IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 24 June 2025, accepted 8 August 2025, date of publication 18 August 2025, date of current version 22 August 2025.

Digital Object Identifier 10.1109/ACCESS.2025.3600010

RESEARCH ARTICLE

Additively Manufactured RF Electronics With Structurally Integrated Physically Unclonable Functions for Wireless System Security

AARON PENDINO, (Member, IEEE), NGHIA NGUYEN, (Graduate Student Member, IEEE), SAIF E. NOUMA, (Graduate Student Member, IEEE), JING WANG, (Senior Member, IEEE), ATTILA A. YAVUZ, (Senior Member, IEEE), YASIN YILMAZ, (Senior Member, IEEE), AND GÖKHAN MUMCU, (Senior Member, IEEE)
Department of Electrical Engineering, University of South Florida, Tampa, FL 33620, USA

Corresponding author: Aaron Pendino (aaronpendino@usf.edu)

Research was sponsored by the Army Research Laboratory and was accomplished under Cooperative Agreement Number W911NF-24-2-0078. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Laboratory or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

ABSTRACT Physically unclonable functions (PUFs) are alternatives to secret keys stored in non-volatile memory. PUFs derive secret keys on demand based on readings invoked from the complexity of their structures or their physical properties. Conventional PUFs rely on the variations and tolerances involved in their manufacturing processes. On the other hand, traditional manufacturing processes aim to achieve cost-effective device replication by minimizing tolerances often through the use of masks for patterning which in turn limits PUF security by reducing their response diversity across multiple devices. Additionally, the fact that manufacturing tolerances are openly known leads to higher quality adversarial attacks towards these conventional PUFs. In contrast to traditional volume manufacturing, emerging additive manufacturing (AM) techniques are mainly mask-free and therefore cost-effective for creating unique randomizations within devices to act as PUFs. With AM, randomizations can be deliberately introduced by the designers in a way to enhance security and/or complicate the PUF operation mechanisms. This manuscript, for the first time, utilizes laser-enhanced direct print additive manufacturing (LE-DPAM) technology to demonstrate that AM based novel PUF security primitives can be structurally integrated with RF electronics such as antennas. Specifically, we investigate the use of compact I/O expander IC packages and demonstrate a PUF that utilizes 4 such IC packages structurally integrated directly under the ground plane of a 5.8 GHz ISM band patch antenna. Each IC package exhibits 48 input/output (I/O) pins leading to a 192-bit PUF security primitive where the I/O pins are randomly connected to high or low digital states. The NIST statistical test results confirm that the generated PUF outputs exhibit a high degree of statistical randomness, as demonstrated with high confidence p-values across all NIST tests. Furthermore, we evaluate the security of the proposed PUF against widely used machine learning (ML) modeling attacks and demonstrate that the PUF is robust with none of the attacks achieving prediction success that exceeds random guessing.

INDEX TERMS Additive manufacturing, 3D printing, physically unclonable function, antenna, wireless system, security, machine learning, modeling attack.

I. INTRODUCTION

With the number of wireless systems continuing to grow, there is an increasing need to keep these systems secure. Current security methods for wireless systems in which a secret key is stored in the device memory are susceptible to attacks, such as fault injection or trojan attacks [1], and they may require a continuous supply of power to their tamper detection/prevention circuitry [2]. Physically unclonable functions (PUFs) are being proposed as alternatives

The associate editor coordinating the review of this manuscript and approving it for publication was Li Yang.

to memory-stored keys to improve device security. Systems utilizing PUFs derive their secret keys on demand often by making measurements on primitive circuits or materials that get impacted by the random process variations occurring during their manufacturing stage. Since manufacturing tolerances give rise to randomized readings, PUFs become device specific and unclonable. PUFs are harder to ascertain and attack since they only generate the key when powered up and requested.

A variety of PUF security primitives have been developed by utilizing different physical phenomena [3]. For example, there are PUFs that rely purely on electrical signals such as delay-based PUFs (e.g. the arbiter and ring oscillator PUFs [4]), and memory-based PUFs (e.g. the SRAM and butterfly PUFs [4]). These PUFs often require error-correcting processes [5] and/or fuzzy extractors [6] to effectively be used for cryptographic purposes. On the other hand, there are also PUFs that employ phenomena other than purely electrical signals such as optical PUFs (e.g. the nanoparticle distribution PUF and liquid crystal PUF [3]), and RF PUFs (e.g. the LC PUF [3]). PUFs that do not purely rely on electricity to function often require specialized equipment, hence they are typically more difficult to integrate and interrogate [3]. PUFs in general suffer in three broader areas: response variations due to sensitivity to the environment; overwhelming process characterizations for achieving response uniformity; and widespread knowledge regarding how PUF is structured and operated. For example, the ring oscillator PUF [5] relies on the varying oscillation frequencies of delay loops stemming from manufacturing tolerances to determine response bits. Since the oscillation frequencies are susceptible to variations in temperature and voltage, a sophisticated error correction mechanism must be employed, increasing design complexity. To alleviate this drawback, PUFs less sensitive to noise can be constructed based on process characterizations to achieve more uniform and repeatable response distributions. However, the process characterizations for such PUFs can be quite cumbersome. One such example is the VIA-PUF [7], [8] which relies on attaining a probability of 50% for successful formation of conductive vertical interconnect accesses (vias). Practically, this is hard to achieve because it requires systematic characterizations to determine an aspect ratio that will have a 50% chance of successful through via formation to provide a conductive path to the ground. Most importantly, the aspect ratio needs to be redetermined if a new process node or substrate thickness is required. Widespread knowledge on how a PUF operates and how it is internally structured is also an important drawback because machine learning based attacks that model the PUF structure are shown to achieve great success towards certain PUF types [9]. Given these drawbacks, it would be desirable to have a PUF with a robust performance that is easy to evaluate, can have a varying physical structure, and can be readily executed without refinement if design parameters are changed.

Emerging additive manufacturing (AM) technologies can greatly alleviate the PUF drawbacks associated with traditional manufacturing. AM is mainly mask-free, which allows cost-effective creation of new randomizations within the device structures to act as PUFs. Such unique randomizations can be deliberately introduced by the designers, with no additional cost, in various ways to enhance the strength and complicate the prediction of the PUF mechanism. Our research group investigated AM techniques, more specifically laser-enhanced direct print additive manufacturing (LE-DPAM) technology, for structurally integrated RF electronics such as a Ku-band antenna integrated with a polarization select switch [10], X-band antenna integrated with a phase shifter IC [11], and mm-wave antennas integrated with beamformer ICs [12]. Recently, we introduced the concept of chaotic antenna arrays that consist of geometrically randomized antenna elements and feed lines to generate device specific enhanced RF fingerprints which are detectable by machine learning for authentication [13], [14] and utilizable as physical layer security encoding during wireless communication [15]. LE-DPAM combines fused deposition modeling (FDM) of thermoplastics, microdispensing of conductive pastes, laser-machining and micromilling to create multilayered structurally integrated electronic systems [16]. In this manuscript, we demonstrate for the first time that LE-DPAM can be used to create novel AM-based digital PUFs that can also be structurally integrated in a compact way with RF electronics such as antennas.

The proposed PUF makes use of low-cost commercial-off-the-shelf input/output (I/O) expander IC packages. The ICs are structurally embedded, and their I/O pins are randomized in connection to high and low digital states using LE-DPAM. A subset of these pin states is read on demand to serve in security measures. Different numbers and types of I/O expander ICs can also be employed by the designers to achieve a vast variety in the PUF format which may further aid as a security measure against modeling attacks. As a specific example, throughout this manuscript, we demonstrate the design, manufacturing, and experimental verification of such a PUF that utilizes 4 identical I/O expander IC packages that are structurally integrated directly under the ground plane of a 5.8 GHz ISM band patch antenna. The selected IC package (Diodes Incorporated PI4IOE5V96248) exhibits 48 I/O pins leading to a 192-bit PUF. We demonstrate the use of these bits within a strong PUF scheme that achieves near ideal performance based on the PUF metrics defined in [17] (i.e. uniformity, uniqueness, reliability, and bit-aliasing). By using software defined radios (SDRs), we also demonstrate that a wireless system employing an antenna can successfully transmit responses acquired by its PUF to get authenticated by another system transmitting the corresponding challenges. Furthermore, we examine the robustness of the proposed PUF against machine learning (ML) modeling attacks and find that it is robust to the commonly used modeling attacks. Section II presents the proposed multilayered structure of

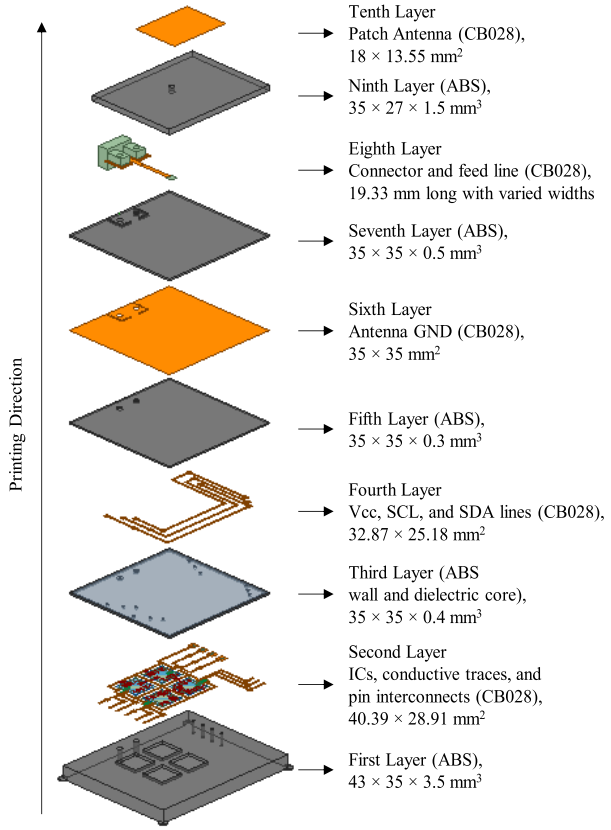


FIGURE 1. Substrate stack-up with four I/O expander ICs.

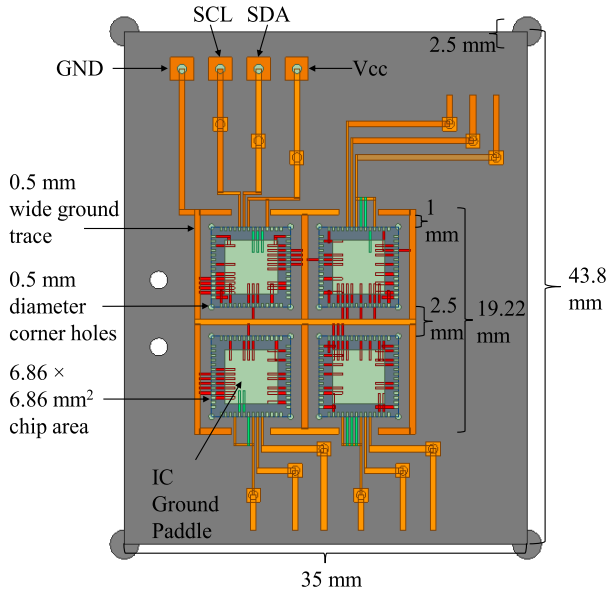


FIGURE 2. IC interconnects and conductive traces (i.e. the second layer layout) microdispensed over the first layer. Address interconnects are shown in green (states: 000 (top left), 011 (top right), 001 (bottom left), and 111 (bottom right)). Meanwhile, interconnects randomizing the states of I/O pins by forcing them to state 0 are shown in red.

the I/O Expander IC PUF (IOE-PUF) and the 5.8 GHz ISM band patch antenna that can be realized with the capabilities of LE-DPAM fabrication. Section III provides the details of the LE-DPAM processes employed to realize the structurally integrated IOE-PUF and antenna. Section IV presents the performance of the device as a PUF. Section V shows the experimental verification of the manufactured device. Section VI examines the IOE-PUF's security against ML modeling attacks. Finally, Section VII draws the key conclusions with a path towards future work.

II. IOE-PUF INTEGRATED ANTENNA DESIGN

A. SUBSTRATE STACK-UP

Fig. 1 depicts the multilayered substrate stack-up proposed for the structurally integrated IOE-PUF and 5.8 GHz ISM band patch antenna. The entire structure consists of ten layers formed from alternating acrylonitrile butadiene styrene (ABS) based dielectric substrates and CB028-based conductive paste layers. In addition, most of the dielectric layers exhibit holes that are filled with CB028 to form vias to achieve vertical transitions among the conductive layers. Some holes are not conductively filled and are included to host the screws for mounting an RF edge connector to test the antenna and employ it along with an external software defined radio (SDR). In addition, there are some unfilled holes to host the header pins that interface with the external microcontroller. The antenna design is carried out with Ansys Electronics Desktop High Frequency Structure Simulator (HFSS) 2022 R1. The IOE-PUF is not an RF device, and its packaging layout can be designed with a diverse set of tools available for printed circuit board (PCB) design. Nevertheless, HFSS is also employed for the layouts involving the IOE-PUF due to its capability to be fully scripted with an external program (e.g. MATLAB) to automate the geometry randomizations. The structure is designed to be printed from bottom to top using LE-DPAM, making the microdispensing to form the patch antenna the last step in manufacturing.

The first layer is a $43.8 \times 35 \times 3.5$ mm^3 ABS substrate which includes cylindrically shaped feet at the corners of the substrate, four holes to host header pins, four cavities for inserting the IC packages (thin quad flat no-leads (TQFN), 7×7 mm^2, 56 pin), and two holes for the RF connector screws. The cylindrical feet placed at each corner of the substrate have diameters of 2.5 mm with centers at the corners of the substrate. These are added to improve adhesion to the printer bed. The four header pins are for interfacing with the power supply (Vcc), data (SDL), clock (SCL), and ground (GND) lines that will run throughout the device for implementing an inter-integrated circuit (I^2C) bus.

The second layer is the CB028 (silver ink) conductive traces microdispensed over the first substrate with further layout details provided in Fig. 2. The IC packages are inserted in cavities upside down to form the package pin and signal line interconnects. Each IC package has three address pins, and these are connected to high (digital 1, 3.3 V, Vcc) or low

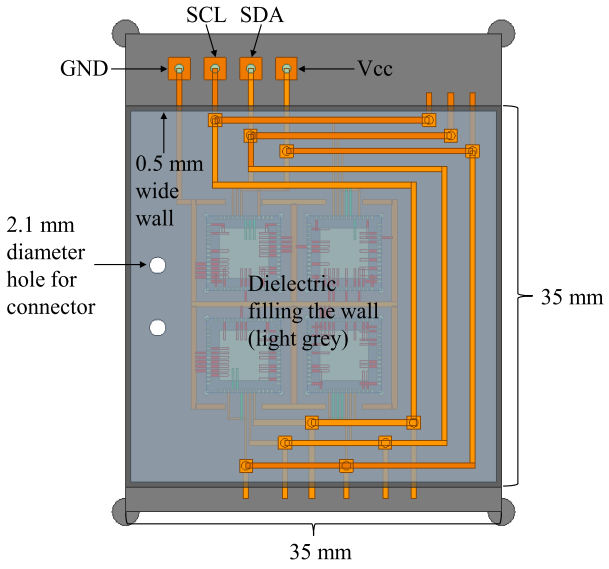


FIGURE 3. Layout of the third and fourth layers for carrying out signal routing.

(digital 0, 0.0 V, GND) states as indicated with green colored interconnects in Fig. 2 to create unique I^2C addresses. The IC package cavities are sized as $6.86 \times 6.86 \times 0.75$ mm^3 based on the dimensions taken from the datasheet. Small holes with diameters of 0.5 mm and centers at the corners of the cavities are micromilled (drilled) to allow for the placement of the square prism shaped IC package into the cavity that is formed with the circular micromilling tool. The cavities are spaced 2.5 mm apart from each other. 0.5 mm wide microdispensed traces run across these gaps and mostly surround all four ICs at a distance of 1 mm from each I/O expander IC. These microdispensed traces that run in between and surround the ICs are at GND level and serve as a potential connection point for the IC package pads. The pads of the IC package are 0.2 mm wide with 0.4 mm pitch. Microdispensing a 0.2 mm wide and 1.3 mm long conductive interconnect to bridge a pad to the surrounding microdispensed trace enforces the corresponding I/O pin of the IC to state 0. The paddle of the IC package must also be grounded. Hence, some I/O pin pads can also be grounded by microdispensing to interconnect the I/O pad to the paddle (which is done with 0.2 mm wide and 2 mm long interconnects), as long as a minimum of one microdispensed interconnect is made that bridges the paddle, pad, and the surrounding GND line together (which is done with 0.2 mm wide and 3 mm long interconnects). The selected I/O expander IC internally sets all floating I/O pins to digital state 1. Hence, no interconnect is needed to realize the high states.

The third layer is 0.4 mm thick and comprised of a 0.5 mm wide wall of ABS filled with EPO-TEK 302-3M dielectric liquid (and cured afterwards) with an overall footprint of 35×35 mm^2 as shown in Fig. 1 and Fig. 3. The dielectric liquid over the IC packages is preferred for several reasons. It fills the gaps between IC package and the surrounding ABS substrate to achieve better and more robust placement and interconnect microdispensing. Moreover, 3D printing ABS directly over the interconnects is found to be not fully reliable. The dielectric liquid eliminates the processing risk of having to carry out FDM directly over the interconnects. The third layer also hosts vias and holes.

The fourth layer is comprised of microdispensed CB028 conductive traces with the layout depicted in Fig. 3. This layer is employed to connect the Vcc, SDL, SCL, and GND pads of the different IC packages together. The fifth layer is an ABS substrate with dimensions of $35 \times 35 \times 0.3$ mm^3, and it is employed for structurally enclosing the layers implementing the IOE-PUF. It is followed by the sixth layer consisting of a conductive CB028 plane to act as the antenna ground plane. The seventh layer is an ABS substrate primarily for the RF signal line and is sized as $35 \times 35 \times 0.5$ mm^3. This layer also hosts holes and vias for RF coaxial edge connector mounting screws and transitioning the connector's body to the ground plane layer. The eighth layer is conductive CB028 for the RF signal line. The ninth layer is an ABS substrate sized as $35 \times 35 \times 1.5$ mm^3 and contributes to the antenna substrate along with the seventh layer. This layer also includes a via connecting the signal line to the patch antenna. The tenth layer is made of conductive CB028 sized as a rectangle to implement the patch antenna.

It is important to note that there are only two aspects of the IOE-PUF design that need to be randomized: 1) the number of the I/O expander ICs, and 2) the interconnects that define the digital high or low states of all the available I/O pads. The number of ICs is mainly dictated by the available area and overall thickness (since ICs can also potentially be vertically stacked in the LE-DPAM technology). Once the placement of the I/O expander ICs is decided on (for example, one layer of ICs and 4 ICs within the layer as in the presented design example), the substrate stack-up can be set to its final configuration in terms of material thickness and number of material layers. For instance, in the presented stack-up, the layer thickness for embedded I/O expander ICs is selected based on the thickness of their QFN packages and the placement of the header pins employed in our experimental verifications. Likewise, the layer thicknesses related to the antenna operation is decided based on well-known RF engineering practices to realize the transmission lines and ISM bandwidth coverage. Randomizations of the I/O pad interconnects are independent from the design of the substrate stack-up.

B. INTERCONNECT RANDOMIZATION

The I/O pads of the ICs are randomized in their digital states in each implementation of the device while all other aspects (such as address, supply, RF signal lines, substrate materials and thicknesses) remain identical. For the design presented in this manuscript, the I/O pin pad interconnect randomizations are first carried out in MATLAB. Specifically, the pseudorandom generator is invoked to obtain numbers that

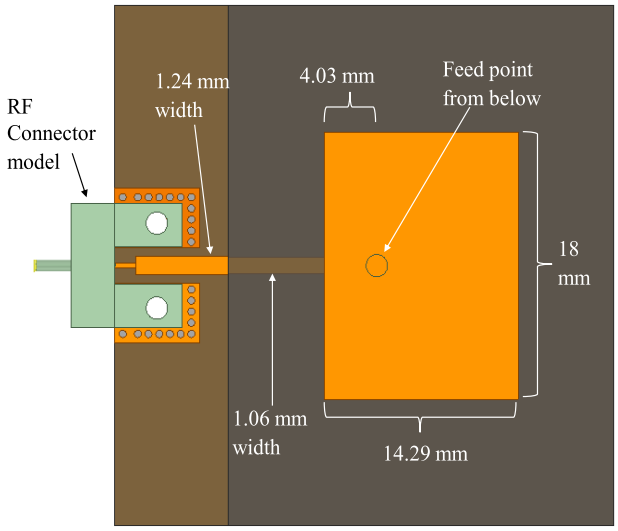


FIGURE 4. Layout details for the 5.8 GHz ISM band patch antenna, microstrip feed line, RF connector model, and its landing pattern.

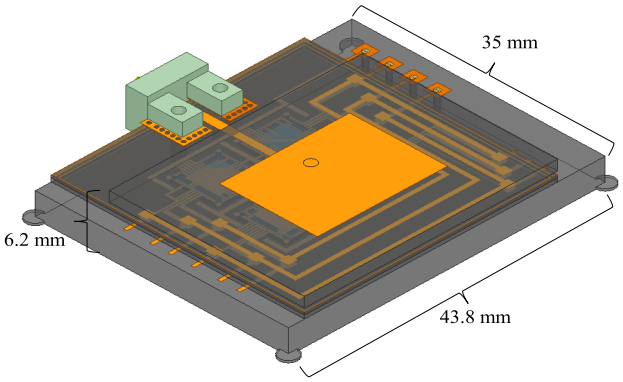


FIGURE 5. 3D design encompassing the IOE-PUF and the 5.8 GHz ISM band patch antenna in a standalone structurally integrated package.

are uniformly distributed between 0 and 1. The digital 0 state is assigned to the numbers between 0 and 0.5. Likewise, the digital 1 state is assigned to the numbers between 0.5 and 1. Since the selected IC exhibits 48 I/O pins, $48N$ random numbers are generated where N denotes the number of ICs. For the design presented in this manuscript, $N = 4$ and there are a total of 192 I/O pins. Due to the default states of the I/O pins being digital 1 when powered on, the MATLAB code is configured to take no action for the digital 1 states. The code generates a python script readable by HFSS and inserts commands to draw the interconnects in HFSS in a way to correspond to the pin pad numbers that are assigned 0 states. Once the MATLAB code generates the script, it invokes the system command line to execute the script in HFSS and export the layout for fabrication. For fabrication simplicity, most of the 0 state I/O pin pads are directly interconnected to the ground paddle of the IC with a few pin pads being interconnected to both the ground pad and the ground lines surrounding the ICs. The code developed can further be advanced to fully automate the process, including conversion of exported design layout files to the file formats employed by the additive manufacturing platform. In addition, all design and manufacturing files can be deleted upon completion to provide further protection. However, such code development is beyond the scope of this manuscript and unnecessary for the experimental demonstration of the proposed IOE-PUF concept.

C. ANTENNA DESIGN

The patch antenna is designed to operate at the 5.8 GHz ISM band. As seen in Fig. 1 from the overall substrate stack-up, the ground plane of the patch antenna provides ample space to structurally embed multiple ICs to develop antennas with structurally integrated PUFs. Inclusion of the patch antenna also allows for demonstration of the IOE-PUF in a wireless system scenario by making use of SDRs. Fig. 4 depicts the layout details of the patch antenna. The relative dielectric constant and loss tangent of the ABS that is utilized in manufacturing is characterized as $\epsilon_r = 2.8$ and $\tan\delta = 0.005$ within the vicinity of 5.8 GHz. The total substrate height seen by the patch antenna is 2 mm, consisting of the stacked 0.5 mm and 1.5 mm ABS layers. Based on the substrate material and thickness, the initial size of the patch and its vertical feed probe location are calculated from the well-known analytical expressions [18]. Ansys HFSS simulations are later employed to fine tune the dimensions to achieve resonance at 5.8 GHz. The width of the 50 Ω RF signal line loaded by the 1.5 mm ABS substrate from the top is calculated as 1.06 mm using the Controlled Impedance Line Designer tool from Keysight's Advanced Design System (ADS). The width of the line that is exposed to air is 1.24 mm and is calculated using the same tool although this can also be calculated from many other tools or analytical expressions for standard microstrip lines. The diameters of the vias used in the RF connector landing patterns are 0.5 mm. At the edge of the substrate, the signal line has a 0.3 mm wide 1.5 mm long section to accommodate the pin of the RF connector. The RF signal line is terminated with a square pad that is 1.875×1.875 mm^2 in size. This pad is connected to the patch with a 1.5 mm diameter via. The simulated $|S_{11}|$ of the antenna is below -25 dB at 5.8 GHz. The $|S_{11}| < -10$ dB bandwidth is from 5.68 GHz to 5.96 GHz. Simulated radiation efficiency is 79% with realized peak gain of 6.40 dBi at 5.8 GHz. Without the connector feed line loss, the antenna exhibits a radiation efficiency of 86%. Lower infill ratio during FDM printing resulting in reduced relative dielectric constant with lower loss tangent and thicker antenna substrates are well-known approaches employed in prior works for further improving the bandwidth and radiation efficiency [10], [11], [19], however, this is not pursued in the presented design.

Fig. 5 depicts the entire 3D device model encompassing the IOE-PUF and antenna which is ready for manufacturing. The overall device structure can be contained within a $43.8 \times 35 \times 6.2$ mm^3 volume. Usage of ABS with black color, structural embedding of PUF ICs, structural embedding of I/O pin pad interconnects, and placement of the ICs within the

proximity of the antenna ground plane are expected to make it impossible to detect the randomized I/O pin connection states by visual and widely available X-Ray based inspections.

III. FABRICATION

Fabricating the design involves three different materials and a variety of techniques. The materials used are ABS, Micromax CB028, and EPO-TEK 302-3M. Black colored ABS is the main structural material selected for its suitability for FDM, relatively low dielectric constant of $\epsilon_r = 2.8$, and loss tangent value of 0.005 near 5.8 GHz. Micromax CB028 (formerly Dupont CB028) is a silver-based conductive paste/ink chosen for its relatively high conductivity among other available conductive inks. Its DC conductivity is reported as 1.45×10^6 S/m [20]. EPO-TEK 302-3M is a clear dielectric epoxy that comes in liquid form with a characterized relative dielectric constant of 3.2 and loss tangent of 0.021. It is selected for its potential to fill gaps, strengthen the fastening of the IC packages within their cavities, and form a protective layer over the microdispensed interconnects at the IC pads when ABS is printed to continue with the manufacturing of the upper layers.

Manufacturing is performed with an nScrypt 3Dn-450HP 3D printer. FDM of ABS is carried out with the extruder and printer bed heated to 235°C and 90°C, respectively. All ABS layers are created using 100% infill. Each ABS layer print is followed by letting the structure cool down to room temperature. This allows the ABS to contract to its nominal size. At this cooled down stage, the top surface of the ABS layer is smoothened using the micromilling tool of the printer by employing a drill bit that is spun at 10,000 rpm. The milling of the surface assists with improvements in the integrity and shape of the structure in subsequent steps of manufacturing. In addition, reducing the surface roughness results in better effective conductivities at RF frequencies. Prior works such as [19], [21] clearly demonstrate that RF conductivity degrades due to surface roughness. Since each substrate is milled for reduced surface roughness, each substrate is printed to be 0.1 mm thicker than its actual design thickness because milling is a subtractive process that approximately removes 0.1 mm thick material volume based on the settings employed in the utilized manufacturing steps.

The CB028 conductive paste/ink is spun at 1000 rpm for 5 min and subsequently spun at 500 rpm for 5 min to ensure a homogenous mixture before microdispensing with a ceramic tip exhibiting 75 μm inner and 125 μm outer diameters. The tip dimensions are selected in a way to realize the narrowest line widths of 0.2 mm. The smallest spacing between lines in the design is also 0.2 mm, and the selected tip allows adjacent lines to remain separated from each other despite some ink spreading that may happen from time to time. Consequently, laser or milling based micromachining [22] over the microdispensed lines is not necessary for the lines related to the IC packages; however, it is applied to the RF signal line for better precision. The optimal microdispensing speed (~1 mm/s), valve pressure (~1 psi), and printing tip height (~40 μm) from the surface of the top layer are iteratively determined during microdispensing in a way to achieve the 0.2 mm line width. Once a layer of conductive paste is microdispensed, the bed is heated up to 90°C and kept at this temperature for 3 hours to cure it.

The first layer of the structure is printed in accordance with the dimensions described in Section II and milled for surface smoothness. Subsequently, the header pin pads, header pin lines, and surrounding ground lines for the ICs are all microdispensed using CB028. After the bed and structure are cooled down, the cavities for the ICs are created using the milling tool. The milling process to create these cavities is executed by milling out small layers of material one at a time until the desired cavity size is reached. The nominal cavity area based on the data sheet of the ICs is 6.86×6.86 mm^2, which is used as the starting point. The cavity areas are further enlarged in iterative steps until each IC package fits into its respective cavity. This resulted in final cavity area of 6.98×6.98 mm^2 for each IC package. The nominal depth of the IC package is 0.75 mm based on data sheet of the ICs. This depth is realized by milling in 0.1 mm steps seven times followed by an eighth pass that is 0.05 mm deep. The flushness of the IC package with the top surface of the cavity is verified with the integrated Keyence laser sensor by inserting the IC package into its cavity. If the IC package is not near perfectly in flush, the depth can be increased iteratively in 0.01 mm milling steps. This is performed for each IC package which eventually resulted in cavity depths of 0.83 mm. The main reason for the variation from the data sheet depth is our desire to bring the pin pads in level with the top surface of the cavity and pin pads exhibit a finite thickness that adds to the overall height of the IC package. Leveling the pin pads with the top surface of the cavity improves the quality achieved in microdispensing the interconnects. Following the insertion of the IC packages into their cavities, EPO-TEK 302-3M is manually placed into the corners of the cavities to fill any minor gap between the ICs and the ABS as well as to hold the ICs in place during subsequent heating and cooling of the printer bed. These allow the interconnects to bridge the gap between the IC pins and ABS more robustly and mitigate the possibility of an interconnect that bridges the gap to become unconnected when the ABS expands during curing. After keeping for 24 hours at room temperature, the EPO-TEK 302-3M is cured, and the randomized connections and address pin connections shown in Fig. 2 are then microdispensed. Testing with a multimeter is performed once the device is cooled down to ensure all connections are in working condition before printing the upper layers. The condition of the prototype by the end of these manufacturing steps is depicted in Fig. 6 and Fig. 7. The black and white stripes observed in Fig. 6 (and also in several upcoming figures related to the manufactured device) are related to the changes in light reflection from the surface once it is micromilled for smoothness. Measurements taken over the surface by the Keyence laser sensor shows that the roughness is contained within $\pm 10\mu$m. Therefore, these color stripes do not correspond to rough surfaces in contrast to what they typically may indicate.

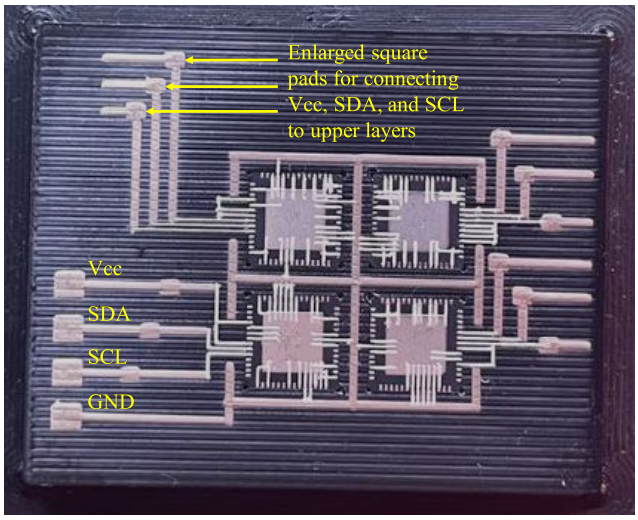


FIGURE 6. First and second layers of the device showing the four I/O expander IC packages in their cavities with microdispensed interconnects.

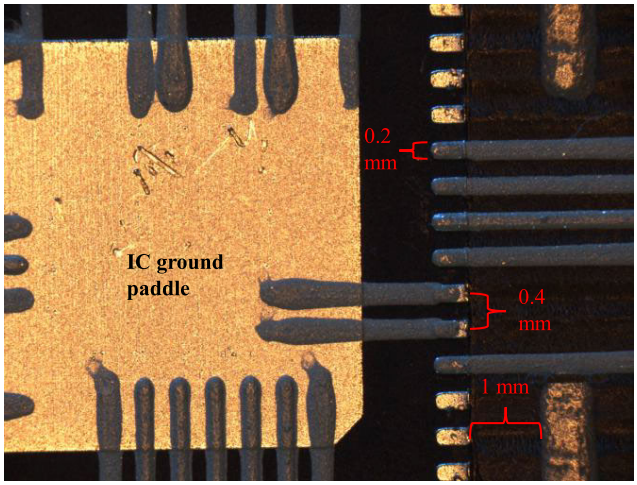


FIGURE 7. Close-up view of microdispensed interconnects on the I/O pin pads and ground paddle of the IC package.

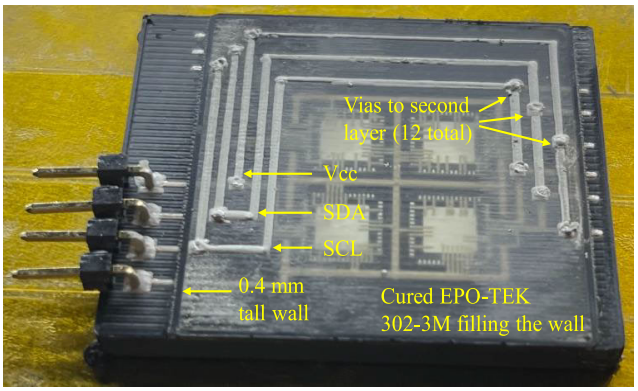


FIGURE 8. Third and fourth layers of the fabricated device showing the wall filled with EPO-TEK 302-3M, top layer (thermally cured), and vias for transitioning to the Vcc, SCL, and SDA lines underneath the top surface.

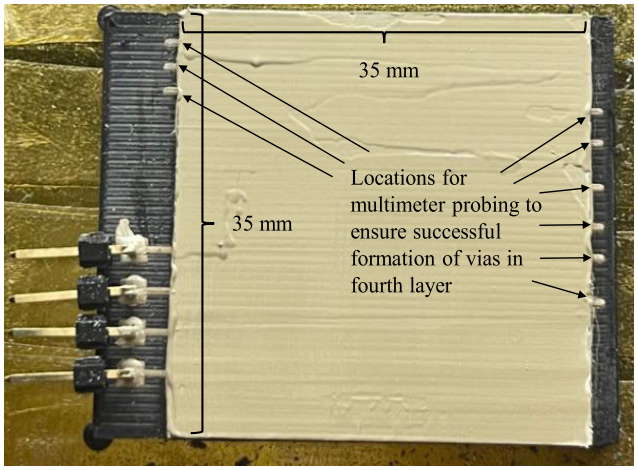


FIGURE 9. Fifth and sixth layers of the fabricated device showing the ground plane of the patch antenna and the probe points in the second layer used for testing the vias created in the third and fourth layer.

With the interconnects completed, the 0.5 mm wide and 0.4 mm tall wall of ABS for the third layer is printed. The interior of the wall is subsequently filled with EPO-TEK 302-3M. Once it is cured, the surface of this layer is smoothened using milling as described before. Holes to touch down to the Vcc, SDA, and SCL pin lines for each of the ICs are created using a 0.5 mm diameter drill bit descending at slow speeds. The process development for the formation of these holes is done by drilling 0.35 mm deep and checking if the connection in the second layer is exposed using a multimeter. If the connection is not exposed, the holes are iteratively drilled and checked in 0.01 mm steps until the connections are exposed to ensure successful via formation. Once the process development for via formation is finalized, the process can be used for all vias in the third layer. The aforementioned process can also be employed in the manufacturing of future devices to expedite their fabrication. With the connection points to the conductive layer on the bottom substrate exposed, the holes are filled with CB028 to form vias. This is followed by microdispensing of routing lines for the Vcc, SDA, and SCL connections. The vias and routing lines are shown in Fig. 8. After cooling down and performing multimeter testing to confirm that the vias are connected properly, a thin layer of Vision Miner nano polymer adhesive high temperature build plate glue is spread over the surface of the design to improve the adhesion between the fourth and fifth layers. This glue is also applied later during fabrication between the sixth and seventh layers and between the eighth and ninth layers. With the glue applied to the fourth layer, the fifth layer is then printed and milled for improving surface smoothness, concluding the fabrication of the stacked layers that embodies the IOE-PUF functionality.

Fabrication of the patch antenna begins with creating the ground plane on the top layer of the IOE-PUF which is done by spreading CB028 over the surface of the fifth layer as seen in Fig. 9. This is followed by printing the 0.5 mm thick seventh layer consisting of ABS. Microdispensing the eighth

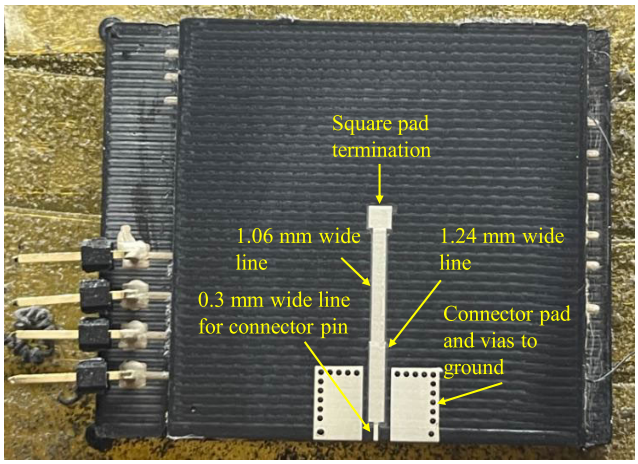


FIGURE 10. Seventh and eighth layers of the device showing the first antenna substrate, RF signal line, and RF coaxial connector landing pattern.

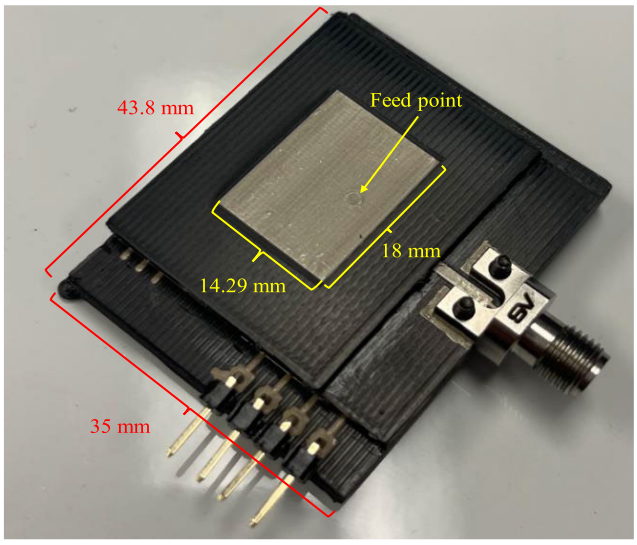


FIGURE 11. Completed device encompassing the IOE-PUF and patch antenna.

layer starts with the formation of the RF coaxial connector landing pattern. Subsequently, the signal line made of CB028 is microdispensed and cured. Since the RF line widths need high precision (in contrast to digital signal lines used for the I/O expander ICs), the line edges are milled with a 0.1 mm drill bit. This helps to achieve the precise width values of 0.3 mm at the RF connector edge, 1.24 mm for the part of the feed line that is exposed to air, and 1.06 mm for the last part of the feed line contained between the two antenna substrates. The last step in the fabrication of the eighth layer is to create the holes on the RF connector pads and fill them with CB028 to form the vias. These vias are created using the same procedures as those used for the vias in the fourth layer by using a 0.5 mm diameter drill bit. The completed eighth layer is shown in Fig. 10. The 1.5 mm thick ninth layer is printed using ABS. Once cooled, the 1.5 mm diameter via connecting the RF signal line to the patch antenna is created with a similar via process and the patch antenna is subsequently microdispensed and cured with dimensions of 18×14.29 mm^2. The last fabrication step is to drill the 2.1 mm-diameter holes for mounting the RF connector. The final structure integrating the IOE-PUF and antenna is shown in Fig. 11.

IV. IOE-PUF PERFORMANCE

A. EMPLOYING IOE-PUF AS A STRONG PUF

It is possible to utilize the proposed IOE-PUF both in weak and strong PUF scenarios. The operation of PUFs is often described with challenge-response pairs (CRPs) that scale with additional complexities, such as more embedded IC packages (i.e. more I/O pins) for the proposed IOE-PUF. Weak PUFs are types of implementations that offer a very limited set of CRPs which gives an adversary the potential to observe and/or obtain all the CRPs in a relatively short time frame. Hence, in most cases, weak PUFs are mainly used as security keys for seeding cryptographic algorithms. For example, all 192-bit states of the manufactured IOE-PUF can be considered as a single CRP and be utilized as a key for seeding a cryptographic algorithm.

On the other hand, strong PUFs are characterized by those implementations that can offer a very large set of CRPs. Moreover, strong PUFs often have an exponentially scaling total CRP number when additional complexities are added to their structure. The extremely large number of CRPs allow a strong PUF to employ a CRP only once and discard it from future use, providing security regarding an adversary's ability to observe the available CRP set and/or perform replay attacks. Strong PUFs are typically envisioned for alleviating the need for cryptographic operations in performing device authentications. The presented IOE-PUF shows promise to be employed in such strong PUF scenarios as well, which we further investigate in this section. We define a CRP as the bit stream that indicates the I/O states of a combination of k pins randomly selected from the total number of $48N$ pins coupled with additional obfuscations. In general, k can be any number between 1 and $48N$. The total number of combinations, i.e. CRPs, can be calculated as

$$\sum_{k=1}^{48N} \binom{48N}{k} = 2^{48N} - 1 \tag{1}$$

which leads to $\sim 2^{192}$ for the $N = 4$ I/O expander ICs employed in the presented IOE-PUF implementation. This shows that the total number of CRPs can be exponentially scaled up with the inclusion of more ICs. For a simpler CRP interrogation protocol, we fix $k = 128$ which produces 128-bit responses with a large number of CRPs $\sim 2^{172}$.

B. PROPOSED AUTHENTICATION PROTOCOL

We assume that the challenge will be transmitted over the air in a wireless scenario by a secure access point (AP) which has securely stored the interconnect states of the

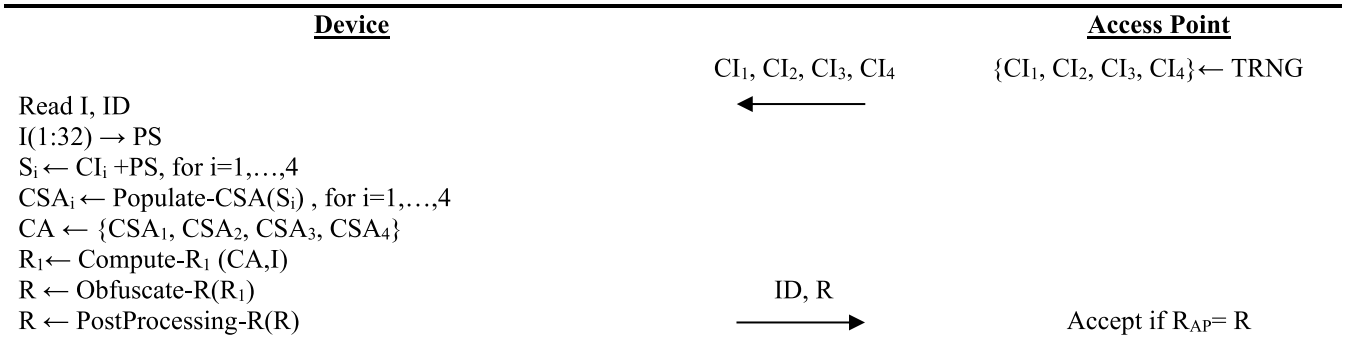


FIGURE 12. IOE-PUF authentication protocol.

Algorithm 1 Population of Challenge Sub-Array (Populate-CSA)

Input: S
Output: CSA
CSA(1:48) ← 0; PRNG_seed ← S; i ← 0
while $\sum_{j=1}^{48}$ CSA(j) < 32
    j ← PRNG mod 48
    CSA(j) ← 1
    i ← i+1

Algorithm 2 Determination of R_1 (Compute-R_1)

Input: CA, I
Output: R_1
j ← 1
for i=1 … 192
    if CA(i) = 1
        R_1(j) ← I(i)
        j ← j + 1

Algorithm 3 Obfuscation of R (Obfuscate-R)

Input: R_1
Output: R
for i=1…192
    R_2(((i+15) mod 192) + 1) ← R_1(i)
    R_3(((i+31) mod192) + 1) ← R_1(i)
    R_4(((i+47) mod 192) + 1) ← R_1(i)
    R_5(((i+63) mod 192) + 1) ← R_1(i)
for i = 1 …192
    R(i) ← R_1(i) ^R_2(i) ^R_3(i) ^R_4(i) ^R_5(i)

Algorithm 4 Post-Processing of R (PostProcessing-R)

Input: R
Output: R
n ← 28
for i=1…128
    idx ← ((i+n) mod 128) + 1
    R(i) ← R(i) ^R(idx)

IOE-PUF during the enrollment phase after manufacturing along with assigning it a corresponding device ID akin to a serial number which allows the AP to construct any desired response given the device ID. To authenticate an IOE-PUF to a network/communication channel, the AP sends out the challenges to the user equipment (UE). The UE transmits its device ID which need not have any secrecy along with the responses to the presented challenges. Upon receiving the IOE-PUF ID, the AP now knows the interconnect states of the specific UE being queried and can determine the appropriate responses to the challenges it sent. Should the device ID be an invalid ID, the AP readily knows to stop communication. With the large number of possible CRPs, multiple CRPs can be utilized for each authentication and can then be subsequently disposed of so they are never utilized again which eliminates the possibility of replay attacks. In this scenario, openly transmitting the particular set of 128 I/O pins being challenged and their corresponding I/O pin state responses will not be secure. If the wireless transmissions are intercepted by an adversary, the entire I/O states of the ICs within the UE may be obtained by intercepting just a few CRP transmissions. Instead, we form the challenges to be transmitted by the AP from four random 32-bit challenge integers (CIs). These numbers are used by the UE hardware (such as a programmed microcontroller in the presented demonstrations in Section V) to obtain the responses that will correspond to the received CIs. Following the response determinations, the IOE-PUF transmits the responses back to the AP. Once the AP verifies that the responses received match the ones specific to the PUF ID, the device is authenticated.

The authentication process is summarized in Fig. 12 with further details of specific processes in the following discussion.

For interpretation of the CIs, the UE hardware has a built-in pseudorandom number generator (PRNG) which can be seeded by a 32-bit integer. A starting point for the PRNG is created using a 32-bit number created from a set of I/O pin states (i.e. 32 bits selected out of the 192 I/O pin states and stored in a PUF state array (PS)) where the I/O pin states are read only when CIs are received and stored in a 192-element interconnect array (I). This makes the starting point device-specific. It would be possible, though unlikely, that two IOE-PUFs would have the same random seed from

the selected 32 selected bits, but the states of the remaining 160 pins would have differences that still make the CRPs unique to each device iteration. To combine the PS and the four CIs, four seed values (S_1, S_2, S_3, and S_4) are created by summing PS with each of the 32-bit CIs. Once the S values are created, 4 48-element integer challenge sub-arrays (CSA_1, CSA_2, CSA_3, and CSA_4) are initialized all with 0 entries. Next, CSAs are filled using Algorithm 1. This algorithm runs independently for all CSAs starting from CSA_1. For forming CSA_1, first S_1 is used to seed the PRNG. Then, the PRNG is called to generate a number between 1 and 48. The generated number is then used as an index of CSA_1 for flipping an element to 1. This process is successively repeated until CSA_1 has a total of 32 ones. Afterwards, CSA_2, CSA_3, and CSA_4 are formed with Algorithm 1 by using S_2, S_3, and S_4 as the seeds, respectively.

Following the completion of Algorithm 1, the CSAs are concatenated together to create the 192-element challenge array (CA) which ends up containing 128 ones. Indices of CA with elements of one are then used to select the elements from interconnect array I to form the 128-element initial response array (R_1) by following Algorithm 2. Next, Algorithm 3 is employed to form the 128-element response array (R). Algorithm 3 begins by generating the R_2, R_3, R_4, and R_5 arrays which are copies of R_1 that are right circularly shifted by 16, 32, 48, and 64 entries, respectively. Subsequently, the algorithm generates R by operating all R_i (i=1, 2, 3, 4, 5) arrays on each other using the bitwise XOR operation (^). The copy, circular shift, and bitwise XOR operations of Algorithm 3 are done to bring the uniformity of R closer to 50%. Without these additional obfuscations, the uniformity of responses read directly from interconnect states can vary from one device to the next as the interconnect states for a particular device are not guaranteed to have half the interconnects set to 0 or 1, so they are required for improving the IOE-PUF performance.

A final step in forming the response array R is post-processing and improving the statistical quality of generated streams. In our scenario, we consider a lightweight non-linear XOR mixing process described in Algorithm 4 where each bit is XORed with a non-adjacent neighbor in the circular view of R. This non-linear self-mixing acts as an arithmetic post-processing layer designed for the conditioning of the response stream and the redistribution of the entropy across the response space [24]. Empirical evaluation using the NIST Statistical Test Suite (see Section IV-E) confirms that this transformation enhances the diffusion properties of the output yielding improved statistical uniformity and success rates thereby reinforcing the overall randomness quality of the responses. Advanced post-processing techniques such as those in [24] and [25] could be used to further improve the randomness quality and increase the entropy extraction efficiency.

The process of generating a response from the UE takes approximately 325 μs. Using a 1 MHz clock speed for the I^2C communication and reading 192 bits individually from the I/O expanders results in a minimum read time of 252 μs including the acknowledge bits and addressing (252 clock cycles in a perfect implementation). Other functions and operations in the authentication protocol contribute to the remaining generation time. Once generated, the response is then modulated and transmitted by the IOE-PUF antenna before securely deleting the data received from the IOE-PUF and waiting for another set of CIs to be received. The AP generates the expected response R_{AP} using the device ID and the known algorithms and compares it to R at which point the device is authenticated if $R = R_{AP}$.

It is important to note that although the PUF scheme described above is expected to be resilient towards interception of wireless signals, it requires the UE hardware (microcontroller used for the presented demonstrations) interfacing with the PUF to remain secure during the formation of responses. Otherwise, an adversary gaining access to the UE hardware can brute force learn the CRPs without physically inspecting the I/O expander IC pin states. Using the proposed additive manufacturing-based packaging approaches, more advanced versions of PUFs can be devised to hide the PUF structure from an adversary even if the adversary gains access to the UE hardware. Such PUF types, consisting of different IC types and CRP mechanisms, are currently being developed and will be reported in the future.

C. SUMAMRY OF DESIGN PARAMETERS

The authentication protocol can be generally applied to any version of the IOE-PUF consisting of more ICs and/or different format of ICs (such as ICs with fewer I/O pin states). Important design parameters are i) the available footprint size for the placement of the ICs, ii) how many I/O states overall will be provided by these ICs, iii) number of ICs, iv) the thickness and layering needed to fit all the ICs within the available footprint, v) how to access/read the pin states form the ICs, and vi) the platform for implementing the authentication protocol. For example, the footprint size available for a single 5.8 GHz patch antenna as in this manuscript is conducive to an IOE-PUF consisting of 4 I/O expander ICs, but an IOE-PUF created for an antenna array of the same antenna would have a significantly larger footprint which would allow it to incorporate more I/O expander ICs. This factors into the desired number of states for the IOE-PUF which will dictate the selection of the I/O expander IC as well as how many are required (if the selected IC has less I/O pins then more ICs will be required). The thickness of layers containing the ICs will be dictated by the thickness of the selected IC packages, and the layering to fit the ICs within the available footprint will depend on the size of the footprint and number/size of the ICs. Specifically, if a smaller area footprint is desired but additional vertical space is available, the designer could integrate two layers of ICs together (as opposed to a single layer like presented in this manuscript). Implementing the pin-state reading and authentication protocol together are the last major design parameters and can be done in tandem. For example, the I^2C protocol

for reading the information from the ICs selected for this manuscript can be done on a microcontroller which is also the platform used for the UE portion of the authentication protocol. A different consideration could be made to implement these design parameters together on another platform, such as FPGA, to achieve a faster read time by reading multiple ICs simultaneously and/or to introduce the IOE-PUF into a more complex system.

D. STATISTICAL PUF METRICS

The IOE-PUF's effectiveness as a PUF depends entirely on its interconnect randomization and implementation. Through process refinement (i.e., the manufacturing steps detailed in Section III), the states of randomized I/O pin pad interconnects with the fabricated device perfectly (100%) reflect the binary states described in the software that randomizes them. Due to the fact that the manufacturing success rate is 100% and the states are solely based on randomly generated numbers, the metrics employed to benchmark the PUF performances according to [17] can be calculated through simulations without necessitating the manufacturing of numerous devices. Furthermore, due to the 100% success rate in mapping randomized interconnects from the interconnect layout design to the actual device, the number of responses that can be generated by the fabricated device is exactly the same as the expected number of CRPs generated in simulations. The PUF metrics require manufacturing many devices, which is out of the scope of this work. However, these metrics can be extracted based on simulations of multiple devices due to the reliability of the fabrication techniques.

The major metrics for describing a PUF's performance are uniformity, uniqueness, reliability, and bit-aliasing [17].

1) UNIFORMITY

Uniformity describes the proportion of bits set to one in the response bits of a PUF with an ideal value at 50% [17]. With the I/O pin pads of the IOE-PUF connected to zero states based on a uniform distribution, the uniformity for a single PUF instance approaches 50%. Furthermore, the additional obfuscations used in the CRP mechanism by creating copies of the selected pin states and performing bitwise XOR operations between all copies further improves the uniformity of the selected 128 bits. For a simulation of 250 IOE-PUF instances each presented with 5,000 random challenges and responses generated corresponding to the CRP mechanism described previously, the average uniformity was 50.00% with a standard deviation of 4.42%.

2) UNIQUENESS

Uniqueness describes the ability to distinguish one PUF from a group of other PUFs of the same type by analyzing the response of different PUF instances to the same challenge and has an ideal value of 50% as described in [17]. Uniqueness (U) is evaluated based on the Hamming Distances (HD) among pairs of PUF responses selected from a set of PUFs

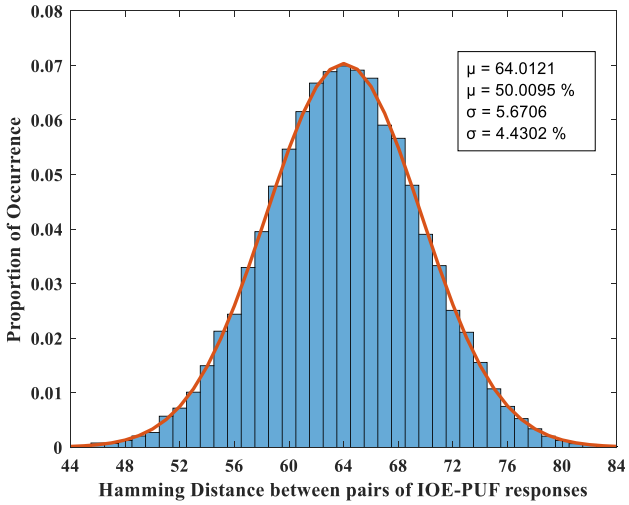


FIGURE 13. Uniqueness evaluated from 250 IOE-PUF instances each having 128 response bits with a fitted normal distribution overlay.

using

$$U = \frac{2}{M\,(M-1)} \sum_{m=1}^{M-1} \sum_{l=m+1}^{M} \frac{HD\,(R_m, R_l)}{k} \times 100\% \tag{2}$$

where R_m and R_l represent k bit responses from the m^{th} and l^{th} PUFs selected from M PUFs. Simulation of (2) with $M = 250$ IOE-PUF instances employing $N = 4$ 48 pin I/O expander chips (using $k = 128$ response bits) results in the uniqueness data shown in Fig. 13. The mean, μ, HD among pairs of PUF responses is 64.01 bits which corresponds to 50.01% of the 128 bits. The standard deviation, σ, is 5.67 bits or 4.43% of the 128 response bits. The uniqueness of the IOE-PUF clearly exhibits a normal distribution with the mean extremely close to the ideal value of 50%. The standard deviation can potentially be reduced by increasing the number of I/O Expander ICs (i.e., the number of response bits) used in the design of the IOE-PUF.

3) RELIABILITY

Reliability describes the ability of a PUF to produce the same response bits to a specific challenge under different operating conditions such as varying temperature and operating voltage with an ideal value of 100% [17]. In the case of the IOE-PUF, the connections made by the CB028 conductive ink will remain connected unless they are physically removed or unless an extremely high temperature, which would otherwise compromise the ABS packaging itself, is reached. Barring such scenarios, the reliability of the IOE-PUF will therefore only be limited by the operation of the I/O expander ICs themselves. The ICs utilized in the IOE-PUF realization within this manuscript operates with a 2.3V - 5.5V supply voltage range and withstands an operating temperature range of -40°C to 85°C. During manufacturing, the ICs and I/O pin pad interconnects (along with several conductive layers) go

TABLE 1. IOE-PUF NIST test results.

Test [a]	P-Value	Success (%)
Frequency	0.4373	100
Block Frequency	0.5544	99
Cumulative Sums (Forward)	0.5955	100
Cumulative Sums (Backward)	0.2368	100
Runs	0.2023	100
Longest Run	0.5341	100
Rank	0.6787	98
FFT	0.5141	98
Non-Overlapping Template – 1	0.8832	100
Overlapping Template	0.6787	100
Universal	0.0519	99
Approximate Entropy	0.3838	99
Random Excursions – 1	0.1453	100
Random Excursions Variant – 1	0.4373	100
Serial	0.1453	100
Linear Complexity	0.6163	99

[a] The number of tested sequences and the sequence length are set to 100 and 10^6 bits, respectively, to satisfy the requirements of all 15 NIST statistical tests. The confidence level for evaluating probability (p)-values is 0.01 as specified in the NIST SP 800-22 standard. The minimum proportion of sequences required to pass each test is 96 out of 100 (i.e. success of 96%).

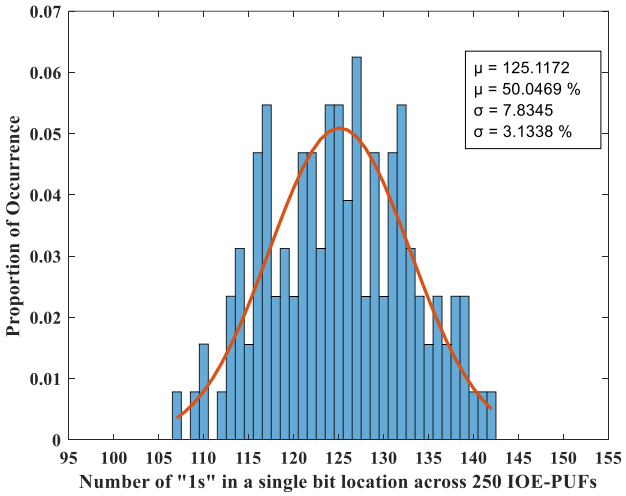


FIGURE 14. Bit-aliasing evaluated from 250 IOE-PUF instances each having 128 response bits with a fitted normal distribution overlay.

through multiple cycles of heating up to 90°C indicating their ability to function reliably after repeated heating and cooling cycles.

To further verify the reliability of the IOE-PUF, the same set of 1,000,000 randomly generated CRPs were measured by the fabricated device under various operating conditions within the limits of the devices. The nominal operating temperature and voltage of the IOE-PUF are 20°C and 3.3V, respectively. The IOE-PUF was subjected to temperatures of -10°C, 4°C, 50°C, and 80°C for two hours each using a Cincinnati Sub-Zero MC-3 Temperature Chamber prior to taking measurements at the nominal operating voltage which were then compared to the baseline measurements taken at 20°C. For each operating temperature, the IOE-PUF produced the same data for all 1,000,000 CRPs as compared to the baseline condition. Additionally, the IOE-PUF was operated within a 3.0V – 3.6V range as the SCL and SDA pins of the microcontroller being used to examine the CRPs are only 3.3V tolerant and were therefore tested in a ±10% operating voltage range at the nominal operating temperature. During these tests, the IOE-PUF produced the same data for all 1,000,000 CRPs as compared to the baseline condition. With broad operating conditions for the IC, the reliable Boolean nature of the interconnects, and the consistent results obtained during both the temperature and voltage reliability tests, it is possible to claim 100% reliability for the presented IOE-PUF.

4) BIT-ALIASING

Bit-aliasing (BA) measures the presence of biasing in the response bits by examining the behavior of each bit across multiple devices for the same challenge having an ideal value of 50% [17]. It is evaluated using the Hamming Weight of the l^{th} bit of the response bits across M PUFs. The calculation can be carried out with the equation

$$(BA)_l = \frac{1}{M}\sum_{i=1}^{M} r_{i,l} \times 100\% \tag{3}$$

where $r_{i,l}$ is the l^{th}bit from an k-bit response of i^{th} PUF selected from M PUFs. The $(BA)_l$ describes the bit-aliasing value for the l^{th} bit. By making using of (3), a simulation of $M = 250$IOE-PUF instances employing $N = 4$ 48 pin I/O expander chips (using $k = 128$ response bits) is carried out to obtain the bit-aliasing data shown in Fig. 14. As seen, the average, μ, bit-aliasing of all the simulated IOE-PUF instances is 125.12 or 50.05% with a standard deviation, σ, of 7.83 or 3.13%. The bit-aliasing of the IOE-PUF exhibits an approximately normal distribution with a mean approaching the ideal value of 50%. Moreover, the standard deviation can be reduced by increasing the number of IOE-PUF instances.

E. NIST TESTS

Although the PUF metrics show near-ideal uniformity, to rigorously assess the statistical quality and entropy distribution of the IOE-PUF responses, a total of 1,000,000 responses were also analyzed using the NIST SP 800-22 Statistic Test Suite [26]. For this evaluation, the dataset was partitioned into 100 sequences of 10^6 bits each to comply with the input requirements for all 15 statistical tests. The confidence level for p-value analysis was set to 0.01, and the minimum success threshold for each test was set to 96% in accordance with NIST SP 800-22 guidelines. As summarized in Table 1, the

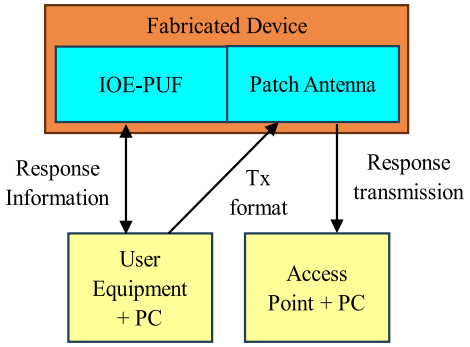


FIGURE 15. Block diagram of the SDR, antenna, and IOE-PUF system. An authenticator party communicates to the device via an SDR which has its own SDR and other hardware to establish secure communications.

IOE-PUF responses successfully pass all 15 tests exhibiting p-values well above the 0.01 threshold and sequence pass rates exceeding the 96% criterion. Notably, the frequency, block frequency, run, FFT, Serial, and Linear Complexity tests, which are particularly sensitive to structural bias and autocorrelation, show robust statistical behavior. Moreover, out of the 100 non-overlapping template matching subsets, the vast majority pass with high margins where the most challenging patterns maintain compliance with the lowest reported success rate equal to 96%. These results collectively indicate a high degree of statistical randomness and entropy dispersion in the response bitstreams confirming that the response set exhibits no detectable bias, correlation, or structural weakness.

V. EXPERIMENTAL VERIFICATION

The fabricated device is tested for three aspects: its PUF response as compared to the designed response generated in MATLAB, its patch antenna performance as compared to the simulated performance in HFSS, and its ability to successfully transmit and receive CRPs by making use of SDRs. A block diagram of the CRP testing setup is shown in Fig. 15. The AP is modeled by an SDR which serves as the transmitter of challenges and receiver of the responses. The patch antenna is connected to another SDR loaded with a series of responses obtained from the UE. These responses are transmitted from the patch antenna to the AP. Upon reception, the responses are reconstructed and verified with their expected values.

Before testing the device with the pair of SDRs, the I/O expander IC connections are first verified for successful manufacturing. The comparison between the device readout via a Teensy 4.1 microcontroller and the interconnects designed in MATLAB demonstrates that all 192 I/O pin interconnects are fabricated successfully. Subsequently, the input reflection coefficient ($|S_{11}|$) response of the patch antenna is measured within the 4-8 GHz band using a VNA to verify that it is operating with the desired resonance characteristics. This measurement is shown in Fig. 16 which depicts that the manufactured antenna operates with an $|S_{11}|$ of -20.4 dB at 5.8 GHz and exhibits an $|S_{11}| < -10$ dB bandwidth ranging from 5.69 GHz to 5.99 GHz. Moreover, it is observed

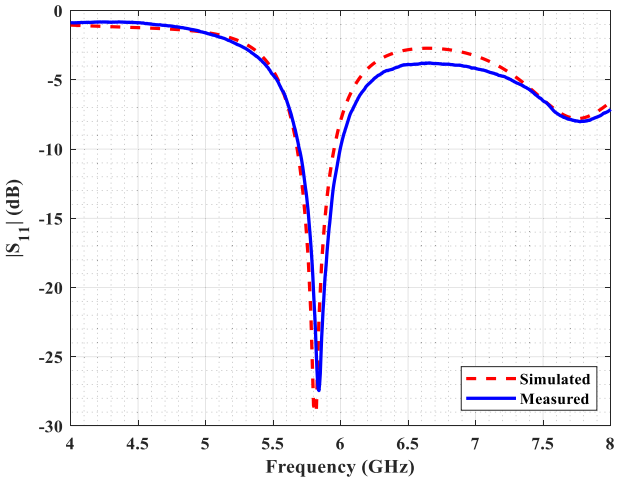


FIGURE 16. Simulated versus measured antenna $|S_{11}|$ performance.

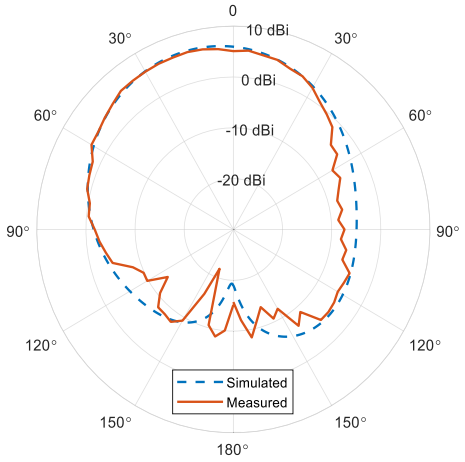


FIGURE 17. E-plane co-polarization realized gain patterns.

that the simulated and measured reflection coefficients are in excellent agreement. As a final verification, the realized gain patterns of the antenna are measured at the USF's anechoic chamber. The E-plane and H-plane realized co-polarization patterns are presented in Fig. 17 and Fig. 18, respectively, along with the patterns expected from HFSS simulations. It is observed that the realized gain agrees well with the simulations, implying that the radiation efficiency of the antenna is also similar to the simulated value. The disagreements between simulations and measurements at the back lobes can likely be ascribed to the presence of a long test cable within the anechoic chamber and the fact that the ground plane of the patch antenna is compactly sized. The maximum measured gain is 6.13 dBi which is on par with the simulated gain of 6.40 dBi.

Having verified the performances of the PUF and antenna components within the 3D printed package, we proceed with the system level verification. MATLAB scripts are written to carry out the tasks related to the system level demonstration. The 3D printed package is also interfaced with a Teensy 4.1 microcontroller which is configured to read 128-bit

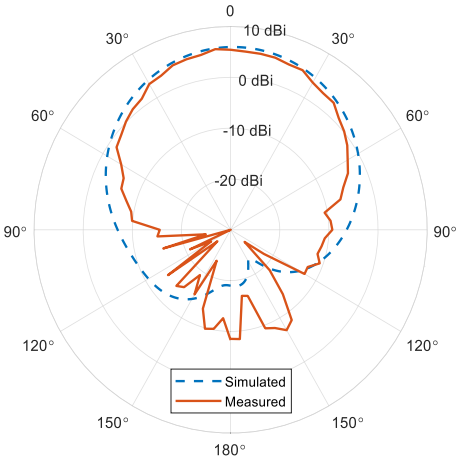


FIGURE 18. H-plane co-polarization realized gain patterns.

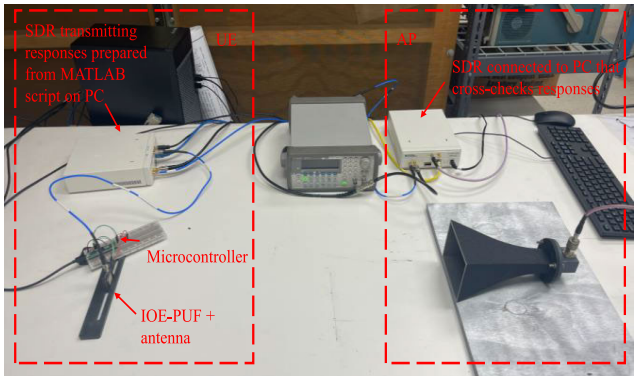


FIGURE 19. SDR and antenna setup used for transmitting and verifying CRPs.

responses corresponding to the challenge integers being sent from MATLAB. Once executed, the MATLAB script sends the challenge integers to the microcontroller and reads back the corresponding response. The script modifies the response by employing a binary phase shift keying modulation scheme and creates a file that can be uploaded to the Ettus N210 SDR used within the presented system demonstration. As a demonstration example, we repeated the above process for a total of 10 unique challenges with arbitrarily chosen groups of four challenge integers. These were used by the AP in this example to generate expected response as well presented to the IOE-PUF to obtain the desired responses. Each transmission is sent using the patch antenna on the IOE-PUF and is received with another SDR operated with a 5.8 GHz standard gain horn antenna. Once the transmissions are received by the AP, another MATLAB script demodulates the information and converts it to its original form to compare with the response that is stored by the AP. As expected, each of these 10 groups of four challenge integers produced the correct response, which then allow the AP to verify the IOE-PUF as a trusted device. Fig. 19 depicts the scene of the system level test. The performance of the IOE-PUF is compared to other PUF designs in terms of area, power, and other aspects of the PUF as listed in Table 2. From the data, it is clear that the IOE-PUF exhibits a robust reliability performance matched only by the VIA-PUF presented in [8] which can be attributed to the Boolean states being used for CRPs that none of the other PUFs exhibit, and the IOE-PUF has the additional benefit of having a modular design due to its additively manufactured nature. This allows it to be implemented in a variety of configurations one of which is underneath antenna ground planes as described in this manuscript as well as in conjunction with antenna arrays which provide more space for further customizations to the design. Regarding the higher power consumption relative to other PUFs, the applications of the IOE-PUF in wireless system designs are such that the power consumption is minimal compared to the power required by the rest of the device such as with drones. Although the IOE-PUF is large relative to many on-chip designs, it has a competitive size compared to off-chip designs. To reduce the size taken up by the IOE-PUF, future work will focus on integrating the PUF mechanism into already-existing antenna substrates thus integrating a PUF into a design without introducing additional area overhead.

VI. SECURITY ANALYSIS AGAINST NON-INVASIVE ATTACKS

The primary strength of the IOE-PUF architecture lies in its discrete mechanism for generating inherently random Challenge-Response Pairs (CRPs). A comprehensive security assessment against machine learning (ML) attacks is critical in evaluating the overall security level of the IOE-PUF. Thus, we conducted evaluations using some widely used ML techniques: Logistic Regression (LR) and Multi-Layer Perceptron (MLP) [35]. Additionally, we employed the PUFmeter [36] framework to characterize the Challenge-Response relationships in terms of the influence of challenge bits on responses, noise sensitivity, and k-junta parameters.

These methods were selected based on their demonstrated effectiveness in PUF modeling attacks and their ability to approximate non-linear relationship between challenges and responses in a PUF. The primary objective was to determine whether any of these models could predict the IOE-PUF response bits with a per-bit accuracy exceeding that of random guessing (50%).

A. EXPERIMENTAL METHODOLOGY

To evaluate IOE-PUF against ML attack methods, we created a dataset with 1 million challenge-response pairs. The dataset was divided into training and test sets with an 80/20 split. Then, we trained and tested each attack method on five different folds of the dataset to avoid data bias and computed the mean and standard deviation of its attack performances.

Since the attackers can know the IOE-PUF design and perform modeling before the use of ML techniques, we explored hand-crafted feature engineering to enhance the learnability of the model. Specifically, we focused on calculating Hamming Distance (HD)-based features derived from the accessible components of CRP, namely the four 32-bit challenge integers and the 128-bit response. To investigate

TABLE 2. Comparison of IOE-PUF to other PUF designs.

PUF	PUF Area	Power	PUF Technology	Mask-Based	Boolean States Used for CRPs	Reliability
This work	369 mm^2	825 µW	Additive Manufacturing	No	✓	100%
XOR APUF [27] [b]	225 – 529 mm^2 [a]	68 mW	28 nm CMOS on Xilinx Artix 7 FPGA	Yes [c]	X	99.41%
Chaotic Bistable Ring PUF [28] [b]	100 – 529 mm^2 [a]	N/A	Xilinx Artix 7 FPGA	Yes [c]	X	N/A
VIA-PUF [8] [b]	0.12 mm^2	N/A	0.18 µm CMOS	Yes	✓	100%
RO PUF [29] [b]	1128 μm^2	119.4 µW	Xilinx Artix 7 TSMC 28 nm CMOS using Xilinx Spartan-3 for reliability	Yes [c]	X	98.22%
Voltage Array PUF [30] [b]	0.0187 mm^2	3.8 µW	65 nm CMOS	Yes	X	95.34%
MEMS PUF [31]	15 mm^2 for sensor	252 µW	Plugging sensor into microcontroller	No	X	92.17%
Optical Flake PUF [32]	25 mm diameter filter and 450 nm laser	100 µW excitation power	Photoluminescence of exfoliated flakes of WS_2	No	X	N/A
LC PUF [33]	1 mm^2 and spectrum analyzer	N/A	Thin film deposition on glass wafers	No	X	N/A
TIR-PUF [34] [b]	Handheld microscope, prism, and laser	0.5 mW	Positions of dispersed spheres mapped using a laser	No	X	93.20%

[a] Exact dimensions are not stated. Hence, the range of their FPGA model sizes are listed.
[b] Additional PUF metrics are also reported for these PUFs, and they are exhibiting near-ideal values like the proposed PUF in this work.
[c] Tested on FPGAs, and these PUFs will require a mask-based process to be implemented on different chips.

TABLE 3. Modeling attack performance, IOE-PUF vs. 4-XOR Arbiter PUF.

ML Method	IOE-PUF	4-XOR APUF
Logistic Regression (LR)	50.84% ± 0.38%	94.80% ± 0.62%
Small MLP-3	50.16% ± 0.20%	98.46% ± 0.99%
Large MLP-4	50.55% ± 0.06%	88.12% ± 0.57%

TABLE 4. PUFmeter performance metrics on IOE-PUF vs. 4-XOR Arbiter PUF.

PUFmeter metrics	IOE-PUF	4-XOR APUF
Avg. Influence on First 32 Bits	49.09%	21.39%
Total Influence	62.894	47.71
Noise Sensitivity ($\delta = 0.01$)	50.17%	38.71%
k-junta	127/128	125/128

potential correlations, we computed the HD between each 32-bit block of the challenge and each 32- bit block of the response. These results were then added as additional features for ML models. This approach is motivated by the internal CRP generation mechanism of the

IOE-PUF, where each 32-bit challenge integer is used to seed a PRNG that generates a 48-bit array filled with exactly 32 ones. Given that each challenge integer independently influences one of the four PRNG-generated blocks, and that the PRNG terminates only when a fixed number of ones is reached, the HD of the inputs may correlate with the structure of the intermediate state and, by extension, the response. We compare all the results with those of 4-XOR Arbiter PUF with a challenge length of 128 bits.

For the LR model, we employed the LBFGS solver for response prediction [35]. The small MLP-3 model consisted of three layers (8 - 16 - 8 neurons) with tanh [37] activation functions throughout, incorporating L2 regularization and dropout for overfitting prevention. The model was trained for 100 epochs using binary cross-entropy loss. Additionally, we implemented a large MLP-4 to study the performance of the IOE-PUF with more complex models. This network has four fully connected layers [1024, 2048, 2048, 1024], and ReLU activation function. While deeper architectures were also considered, they did not provide better results.

All experiments were performed on a computing system with the following specifications: AMD Ryzen 7 7800X processor, 64 GB RAM, and an NVIDIA RTX 4080S GPU.

B. RESULTS

Table 3 summarizes the predictive performance of two commonly used machine learning models: Logistic Regression (LR) and Multi-Layer Perceptron (MLP) when applied to the IOE-PUF and a 4-XOR Arbiter PUF as a baseline.

As observed, all LR and MLP models failed to model the IOE-PUF effectively, with prediction accuracies remaining close to 50%, not better than random guessing. In contrast, the same models achieved significantly higher accuracies, around 94.80%, 98.46%, and 88.12% on the 4-XOR Arbiter PUF for LR, Small MLP-3, and Large MLP-4, respectively. These results underline the vulnerability of conventional Arbiter PUFs to ML attacks and, conversely, demonstrate the inherent modeling resistance of the IOE-PUF, even against nonlinear learners such as MLPs.

To further evaluate the IOE-PUF, we implemented PUFmeter [36], a toolbox that provides provable, theory-driven metrics to assess PUF quality and security level. In our experiments, we set the desired accuracy parameter at $\epsilon = 0.05$ and

the confidence level to $\delta = 0.01$ [36] to evaluate the security level of IOE-PUF. Specifically, ϵ determines how close the reported result is to the true value (the maximum tolerable error). In this case, $\epsilon = 0.05$ means we aim to achieve an error of at most 5% when modeling the PUF's behavior. On the other hand, δ represents the acceptable confidence level, $\delta = 0.01$ specifies that the desired accuracy will be achieved with at least 99% probability. These parameters directly influence the number of CRPs required: higher accuracy and confidence require more CRPs, but provide better reliability in the reported security metrics. Table 4 presents the results of this evaluation using four key metrics: Average Influence, Total Influence, Noise Sensitivity, and k-junta proximity.

- **Average Influence** quantifies how much a single challenge bit when being flipped affects the response. For IOE-PUF, each bit in the first integer, i.e., first 32 bits in the challenge, is flipped. The result shows an average influence of 49.09%, a near-optimal balance where each bit influences the output approximately half the time. In contrast, the 4- XOR Arbiter PUF showed only 21.39%, indicating uneven influence and potential learnable bias in input-output mapping.
- **Total Influence:** The sum of all individual bit influences is measured at 62.894 for the IOE-PUF (out of 128 bits), which is approximately 0.491 per bit, suggesting that almost all input bits contribute equally. The 4-XOR Arbiter PUF, by comparison, has a lower total influence of 47.71, which is 0.373 per bit, showing that fewer bits have a significant effect on the response.
- **Noise Sensitivity** quantifies the probability that a small perturbation (e.g., a single-bit flip) in the challenge causes the response to change. The IOE-PUF attains a near-optimal value of 50.17%, showing strong unpredictability. The 4-XOR Arbiter PUF exhibits less robust performance with a score of 38.71%.
- **k-junta Proximity** indicates how many challenge bits are needed to determine the output. A PUF that relies heavily on only a few bits (i.e., a low k-junta) is more vulnerable to modeling. The IOEPUF exhibits a k-junta value of 127/128, meaning almost all bits are influential, whereas the 4-XOR Arbiter PUF requires only 125 bits to account for its behavior, implying potential redundancy or bias in the remaining bits.

C. ROBUSTNESS AGAINST MODELING ATTACKS

Collectively, these results demonstrate the superiority of the IOE-PUF in resisting modeling attacks. The failure of ML models to exceed random-guess accuracy, coupled with strong PUFmeter metrics—balanced bit influence, high noise sensitivity, and near-maximal junta size—attests to the IOE-PUF's robustness. Unlike traditional Arbiter PUFs, which rely on delay-based analog properties [38], [39], [40] and are thus susceptible to modeling of their continuous-valued mapping from challenge to response via linear or neural approximators, the IOE-PUF implements a high-dimensional Boolean transformation, using logic operations instead of a continuous-valued function, that is both structurally obfuscated and mathematically elusive to standard attack methods.

D. LIMITATIONS AND FUTURE WORK

Although the proposed IOE-PUF is secure against non-invasive modeling attacks, it is vulnerable to invasive attacks which can access the microcontroller memory since the response to each challenge is generated in the microcontroller using the randomized interconnect bits. To avoid such attacks, in a future work, we plan to eliminate the need for microcontroller in the IOE-PUF.

VII. CONCLUSION

This paper introduced, for the first time, an additively manufactured RF antenna with a structurally integrated PUF. Unlike conventional PUFs, the operational principle of the presented PUF relies on intentional randomizations that can be cost-effectively realized by making use of mask-free additive manufacturing techniques. The PUF was integrated under the ground plane of a 5.8 GHz ISM band patch antenna and employed multiple I/O expander IC packages with randomized interconnect states to obtain a bit sequence to be utilized under PUF security scenarios. Analysis of the presented PUF with respect to various PUF metrics and against ML modeling attacks indicate that its performance approaches ideal values. The fabrication done through the presented additive manufacturing processes and the successful experimental verifications of the IOE-PUF demonstrate that additive manufacturing of RF electronics can also play an important role in the future of wireless system security measures. Future work is likely to focus on alternative PUF realizations and integrations that will provide further response diversity and higher levels of security for wireless system designers. Specifically, for the IOE-PUF, alternate realizations can be made using different types, numbers, and/or configurations of I/O expander ICs. Additionally, different CRP mechanisms can also be created within the microcontroller aside from the one detailed in this manuscript. Most importantly, the presented additive manufacturing based PUF can pave the way for other novel digital domain PUFs that can be directly placed within antenna substrates and innovative antenna randomizations that can serve as RF fingerprints (such as in [13] and [14]). These may provide benefits in size miniaturization and offer more diverse sets of security mechanisms that can be employed by the hardware and system designers.

REFERENCES

[1] M. N. I. Khan and S. Ghosh, "Comprehensive study of security and privacy of emerging non-volatile memories," *J. Low Power Electron. Appl.*, vol. 11, no. 4, p. 36, Sep. 2021, doi: 10.3390/jlpea11040036.

[2] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.

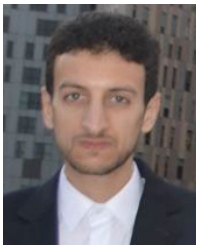
[3] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, "A PUF taxonomy," *Appl. Phys. Rev.*, vol. 6, no. 1, Mar. 2019, Art. no. 011303, doi: 10.1063/1.5079407.

[4] I. Verbauwhede and R. Maes, "Physically unclonable functions: Manufacturing variability as an unclonable device identifier," in *Proc. 21st Great Lakes Symp.*, May 2011, pp. 455–460.
[5] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Conf. Design Autom.*, San Diego, CA, USA, Aug. 2007, pp. 9–14.
[6] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Proc. EUROCRYPT*, 2004, pp. 523–540.
[7] T. W. Kim, B. D. Choi, and D. K. Kim, "Zero bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process," *Electron. Lett.*, vol. 50, no. 12, pp. 876–877, Jun. 2014, doi: 10.1049/el.2013.3474.
[8] D. Jeon, J. H. Baek, D. K. Kim, and B.-D. Choi, "Towards zero bit-error-rate physical unclonable function: Mismatch-based vs. physical-based approaches in standard CMOS technology," in *Proc. Euromicro Conf. Digit. Syst. Design*, Madeira, Portugal, Aug. 2015, pp. 407–414, doi: 10.1109/DSD.2015.57.
[9] U. Rührmair and J. Sölter, "PUF modeling attacks: An introduction and overview," in *Proc. Design, Autom. Test Eur. Conf. Exhib. (DATE)*, Mar. 2014, pp. 1–6, doi: 10.7873/DATE.2014.361.
[10] M. Kacar, T. M. Weller, and G. Mumcu, "3D printed wideband multilayered dual-polarized stacked patch antenna with integrated MMIC switch," *IEEE Open J. Antennas Propag.*, vol. 2, pp. 38–48, 2021, doi: 10.1109/OJAP.2020.3041959.
[11] M. Kacar, J. Wang, G. Mumcu, C. Perkowski, K. Church, B.-I. Wu, and T. Weller, "Phased array antenna element with embedded cavity and MMIC using direct digital manufacturing," in *Proc. IEEE Int. Symp. Antennas Propag. USNC-URSI Radio Sci. Meeting*, Atlanta, GA, USA, Jul. 2019, pp. 81–82, doi: 10.1109/APUSNCURSINRSM.2019.8888323.
[12] R. Liu, J. Braun, G. Mitchell, J. Wang, and G. Mumcu, "Packaging of a beamforming IC by laser enhanced direct print additive manufacturing (LE-DPAM)," in *Proc. 3rd URSI Atlantic Asia–Pacific Radio Sci. Meeting (AT-AP-RASC)*, Gran Canaria, Spain, May 2022, pp. 1–3, doi: 10.23919/AT-AP-RASC54737.2022.9814384.
[13] J. McMillen, G. Mumcu, and Y. Yilmaz, "Deep learning-based RF fingerprint authentication with chaotic antenna arrays," in *Proc. IEEE Wireless Microw. Technol. Conf. (WAMICON)*, Melbourne, FL, USA, Apr. 2023, pp. 121–124, doi: 10.1109/WAMICON57636.2023.10124899.
[14] J. O. McMillen, F. Abdul Razak, G. Mumcu, and Y. Yilmaz, "Hardware and deep learning-based authentication through enhanced RF fingerprints of 3D-printed chaotic antenna arrays," *IEEE Access*, vol. 13, pp. 6893–6908, 2025, doi: 10.1109/ACCESS.2025.3526583.
[15] T. Ranstrom, H. Arslan, and G. Mumcu, "Physical layer security using chaotic antenna arrays in point-to-point wireless communications," in *Proc. IEEE Wireless Microw. Technol. Conf. (WAMICON)*, Clearwater, FL, USA, Apr. 2024, pp. 1–4, doi: 10.1109/WAMICON60123.2024.10522807.
[16] K. H. Church, N. B. Crane, P. I. Deffenbaugh, T. P. Ketterl, C. G. Neff, P. B. Nesbitt, J. T. Nussbaum, C. Perkowski, H. Tsang, J. Castro, J. Wang, and T. M. Weller, "Multimaterial and multilayer direct digital manufacturing of 3-D structural microwave electronics," *Proc. IEEE*, vol. 105, no. 4, pp. 688–701, Apr. 2017, doi: 10.1109/JPROC.2017.2653178.
[17] A. Maiti, V. Gunreddy, and P. Schaumont, "A systematic method to evaluate and compare the performance of physical unclonable functions," in *Proc. Embedded Syst. Design FPGAs*, 2012, pp. 245–267.
[18] C. A. Balanis, "Microstrip and mobile communications antennas," in *Antenna Theory Analysis and Design*, 4th ed., Hoboken, NJ, USA: Wiley, pp. 783–861.
[19] M. Kacar, C. Perkowski, P. Deffenbaugh, J. Booth, G. Mumcu, and T. Weller, "Wideband Ku-band antennas using multi-layer direct digital manufacturing," in *Proc. IEEE Int. Symp. Antennas Propag. USNC/URSI Nat. Radio Sci. Meeting*, San Diego, CA, USA, Jul. 2017, pp. 1243–1244, doi: 10.1109/APUSNCURSINRSM.2017.8072664.
[20] R. Murphy, "Packaging of active RF beamforming IC utilizing additive manufacturing," M.S. thesis, Dept. Elect. Eng., University of South Florida, Tampa, FL, USA, 2021. [Online]. Available: https://digitalcommons.usf.edu/etd/9601/
[21] T. P. Ketterl, Y. Vega, N. C. Arnal, J. W. I. Stratton, E. A. Rojas-Nastrucci, M. F. Córdoba-Erazo, M. M. Abdin, C. W. Perkowski, P. I. Deffenbaugh, K. H. Church, and T. M. Weller, "A 2.45 GHz phased array antenna unit cell fabricated using 3-D multi-layer direct digital manufacturing," *IEEE Trans. Microw. Theory Techn.*, vol. 63, no. 12, pp. 4382–4394, Dec. 2015, doi: 10.1109/TMTT.2015.2496180.
[22] M. Kacar, T. Weller, and G. Mumcu, "Conductivity improvement of microdispensed microstrip lines and grounded coplanar waveguides using laser micromachining," *IEEE Trans. Compon., Packag., Manuf. Technol.*, vol. 10, no. 12, pp. 2129–2132, Dec. 2020, doi: 10.1109/TCPMT.2020.3038332.
[23] Y. Wang, C. Wang, C. Gu, Y. Cui, M. O'Neill, and W. Liu, "A generic dynamic responding mechanism and secure authentication protocol for strong PUFs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 30, no. 9, pp. 1256–1268, Sep. 2022.
[24] R. Zhang, H. Zhang, X. Wang, Y. Ziyang, K. Liu, S. Nishizawa, K. Niitsu, and H. Shinohara, "De-correlation and de-bias post-processing circuits for true random number generator," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 11, pp. 5187–5199, Nov. 2024, doi: 10.1109/TCSI.2024.3421663.
[25] R. Zhang, X. Wang, and H. Shinohara, "Energy-efficient post-processing technique having high extraction efficiency for true random number generators," *IEICE Trans. Electron.*, pp. 300–308, Jul. 2021, doi: 10.1587/transele.2020cdp0006.
[26] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Dept. U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST SP 800-22, 2001.
[27] N. N. Anandakumar, M. S. Hashmi, and M. A. Chaudhary, "Implementation of efficient XOR arbiter PUF on FPGA with enhanced uniqueness and security," *IEEE Access*, vol. 10, pp. 129832–129842, 2022, doi: 10.1109/ACCESS.2022.3228635.
[28] M. Thirumoorthi, M. Jovanovic, M. Mirhassani, and M. Khalid, "Design and evaluation of a hybrid chaotic-bistable ring PUF," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 29, no. 11, pp. 1912–1921, Nov. 2021, doi: 10.1109/TVLSI.2021.3111588.
[29] D. Deng, S. Hou, Z. Wang, and Y. Guo, "Configurable ring oscillator PUF using hybrid logic gates," *IEEE Access*, vol. 8, pp. 161427–161437, 2020, doi: 10.1109/ACCESS.2020.3021205.
[30] A. Venkatesh, A. B. Venkatasubramaniyan, X. Xi, and A. Sanyal, "0.3 pJ/Bit machine learning resistant strong PUF using subthreshold voltage divider array," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 8, pp. 1394–1398, Aug. 2020, doi: 10.1109/TCSII.2019.2943121.
[31] A. Aysu, N. F. Ghalaty, Z. Franklin, M. P. Yali, and P. Schaumont, "Digital fingerprints for low-cost platforms using MEMS sensors," in *Proc. Workshop Embedded Syst. Secur.*, Sep. 2013, pp. 1–6, doi: 10.1145/2527317.2527319.
[32] Y. Cao, A. J. Robson, A. Alharbi, J. Roberts, C. S. Woodhead, Y. J. Noori, R. Bernardo-Gavito, D. Shahrjerdi, U. Roedig, V. I. Fal'ko, and R. J. Young, "Optical identification using imperfections in 2D materials," *2D Mater.*, vol. 4, no. 4, Sep. 2017, Art. no. 045021, doi: 10.1088/2053-1583/aa8b4d.
[33] J. Guajardo, B. Škorić, P. Tuyls, S. S. Kumar, T. Bel, A. H. M. Blom, and G.-J. Schrijen, "Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions," *Inf. Syst. Frontiers*, vol. 11, no. 1, pp. 19–41, Mar. 2009, doi: 10.1007/s10796-008-9142-z.
[34] Z. Wang, H. Wang, P. Wang, and Y. Shao, "Robust optical physical unclonable function based on total internal reflection for portable authentication," *ACS Appl. Mater. Interfaces*, vol. 16, no. 21, pp. 27926–27935, May 2024, doi: 10.1021/acsami.4c03283.
[35] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. 17th ACM Conf. Comput. Commun. Secur.*, Oct. 2010, pp. 237–249.
[36] F. Ganji, D. Forte, and J.-P. Seifert, "PUFmeter a property testing tool for assessing the robustness of physically unclonable functions to machine learning attacks," *IEEE Access*, vol. 7, pp. 122513–122521, 2019.
[37] K. T. Mursi, B. Thapaliya, Y. Zhuang, A. O. Aseeri, and M. S. Alkatheiri, "A fast deep learning method for security vulnerability study of XOR PUFs," *Electronics*, vol. 9, no. 10, p. 1715, Oct. 2020.
[38] P. Santikellur, A. Bhattacharyay, and R. S. Chakraborty, "Deep learning based model building attacks on arbiter PUF compositions," *Cryptol. ePrint Arch.*, vol. 2019, p. 566, Oct. 2019.
[39] D. P. Sahoo, D. Mukhopadhyay, R. S. Chakraborty, and P. H. Nguyen, "A multiplexer-based arbiter PUF composition with enhanced reliability and security," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 403–417, Mar. 2018.
[40] U. Rührmair, J. Sölter, and F. Sehnke, "On the foundations of physical unclonable function," *Cryptol. ePrint Arch.*, vol. 2009, p. 277, Jun. 2009.

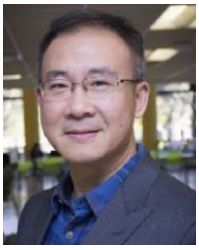
AARON PENDINO (Member, IEEE) received the B.S. degree in electrical engineering from the University of South Florida, Tampa, FL, USA, in 2023. He is currently a Graduate Research Assistant with the Department of Electrical Engineering, University of South Florida. His research interests include additive manufacturing of physically unclonable functions and integration of physically unclonable functions with wireless systems for improved security.

NGHIA NGUYEN (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from the HCMC University of Technology, Ho Chi Minh, Vietnam, in 2019, and the M.S. degree in electrical engineering from the University of South Florida, Tampa, FL, USA, in 2024.

He is currently a Graduate Research Assistant with the Department of Electrical Engineering, University of South Florida. His research interests include hardware and deep learning-based authentication, physically unclonable functions, and anomaly detection.



SAIF E. NOUMA (Graduate Student Member, IEEE) received the Bachelor of Engineering degree from the École Polytechnique de Tunisie, Tunisia, in 2020. He is currently pursuing the Ph.D. degree with the Bellini College of Artificial Intelligence, Cybersecurity, and Computing, University of South Florida. His research interests include lightweight and post-quantum cryptography tailored for the Internet of Things (IoT) and digital twins.



JING WANG (Senior Member, IEEE) received the dual B.S. degree in mechanical engineering and electrical engineering from Tsinghua University, Beijing, China, in 1999, and the dual M.S. degree in electrical engineering and mechanical engineering and the Ph.D. degree from the University of Michigan, Ann Arbor, MI, USA, in 2002 and 2006, respectively.

He is currently a Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. He has authored or co-authored more than 200 peer-reviewed articles and holds 11 U.S. patents. His research work has been funded by federal agencies [National Science Foundation (NSF), Defense Threat Reduction Agency (DTRA), U.S. Army, and U.S. Air Force] and many companies totaling over $20 M. His current research interests include RF additive manufacturing for structural electronics and packaging, RF/microwave/millimeter-wave circuits, phased antennas, and systems, monolithic microwave integrated circuits (MMICs), micromachined transducers, RF/bio-MEMS, wireless sensors, and functional nanomaterials.

Dr. Wang was a recipient of the 2024 and 2018 Faculty Outstanding Research Achievement Award and the 2022 Excellence in Innovation Award at the University of South Florida.

ATTILA A. YAVUZ (Senior Member, IEEE) received the M.S. degree in computer science from Boğaziçi University, Istanbul, Türkiye, in 2006, and the Ph.D. degree in computer science from North Carolina State University, in 2011. He was an Assistant Professor with the School of Electrical Engineering and Computer Science, Oregon State University, from 2014 to 2018, and the Department of Computer Science and Engineering, University of South Florida (USF), from 2018 to June 2021. He was a member of the Security and Privacy Research Group, Robert Bosch Research and Technology Center North America, from 2011 to 2014. He is currently an Associate Professor with the Bellini College of Artificial Intelligence, Cybersecurity, and Computing, USF, the Director of the Applied Cryptography Research Laboratory, and the Co-Director of the Center of Cryptologic Research, USF. He is broadly interested in the design, analysis, and application of cryptographic tools and protocols to enhance the security of computer systems. He was a recipient of the NSF CAREER Award, the Cisco Research Award (thrice), unrestricted research gifts from Robert Bosch (five times), the USF Faculty Outstanding Research Achievement Award, the USF Excellence in Innovation Award, and the USF College of Engineering's Outstanding Research Achievement Award. He has authored more than 110 products, including research articles in top conferences, journals, and patents. His work resulted in technology transfers (e.g., intra-vehicular network, searchable encryption) positively impacting tens of millions of users across the world.

YASIN YILMAZ (Senior Member, IEEE) received the B.S. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Türkiye, in 2008, the M.S. degree in electrical and computer engineering from Koc University, Istanbul, Türkiye, in 2010, and the Ph.D. degree in electrical engineering from Columbia University, New York, NY, USA, in 2014.

He is currently an Associate Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. His research interests include machine learning, statistical signal processing, and their applications in computer vision, cybersecurity, biomedical, energy, transportation, communication, environmental, and socioeconomic systems. His awards and honors include the Highly Ranked Scholar by ScholarGPS, Top 2% most cited scientist globally by Stanford University, the Best Paper Award at the 2023 IEEE Conference on Dependable and Secure Computing, and the 2023 Outstanding Research Achievement Award from the University of South Florida. He has been serving as a Topic Editor for *Frontiers in Robotics and AI* and an Editorial Board Member for *Discover Data* (Springer-Nature). He was the Technical Chair of Signal Processing and Machine Learning for Social Good Symposium at IEEE GlobalSIP 2019 and the Vice Chair of the Special Interest Group on AI Embedded Cognitive Networks, Technical Committee on Cognitive Networks, IEEE Communications Society.

GÖKHAN MUMCU (Senior Member, IEEE) received the B.S. degree in electrical engineering from Bilkent University, Ankara, Türkiye, in 2003, and the M.S. and Ph.D. degrees in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2005 and 2008, respectively.

He is currently a Professor with the Electrical Engineering Department, University of South Florida, Tampa, FL, USA. His research interests include reconfigurable antennas and RF circuits with their mm-wave applications, additive manufacturing of structural antennas and phased array antennas with integrated RF electronics, microfluidics for highly reconfigurable RF devices, and new concepts (e.g., metamaterials, volumetric 3-D reactive loading, polymers) for designing conformal, miniature, and multifunctional antennas. He was a recipient of the 2014 CAREER Award from the U.S. National Science Foundation, the 2014 and 2024 Faculty Outstanding Research Awards from the University of South Florida, and the 2008 Outstanding Dissertation Award of The Ohio State University, ElectroScience Laboratory. He was a recipient of the 1999 International Education Fellowship of Turkish Ministry of Education. He ranked first in the national university entrance exam taken annually by over 1.5 million Turkish students in 1999. He served as the Technical Program Committee Chair of the 2013 IEEE International Symposium on Antennas and Propagation and USNC/URSI National Radio Science Meeting, the 2016 and 2025 International Workshop on Antenna Technology, and the 2022 IEEE Wireless and Microwave Technology Conference (WAMICON). In addition, he served as the Vice and General Chair for IEEE WAMICON in 2023 and 2024, respectively.