




Article

NotchPUF: Printed Circuit Board PUF Based on Microstrip Notch Filter

Mitchell Martin and Jim Plusquellic * 

Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131, USA; mmartin3@unm.edu

* Correspondence: jimp@ece.unm.edu

Received: 6 March 2020; Accepted: 31 March 2020; Published: 4 April 2020



Abstract: Physical Unclonable Functions (PUFs) are primitives that are designed to leverage naturally occurring variations to produce a random bitstring. Current PUF designs are typically implemented in silicon or utilize variations found in commercial off-the-shelf (COTS) parts. Because of this, existing designs are insufficient for the authentication of Printed Circuit Boards (PCBs). In this paper, we propose a novel PUF design that leverages board variations in a manufactured PCB to generate unique and stable IDs for each PCB. In particular, a single copper trace is used as a source of randomness for bitstring generation. The trace connects three notch filter structures in series, each of which is designed to reject specific but separate frequencies. The bitstrings generated using data measured from a set of PCBs are analyzed using statistical tests to illustrate that high levels of uniqueness and randomness are achievable.

Keywords: physical unclonable functions; PUF; printed circuit board; PCB, band-reject filter; notch filter; PCB variations; interdigital capacitor

1. Introduction

Counterfeit electronic components are an increasing concern in the global supply chain of electronic goods. These concerns are reflected in many nations around the world. A 2016 report from the U.S. Chamber of Commerce cites a study conducted by Organization for Economic Co-operation and Development (OECD) estimating that, “global trade-related counterfeiting accounts for 2.5 percent of world trade, or 461 billion [1] U.S. Dollars. This is an increase of 55 percent in less than 10 years. Besides the economic impact, the biggest issue with counterfeit electronic components is the reliability and authenticity of the components being used. Most of the existing work to address these issues utilize Physical Unclonable Functions (PUFs), counterfeit detection techniques, or cryptographic algorithms in hardware or software built into critical parts of the system.

PUFs derive randomness from the physical characteristics of a device that are relatively easy to measure but difficult to clone. Often, they arise from variations in the manufacturing process that result in unique characteristics of individual devices. PUFs are poised to represent the next generation of hardware security primitives for integrated circuits (ICs) and fabricated Printed Circuit Boards (PCBs). The specific identifiers produced by PUFs can serve several applications including unique IDs, authentication, and encryption. PUFs measure and digitize the natural variations that occur in, for example, path delays, leakage current and SRAM power-up patterns, to produce a long sequence of random bits, that is, a bitstring. Most of the applications that use these bitstrings require that they be random and unique among the population, and reproducible across adverse environmental conditions. While many of these techniques have matured for manufactured ICs, field-programmable gate arrays (FPGAs), and so forth, opportunities for improving anti-counterfeiting techniques for PCBs still exist.

To address this board-level security gap, we propose a novel physical unclonable function for PCBs that contains multiple structures to help increase the amount of entropy extracted from a single copper board trace. The proposed solution, called NotchPUF, consists of a number of interdigital capacitor copper trace structures fabricated on the top layer of a 2-layer FR-4 PCB. These structures are designed and tuned to reject 1, 2 and 3 GHz frequencies with various attenuation factors. These frequencies were chosen to prevent aliasing from each series connected structure's response. Before fabrication, simulations are used to tune each of the three filters individually, and once optimized, additional simulations are used to tune the unified structure with all three filters inserted in series.

The filters are inserted in series to reduce the number of physical I/O driver resources and the amount of time needed for measurement and bitstring generation. To ensure that the PUF design produces bitstrings that are unique among the population, we design the filters' dimensions to the minimum design rule sizes supported by the fabrication house, thereby maximizing the amount of manufacturing variation effects. The bitstring generation strategy utilizes multiple properties of the measured S_{21} waveform. S-parameters describe the input-output relationship between ports (or terminals) in an electrical system. For instance, in the proposed 2 port system, the symbol S_{21} represents the power transferred from Port 1 to Port 2. We fabricated 48 boards to validate the proposed PUF. The results show that the NotchPUF exhibits high levels of uniqueness and randomness, which are two important statistical properties associated with PUF-generated bitstrings.

This paper is organized into seven sections. Section 2 gives the background on previous PUF designs and techniques. Section 3 presents the NotchPUF design. Section 4 shows simulation results to verify the proposed design. Section 5 discusses the variations that were observed in the fabricated PCBs. Experimental results in Section 6 show the properties, benefits and limitations of the NotchPUF using hardware experiments. Finally Section 7 concludes the paper.

2. Background

Encryption, authentication, identification and feature activation each utilize random bitstrings as the root component from which the security features of the algorithm and/or protocol are derived. PUFs were introduced in Reference [2], and later refined in Reference [3], to produce unclonable, random and unique keys and bitstrings for these security functions. Since their introduction, a wide range of PUF architectures have been proposed. Each architecture defines a source of entropy, that is, device-level features that vary randomly because of non-zero manufacturing tolerances. For example, Reference [2] leverages random variations in transistor threshold voltages, Reference [3] uses variations in speckle patterns, References [4–7] measure variations in delay chains and ring oscillators (ROs), Reference [8] reads out random power-up patterns in SRAMs, while References [9,10] leverage variations in metal resistance.

As these previous solutions have matured, it has become increasingly apparent that PCBs have many of the same security issues that ICs possess. Similar issues between ICs and PCBs such as counterfeiting and trojan insertion, are described by Ghosh [11]. These authors also present a technique that scrambles the traces on a board, making reverse engineering (RE) more difficult. An obfuscation based approach is described in Reference [12], which uses COTS parts such as a complex programmable logic device (CPLD) or an FPGA. Their obfuscation approach uses a permutation approach designed to hide inter-chip connections between chips. These types of techniques complicate attempts to reverse engineer layouts to synthesized netlists.

When comparing security issues that exist between both ICs and PCBs, printed circuit boards suffer from a size difference that is several orders of magnitude larger when compared to ICs. Because of this, board features are far more accessible to basic types of manipulations and attacks such as those described by Bhunia and Tehranipoor [13]. Some protections against PCB based attacks are proposed in References [14–16], which physically protect the PCB using an active protection scheme that is able to detect physical tampering. Other protection schemes construct and combine fingerprints of different components on a PCB into a fusion PUF [17]. This fingerprint can be extracted from a

variety of components such as a FPGA, SRAM, processor and non-volatile memory. While effective, the components used for PCBs also have supply chain/counterfeit issues. A solution to this issue is proposed in Reference [18] which uses thermal imaging, statistical analysis and machine learning for identification of counterfeit boards and components.

Other authentication techniques have been proposed that fingerprint PCB surface imperfections [19]. Moreover, visual imperfections that occur within PCB vias or through-hole solder pads are used in the fingerprinting process. Although good results are expected during enrollment, a fielded unit may exhibit problems with reproducibility during regeneration if any of the exposed fingerprinted areas suffer from normal “wear and tear” scrapes to the copper plating.

Furthermore, designs have been proposed that analyze variations within passive components [20], debug components [21], or a combination of passives that define a filter structure [22]. While surface mount components are plentiful on any modern PCB design, measuring each individual component to create a unique identifier becomes impractical and costly. Another element present on all PCBs are copper traces. The variations that exist within copper traces have been used as the foundation of unique identifiers [20,23–25]. These techniques measure variations in single and double layer copper traces that are replicated across the PCB at different locations [20,23]. Double layer copper traces are constructed as transmission lines and used with several PCB elements to check the integrity of the PCB. These elements have embedded PUFs that are capable of generating individual authentication IDs.

A type of device that is commonly utilized in association with RF equipment is the notch filter (aka band reject/stop filter). These filters are typically composed of a low-pass and high-pass filter that are connected in a parallel configuration. The notch filter device enables passage of specific frequencies and rejects others. It is also called band elimination filter or notch filter. In 1970, Alley [26] proposed interdigital capacitors for use in lumped-element microwave ICs. The microstrip interdigital resonator is equivalent to the planar interdigital capacitor, whose operating frequency can be changed by controlling the capacitance. The microstrip notch filter uses open circuited stubs consisting of one main transmission line coupled to a half-wavelength resonator, which is typically electrically and magnetically coupled to it. The resonance frequency depends on the half-wavelength resonator. However, open-circuited stubs are large and not well suited as a PCB PUF. The microstrip notch filter with shunt stubs of a quarter wavelength must be larger than the quarter-wavelength resonator [27]. To increase the number of PUF structures that can exist on a PCB, a compact solution is needed. A number of structures have been proposed that show the decrease in size that PCB resonators have undergone over the years [28–30].

IC PUFs have continued to mature while the need for a reliable PCB based PUF still exists. Current work in the PUF field has laid the ground work for more complex structures such as those introduced in this paper for the first time. Besides trace impedance variations, there exists many additional sources of entropy in a PCB that have yet to be fully utilized. Motivated by the above, we propose the NotchPUF, a set of tuned microstrip filter PCB structures that leverage this entropy for the creation of a unique board identifier.

3. Interdigital Notch Filter

The goal of the NotchPUF is to leverage random manufacturing variations that exist within a sequence of microstrip resonator structures to create a unique, unclonable identifier for the PCB, which can be used for authentication. In this section, we describe the structural and electrical characteristics of the proposed NotchPUF.

3.1. Double Interdigital Resonator

The NotchPUF consists of three structures that each contain a double interdigital resonator, which can be tuned to reject specific frequencies. Given the high-frequency nature of RF circuits, these resonators are inherently sensitive to various physical parameters of the PCB, such as trace widths, spacing, board thickness, substrate dielectric constant, and so forth. The double resonator structure is

shown in Figure 1. The input port (Port 1) and output port (Port 2) are connected via two resonators and a length of copper (W_3), to form the notch filter structure. Since each resonator has more than two fingers, the interdigital capacitance between each finger must be considered. Equation (1) from Reference [26] can be used to estimate the interdigital capacitance for a single resonator structure.

$$C(\rho F) = \frac{\epsilon_r + 1}{W_1} l_2 (\epsilon_r + 1) [0.1(n - 3) + 0.11]. \quad (1)$$

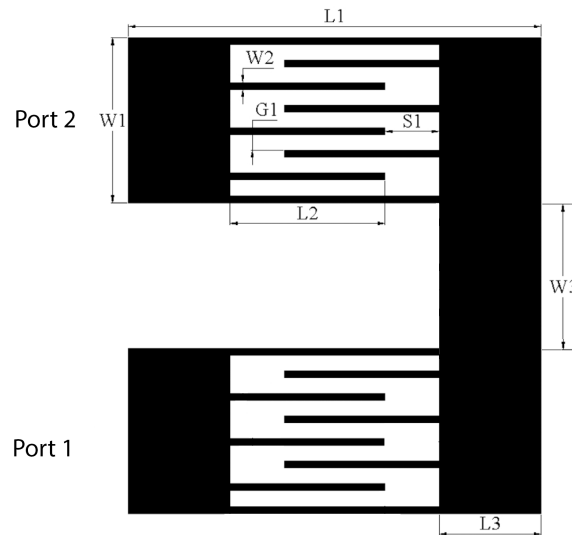


Figure 1. Printed Circuit Board (PCB) structure of a single notch filter with a double microstrip interdigital resonator.

Here, n is the number of fingers (6 in this case), and W_1 is the line width (3 mm) of the microstrip interdigital resonator, as shown in Figure 1. The interdigital capacitance affects the center frequency of the designed filter, which classifies the interdigital notch filter as a semi-lumped element device. Furthermore, the center frequency of the filter can be tuned by varying the number of fingers (n) and the gap spacing S_1 . Using (1), we were able to derive an accurate capacitance value that enabled each of the filter structures to be tuned to a specific rejection frequency.

3.2. NotchPUF

The proposed notch filter is designed to increase the level of randomness that can be extracted over that of single copper trace lines by amplifying small PCB manufacturing variations, in particular, those associated with the interdigital capacitor. In contrast, single copper trace wires that traverse the PCB can suffer from an “averaging effect” where small board-level variations in wire widths and capacitances are averaged out over the length of the trace, effectively reducing the magnitude of signal variations that can be measured and leveraged by the PUF.

To reduce the area overhead associated with the proposed NotchPUF, we connect 3 notch filter elements in series. The three filters have similar physical characteristics but are distinct in their rejection frequencies. For example, each notch filter has the same size traces, the same distance between fingers, the same 50 ohm characteristic trace impedance, and only the length L_1 is varied among the 3 copies to achieve different rejection frequencies. A full-wave electromagnetic (EM) simulator [31] was used to design and tune the proposed notch filter with interdigital resonator center frequencies of 1, 2, and 3 GHz. These filters are then combined in series, and re-simulated to further tune the response of the individual filters. The process used for tuning each these structures is discussed in more detail in Section 4. The final structure of the NotchPUF is shown in Figure 2.

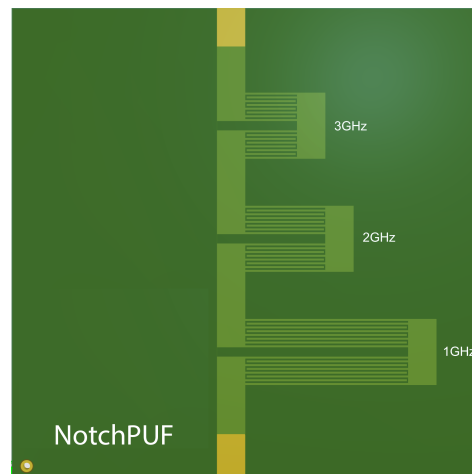


Figure 2. PCB structure of a single NotchPUF

4. Simulations

Full-wave EM simulations were run to determine the optimal size and spacing of the filter's physical geometries to achieve the target notch frequencies of 1, 2 and 3 GHz. Each of the three notch filters were simulated individually while varying the parameters shown in Figure 1 across a range of values. Additional details of these simulations are provided in the following.

4.1. Tuning

In CST Studio [31], a single double-resonator was modeled on a FR-4 substrate with a thickness of 1.6 mm. FR-4 is a low-cost printed circuit board material, manufactured from fiberglass cloth embedded within an epoxy resin. A full copper ground plane is placed on the entire bottom layer of the board with a 1 oz copper pour (1.4 mils). Using simulations, the length parameters L_1 , L_2 , S_1 , W_2 , and G_1 (Figure 1) were tuned until the double interdigital resonator had a center frequency of 1 GHz. Once the optimal parameters for the 1 GHz structure were determined, only L_1 was changed to get center frequencies of 2 and 3 GHz. Figure 3 illustrates the impact of using several different values of parameter L_1 on the center frequency of the double microstrip resonator. From the plot, decreasing L_1 causes the center frequency to increase. Moreover, because the other length parameters are held constant, and not simultaneously optimized in these simulation results, the fractional bandwidth (FBW) percentage also increases (filter gets wider).

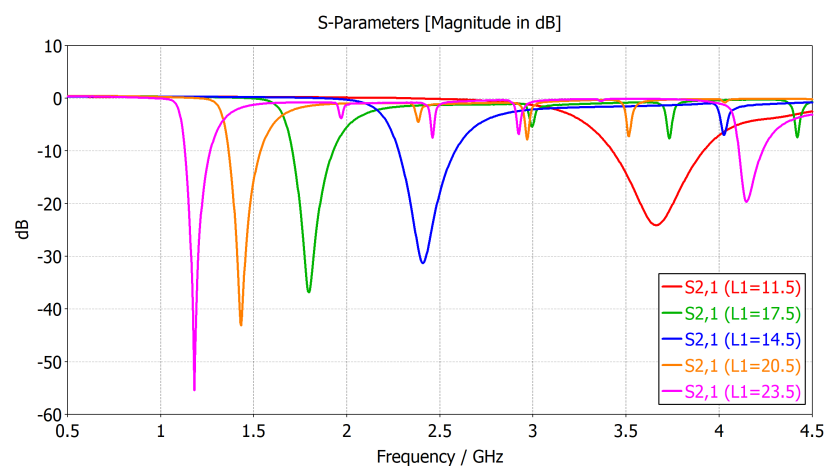


Figure 3. S_{21} Notch filter tuning.

The simulation process that we used tuned all parameters simultaneously to achieve the optimal result, which yielded the following values: $L_{1(1\text{GHz})} = 23.30$ mm, $L_{1(2\text{GHz})} = 14.50$ mm, $L_{1(3\text{GHz})} = 11.50$ mm, $L_2 = 8.35$ mm, $L_3 = 3.0$ mm, $W_1 = 3.0$ mm, $W_2 = 0.20$ mm, $W_3 = 1.0$ mm, $G_1 = 0.40$ mm and $S_1 = 0.15$ mm. As noted earlier, only L1 is different in the 3 versions of the filter.

4.2. NotchPUF Simulations and Validation in Hardware

The individually tuned double-resonator structures were then connected in series to define the proposed structure of the NotchPUF as shown in Figure 2. Additional simulations were used to fine tune the parameters of the unified NotchPUF structure. Figure 4 plots the simulated performance and actual performance of a fabricated NotchPUF PCB together. Table 1 gives the values of several important response characteristics of the NotchPUF obtained from the simulations.

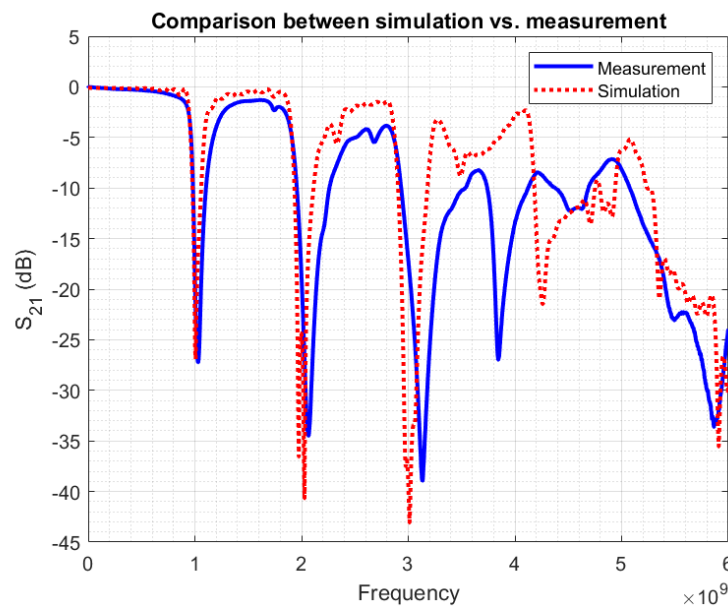


Figure 4. NotchPUF Simulation vs. Measurement.

Table 1. Simulation Properties.

Structure	f_c (GHz)	FBW	IL (dB)
1 GHz	1.008	15.9%	−26.91
2 GHz	2.028	17.8%	−40.68
3 GHz	3.012	13.6%	−43.09

Here, f_c is the central frequency, FBW is the -3dB fractional bandwidth, and IL is the insertion loss. Equation (2) gives the expression to compute the fractional bandwidth.

$$FBW = (f_2 - f_1) / f_c. \quad (2)$$

Here, f_1 is the lower frequency, f_2 is the upper frequency and f_c is the center frequency. Although differences between the measured and simulated frequencies can be attributed to modeling errors, we show in the following that a large fraction of this difference is actually introduced by variations in the fabrication process.

5. PCB Variation

The NotchPUF leverages shifts in the rejection frequency and changes in the attenuation at the rejection frequency as a source of entropy. Variations that occur in these response characteristics across

PCBs are rooted in the PCB manufacturing process. PCBs are fabricated by decomposing the elements in the design, wires and vias, into a sequence of layers. For example, a two layer board consists of a top copper layer, a middle dielectric substrate layer (usually woven glass and epoxy) and a bottom copper layer. The copper and substrate layers are bonded together using a lamination process that applies heat and pressure to the three layers. Traces on the copper layers are created using a mask and high intensity UV light. The unexposed regions are then etched with a chemical solution. Conducting vias between the layers are created using a drilling and plating process. PCBs with additional layers are created by applying a dielectric prepreg bonding layer to the two layer board and then another etched copper layer, with drilling and plating as needed. The outside layers are finished by using a solder mask and tinning process. Additional details can be found in Reference [32].

All of these PCB processing steps are subject to manufacturing variations. Moreover, the magnitude of the variation is directly related to the size of the drawn component, with smaller features typically exhibiting larger levels of variations. We designed the geometries of the NotchPUF to be close to the minimum feature size allowed by the fabrication house as a means of increasing the probability that different boards will produce different responses. We used the PCB board manufacturer specified tolerances to guide our selection of certain design parameters. For example, the manufacturer specified tolerances on wire width and spacing are $\pm 20\%$ [33]. In order to maximize the impact of these tolerances on the filters' response characteristics, we designed the metal wires within the notch filter to be the minimum trace width and spacing of approx 7 mils. Other design-independent tolerances, such as $\pm 10\%$ on board thickness, also impact the filters' response characteristics.

The NotchPUF is composed of a microstrip transmission line with series-inserted filter elements. Microstrip transmission lines possess a characteristic impedance that can be modeled by Equations (3) through (8), taken from Reference [34].

For $\frac{W}{h} < 1$:

$$\epsilon_{eff} = \frac{\epsilon_r + 1.0}{2} + \frac{\epsilon_r - 1.0}{2} \left[\frac{1}{\sqrt{1 + \frac{12h}{W}}} + 0.04 \left(1 - \frac{W}{h} \right)^2 \right] \quad (3)$$

Else:

$$\epsilon_{eff} = \frac{\epsilon_r + 1.0}{2} + \frac{\epsilon_r - 1.0}{2} \left[\frac{1}{\sqrt{1 + \frac{12h}{W}}} \right] \quad (4)$$

And:

$$Z_0 = \frac{120\pi}{2\sqrt{2}\pi\sqrt{\epsilon_r + 1}} \ln \left\{ 1 + \frac{4h}{W'} \left[\frac{14 + 8/\epsilon_{eff}}{11} \frac{4h}{W'} \right] + \sqrt{\left(\frac{14 + \frac{8}{\epsilon_{eff}}}{11} \right)^2 \left(\frac{4h}{W'} \right)^2 + \frac{1 + \frac{1}{\epsilon_{eff}}}{2} \pi^2} \right\} \quad (5)$$

Where:

$$W' = W + \Delta W' \quad (6)$$

$$\Delta W' = \Delta W \left(\frac{1.0 + \frac{1.0}{\epsilon_{eff}}}{2} \right) \quad (7)$$

$$\Delta W = \frac{t}{\pi} \ln \left[\frac{4e}{(t/h)^2 + \left(\frac{1/\pi}{w/t + 1.1} \right)^2} \right] \quad (8)$$

Here, ϵ_r is the relative dielectric constant, W is the width of the copper trace, t is the thickness of the copper track, and h is the thickness of the dielectric substrate. From these equations, we investigate variations in the following parameters:

- (A) Board thickness
- (B) Trace width
- (C) Substrate relative dielectric constant

While not a comprehensive list of parameters that exhibit variations in the PCB manufacturing process, these particular parameters have the largest tolerance levels, and therefore, are the most difficult to precisely control during manufacturing.

To better understand the impact of these parameters on the filters' response characteristics, we fabricated a set of 46 2-layer FR-4 boards and measured the actual board thickness and trace widths directly. In a second experiment, we fabricated another set of 2-layer FR-4 boards and measured the variations in the relative dielectric constant of the substrate. It should be noted that although two different test boards are used in our measurements, all PCBs came from the same 18 inch by 24 inch panel used as the source material in the manufacturing process.

5.1. Board Thickness Variations

To quantify the amount of variation in the fabricated boards, 10 board thickness measurements were taken at each of the 3 locations on each of the NotchPUF boards as shown in Figure 5. The position indicated with an "X" was not used because a board label on the bottom-side of the board (not shown) adds to the thickness and would skew the results. The ground plane on the bottom-side of the board is added using a 1 oz copper layer process, which is nominally 1.4 mils in thickness. The manufacturer specifies the nominal thickness of the FR-4 substrate as 1.6 mm (or 63 mils). In addition to these two layers, the solder mask on each side of the PCB also adds to the thickness. Although not specified by the manufacturer, these layers are typically approximately 0.8 mils to the thickness. Therefore, the nominal thickness of the PCB is 1.68 mm (66 mils) when all layers are considered.

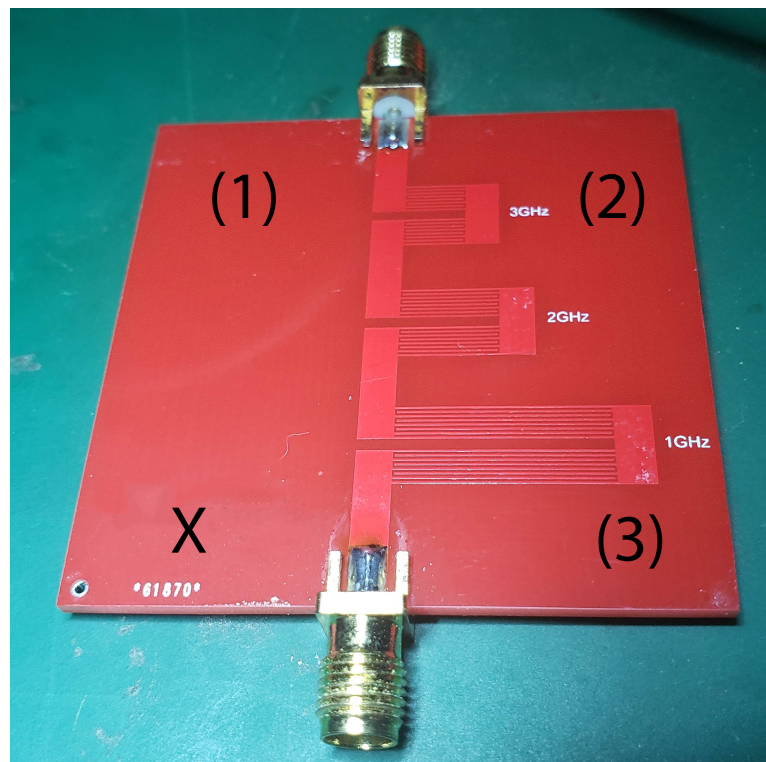


Figure 5. NotchPUF Board Measurement Locations.

Each position was measured with a calibrated micrometer with an accuracy of 0.0001". The three measurements from each board were averaged to give the overall thickness per board. The results of these measurements are shown in Figure 6. The average board thickness of all boards combined is 1.5375 mm which differs from the nominal value by approximately 9%. Although the thickness are smaller than the expected 1.68 mm (66 mils), they are still within the 20% allowable manufacturing tolerance.

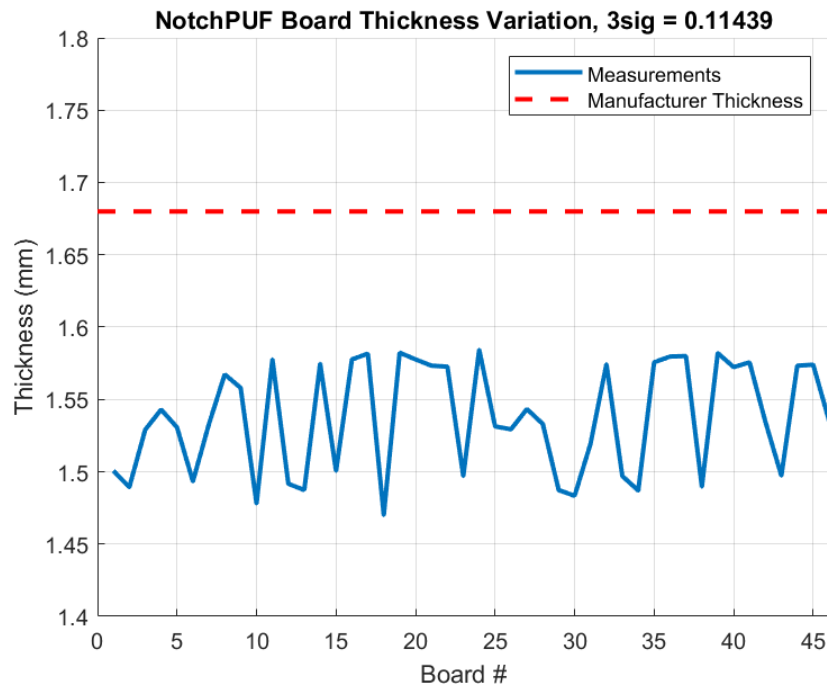


Figure 6. Board Thickness Graph.

5.2. Trace Width Variation

To analyze trace width variations, we used an image processing approach where the 3 filter structures were imaged under a microscope. All of the images were aligned via Matlab image processing code, and then the raw files were converted to gray-scale. The gray-scale images were processed with a tuned 'canny' edge detection filter that produced a low noise delineation of the copper traces. The widths of the traces were measured by counting the number of pixels between opposing edges.

The length of a pixel was determined using a microscope calibration slide with 0.01 mm line resolution. The calibration slide was imaged with the same zoom and focus levels that were used to image the NotchPUF structures. The measurements were divided by the pixel widths of the calibration sources to derive an estimate of the pixel length. From these measurements, each pixel was determined to be .002217 mm (or 2.217 μm).

The distribution of trace widths obtained from these measurements are shown in Figure 7. As noted earlier in reference to W2 in Figure 2, the designed finger trace widths is 0.2 mm. The title bar indicates that the 3σ variation of the trace widths is approximately 0.0302 mm. The average trace width (not shown) is 0.1930 mm, which is slightly smaller than the design width of 0.2 mm. These results show that the finger trace widths vary by approx. 15%, which are again within the manufacturing tolerance of 20%. This same amount of variation (0.03 mm) was observed on both lengths L3 and W1. From simulations, this variation was determined to have negligible effect on the NotchPUF response when compared to the finger width.

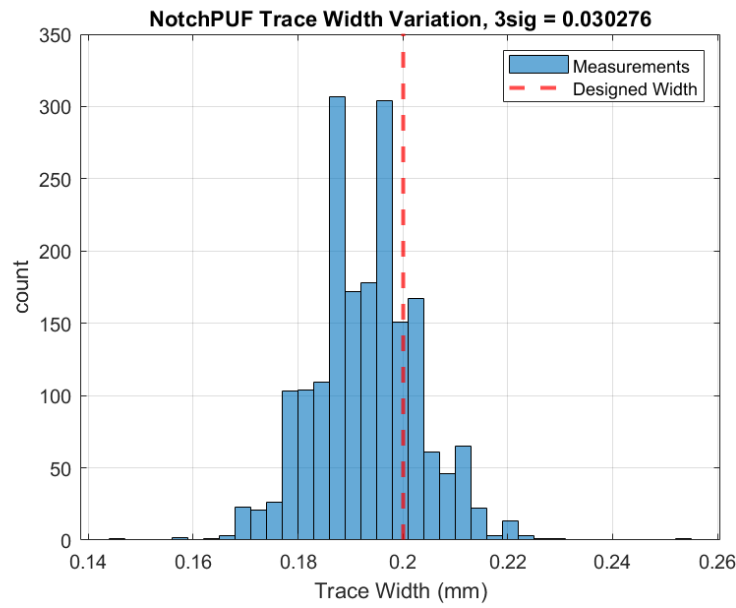


Figure 7. Trace Thickness Graph.

5.3. Substrate Relative Dielectric Constant Variation

To determine the substrate relative dielectric variation, measurements were taken on a different set of 20 PCBs which included a specialized trace configuration. On this PCB, two 50-Ω microstrip transmission lines are copper etched with lengths 50 mm and 100 mm, respectively. A photo of this board is shown in Figure 8. We use an Agilent 8753E vector network analyzer (VNA) to measure the difference between the electrical lengths of the two microstrips. The VNA applies a sequence of sine wave signals at specific frequencies to the input port and measures the response on the output port. The responses are then analyzed to derive the effective dielectric constant ϵ_{eff} of the microstrip structure as a function of frequency using Equations (9)–(11). For a microstrip structure, part of the electric field is in air and a part is in the dielectric. If the dielectric constant of the material is ϵ_r , the effective dielectric constant ϵ_{eff} must be less than ϵ_r , that is, between 1 and ϵ_r , because part of the electric field is in air and the dielectric constant of air is 1 [35].

$$\Delta\phi = 2\pi f(\Delta l_p) \frac{\sqrt{\epsilon_{eff}}}{c} \quad (9)$$

Where:

$$\Delta l_p = l_{p1} - l_{p2} \quad (10)$$

And

$$\Delta l_e = \sqrt{\epsilon_{eff}} * \Delta l_p \quad (11)$$

In these equations, $\Delta\phi$ is the transfer phase difference through the two lines at a particular frequency, Δl_p is the difference between the physical lengths and Δl_e is the electrical lengths of the lines. Our test board setup shown in Figure 8 which includes two microstrip lines of different lengths allows the impact of the SMA connectors on the response to be removed because all 4 cable-to-microstrip transitions are identical. This is achieved through subtraction when computing Δl_e in Equation (11) [36]. This method has been shown to be capable of accurately measuring the dielectric constant of a substrate with an error margin between 0.5% and 1.0% [36]. We observed a variation of approx. 4.7% in the effective dielectric constant of the microstrip structure. Table 2 gives the average $\Delta\phi$ and ϵ_{eff} computed using data from all 20 PCBs for a range of frequencies between 1.0 and 4.0 GHz. The 3σ for ϵ_{eff} is shown in the right-most column.

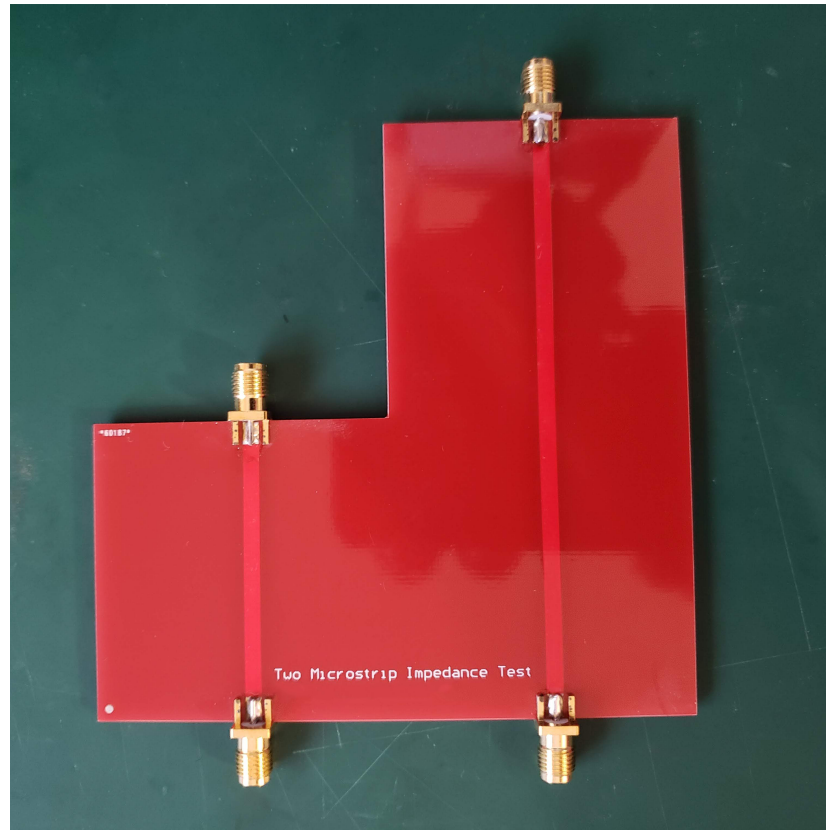


Figure 8. Two Microstrip Dielectric Constant Experiment.

Table 2. Average Measurement of $\Delta\phi$ (degrees) and ϵ_{eff} Variations in FR-4 ($\epsilon_r = 4.8$) Substrate.

f (GHz)	$\Delta\phi$ (Measured)	ϵ_{eff} (Calculated)	3σ
1.0	114.59°	3.63	0.17
1.5	174.15°	3.73	0.17
2.0	231.50°	3.72	0.17
2.5	288.13°	3.68	0.18
3.0	345.10°	3.67	0.19
3.5	400.03°	3.62	0.15
4.0	463.06°	3.71	0.22

From these measurements, we were then able to determine ϵ_r of the substrate around the test frequency using an analysis of the microstrip propagation constant. The following system of equations can be solved to derive the relative dielectric constant of the FR4 substrate: [37].

$$\epsilon_{eff}(u, \epsilon_r) = \frac{\epsilon_r + 1}{2} + \frac{\epsilon_r - 1}{2} \left(1 + \frac{10}{u}\right)^{-a(u)b(\epsilon_r)} \quad (12)$$

$$a(u) = 1 + \frac{1}{49} \ln \frac{u^4 + (u/52)^2}{u^4 + 0.432} + \frac{1}{18.7} \ln \left[1 + \left(\frac{u}{18.1}\right)^3\right] \quad (13)$$

$$b(\epsilon_r) = 0.564 \left(\frac{\epsilon_r^{-0.9}}{\epsilon_r + 3}\right)^{0.053} \quad (14)$$

$$u = w/h \quad (15)$$

Here, u is the strip width normalized with respect to substrate height. We used Matlab [38] to iteratively solve this system of equations for different values of ϵ_r until a match occurred to the measured values ϵ_{eff} .

The calculated ϵ_r was then analyzed and compared between all 20 boards and shown to have Approx 5.3% variation amongst the population of PCBs. ϵ_r was then averaged to indicate the expected dielectric constant for the substrate of the entire PCB panel. These are summarized in Table 3 below.

Table 3. Variation of ϵ_r between boards in FR-4 ($\epsilon_r = 4.8$) Substrate.

f (GHz)	ϵ_r (Calculated)	3σ
1.0	4.86	0.26
1.5	5.02	0.25
2.0	4.99	0.25
2.5	4.93	0.27
3.0	4.91	0.27
3.5	4.85	0.22
4.0	4.98	0.33

5.4. Summary

The previous three sections provide evidence that manufacturing variations in PCBs are significant, and therefore, can serve as a source of randomness for PUFs. We summarize our findings as follows:

Board Thickness: The average board thickness (with the bottom copper layer) was shown to be 1.5375 mm which is approximately 9.2% thinner than the manufacturer specified thickness of 1.68 mm. More importantly, the average 3σ variation across boards was measured to be 0.1143 mm or approximately 7.4%. Although relatively small in comparison to other sources of variations, these board thickness variations impact the characteristic impedance of the microstrip line within the NotchPUF, and therefore add to the variations in the measured response discussed below in the experimental results.

Trace Width Variation: The average width of a trace was determined to be approximately 0.1930 mm with a $3\sigma = 0.0302$ mm. Although the average differs by only 3.6% from the drawn width, the 3σ variation is much larger at approximately 15%. Similar to board thickness variations, trace width variations impact the characteristic impedance of the transmission line. As we show in the next section, trace width variations have a significant impact on the center frequencies of the notch filters.

Substrate Relative Dielectric Variation: We computed the average value for ϵ_r at all frequencies to be approx. 4.93, which is approximately 2.7% greater than the manufacturer claimed value of 4.8. The mean 3σ was computed to be 0.26, which represents a 5.3% variation. Although the level of variations here are smaller than the former two, dielectric variations also impact characteristic impedance, and add to the randomness we observe in the center frequency and magnitude of the response characteristics of the NotchPUF.

6. Experimental Results

6.1. Experimental Setup

The proposed NotchPUF is fabricated on a 50 mm by 50 mm, 2-layer FR-4 PCB with a thickness of 1.6 mm and a relative permittivity ϵ_r of 4.8. We fabricated 46 boards and used an Agilent 8753E VNA and an 85047A S-Parameter test set to make the measurements. Because the VNA is limited to 1601 points of data for a given center frequency and span, three separate measurements were taken at frequency spans of 1 GHz, with center frequencies set to 1, 2 and 3 GHz. At each center frequency, we repeated the testing to obtain 200 samples. A set of 20 sample averages were computed from this raw data by averaging 10 consecutive measurements. Figure 9 shows the instrumentation setup with the Agilent VNA tasked with data collection and the HP 85047A applying the S-Parameter test set to the NotchPUF PCB connected between Ports 1 and 2.

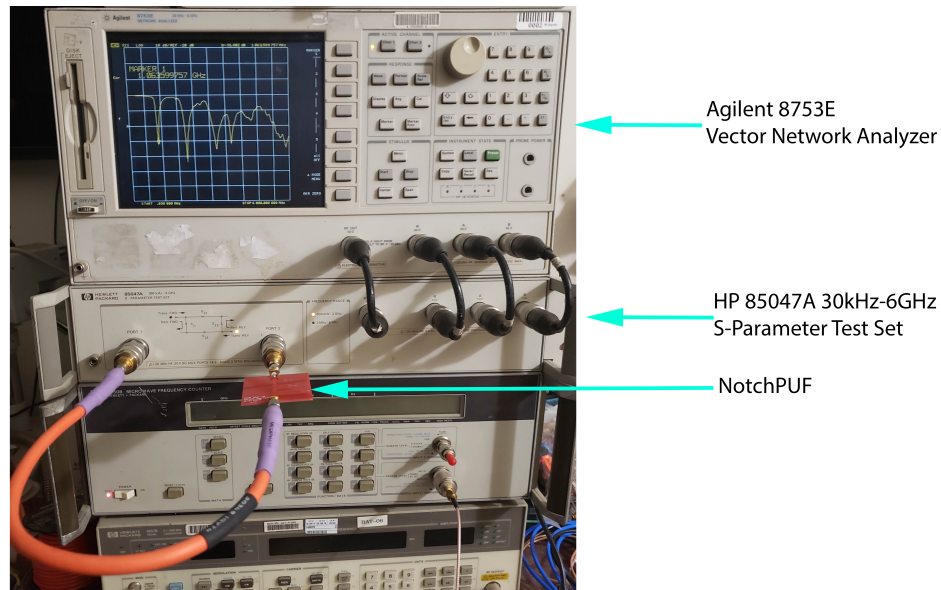


Figure 9. Experimental Test Setup.

Prior to data collection, a full 2-port calibration was performed on the VNA with an open, load and short calibration standard suite of tests. Calibration is designed to reduce instrumentation error including directivity error, crosstalk, source match error, frequency response reflection tracking error, and frequency response transmission tracking error. Calibration records data within the instrument to address a total of twelve error terms, six associated with the forward direction tests and six with the reverse direction tests. The same phase stable cable was used during calibration and NotchPUF testing, which further reduced instrumentation-related noise. The 2 SMA connectors on each board were also analyzed to ensure minimal impact to the NotchPUF measurements. All connectors were validated to have a worst case insertion loss SMA_{IL} as shown in Equation (16).

$$SMA_{IL} = 0.05\sqrt{f(\text{GHz})} \text{ dB}. \quad (16)$$

After calibration, S_{21} measurements were taken from each board and post-processed to extract a set of response characteristics including center rejection frequency, maximum insertion loss (lowest -dB), fractional bandwidth (FBW), and points of maximum roll-off (slope of curve). The values of these parameters were then combined with the frequency and insertion loss after applying a modulus technique similar to that in References [10,39]. We use a modulus operation to ensure an unbiased response bitstring, defined here as a 15-bit ID for each NotchPUF PCB, as we explain further below.

The statistical quality of the bitstrings produced by NotchPUF are evaluated using several statistical metrics. In particular, we compute inter-board Hamming distance which measures the uniqueness of the IDs. We also compute intra-board Hamming distance using bitstrings generated by the same NotchPUF PCB to determine how well each NotchPUF is able to reproduce the bitstring. We compare the computed statistics with the ideal values of 50% for uniqueness and 0% for reproducibility.

6.2. Signal Analysis and Bitstring Generation

First, we report on the average frequency and S_{21} insertion loss generated by each NotchPUF PCB. The rejection center frequency and the insertion loss are plotted as separate curves with one point for each of the 46 boards identified along the x-axis in Figure 10. The rejection frequencies for the PCBs varies above and below the target rejection frequency, for example, 1 GHz as shown on the y-axis in Figure 10a. The results of the NotchPUF measurements are summarized in Table 4 below. The average center rejection frequency for each filter represents approximately a 4.4% deviation from

the target frequencies of 1, 2 and 3 GHz. The FBW 3σ for each structure is 67.99 MHz, 94.73 MHz, and 187.75 MHz. The variations that occur in each of these response parameters are used to define a 15-bit identifier for each PCB as we discuss in the following.

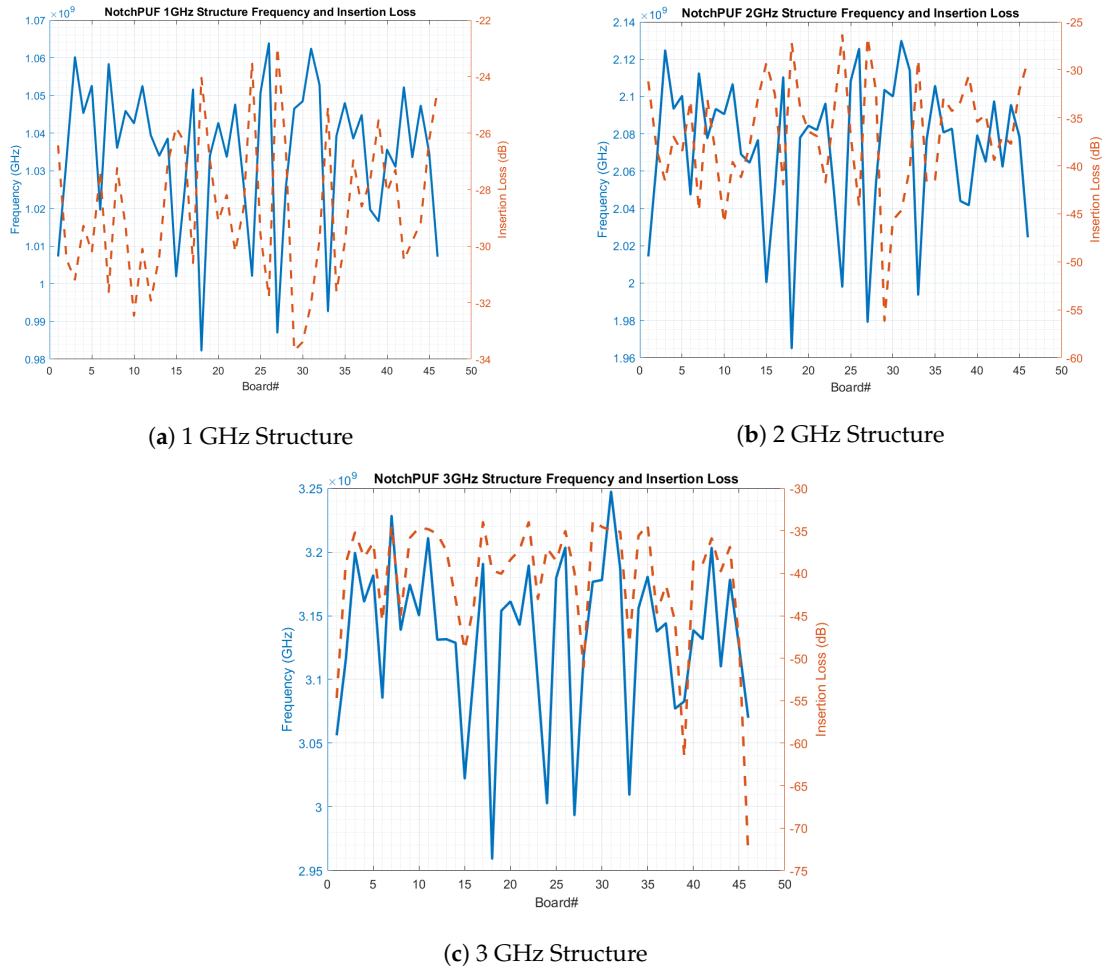


Figure 10. Frequency and Insertion Loss for NotchPUF PCBs.

Table 4. NotchPUF Parameter Results.

	Structure		
	1 GHz	2 GHz	3 GHz
Center rejection frequency	1.034 GHz	2.072 GHz	3.134 GHz
Rejection Frequency 3σ	59.18 MHz	118.4 MHz	192.3 MHz
Insertion Loss 3σ	−7.87 dB	−17.92 dB	−23.27 dB
FBW	304.64 MHz	561.67 MHz	414.54 MHz

We create a graph in Figure 11 which plots insertion loss (y-axis) against frequency (x-axis) for each of the 46 boards as a means of converting the measured values into a bitstring. The data shown here is for the 2 GHz filters, but similar graphs can be created using the 1 and 3 GHz data. Each PCB is associated with one cluster of points in the graph, where the points in the clusters represent the 20 sample averages discussed earlier. The sample averages allow the noise levels associated with the measurements to be compared directly to magnitude of the variations that occur between PCBs in the population.

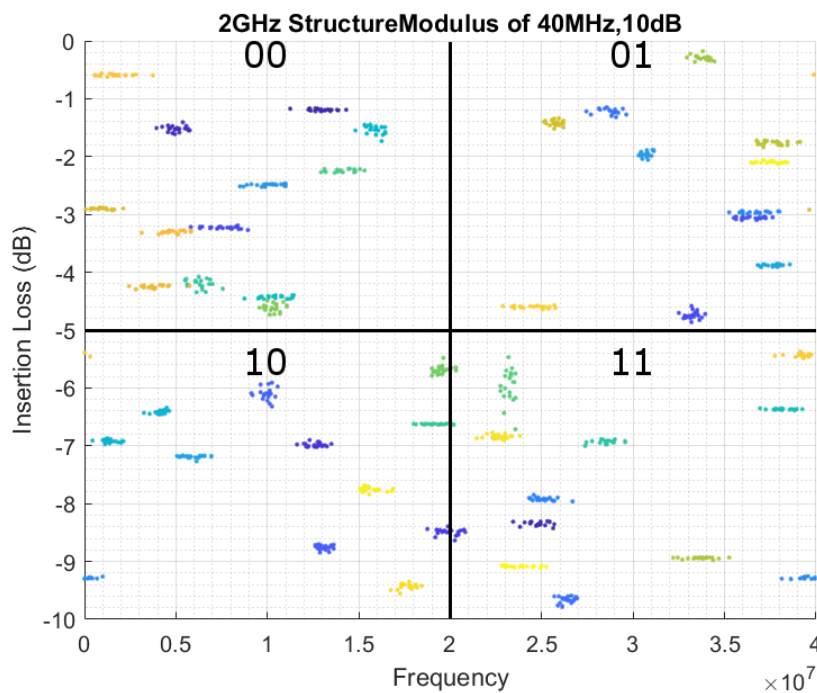


Figure 11. 2 GHz Modulus Operation Results.

The variations that occur in the filters' response are very large, which enables more than one bit to be obtained from the measurements. The data plotted in Figure 11 is reduced in amplitude over the original values by applying a modulus operation, which effectively wraps the values into a smaller region. The modulus operation accomplishes two goals. First, it translates the (x,y) points associated with each PCB into a fixed size region. In our example, the region is bounded by 0 to 40 MHz along the x-axis and -10 to 0 along the y-axis. The fixed size region in turn enables boundaries to be defined for the assignment of bit values, as shown by the four quadrants in the figure. Second, the modulus removes bias that occurs across PCBs but preserves the within-PCB variations, which improves randomness in the generated bitstrings.

From Figure 11, there are cases in which the cluster of points for each PCB cross over a boundary. When this occurs during regeneration in the field, bit-flip errors will occur in the bitstrings. Although the bit-flip errors occur in our experiments because of measurement noise, we also expect this to occur if the temperature of the environment changes. In either case, we propose to use error correcting techniques to deal with bit-flip errors as others have done in previous work [40].

Applying this process to the data from the three filters on each PCB generates six bits of the PCB's ID. Three additional bits are obtained by processing the FBW data, and another six bits using the maximum rolloff variation on each side of the S_{21} response. Therefore, a total of 15 bits can be generated for each PCB using the three filters.

A bitstring of size 80-bits is traditionally considered the smallest acceptable size for authentication operations. The size of the structure containing all three filters as shown in Figure 5 is $31\text{ mm} \times 23.3\text{ mm}$. A 2×3 array of the NotchPUF structures would be able to generate 90 bits and would occupy a board area of $70\text{ mm} \times 62\text{ mm}$, less than a $3'' \times 2.5''$ area of board real estate. Although 18 notch filter structures are included in this array, the number of required inputs and outputs is only 6 because of the series connection strategy.

We would also like to point out that the NotchPUF does not need to be implemented on the top or bottom layers of the PCB, as we have done here. In fact, a better location would be to embed them in a buried layer within a multi-layer PCB. A buried implementation would increase the difficulty of physical tampering. Moreover, the widths of the notch filters' wires, and overall size, would decrease because of their close proximity to adjacent ground planes.

6.3. Bitstring Analysis

The uniqueness and reliability characteristics of the 15-bit bitstrings from the 46 boards were evaluated using inter-PCB and intra-PCB hamming distance (HD). The HD between two n-bit bitstrings x and y is defined as

$$HD(x, y) = \sum_{i=1}^n (x_i \oplus y_i). \quad (17)$$

Figure 12 plots the inter-PCB hamming distance distribution while Figure 13 plots intra-PCB distribution. To increase statistical significance, the distributions were created using all 200 measurements taken per NotchPUF PCB. The mean inter-PCB HD from Figure 12 is 48.7%, which is close to the ideal value 50%. From Figure 13, the intra-PCB HD is computed as 2.8%, which is well within the error correction capabilities of error correction methods. We observed larger numbers of bit-flip errors for the 3 GHz filter, suggesting that filters with higher rejection frequencies are more sensitive to noise.

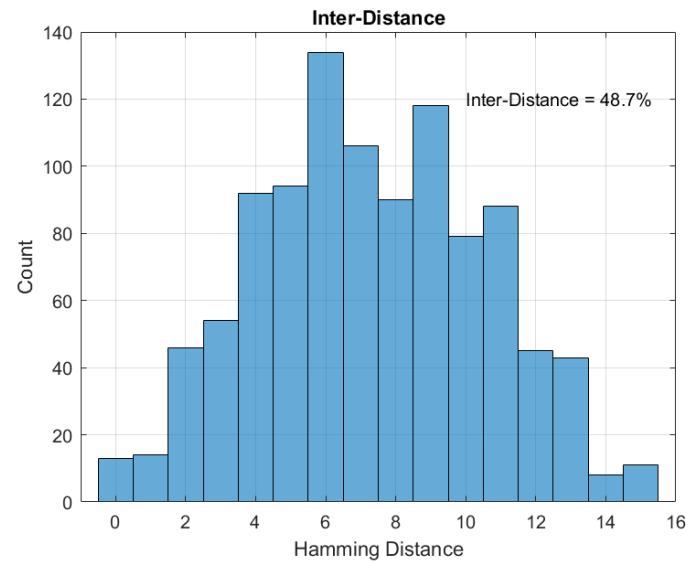


Figure 12. Inter-Distance.

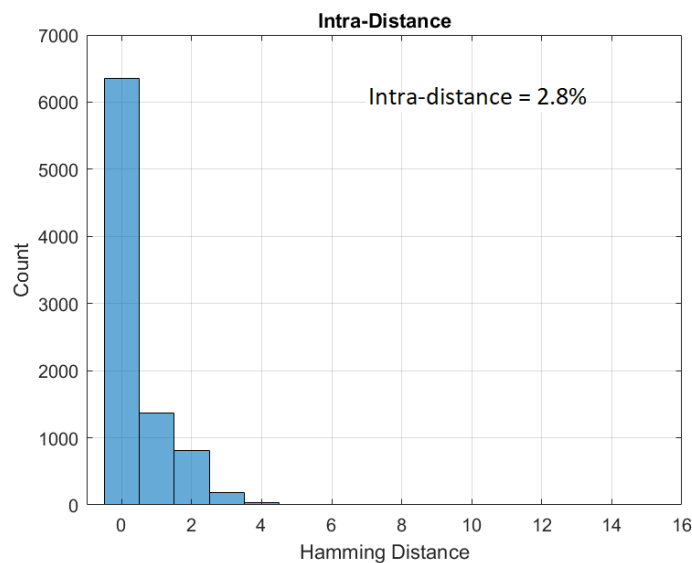


Figure 13. Intra-Distance.

FR-4 is an inexpensive board material and is therefore very popular. However, the signal losses are much higher than they are for more specialized (and expensive) board materials, such as polytetrafluoroethylene (PTFE), which has excellent dielectric properties at microwave frequencies. However, we expect FR-4 will be the material of choice in most cases, and therefore recommend that notch filter designs be constrained to operate below 3 GHz for repeatability.

The experiments here were only performed at nominal temperature (25 °C). As ambient temperature increases, the FR-4 PCB dielectric constant increases approximately 4% from −30 °C to 105 °C [41]. This change in ϵ_r results in a corresponding linear change to the center rejection frequencies of the NotchPUF. Simulation results illustrating the temperature effect on ϵ_r are shown in Figure 14. The change in center frequency is proportional to the percentage change of the relative dielectric change (5%). For example, the value of ϵ_r is 4.3 at room temperature (25 °C) and is 4.6 at 105 °C. The shift in ϵ_r introduced by changes in temperature can be calibrated by offsetting the measured center frequency. However, this requires that the PCB have components capable of measuring the ambient temperature or that the PCB is able to store a set of reference “room temperature” values for each filter in a non-volatile memory.

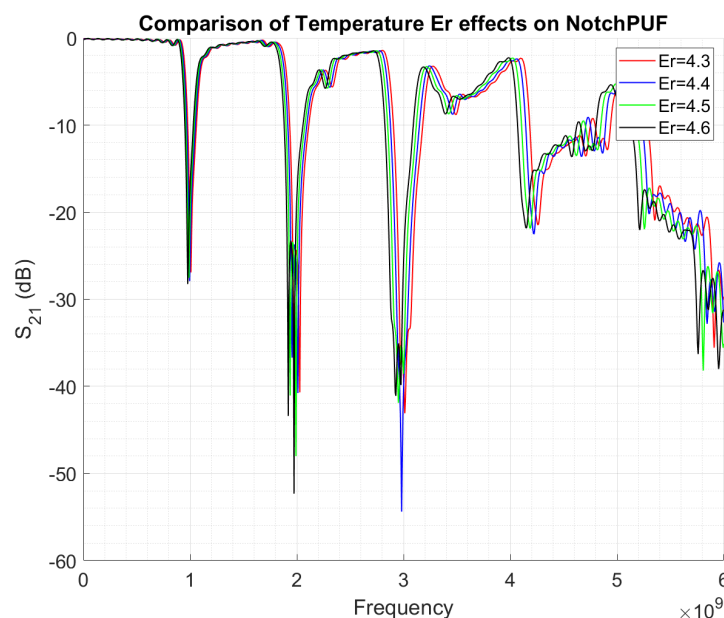


Figure 14. Changes in ϵ_r with Temperature.

7. Conclusions

In this paper, a novel PUF called NotchPUF is proposed that utilizes PCB variations in notch filter structures for the creation of unique IDs for PCBs. The proposed design creates a series connected set of notch filters with different rejection frequencies to reduce the area overhead of the PUF architecture. Simulation experiments are used to tune wire sizes and other parameters associated with a set of three filter designs with target rejection frequencies of 1, 2 and 3 GHz. Fabricated PCBs are designed and tested to measure the magnitude of the variations associated with the fundamental elements of PCBs including wire width, substrate thickness and dielectric constants. Data from the PCBs are processed into bitstrings using a novel quadrant-based modulus scheme, and the bitstrings from 46 PCBs are analyzed using standard statistical bitstring quality tests to illustrate that high levels of randomness and uniqueness can be achieved from the NotchPUFs in our proof-of-concept experiments.

Future designs of the NotchPUF could benefit from the added protection of being embedded into a multi-layer PCB. Further, additional NotchPUF structures would allow bitstrings of a greater length to be produced. While the current bitstring generation techniques are highly effective, new techniques

for bitstring generation of the raw NotchPUF response waveform could prove highly valuable. Various machine learning or neural network approaches can provide high accuracy and noise rejection traits that are valuable for PUFs that are susceptible to errors from noise.

Author Contributions: Conceptualization, M.M.; methodology, M.M. and J.P.; software, M.M.; validation, M.M.; formal analysis, M.M.; investigation, M.M.; writing—original draft preparation, M.M.; writing—review and editing, M.M. and J.P.; visualization, M.M.; supervision, J.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Center, Global Innovation Policy. *Measuring the Magnitude of Global Counterfeiting Creation of a Contemporary Global Measure of Physical Counterfeiting*; U.S. Chamber of Commerce: Washington, DC, USA, 2016; p. 4.
- Lofstrom, K.; Daasch, W.; Taylor, D. IC identification circuit using device mismatch. In Proceedings of the 2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers, San Francisco, CA, USA, 9 February 2000; pp. 372–373. [\[CrossRef\]](#)
- Pappu, R.; Recht, B.; Taylor, J.; Gershenfeld, N. Physical one-way functions. *Science* **2002**, *297*, 2026–2030. [\[CrossRef\]](#) [\[PubMed\]](#)
- Gassend, B.; Clarke, D.; van Dijk, M.; Devadas, S. Controlled physical random functions. In Proceedings of the Computer Security Applications Conference, Las Vegas, NV, USA, 9–13 December 2002; pp. 149–160. [\[CrossRef\]](#)
- Majzoobi, M.; Koushanfar, F.; Potkonjak, M. Lightweight secure PUFs. In Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design, San Jose, CA, USA, 10–13 November 2008; pp. 670–673. [\[CrossRef\]](#)
- Qu, G.; Yin, C.E. Temperature-aware cooperative ring oscillator PUF. In Proceedings of the 2009 IEEE International Workshop on Hardware-Oriented Security and Trust, Francisco, CA, USA, 27 July 2009; pp. 36–42. [\[CrossRef\]](#)
- Maiti, A.; Schaumont, P. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. In Proceedings of the 2009 International Conference on Field Programmable Logic and Applications, Prague, Czech Republic, 31 August–2 September 2009; pp. 703–707. [\[CrossRef\]](#)
- Guajardo, J.; Kumar, S.; Schrijen, G.J.; Tuyls, P. Physical Unclonable Functions and Public-Key Crypto for FPGA IP Protection. In Proceedings of the 2007 International Conference on Field Programmable Logic and Applications, Amsterdam, The Netherlands, 27–29 August 2007; pp. 189–195. [\[CrossRef\]](#)
- Helinski, R.; Acharyya, D.; Plusquellic, J. A physical unclonable function defined using power distribution system equivalent resistance variations. In Proceedings of the 2009 46th ACM/IEEE Design Automation Conference, San Francisco, CA, USA, 26–31 July 2009; pp. 676–681.
- Ju, J.; Plusquellic, J.; Chakraborty, R.; Rad, R. Bit string analysis of Physical Unclonable Functions based on resistance variations in metals and transistors. In Proceedings of the 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, USA, 3–4 June 2012; pp. 13–20. [\[CrossRef\]](#)
- Ghosh, S.; Basak, A.; Bhunia, S. How secure are printed circuit boards against trojan attacks? *IEEE Des. Test* **2014**, *32*, 7–16. [\[CrossRef\]](#)
- Guo, Z.; Di, J.; Tehranipoor, M.M.; Forte, D. Obfuscation-based protection framework against printed circuit boards unauthorized operation and reverse engineering. *ACM Trans. Des. Autom. Electron. Syst. (TODAES)* **2017**, *22*, 54. [\[CrossRef\]](#)
- Bhunia, S.; Tehranipoor, M. *Hardware Security: A Hands-on Learning Approach*; Morgan Kaufmann: Burlington, MA, USA, 2018.
- Immler, V.; Obermaier, J.; König, M.; Hiller, M.; Sig, G. B-TREPID: Batteryless tamper-resistant envelope with a PUF and integrity detection. In Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 30 April–4 May 2018; pp. 49–56. [\[CrossRef\]](#)

15. Paley, S.; Hoque, T.; Bhunia, S. Active protection against PCB physical tampering. In Proceedings of the 2016 17th International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 15–16 March 2016; pp. 356–361. [\[CrossRef\]](#)
16. Fujimoto, D.; Nin, S.; Hayashi, Y.I.; Miura, N.; Nagata, M.; Matsumoto, T. A Demonstration of a HT-Detection Method Based on Impedance Measurements of the Wiring Around ICs. *IEEE Trans. Circuits Syst. II Express Briefs* **2018**, *65*, 1320–1324. [\[CrossRef\]](#)
17. Aysu, A.; Gaddam, S.; Mandadi, H.; Pinto, C.; Wegryn, L.; Schaumont, P. A design method for remote integrity checking of complex PCBs. In Proceedings of the 2016 Design, Automation Test in Europe Conference Exhibition (DATE), Dresden, Germany, 14–18 March 2016; pp. 1517–1522.
18. Frazier, P.D.; Gilmore, E.T.; Collins, I.J.; Samotshozo, W.E.; Chouikha, M.F. A Novel Counterfeit Detection Approach for Integrated Circuit Supply Chain Assurance. *J. Hardw. Syst. Secur.* **2018**, *2*, 240–250. [\[CrossRef\]](#)
19. Iqbal, T.; Wolf, K.D. PCB Surface Fingerprints Based Counterfeit Detection of Electronic Devices. *Electron. Imaging* **2017**, *2017*, 144–149. [\[CrossRef\]](#)
20. Hamlet, J.R.; Martin, M.T.; Edwards, N.J. Unique signatures from printed circuit board design patterns and surface mount passives. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–6. [\[CrossRef\]](#)
21. Hennessy, A.; Zheng, Y.; Bhunia, S. Jtag-based robust pcb authentication for protection against counterfeiting attacks. In Proceedings of the 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, China, 25–28 January 2016; pp. 56–61.
22. Quadir, S.E.; Chandy, J.A. Low Pass Filter PUF: Authentication of Printed Circuit Boards Based on Resistor and Capacitor Variations. *Int. J. High Speed Electron. Syst.* **2018**, *27*, 1840021. [\[CrossRef\]](#)
23. Zheng, X.; Zhang, Y.; Zhang, J.; Hu, W. Design Impedance Mismatch Physical Unclonable Functions for IoT Security. *Act. Passiv. Electron. Components* **2017**, *2017*, 4070589. [\[CrossRef\]](#)
24. Wei, L.; Song, C.; Liu, Y.; Zhang, J.; Yuan, F.; Xu, Q. BoardPUF: Physical Unclonable Functions for printed circuit board authentication. In Proceedings of the 2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), Austin, TX, USA, 2–6 November 2015; pp. 152–158. [\[CrossRef\]](#)
25. Zhang, F.; Hennessy, A.; Bhunia, S. Robust counterfeit PCB detection exploiting intrinsic trace impedance variations. In Proceedings of the 2015 IEEE 33rd VLSI Test Symposium (VTS), Napa, CA, USA, 27–29 April 2015; pp. 1–6. [\[CrossRef\]](#)
26. Alley, G.D. Interdigital capacitors and their application to lumped-element microwave integrated circuits. *IEEE Trans. Microw. Theory Tech.* **1970**, *18*, 1028–1033. [\[CrossRef\]](#)
27. Hong, J.S.G.; Lancaster, M.J. *Microstrip Filters for RF/Microwave Applications*; John Wiley & Sons: Hoboken, NJ, USA, 2004; Volume 167.
28. Yang, R.Y.; Weng, M.H.; Hung, C.Y.; Chen, H.J.; Houng, M.P. Novel compact microstrip interdigital bandstop filters. *IEEE Trans. Ultrason. Ferroelectr. Freq. Control* **2004**, *51*, 1022–1025. [\[CrossRef\]](#) [\[PubMed\]](#)
29. Alkanhal, M.A. Compact bandstop filters with extended upper passbands. *Act. Passiv. Electron. Components* **2008**, *2008*, 356049. [\[CrossRef\]](#)
30. Meesomklin, S.; Chomtong, P.; Akkaraekthalin, P. A Compact multiband BPF using step-impedance resonators with interdigital capacitors. *Radioengineering* **2016**, *25*, 258–267. [\[CrossRef\]](#)
31. Studio, C.M. ver. 2018. CST AG Bad Nauheimer Str **2018**, *19*, 21.
32. Landers, T.L.; Brown, W.D.; Fant, E.; Malstrom, E.M.; Schmitt, N.M. *Electronics Manufacturing Processes*; Prentice Hall: Upper Saddle River, NJ, USA, 1994.
33. Sunstone. Manufacturing Tolerances. August 2019. Available online: <https://www.sunstone.com/pcb-manufacturing-capabilities/tolerances> (accessed on 3 April 2020).
34. Wadell, B.C. *Transmission Line Design Handbook*; Artech House: Norwood, MA, USA, 1991.
35. Shukla, V. *Signal Integrity for PCB Designers*; Reference Designer: Foxboro, MA, USA, 2009.
36. Das, N.K.; Voda, S.M.; Pozar, D.M. Two methods for the measurement of substrate dielectric constant. *IEEE Trans. Microw. Theory Tech.* **1987**, *35*, 636–642. [\[CrossRef\]](#)
37. Hammerstad, E.; Jensen, O. Accurate models for microstrip computer-aided design. In Proceedings of the 1980 IEEE MTT-S International Microwave Symposium Digest, Washington, DC, USA, 28–30 May 1980; pp. 407–409.
38. *MATLAB version 9.3.0.713579 (R2017b)*; The Mathworks, Inc.: Natick, MA, USA, 2017.

39. Che, W.; Martin, M.; Pocklassery, G.; Kajuluri, V.; Saqib, F.; Plusquellic, J. A privacy-preserving, mutual PUF-based authentication protocol. *Cryptography* **2017**, *1*, 3. [[CrossRef](#)]
40. Yu, M.D.; Devadas, S. Secure and Robust Error Correction for Physical Unclonable Functions. *IEEE Des. Test Comput.* **2010**, *27*, 48–65. [[CrossRef](#)]
41. Heinola, J.M.; Latti, K.P.; Silventoinen, P.; Strom, J.P.; Kettunen, M. A new method to measure dielectric constant and dissipation factor of printed circuit board laminate material in function of temperature and frequency. In Proceedings of the 9th International Symposium on Advanced Packaging Materials: Processes, Properties and Interfaces (IEEE Cat. No. 04TH8742), Atlanta, GA, USA, 24–26 March 2004; pp. 235–240.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).