RF Fingerprinting Physical Objects for Anticounterfeiting Applications

Vasileios Lakafosis, *Student Member, IEEE*, Anya Traille, Hoseon Lee, Edward Gebara, *Member, IEEE*, Manos M. Tentzeris, *Fellow, IEEE*, Gerald R. DeJean, *Member, IEEE*, and Darko Kirovski, *Member, IEEE*

***Abstract*—Rendering typical RF identification (RFID) tags physically unique and hard to near-exactly replicate by complementing them with unique RF certificates of authenticity (RF-CoAs) can prove a valuable tool against counterfeiting. This paper introduces a new robust RFID system with enhanced hardware-enabled authentication and anticounterfeiting capabilities that relies on the near-field RF effects between a 5 × 5 antenna array and the uniquely modified substrate of the RF-CoAs. A microcontroller-enabled, low-power, and low-cost reader is used to accurately extract the near-field response ("RF fingerprint") of the certificates meant to complement typical RFID tags in the 5–6-GHz frequency range. The RF characterization of all the reader's components, with an emphasis on the accuracy provided, has been performed. The state diagram of the fast and accurate reader operation is outlined. Rigorous performance and security test results are presented and verify the unique features of this technology.**

***Index Terms*—Anticounterfeiting, multiantenna systems, near-field, RF certificate of authenticity (RF-CoA), RF fingerprint, RF identification (RFID), wireless.**

I. Introduction

With the World Customs Organization and International Chamber of Commerce, according to Interpol, estimating that roughly 8% of world trade every year is in counterfeit goods [1], the Business Software Alliance estimating that 35%–45% of software sales worldwide are counterfeit [2], and Glaxo-Smith-Kline, in a study with the U.S. Food and Drug Administration, estimating that counterfeit drugs account for 10% of the global pharmaceuticals market [3], there is no doubt that counterfeiting accounts for a huge economic impact on industries such as software and hardware, pharmaceutical, and, of course, the entertainment and fashion industry. With the ease of marketing products on-line, it seems that selling counterfeit objects has never been easier.

In contrast with piracy, where the buyer is confident that the purchased object is not genuine due to a very low price, the counterfeiter fools the buyer into believing that the merchandise is authentic and collects substantial revenue with profit margins typically higher than that of the original manufacturer. In the battle against piracy and counterfeiting, traditional RF identifications (RFIDs) with encoded digital information cannot be relied upon since they can easily be replicated.

This paper presents the full implementation of a novel RF anticounterfeiting system that aims to address this problem in a completely hardware-based ("RF-fingerprinting") way. This is the first reported approach that aims to bridge the RFID technologies with the anticounterfeiting world utilizing modified material scattering characteristics. The fundamental idea is to complement an RFID with an inexpensive physical object that behaves as an RF certificate of authenticity (RF-CoA) in the electromagnetic (EM) 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 3-D-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 verification of its authenticity within its near-field with low probability of a false alarm.

Fundamental to the following discussion is the definition of the "RF Fingerprint." An "RF fingerprint" of an RF-CoA is a set of S_{21} parameters observed over a specific frequency band and collected for (a subset of or) all possible antenna couplings of a reader's array. The main aim of the reader design, presented below, 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. A graphical representation of this fingerprint, as extracted from the reader for all its 72 different antenna element permutations using a signal processing method described in detail in Section VI, is shown in Fig. 1.

II. Related Work

CoAs in the RF domain have been proposed in the past[1,2] [4], [5]. The common characteristic of all proposed solutions, to the best of our knowledge, is that they aim to detect the

Manuscript received September 07, 2010; revised October 13, 2010 and November 01, 2010; accepted November 08, 2010. Date of publication December 30, 2010; date of current version February 16, 2011. This work was supported in part by the IFC/SRC. This paper is an expanded paper from the IEEE MTT-S International Microwave Symposium, Anaheim, CA, May 23–28, 2010.

V. Lakafosis, A. Traille, H. Lee, E. Gebara, and M. M. Tentzeris are with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30308 USA (e-mail: vasileios@gatech.edu; atraille@ece.gatech.edu; hoseon@gatech.edu; gebara@ece.gatech.edu; etentze@ece.gatech.edu).

G. R. DeJean and D. Kirovski are with Microsoft Research, Redmond, WA 98052 USA (e-mail: dejean@microsoft.com; darkok@microsoft.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TMTT.2010.2095030

[1] Inkode Inc., Vienna, VA, 2007. [Online.] Available: http://www.inkode.com

[2] RF SAW Inc., Richardson, TX, 2007. [Online.] Available: http://www.rfsaw.com/tech.html

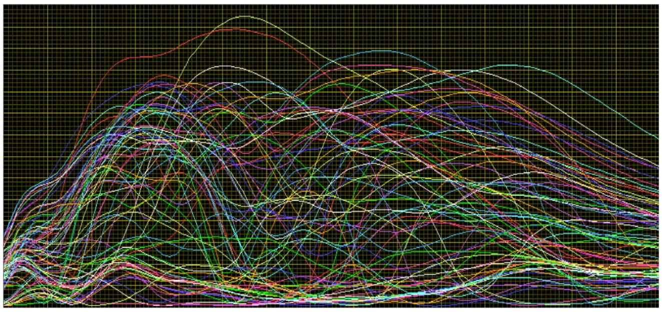


Fig. 1. Graphical representation of an "RF fingerprint" as extracted by our fabricated reader for all its 72 different antenna element permutations.

CoA's random structure in the far-field over the "expensive" 60-GHz frequency range. Under the same far-field category, but in the 5–7-GHz frequency band, also falls a printable chipless RFID tag [6] presented for secure banknote applications, the anticounterfeiting robustness of which relies only on a bit sequence formed by a multiresonating circuit.

Our proposed system, the operation of which relies on the near-field observation of the CoA's EM (scattering) effects, possesses some important qualitative features not exhibited by other types of CoAs. First of all, the near-field observation enables relatively high variance of the EM field, causing better discriminating characteristics compared to the far-field responses that typically represent certain average characteristics of random discrete scatterers [7]. Characteristics of this near-field region, which is located less than one wavelength (more precisely, $2D^2/\lambda$, where D is the largest dimension of the source of the radiation) from the source, are that the relationship between the electric field component E and the magnetic field component H becomes often too complex to predict with either field component (E or H) possibly dominating at any particular point and that all four polarization types, namely, horizontal, vertical, circular, or elliptical, can be present, as opposed to the far field. Still, since the readout of the CoA does not require a physical contact, RF-CoAs may be built with superior "wear and tear" properties. Second, it is hard to eavesdrop or maliciously jam near-field communication compared to the far-field one that is prone to both potentially devastating attacks. As an additional advantage of the very short-range observation and discrimination feature, the reader can operate with low power and use low-efficiency antenna designs.

III. RF-CoA Technology

A. Fabrication Process

This process takes place in the controlled environment of an RF-CoA factory. Here, after an RF-CoA instance is created, the issuer digitally signs the instance's RF response using traditional cryptography.

In particular, first the unique "RF fingerprint" of the newly fabricated RF-CoA instance is digitized with the use of a reader and compressed into a fixed-length bit string. This information is afterward concatenated to the information associated with the tag, such as product ID, color, and expiration date, and the resulting combined bit string is encrypted using a cryptographically strong algorithm such as SHA256 [8].

Adopting a public-key cryptosystem (PKCS) such as Rivest, Shamir, and Adleman (RSA) [9], this hash is signed using the issuer's private key to form, together with the plain initial bit string of the fingerprint, a message that is directly encoded onto the RFID chip. The use of asymmetric key algorithms that involve the use of a public key known to everyone and a secret private key is the distinguishing characteristic of public key cryptography. The keys are related mathematically, but it is virtually impossible to deduce the private key from the public key. Thus, in our application only the issuer can digitally sign the RF-CoA with the secret private key.

B. Verification Process

The digitally encoded message, described above, is the one used to validate whether a product is authentic or not; a process that typically takes place in a store or a warehouse.

The verifier first reads the aforementioned message and verifies the integrity of the plain bit string of the fingerprint with respect to its encrypted and signed version using the corresponding issuer's public key. In case the integrity test is successful, which means that no one else, except the possessor of the matching private key, has encrypted the message, the original "RF fingerprint" and associated product data are extracted. This extracted fingerprint is afterward compared with a new reading of the tag's CoA that the verifier takes with his own reader. Only if the level of similarity between these two fingerprints, read and extracted, exceeds a predefined and statistically validated threshold, the verifier declares the CoA instance to be authentic.

C. Potential Attacks

In order for an adversary to counterfeit protected objects, he needs to do the following:

1) compute the private key of the issuer so that he can store his one fixed-length bit string f; a task which can be made arbitrarily difficult by adjusting the key length of the used public-key crypto-system, or
2) misappropriate signed CoA instances; a responsibility of the CoA object issuer, or
3) devise a manufacturing process that can exactly or nearly exactly replicate an already signed CoA instance; a task that is not infeasible, but requires certain expense by the malicious party. In particular, our RF-CoA designs require by the counterfeiter not only physical access to the original CoA, but also the ability to accurately scan and reconstruct arbitrary 3-D structures and embed them in a soft or hard encapsulating sealant; a high-cost process.

From the last attack's perspective, it is obvious that the CoAs can be used to protect objects, the value of which does not exceed the cost of forging a single CoA instance including the accumulated development cost of a successful adversarial manufacturing process.

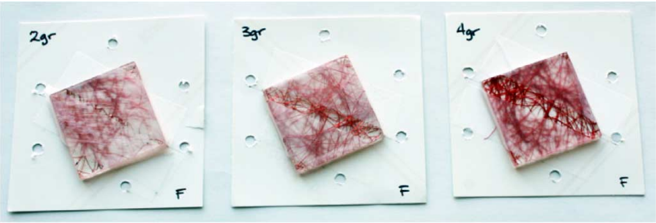


Fig. 2. CoAs of different copper weight, namely, 2, 3, and 4 g per mold.

IV. RF-CoA Tag

The proposed RF-CoA tag is the first low-cost physical object that enables anticounterfeiting based completely on its hardware implementation and the resulting RF effects. The physical RF-CoA instance consists 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.

As is also the case with the reader, the design of these anticounterfeiting tags has to be optimized so that maximum entropy of the scattering results is achieved, and in the same time, the results extracted by the same instance are repeatable with very high reliability. This optimization 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 to consider is the individual scatterers' resonance and interference in compact "credit-card" size dimensions. 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' nonperiodicity 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 easy RF-CoAs can be counterfeited in a given central frequency, bandwidth, and RF-CoA's dimensions.

The tags can be divided into two main categories, namely, the copper-based ones and the inkjet-printed ones. Examples of the first category are shown in Fig. 2 and are used throughout Section VII for all the performance tests. These have been fabricated by an injection molding company[3]; essentially the process involves the encapsulation of copper wire of variable gauge into plastic mold. Randomness in this process has been achieved by introducing techniques that are absolutely nondeterministic, such as blending with different speeds and for different amount of time and using air fans.

As for the second category of physical RF-CoA objects, we relied upon inkjet printing technique as a means of a very fast, low-cost, and in-house process; a direct-write technique by which the design pattern is transferred directly to the substrate in means of multiple inkjet layers, without any requirement of masks. The final 3-D structure was created by tightly stacking multiple 2-D CoAs one on top of each other to give the projection, shown in Section VIII, and are used for the 3-D attacks test described in Section VIII.

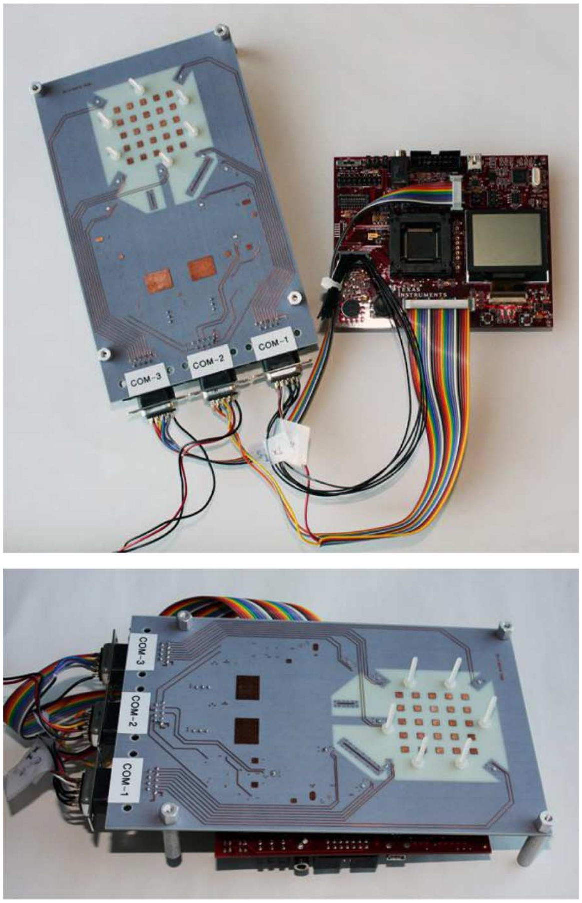


Fig. 3. (a) "RF plane" and "control plane" of the RF-CoA reader. (b) Overall stacked two-layer RF-CoA system.

V. RF-CoA Reader

The extraction of the unique RF fingerprint of an RF-CoA object is done as follows. RF power is radiated from a particular element of the antenna array, scattered and reflected by the conductive material of the RF-CoA instance placed about 1 mm away from the array and received by another antenna element. During the readout, it is ensured that the placement of the RF-CoA instance is fixed and geometrically unique, using short plastic poles, shown in Fig. 3(b), the relative position of which on the array's plane is nonsymmetrical.

The overall design, shown in Fig. 4, consists of four metallic and three substrate layers of variable thickness and the total thickness does not exceed 1.6 mm. The elements of the antenna array are placed on the top and second metal layers at distances of approximately 3 mm between each other. 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 copper's conductivity is $5.88 \cdot 10^7$ S/m $(1.493 \cdot 10^6$ S/in$)$. The substrate for the design is FR-408 with relative dielectric constant $\varepsilon_r = 3.715$ in our frequency band of interest (5–6 GHz), relative permeability $\mu_r = 1$, and loss tangent $\tan\delta = 0.01$.

[3] Aero-plastics Inc., Renton, WA, 2009. [Online.] Available: http://www.aero-plastics.tmcsweb.com/

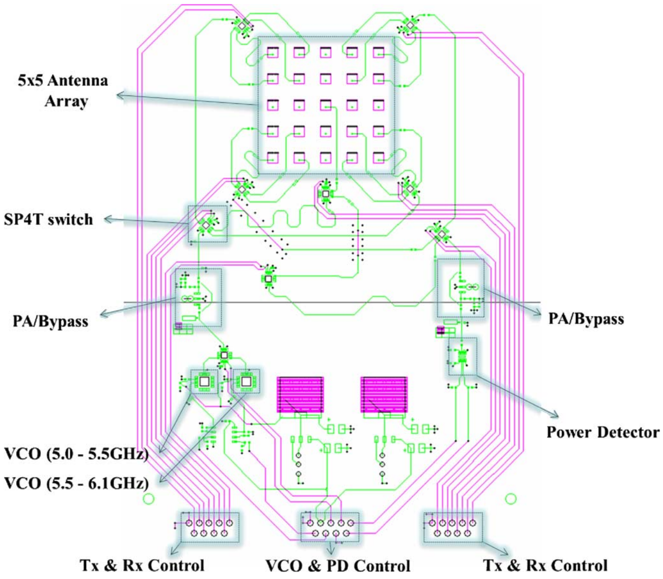


Fig. 4. RF-COA reader circuit schematic.

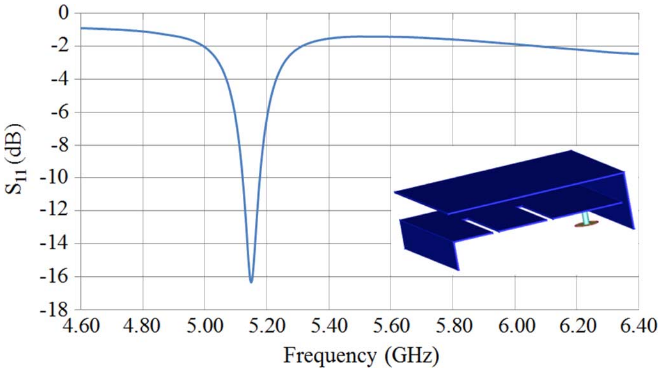


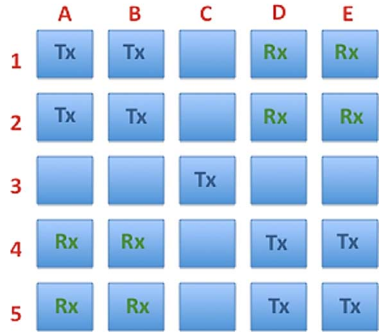
Fig. 5. $S11$ curve of an individual antenna element. Its 3-D design is shown in the lower right corner.

A. Antenna Elements and Coupling

The antenna elements are individual microstrip patch antennas. Since it was desired to pack as many antennas as possible in a 1 × 1 in area, emphasis was stressed on making use of a folding minimization technique; the antenna's technical characteristics and design strategy are detailed in [10]. Given that the half-wavelength in this range of frequencies is around 2.75 cm and given the properties of the folding minimization technique, we were finally able to fit 25 elements.

The antenna's 3-D element design is shown in the insert figure of Fig. 5. A single such element has a return loss of 16.3 dB[4] at a resonant frequency of 5.149 GHz (when a single element is measured by itself and not in the presence of neighboring elements), as shown in Fig. 5. The aforementioned miniaturization technique, however, does not come without cost and the major negative effect is the limited 10-dB bandwidth of this antenna element, which does not exceed 5 MHz. Despite that, the strength of the electric field extracted by these elements even 0.5 GHz away from the resonant frequency can be very high (> -10 dB), as shown in performance tests of Section VII.

Out of all the 25 elements of the 5 × 5 antenna matrix, nine of them are operating as transmit-only and eight of them as receive-only, eliminating the need for single-pole double-throw (SPDT) switches for dual operation of the elements and reducing the number of the required digital input/output control lines. This pattern is shown in Fig. 6.



	A	B	C	D	E
1	Tx	Tx		Rx	Rx
2	Tx	Tx		Rx	Rx
3			Tx		
4	Rx	Rx		Tx	Tx
5	Rx	Rx		Tx	Tx

Fig. 6. Diagram of the functionality of the reader's 5 × 5 antenna array elements.

The reason that each of the transmit- and receive-only elements have been split into sets of fours, placed as farthest as possible in the four corners of the array, and that the rest of the eight elements on the cross of the structure, with the exception of the central one, have been rendered useless (unconnected) is that we wanted to minimize the coupling due to proximity and, thus, attribute most of the coupling measured to the presence of the metallic material of the CoA. To quantify this, the S_{21} curves of all possible different antenna element spacings of a standalone 3 × 3 antenna array in the absence of any CoA is shown in Fig. 7 (bottom). This array has been manufactured in the exact same way as the finally used 5 × 5 array so that subminiature A (SMA) RF connectors are available and more intuitive conclusions can be drawn by fewer elements. These six different curves, captured over the 4.6–6.4-GHz band for 3-MHz step sizes, are labeled with a "x–y" format corresponding to the "x" numbered element, as shown in Fig. 7 (top), transmitting and the "y" numbered element receiving. As expected, all curves have their maximum at around the resonant frequency of the antenna elements and the shorter the relative distance the higher this maximum is $(1{-}4 > 2{-}4 > 2{-}3 > 1{-}2 > 3{-}4 > 1{-}3)$. It should be noted that the worst case scenario for the actual 5 × 5 board and given the functionality assigned to the active elements, described above and shown in Fig. 6, corresponds to the cases of 1–2 and 2–3 (C3-B4 and C3-D2), for which the magnitude of the maximum points does not exceed -20 dB. In other words, the maximum coupling between any pair of elements of the 5 × 5 array in the absence of a CoA never exceeds 20 dB.

B. Single-Pole Four-Throw (SP4T) Switches

A particular antenna transmit and receive coupling, out of the board's 72 possible permutations, is chosen by digitally controlling eight identical HMC345LP3 [11] SP4T switches, arranged in two hierarchical levels, as shown in the block diagram of Fig. 8. Based on this arrangement, there are always two switches preceding the transmit-only antenna element and two switches following the receive-only 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 $50\ \Omega$

[4] Using the Rohde & Schwarz ZVA 8 vector network analyzer (VNA).

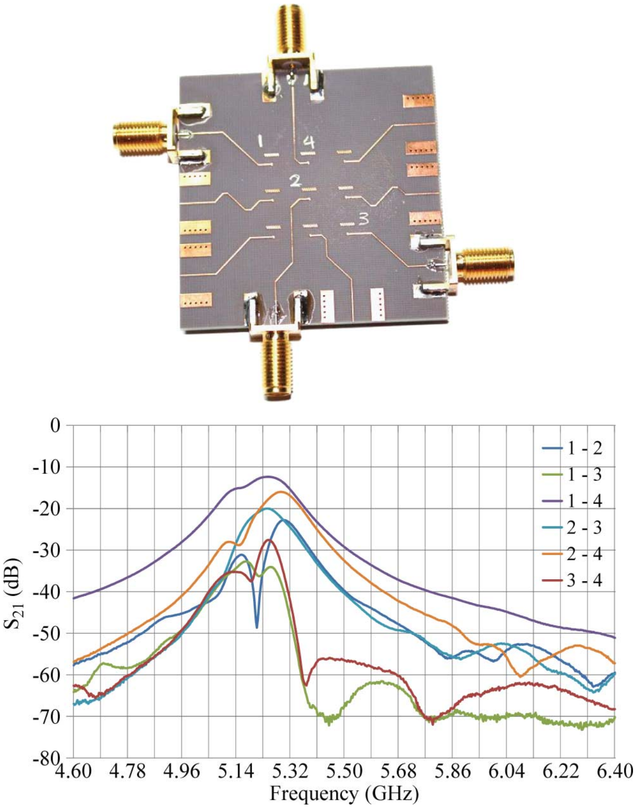


Fig. 7. (*top*) Bottom view of a 3 × 3 antenna array fabricated in the exact same way as the reader's 5 × 5 array. (*bottom*) S_{21} curves of all possible different antenna element spacings of a subset 3 × 3 array in the absence of any CoA.

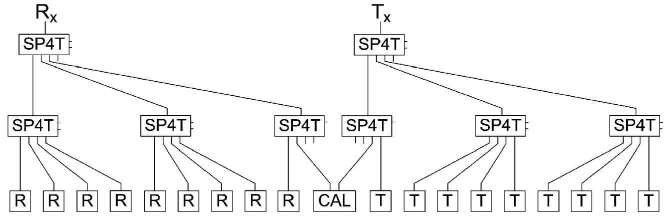


Fig. 8. SP4T switches arranged in two hierarchical levels.

and it has been 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 4.5–6.5-GHz band has been measured 1.074 dB.[5] The S_{21} and S_{11} parameters of the two-port system between the transmit and receive power amplifiers (PAs) have been shown in [12].

The losses of the reader's components are expected to vary from lot of circuit components to lot and, as a result, from reader to reader. In order to achieve consistency and elimination of false negatives among different readers, i.e., for calibration purposes, all coupling channels (S_{21}) for all possible antenna permutations over the whole supported frequency band are measured for each RF-CoA reader in the absence of any CoA and stored into the Microcontroller Unit's (MCU) nonvolatile memory. Right after the CoA's fabrication, these S_{21} curves are subtracted from the corresponding S_{21} curves of the CoA's RF fingerprint and the difference is what becomes embedded in the RFID chipset. The same "subtraction," of course, takes place also at the verifier's premises.

VI. MCU-Enabled Reader Operation

The functionality of the RF-CoA reader is summarized in the following four main tasks:

- generates the appropriate RF power and controls the frequency output of the voltage-controlled oscillator (VCO);
- dictates the path that the RF signal follows through the two-layer SP4T switch hierarchy and the coupling, eventually between the T_x and R_x antenna element;
- measures the power captured by the power detector (PD) by monitoring its output voltage;
- uploads the set of measured data that comprise the RF-CoA's fingerprint to a computer.

The most important advancement in regards with the first version of the RF-CoA board, presented in [12], has been the addition of a 16-bit RISC architecture ultra-low-power MCU that provides not only a very fast means of capturing the RF fingerprint, but also the accuracy required toward our effort to maximize the fingerprint's entropy. As a result, the overall reader design consists of a double-stacked-layer solution; the "control plane" and the "super high frequency (SHF) RF plane." As implied by their names, the first layer houses the MCU and the data acquisition interface and the other includes the CoA reading slot, the antenna matrix, as well as all required digital and analog circuitry. The upper layer of this new prototype RF-CoA reader, represented with pink lines (in online version) in Fig. 4, is the "control plane" and the lower one, represented with green lines (in online version) is the "SHF RF plane."

Regarding the "SHF RF plane," it should be noted that its design is an improved version of our preliminary design [12]. First, this new board is smaller in its width, occupying 13% less space (4.301 × 6.775 in). Second, this design does not rely on a single VCO, but two of them, namely, the HMC430LP4 [13] and HMC431LP4 [14], which both together optimally cover the 5.0–6.1-GHz frequency band.

At the heart of the "control plane" is the TI MSP-EXP430F5438 MCU [15] that features an up to 18-MHz system clock, high-frequency crystals up to 32 MHz and multiple high-resolution analog-to-digital converters (ADCs). The MCU is accompanied by push buttons and a USB interface for data transfer. The state diagram of the MCU, which reflects the sequence of all the steps mentioned in the beginning of this section, is shown in Fig. 9.

For its powering, the "control plane" does not rely on batteries (although a 2 AA battery option is available), but on the current supplied by the USB cable, which is used anyway for the RF-CoA fingerprint acquisition by a desktop or a laptop computer. When the board is initially connected to a computer through the USB cable, it finds itself in the low-power mode 4 (LPM4) sleep mode. This is a deep sleep mode of 1.69-μA current consumption at 3.0 V in which the CPU and all clocks are disabled, the crystal oscillator is stopped, but the supply supervisor is operational and full RAM retention and fast wake-up are provided.

[5] Using the Rohde & Schwarz ZVA 8 VNA.

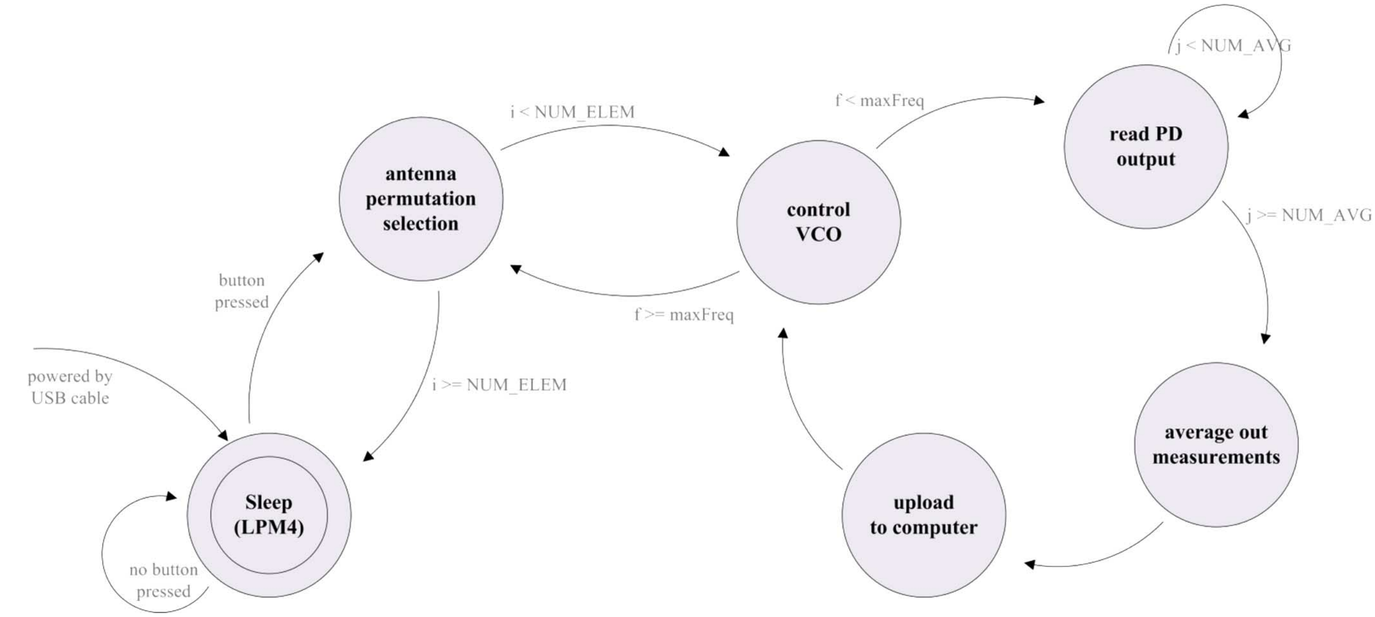


Fig. 9. State diagram of the RF-CoA reader's operation.

In short time intervals, the 32-kHz auxiliary clock is enabled and used to check if a button is pressed. Given that a human would be pressing the button for at least half a second, the time duration of this button monitoring lasts for only a few milliseconds, leading eventually to a very low duty cycle monitoring. As soon as a press on the button is detected, the MCU exits the deep sleep mode and the "control plane" transits to the antenna permutation selection state. Here, a particular antenna element pair is selected by appropriately configuring the two digital logic control pins (0 $V_{\rm dc}$ for logical 0 and 3.2 $V_{\rm dc}$ for logical 1) of the SP4T switches, shown in Fig. 9. In particular, a 16-bit sequence is generated by the digital output pins of the MCU and this selection remains active until a new bit sequence is generated. The next time the "control plane" returns to the antenna permutation selection state, a check is performed as to whether the maximum number of antenna permutations (NUM_ELEM), namely, 72, has already been selected; in which case the MCU reverts to the sleep mode.

If all possible antenna element permutations have not been enabled, the next step is to generate a sinusoidal power signal at a particular frequency, nearly monochromatic, by controlling the HMC431LP4 [14] VCO. The peak power of this signal, after it is amplified by 11.25 dB by the RF3378 [16] PA, is measured to be 4.03 dBm.[6] The S_{21} RF-CoA fingerprint is captured over the frequency band of 5.1–5.9-GHz at steps of 12.3 MHz. The selection of these steps is achieved by altering the VCO's tune voltage. Since the MCU provides no DACs, the latter's functionality is emulated by a high-frequency pulsewidth modulation (PWM) signal. The output voltage is configured based on a variable duty cycle that is derived from the ratio between the PWM's emulated voltage and the USB rail of 3.2 V. The next time the "control plane" returns to the control VCO state, a check is performed as to whether the maximum number of frequency steps (maxFreq) has already been reached; in which case the MCU returns to the antenna permutation selection state.

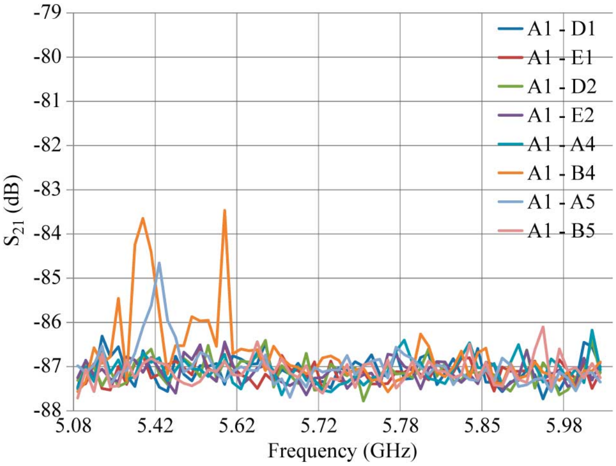


Fig. 10. Standard deviation of eight antenna coupling for the repeatability test.

With the T_x antenna element radiating power toward the CoA that is placed just 1 mm away from the antenna matrix, the next step is to amplify the captured reflected and refracted signal and feed it to the LT5581 root mean square (rms) [17] PD. For calibration purposes, the latter's voltage output has been accurately mapped to the input power generated by a signal generator[7] before the PA ranging from −55 up to 5 dBm. For this task, of course, the highest (12-bit precision) mode supported by the ADC of the MCU is chosen.

Regarding the effective bit length of entropy (EBLE) achieved with the results presented in the next two sections, this number cannot be cited as simply $72\ (\text{permutations}) \times 65\ (\text{frequencies}) \times 12\ (\text{bit of ADC resolution}) = 56\,160$ bits since interdependencies of all responses need to be taken into account. However, our achieved EBLE is substantially higher than what common cryptographic standards demand.

Based on extensive measurements carried out under a controlled environment of predetermined signal power amplitude,

[6] Tektronix RSA 3408A real-time spectrum analyzer (RSA).

[7] HP 83622B Swept Signal Generator.

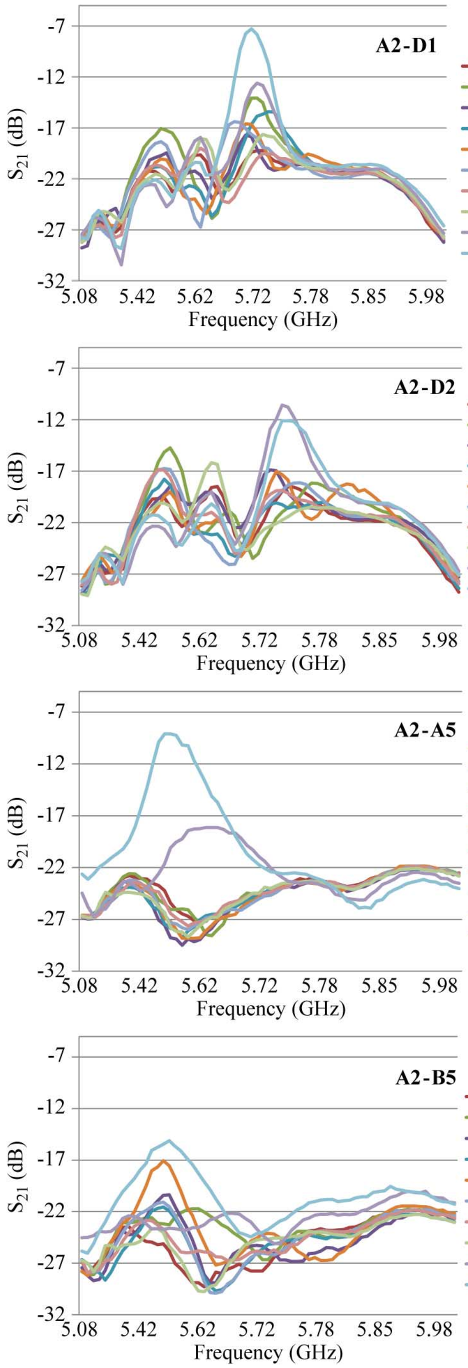


Fig. 11. "RF fingerprints" of ten different CoAs for four different antenna couplings for the "false positives" test.

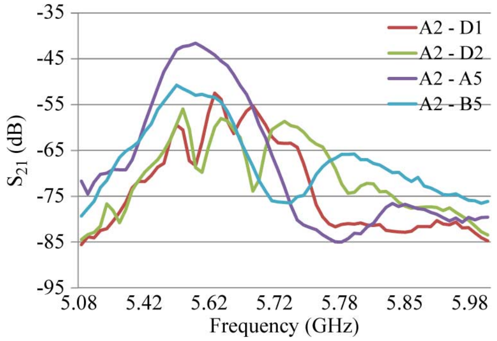


Fig. 12. Standard deviation of ten different S_{21} curves shown in Fig. 11 for four antenna couplings.

we have found that a single analog-to-digital conversion is not enough. In particular, although the voltage reference used (3.2 V) for the ADC and supplied by the USB input has been measured to remain steady over time, we have recorded AD conversions to be as far as 20% off from the same actual input signal for more than 100 measurements. The two major sources of inaccuracy in ADC testing of mixed-signal circuits have been identified to be the approximations of IEEE Standard for Digitizing Waveform Recorders and IEEE Standard for Terminology and Test Methods for ADCs [18] and the fact that the dc offset and the amplitude of the input analog signal evaluated on the base of the digital output differ from their true values [19]. However, this deviation easily drops to less than 8% by performing 20 consecutive conversions, storing them in the successive approximation register (SAR) and afterward simply averaging them. The latency incurred as a result of the additional 19 conversions is totally negligible given that each 12-bit resolution conversion requires only 13 MCU clock cycles, the total time duration of which is less than 0.8 μs. The NUM_AVG variable shown in the state diagram of Fig. 9 corresponds to the maximum number, i.e., 20, of consecutive analog-to-digital conversions before the averaging is performed.

Each entry consisting of antenna permutation, frequency, and received power in decibels is uploaded to the computer at 57.6 kb/s with the use of the USCI module of the MCU that supports the UART protocol used to communicate with the TI TUSB chip. An LED that remains on until all the aforementioned steps for the RF fingerprint extraction are completed is indicative of the activity of the "control plane" before it returns back to its sleep mode state. For this currently running software version, where significantly conservative long guard times are kept between consecutive operations that account for a multiple of the real running time, and which will gradually be removed from the next software versions, the overall time required to extract all 72 RF fingerprints is around 22 s.

VII. Performance Tests

A number of different types of tests have been conducted in order to assess the performance of our proposed RF authenticity certification technology. For all tests presented in this section, physical objects that are conceptually very close to the final envisioned product have been used as RF-CoAs. These objects are described in Section IV and examples of such three certificates are shown in Fig. 2.

As explained previously, the RF-CoA instances were attached to the reader through the plastic poles, shown in Fig. 3(b), against the antenna matrix of the manufactured RF-CoA reader at a distance of 1 mm. For this 1-mm spacing, a sturdy dielectric foam material with characteristics close to that of air was used. The certificates' dimensions were 0.75 in × 0.75 in and as such could not occupy the whole 1 in × 1 in area of the antenna matrix. However, their position has been rotated around the array's central axis so that not all areas around the

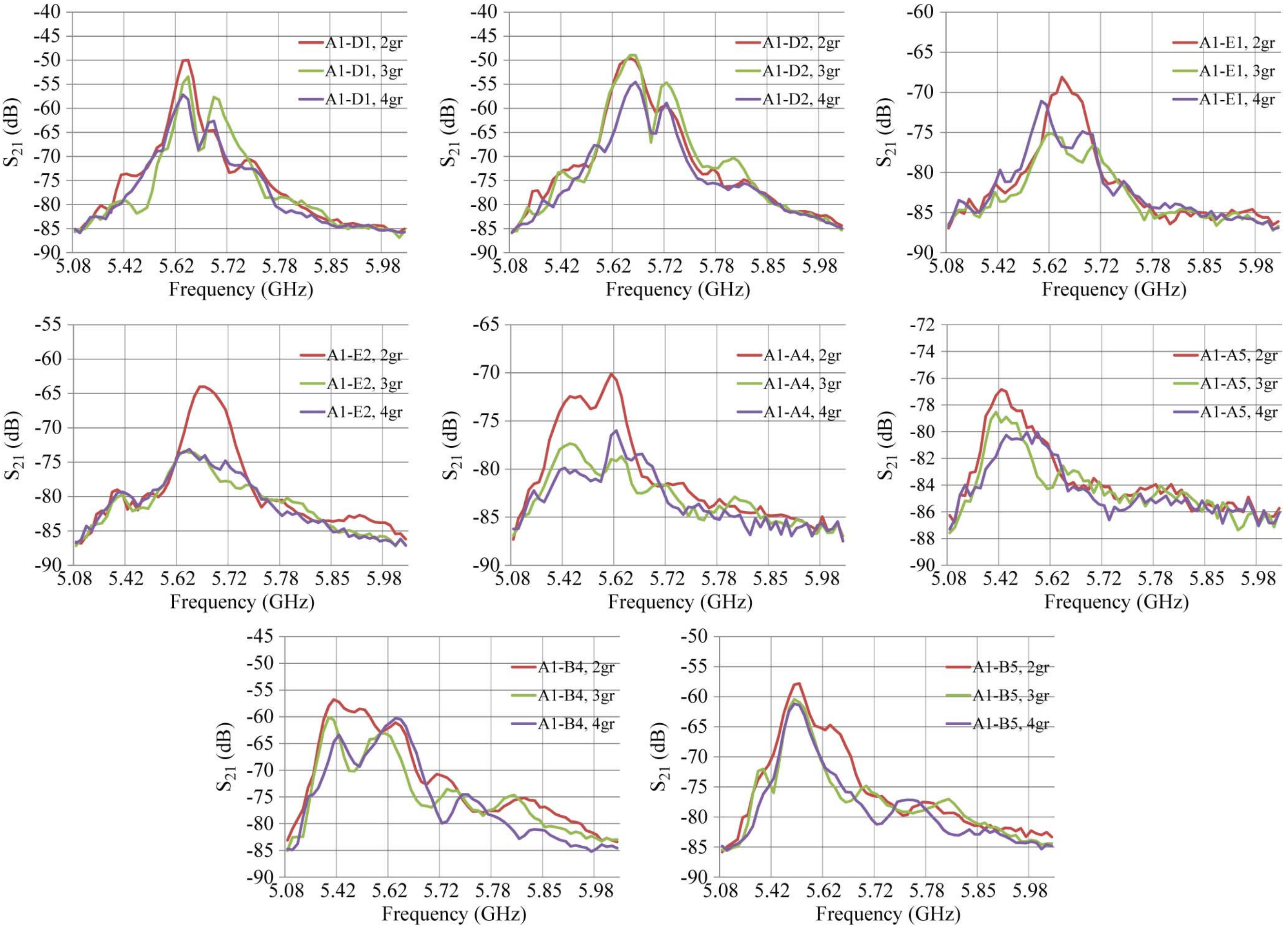


Fig. 13. Standard deviation of all the “RF fingerprints” of the different metal density certificates for each one of the eight antenna permutations.

circumference of the array are left uncovered. This is shown in the example tags of Fig. 2.

In each of the graphs presented hereafter, the y axis corresponds to the output of the PD based on its received signal strength of the monochromatic signal, and the x axis corresponds to the different frequency points sampled by the MCU’s ADC. Essential to the evaluation of the results of the following tests is the standard deviation (std);the square root of an estimator of the variance of the received signal strength by the R_x element for different CoAs at the same frequency points and antenna couplings. In particular, the equation used for the standard deviation is as follows:

$$\text{std} \triangleq \left(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \overline{x})^2\right)^{\frac{1}{2}}. \tag{1}$$

A. Repeatability

In order to ensure that always nearly exact replicate “RF fingerprints” are extracted by the same RF-CoA, i.e., to show the robustness of the RF-CoA reader, ten duplicate measurements of the exact same CoA are taken. In particular, a single RF-CoA instance is placed on the reader, then taken off, and then placed back on the reader to indicate any changes in measurement results; the whole process is repeated nine times.

Fig. 10 shows the standard deviation of the aforementioned duplicate measurements for eight “RF fingerprints,” which are extracted against eight different transmitter and receiver couplings (shown in the legend) that correspond to all eight R_x elements interchanged for the same T_x element (see Fig. 6). The fact that these std curves exhibit a very low magnitude that does not exceed -86 dB with the exception of just two antenna couplings, the maximum of which reaches -83.5 dB in the low part of the spectrum and of which curves can be decided to be excluded, if necessary, from future readings, indicates that the resolution captured by the reader for slightly different placements of the CoA in all three directions relative to the antenna array and under different environmental changes, namely, RF interference, temperature, etc. is very high. This result is well above the initial precision requirement of 2 dB [12] and, consequently, demonstrates the system’s repeatability robustness.

B. False Positives

The uniqueness among different RF-CoA designs, in terms of as high a variability as possible between different “RF fingerprints” extracted, is tested here by investigating the near-field frequency response for ten different RF-CoA objects across four different T_x/R_x couplings, shown in Fig. 11. It should be noted

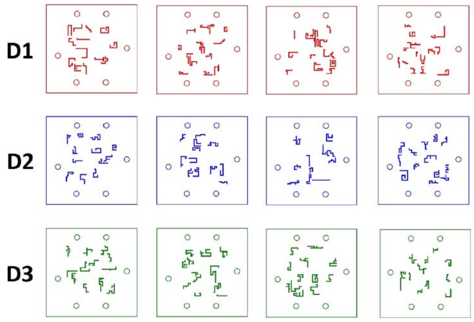


Fig. 14. Projection sets D1, D2, and D3.

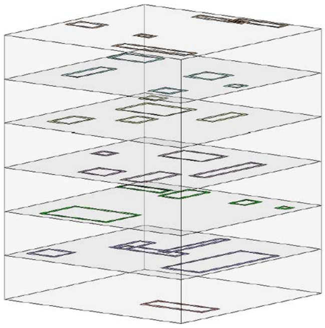


Fig. 15. 3-D stacked set example.

that, particularly, certificates I and J were different than all the other CoAs since their dimensions were 1.2 in × 1.2 in and holes for the reader's plastic poles had to be drilled through them.

The differentiation between the different colored "RF fingerprints" is visually obvious for all but the A2–A5 plot in Fig. 11. This particular plot provides valuable feedback about the importance of the amount of area of the array covered by the RF-CoA; specifically, certificates I and J yield high couplings for all four presented permutations, whereas that is not the case for all the others that, due to their smaller dimensions, do not present significant metal amount across A2–A5, and thus, give lower amplitude couplings.

Of course, a more reliable evaluation of the aforementioned differentiation is provided by their standard deviation curves shown in Fig. 12. Here, all four couplings provide significant amount of entropy, which is more prominent around the resonant frequency of the antenna elements mentioned above.

It is worthy to note that the lengthier antenna couplings A2–A5 and A2–B5 (see Fig. 6) are the ones that yield the highest deviation.

C. Metal Density

With this test we are investigating, the effect of the amount of metal density in the structure of the RF-CoA to the entropy in its frequency response. For this purpose, three different sets of CoAs of different copper weight, namely 2, 3, and 4 g per mold, are used. For each one of these categories, we created 15 certificates, examples of which are shown in Fig. 2.

The results of the standard deviation of all the certificates for each one of the eight antenna permutations are shown in Fig. 13. From these plots it is, first of all, verified that the metal density does indeed affect the entropy of the frequency response; in some cases, as in the A1–E2 plot, this difference in the achieved entropy can be as high as 100%. The conclusion drawn by this particular test is that the lighter copper-based certificates always yield higher response differentiation. On the other hand, it is shown that, though there is not that much of a great difference with the 3-g one, the heavier one provides the least entropy.

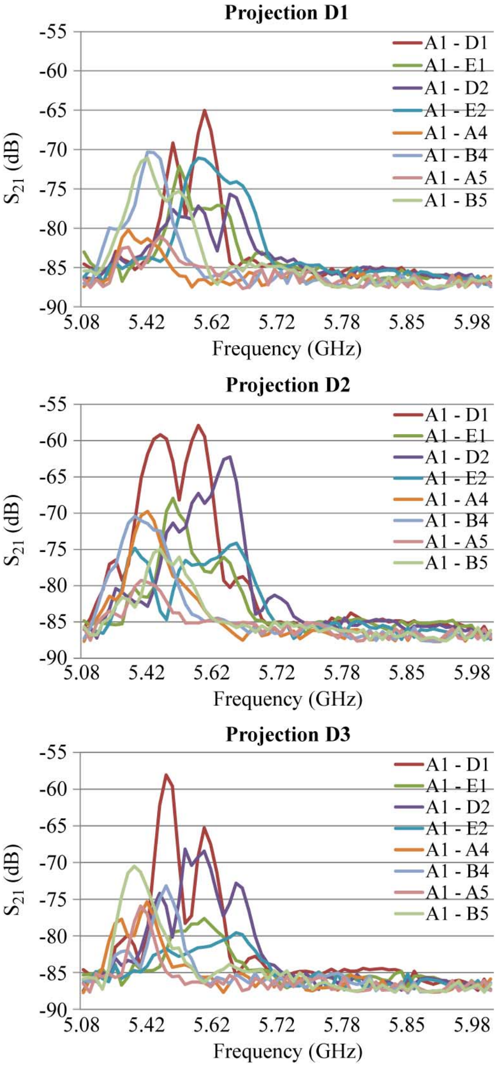


Fig. 16. Standard deviation of all 24 different orders of stacked 2-D CoAsfor projections D1, D2, and D3 for eight antenna permutations.

VIII. Defense Against 3-D Attacks

In Section III-C, the 3-D manufacturing ability was cited as one of the potential attacks against our anticounterfeiting system. This experiment aims to test the invincibility of our system against this type of attacks.

The RF-CoA design used here consists of a random constellation of 1 × 1 mm pixels that trace the form of the final geometry, as shown in Fig. 14. As described in Section IV, for the tags' fabrication, we relied upon inkjet printing technique with seven layers of conductive silver nanoparticle ink. The final 3-D structure was created as a stack of multiple inkjet-printed 2-D CoAs, as shown in Fig. 15.

In particular, what we have compared is the near-field response of three different-ordered stacked sets of the same RF-CoA instances, namely, D1, D2, and D3, shown in Fig. 14.

For each set, 24 different orders of stacked 2-D CoAs have been measured and their standard deviation curves are shown in Fig. 16 for each of eight antenna permutations. The results indicate that there is significant variation in the near-field for the different permutations, again especially around the resonant frequency of the antenna elements. This ensures that even slight variations in manufacturing in the z-axis, i.e., thickness, will produce distinct enough "RF fingerprints."

IX. Conclusion

A high-performing robust standalone reader for anticounterfeiting applications, which is smaller, computationally more powerful, and more accurate than its predecessor [12], 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. The algorithm behind its fast and accurate MCU-assisted "RF fingerprint" extraction has been described in detail.

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, variation in conductive material density of the certificate, and 2-D to 3-D projection attacks have been conducted yielding very promising results.

This paper has demonstrated in the most straightforward manner that uniquely authenticated "super" RFID tags, in the form of badges of a small dielectric profile (e.g., 2 mm, for alignment purposes with the presented RF-CoA reader) directly affixed onto objects or in the form of carefully attached product tags, can prove a valuable tool against the ever-increasing action of counterfeiters.

References

[1] M. Robyn, "Market-driven fraud: The impact and consequences of counterfeit products and intellectual property violations," presented at the ASC Annu. Meeting, St. Louis, MO, Nov. 2008.

[2] "Seventh annual global software piracy study," Business Softw. Alliance, Washington, DC, 2009. [Online]. Available: http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009.pdf

[3] "Counterfeiting report," Glaxo-Smith-Kline, Middlesex, U.K., 2009. [Online]. Available: http://www.gsk.com/responsibility/supply-chain/counterfeiting.htm

[4] Firewall protection for paper documents," CrossID Inc., Hauppauge, NY, 2004. [Online]. Available: http://www.rfidjournal.com/article/articleview/790/1/44

[5] J. Collins, "RFID fibers for secure applications," *RFID J.* 2004 [Online]. Available: http://www.rfidjournal.com/article/articleview/845/1/14

[6] S. Preradovic and N. C. Karmakar, "Design of fully printable chipless RFID tag on flexible substrate for secure banknote applications," in *3rd Int. Anti-Counterfeiting, Security, Identification Commun. Conf.*, Aug. 2009, pp. 206–210.

[7] L. Tsang *et al., Theory of Microwave Remote Sensing*. New York: Wiley, 1985.

[8] C. M. Gutierrez and P. Gallagher, "Secure hash standard," Fed. Inform. Process. Standards, Gaithersburg, MD, FIPS PUB 180-3, Oct. 2008.

[9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[10] R. L. Li, G. DeJean, M. M. Tentzeris, and J. Laskar, "Development and analysis of a folded shorted-patch antenna with reduced size," *IEEE Trans. Antennas Propag.*, vol. 52, no. 2, pp. 555–562, Feb. 2004.

[11] "GaAsmmIC SP4T non-reflective positive control switch, DC—8 GHz," Hittite, Chelmsford, MA, 2008. [Online]. Available: www.hittite.com/content/documents/data_sheet/hmc345lp3.pdf

[12] V. Lakafosis, A. Traille, H. Lee, G. Orecchini, E. Gebara, M. M. Tentzeris, G. DeJean, and D. Kirovski, "An RFID system with enhanced hardware-enabled authentication and anti-counterfeiting capabilities," in *IEEE MTT-S Int. Microw. Symp. Dig.*, Anaheim, CA, Jun. 2010, pp. 840–843.

[13] "mmIC VCO with buffer amplifier, 5.0–5.5 GHz," Hittite, Chelmsford, MA, 2008. [Online]. Available: www.hittite.com/content/documents/data_sheet/hmc430lp4.pdf

[14] "mmIC VCO with buffer amplifier, 5.5–6.1 GHz," Hittite, Chelmsford, MA, 2008. [Online]. Available: www.hittite.com/content/documents/data_sheet/hmc431lp4.pdf

[15] *"MSP-EXP430F5438 Experimenter Board User's Guide (Rev. D),"* Texas Instruments Incorporated, Dallas, TX, Dec. 2009.

[16] "General purpose amplifier," RFMD, Greensboro, NC, 2006. [Online]. Available: www.rfmd.com/CS/Documents/3378DS.pdf

[17] 6 GHz RMS power detector, linear," Milpitas, CA, 2008. [Online]. Available: cds.linear.com/docs/Datasheet/5581fa.pdf

[18] J. Blair, "Sine-fitting software for IEEE standards 1057 and 1241," in *Proc. IEEE Instrum. Meas. Technol. Conf.*, Venice, Italy, May 1999, pp. 1504–1506.

[19] K. Hejn and A. Pacut, "Sine-wave parameters estimation—The second source of inaccuracy," in *Proc. 20th IEEE Instrum. Meas. Technol.Conference*, May 2003, vol. 2, pp. 1328–1333.

Vasileios Lakafosis (S'07) received the Diploma degree in electrical and computer engineering from National Technical University, Athens, Greece, in 2006, the M.Sc. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, in 2009, and is currently working toward the Ph.D. degree at the Georgia Institute of Technology.

He has authored or coauthored over 12 papers in peer-reviewed journals and conference proceedings and one book chapter. His research interests include networking protocols in the areas of wireless mobile ad hoc, mesh, and sensor networks. His research has currently been focused on single- and multihop wireless localization techniques, delay-tolerant and opportunistic networks, and perpetual low-power network protocols.

Mr. Vasileios is also a member of the Association for Computing Machinery (ACM) and the Technical Chamber of Greece.

Anya Traille was born in Washington, DC, in 1982. She received the B.S. and M.S. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, in 2004 and 2009, respectively.

She is currently a Research Engineer with the School of Electrical and Computer Engineering, Atlanta, GA. From 2004 to 2007, she was a Full-Time Research Engineer with the Georgia Tech Research Institute, Smyrna, GA. In 2008, she was a Visiting Scholar with Imperial College, London, U.K. In 2009, she was a Visiting Researcher with Georgia Tech Ireland, Athlone, Ireland. In 2010, she was a Visiting Researcher with LAAS-CNRS, Toulouse, France. Her main areas of research include antenna arrays, waveguides, RFID, and liquid antennas for bio-signal monitoring in which she has organized and chaired numerous conference sessions.

Ms. Traille was the recipient/corecipient of the IEEE IGARSS 2009 Student Travel Award, the ISAP 2007 Best Poster Paper Award, the Second Place Best Paper Award of the Georgia Institute of Technology Graduate Research Fair 2006 and the Best Session Paper Award of IEEE ECTC 2010. She was also a finalist in the 2008 IEEE AP-S Best Student Paper Competition and a finalist in the 2007 ACES Symposium Best Student Paper Competition.

Hoseon Lee received the B.S. and M.S. degrees from the Georgia Institute of Technology, Atlanta, in 2002 and 2005, respectively, and is currently working toward the Ph.D. degree in electrical engineering at the Georgia Institute of Technology.

From 2006 to 2009, he was a naval officer and Assistant Professor with the Republic of Korea (ROK) Naval Academy. His research interests include low-cost organic solutions for radars, communication, sensing and identification systems, inkjet printing, and power scavenging for RF applications.

Edward Gebara (S'03–M'06) received the B.S. (with highest honors), M.S., and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, in 1996, 1999 and 2003, respectively.

From 1999 to 2000, he was an Invited Scientist with Chalmers University, Göteborg, Sweden. In 2001, he applied the results of his research to define the core technology for Quellan Inc., as its initial employee, which is now part of Intersil (NASDQ: ISIL). These technologies served as the basis for signal integrity solutions developed for the enterprise, video, storage, and wireless markets. While working with Quellan Inc., he maintained a research faculty position with the Georgia Institute of Technology, where he led the research efforts of the Mixed-Signal Team. In early 2008, he joined the Georgia Institute of Technology on a full-time basis. Since 2003, he has supervised nine Ph.D. students whose research focuses on equalization, crosstalk cancellation, and self-healing mixed signal techniques in pure CMOS. These technologies are applied to next-generation optics and wired and wireless communication systems. He has authored or coauthored over 70 papers. He holds five patents.

Dr. Gebara is a reviewer for the IEEE International Symposium and Circuits and Systems (ISCAS) and for the IEEE Microwave Theory and Techniques Society (IEEE MTT-S) International Microwave Symposium (IMS). He also served as workshop and tutorial chair of the Technical Program for the 2008 IEEE MTT-S IMS.

Manos M. Tentzeris (S'89–M'92–SM'03–F'10) received the Diploma degree in electrical and computer engineering (*Magna Cum Laude*) from the National Technical University of Athens, Athens, Greece, and the M.S. and Ph.D. degrees in electrical engineering and computer science from The University of Michigan at Ann Arbor.

He is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology. He has authored or coauthored over 370 papers in refereed journals and conference proceedings, five books, and 19 book chapters. He has helped develop academic programs in highly integrated/multilayer packaging for rf and wireless applications using ceramic and organic flexible materials, paper-based RFIDs and sensors, "green" electronics and power scavenging, nanotechnology applications in RF, microwave microelectromechanical systems (MEMS), system-on-package (SOP)-integrated (ultra-wideband (UWB), mutliband, conformal) antennas and adaptive numerical electromagnetics (finite difference time domain (FDTD) multiresolution algorithms), and heads the ATHENA Research Group (20 researchers). He is an Associate Editor for the *International Journal on Antennas and Propagation*.

Dr. Tentzeris is a member of URSI Commission D and the MTT-15 Committee. He is an associate member of the European Microwave Association (EuMA). He is a Fellow of the Electromagnetic Academy. He is a member of the Technical Chamber of Greece. He is one of the IEEE Microwave Theory and Techniques Society (IEEE MTT-S) Distinguished Microwave Lecturers (2010–2012). He is an associate editor of the IEEE TRANSACTIONS ON MICROWAVE THEORY AND TECHNIQUES and the IEEE TRANSACTIONS ON ADVANCED PACKAGING He has given more than 100 invited talks to various universities and companies all over the world. He is the vice-chair of the RF Technical Committee (TC16) of the IEEE CPMT Society. He is the founder and chair of the RFID Technical Committee (TC24) of the IEEE MTT-S and the secretary/treasurer of the IEEE C-RFID. He was the recipient/corecipient of the 2010 IEEE Antennas and Propagation Society Piergiorgio L. E. Uslenghi Letters Prize Paper Award, the 2010 Georgia Tech Senior Faculty Outstanding Undergraduate Research Mentor Award, the 2009 E. T. S. Walton Award from the Irish Science Foundation, the 2006 IEEE MTT-S Outstanding Young Engineer Award, the 2003 NASA Godfrey "Art" Anzic Collaborative Distinguished Publication Award, the 2003 IBC International Educator of the Year Award, the 2003 IEEE CPMT Outstanding Young Engineer Award, the 2002 Georgia Tech Electrical and Computer Engineering (ECE) Outstanding Junior Faculty Award, and the 2000 National Science Foundation (NSF) CAREER Award.

Gerald R. DeJean (S'03–M'06) received the B.S. degree in electrical and computer engineering (*Suma Cum Laude*) from Michigan State University, East Lansing, in 2000, and the M.S. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, in 2005 and 2007, respectively.

He is currently a Researcher with Microsoft Research, Redmond, MA, where he is involved in the field of RF design. He has authored or coauthored over 40 papers in refereed journals and conference proceedings. He has been involved in a number of research projects as a member of the National Science Foundation (NSF) Packaging Research Center and the Georgia Electronic Design Center. His research interests include antenna design, RF/microwave design and characterization, and 3-D system-on-package (SOP) integration of embedded functions that focuses largely on modern commercial RF systems such as cellular phones for personal communications system (PCS) applications, Bluetooth and 2.4-GHz industrial–scientific–medical (ISM) applications, RFIDs, WLAN (802.11a,b,g), LMDS, and millimeter-wave applications at 60 GHz. He has dedicated his research to making the antenna more compact and integrable with multilayer packages such as low-temperature cofired ceramic (LTCC), liquid crystal polymer (LCP), and multilayer organic (MLO), while maintaining the full functionality of the device for wideband and/or multiband applications. He is also interested in equivalent circuit modeling techniques to assist in the design and optimization of compact antennas.

Dr. DeJean is a member of Eta Kappa Nu and Tau Beta Pi. He was the recipient of the Microsoft Research Fellowship Award for excellence in graduate research. He was twice a finalist of the Student Paper Competition of the 2004 and 2005 IEEE Antennas and Propagation Society Symposia.

Darko Kirovski (M'09) received the Ph.D. degree in computer science from the University of California at Los Angeles (UCLA), in 2001.

Since joining Microsoft Research, Redmond, WA, in 2000, he has split time between the Crypto and Machine Learning Groups, during which time he has been involved on a wide variety of system projects that span authentication, anticounterfeiting, and XBOX Kinect games, among others. He has coauthored over 100 conference and journal papers. His inventions have been recorded in over 70 patent filings.

Dr. Kirovski is involved with the IEEE Information Forensics and Security Subdivision, Signal Processing Society (SPS). He was the recipient of several awards, including the 2001 Association for Computing Machinery (ACM)/IEEE Outstanding Ph.D. Dissertation in Electronic Design Automation, the Microsoft Graduate Fellowship, and the ACM Multimedia Best Paper Award.