RF-PSF: Zero-Trust Radio Frequency Process Specific Functions as Process Distinction Method

Md Faizul Bari[#1], Baibhab Chatterjee[#2], Luke Duncan[$3], Shreyas Sen[#4]
[#]Department of ECE, Purdue University, USA
[$]KBR, USA
[1]mbari@purdue.edu, [2]bchatte@purdue.edu, [3]luke@niobiummicrosystems.com, [4]shreyas@purdue.edu

***Abstract*— In this work, we propose a manufacturing process technology distinction method, RF-PSF, that applies artificial intelligence to the transmitted RF signal to exploit process-specific inherent properties embedded in it. By performing the design and simulation of a QPSK transmitter in 14 nm, 22 nm, and 65 nm process technologies, we have shown that on average $\sim 90\%$ accuracy can be achieved for process distinction with $> 99\%$ in the best-case scenario. The effect of sampling rate and quantization, two practical limitations in RF systems, have also been explored. This work establishes RF-PSF as a process distinction method towards zero-trust radio architectures.**

***Keywords*— radio frequency, zero-trust, artificial intelligence, multilayer perceptron, manufacturing process, counterfeit.**

I. Introduction

A zero-trust architecture is a unique environment where all users are treated as potential threats without any predefined trust and access to information and resources is granted only when they get verified. This concept can be applied to the semiconductor supply chain, which is vulnerable as the design is usually performed in one country but fabricated offshore. In a zero-trust environment, even the ICs from an authorized vendor are tested extensively, leaving no space for the breach of trust (as there is none by default!). In 2011, IHS has reported \$169B annual risk due to counterfeiting, with an annual growth of 25%. IC counterfeiting involves recycling and remarking, cloning, tampering, etc. Detection of counterfeiting requires both invasive physical and electrical testing which are costly and time-consuming, especially in the zero-trust approach where the testing load is much heavier. So, it is desirable to extract some of the manufacturing information from the electrical signal of the ICs which can be much cheaper, non-intrusive, and reduce time overhead.

Every process technology has unique design parameters along with process variations that manifest themselves as system-level nonidealities. These *deterministic* parameters and *random* variation-based RF nonidealities in combination form a unique identifier of a process which we define as *Radio Frequency Process Specific Function (RF-PSF)*. In a standard RF receiver, the nonidealities in the received signal are discarded. In RF-PSF, those nonidealities, which contain process information embedded in it, are used to train an artificial neural network (NN), which can then make a distinction among the processes. One particular counterfeiting method, *cloning*, involves IC fabrication using a different process than it is intended. *RF-PSF itself doesn't detect IC cloning, rather it makes a distinction among different process technology. That information is an important part of cloning detection.* In this work, processing simulated data for 3 different processes (14 nm, 22 nm, and 65 nm) and using an artificial neural network, it has been shown that the trained network can distinguish the processes with $> 99\%$ accuracy in the best-case scenario.

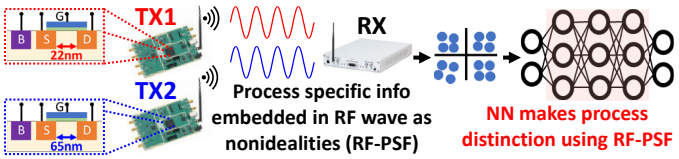

Fig. 1. Process-specific information or function are reflected as rf nonidealities in the transmitted wave, which can be harnessed by an artificial intelligence technique (multilayer neural network) to make process distinctions.

A. Our Contribution

1) In this work, **for the first time, manufacturing process-specific properties, manifested in the transmitted RF signal, are used to make a distinction among different process technologies** using simulated data from 14 nm, 22 nm, and 65 nm technology. It establishes the concept of **RF-PSF** as a fast, cheap, and non-intrusive process distinction method.

2) It has been shown that $>$ **99% accuracy can be achieved for process distinction in the best-case scenario**, with $> 80\%$ accuracy in all cases.

3) **The effect of two practical circuit limitations: baseband sampling rate and ADC resolution, has been addressed** and their impact on detection accuracy has been analyzed.

II. Related Works

Sensitive networks face a wide attack surface which forced the defense agencies to adopt a "zero-trust" architecture [2]-[3]. Borrowing that concept to the semiconductor supply chain raises the issue of time and cost overhead for additional testing. Manufacturing process information is an important part of counterfeiting (especially cloning) detection[4], which requires time-consuming tests [5]. According to a review, counterfeits cost the industry more than $\$100B$ per year back in 2007 [6]. In 2010, an assessment by the U.S. Department of Commerce shows an increase of 141% in counterfeit cases over a period of four years [7]. A police raid on a suspected counterfeiter in China's Guangdong province found fake computer parts worth US \$1.2 million, which is

2022 IEEE/MTT-S International Microwave Symposium - IMS 2022 | 978-1-6654-9613-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/IMS37962.2022.9865379

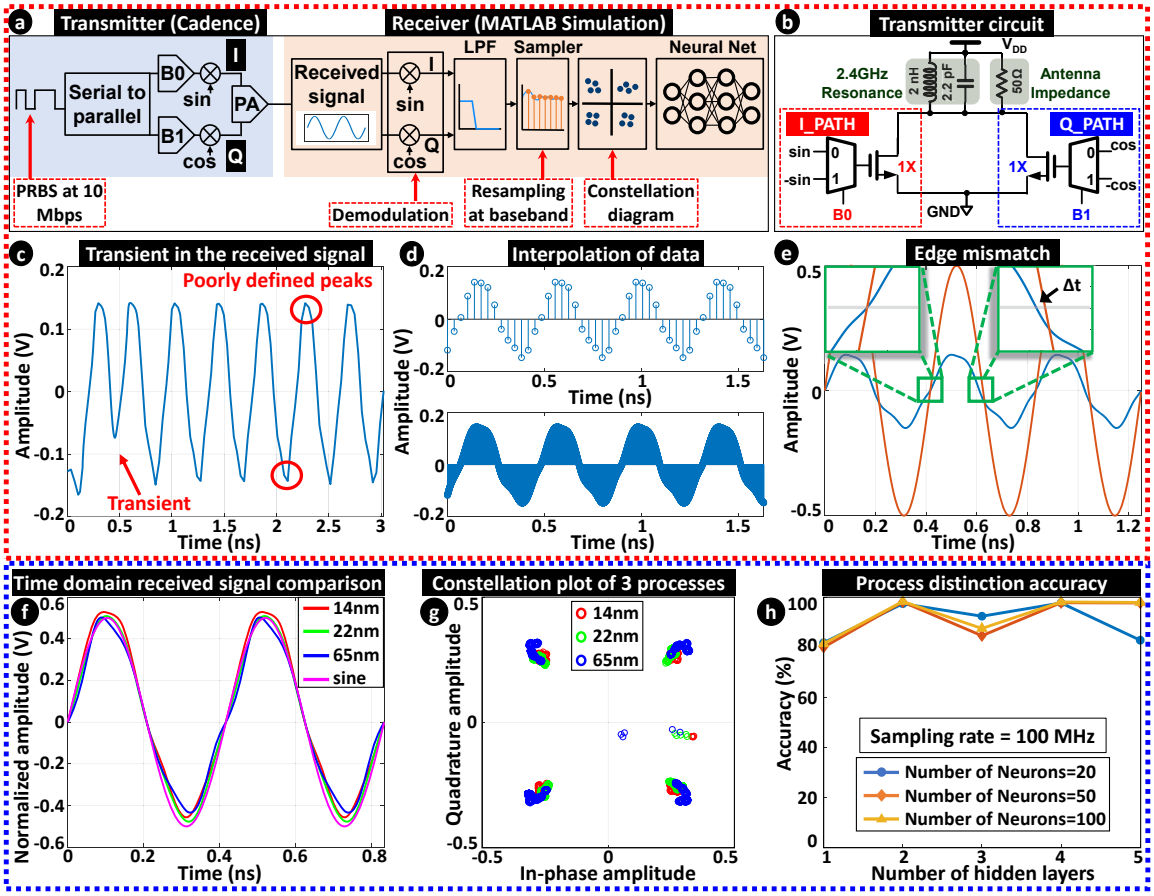

Fig. 2. The dotted red box on top shows simulation and data processing while the dotted blue box at the bottom shows process comparison. (a) Simulation block diagram. The transmitter is simulated in Cadence where PRBS data are transmitted using QPSK modulation. The receiver is simulated in MATLAB where the RF signal is processed. (b) Transmitter circuit diagram. (c) Initial transient in the received signal shows irregularity in the wave. (d) Data is interpolated with a factor of 100 to get a well-defined wave. (e) Although the rising edge of the signal matches (left inset), the falling edge doesn't (right inset). This is due to DC offset and corrected. Comparison of 3 processes in (f) time domain signal (g) constellation (h) accuracy of NN.

enough to make computer servers and a lot of personal PCs [8]. Manufacturing process variation-based 'device-specific signatures' have been for RF fingerprinting in literature [9], [10], [11], [12]. This mapping can be extended to use *process specific functions* to distinguish among different processes.

III. Simulation Method

Fig. 2(a) shows the TX and RX designed in Cadence and MATLAB respectively. A 7-bit PRBS is used to generate random bits at 10 Mbps, which is converted to 2-parallel streams (**B0** and **B1**). They are modulated using sine and cosine carriers of 2.4 GHz to provide a QPSK modulated signal. A low-power, RF-DAC PA with 50 Ω antenna impedance is used at the end of the transmitter chain which resonates at 2.4 GHz to produce the final RF output signal (fig. 2(b)). The transient analysis is performed for 15 µs for 3 different processes: 65 nm, 22 nm, and 14 nm.

IV. Data Processing

A. Discarding Transients and Interpolation of Data

Fig. 2(c) shows that the received signal has initial transients that lead to shape distortion. This transient is removed by discarding the first 1 µs data. Fig. 2(c) also shows that the wave peaks are lineated due to a low sampling rate (as we are in high frequency RF domain). While the step size is optimum to keep enough information about each cycle in Cadence, we might lose significant information while data processing. Hence, an interpolation factor of 100 is used with a uniform step size of 34.62 ps to interpolate the RF data as shown in Fig. 2(d).

B. Time Axis Shifting

The interpolated signal is shifted slightly on the time axis to start at the zero-crossing point of the rising edge. This is important because otherwise, these initial few sample differences with the clock (which begins at t=0) will lead to a constant phase difference erroneously.

C. Edge Matching and Normalization

Shifting the wave along the time axis matches the rising edge of it with the reference clock (left inset), but the falling edge doesn't match as shown in the right inset of fig. 2(e). This is due to DC offset and leads to a constant time difference Δt erroneously. This is a computational artifact which is unrelated to manufacturing process. Hence, the offset is removed to

make it 50% duty cycle. Also, the waves are normalized to bring it in the range of 1 V.

D. Demodulation and Filtering

Two reference clocks (sine and cosine) of 2.4 GHz frequency are generated in MATLAB. The edge-matched and normalized RF signal is multiplied with the sine and cosine wave to produce the I and Q-channel respectively. A low-pass filter is used to filter out the high-frequency RF components from the demodulated signal.

E. Resampling at Baseband

The very high sampling rate in the RF domain is no longer required in the baseband. So, the filtered signal is resampled to convert it to a sampling rate of 100 MHz (10 times the original data rate).

F. Neural Network

The resampled data are used to train an artificial neural network (ANN or MLP). The raw I-Q samples in each quadrant are taken as features (2 I-Q points $\times$ 4 quadrants = 8 features). The feature set is divided into 70%, 15%, and 15% ratios for train, validation, and test purposes.

V. Results

A. Performance of Process Distinction

1) Comparison of the Received Signal

Fig. 2(f) shows the received signals in the time domain (FF corner of all processes) with a reference sine clock. Time-domain signals show the presence of the process information in the transmitted signal with a clear distinction in size and shape.

2) Comparison in Constellation Diagram

Fig. 2(g) compares 3 process technologies (red, green, and blue represents 14 nm, 22 nm, and 65 nm processes) in terms of constellation diagram. Here, all 5 process corner data are plotted as one combined group. It can be observed from the plot that, the 3 processes form distinct regions with some overlapping. This represents that although some process information is lost (overlapping) in the data generation, transmission, and processing pipeline, most of them are retained in the baseband.

3) Detection Accuracy

We train a neural network with the constellation data. Fig. 2(h) shows the detection accuracy of 3 processes for different NN configurations. It can be observed that the accuracy is always $> 80\%$ and can reach up to $> 99\%$. But on average, it remains $\sim 90\%$.

B. Effect of Sampling Rate

Fig. 3(a) shows the effect of the sampling rate at the baseband. It can be seen that below the Nyquist rate, the accuracy drops significantly due to a loss of information. However, at or above the Nyquist rate, it remains pretty good.

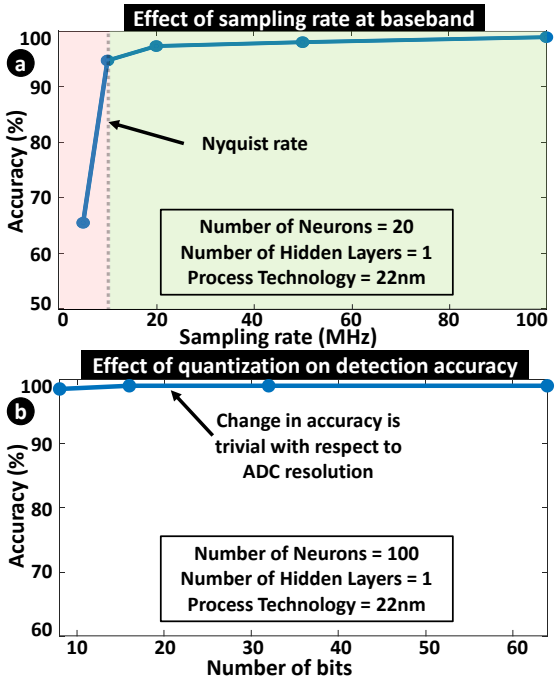

Fig. 3. (a)Effect of different sampling rates at the baseband. Below the Nyquist rate (light red region), the accuracy drops significantly. However, at or above the Nyquist rate (light green region), the accuracy remains high. (b) ADC resolution or data quantization has trivial effect on performance.

C. Effect of Quantization

In MATLAB, the data have 64 bit resolution by default. However, actual ADCs are typically 8 or 16 bits. So, it is important to see if our results hold for low resolution, i.e. low-bit ADC. Fig. 3(b) shows the accuracy versus number of bits. We see that even at 8 bit, accuracy remains almost unchanged. So, practical ADC resolution has a trivial impact on the performance.

VI. Conclusion

In this work, the concept of radio frequency process-specific function (RF-PSF) has been proposed by applying artificial intelligence to the processed RF signal. RF-PSF is used to make a distinction among 3 process technologies: 14 nm (GlobalFoundries), 22 nm (GlobalFoundries), and 65 nm (TSMC). Using simulated data from Cadence and processing it in MATLAB, it has been shown that, $> 80\%$ accuracy can be achieved in different NN configurations with a best-case performance of $> 99\%$ accuracy. Practical RF receiver is limited in terms of baseband sampling rate and ADC resolution. The effect of these two parameters has been explored in detail. To conclude, the analysis of the time-domain signals and constellation plot, along with performance evaluation using I-Q data in neural networks proves the existence of process-specific function in the RF domain which still exists in the downsampled, baseband signal at the receiver end and can be utilized as a cheap, non-intrusive, fast, and zero power overhead process distinction method.

REFERENCES

[1] "THE COMMITTEE'S INVESTIGATION INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN," Nov. 8, 2011. Accessed on: Nov. 30, 2021. [Online]. Available: https://www.govinfo.gov/content/pkg/CHRG-112shrg72702/html/CHRG-112shrg72702.htm

[2] "COVID-Related Telework Accelerates DISA's Zero-Trust Adoption," Dec. 1, 2020. Accessed on: Nov. 30, 2021. [Online]. Available: https://www.defense.gov/Explore/News/Article/Article/2431541/covid-related-telework-accelerates-disas-zero-trust-adoption/

[3] Barnett, Jackson, "Air Force pushing 'mission-critical' applications to zero trust,". Accessed on: Nov. 30, 2021. [Online]. Available: https://www.fedscoop.com/air-force-zero-trust-mission-critical-frank-konieczny/

[4] Pecht, Michael. "The counterfeit electronics problem." Open Journal of Social Sciences 1, no. 07 (2013): 12.

[5] Sood, Bhanu, Diganta Das, and Michael Pecht. "Screening for counterfeit electronic parts." Journal of Materials Science: Materials in Electronics 22, no. 10 (2011): 1511-1522.

[6] Lowry, Robert K. "Counterfeit electronic components-an overview." In Military, Aerospace, Spaceborne and Homeland Security Workshop (MASH). 2007.

[7] Collier, Zachary A., Steve Walters, Dan DiMase, Jeffrey M. Keisler, and Igor Linkov. "A semi-quantitative risk assessment standard for counterfeit electronics detection." SAE International Journal of Aerospace 7, no. 2014-01-9002 (2014): 171-181.

[8] M. Pecht and S. Tiku, "Bogus: electronic manufacturing and consumers confront a rising tide of counterfeit electronics," in IEEE Spectrum, vol. 43, no. 5, pp. 37-46, May 2006, doi: 10.1109/MSPEC.2006.1628506.

[9] M. F. Bari, B. Chatterjee and S. Sen, "DIRAC: Dynamic-IRregulAr Clustering Algorithm with Incremental Learning for RF-Based Trust Augmentation in IoT Device Authentication," 2021 IEEE International Symposium on Circuits and Systems (ISCAS), 2021, pp. 1-5, doi: 10.1109/ISCAS51556.2021.9401403.

[10] M. F. Bari, B. Chatterjee, K. Sivanesan, L. L. Yang and S. Sen, "High Accuracy RF-PUF for EM Security through Physical Feature Assistance using Public Wi-Fi Dataset," 2021 IEEE MTT-S International Microwave Symposium (IMS), 2021, pp. 108-111, doi: 10.1109/IMS19712.2021.9574917.

[11] B. Chatterjee, D. Das, S. Maity and S. Sen, "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," IEEE Internet of Things Journal, 2019.

[12] M. F. Bari, P. Agrawal, B. Chatterjee and S. Sen, "Statistical Analysis Based Feature Selection Enhanced RF-PUF with >99.8% Accuracy on Unmodified Commodity Transmitters for IoT Physical Security," arXiv:2202.05684 [cs.CR], Feb. 2022.