Investigation of unique broadband nonlinear RF response of electronic devices

Ashish Mishra[1], Chen Song[2], Wenyao Xu[2], Changzhi Li[1]

[1]Electrical and Computer Engineering, Texas Tech University, Lubbock, TX, 79409, USA

[2]Department of Computer Science & Engineering, State University of New York, Buffalo, NY, USA

***Abstract* – Modern electronic devices with the same part number fabricated by the same company show different nonlinear responses when probed by broadband radio frequency (RF) signals. The difference in the response is primarily due to process variation during device fabrication. In this paper, the individual variation of device intermodulation response is studied. Experiments are performed to demonstrate that devices with the same design and layout can be differentiated based on their broadband intermodulation responses. This makes it possible to use RF technology to remotely identify and authenticate electronic devices.**

***Index Terms* — Nonlinear measurement, process variation, broadband, third order intermodulation, intermodulation.**

I. Introduction

Security became a major concern for government and civilian life in recent years. Related topics include cyber security and device counterfeiting, etc. Hacking attempts can be reduced to a large extent if authorized devices can be remotely distinguished from the counterfeiting ones. There are many methods available in the market for device authentication for integrated circuit chips (IC) and printed circuit boards (PCB). Examples include impedance measurement, DNA marking, RFID etc. DNA marking is limited to authenticating detect the individual components (specifically chips) only and not the PCB [1]. RFID is considered more robust among the traditional ones, but these RFIDs can easily be cloned. Cloned RFIDs are hard to distinguish from authentic ones. Advanced methods to detect process variations such as Physical Unclonable Function (PUF) cannot be used for authentication on PCB level circuits as they require special measurement setup and takes a long time to perform authentication. [2].

The harmonics generated by the devices can also be used to differentiate the device of interest from the counterfeit ones [3]. But the harmonics measurement method suffers from two drawbacks. First, there is stringent linearity requirement on the detector front-end. Since conventional filters cannot meet the linearity requirement, expensive diplexers are used to isolate the secondary harmonics from the transmitter [4]. Second, the detector has to accommodate different bands for the transmitted and received signals [3]. For example, if the fundamental tone is located in the frequency band centered at *f*, then the second harmonic will be located in the frequency band around *2f*.

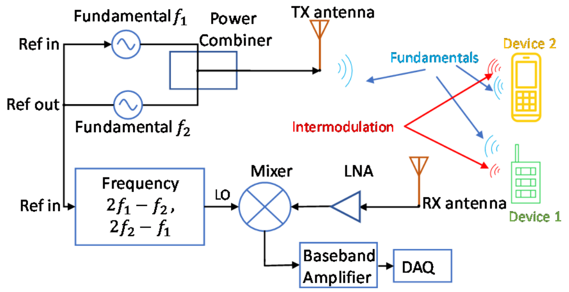


Fig. 1. Block diagram illustrating remote device identification and authentication based on nonlinear measurement.

On the other hand, for intermodulation, the probing signal and the returned signal are located in the same band. Also, the linearity requirement of the transmitter can be relaxed. So, the cost of the system comes down as it eliminates the use of high performance filters as the frequency selectivity is achieved by synchronized signal synthesizers. All these makes the system easy to setup and operate.

In this paper, intermodulation is utilized to distinguish circuits with the same design and same layout. Two devices are exposed to the same two-tone RF signals scanned from 3 GHz to 11 GHz. The return fundamental and intermodulation tones are measured, and the peak positions were noted for the fundamental and intermodulation tones. The paper is divided into four sections. Section II discusses intermodulation-based detection and the operation of the system. Section III presents the measurement setup and experimental results. A conclusion is drawn in Section IV

II. Detection Theory

When two fundamental tones are passed through a nonlinear device, intermodulation generates additional frequency tones. For example, if two fundamental tones f_1 and f_2 are fed into a nonlinear device, additional tones such as $2f_1$-f_2 and $2f_2$-f_1 (third order intermodulation), and $3f_1$-$2f_2$, $3f_2$-$2f_1$ (fifth order intermodulation) will be formed. Generally speaking, the amplitude of the intermodulation

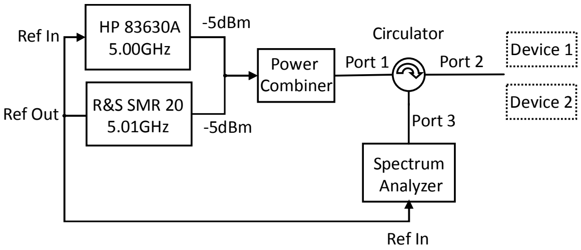


Fig. 2. Simplified measurement Setup.

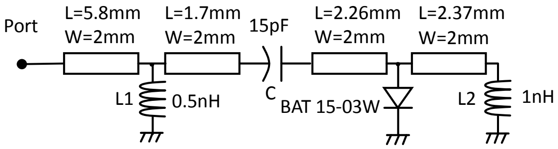
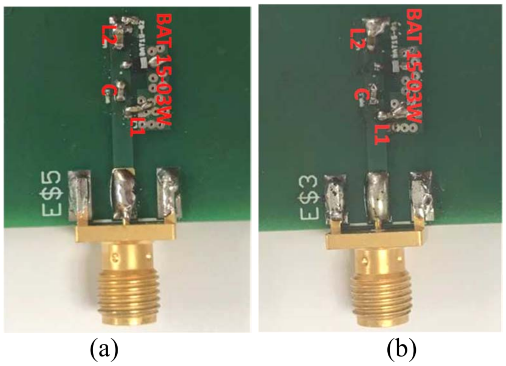


Fig. 3. Device Schematic.



(a) (b)

Fig. 4. Two tested devices with the same design and layout.
(a) Device 1, (b) Device 2.

components reduces as we go higher up in order [5]. In this paper, we consider the third order intermodulation to characterize the response of the devices at various frequencies.

Figure 1 illustrates remote device identification and authentication based on nonlinear measurement performed by a nonlinear detector. Two fundamental tones of frequencies f_1 and f_2 will be transmitted from the transmitting antenna of the detector. Electronic devices such as mobile phones will receive these frequency tones. Because these devices have many nonlinear components such as diodes, transistors inside, they will generate additional frequency tones at $2f_1$-f_2 and $2f_2$-f_1. Some of the generated tones will leak back to space and be captured by the receiving antenna of the detector. Then the third-order intermodulation tones will be amplified and down-converted to baseband by the nonlinear detector. Since these electronic devices produce different levels of intermodulation tones at various frequencies due to process variations and parasitic, they can be distinguished based on the broadband measurement result from the detector. In this paper, a simplified experiment is carried out to demonstrate that the nonlinear RF response of two devices vary even when they have the same design and layout.

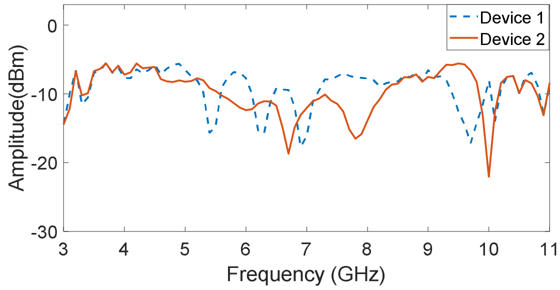


Fig. 5. Lower Fundamental tone response of the devices *(f_1)*.

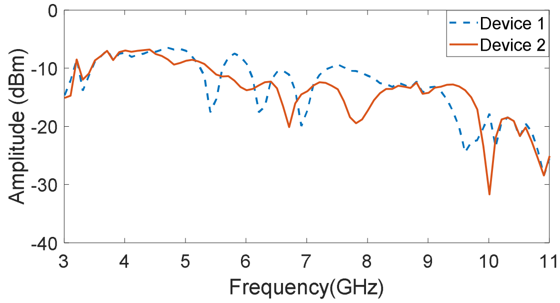


Fig. 6. Higher fundamental tone response of the devices (f_2).

III. Experimental Setup and Test Result

Figure 2 shows a simplified setup to measure the fundamental and intermodulation responses of the device under test (DUT). Here, two fundamental tones are sent to the device through a power combiner and a circulator. The power of the fundamental and intermodulation tones reflected from the DUT are observed with a spectrum analyzer (Rhode and Schwarz FSU). The power level of the signal generators is calibrated to make the fundamental tones equal at 5 GHz. A calibration was performed at the beginning of measurement to set the power of probing fundamental tones to be -5 dBm. Then the frequencies of the two tones were swept from 3 GHz to 11 GHz, with a 10-MHz difference between the two tones. The power of the reflected fundamental and intermodulation tones were recorded from the spectrum analyzer for the two devices.

Figure 3 shows the schematic of the two devices. The circuit was originally designed as a narrow-band matching circuit for diode BAT 15-03W at 0V bias at 5.8 GHz on FR4 substrate. Figs. 4 (a) and (b) are the images of the devices used in measurement. To maintain the coherence, the signal generators and the spectrum analyzer shared the same reference during measurement.

Figure 5 shows the power level of the reflected lower fundamental tone, and the reflected higher fundamental tone is shown in Fig. 6. From the measurement result of fundamental tones, both the devices show approximately the same RF behavior. At 10 GHz, the difference in the fundamental tone (i.e., about 15dB) is the largest for both

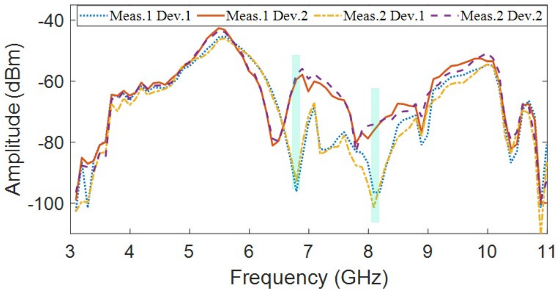


Fig. 7. Lower third order intermodulation *(2f*1*-f*2*)*.

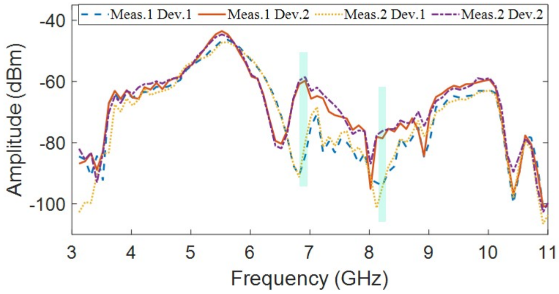


Fig. 8. Higher third order intermodulation *(2f*2*-f*1*)*.

the lower and higher frequencies. As will be shown next, this power level difference is not the most significant for distinguishing the two devices. Therefore, further measurements were not recorded for the fundamental returns.

Figures 7 and 8 show the power level of the reflected lower ($2f_1$-f_2) and higher ($2f_2$-f_1) intermodulation tones, respectively. From the measurement result, these devices show similar or small differences in power level from 3 GHz to 6.6 GHz, and from 8.2 GHz to 11 GHz, for both the lower and higher third-order intermodulation tones.

For the frequency range from 6.6 GHz to 8.2 GHz, the intermodulation tones generated from the devices were significantly different. In Fig. 7, the difference in the power level at 6.79 GHz for Devices 1 and 2 is 35.17 dB. In Fig. 8 for Device 1, the intermodulation tones decreased from 6.6 GHz to 6.8 GHz and then an increase in power level was observed from 6.82 GHz to 7.12 GHz. In the same interval, the intermodulation tone for Device 2 recorded a rise in the power level from 6.6 GHz to 6.92 GHz. The higher third-order intermodulation power measured from Device 1 at 6.82 GHz was -91.22dBm while for Device 2, the power is -59.67 dBm, leading to a 31.55-dB difference.

To verify the repeatability of the measurement, the power level of reflected intermodulation tones were recorded twice and plotted in Figs. 7 and 8. Based on repeated measurements, the frequency range where the two devices can be clearly differentiated is highlighted in the figures. Therefore, it is shown that although the two devices are fabricated based on the same schematic design and layout, the process variation during fabrication leads to different characteristic broadband frequency response for their intermodulation reflections.

IV. Conclusion

In this paper, a method for remote device identification and authentication is presented. This method relies on detecting the unique frequency response of reflected intermodulation tones due to process variation during device fabrication. By performing broadband measurements, we can show that it can be used as an effective tool for device identification as every electronic device has its unique broadband nonlinear RF response and thus can be potentially used for the detection of unauthorized devices for security applications. Compared with the harmonic measurement technique, the transmit and receive chains of the detector operate in the same bandwidth, thus reducing the complexity in detector design. The future work is to design and implement a portable broadband detector based on the proposed concept.

Acknowledgement

The authors would like to acknowledge grant support from National Science Foundation (NSF) CNS-1718483 and ECCS-1760497.

References

[1] J.A. Hayward, J. Meraglia, “DNA Marking and Authentication: A unique, secure anti-counterfeiting program for the electronics industry,” In International Symposium on Microelectronics, vol. 2011, no. 1, pp. 107-112, 2011.

[2] F. Zhang, A. Hennessy and S. Bhunia, “Robust counterfeit PCB detection exploiting intrinsic trace impedance variations,” 2015 IEEE 33rd VLSI Test Symposium (VTS), Napa, CA, 2015, pp. 1-6

[3] Z. Peng, D. Psychogiou, and C.Li. “Investigation of the Roles of Filters for a Harmonic FMCW Radar,” *2017 International Applied Computational Electromagnetics Society (ACES) Symposium*, Suzhou, 2017.

[4] K.A. Gallager, “Harmonic Radar: Theory and Applications to nonlinear target detection, tracking, imaging and classification”, PhD dissertation, Penn State University, 2015.

[5] R. McArthur. “Intermodulation Fundamentals.” N.p., n.d. Web.http://www.sinctech.com/wpcontent/uploads/2012/10/final.pdf.