacturing process variations-borne random fluctuations in device properties, *e.g.*, gate delay, threshold voltages, *etc.*, to generate device-specific unique fingerprints. These uncontrollable random variations are known as entropy sources of the PUF. In the existing literature, there are a plethora of physical parameters that have been utilized to design and implement various PUFs, such as time, frequency, voltage/current, logical states, delay, capacitance, electrical/magnetic field, and intensity [1].

The early concept of the frequency-based PUF was realized using ring oscillators (ROs) in the RO PUF [2]. In this concept, a pair of ring oscillators containing an odd number of inverters are put into race condition, and their outputs are fed into a comparator circuit. Based on the frequency/speed of each oscillator, the comparator outputs a binary '0' or '1'. The inherent delays in the lines or the logic gates are primarily uncorrelated. As a result, this feature was used to design the RO PUF. As RO PUF suffers from inter-dependence issues of the ring oscillators, to alleviate their mutual locking mechanism, a new structure named TERO PUF (Transient Effect Ring Oscillator) was proposed [3]. Instead of ROs, the TERO structure consists of an SR latch with two AND gates and an even number of inverters (two or more), known as the TERO loop. A single CTRL signal governs the S and R input of the loop. Instead of utilizing the oscillation frequencies, it takes advantage of the number of oscillations, eliminating the locking phenomenon.

Acoustical PUF (APUF) [4] is an example of a PUF that is built on the characterization of an electronic property. It utilizes the frequency spectrum of glass delay lines that transform the electrical signal into ultrasound; then, the data dimensionality is reduced with principal component analysis (PCA) to generate unique signatures. A few other PUF instances that employ the optical frequencies and structural imperfections of optical materials are FiberID [5], liquid crystal PUF [6], and quantum optical PUF [7]. The FiberID exploits the unique Rayleigh backscatter patterns at the molecular level within the optical fiber structure. These patterns are generated due to manufacturing process variations captured through optical frequency domain reflectometry (OFDR). On the other hand, Cholesteric Liquid Crystal (ChLC) shells reflect unique and colorful light patterns once illuminated. These random and unpredictable patterns are the frequency

S. D. Paul, A. Dasgupta, and S. Bhunia are with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, 32611 USA (e-mail: joyshubhra.eee@gmail.com, aritradasgupta@ufl.edu, swarup@ece.ufl.edu).

response of the reflected light, and these are generated due to structural variations, which the liquid crystal PUF exploits for object authentication [6]. Authors in [7] proposed that it takes advantage of the nanoscale deformities in 2D materials. These defects and spatial variations in the material bandgap are spawned during crystal growth and are characterized by photoluminescence measurements. Apart from utilizing variations in optical parameters, some alternative techniques utilize radio frequency (RF) to generate device-level identifiers or digital fingerprints. RF-DNA PUF uses radio-frequency scattering instead of optical refraction [8], RF-PUF [9] utilizes the inherent frequency offsets and I-Q imbalances within the data transmission channel.

One of the significant drawbacks of the analog electrical signal is the associated environmental noise. The presence of such unavoidable noise impairs the integrity of the waveform. Additionally, such noise belongs to higher harmonics of the fundamental frequencies. These harmonics also contain a tiny fraction of the overall signal energy, thus contaminating the signals. However, it is nearly impossible to analyze a signal in the time domain and remove such undesired components, which motivates us to develop this frequency-domain PUF.

In this paper, we introduce frequency-domain PUF, or FDPUF, a novel PUF methodology that analyzes the time-domain current waveforms, decomposes them into the frequency domain, removes unnecessary/low-energy signal components, performs noise filtering, then reconstructs the signal to generate device-specific biometric fingerprints/signatures for authentication. We re-use the current measurements that are collected in designing *CurIAs* [10]. *CurIAs* demonstrated superior performance as PUF in terms of uniqueness, robustness, and randomness. This study aims to improve robustness performance through frequency-domain analysis compared to its time-domain counterpart. We apply the DCT technique to compress and transform the time domain signal into spectral coefficients to achieve this. Then we set a threshold of signal energy level to filter out the components that do not contain any significant signal information. From the nature of DCT, most of these low-energy components belong to higher frequencies. We set these redundant coefficients to zero and employ the Wiener filter to remove signal noise. Hence, we perform an inverse DCT (IDCT) to reconstruct the denoised signal. Finally, we implement our signature generation technique (discussed in [10]) on the reconstructed waveforms, transform them into digital signatures, and compute the PUF metrics such as uniqueness, robustness, uniformity, and randomness. We explore that the FDPUF demonstrates better uniqueness and robustness compared to *CurIAs*. To the best of our knowledge, this is the only existing PUF design based on the frequency domain analysis of the current signals. Fig. 1 depicts how FDPUF can be used for authenticating edge devices in the field.

The remainder of the paper is organized as follows. We provide background on PUF technology and a brief survey of existing PUF research and practice in Section II. We present the FDPUF design methodology and describe the signature extraction steps in Section III. In Section IV, we present the experimental measurement setup, supply current data collection, and analysis of FDPUF signatures. We conclude and present potential future work in Section V.

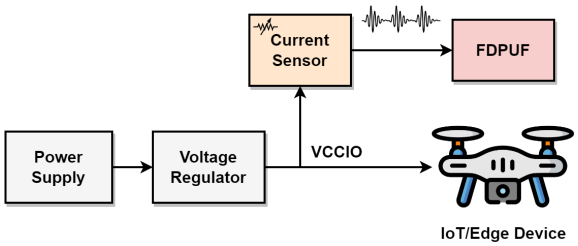


Fig. 1: FDPUF can be used to authenticate edge devices in-field through sensing and analysis of supply current in response to specific workloads.

II. Background

A. Device Life-cycle and Hardware Supply Chain

The modern electronic supply chain is long and complex as the entities/parties involved in this process can be spread across the globe. Fig. 2 depicts a simplified view of the different stages of a device's life cycle and its involvement in the modern IC supply chain. The production starts with the process of the device specifications. After the specs are finalized, the design process kicks off. The overall design procedure consists of three significant steps, starting from RTL design to the generation of GDSII fabrication files. In the first step, the RTL designers perform behavioral circuit description simulations. Once the circuits pass the RTL simulations, the IC designers transform the hardware description circuits into gate-level circuits. Next, the physical design and layout process begins. At the end of the layout stage, the digital GDSII files are generated and passed down to the foundries for fabrication.

The foundries fabricate the ICs, perform functionality tests, assemble them, and distribute them through the marketing partners. After the system integration takes place, the devices are deployed in-field. After a certain deployment period, a couple of things can happen to the devices. Firstly, they might reach their end-of-life and are no longer usable. As a result, they are discarded or recycled for usable components. On the other hand, they might also need periodic service for maintenance or repair. So they are transferred to the authorized service centers. If the service centers can successfully repair the devices, they get redeployed for further usage.

Threat Model: For the proposed authentication protocol, we consider the following threats associated with the IC life cycle:

1) Supply Chain Threats: Hardware supply chain management is a growing issue due to the increasing vulnerabilities and threats associated with different levels/stages. Any untrusted party within the supply chain can potentially inject vulnerabilities/malicious components in both software/hardware levels, manipulate and exfiltrate data/secret information with a mischievous intent [13]. The supply chain has become even more susceptible to attacks in recent times due to the high cost of foundry/fabrication facility maintenance, from design to packaging of hardware, which in turn requires third-party

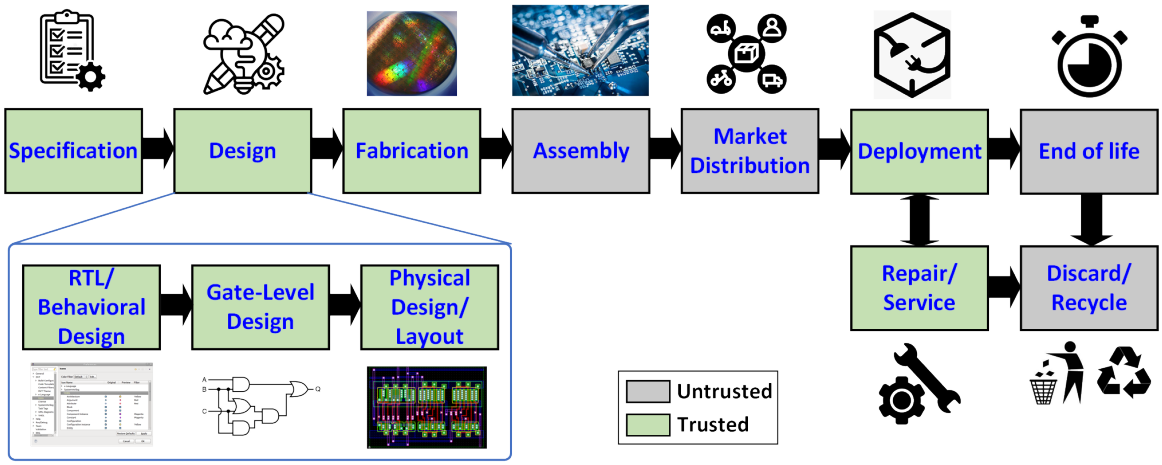


Fig. 2: The life-cycle of an integrated circuit (IC)/device and various stages of a modern IC supply chain [11], [12].

outsourcing vendors for specific steps within the fabrication process, as illustrated in Fig. 2. The outsourcing required for these specific steps within the fabrication process creates a new realm of security concerns for IC designers due to the lack of trustworthiness in the various entities involved in IC/SoC (System on a Chip) design and fabrication. Once the design is shipped to the foundry for fabrication, it is entirely out of the hands of the designers. It elevates the distrust between the parties/individuals involved from the design to fabrication.

2) Post-Deployment Threats (for IoT/Edge Devices): Once the ICs have been integrated into consumer devices (e.g., drones, home-security appliances, smart home devices, etc.) in IoT systems and deployed in the field, they are vulnerable to diverse physical attacks. Replacement of a hardware component, e.g., an IC by a compromised one, altering device functionality through addition/removal of components, rewiring the components, etc., constitutes powerful physical attacks on edge devices. These attacks have emerged as significant attack vectors for edge computing devices used in wide-ranging applications, e.g., environmental sensing, structural monitoring, and military/defense surveillance, which expose the hardware to an adversary and make it vulnerable to physical attacks. We incorporate this threat into our threat model definition.

Trust Model: In our authentication protocol trust model, we assume that:

- the IC designer is ***trusted***,
- the IC fabricator/manufacturer is ***untrusted***,
- the system integrator is ***trusted***,
- the device is deployed in ***untrusted*** setting, and
- the authenticator/verifier is ***trusted***.

B. Related Works

Some published works perform electromagnetic (EM) and side-channel analysis in the frequency domain to prevent potential attacks on hardware. For example, the authors in [14] proposed an analysis scheme to compute the oscillation frequency and location of small RO PUF blocks via EM emission measurements. They successfully launched an attack on FPGA-based RO PUF and extracted the primary signal paths, including the complete PUF model. The authors in [15] evaluated the EM analysis (EMA) threats on RO PUFs through EM trace measurements to sniff out the PUF responses from the geometric/current-path leaks. Similarly, a side-channel-based analysis and physical security of TERO PUF were presented in [16]. The authors launched attacks on TERO PUF by measuring the time domain signals and analyzing them via short-time Fourier Transform (STFT) to reveal the frequency domain information. This attack was able to extract a significant chunk of the PUF bits with reasonable accuracy.

On the other hand, frequency domain analysis has been widely used for fault detection in analog circuits. The authors in [17], [18] employed Discrete Wavelet Transformation (DWT) techniques on dynamic supply current waveforms for both fault detection/diagnosis and localization. Wavelet transformation is more advantageous than FFT because the former contains both time and frequency information in the decomposed data. In these approaches, the authors acquired the current signature from the golden or fault-free device, performed simulation and measurements of test circuits that may or may not contain faults, and finally compared the computed wavelet coefficients from both cases.

For fault detection, several researchers have adopted another frequency domain analysis technique, Discrete Cosine Transform (DCT). Reference [19] demonstrated a DCT-based approach to detect faults in physical materials. DCT has also been used in fault detection in electric vehicles' batteries [20] and in electrical/mechanical fault detection in induction motors [21]. These techniques analyzed the voltage, current, and vibration waveforms for fault characterization and detection. Some authors even applied a DCT-based approach in developing fault-tolerant [22] and process variation tolerant [23] architectures for Peak Signal-to-Noise Ratio (PSNR) improvement and yield enhancement.

Our comprehensive literature review reveals that the articles incorporate the random variations in either optical, or radio frequency (RF), or electromagnetic (EM) emission at the physical level to design various PUF structures. Some other aspects of frequency domain-based analysis were used in a circuit's fault detection using power/voltage/current traces.

However, to the best of our knowledge, none of the current works focus on analyzing electrical signals in the frequency domain and extracting the inherent randomness/irregularities as entropy sources.

C. Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) was introduced by Ahmed *et al.* in 1973 for pattern recognition and Wiener filtering purposes [24]. Today, DCT is widely used in speech, image, and video compression due to its energy compaction characteristics. A fairly accurate reconstruction is possible using a handful of DCT coefficients because the neighboring coefficients are highly correlated [25]. As a result, DCT is extremely successful in the reduction of data or truncation of feature space [26].

The DCT of a signal/sequence $Y(n), n = 0, 1, ..., (N-1)$ is expressed as:

$$\begin{aligned} C_y(0) &= \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} Y(n) \\ C_y(k) &= \frac{2}{N} \sum_{n=0}^{N-1} Y(n) \cos \frac{k(2n+1)\pi}{2N}, \end{aligned} \tag{1}$$

here, $C_y(k)$ is the k^{th} DCT coefficient and $k = 1, 2, 3, ..., (N-1)$. Eqn. (1) can be generalized as:

$$C_y(k) = \alpha(k) \sum_{n=0}^{N-1} Y(n) \cos \frac{k(2n+1)\pi}{2N}, \tag{2}$$

where, $\alpha(k)$ is the scaling factor defined as:

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}}, & k = 0 \\ \sqrt{\frac{2}{N}}, & k = 1, 2, 3, ...(N-1). \end{cases} \tag{3}$$

The basis vectors of this transform, $[\sqrt{\frac{1}{2}}, \cos \frac{k(2n+1)\pi}{2N}]$ belong to one of the Chebyshev polynomial classes. The k^{th} Chebyshev polynomial can be expressed as, $\hat{T}_k(\gamma_q), q = 1, 2, ..., N$ [27]. The $\hat{T}_k(q)$ is equivalent to:

$$\begin{aligned} T_0(n) &= \sqrt{\frac{1}{2}} \\ T_k(n) &= \cos \frac{k(2n+1)\pi}{2N}, \end{aligned} \tag{4}$$

here, $k = 1, 2, ..., (N-1)$ and $n = 0, 1, ..., (N-1)$. The inverse discrete cosign transformation (IDCT) is defined as:

$$Y(n) = \sqrt{\frac{1}{2}} C_y(0) + \sum_{k=1}^{N-1} C_y(k) \cos \frac{k(2n+1)\pi}{2N} \tag{5}$$

Eqn. (5) can be generalized as:

$$Y(n) = \sum_{k=0}^{N-1} \alpha(k) C_y(k) \cos \frac{k(2n+1)\pi}{2N} \tag{6}$$

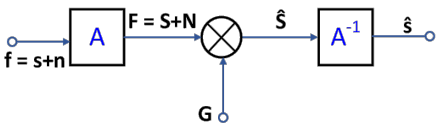


Fig. 3: A general Wiener filtering structure [29].

The orthogonality property can be applied to achieve [27], [24]:

$$\sum_{n=0}^{N-1} T_k(n) T_l(n) = \begin{cases} N/2, & k = l = 0 \\ N/2, & k = l \neq 0 \\ 0, & k \neq l. \end{cases} \tag{7}$$

If DCT possessed orthonormality property, it could be considered as a unitary transform [28], which implies that:

$$\sum_{n=0}^{N-1} [Y(n)]^2 = \sum_{k=0}^{N-1} [C_y(k)]^2. \tag{8}$$

From Eqn. (1) and (5), it is clear that DCT synthesis is both periodic and evenly symmetric due to the *cosine* operations [28]. Compared to the Discrete Fourier Transform (DFT), DCT is computationally more efficient as the latter uses only real numbered coefficients and does not require complex additions or multiplications. As a result, 1-D DCT (DCT Type-2) is a great choice for analyzing finite-length current waveforms for PUF applications because it reduces the total system overhead for implementation.

D. Energy Compaction with DCT

It is an inherent property of the DCT-2 that the signal energy is mainly concentrated in the initial coefficients. Following Parseval's theorem,

$$\sum_{n=0}^{N-1} |Y(n)|^2 = \frac{1}{N} \sum_{k=0}^{N-1} \alpha(k) |C_y(k)|^2. \tag{9}$$

As DCT energy is concentrated within lower indices, the signal tends to have most of its energy fixed in the lower frequencies. So, if the remainder of the coefficients is set to zero, it will remove the higher frequency components, and it might not have any severe impact on the signal [28].

E. Wiener Filtering

Wiener filtering is a well-known technique in the field of signal and image processing, where it restores the signals that are contaminated by additive random noise [29], [30]. In a practical scenario, most of this noise is unknown and needs to be extracted and estimated from data segments.

Fig. 3 depicts a generalized Wiener filter structure. Here, a N-element column vector, f that contains a signal, s and noise component, n. We assume that the signal and noise are mutually uncorrelated. For a $N \times N$ unitary transformation matrix, A being applied to f, we can write:

$$F = Af = As + An \equiv S + N. \tag{10}$$

A few examples of the unitary transformations would be Fourier, Hadamard, Karhunen-Loève, DCT, *etc.*. Multiplying F with a $N \times N$ filter matrix, G, we get the filtered matrix, $\hat{S}$. Finally, the inverse unitary transformation takes place to retrieve/reconstruct the denoised estimated signal (Eqn. (11)). The filter parameter, G, is chosen carefully to minimize the Mean Square Error (MSE).

$$\hat{s} = A^{-1}GF = A^{-1}GAf. \tag{11}$$

F. MSE and PSNR

The mean square error (MSE) is defined as:

$$MSE = \frac{1}{N}\sum_{n=0}^{N-1}[Y(n) - \hat{Y}(n)]^2, \tag{12}$$

where $\hat{Y}(n)$ is the estimated version of the N-bit long original signal/vector, $Y(n)$.

The Peak Signal-to-Noise Ratio (PSNR) is expressed as [31]:

$$PSNR = 10\log_{10}\left[\frac{(PeakValue)^2}{MSE}\right]. \tag{13}$$

For proper signal quality restoration, the PSNR value of the reconstructed signal should be >30 dB [23].

III. FDPUF Design Methodology

A. System Architecture

The design methodology of the FDPUF is similar to supply current analysis in the time domain, *CurIAs* [10]. We employ the dynamic current variations due to temporal switching activities within sequential circuit structures, *e.g.*, Linear/Non-Linear Feedback Shift Register (LFSR/NLFSR), as our entropy source. They can be implemented into the hardware components of an edge device (e.g., custom system-on-chip, FPGA, microcontroller) either by adding separate sequential structures or re-purposing existing circuit blocks (e.g., counter, shift register, pipeline register, boundary scan, etc.) to be configured as LFSR/NLFSR during authentication, to minimize hardware overhead.

Dynamic current waveforms are measured from an edge hardware, as in *CurIAs*. The primary novelty of this work lies in performing data analysis in the frequency domain instead of the time domain to create robust device-specific authentication signatures, which can be verified by an external verifier during the authentication process.

Fig. 4 illustrates the overall architecture of FDPUF. Firstly, we assume that the collected time-domain current measurement data or waveforms are noisy. We apply DCT to the signal. After computing the DCT coefficients, we apply energy thresholds to them as discussed in Section II-C in detail. The energy thresholding allows us to detect the redundant high-frequency coefficients that do not significantly contribute to signal formation. We set the values of those redundant coefficients to zero. In the next step, we apply Wiener filtering for noise reduction. Hence, we apply inverse DCT (IDCT) to compute the estimated signal/waveform on the denoised signal. We apply the same signature generation technique to transform IC-specific digital signatures.

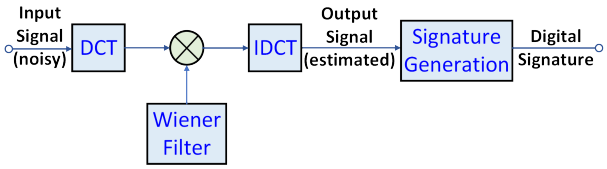


Fig. 4: Architectural block diagram for the proposed FDPUF based edge device authentication approach.

B. Frequency Domain Analysis Scheme using DCT

We start our frequency domain analysis by applying DCT to the current waveforms in MATLAB[1]. We incorporate MATLAB's built-in function `dct` for this purpose. Every current signal contains 100,000 datapoints, and as a result, every DCT operation will produce 100,000 DCT coefficients.

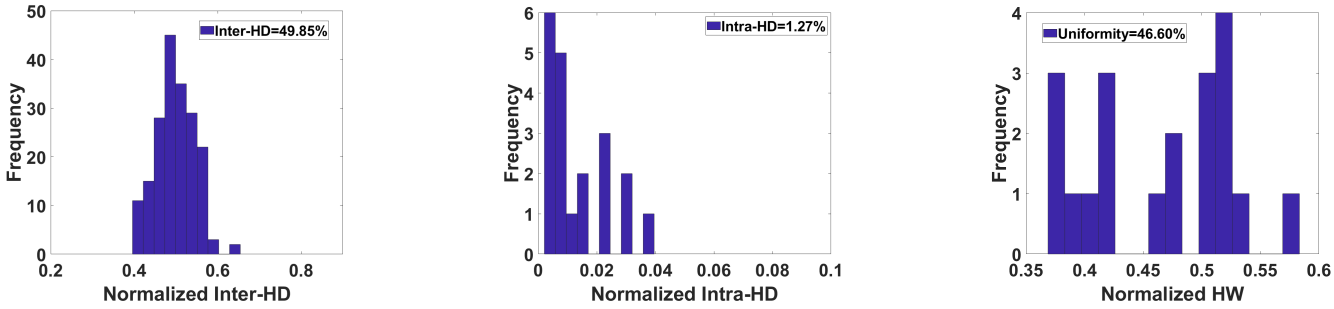
1) Thresholding: After we collect the coefficients, we apply the thresholding technique. In our method, we set the energy threshold as 99.9%. Only a handful of the coefficients will carry over 99.9% signal energy, and those that satisfy these criteria are selected. We set the rest of the coefficients to zero, as they can be considered mainly to belong to high frequencies and unwanted components adding to the signal noise floor.

2) Applying Wiener Filter: Once we compute the modified coefficient vector, we apply Wiener filtering using MATLAB's built-in function, `wiener2`. The `wiener2` function takes two main arguments, the input signal and the filter size, $[m.n]$. The filter size input argument creates a neighbor size of $m \times n$ to estimate noise through local image mean and standard deviation. We are applying 1-D DCT to our current waveforms, and we set the filter size as [2,2].

3) Signal Reconstruction: To reconstruct the signal, we employ the built-in inverse DCT function of MATLAB, `idct` on the filtered signal. We measure signal quality using MSE, PSNR, and SNR. Before generating the digital signature from the reconstructed signal, we ensure that they have calculated PSNR $>$ 30 dB.

4) Signature Generation: Similar to *CurIAs*, we apply 64 different challenges to each of the 20 ICs and collect challenge-specific currents. After applying DCT, thresholding and coefficients selection, Wiener filtering, and IDCT, we acquire the estimated waveform that is mostly free from high-frequency and unwanted components that impact signal integrity. Each of the current waveforms contains 100,000 datapoints, and we take an average over all the data points for each measurement. Thus, we get 64 average current values for every single IC. Then, for every IC, we divide the 64 current values into four groups, with each group containing 16 values. This selection is based on the mean and standard deviations among them. By applying mutual comparison between each of the current values within these four groups, we assign a binary bit. Thus, for each group, we get ${}^{16}C_2 = 120$ binary values, and for every IC, we get a total 120×4 = 480-bit signature.

[1]https://www.mathworks.com/products/matlab.html



(a) (b) (c)

Fig. 5: Uniqueness, robustness, and uniformity results for 20 ICs at nominal operating conditions ($T = 25$ °C, $V_{Supply} = 3\ V$). Here, the X-axes of the plots represent the average inter and intra-Hamming distances (HD), and Hamming weights (HW), measured using Eqn. (14), (15), and (16); Y-axes denote the corresponding frequencies; for 480-bit signatures over 20 ICs: (a) Inter-HD results; (b) Intra-HD results; and (c) Uniformity.

IV. Experimental Results and Security Analysis

In this section, we present FDPUF evaluation results using experiments performed on 20 Intel MAX10 FPGA chips on 20 custom Printed Circuit Boards (PCBs), each of which represents an independent edge device. We measure supply current values from each PCB corresponding to several input challenges. After compression, filtering, and reconstructing the current signals, we apply the proposed signature generation technique and generate 480-bit signatures for each PCB. For the data collection process, we define the nominal conditions as $V_{Supply} = 3.0V$, and environmental temperature as 25°C.

A. Uniqueness of Signatures

Uniqueness signifies the quality of a PUF in generating distinct responses over multiple instances of the same entity for the same challenge/input. For example, if a group of ten PUFs is designed and fabricated within ten different chips and a single challenge is applied to them, each PUF should generate different responses. Inter-Hamming distance (Inter-HD) is the parameter commonly used to quantify the uniqueness of a PUF. As the probability of the maximum difference between two binary digits, '0' and '1', is 50%, in an ideal scenario, the average inter-HD of a group of PUFs should be 50%. The average inter-HD is defined as as [32]:

$$\text{HD}_{Inter,Avg.} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\%, \tag{14}$$

where R_i and R_j are n-bit response from i^{th} and j^{th} instance of the PUF ($i \neq j$) for challenge C, and k is the total number of PUF instances under evaluation.

In our proposed method, we conduct practical experiments on 20 Intel MAX 10 FPGAs on 20 different HaHa boards and measure supply current values corresponding to the input challenges. After compression, filtering, and reconstructing the current signals, we apply signature generation techniques discussed in Section III-B4 and generate 480-bit signatures for each IC. For the data collection process, we define the nominal conditions as $V_{Supply} = 3.0$ V, and environmental temperature as 25 °C. Fig. 5(a) illustrates the computed uniqueness of this PUF in terms of the inter-HD histogram of the signatures at nominal conditions. The plot demonstrates that the average intra-HD is 49.85%, close to the ideal value of 50%. The X-axis of this plot represents the normalized Hamming distances between signatures, *i.e.*, and the percentage of bit differences between PUF responses. The distribution is spread from 0.4 to 0.7, indicating a tight distribution with a substantial uniqueness property.

B. Robustness of Signatures

Robustness, also known as reproducibility, is the metric to determine whether the PUF can accurately regenerate the same responses for the same challenge sets, irrespective of the environmental conditions. As the performance of any electronic device depends on environmental stress factors such as supply voltage, temperature, and time, the robustness gauges the capacity of the PUF to produce the same responses under the stressed circumstances compared to the nominal condition. PUF randomness is measured by intra-Hamming distance (intra-HD) and expressed by Eqn. (15). Ideally, a PUF should be able to regenerate its response independent of the stress factors exactly, so the average intra-HD should be 0%.

$$\text{HD}_{Intra,Avg.} = \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_{i,1}, R_{i,2})}{n} \times 100\%, \tag{15}$$

here $R_{i,1}$ and $R_{i,2}$ are the n-bit responses from the i^{th} instance for challenge C for 1st and 2nd measurement, respectively. The intra-HD is computed by averaging the total differences in responses over k different PUFs.

We assess the robustness of our proposed PUF in three different scenarios. First, we perform two sets of measurements under the nominal conditions and compare the results. Then, we change the supply voltage of the HaHa board and repeat the experiments under the nominal temperature (25 °C). Hence, we perform further measurements by altering the surrounding temperature; however, this time, we operate the board at the

nominal supply voltage (3.0 V). We discuss the outcomes of the experiments in the following sections.

Fig. 5(b) elucidates the intra-HD of our proposed PUF in nominal conditions. We perform two sets of experiments under nominal operating conditions for 20 ICs, generate 480-bit PUF responses/each, and compare the results to determine their reproducibility. From the plot, we observe that the average intra-HD is calculated as 1.27%, which is close to the ideal value of 0%. We can conclude that the PUF can accurately replicate the response bits over multiple measurements. We note another important aspect once we closely compare Fig. 5(a) and 5(b) as both of them have a similar X-axis (normalized HD). We discover that the spread of these two distributions does not overlap. It is a vital feature while examining PUF quality, as any overlap between these two distributions will cause ambiguity between the uniqueness and robustness of a PUF. As there is no overlap between these two distributions, we can safely assume that the PUF can not only generate unique device-specific signatures, but they are also recreating the responses with high probability.

1) Supply Voltage Variations: Our experimental platform, the HaHa board, can operate within the supply voltage range 2.1 V – 3.3 V. We take advantage of this operating range to extend our experiments across four different voltage levels: 2.1, 2.5. 3.0 (nominal) and 3.3 V by keeping the nominal/ambient temperature. We apply the same challenge vectors to the PUF and measure the supply currents at specified voltages. Fig. 6 demonstrates the inter-HD and intra-HD results for these experiments. We discover that for 2.1, 2.5, 3.0, and 3.3 V, the intra-HD values calculated are 3.83%, 3.2%, 1.27%, and 2.29%, respectively. It means that there are minimal bit-errors for this large supply voltage variation, which signifies our proposed approach's strong robustness property. On the other hand, the computed average inter-HD values are 50.3%, 49.33%, 49.85%, and 49.75% for 2.1, 2.5, 3.0, and 3.3 V, respectively. All these values are very close to the ideal 50%, which manifests that the PUF can generate unique signatures under stressed conditions.

2) Operating Temperature Variations: In our next approach to quantifying the robustness of the proposed PUF in different operating conditions, we vary the surrounding temperature. We use an ATS-505 Thermostream as the external variable thermal source to achieve and apply controlled temperature directly on the ICs for conducting temperature variation experiments for four different temperatures: 10 °, 25 °, 55 °, and 85 °C. We maintain the supply voltage constant at 3.0 V during temperature alteration experiments. Fig. 7 exhibits the complete results of temperature variation experiments in terms of inter-HD and intra-HD values. The calculated intra-HD values for 10 °, 25 °, 55 °, and 85 °C are 3.9%, 1.27%, 4.47%, and 6.42%, respectively. The plots signify that the operating temperature has a significant impact on the robustness of a PUF, and the further the operating temperature is from the nominal condition, the performance gradually degrades. Especially at 85 °C, there is a comparatively higher percentage of bit-errors than the nominal. However, we can explain this scenario from the manufacturing specifications of Intel MAX 10 FPGAs. The HaHa board is designed based on the commercial version of MAX 10, which can withstand a maximum of 85 °C. At this extreme temperature (according to the device specifications), the degradation of overall performance is expected, and we experience a high value of average intra-HD. On the contrary, the average inter-HD values are recognized as 50.24%, 49.85%, 49.99%, and 49.58% at 10 °, 25 °, 55 °, and 85 °C, respectively. It signifies that even if the operating temperature is altered from the nominal one, the PUF holds a strong uniqueness property and can generate unique and uncorrelated signatures with a high probability.

C. Uniformity of Signatures

Another vital metric for PUF evaluation is the uniformity of its response bits. The uniformity of a PUF is an estimation of how proportionately the '0's and '1's are distributed within the response vectors. Ideally, a PUF must have a uniformity of 50%, which means that the PUF signature must possess an equal number of '0's and '1's. Uniformity, as expressed in terms of percentage Hamming Weight (HW), is defined in Eqn. (16), where $R_{i,k}$ is the k^{th} response bit from the i^{th} PUF instance consisting of n-bit signature length [32].

$$\text{Uniformity}_i = \frac{1}{n}\sum_{k=1}^{n} R_{i,k} \times 100\%, \tag{16}$$

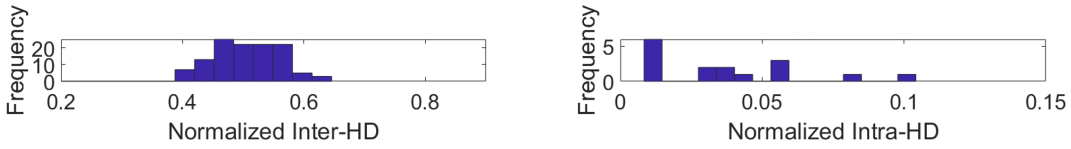
where $R_{i,k}$ is the k^{th} response bit from the i^{th} PUF instance and each signature is n-bit long.

Fig. 5(c) embodies the uniformity results of our proposed PUF for 20 ICs, each of them having a 480-bit signature. The X-axis on this plot represents the normalized Hamming weight (HW), and the Y-axis shows their frequencies. Using Eqn. (16), the calculated average uniformity is 46.6% ($\sigma_{HW-norm}$ = 0.064), which is relatively close to the ideal value. It means that out of 480 bits in a PUF signature, there are 224 '1's and 256 '0's. Thus, our proposed technique delivers a strong uniformity feature.

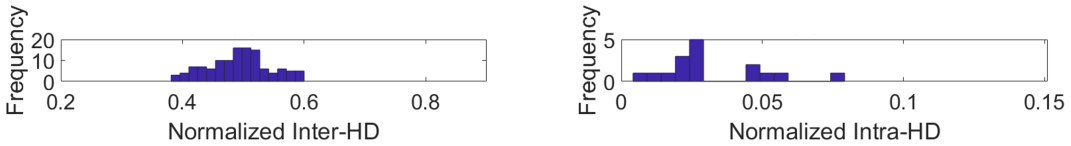
D. Randomness of Signatures

Randomness is one of the most critical PUF quality metrics that need to be assessed due to their application in cryptography and security applications. Every PUF exploits the process variations as the source of entropy, and these variations are unpredictable. For a PUF to be considered a gatekeeper of the authentication procedure, there should be uniformity between the '0's and '1's within the generated responses; specific statistical properties must also be maintained between them. As a result, proper verification of the PUF responses is required to ensure random bit sequence production. The National Institute of Standards and Technology (NIST) provides the test suite SP 800-22 [33] for this purpose. This test suite is a statistical package that contains a series of statistical tests that assess the randomness and unpredictability of any random or pseudo-random binary generator.

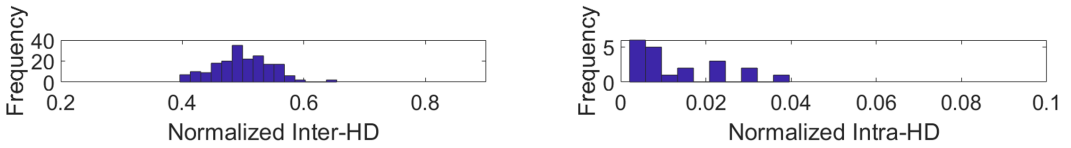
The statistical tests in this test suite are designed to test a particular null hypothesis (H_0) that assumes the sequence is random. The associated alternative hypothesis (H_a) assumes the opposite, which means the sequence is not random. The



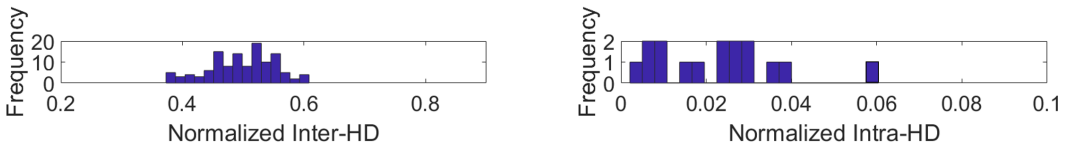
(a) **At 2.1 V; Avg. Inter-HD = 50.30%, Avg. Intra-HD = 3.83%**



(b) **At 2.5 V; Avg. Inter-HD = 49.33%, Avg. Intra-HD = 3.20%**

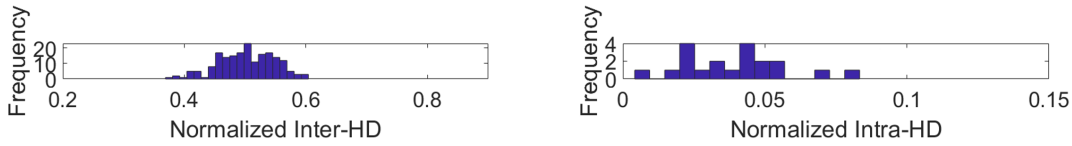


(c) **At 3.0 V; Avg. Inter-HD = 49.85%, Avg. Intra-HD = 1.27%**

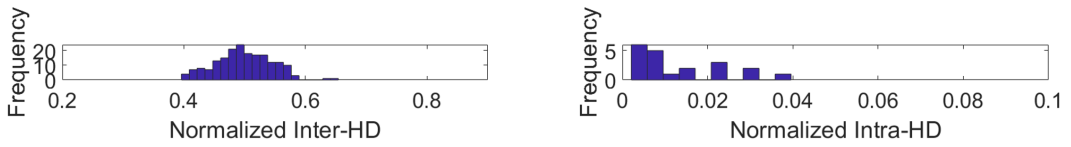


(d) **At 3.3 V; Avg. Inter-HD = 49.75%, Avg. Intra-HD = 2.29%**

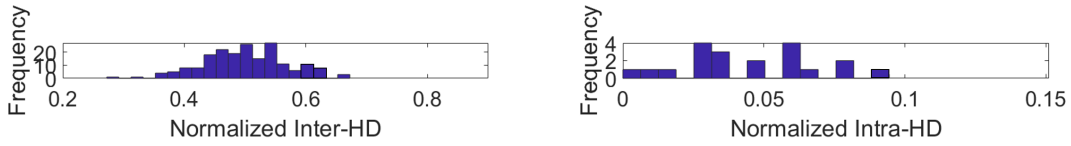
Fig. 6: Robustness results (Inter-HD and Intra-HD) for V_{Supply} variations: (a) 2.1 V; (b) 2.5 V; (c) 3.0 V (nominal); and (d) 3.3 V. The experiments are performed at 25 °C temperature, and 480-bit signatures are generated for 20 different ICs. Here, the X-axes of these histograms represent the average inter and intra-Hamming distances (HD) measured using Eqn. (14) and (15) and Y-axes denote corresponding frequencies.



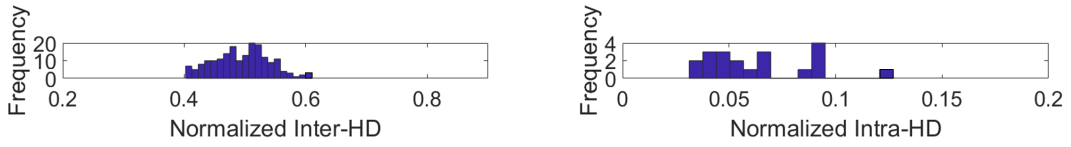
(a) **At 10 °C; Avg. Inter-HD = 50.24%, Avg. Intra-HD = 3.90%**



(b) **At 25 °C; Avg. Inter-HD = 49.85%, Avg. Intra-HD = 1.27%**



(c) **At 55 °C; Avg. Inter-HD = 49.99%, Avg. Intra-HD = 4.47%**



(d) **At 85 °C; Avg. Inter-HD = 49.58%, Avg. Intra-HD = 6.42%**

Fig. 7: Robustness results (Inter-HD and Intra-HD) with Temperature variations: (a) 10 °C; (b) 25 °C (nominal); (c) 55 °C; and (d) 85 °C. The experiments are performed at 3.0 V, and 480-bit signatures are generated for 20 different ICs.

hypothesis is tested against a predefined significance level, α. For our experiments, we set $\alpha = 0.001$. For each test, the outcome is defined as the *P-value* and compared against α. If the computed P-value $> \alpha$, then we conclude that the sequence is random with the confidence level of 99.9% ((1-α)$\times$100%). On the other hand, if *P-value* $< \alpha$, then the sequence is considered non-random with the same confidence level. In addition to the *P-value*, a minimum number of sequences needs to pass the tests individually for a series of generated sequences to be considered as passing the comprehensive test.

TABLE I: NIST Test Suite results for the uniformity of *P-value*s and the proportion of passing sequence at a significance level, $\alpha = 0.001$. The tests are performed for 20 PUF sequences, 480-bit long/each.

Statistical Test	***P-value***	**Pass Proportion**	**Pass?**
Frequency	0.437274	20/20	Y
Block Frequency	0.739918	20/20	Y
Cumulative Sums (Forward)	0.739918	20/20	Y
Cumulative Sums (Backward)	0.437274	20/20	Y
Runs	0.350485	20/20	Y
Longest Run	0.534146	20/20	Y
Approximate Entropy	0.834308	20/20	Y
Serial (Forward)	0.017912	19/20	Y
Serial (Backward)	0.090936	20/20	Y
Linear Complexity	0.004301	20/20	Y
FFT (960-bit, 10 sequences)	0.534146	10/10	Y
Non-Overlapping Template (960-bit, 10 sequences)	0.213309	9/10	Y

We assess the randomness of our 20 PUF sequences, where each sequence is 480-bit long. The *P-value*s corresponding to the tests must be > 0.001 for the tests to pass. At least 19 out of the 20 sequences need to pass the test according to the test standard. Table I depicts the results of the NIST randomness test suite, where we conduct 10 of the tests within the suite. We found that eight out of the ten tests pass for sequences that are 480-bit long. The remaining tests (FFT/Spectral and non-overlapping template) require approximately 1000-bit long sequences. As a result, we concatenate a pair of sequences, thus creating a unique signature of 960-bit, then run the test. With this update, the tests run successfully, and the sequences pass. From Table I, we note that in these two tests, the number of passing sequences is compared against 10, as the number of sequences is halved in this scenario. By incorporating proper bit selection techniques, the randomness performance of the PUF can be strengthened even further [34].

E. Varying the Signal Energy Threshold

One final aspect we study of the proposed frequency-domain PUF is changing the input signal energy threshold while calculating the DCT coefficients with MATLAB. In Section III, we discuss how we calculate the number of DCT coefficients that represent a very high percentage of the energy, and we set zero to the rest of the coefficients. We only consider the coefficients that contain more than 99.9% of the signal energy in our best-case scenario. We analyze the waveforms by lowering the signal energy threshold as low as 70%, then 80%, and 90%, and ensure that the signal can be reconstructed after filtering with minimal errors. We found that the compressed signal can not be adequately reconstructed by further lowering the threshold. We also note that gradually increasing the signal energy threshold also increases the number of DCT coefficients, and so does the accuracy of the reconstructed signals as the MSEs drop as we boost up the signal energy threshold. Fig. 8 illustrates the comparison between the original signal and the compressed, filtered, and reconstructed signal. Increasing the signal threshold of the DCT coefficient calculation improves the signal reconstruction.

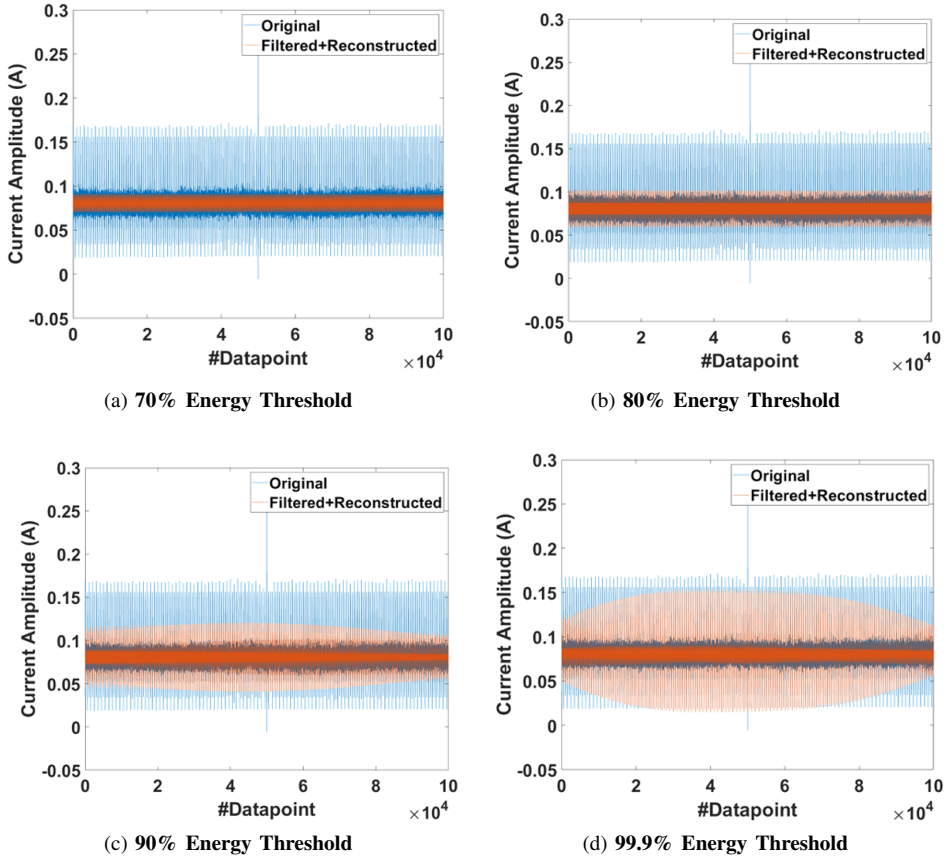
TABLE II: Impact of signal energy threshold variations.

	Signal energy threshold			
	70%	**80%**	**90%**	**99.9%**
Required coefficients	223	396	850	6567
MSE	2.99×10^{-4}	2.75×10^{-4}	2.43×10^{-4}	1.60×10^{-4}
PSNR (dB)	35.3	35.65	36.2	38.0
SNR (dB)	17.25	17.61	18.14	19.96
Inter-HD (%)	48.99	49.83	50.35	49.85
Intra-HD (%)	1.67	1.63	1.49	1.27

Table II summarizes the results by varying signal energy threshold. We compute the number of coefficients required to represent the defined energy level. Typically, the higher threshold should increase the number of required DCT coefficients to compress the signal. The table also confirms that we need 223, 396, 850, and 6567 coefficients out of 100,000 datapoints to compress the signal for 70%, 80%, 90%, and 99.9% energy thresholds, respectively. The next row of the table also substantiates that increasing the signal threshold decreases the MSE, *i.e.*, the higher threshold corresponds to more accurate signal reproduction. In addition to MSE, we also compute the uniqueness and robustness of the reconstructed signals over the various levels of the signal threshold. Table II and Fig. 9 summarize these results. We discover that increasing the signal threshold improves the robustness of the proposed PUF as we compute the average intra-HDs as 1.67%, 1.63%, 1.49%, and 1.27% for 70%, 80%, 90%, and 99.9% energy threshold, respectively. It denotes that increasing the signal threshold improves the reconstruction and accuracy, enhancing the signature reproduction. On the other hand, the average inter-HDs are 48.99%, 49.83%, 50.35%, and 49.85% for different thresholds, indicating a strong uniqueness.

F. Comparison with existing PUF structures

Table III provides a broader comparison between the proposed frequency domain PUF with other existing state-of-the-art methods, including its time domain counterpart, *CurIAs* [10]. Fig. 10 depicts the overall comparisons between the performance of FDPUF and *CurIAs* over identical supply voltage and temperature variations. We observe that the frequency domain demonstrates slightly better performance in terms of uniqueness and robustness compared to *CurIAs*, but the latter exhibits marginally better uniformity.



(a) **70% Energy Threshold** (b) **80% Energy Threshold**

(c) **90% Energy Threshold** (d) **99.9% Energy Threshold**

Fig. 8: Comparison of original and reconstructed current waveforms at various energy thresholds: (a) 70%; (b) 80%; (c) 90%; and (d) 99.9%. The original waveform is first compressed using DCT, then filtered using a Wiener filter, and then reconstructed using inverse DCT. The X-axis of the plot represents the number of datapoints, and the Y-axis denotes the current waveform amplitude (A) for each of the 100,000 datapoints.

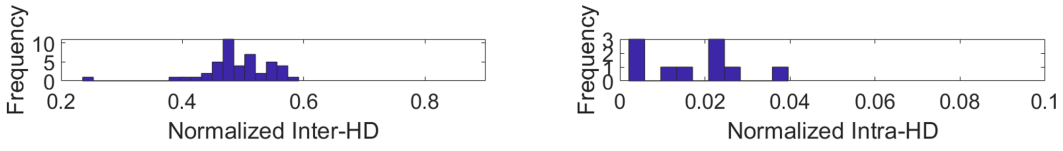
TABLE III: Comparison of FDPUF with existing works on PUF structures.

	Leakage PUF [35]	**SRAM PUF** [36]	**PiRA PUF** [37]	**Analog PUF** [38]	**CMA PUF** [39]	**MMPUF** [40]	**MeLPUF** [41]	**CurlAs** [10]	**FDPUF** *
Device Technology	IBM 90nm	N/A	N/A	65nm CMOS	AMS 350nm	TSMC 28nm	TSMC 55nm	TSMC 55nm	TSMC 55nm
Platform	Simulation	SRAM	PIC16	ASIC	ASIC	FPGA	FPGA	FPGA	FPGA
Hardware Implementation	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Uniqueness (Inter-die HD)	N/A	43.65%	50.7%	49.59%	51.48%	40.60%	50.05%	49.3%	49.85%
Uniformity	N/A	N/A	N/A	N/A	N/A	N/A	N/A	49.63%	46.65%
Bit-Error (Optimum)	∼3%	4.61%	6.8%	5.3%	0.16%	3.35%	2.57%	1.32%	1.27%
Bit-Error (Worst)	∼18%	N/A	N/A	8.8%	∼17%	N/A	N/A	7.5%	6.42%
Randomness (NIST test)	N/A	Yes	N/A	Yes	Yes	N/A	Yes	Yes	Yes
V_{Supply} Range	1.0 to 1.4 V	5 V	5.5 V	0.9 to 1.2 V	1.0 to 1.5 V	0.9 to 1.1 V	2.0 to 3.3 V	2.1 to 3.5 V	2.1 to 3.5 V
Temperature Range	0 to 75 °C	25 °C	25 °C	0 to 50 °C	-45 to 90 °C	0 to 70 °C	25 °C	10 to 85 °C	10 to 85 °C
Signature Length	100-bit	16-bit	80-bit	2048-bit	5000-bit	128-bit	1024-bit	1200-bit	480-bit
Hardware Overheads	Low to Moderate	Moderate	Low	Low to Moderate	Low to Moderate	Low	Low to Moderate	<1% LEs used	<1% LEs used

* Current Work
N/A: Not Available

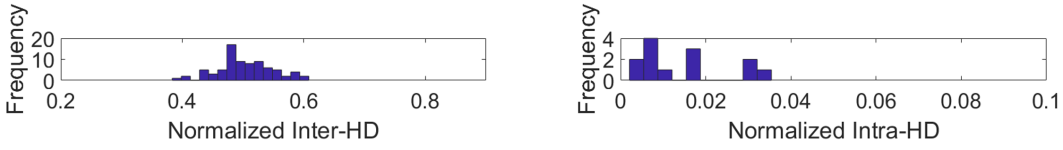
V. Conclusion

In this paper, we have presented FDPUF, a novel PUF-based hardware authentication solution that creates a digital signature by analyzing the supply currents in the frequency domain. We utilized the time-domain current measurements collected by precision current sensors and applied discrete cosine transform (DCT) on them. We reconstructed the signals after applying energy thresholds, Wiener filtering, and inverse DCT (IDCT). The transformed signals delivered high PSNRs ($>$ 30db), ensuring that most of the noise was removed from the original time-domain signal. For each of the 20 test chips under test, we generated 480-bit signatures. The PUF signatures demonstrate high uniqueness ($\sim$ 49.85% avg. inter-HD), robustness ($\sim$ 1.27% avg. intra-HD), uniformity (46.65 %), and randomness. We have performed experiments by varying the supply voltage and the operating temperature. Based on our evaluation, the FDPUF exceeds the robustness performance compared to *CurIAs*, its time-domain counterpart. Using DCT allows the PUF to be implemented with minimal additional overhead, as this technique requires fewer computational resources than other frequency domain analyses. Future work will explore alternative frequency domain techniques, such as discrete wavelet transformation (DWT). We expect that the robustness can be enhanced even further by taking advantage of DWT's

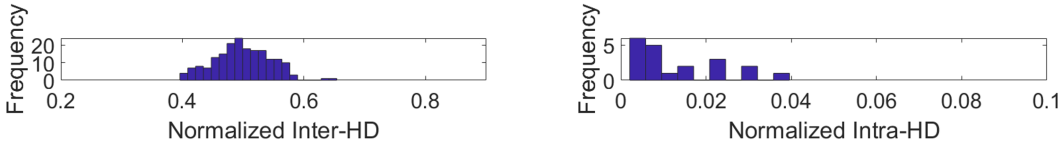


(a) **At 70%; Avg. Inter-HD = 48.99%, Avg. Intra-HD = 1.67%**

(b) **At 80%; Avg. Inter-HD = 49.83%, Avg. Intra-HD = 1.63%**

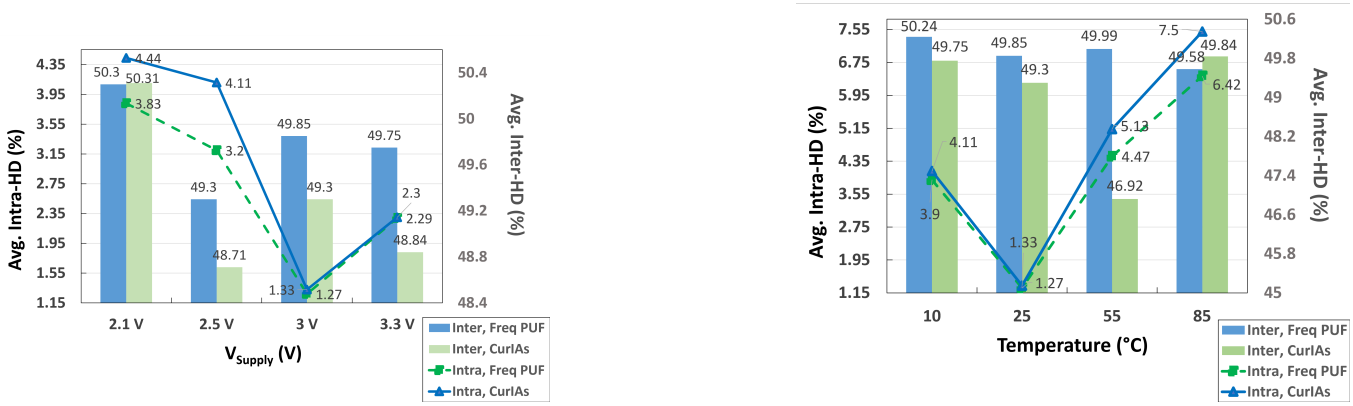


(c) **At 90%; Avg. Inter-HD = 50.35%, Avg. Intra-HD = 1.49%**



(d) **At 99.9%; Avg. Inter-HD = 49.85%, Avg. Intra-HD = 1.27%**

Fig. 9: Comparison of percentage bit-error at different signal energy thresholds: (a) 70%; (b) 80%; (c) 90%; and (d) 99.9%.



(a) (b)

Fig. 10: Comparison of uniqueness and robustness between FDPUF and *CurIAs* over supply voltage and temperature variations: (a) Comparison of V_{Supply} variation results at $Temp = 25$ °C. (b) Comparison of temperature variation results at $V_{Supply} = 3.0$ V. The bit-errors increase as the observation points deviate from the optimum conditions.

joint time-frequency resolution.

The proposed authentication scheme is suitable for fingerprinting hardware used for edge computing applications that are vulnerable to counterfeiting, cloning, as well as in-field tampering (e.g., replacement of a hardware component) through physical attacks. FDPUF-based authentication paradigm can be effectively employed on microelectronic devices that do not have dedicated PUF structures, e.g., commercial off-the-shelf (COTS) hardware components, such as FPGAs and micro-controllers, which are widely used in edge computing. In COTS devices, the FDPUF paradigm can be used to generate unique and robust authentication signatures through frequency domain analysis of transient current waveform acquired in response to specific workloads, such as the boot code for a microcontroller. The workload can be varied (as challenge vectors) to create a large challenge-response space to further enhance the PUF's applicability for these devices. Extension of FDPUF to different classes of microelectronic devices, including COTS, can be another significant research area for future exploration.

ACKNOWLEDGMENT

The authors acknowledge funding support for this work through award number FA8651-19-F-1032 (AFOSR-Eglin).

REFERENCES

[1] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Applied Physics Reviews*, vol. 6, no. 1, p. 011303, 2019. [Online]. Available: https://doi.org/10.1063/1.5079407

[2] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, San Diego, CA, USA, June 2007, pp. 9–14.

[3] L. Bossuet, X. T. Ngo, Z. Cherif, and V. Fischer, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 1, pp. 30–36, 2014.

[4] S. Vrijaldenhoven *et al.*, "Acoustical physical uncloneable functions," *Philips internal publication PR-TN-2004-300300*, 2004.

[5] Z. Chen, Y. Zeng, G. Hefferman, Y. Sun, and T. Wei, "FiberID: molecular-level secret for identification of things," in *2014 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2014, pp. 84–88.

[6] G. Lenzini *et al.*, "Security in the shell: An optical physical unclonable function made of shells of cholesteric liquid crystals," in *2017 IEEE Workshop on Information Forensics and Security (WIFS)*, 2017, pp. 1–6.

[7] Y. Cao *et al.*, "Optical identification using imperfections in 2D materials," *2D Materials*, vol. 4, no. 4, p. 045021, sep 2017. [Online]. Available: https://doi.org/10.1088/2053-1583/aa8b4d

[8] G. DeJean and D. Kirovski, "RF-DNA: Radio-frequency certificates of authenticity," in *Cryptographic Hardware and Embedded Systems - CHES 2007*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 346–363.

[9] B. Chatterjee, D. Das, and S. Sen, "RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning," in *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2018, pp. 205–208.

[10] S. D. Paul and S. Bhunia, "CurIAs: Current-Based IC Authentication by Exploiting Supply Current Variations," *IEEE Transactions on Computers*, pp. 1–1, 2022.

[11] K. Xiao, D. Forte, Y. Jin, R. Karri, S. Bhunia, and M. Tehranipoor, "Hardware Trojans: Lessons learned after one decade of research," *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 22, no. 1, pp. 1–23, 2016.

[12] M. M. Tehranipoor, U. Guin, and D. Forte, "Counterfeit Integrated Circuits," in *Counterfeit Integrated Circuits*. Springer, 2015, pp. 15–36.

[13] National Institute of Standards and Technology, "Glossary of key information security," https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, 2013.

[14] D. Merli, J. Heyszl, B. Heinz, D. Schuster, F. Stumpf, and G. Sigl, "Localized electromagnetic analysis of ro pufs," in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 19–24.

[15] M. Shiozaki and T. Fujino, "Simple electromagnetic analysis attack based on geometric leak on asic implementation of ring-oscillator PUF," *Journal of Cryptographic Engineering*, vol. 11, no. 3, pp. 201–212, 2021.

[16] L. Tebelmann, M. Pehl, and V. Immler, "Side-channel analysis of the TERO PUF," in *Constructive Side-Channel Analysis and Secure Design*, I. Polian and M. Stöttinger, Eds. Cham: Springer International Publishing, 2019, pp. 43–60.

[17] S. Bhunia and K. Roy, "Dynamic supply current testing of analog circuits using wavelet transform," in *Proceedings 20th IEEE VLSI Test Symposium (VTS 2002)*, 2002, pp. 302–307.

[18] S. Bhunia, K. Roy, and J. Segura, "A novel wavelet transform based transient current analysis for fault detection and localization," in *Proceedings of the 39th Annual Design Automation Conference*, ser. DAC '02. New York, NY, USA: Association for Computing Machinery, 2002, p. 361–366. [Online]. Available: https://doi.org/10.1145/513918.514011

[19] F. M. Megahed and J. A. Camelio, "Real-time fault detection in manufacturing environments using face recognition techniques," *Journal of Intelligent Manufacturing*, vol. 23, no. 3, pp. 393–408, 2012.

[20] L. Yao, Z. Wang, and J. Ma, "Fault detection of the connection of Lithium-ion power batteries based on entropy for electric vehicles," *Journal of Power Sources*, vol. 293, pp. 548–561, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378775315009921

[21] P. Gangsar and R. Tiwari, "Online diagnostics of mechanical and electrical faults in induction motor using multiclass support vector machine algorithms based on frequency domain vibration and current signals," *ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg*, vol. 5, no. 3, 2019.

[22] K. Gaedke, J. Franzen, and P. Pirsch, "A fault-tolerant DCT-architecture based on distributed arithmetic," in *1993 IEEE International Symposium on Circuits and Systems*. IEEE, 1993, pp. 1583–1586.

[23] N. Banerjee, G. Karakonstantis, and K. Roy, "Process variation tolerant low power dct architecture," in *2007 Design, Automation & Test in Europe Conference & Exhibition*. IEEE, 2007, pp. 1–6.

[24] N. Ahmed, T. Natarajan, and K. R. Rao, "Discrete Cosine transform," *IEEE transactions on Computers*, vol. 100, no. 1, pp. 90–93, 1974.

[25] J. James and V. J. Thomas, "Audio compression using dct and dwt techniques," *Journal of Information Engineering and Applications*, vol. 4, no. 4, pp. 119–124, 2014.

[26] S. Narasimhan, K. Kunaparaju, and S. Bhunia, "Healing of dsp circuits under power bound using post-silicon operand bitwidth truncation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 59, no. 9, pp. 1932–1941, 2012.

[27] C. T. Fike, *Computer evaluation of mathematical functions*. Prentice-Hall, 1968.

[28] A. V. Oppenhein, R. W. Schafer, and J. R. Buck, "Discrete-time signal processing," *Prince Hall, Sec*, vol. 11, 1999.

[29] W. K. Pratt, "Generalized Wiener filtering computation techniques," *IEEE Transactions on Computers*, vol. 100, no. 7, pp. 636–641, 1972.

[30] J. S. Lim, "Two-dimensional signal and image processing," *Englewood Cliffs*, 1990.

[31] The MathWorks, Inc. (1999) Peak signal-to-noise ratio (psnr). Available: https://www.mathworks.com/help/images/ref/psnr.html.

[32] A. Maiti, V. Gunreddy, and P. Schaumont, *A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions*. New York, USA: Springer New York, 2013, pp. 245–267.

[33] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," Gaithersburg, MD, United States, Tech. Rep., 2010.

[34] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proceedings of the 51st Annual Design Automation Conference*, 2014, pp. 1–6.

[35] Y. Zheng, A. R. Krishna, and S. Bhunia, "ScanPUF: Robust ultralow-overhead PUF using Scan chain," in *2013 18th Asia and South Pacific Design Automation Conference (ASP-DAC)*, Yokohama, Japan, Jan 2013, pp. 626–631.

[36] F. Zhang, S. Yang, J. Plusquellic, and S. Bhunia, "Current based PUF exploiting random variations in SRAM cells," in *2016 Design, Automation Test in Europe Conference Exhibition (DATE)*, Dresden, Germany, March 2016, pp. 277–280.

[37] Z. Wang, Y. Chen, A. Patil, C. H. Chang, and A. Basu, "Current mirror array: A novel lightweight strong PUF topology with enhanced reliability," in *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*, Baltimore, MD, USA, May 2017, pp. 1–4.

[38] A. Basak, F. Zhang, and S. Bhunia, "PiRA: IC authentication utilizing intrinsic variations in pin resistance," in *2015 IEEE International Test Conference (ITC)*, Anaheim, CA, USA, Oct 2015, pp. 1–8.

[39] M. Danesh *et al.*, "Unified Analog PUF and TRNG Based on Current-Steering DAC and VCO," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 11, pp. 2280–2289, 2020.

[40] Y. Cui *et al.*, "Lightweight Modeling Attack-Resistant Multiplexer-Based Multi-PUF (MMPUF) Design on FPGA," *Electronics*, vol. 9, no. 5, 2020. [Online]. Available: https://www.mdpi.com/2079-9292/9/5/815

[41] C. Vega, P. Slpsk, S. D. Paul, A. Chatterjee, and S. Bhunia, "MeLPUF: Memory-in-Logic PUF Structures for Low-Overhead IC Authentication," in *2023 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, 2023, pp. 1–7.