An RFID System with Enhanced Hardware-Enabled Authentication and Anti-counterfeiting Capabilities

Vasileios Lakafosis[†], Anya Traille[†], Hoseon Lee[†], Giulia Orecchini[■,†], Edward Gebara[†],
Manos M. Tentzeris[†], Joy Laskar[†], Gerald DeJean[‡], and Darko Kirovski[‡]

† School of ECE, Georgia Institute of Technology, Atlanta, GA 30332, USA
■ Department of Electrical Engineering, University of Perugia, Italy
‡ Microsoft Research, Redmond, WA 98052, USA

Abstract — This paper introduces a new RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities. The system relies on the near-field RF effects between the multiple antennas of the reader and the uniquely modified substrate of the RF certificates of authenticity. A new stand-alone, low cost reader with 5 by 5 antennas is used to accurately extract the near-field response of RF certificates of authenticity meant to complement typical RFID tags in the 5 to 6 GHz frequency range. The RF characterization of all the reader's components, with an emphasis on accuracy and insertion loss introduced, has been performed for calibration purposes. The design methodology for generating RF-COA instances that yield unique RF fingerprints is outlined. Rigorous, yet preliminary, performance and robustness test results, including uniqueness among different instances, repeatability robustness for same instance, 2D to 3D projection comparison and variation in conductive material density, are reported and verify the unique features of this technology.

Index Terms — RF certificate of authenticity, RF fingerprint, RFID, RFID reader, near-field, multi-antenna systems.

I. INTRODUCTION

In the battle against piracy and counterfeiting, which both account for between 7-8% of the world trade, traditional RFIDs with encoded digital information cannot be relied upon since they can easily be replicated. However, a solution that aims to address this problem has been proposed by Dejean and Kirovski [1]. The fundamental idea is to complement an RFID with an inexpensive physical object that behaves as a certificate of authenticity (RF-COA) in the electromagnetic field so that this "super-tag" is not only digitally but also physically unique and hard to near-exactly replicate.

The RF-COA can be created as a random constellation of small, randomly 3D-shaped conductive and/or dielectric objects that exhibits a distinct behavior in its near-field when exposed to RF waves coming from a specific point over a particular RF spectrum. This enables, on one hand, the extraction of the data about the product in the far-field and, on the other hand, the offline verification of its authenticity within its near-field with low probability of a false alarm. The rationale behind the near-field observation of the EM effects is, primarily, the relatively high variance of the EM field, which possesses better distinctive characteristics compared to the far-field responses that typically represent certain average characteristics of random discrete scatterers [2]. In addition, the near-field communication can hardly be maliciously jammed. Although COAs in the electromagnetic domain have been proposed [3, 4, 5, 6], all of them aim to detect the COA's random structure in the far-field over the "expensive" 60GHz frequency range. Under the above far field category but in the 5-7GHz frequency band falls also a printable chip-less RFID tag [7] presented for Secure Banknote Applications, the anti-counterfeiting robustness of which relies only on a bit sequence formed by a multi-resonating circuit.

In this paper we present the first fabricated RF-COA reader that can extract the RF "fingerprint" of an RF-COA instance; a set of complex S_{21} parameters over the 5 to 6 GHz frequency band for a subset of or all possible antenna couplings of its antenna array. Since the RF-COA reader is intended to be used, for example, at numerous customs offices and stores during the check-in process, its manufacturing cost has been kept low. In particular, the total cost of the presented prototype, shown in the insert of Fig. 1, consisting of an antenna array and a number of out-of-the-shelf components, serving as analog/digital back-end, before it is integrated with a microcontroller unit is less than $50. The main aim of the reader's design is to maximize the entropy, i.e. randomness, of the RF "fingerprint", given the accuracy of the analog and digital circuitry used, as well as the noise due to external factors.

Based upon the characterization of all the RF components and the radiation behavior of the antenna element of the array, the performance of the RF-COA reader is studied. Its high efficiency, albeit its simple and low cost implementation, is demonstrated with robustness and repeatability tests using random structures formed by conductive silver nano-particle ink printed on paper substrate. The results clearly render this RF-COA reader a unique candidate, optimally meeting the application's requirements.

II. RF-COA READER DESIGN AND IMPLEMENTATION

In order for the RF-COA reader to extract the RF fingerprint, RF power is radiated from a particular antenna element, scattered and reflected by the conductive material of the RF-COA instance placed at about 1mm away from the array and received by another antenna element. In this 5 by 5 antenna matrix, 9 of the elements are operating as transmitter only and 8 of them as receiver only, eliminating the need for SPDT switches for dual operation of the elements and
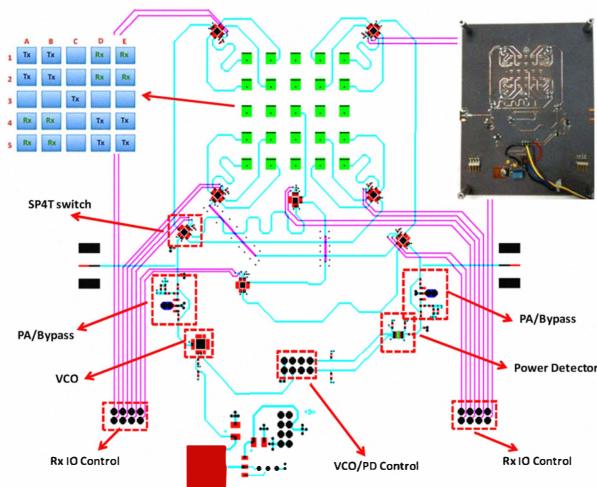
Fig. 1. Circuit layout of the RF-COA reader and its first fabricated version.

reducing the number of the required digital input/output control lines. During the read-out, it is ensured that the placement of the RF-COA instance is fixed and geometrically unique, using plastic poles whose relative position on the array's plane is non-symmetrical.

The first step toward the implementation of this prototype reader involved the design of an individual microstrip patch antenna with an operating frequency in the mid 5 to 6 GHz range. Since it was desired to pack as many antennas as possible in a 1 by 1 inch area, emphasis was stressed on the folding minimization technique; the antenna's technical characteristics and design strategy are detailed in [8].

The 25 single folded patch elements are placed on the top and second metal layers at distances of approximately 3mm between each other; the overall design consists of four metallic and three substrate layers of variable thickness. The ground plane is placed on the third metal layer, the RF part on the bottom layer and the digital lines on the top layer. The used copper's conductivity is 1.493e6 S / inch and 5.88e7 S/m. The substrate for the design is FR-408 with $\varepsilon_r = 3.715$, $\mu_r := 1$ and a loss tangent $\tan\delta = .01$. Using the Rohde & Schwarz ZVA 8 Vector Network Analyzer (VNA), the return loss of a single antenna element was measured -27.4 dB at a resonant frequency of 5.26 GHz, as shown in the insert of Fig. 2. The reason this result is off the simulated one is that the latter was taken for a single antenna element in free space and not in the presence of all the rest 24 due to considerably high computational time required.

A particular antenna transmit and receive coupling, out of the board's 72 available permutations, can be chosen by digitally controlling 8 identical HMC345LP3 SP4T switches, arranged in two hierarchical levels as shown in the block diagram of Fig. 1. Based on this arrangement, there are always two switches preceding the transmit antenna element and two switches following the receive element. The location and order of the switches has been optimized so that the coupling between the RF lines is minimal. In particular, all connections are 50 Ohm and it is ensured that the length of the lines

connecting the appropriate switches for any antenna permutation is constant. The average insertion loss introduced by a single SP4T switch across the 4.5 to 6.5 GHz band has been measured 1.074 dB using the aforementioned VNA. The S_{21} and S_{11} parameters of the two-port system between the transmit and receive power amplifiers are shown in Fig. 2. For calibration purposes, a copper line between the middle two switches, out of the overall four ones in serial, has been used for this measurement. This measurement is of great importance since the losses are expected to vary from lot of circuit components to lot and, as a result, from reader to reader. Only after this curve is captured right after the reader's fabrication and afterward de-embedded from its future measurements, i.e. reader is calibrated, can the RF fingerprint be considered valid and checked against the in-chip stored waveform, regardless of the reader used. As depicted in the same figure, the average S_{21} value of -16.566 dB and the curve across the 4.5 to 6.5 GHz spectrum agrees with the simulated overall loss, which is the sum of the attenuation due to the total line length itself as calculated by ADS [9] with the 4.296 dB attenuation due to the four switches.

The RF signal radiated toward the RF-COA instance is generated by the HMC431LP4 voltage-controlled oscillator (VCO). The exact VCO's mapping of the input control 0 - 10 V voltage range to the 5.1 - 6.3 GHz frequency spectrum is characterized with the Tektronix RSA 3408A Real-Time Spectrum Analyzer (RSA). The peak power of the generated, nearly mono-chromatic signal, after it is amplified by 11.25 dB by the RFMD RF3378 power amplifier (PA), is measured 4.03 dBm with the same RSA. The scattered, reflected and refracted signal received is amplified by the same PA and the RF power is monitored by the Linear Technology LT5581
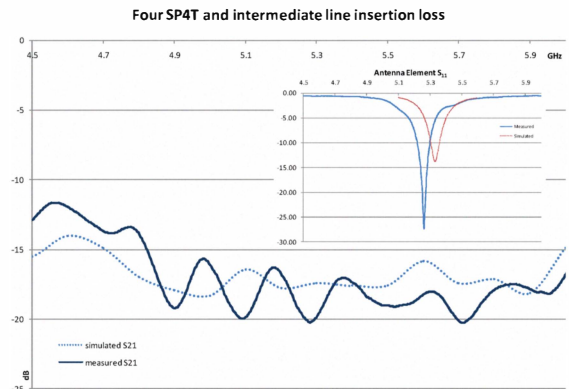

Fig. 2 Simulated and measured results of the insertion loss introduced by four consecutive SP4T switches and of the single antenna's S11 parameter.

RMS power detector (PD). Its voltage output has been accurately mapped to the input power generated by the HP 83622B Swept Signal Generator before the PA ranging from -55dBm up to 5 dBm.

Finally, for this first prototype implementation, the National Instruments USB-6259 board is used to generated the 16-bit sequence that dictates the path of the RF signal through the two-layer SP4T switches hierarchy, controls the frequency
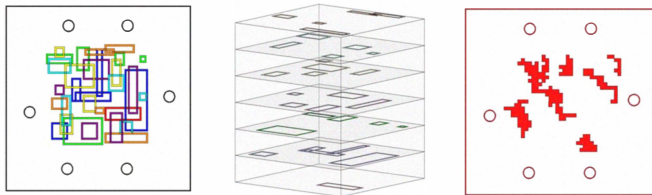
Fig. 3. a) Single Layer COA of rhombic loops. b) 3D-stacked RF-COAs of rhombic loops. c) RF-COA as a random trajectory of pixels.

output of the VCO through the corresponding input voltage and measures the power detected by monitoring the PD's output voltage.

III. RF-COA INSTANCE

The physical RF-COA object is to consist of an extremely difficult to replicate, random arrangement of scatterers that produces a unique and repeatable response in the near field. Since the RF-COA instance is completely passive, it is imperative that every different scatters' configuration should provide a unique RF signature within the frequency range of the reader's illumination based only on the spatial arrangement. Thus, the presented RF-COA is the first low cost physical object that enables anti-counterfeiting based completely on its hardware implementation and the resulting RF effects. For the realization of this first generation of objects, inkjet printing technique [10] was chosen as a direct-write technique by which the design pattern is transferred directly to the substrate, without any requirement of masks, resulting in a very fast and low cost process.

The optimization of such an RF-COA is challenging, as it is necessary to perform a detailed systematic analysis of various near-field phenomena by investigating distinct geometries for the RF-COA design. The first and most important factor that was investigated was the individual scatterers' resonance and interference in ultracompact ("credit-card" size) dimensions. To evaluate the effect of the shape and the dimensions of the resonating scatterers, a set of overlapping rhombic loop conductors were used, with each loop being assigned a random aspect ratio and overall circumference. The folded shape was chosen for dimensional miniaturization and density maximization. The average loop circumference is 18.6 mm, approximately between half wavelength and one wavelength in size. Multiple such RF-COAs are shown in separate layers in Fig. 3b before they are tightly stacked to give the projection, shown in Fig. 3a. Another RF-COA design that was also used for the experiments of Section IV consists of a random constellation of 1 by 1mm pixels that trace the form of the final geometry, shown in Fig. 3c.

Other factors to consider include the dimensions of the spaces between conductors as a fraction of reader's wavelength and how the RF-COA's scatterers' non-periodicity affects the response for various densities. These parameters are expected to be critical in the determination of the system's discrimination capability that will effectively decide how hardly RF-COAs can be counterfeited in a given central frequency, bandwidth and RF-COA's dimensions. To evaluate the effect of inclusions and disruption of periodicity,

the position of the loops was randomized while the quantity of loops used was incremented. N = 1, 6, 11, 16, 21, 26 and 31.

IV. PERFORMANCE TESTS

In order to verify the feasibility of this RF authenticity certification technology, a number of different test results are given in the following subsections. For this set of experiments, the RF-COA instances presented in the previous section, among others, were placed through the plastic poles against the antenna matrix of the manufactured RF-COA reader at a distance of 1mm.

A. Uniqueness among different RF-COAs

In order to demonstrate the uniqueness, in terms of high variability of RF fingerprint extracted, among different RF-COA designs, the entropy of the near-field frequency response for three different RF-COA instances across three different Tx/Rx couplings is investigated. As can be seen in Fig. 4, the thick, thin, and dotted lines representing a single COA at different Tx/Rx couplings indicate significant change in the pattern which ensures uniqueness. Also, three different COAs at the same Tx/Rx coupling also show high variation in response. Only for the A1/A5 transmitter and receiver coupling does there seem to be some convergence at a portion of the higher frequencies. However, the graph shows only 3
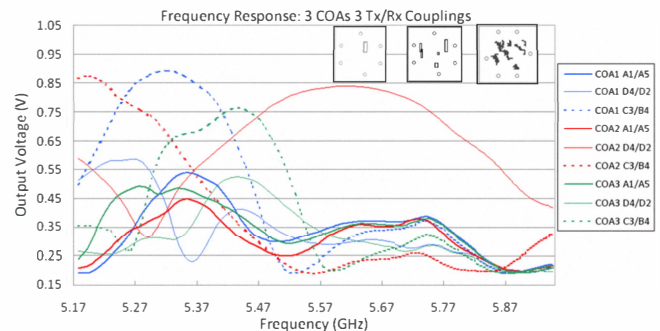

Fig. 4. Uniqueness test showing high variance in frequency response among three different COA designs at three different Tx/Rx couplings.

out of 72 available Tx/Rx couplings. For a single scan, 72 couplings give enough data to ensure uniqueness between COAs.

B. Repeatability for same RF-COA

In order to ensure the robustness of the RF-COA reader, a single RF-COA instance is placed on the reader, then taken off and then placed back on the reader to indicate any change in measurement results. Fig. 5 shows the results of an RF-COA measured twice against a subset of six different transmitter and receiver couplings, shown in the legend. The figure seems to indicate that there is very little deviation from the two measurement runs. For a quantifiable assessment, the difference between voltage outputs of the power detector of the two runs is shown in the insert of Fig. 5. The maximum voltage difference is 0.025V is across C3/B4 coupling.
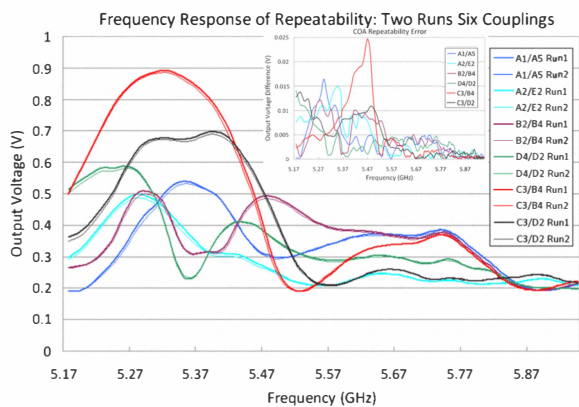
C. 2D to 3D projection comparison

Fig. 5. Frequency response of repeatability test across six Tx/Rx couplings using COA shown in Fig. 3b and of voltage difference between the two measurement runs in (top) figure. The maximum voltage error is approximately 0.025V at C3/B4 coupling.
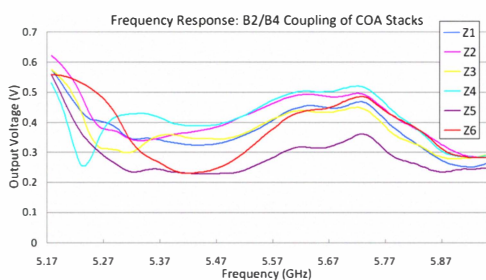

Fig. 6. Frequency response across Tx/Rx coupling at B2/B4 of 3D stacked COAs as shown in Fig B, with six different stacking permutations represented as Z1 through Z6.
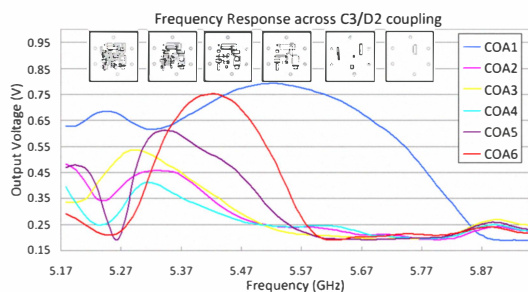

Fig. 7. Effect of the conductive material density on frequency response across Tx/Rx coupling at C3/D2 with six COAs with COA1 being the densest and COA6 the sparsest.

This experiment aims to compare the near-field response of different-ordered stacked sets of the same RF-COA instances, shown as separate layers in Fig. 3b. In particular, Z1 in Fig. 6 is a stack of seven RF-COAs with rhombic loops in a certain order, and Z2 thru Z6 are also stacks of the exact same RF-COAs but in different orders. The remaining clear distinction between the different near-field responses verifies that even slight differentiations across the third dimension, i.e. thickness, of the RF-COA object yields distinct enough RF fingerprints.

D. Variation in conductive material density

With this experiment, the effect of the amount of metal density in the structure of the RF-COA to the differentiation in its frequency response is investigated. This test is conducted by initially using a single RF-COA design and afterward

reducing the density of the metal by removing metal patterns from the RF-COA to create another RF-COA with sparser metal. A total of 6 RF-COA instances, shown in the insert of Fig. 7, were used for this test with RF-COA1 having the densest amount of metal and RF-COA 6 having the sparsest amount of metal. As verified by the same figure, the density of metal does indeed affect the uniqueness of the frequency response increasing the entropy by itself as a factor as well.

V. CONCLUSION

Rendering typical RFID tags physically unique and hard to near-exactly replicate by complementing them with 25 x 25 x 2 mm sized RF-COA instances is a valuable tool against piracy and counterfeiting. The first standalone reader for the RF-COA application has been designed and fabricated. The RF characterization of all components, comprising the reader, with an emphasis on accuracy and insertion loss introduced, has been done. Next, the design strategy behind creating RF-COA instances that yield unique and highly divergent RF fingerprints has been analyzed. As a means to verify the reader's performance in extracting the near-field frequency response of the RF-COA physical structures, a number of tests, namely uniqueness among different instances, repeatability robustness for same instances, 2D to 3D projection comparison and variation in conductive material density, are conducted. Even though many more experiments for all available antenna couplings and instance designs are required, these initial results provide the confidence that the fabricated reader coupled with the novel inkjet-printed instances exceed the application's requirements.

REFERENCES

[1] G. DeJean, D. Kirovski, "Certifying Authenticity using RF Waves", IST Mobile Summit 2006
[2] Tsang, Jin A. Kong, K. Ding, C.O. Ao, "Scattering of Electromagnetic Waves, Numerical Simulations", ISBN 0-471-38800-9. Wiley-VCH , 2001.
[3] J. Collins. RFID Fibers for Secure Applications. RFID Journal, 2004. Available on-line: http://www.rfidjournal.com/ article/articleview/845/1/14.
[4] CrossID, Inc. Firewall Protection for Paper Documents. Available on-line at: http://www.rfidjournal.com/article/ articleview/790/1/44.
[5] Inkode, Inc. Available on-line at: http://www.inkode.com.
[6] RF SAW, Inc. Available on-line at: http://www.rfsaw.com/ tech.html
[7] Preradovic, S.; Karmakar, N.C., "Design of fully printable chipless RFID tag on flexible substrate for secure banknote applications," 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication, pp.206-210, Aug. 2009.
[8] R.L. Li, G. DeJean, M.M. Tentzeris, J. Laskar, "Development and analysis of a folded shorted-patch antenna with reduced size," Antennas and Propagation, IEEE Trans. on, vol.52, no.2, pp. 555-562, Feb. 2004
[9] Advanced Design System (ADS), electronic design automation software system produced by Agilent EEsof EDA.
[10] L. Yang, A. Rida, R. Vyas, and M. M. Tentzeris, "RFID tag and RF structures on a paper substrate using inkjet-printing technology," IEEE Trans. on Microwave Theory and Techniques, vol. 55, no. 12, pp. 2894–2901, 2007.