

A Reinforcement-Learning-Assisted Power Amplifier for RF Fingerprint Generation in 65 nm CMOS

Jiachen Xu[✉], Yuyi Shen[✉], Junting Deng[✉], Ethan Chen[✉], and Vanessa Chen[✉], *Senior Member, IEEE*

Abstract—A reconfigurable power amplifier (PA) is implemented in CMOS 65nm to enable radio identification for secure wireless communication by injecting tunable radio frequency fingerprints (RFFs) into the physical layer. The large ensemble of RFFs is achieved by offsetting the distributions of process variations affecting the PA's hardware features. The resulting large RFF capacity is exploited to increase resilience to noise and temperature changes by selecting distinct RFFs from the ensemble and reconfiguring the PA to restore nominal RFFs following temperature shifts. The secure PA achieves over 14000 time-varying RFFs while consuming only 22 mW and occupying a core area of $<0.0951 \text{ mm}^2$. A reinforcement learning (RL)-based control has been implemented on FPGA for closed-loop reconfiguration of the transmitter to achieve robust and low-overhead security measures that overcome noise and temperature influences in dynamic environments.

Index Terms—Wireless device authentication, power amplifier, IoT, hardware security, reinforcement learning, energy efficient, RF fingerprint.

I. INTRODUCTION

THE commonality of resource-constrained IoT devices has spurred the investigation of low-overhead physical (PHY) layer authentication mechanisms [1]. These largely consist of schemes based on extracting RF fingerprints (RFFs) from the wireless channel [2], [3] and transmitter-specific hardware features [4], [5]. The RFFs intrinsic to transmitters can be susceptible to low reliability and can exhibit limited distinguishability [6]. Attackers may also observe and spoof intrinsic transmitter RFFs to overcome the authentication. This has motivated the integration of tuneability into RF fingerprinting-based authentication systems for mitigating these disadvantages [6], [7], [8].

To prevent an attacker from cloning a significant portion of the RFF configuration space in a tunable RFF scheme, individual radio transmitters need to be able to inject a great many more distinguishable RF fingerprints into the wireless

physical layer to enable time-varying RF fingerprint-based authentication, as illustrated in Fig. 1. The sequence of RF fingerprints can be synchronized during the handshake process to avoid having to exchange it online. Frequently switching the RF fingerprint embedded in the transmitted signal makes it unpredictable for an attacker to observe-and-spoof. However, tunable RF fingerprint schemes in the literature have only demonstrated a limited search space of RFFs. Furthermore, the impact of environmental changes such as temperature shifts on these tunable RF fingerprint schemes has not been sufficiently investigated [6], [7], [8].

The limited range of prior tunable RF fingerprint schemes is still vulnerable to interception by adversary receivers using a prolonged observation time to mimic transmitted signals [9]. Tunable RF fingerprint schemes by themselves also remain vulnerable to the impact of temperature variations on the transmitter impairments they rely on for authentication decisions [10]. Many semiconductor device parameters exhibit a significant temperature coefficient that directly impacts upon transmitter behavior, resulting in RFFs exhibiting temperature dependency [11], [12]. The key challenges faced by tunable RFF-based authentication schemes can be summarized as follows: individual devices need to support a very wide range of RFFs to counter spoofing attacks and the consistency of the generated RFFs is degraded by circuit sensitivity to environmental changes. The methodology for compensating the effects of a time-varying operating environment is strongly dependent on the system characteristics. Previous study has shown that the thermal coefficient of a transmitter's crystal oscillator may be compensated using a simple calibration in the phase-locked loop (PLL) for the frequency offset across temperature [13]. However, more complex systems, such as the PA of a wireless transmitter often require complex online estimation/compensation methods [14], [15] to effectively manage and compensate for environmental variations.

To further address these issues, this work presents a solution to achieve a significantly larger RF fingerprint capacity on an RF power amplifier by skewing the distributions of intrinsic process variations of CMOS circuits and exploiting the search space in electromagnetic (EM) domain. The proposed PA was manufactured in 65nm CMOS targeting 6 GHz to generate over 14,000 RF fingerprints. A reinforcement learning (RL)-based PA controller is implemented on FPGA to automatically characterize the PA's high-dimensional tunable parameters and control the PA for restoring the RF fingerprints across temperature variations in order to achieve reliable identification in dynamic environments.

Manuscript received 28 October 2023; revised 23 December 2023 and 22 March 2024; accepted 14 April 2024. Date of publication 30 April 2024; date of current version 28 June 2024. This work was supported in part by the National Science Foundation under Grant 1952907, Grant 1953801, and Grant 2028893; and in part by Army Research Office under Award W911NF-23-1-0073. This article was recommended by Associate Editor X. Zhu. (Corresponding author: Jiachen Xu.)

The authors are with the Electrical and Computer Engineering Department, Carnegie Mellon University, Pittsburgh, PA 15213 USA (e-mail: jxu3@andrew.cmu.edu; yuyis1@andrew.cmu.edu; juntungd@andrew.cmu.edu; ethanchen@cmu.edu; vanessachen@cmu.edu).

Color versions of one or more figures in this article are available at <https://doi.org/10.1109/TCSI.2024.3390694>.

Digital Object Identifier 10.1109/TCSI.2024.3390694

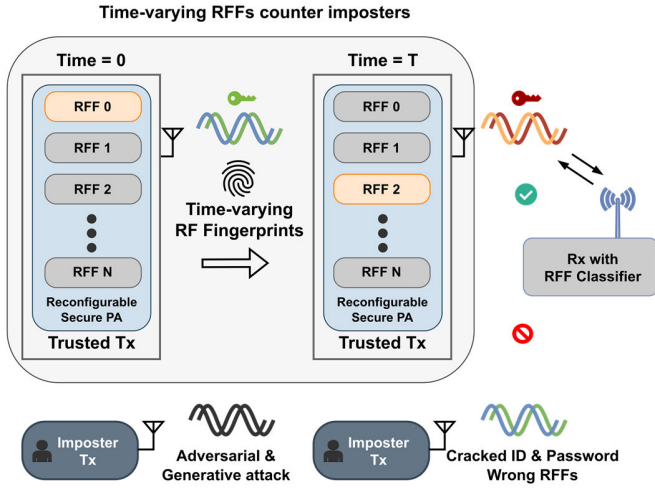


Fig. 1. Overview of authenticating radio devices using RF fingerprints. Only devices with correct time-varying RF fingerprints will be authenticated by the classifier on the receiver.

The remainder of this paper is organized as follows. Section II introduces the system architecture and reconfigurable combinatorial PA architecture. Section III presents the measurement results of the fabricated PAs with temperature variations. The classification results for determining the RFF capacity of the device equipped with the proposed PA are presented in section IV. Section V discusses the RL controller for restoring distorted RF fingerprints from temperature variations with an FPGA implementation. Section VI concludes the paper.

II. TIME-VARYING RF FINGERPRINTS WITH RECONFIGURABLE POWER AMPLIFIER

A. System Overview

Having a large ensemble of RFFs on the transmitter expands the capacity of the time-varying scheme to improve the security. It also enables the improvement of the scheme's noise resilience by dropping indistinct fingerprints from the ensemble to reduce RFF feature overlaps while maintaining most of the intrinsic RF fingerprint capacity. This process is illustrated in the middle of Fig. 2. Furthermore, CMOS circuits exhibit significant temperature dependencies that may distort the original fingerprint as the temperature of the device environment changes, as shown in the bottom of Fig. 2. To achieve system resilience against these temperature coefficients, alternative PA configurations are extracted from the large ensemble and substituted in to restore the nominal RF fingerprints. This work proposes a reinforcement learning controller for automatically characterizing the PA and adjusting the PA configuration for overcoming such environmental variations. The system diagram for such a transmitter equipped with the reconfigurable PA and RL controller for reliable time-varying RF fingerprints is shown in Fig. 3. The rest of the paper introduces the components of the system in detail.

B. Reconfigurable PA

The Wi-Fi 6E specification takes advantage of the first new spectrum granted for Wi-Fi in the U.S. since Wi-Fi 3 to

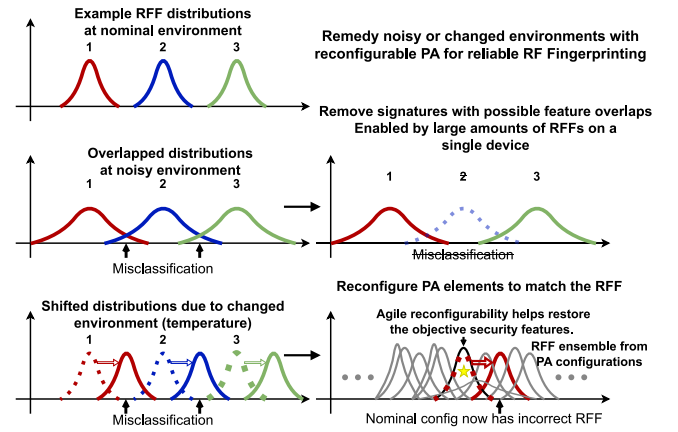


Fig. 2. The methods proposed for counteracting the effects of noise and temperature variations on an ensemble of RF fingerprints are visualized using example RFF distributions.

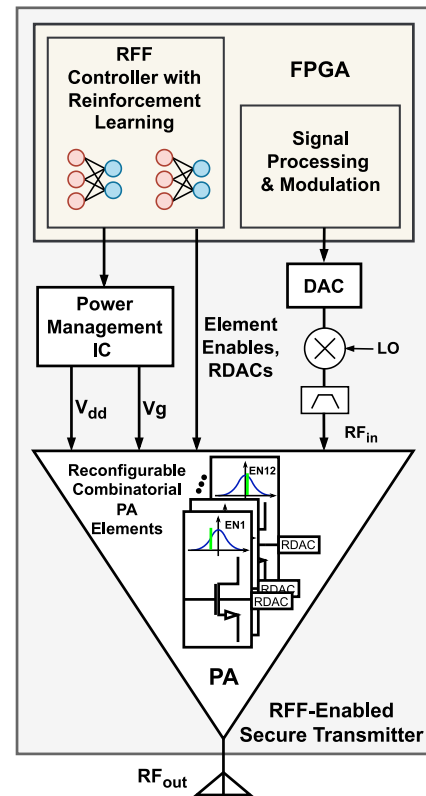


Fig. 3. System diagram of the proposed transmitter. The PA is reconfigurable to produce large numbers of RF fingerprints on transmitter for time-varying RFF identification. The RF fingerprint controller on FPGA uses reinforcement learning to control the PA and counteract environmental variations.

deliver enhanced performance using the uncongested, lower noise environment of the 6 GHz band [16]. The Very Low Power access class of this specification enables indoor/outdoor operation without imposing significant interference using low transmit PSD limits. The reconfigurable 6-GHz PA designed in 65 nm CMOS for this work targets this resource-constrained application using a PSD limit of -8 dBm/MHz, which specifies a maximum transmit power of 5 dBm for a typical 20 MHz Wi-Fi channel [16]. To achieve a greatly enlarged RF fingerprint search space, the circuit design builds on prior work

that relies on combinatorial randomness for achieving RF fingerprint tunability [8]. By itself, this method requires the slicing of the differential pair of the PA output stage into small-size selectable elements, resulting in greater individual element-level process variation that may be combinatorially selected to yield a greatly variable composite RF fingerprint [17]. The direct approach to enhancing the tuning range of this method is to introduce non-uniform sizing of each selectable element, but this introduces significant layout complications for the output stage transistor of a PA [18]. This work instead extends the concept of the multi-gate transistor linearization technique by retaining evenly sized selectable elements and modifying element-level operating points with body bias DACs for achieving a similar expansion effect on the RFF tuning range [7]. The set of control vectors for the body bias DACs is chosen to result in an approximately constant overall quiescent current for the output stage as the PA is configured between them. This prevents drastic changes in PA performance as the body bias offsets applied to individual slices are varied to sweep the RF fingerprint. Meanwhile, the power supply and gate bias are made configurable to maximize the PA fingerprint capacity. With a large number of RFFs, indistinct fingerprints can be removed to enable greater noise resilience. Furthermore, it provides a large state space that significantly increases the successful rate for the reinforcement learning controller to enable temperature-resilient configurations to counter environmental changes.

As depicted in Fig. 4, the structure of the PA is composed of off-chip matching networks, a driver stage, and the reconfigurable output stage for achieving variable and resilient RFFs. The driver stage is a linear Class-A biased differential pair with cascoded transistors and feeds into the configurable differential pair of the output stage with a shunt inductor for inter-stage matching. Neutralization capacitors are used to reduce the C_{gd} of the large input pair for improving driver stage gain. The output stage's differential pair is nominally biased in Class-B/deep AB with constant voltage bias and divided into 12 parallel device pairs with enable switches. Linear Class-A and Class-B/deep AB bias are chosen to avoid introducing significant intercarrier interference into the OFDM Wi-Fi signal [19]. Each device pair is laid out inside a separate deep n-well to allow individualized forward body bias operation with a 3-bit resolution resistive DAC (RDAC). 9 device pairs are enabled at a time during amplifier operation for a target power specification of 5 dBm, yielding a measured 4.5 dBm of power at room temperature with body bias DACs disabled and a nominal supply voltage of 1.2 V. Selecting 9 device pairs from 12 available elements at a time allows the PA output stage to be reconfigured between 220 possible combinations of device pair mismatch, yielding a large baseline capacity of RFFs that can be further expanded upon with skewed body bias. Furthermore, the resultant output power reduction from sacrificing 3 device pairs for implementing this form of RF fingerprint tunability is kept to 1.8 dB relative to enabling all 12 device pairs.

The schematics of the off-chip matching networks are shown in Fig. 5 with transmission line dimensions. In the input microstrip network, the interdigital microstrip capacitor,

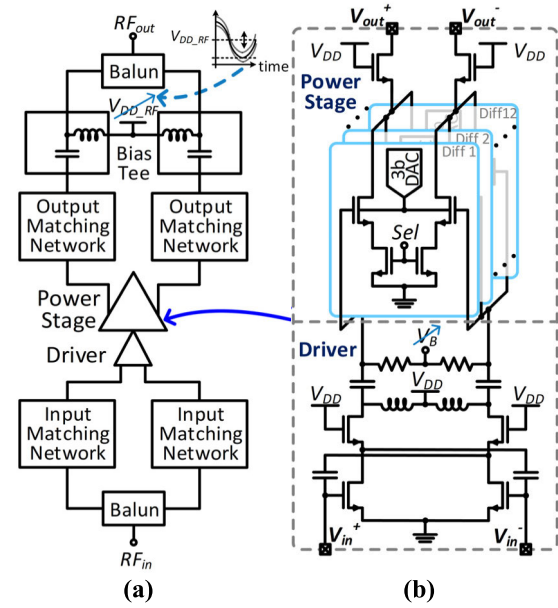


Fig. 4. The schematic of the reconfigurable 6-GHz PA is shown with the arrangement of off-chip components (a) and the on-chip design (b).

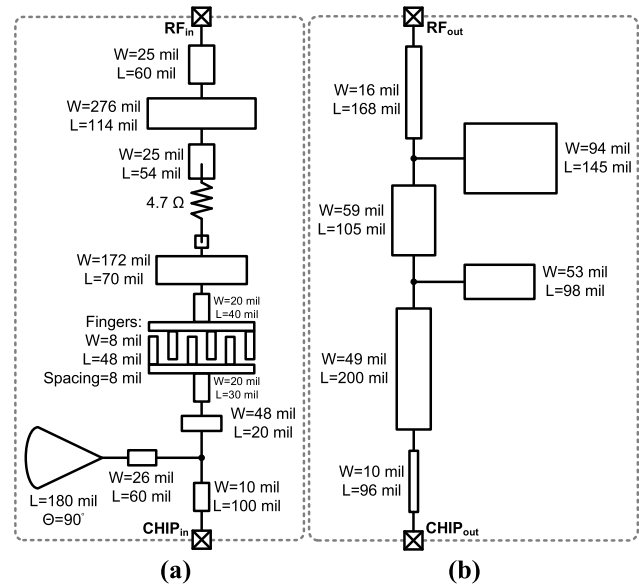


Fig. 5. The dimensions and schematics of the reconfigurable PA's off-chip input matching network (a) and output matching network (b) on one side of the differential PA are shown.

short-line segment, and short-circuited stub near the connection to the chip are sized to compensate the impact of the input-side bondwire, with the radial stub serving as a short circuit. The remainder of the elements are dimensioned to achieve matching to the 50 Ohm system impedance. As for the output-side microstrip network, the uppermost open-circuited stub in Fig. 5b is sized to yield a short-circuit at the second harmonic for enabling control of the first and second harmonic loading impedances at the output stage transistor drain. The remainder of the lines in the output-side microstrip network are sized for providing a power match to the output stage transistor at the operating frequency and a short at the second harmonic.

C. PA Fingerprint Analysis

The hardware features injected by the PA into the transmitter RFF are a function of the composite response of each selected device pair in the output stage and can be analyzed through the impact of global and local reconfiguration on the AM/AM response of the amplifier. In the passband, a weakly nonlinear PA can be modeled as a memoryless polynomial [20] whose coefficients determine the hardware features imprinted by the PA on the input signal. To determine the overall RF fingerprint response of the PA, we examine the impact of reconfiguration at the level of one side of an individual selectable device pair.

Neglecting dependencies on drain voltage, the drain current $i_d(\theta)$ of a MOSFET fed with a sinusoidal input exhibits a nonlinear dependence on the conduction angle α and is proportional to the peak drain current I_{MAX} [21]. The conduction angle α itself is dependent on input amplitude A_{in} , MOSFET threshold voltage V_{TH} , and bias voltage V_B . Furthermore, peak drain current I_{MAX} is linearly proportional to input amplitude A_{in} and $I_{MAX,ideal}$, the maximum drain current supported by the MOSFET. These dependencies are summed up below, with V_{DD} denoting supply voltage.

$$i_d(\theta) = I_{MAX}(\cos \theta - \cos(\alpha/2))/(1 - \cos(\alpha/2)) \quad (1)$$

$$\alpha = 2 \cos^{-1}((V_{TH} - V_B)/A_{in}) \quad (2)$$

$$I_{MAX} = I_{MAX,ideal}(V_B + A_{in} - V_{TH})/(V_{DD} - V_{TH}) \quad (3)$$

To widen the range of available RFFs, the PA operating point is shifted globally by modifying V_{DD} and bias voltage V_B in addition to changing the selection of device pairs and body bias DAC settings at the local level. V_{DD} shifts impact the drain voltage waveform and the peak drain current I_{MAX} , while shifts in bias voltage propagate to I_{MAX} and the MOSFET conduction angle. Notably, a change of ΔV_{DD} from the original $V_{DD,old}$ affects I_{MAX} through the maximum supported drain current $I_{MAX,ideal}$ by $\Delta I_{MAX,ideal}$ in addition to the denominator term of (3):

$$\Delta I_{MAX,ideal} = (I_{MAX,ideal} \Delta V_{DD}) / (V_{DD,old} - V_{TH}) \quad (4)$$

At the element level, modifying body bias levels systematically shifts V_{TH} and thus $I_{MAX,ideal}$. The impact of a V_{TH} shift on $I_{MAX,ideal}$ can be approximated assuming a linear device characteristic [22], leading to the following expression for the new value of the maximum supported drain current:

$$I_{MAX,ideal,new} = \frac{I_{MAX,ideal}(V_{DD} - V_{TH,new})}{V_{DD} - V_{TH,old}} \quad (5)$$

The effects of systematic shifts in these element-level and global operating points in the reconfigurable PA's output stage are illustrated in Fig. 6. The overall characteristic of the output stage on one side of the differential pair can then be written as follows by summing over 9 selected device pairs using function notation for denoting the global and local (subscripted) dependencies of conduction angle α ($\Delta V_{TH,i}$, ΔV_B), peak drain current I_{MAX} ($\Delta V_{TH,i}$, ΔV_B), and MOSFET knee voltage V_K ($\Delta V_{TH,i}$, ΔV_B):

$$I_{dtot}(\theta) = \sum_{i=1}^{N=9} D_i(\theta) K_i (\cos \theta - \cos(\frac{1}{2}\alpha(\Delta V_{TH,i}, \Delta V_B))) \quad (6)$$

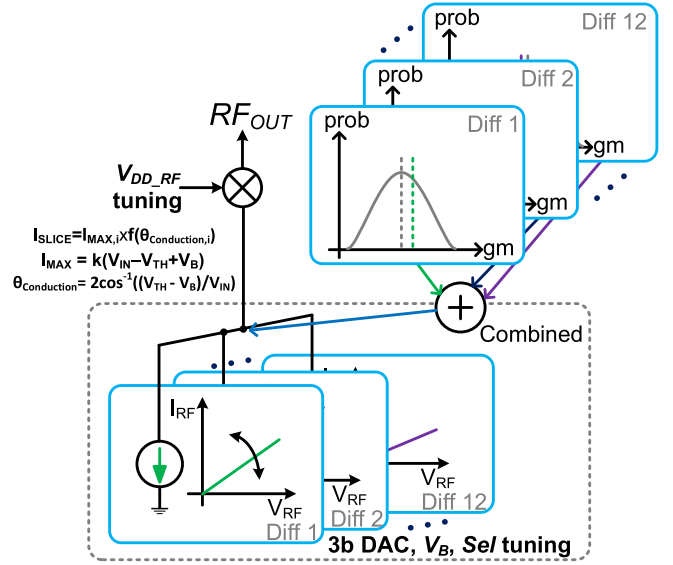


Fig. 6. Intentional offsets applied to each slice of the output stage differential pair, and global control of output stage quiescent voltage V_B and supply voltage are used to maximize the PA's fingerprint capacity.

$$K_i$$

$$= I_{MAX} (\Delta V_{TH,i}, \Delta V_B) / [1 - \cos(\frac{1}{2}\alpha(\Delta V_{TH,i}, \Delta V_B))] \quad (7)$$

$$D_i(\theta)$$

$$= 1 - \exp(-V_D(\theta)/V_K(\Delta V_{TH,i}, \Delta V_B)) \quad (8)$$

$$V_D(\theta)$$

$$= V_{DD} + \Delta V_{DD} - I_{dtot}(\theta) R_{OPT} \cos(\theta) \quad (9)$$

Here, the $D_i(\theta)$ term adds back in the dependency of element-level MOSFET drain current on the shared drain voltage $V_D(\theta)$ of the output stage's selected elements, while K_i factors in the scaling of each selected device pair's peak drain current through the global and element-level systematic offsets. $V_D(\theta)$ is simply modeled by assuming all harmonics are shorted with the only time-varying component being the fundamental frequency sinusoid $-I_{dtot}(\theta) R_{OPT} \cos(\theta)$. $I_{dtot}(\theta)$ denotes the total drain current of all 9 selected output stage MOSFETs and R_{OPT} refers to the impedance seen by the output stage drain. R_{OPT} is set to the value required for power matching the output stage transistors under the nominal condition (no systematic offsets applied). The fundamental Fourier coefficient of $I_{dtot}(\theta)$ can then be used to compute the overall P_{out} vs. P_{in} output characteristic curve that defines the PA RF fingerprint response.

The variability that is achieved by this tunable RFF scheme can then be found by propagating the uncertainties associated with device mismatch to the output stage's overall response [23]. For simplicity, we consider V_{TH} and the current factor β with the following self-mismatch standard deviations [24]:

$$\sigma_{VT} = \frac{1}{\sqrt{2}} \frac{A_{VT0}}{\sqrt{WL}} \quad (10)$$

$$\sigma_{\beta} = \frac{1}{\sqrt{2}} \frac{\beta A_{\beta}}{\sqrt{WL}} \quad (11)$$

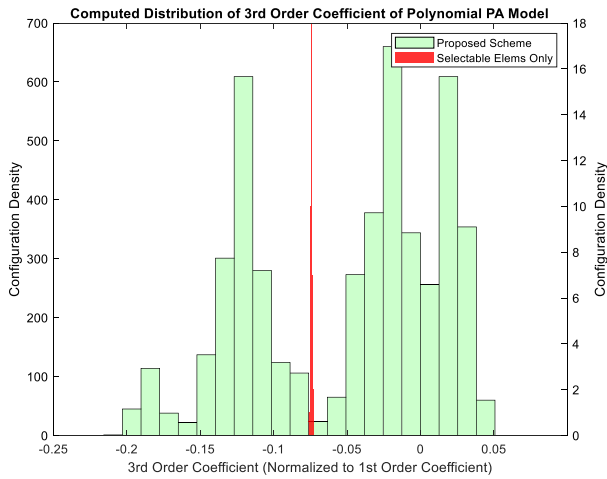


Fig. 7. The greatly expanded search space of hardware features provided by the proposed PA reconfigurability scheme is visualized using a 3rd order behavioral PA model fitted to the computed output stage characteristic.

The impact of the body effect on V_{TH} mismatch can be accounted for by characterizing the self-mismatch across body-bias DAC settings [25]. To determine the increase in fingerprint capacity afforded by the proposed reconfigurability scheme, we compare against the variability achieved in the absence of systematic offsets such as forward body bias voltages, V_{DD} , V_B by solely applying selectable element switching, corresponding to a previously proposed scheme for integrating tunability into the RFF injected by a PA [8]. If we consider the case of configuring the PA across $\pm 20\%$ variations in V_{DD} and V_B with a set of 8 possible pseudo-random control vectors for the body bias DACs in addition to the 220 available combinations of output stage slices, the proposed scheme results in a far greater variability in the PA hardware features. Compared to an approach that simply exploits intrinsic device variations through selecting differing combinations of output stage transistor slices, a much greater fingerprint capacity is achieved. This is illustrated in Fig. 7, wherein a 3rd-order polynomial model is fitted to the computed PA output characteristic distribution in order to plot the spread of the 3rd-order coefficient as a PA hardware feature. We further validate this analysis by conducting a post-layout Monte Carlo analysis of the corners of this scenario wherein Monte Carlo is run for 3 of the 8 possible DAC control vectors for $\pm 20\%$ variations in V_{DD} and V_B . Here, simulations are only conducted for $+20\%$ and -20% variation in both V_{DD} and V_B to cover the corner cases. The resultant distributions are plotted in Fig. 8, where it is seen that our proposed scheme provides a significant enhancement in the tuning range.

D. Temperature Sensitivity Analysis for PA RF Fingerprints

Owing to the temperature coefficients of parameters such as V_{TH} and transistor mobility μ , the fingerprint of the PA is systematically shifted by temperature changes in the device environment. Both transistor mobility and V_{TH} exhibit significant increases as the temperature decreases [11], [12]. Furthermore, drain current mismatch improves as temperature rises, with the extent of the improvement increasing significantly as the transistor bias approaches weak inversion. The primary contributor to this trend is current factor

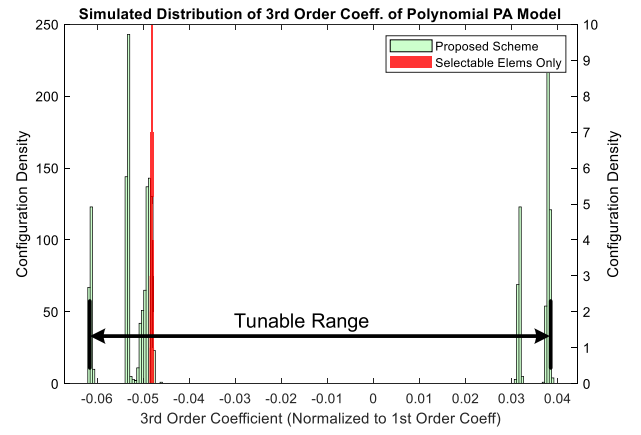


Fig. 8. The greatly expanded search space of hardware features is shown using post-layout Monte Carlo simulation using a small subset of the systematic offsets considered in Fig. 7's analysis.

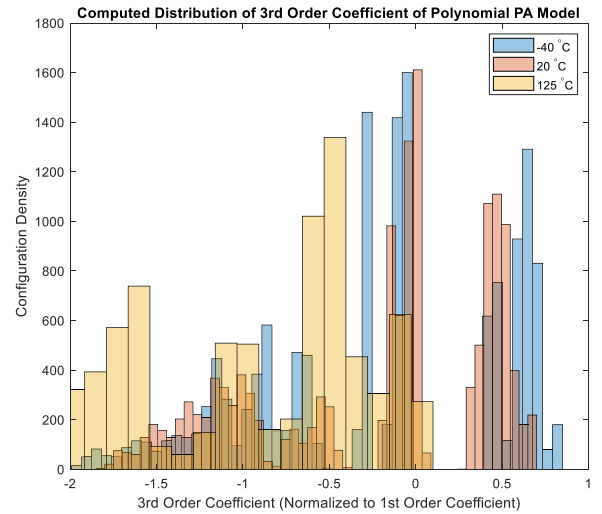


Fig. 9. A fitted 3rd order PA polynomial model's 3rd order coefficient is used to visualize the overlaps between the search space of RF fingerprints across temperature corners.

mismatch [26]. This effect causes temperature shifts to impact the variability achievable by the proposed reconfigurable RFF scheme, and thus the fingerprint capacity.

The overall impact of temperature shifts on the proposed reconfigurable RFF scheme can therefore be modeled by integrating the temperature dependencies of the Pelgrom coefficient A_β , V_{TH} and β into (1)-(4). We determine the ability of the proposed system to compensate for temperature changes in the environment by computing the fingerprint variability achieved across -40°C to 125°C for the same case as Fig. 7 and showing the overlap between the RFF distributions. This overlap is plainly seen in Fig. 9, demonstrating the capacity of the proposed scheme to restore nominal fingerprints following a temperature change. Post-layout Monte Carlo analysis for a single DAC control vector across $+20\%$ and -20% variation in both V_{DD} and V_B for covering the corner cases is used to validate the existence of the overlap in tuning range across temperatures, as shown in Fig. 10.

III. PA MEASUREMENT RESULTS

To demonstrate the proposed system, the 6-GHz PA was taped out in 65 nm CMOS and evaluated using Wi-Fi 6E SU

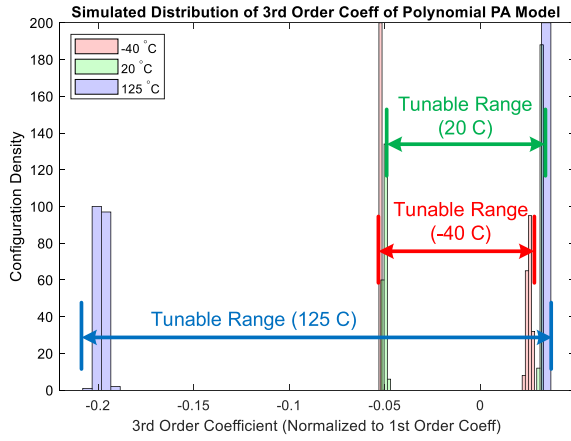


Fig. 10. Post-layout Monte Carlo analysis of a single body bias control vector across corners in supply and bias voltage variation is used to show the overlap in RF fingerprint tuning range across temperature.

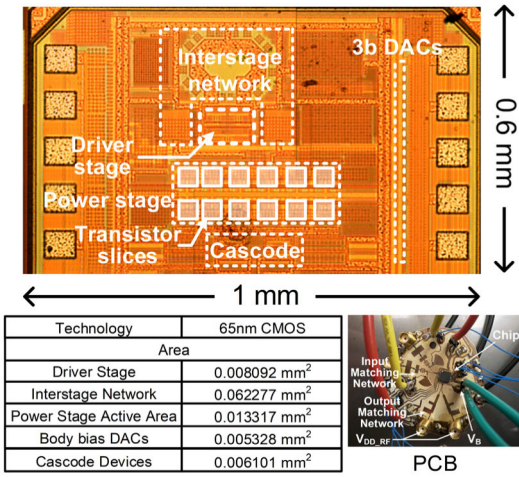


Fig. 11. The PA die micrograph and area estimates are shown alongside a picture of the PCB with the off-chip matching networks.

packets with a 20 MHz channel width as a test signal. The die micrograph of the PA and test board is shown in Fig. 11, with the design occupying a core area of less than 0.0951 mm².

A. Measured Performance

The nominal configuration of the PA is defined to be setting $V_{DD} = 1.2$ V, $V_G = 0.36$ V, 9 output stage differential pairs enabled with body bias RDACs disabled. The measured power and efficiency curves for the nominal configuration of the PA are shown in Fig. 12 for temperature corners from -40 °C to 125 °C. At room temperature, the PA's nominal configuration achieves a compression power of 4.5 dBm and an efficiency of 12.5% at 5.985 GHz. The measured frequency response and constellation diagram are shown in Fig. 13 and Fig. 14. The response in Fig. 13 displays a 3-dB bandwidth of 140 MHz, ranging from 5.91 GHz to 6.05 GHz, effectively accommodating the 20 MHz Wi-Fi channel with ample margin. To verify that reconfiguring the PA between the pseudorandom body bias DAC control vectors for applying slice-level offsets doesn't cause drastic changes in PA performance, the transmit spectrum was measured across all 220 possible nominal configurations, where each

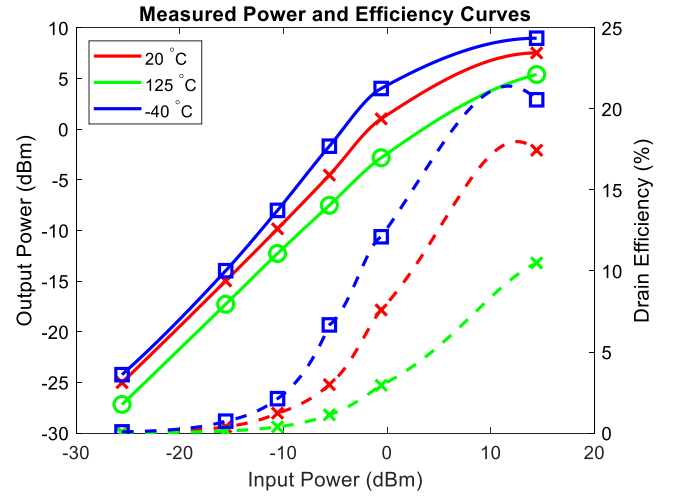


Fig. 12. The measured PA power and efficiency curves are plotted from -40 °C to 125 °C with the PA in a nominal configuration with body bias DACs disabled.

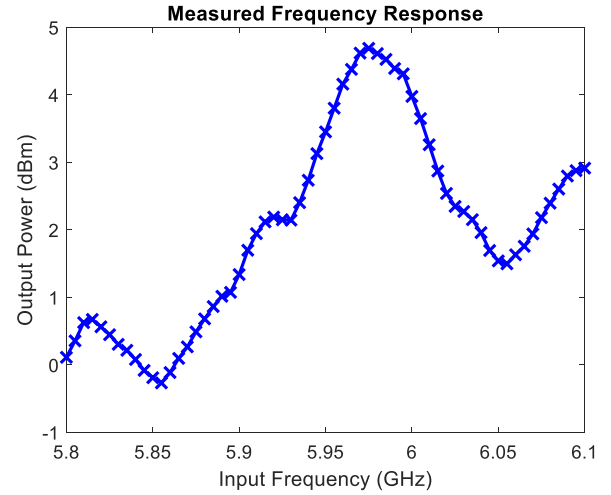


Fig. 13. The measured frequency response of the PA at room temperature with the PA in a nominal configuration with body bias DACs disabled.

was configured with 8 pseudorandom body bias DAC control vectors for a 20 MHz bandwidth 16QAM Wi-Fi 6E test signal at 5.985 GHz. The resultant spectra and histogram of adjacent channel power ratio (ACPR) are shown in Fig. 15 alongside the spectral mask and in Fig. 16.

B. Data Collection Methodology

Although the nominal PA configurations support transmitting 64QAM signals, to fully explore the reconfigurability of the PA in this work, the error vector magnitude (EVM) performance for packets transmitted from the PA across the full configuration range and temperatures was measured to achieve the -19 dB specification for 16QAM. Therefore, 16QAM Wi-Fi 6E SU packets at a center frequency of 5.985 GHz were used as test signals in this work.

The full system integration setup is shown in Fig. 17. The PA test board was connected by coaxial cable to the AD9082 RF setup and the injected RF fingerprint was reconfigured by PA. In order to efficiently perform data analysis on a large number of PA ensembles, a certain number of discrete values

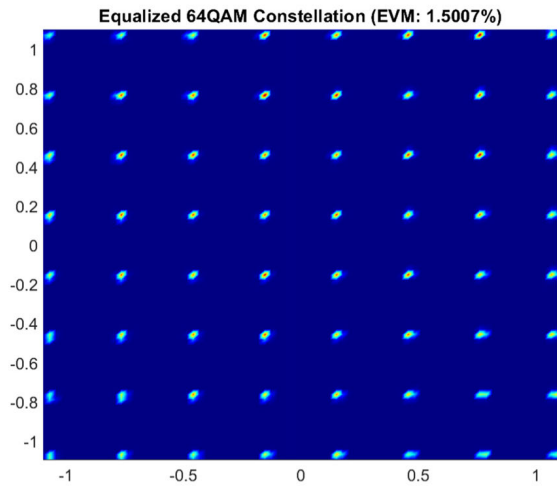


Fig. 14. With the PA in a nominal configuration with body bias DACs disabled, the measured constellation diagram with a 64QAM modulation test signal is shown.

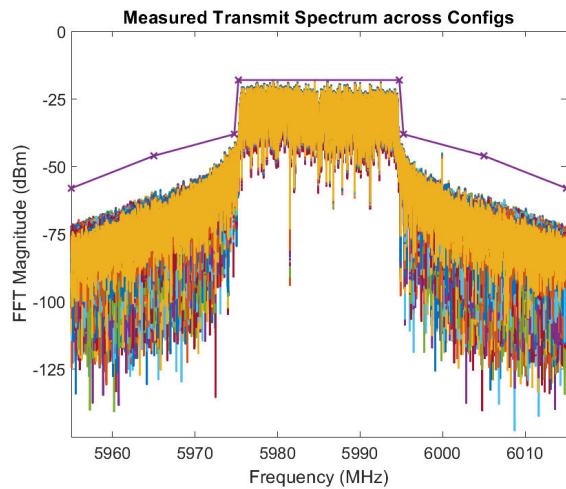


Fig. 15. The measured transmit spectrum across all available combinations of PA output stage device pairs and a set of 8 body bias DAC control vectors.

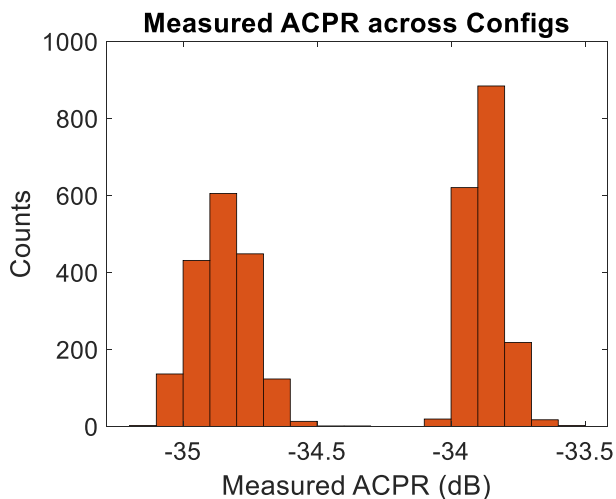


Fig. 16. The measured ACPR across all available combinations of PA output stage device pairs and a set of 8 body bias DAC control vectors.

for each PA configurable variable were selected to provide for a wide range of search space for generating the RFFs. The fingerprint was reconfigured by sweeping $\pm 10\%$ nominal supply

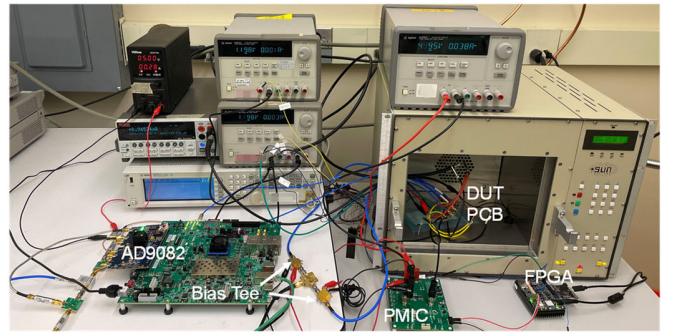


Fig. 17. The system integration setup is pictured above, with the PA test board placed within the EC1A temperature chamber.

voltage V_{DD} (1.08 V, 1.2 V, and 1.32 V), ± 0.1 V nominal PA output stage bias V_G (0.26 V, 0.36 V, and 0.46 V) across all $C(9, 12) = 220$ possible combinations of output stage device pairs with 8 sets of random body bias RDACs, totaling $3 \times 3 \times 220 \times 8 = 15,840$ PA configurations representing the number of presumed RFFs in the dataset. The small tunable range for V_{DD} is chosen to reflect the resource-constrained target application since the proposed system may not afford a wide-range PMIC for powering the PA. The ± 0.1 V gate bias range is chosen to avoid including PA configurations that result in poor EVM performance.

Sufficient data points were collected to extract 10 Wi-Fi packets at a sampling rate of 20 MS/sec for each of the 15,840 unique PA configurations. A Sun Systems EC1A temperature chamber was used to collect data for -40°C , -20°C , 0°C , 20°C , 40°C , 60°C , 85°C , and 125°C .

C. Environmental Variations Modeled by SNR and Temperature

During the data collection process, the signal-to-noise ratio (SNR) in the lab environment was approximately 45dB, additional SNR degradations of 10dB, 15dB, 20dB, and 25dB were applied to the dataset with additive white Gaussian noise (AWGN) for testing the robustness of RFF identification at noisy environments. RF fingerprints that can be successfully identified at lower SNR conditions are expected to offer better noise resistance than others. Furthermore, the fingerprints are sensitive to changes in CMOS circuit properties caused by external factors like environmental variations [10], [27], [28], [29], including temperatures, humidity, and device aging. The changes of the PA characteristic are eventually reflected as the changes in PA nonlinearities and therefore distort the RFFs to degrade identification reliability. In this work the environmental variations are modeled with temperature shifts.

Temperature sweeping was performed during the data collection process to evaluate its effect on the RF fingerprints and investigate compensation of temperature dependencies. EVM for each packet collected from each PA configuration was calculated to evaluate the PA configurations' nonlinearities at different temperatures. Fig. 18 shows the cubic plots for EVM performance of the collected Wi-Fi 16QAM packets across interpolated V_{DD} , V_G , and coherent RDAC levels (i.e., the body bias levels of the output stage differential pairs

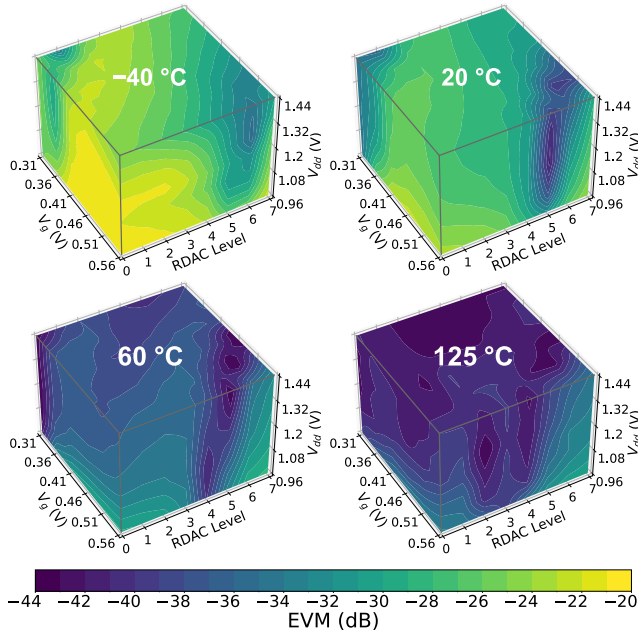


Fig. 18. The measured impact of PA configuration settings on EVM across temperatures is plotted for a 16QAM Wi-Fi 6E test signal.

were varied by sweeping each RDAC setting from 0 to full-scale together) with the first nine output stage selectable elements enabled in the PA. The result indicates that the temperature has a considerable effect on the nonlinearity of the PA. At changed temperatures, especially at low temperatures, some of the PA configurations' transmitted packets do not meet the EVM requirement of 64QAM. Therefore, there exists a trade-off between the number of usable PA configurations for security purposes and using higher-order QAMs.

To more directly assess the response of the RF fingerprint search space to changing SNR and temperature conditions, t-distributed stochastic neighbor embedding (t-SNE) clustering [30] was performed from measurement data (I/Q raw samples), and the results are plotted in Fig. 19. The clustering processes were done with the same eight random PA configurations scanned across temperature variations from three different PA samples. The clustering results consolidate the presumptions in Fig. 2 that SNR degradation obscures the distinct RFF features to affect the success rate of identification. Moreover, the shifted distribution of clusters caused by temperature variations may more seriously distort the established RFF identification scheme. Hence, special measures need to be addressed to counteract distorted RF fingerprints from environmental variations.

IV. RF FINGERPRINT CLASSIFICATION

The reconfigurable PA design expands the PA configuration space with combinatorial PA slices and individual RDAC control. It also enables a very large number of PA configurations by programming the continuous V_{DD} and V_G control space. It is expected that some PA configurations may exhibit overlapped hardware features, therefore it is important to discover how many distinctive RF fingerprints can be utilized for each wireless transmitter. The hardware features associated with

each PA configuration manifest themselves as imperfections such as nonlinearity in the PA's transfer function. For example, the PA transfer function is modeled in Section II-C as a 3rd order polynomial for examining the RF fingerprint variability achievable through the proposed RFF reconfigurability scheme, with the higher-order coefficients taken as measures of these imperfections. These transfer function imperfections produce slight distortions in the signal amplified by the PA, shifting the received I/Q samples from their original values. This deviation constitutes the RF fingerprint of the transmitter and can be extracted using specialized signal processing techniques to compute features from received I/Q samples that represent the RF fingerprint for classification. However, this naïve approach can require computationally expensive signal processing steps and presents a further problem in the form of feature selection, making it challenging to scale the number of fingerprints in the system [31]. This work applies a deep neural network model embedded in the receiver to perform classification tasks on a dataset collected from a large number of PA configurations. A convolutional neural network (CNN) is used to directly process raw I/Q samples as in [31], detect, and capture data features that represent the latent RF fingerprint information embedded in the I/Q samples.

A. RFF Data Format

In this work, raw I/Q samples from preambles in the data packet from transmitted signals are used for RFF classification. Re-using preambles' raw I/Q samples requires minimum data processing that avoids extra overhead to the system and eliminates influence on communication throughput. The format of the baseband data packet [32] and the usage of raw samples from preambles are illustrated in Fig. 20.

As mentioned in section III-B, a dataset was collected with discrete values for each PA configurable variable to provide a large RF fingerprint search space. With $V_{DD} = 1.08$ V, 1.2 V, and 1.32 V, $V_G = 0.26$ V, 0.36 V, and 0.46 V across 220 element configurations and 8 RDAC vectors, 15,840 packets with 20MS/sec sampling rate were extracted from the collected dataset for classification purposes. Different levels of synthesized AWGN were added to the I/Q samples collected in the lab environment to compose the data used in the machine learning tasks.

B. CNN Classification for Determining the RF Fingerprint Capacity

The structure of the CNN used in this work is shown in Fig. 21. The 15,840-class CNN being used here is solely for comparing the distinctiveness of RF fingerprints generated from each PA configuration to select classifiable RFFs. Among the large search space, the number of distinctive RFFs was determined by setting thresholds on the classification accuracies (95% and 99%) on this 15,840-class classification task across SNR variations. In this setup, if a certain RFF class's testing signals can be successfully classified with accuracy above the threshold, this RFF is considered distinctive. The CNN training and testing are conducted using the PyTorch deep learning framework. The training process leverages

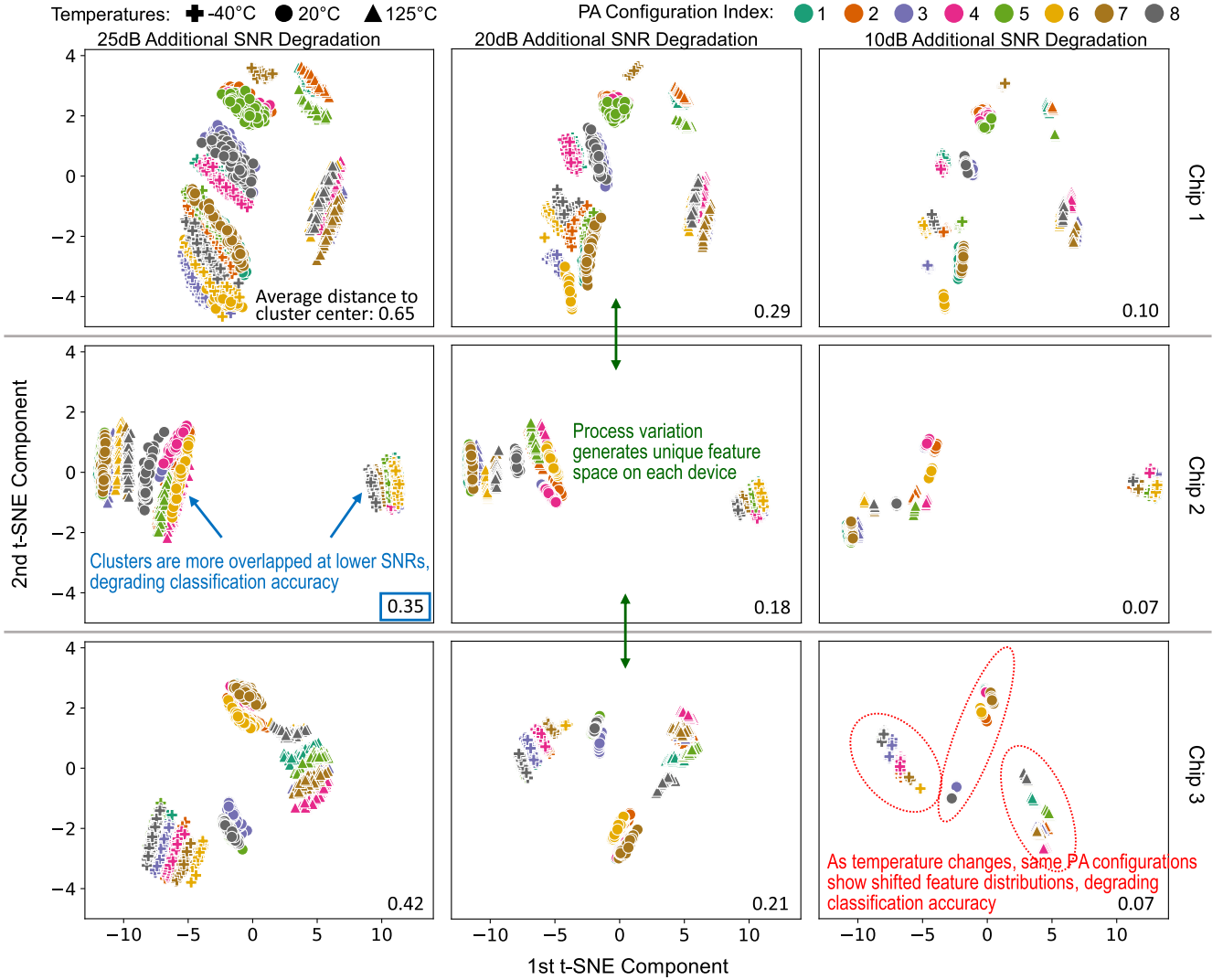


Fig. 19. Clustering plots after dimensionality reduction using t-SNE for measured I/Q samples. They represent RF fingerprints generated from the reconfigurable PA across SNR, temperature, and three chips. The data points in the plots are shaped and colored according to their attributes. Averaged clusters' Euclidean distances to centers grouped by their attributes are calculated to quantize the SNR's effects. Only eight random PA configurations are used in these plots for clarity. The selected PA configurations are consistent across plots. The plots consolidate the example distribution plots in Fig. 2.

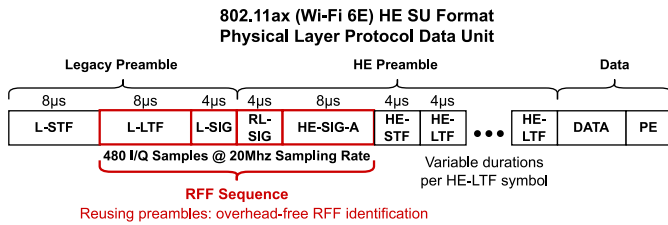


Fig. 20. The Wi-Fi packet format being used in data collection and the preamble sections used in low-overhead RFF classification.

real-time sampling by incorporating artificial AWGN into the collected data. During the training, different levels of AWGN are added to the collected signals in the PyTorch data loader. Each time the data loader is invoked, a fresh batch of signals with artificial noise is retrieved as training data. As a result, the data loader also serves the purpose of generating validation data. The CNN model was trained to minimize the validation loss and then tested on a testing dataset, which includes 1000 testing signals for each PA configuration with different

AWGN levels. The measurements were conducted using three chips to demonstrate the proposed PA's consistent ability to generate a large number of RFFs with different samples. The testing results, which show the number of RFFs generated from each PA configuration that can surpass the classification accuracy thresholds for each chip, are summarized in Fig. 22. The results match the clustering analysis in Fig. 19 where it shows the SNR degradation makes signal feature clusters overlap and affects the signal identification performance by different levels. On top of the testing environment with an additional SNR degradation of 10 dB (35dB SNR), the transmitter equipped with the reconfigurable PA shows over 14,000 RF fingerprints with >95% identification accuracy and over 9,500 RFFs with >99% identification accuracy.

V. RFF RESTORATION FROM TEMPERATURE VARIATION

A. Restoring Distorted RF Fingerprints With RL

As concluded in section III-C, special measures need to be investigated to address the temperature distortion of RFFs

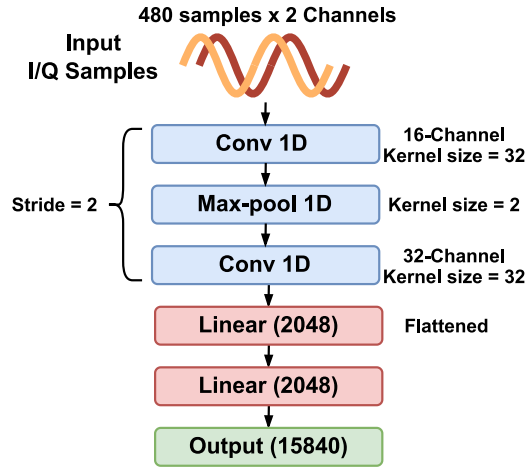


Fig. 21. The structure of the CNN used in finding the number of distinctive RF fingerprints across PA configurations.

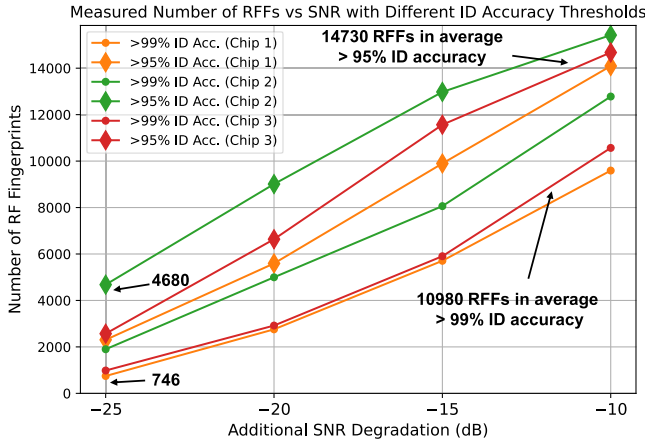


Fig. 22. Classification results of the on-chip RF fingerprints across SNRs and PA samples. Thresholds are set to quantify the distinctiveness of the RF fingerprints.

for reliable RFF identification. Due to the classifier's limited generalizability on unpredictable RF signals [28], [33] excluded from the training dataset, the classifier on the receiver for RFF identification requires frequent retraining after the deployment of the system to adapt to dynamic environmental changes. However, such design complexity and overhead are too high to be integrated into a low-power IoT authentication system. Through exploitation of various ensembles of PA configurations at different temperatures, a high successful rate is achieved for identifying a configuration that can exhibit nominal RFFs predefined at nominal (room) temperature, as illustrated in Fig. 2. With a proper configuration of the PA, the transmitter's RFF features are self-healed to emit undistorted fingerprints. In other words, instead of taking the classifier offline for retraining with distorted new input features at different temperatures, the PA can be automatically reconfigured to generate consistent RF fingerprints across temperature changes.

The large number of PA configurations requires precise characterization to achieve self-healing purposes. In addition to that, configurations for different devices vary due to the

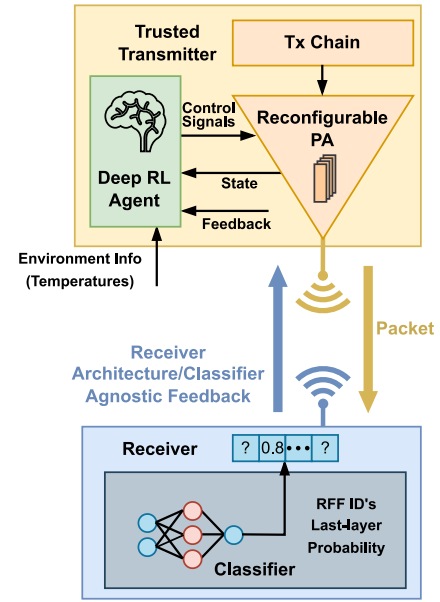


Fig. 23. The RL module is embedded in the transmitter that explores PA programmability to transmit nominal RF fingerprints.

process variations. Hence, it is important to facilitate the automation of the PA's characterization process and control scheme without human intervention. To overcome environmental variations, as shown in Fig. 23, this work proposes a deep reinforcement learning module to adaptively characterize and respond to system dynamics through the exploitation of agile reconfigurability for closed-loop control of the reconfigurable PA.

Deep RL based on Deep Q-Network (DQN) [34] has been proposed to achieve unmanned control schemes for certain sophisticated tasks. In this work, a multi-layer-perceptron (MLP)-based DQN is adapted to configure the PA to generate desired RF fingerprints. A modified deep Q network algorithm tailored for compatibility with fixed-point hardware to facilitate energy-efficient training is used where the hyperparameters have been adjusted accordingly. Specifically, the discount factor γ in the Q function ($Q^\pi(s, a) = r + \gamma Q^\pi(s', \pi(s'))$) is set to 1 and the τ in updating the target network's weights ($\theta' \leftarrow \tau\theta + (1 - \tau)\theta'$) is set to 0 to enhance computation efficiency. In the RL model, the agent and target neural networks' layer sizes including input and output are 17-64-64-64-30 with ReLU activation functions in between. The input vector for the RL neural networks has 17 scalar values and they are 1. The index of the RFF to be generated. 2. Ambient temperature 3. V_{DD} for the specific RFF at room temperature (nominal). 4. Nominal V_G . 5. Nominal RDAC level, and 6-17. The 12 PA's on and off (0/1) status in the nominal RFF condition. The neural network's output vector Z contains 30 possible discrete values for controlling PA's V_{DD} (0.96V, 1.08V, 1.2V, 1.32V, 1.44V), V_G (0.16V, 0.26V, 0.36V, 0.46V, 0.56V), RDAC level (0-7), and enabled elements (12 in total). The decision on which action to apply for controlling the PA is made by $\arg\max(Z_s)$ for each subset (s) of the controllable PA variables. Furthermore, the 9 elements to be enabled in the 12 PA slices are determined by indices of the top 9 elements in the output vector in terms of their values, represented

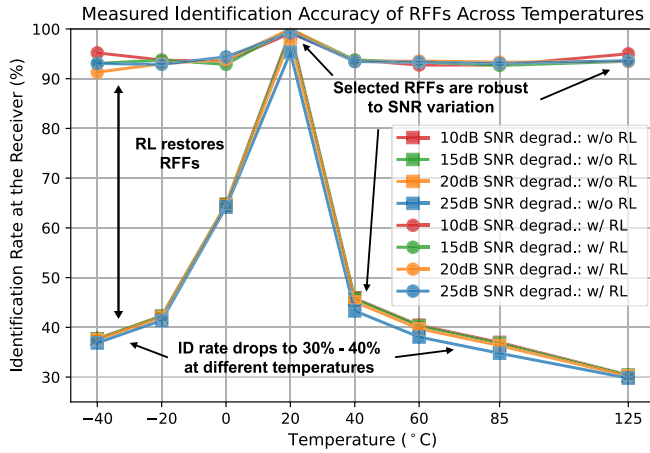


Fig. 24. The RFF identification accuracies with and without RL on the transmitter. The identification accuracies suffer degradation from temperature variations and are restored by RL.

as $\arg\max_9(Z_s)$. The reward function depends exclusively on the receiver classifier's structure-agnostic feedback [35], which reflects the probability (logits) of the classifier's predicted class, ranging between 0 and 1. This work employs a reward function denoted as $r = A * (P_C - B)$ where A and B are constants used for shifting and scaling the obtained logits (P_C) to gauge the effectiveness of the transmitter's RFF restoration. The constants are empirically set to $A = 4$ and $B = 0.5$.

The RL model is fully implemented with fixed-point training and inference for low-overhead hardware implementation on FPGA. 18-bit fixed-point with 9-bit integer part and 9-bit fractional part are adopted to balance the precision and dynamic range for successful training of the model. For the purpose of verifying the performance of the proposed RL, groups of 16 RFFs were randomly sampled from the RFF pool that achieves >99% classification accuracy across SNRs obtained from the testing results in Fig. 22. For this task, a CNN classifier was only trained at room temperature (20 °C) to perform classification on these RFFs across all temperatures. The classification results with and without RL on the transmitter for the selected RFF group across temperature variations are shown in Fig. 24, respectively. The RF fingerprints suffer significant performance degradation for RFF authentication due to the varying PA characteristics at different temperatures. By reconfiguring the PA at different temperatures, the RL successfully restored RFFs back to the nominal state. Such closed-loop control enables uninterrupted operations across temperatures ranging from -40 °C to 125 °C (industrial rating).

B. FPGA Implementation and Performance Summary

The FPGA implementation of the RL controller follows the idea of allocating the computing unit surrounded by data movement logic for neural network training and inference. Its architecture and data path are shown in Fig. 25. The DQN algorithm with two copies of neural networks (agent and target) doubles the model parameter memory requirement compared to in-place parameter updates in traditional supervised learning. The computed gradients from backpropagation

TABLE I
RL ON FPGA PERFORMANCE SUMMARY

ZU3EG A484	Spec
Frequency	50MHz
Quantization	18-bit fixed point (18,9)
Performance	239K inferences/s 122K full backprop/s 38.5 GOPS/W
Power	249mW
Resource	Utilization
DSP	64 (18%)
BRAM	48 (22%)
LUT	42,670 (60%)
FF	27869 (21%)

also need to be saved in memory due to the nature of neural network training. In this work, single-port BRAMs are allocated for storing the neural networks' weights due to their read-only property during the inference. Dual-port BRAMs are allocated for storage of the computed gradients to improve the neural network training's latency and throughput because 50% of the backpropagation operations read and write the model's gradients at the same time.

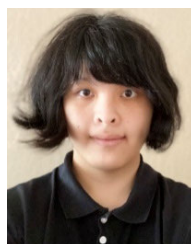
The computing unit carries out all arithmetic operations in the RL. A multiply-accumulate (MAC) array with 64 (intermediate layer size) MAC units is allocated with 64 DSP units on FPGA for matrix multiplication and accumulation operations, followed by a quantization unit (round-to-nearest). An adder tree based on carry-lookahead adders is connected to the output of the MAC array. It enables the row summation mode for training operations. The accumulation mode is mostly used in the forward pass of inference to generate the intermediate neural network outputs, and the summation mode enables the operations in backpropagation to generate gradients of intermediate neural network outputs. The quantization unit is responsible for truncating the MAC output with excessive MSBs and LSBs (bit-width = 36) to the original bit-width (18) with decimal point position and overflow correction (saturation). The Rectified Linear Unit (ReLU) in the neural network's activation layer is directly integrated into the quantization unit as part of the overflow logic. A pipeline layer is added before the adder tree to clock-gate its input to improve the computing unit's throughput and reduce power consumption.

The resource usage and performance of the RL on FPGA are summarized in Table I. There exist trade-offs between latency/throughput of the control, hardware allocation, and power overhead of the RL module's digital implementation. For example, the actual power consumption and throughput depend on the operational period and clock frequency of the controller. The number of allocated MAC units and other hardware resources could be decreased or increased to improve or diminish the performance on latency and throughput. These parameters would vary depending on different application scenarios. The overall performance of the reconfigurable combinatorial PA and its comparison with other works that embed physical layer security features are summarized in Table II.

- [6] S. Rajendran, Z. Sun, F. Lin, and K. Ren, "Injecting reliable radio frequency fingerprints using metasurface for the Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1896–1911, 2021, doi: [10.1109/TIFS.2020.3045318](https://doi.org/10.1109/TIFS.2020.3045318).
- [7] Q. Zhou, Y. He, K. Yang, and T. Chi, "Exploring PUF-controlled PA spectral regrowth for physical-layer identification of IoT nodes," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, vol. 64, Feb. 2021, pp. 204–206, doi: [10.1109/ISSCC42613.2021.9365941](https://doi.org/10.1109/ISSCC42613.2021.9365941).
- [8] Y. Shen, J. Xu, J. Yi, E. Chen, and V. Chen, "Class-E power amplifiers incorporating fingerprint augmentation with combinatorial security primitives for machine-learning-based authentication in 65 nm CMOS," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 5, pp. 1896–1909, May 2022, doi: [10.1109/TCSI.2022.3141336](https://doi.org/10.1109/TCSI.2022.3141336).
- [9] S. Karunaratne, E. Krijestorac, and D. Cabric, "Penetrating RF fingerprinting-based authentication with a generative adversarial attack," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Montreal, QC, Canada, 2021, pp. 1–6, doi: [10.1109/ICC42927.2021.9500893](https://doi.org/10.1109/ICC42927.2021.9500893).
- [10] Ö. Yilmaz and M. A. Yazici, "The effect of ambient temperature on device classification based on radio frequency fingerprint recognition," *Sakarya Univ. J. Comput. Inf. Sci.*, vol. 5, no. 2, pp. 233–245, 2022. [Online]. Available: https://saucis.sakarya.edu.tr/en/pub/issue/72246/1138577#article_cite
- [11] F. Balestra and G. Ghibaudo, "Physics and performance of nanoscale semiconductor devices at cryogenic temperatures," *Semicond. Sci. Technol.*, vol. 32, no. 2, Feb. 2017, Art. no. 023002, doi: [10.1088/1361-6641/32/2/023002](https://doi.org/10.1088/1361-6641/32/2/023002).
- [12] N. C. Dao, A. E. Kass, M. R. Azghadi, C. T. Jin, J. Scott, and P. H. W. Leong, "An enhanced MOSFET threshold voltage model for the 6–300 K temperature range," *Microelectron. Rel.*, vol. 69, pp. 36–39, Feb. 2017, doi: [10.1016/j.microrel.2016.12.007](https://doi.org/10.1016/j.microrel.2016.12.007).
- [13] T. Haapala, A. Liscidini, and K. A. I. Halonen, "Temperature compensation of crystal references in NB-IoT modems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 7, pp. 2467–2480, Jul. 2020, doi: [10.1109/TCSI.2020.2973908](https://doi.org/10.1109/TCSI.2020.2973908).
- [14] H.-C. Liu, Z.-C. Huang, N.-G. Doan, C.-W. Jen, and S. J. Jou, "Joint digital online compensation of TX and RX time-varying IQ mismatch and DC-offset in mmWave transceiver system," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 2, pp. 919–932, Feb. 2022, doi: [10.1109/TCSI.2021.3118052](https://doi.org/10.1109/TCSI.2021.3118052).
- [15] S. Xu, F. Wang, H. Wang, and J. Romberg, "In-field performance optimization for mm-wave mixed-signal Doherty power amplifiers: A bandit approach," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5302–5315, Dec. 2020, doi: [10.1109/TCSI.2020.3022936](https://doi.org/10.1109/TCSI.2020.3022936).
- [16] (Nov. 2021). *Wi-Fi 6E: The Next Great Chapter in Wi-Fi*. San Jose, CA, USA. [Online]. Available: <https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/802-11ax-solution/nb-06-wi-fi-6e-wp-cte-en.html>
- [17] V. H.-C. Chen and L. Pileggi, "A 69.5 mW 20 GS/s 6b time-interleaved ADC with embedded time-to-digital calibration in 32 nm CMOS SOI," *IEEE J. Solid-State Circuits*, vol. 49, no. 12, pp. 2891–2901, Dec. 2014, doi: [10.1109/JSSC.2014.2364043](https://doi.org/10.1109/JSSC.2014.2364043).
- [18] R. Liu, J. A. Weldon, and L. Pileggi, "Extended statistical element selection: A calibration method for high resolution in analog/RF designs," in *Proc. 53rd ACM/EDAC/IEEE Design Automat. Conf. (DAC)*, Austin, TX, USA, Jun. 2016, pp. 1–6, doi: [10.1145/2897937.2898022](https://doi.org/10.1145/2897937.2898022).
- [19] C. A. R. Fernandes, J. C. M. Mota, and G. Favier, "Analysis and power diversity-based cancellation of nonlinear distortions in OFDM systems," *IEEE Trans. Signal Process.*, vol. 60, no. 7, pp. 3520–3531, Jul. 2012, doi: [10.1109/TSP.2012.2193395](https://doi.org/10.1109/TSP.2012.2193395).
- [20] L. Ding and G. T. Zhou, "Effects of even-order nonlinear terms on power amplifier modeling and predistortion linearization," *IEEE Trans. Veh. Technol.*, vol. 53, no. 1, pp. 156–162, Jan. 2004, doi: [10.1109/TVT.2003.822001](https://doi.org/10.1109/TVT.2003.822001).
- [21] S. C. Cripps, *RF Power Amplifiers for Wireless Communications*, 2nd ed. Norwood, MA, USA: Artech House, 2006. [Online]. Available: <http://ieeexplore.ieee.org/document/9101120>
- [22] T. Sakurai and A. R. Newton, "A simple short-channel MOSFET model and its application to delay analysis of inverters and series-connected MOSFETs," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 1990, pp. 105–108, doi: [10.1109/ISCAS.1990.111928](https://doi.org/10.1109/ISCAS.1990.111928).
- [23] P. G. Drennan and C. C. McAndrew, "Understanding MOSFET mismatch for analog design," *IEEE J. Solid-State Circuits*, vol. 38, no. 3, pp. 450–456, Mar. 2003, doi: [10.1109/JSSC.2002.808305](https://doi.org/10.1109/JSSC.2002.808305).
- [24] M. J. M. Pelgrom, A. C. J. Duinmaijer, and A. P. G. Welbers, "Matching properties of MOS transistors," *IEEE J. Solid-State Circuits*, vol. 24, no. 5, pp. 1433–1439, Oct. 1989, doi: [10.1109/JSSC.1989.572629](https://doi.org/10.1109/JSSC.1989.572629).
- [25] J. A. Croon, M. Rosmeulen, S. Decoutere, W. Sansen, and H. E. Maes, "An easy-to-use mismatch model for the MOS transistor," *IEEE J. Solid-State Circuits*, vol. 37, no. 8, pp. 1056–1064, Aug. 2002, doi: [10.1109/JSSC.2002.800953](https://doi.org/10.1109/JSSC.2002.800953).
- [26] P. Andricciola and H. P. Tuinhout, "The temperature dependence of mismatch in deep-submicrometer bulk MOSFETs," *IEEE Electron Device Lett.*, vol. 30, no. 6, pp. 690–692, Jun. 2009, doi: [10.1109/LED.2009.2020524](https://doi.org/10.1109/LED.2009.2020524).
- [27] S. U. Rehman, K. W. Sowerby, S. Alam, and I. Ardekani, "Radio frequency fingerprinting and its challenges," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2014, pp. 496–497, doi: [10.1109/CNS.2014.6997522](https://doi.org/10.1109/CNS.2014.6997522).
- [28] Z. He, S. Zhou, and M. Nie, "Experimentally investigating the performance degradations of the CMOS PA at different temperatures," *AIP Adv.*, vol. 11, no. 11, Nov. 2021, Art. no. 115205, doi: [10.1063/5.0071801](https://doi.org/10.1063/5.0071801).
- [29] X. Aragones et al., "Aging in CMOS RF linear power amplifiers: Experimental comparison and modeling," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2019, pp. 1–5, doi: [10.1109/ISCAS.2019.8702100](https://doi.org/10.1109/ISCAS.2019.8702100).
- [30] L. Van der Maaten and G. Hinton, "Visualizing data using t-SNE," *J. Mach. Learn. Res.*, vol. 9, no. 86, pp. 2579–2605, 2008.
- [31] K. Sankhe, M. Belgiovine, F. Zhou, S. Riyaz, S. Ioannidis, and K. Chowdhury, "ORACLE: Optimized radio classification through convolutional neural networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2019, pp. 370–378, doi: [10.1109/INFOCOM.2019.8737463](https://doi.org/10.1109/INFOCOM.2019.8737463).
- [32] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks-Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*, Standard IEEE Std 802.11ax-2021 (Amendment to IEEE Std 802.11-2020), 2021, pp. 1–767, doi: [10.1109/IEEESTD.2021.9442429](https://doi.org/10.1109/IEEESTD.2021.9442429).
- [33] X. Gu et al., "TeRFF: Temperature-aware radio frequency fingerprinting for smartphones," in *Proc. 19th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Sep. 2022, pp. 127–135, doi: [10.1109/SECON55815.2022.9918173](https://doi.org/10.1109/SECON55815.2022.9918173).
- [34] V. Mnih, "Human-level control through deep reinforcement learning," *Nature*, vol. 518, pp. 529–533, Feb. 2015, doi: [10.1038/nature14236](https://doi.org/10.1038/nature14236).
- [35] S. D'Oro, F. Restuccia, and T. Melodia, "Can you fix my neural network? Real-time adaptive waveform synthesis for resilient wireless signal classification," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2021, pp. 1–10, doi: [10.1109/INFOCOM42981.2021.9488865](https://doi.org/10.1109/INFOCOM42981.2021.9488865).
- [36] X. Lu, L. Hong, and K. Sengupta, "An integrated optical physically unclonable function using process-sensitive sub-wavelength photonic crystals in 65 nm CMOS," in *IEEE Int. Solid-State Circuits Conf. (ISSCC) Dig. Tech. Papers*, Feb. 2017, pp. 272–273, doi: [10.1109/ISSCC.2017.7870366](https://doi.org/10.1109/ISSCC.2017.7870366).



Jiachen Xu received the B.S. degree in computer engineering from Purdue University in 2020. He is currently pursuing the Ph.D. degree at Carnegie Mellon University. His interests include machine learning for sensor interfacing, energy-efficient ASIC and FPGA design for machine learning acceleration, and embedded system design for wireless applications.



Yuyi Shen received the B.S. degree in electrical and computer engineering from Carnegie Mellon University in 2020, where she is currently pursuing the Ph.D. degree. She held an internship position with Apple Inc. in 2020. Her research interests include RFIC design with a focus on the application of RF circuits to security and device identification. She was a recipient of the International Solid-State Circuits Conference Analog Devices Outstanding Student Designer Award in 2021 and the Ben Cook Graduate Fellowship in 2022.



Juntong Deng received the B.S. degree in communication engineering from the University of Electronic Science and Technology of China in 2020 and the M.S. degree in interdisciplinary information studies from The University of Tokyo in 2022. She is currently pursuing the Ph.D. degree at Carnegie Mellon University. Her research interests include machine learning and signal processing algorithms for wireless security applications.



Ethan Chen is currently a Research Scientist with the Energy-Efficient Circuits and Systems Laboratory, Carnegie Mellon University. His research interests include neuromorphic computing, hardware security, and biomedical interfaces.



Vanessa Chen (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University in 2013.

Before joining Carnegie Mellon University as an Assistant Professor, she was affiliated with The Ohio State University. During her Ph.D. studies at Carnegie Mellon University from 2010 to 2013, she conducted research on algorithm-assisted approaches for improving energy efficiency and ultra-high-speed ADCs with on-chip real-time calibration, and interned at the IBM T. J. Watson Research Center in 2012. Prior to academia, she was a Circuit Designer at Qualcomm in San Diego and Realtek, Hsinchu, Taiwan, focusing on self-healing RF/Mixed-signal circuits. Her research interests include AI-enhanced circuits and systems, which include intelligent sensory interfaces, RF/mixed-signal hardware security, and ubiquitous sensing and computing systems.

Dr. Chen has received the NSF CAREER Award, the IBM Ph.D. Fellowship, and the Analog Devices Outstanding Student Designer Award. She has also been involved in various technical program committees, including the IEEE International Solid-State Circuits Conference, the IEEE Symposium on VLSI Circuits, the IEEE Custom Integrated Circuits Conference, the IEEE Asian Solid-State Circuits Conference, and the IEEE/ACM Design Automation Conference. She has served as an Associate Editor for several IEEE journals, including IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, IEEE TRANSACTIONS ON BIOMEDICAL CIRCUITS AND SYSTEMS, and IEEE OPEN JOURNAL OF CIRCUITS AND SYSTEMS. Additionally, she has contributed as a Guest Editor for the *ACM Journal on Emerging Technologies in Computing Systems*.