RFID-CoA: The RFID tags as Certificates of Authenticity

Vasileios Lakafosis†, Anya Traille†, Hoseon Lee†, Edward Gebara†,
Manos M. Tentzeris†, Gerald DeJean*, and Darko Kirovski*

vasileios@gatech.edu

† School of ECE, Georgia Institute of Technology, Atlanta, GA 30332, USA

* Microsoft Research, Redmond, WA 98052, USA

***Abstract* — The inadequacy of the traditional, digitally encoded RFID tags in combating counterfeiting prompts us to investigate new hardware-enabled technologies that can complement the remote identification functionality of typical RFIDs in an effective and very low cost way. In this paper, we present RFID-CoA; a system that aims to render typical RFID tags physically unique and hard to near-exactly replicate by complementing them with random 3D scattering structures, which serve as certificates of authenticity (CoA). The unique near-field response, or "fingerprint", of the CoAs is extracted as a set of S_{21} curves by our reader prototype, the design and development details of which are discussed. The results of our performance analysis show that the intersection probability of the false positive and false negative error probability curves is inconceivably small ($<10^{-200}$). The RFID-CoA tag's lifecycle from fabrication site to store is presented, and a strategy to block potential attacks is discussed. Our system bridges the world of RFID with a large array of anti-counterfeiting applications by exploiting "hardware-enabled", modified-material scattering characteristics in the near-field. Based on our multifaceted analysis, we firmly believe that the demonstrated RFID-CoA technology can prove a valuable tool for the low-cost ubiquitous applicability of RFID technology against counterfeiting.**

***Index Terms* — RFID, RF certificate of authenticity, RF fingerprint, anti-counterfeiting, near-field, antenna array, wireless**

I. Introduction

As opposed to piracy, where the buyer is confident that the object he is purchasing is not genuine due to a very low price, the counterfeiter deceives the buyer into believing that the merchandise is genuine and collects substantial revenue with profit margins typically higher than that of the original manufacturer. With Glaxo-Smith-Kline, in a study with the US Food and Drug Administration, estimating that counterfeit drugs account for 10% of the global pharmaceuticals market [1], the Business Software Alliance estimating that 35-45% of software sales worldwide are counterfeit [2] and the World Customs Organization and the International Chamber of Commerce estimating that roughly 8% of the world trade every year is in counterfeit goods [3], undoubtedly counterfeiting amounts to a huge economic impact on industries, such as the entertainment, the fashion, the software and the pharmaceutics.

In the battle against counterfeiting, traditional RFID tags with encoded digital information cannot be relied upon since they can easily be replicated. This paper presents a complete RFID anti-counterfeiting solution that aims to address this problem in an entirely hardware, "RF-fingerprinting"-based manner. The fundamental idea is to complement an RFID tag with an inexpensive physical object that behaves as a *Certificate of Authenticity* (CoA) in the electromagnetic field, so that this enhanced RFID-CoA tag is not only digitally but also physically unique and hard to near-exactly replicate. An example of such a unique RFID-CoA is shown in Fig. 1.

The RFID-CoA is essentially the result of the combination of a typical RFID tag with an inexpensive CoA that can be created as an arbitrary constellation of small, randomly 3D-shaped conductive and dielectric materials, and which exhibits a distinct behavior in its near-field when exposed to RF waves over a particular RF spectrum. This enables, on one hand, the extraction of the product information in the far field and, on the other hand, the verification of its authenticity within its near field with a virtually impossible false alarm, as shown in Section IV.

The contribution of this paper is that it bridges the world of RFID with a large array of anti-counterfeiting applications by exploiting the near field modified material scattering characteristics of very cheap, randomly structured conductive physical objects with a superior robust performance. The remainder of this paper is organized as following: we start by presenting the underlying electromagnetic effects that enable our RFID-CoA anti-counterfeiting technology (Section II); next, we provide details on the RF part and digital part of our

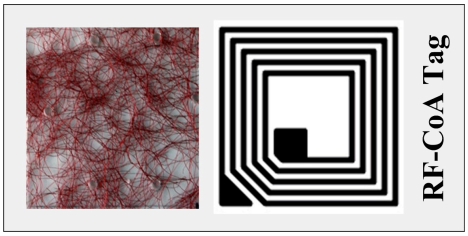

Fig. 1. The RFID-CoA Tag.

system's reader design and development (Section III); a systematic performance analysis of the uniqueness, or entropy, among different RF fingerprints extracted from different CoA designs by our prototype reader is also presented (Section IV); then, the following section (Section V) covers the RFID-CoA tag's life cycle from the fabrication site to a store, discusses potential attacks on our system and how they are eliminated, and points out some of the potential emerging applications; the last two sections highlight the aspects that distinguish our technology from the related work (Section VI) and conclude (Section VII).

II. RFID-CoA Technology

The physical CoA instance consists of an extremely difficult to replicate, random arrangement of a conductive material, such as copper wire, mixed with a firm dielectric material, such as plastic PET mold, that produces a unique and repeatable response in the near-field. In effect, the RFID-CoA system harnesses the entropy exhibited by the near-field response of a random constellation of scatterers. Characteristics of this near-field electromagnetic region, which extends to less than one wavelength far from the source (more precisely $2D^2/\lambda$, where D is the largest dimension of the source of the radiation and λ is the wavelength), are that:

i. 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,
ii. all four polarization types, namely horizontal, vertical, circular, or elliptical, can be present, as opposed to the far-field.

Since the RFID-CoA instance is completely passive, it is imperative that each different scatterer arrangement should provide a unique RF signature within the frequency range of the reader's illumination. The aforementioned RF signature is what we call an *RF Fingerprint*. In particular, we define the RF fingerprint of an RFID-CoA as a set of S_{21} parameters observed over a defined frequency band and collected for a subset of or all possible antenna element couplings of a reader's array. The main aim of the reader design, presented in the next Section, 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 introduced by 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 III, is shown in Fig. 2.

The first advantage of this near field observation approach, as opposed to the far field based solutions, is that the former enables relatively high variance of the EM field, causing better discriminating characteristics; the far field responses typically just represent certain average characteristics of random discrete scatterers [4]. Second, the near field communication cannot be eavesdropped or maliciously jammed, as can be the case with 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

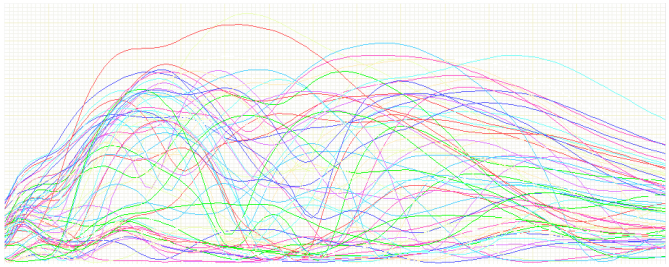

Fig. 2. A single RF fingerprint consisting of 72 different S_{21} curves as captured by all possible antenna element permutations of the reader's antenna array.

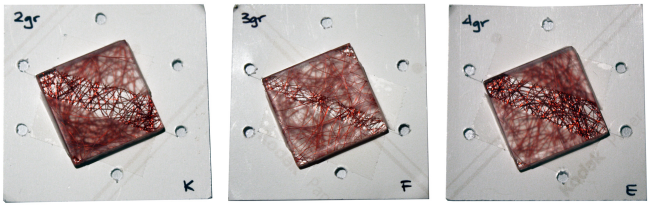

Fig. 3. CoAs of different copper weight, namely 2 (right), 3 (middle) and 4 (right) grams per mold.

can operate with low power and use low efficiency antenna designs. Last, since the readout of the CoA still does not require a physical contact, RFID-CoAs may also be built with superior "wear and tear" properties.

The design of these anti-counterfeiting hardware certificates is challenging and very critical as it determines the system's discrimination capability. The cost of the proposed CoA has to be comparable, if not cheaper, to the cost of a typical RFID tag that it accompanies. As of today's design, the certificates are fabricated with a process that involves the encapsulation of copper wire of variable gauge into a 1in x 1in x 0.08in plastic mold. Randomness in the arrangement of the scattering copper wire has been achieved by introducing techniques that are non-deterministic, such as blending different amounts and gauges of copper wire with the plastic mold with time varying rotational speeds and for different time periods. Examples of these first prototypes are shown in Fig. 3.

III. RFID-CoA Reader Design and Development

The extraction of the unique RF fingerprint of an RF-CoA object by the reader is achieved as following: RF power is radiated from a particular element of the reader's antenna array, scattered and reflected by the conductive material of the RF-CoA instance placed at a distance of 1mm up to 8mm away from the array, as long as this distance is kept the same across different CoA and different reader measurements and allowing for ±0.2 mm vertical displacement, and received by another antenna element. The major objectives of the reader design are to provide:

- as highest a randomness, or entropy, of the near-filed response of the CoA as possible, and
- exhibit consistency of extracted RF fingerprint across multiple readings of the same RFID-CoA, as well as across readings of the same RFID-CoA tag by different readers.

The reader board circuit design is shown in Fig. 4, the major

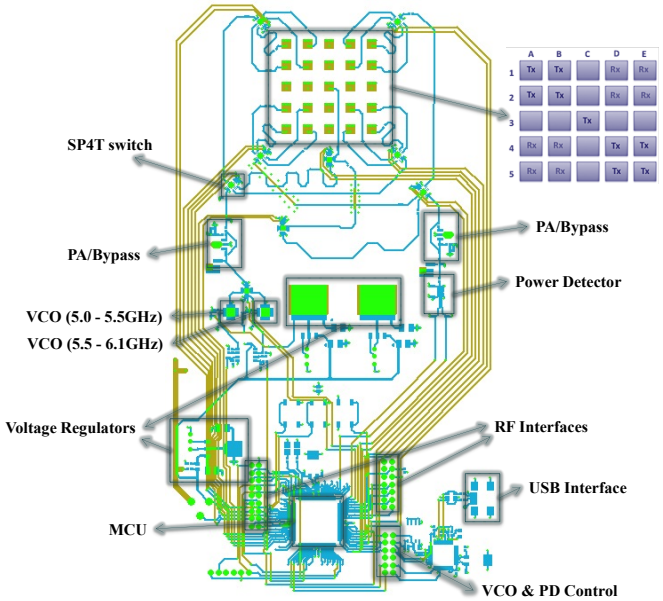

Fig. 4. The RFID-CoA reader board circuit schematic.

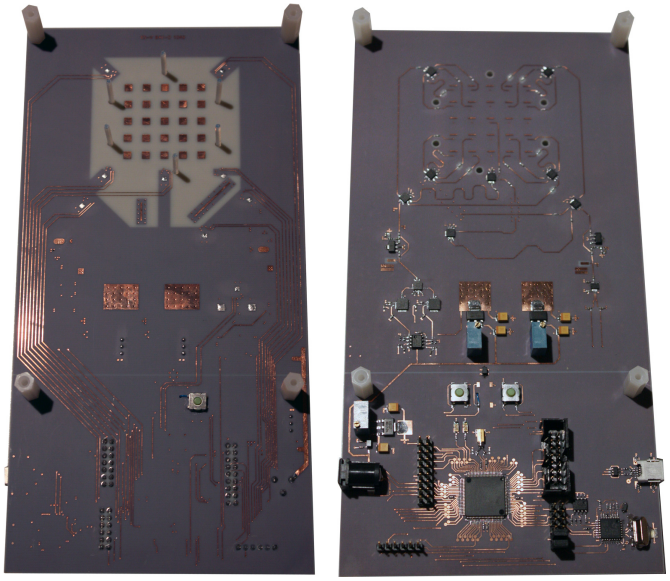

Fig. 5. a) The RFID-CoA reader's top RF plane, including the antenna (top), b) The RFID-CoA reader's bottom digital plane, including the MCU (bottom).

analog and digital components of which are annotated. The board occupies a 3.85 in x 7.8 in area and consists of four metallic and three substrate layers, the total thickness of which does not exceed 1.6 mm. The substrate of the board is FR-408 with relative dielectric constant ε_r = 3.715 in our near field frequency band of interest (5 – 6 GHz), relative permeability μ_r = 1 and loss tangent tanδ = 0.01. The antenna array elements are placed on the top two metal layers at planar horizontal and vertical distances of approximately 3 mm between each other. The RF lines are on the top layer (gold colored lines in the diagram of Fig. 4). The ground plane is placed on the third metal layer and the digital control lines on the bottom layer (turquoise colored lines in the diagram of Fig. 4). A micro-controller unit (MCU) chip is also housed at the bottom part of the board with the majority of its 40 pins being used for different operations, as described in a following subsection. It should be noted that, for this single board solution to be realized and maintain its high efficiency, rigorous simulations on ADS[1] had to be carried out. In particular, the optimal placement of the MCU chip and its supporting components involved two main goals, namely the elimination of the electromagnetic interference between digital and analog circuitry and the signal integrity preservation of the RF fingerprint.

A. RF Part

A very critical component of the reader is, first of all, the antenna array. Since it was desired that the planar dimensions of the first generation of CoAs do not exceed 1 in x 1 in for practical reasons, such as mounting them on small sized products, and given that the certificate read-out involves the near field response of its scatterers, the antenna array should also occupy the same area. On the other hand, it was desired that a single RF fingerprint consist of as a large set of S_{21} curves of antenna element couplings as possible. These contradictory design requirements necessitated the use of an antenna folding minimization design technique that enormously helps in packing as many individual microstrip patch antennas as possible in the aforementioned area. By choosing an operating frequency range of 5 - 5.8 GHz that yields a half wavelength (λ/2) of around 2.75 cm, we eventually managed to fit 25 (5x5) elements within the constrained 1 in x 1 in area available. Special care has also been taken so that the placement of the RF-CoA instance, during the read-out, is fixed and geometrically unique by aligning the latter with short plastic bars, the relative position of which is non-symmetrical on the array's plane; see Fig. 5a.

As shown in the insert picture in the upper right corner of Fig. 4, out of the 25 elements, nine are operating as transmit-only antennas and eight of them as receive-only antennas. The transmit-only and receive-only elements have been arranged as shown in Fig. 4, each type placed as far away as possible from the other type in the four corners of the array. The reason for doing this and rendering the remaining eight elements on the middle horizontal and vertical line of the structure unusable (unconnected), with the exception of the central element, is that we wanted to minimize the coupling of an antenna pair due to proximity and, thus, attribute most of the coupling measured to the presence of the metallic material of the CoA. A particular antenna transmit and receive coupling, out of the board's 72 possible permutations, is selected by digitally controlling eight identical single-pole four-throw (SP4T) RF switches. The placement of the switches on the board has also been optimized so that the coupling between the RF lines is minimized.

B. Digital (MCU) part

The control of all the digital and analog components of the reader is performed by a 16-Bit RISC architecture ultra-low-power TI MCU[2] that features an up to 18-MHz System Clock,

[1] Advanced Design System (ADS) Simulation Environment, Agilent. [Online]. Available: http://www.home.agilent.com/.

[2] MSP-EXP430F5438 Experimenter Board User's Guide (Rev. E), Texas Instruments, Oct. 2010.

high-frequency crystals up to 32 MHz and multiple, high-resolution analog-to-digital converters (ADC). In particular, the functionality of the MCU in regards with this application is summarized in the following four main tasks: (i) generates the appropriate RF power and controls the frequency output of the voltage-controlled oscillator (VCO)[3], (ii) 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, (iii) measures the power captured by the power detector[4] by monitoring its output voltage and (iv) uploads the set of measured data that comprise the RF-CoA's fingerprint to a computer host or server.

The MCU provides multiple digital output pins for controlling the SP4T switches, a connection to a physical push button, a USB interface for data transfer and powering (if battery operation is not desired) and two different RF interfaces, where very small, Zigbee and Bluetooth modules can be attached. Specifically, two very good such compatible wireless networking module options are TI CC2530[5] and TI CC2540[6], for Zigbee and Bluetooth, respectively. Of course, a JTAG interface is also provided for re-programming the MCU.

The algorithm implemented by the reader is fairly simple. When the power switch of the USB or 3 AA batteries powered board is turned on, the MCU 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 is provided. In short time intervals the 32 kHz auxiliary clock is enabled and used to check if the button is pressed. As soon as a "press" is detected, the MCU exits the deep sleep mode and initiates the antenna permutation task. Here a particular antenna element pair (one antenna element to illuminate the RF-CoA and the other to receive the scattered energy) is selected by appropriately configuring the two digital logic control pins (0 V_{dc} for "logical 0" and 3.2 V_{dc} for "logical 1") of the SP4T switches. 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.

For every particular antenna element pair, the S_{21} RF-CoA fingerprint is captured over the frequency band of 5 to 5.8 GHz at steps of 12 MHz. The selection of these steps is made by altering the board's voltage control oscillator's tune voltage. Since the MCU provides no DACs, the latter's functionality is emulated by a high-frequency pulse width 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 regulated USB or battery rail of 3.2 V. With the T_x antenna element radiating a sinusoidal power signal at a particular, nearly monochromatic, frequency toward the CoA that is placed against the antenna matrix, the next step is to amplify the captured reflected and refracted signal and feed it to the board's power detector. This component's output voltage, which essentially represents the received signal strength, is read by the ADC of the MCU with its highest, 12-bit precision, mode.

It should be noted that we have found that a single analog-to-digital conversion is not enough. In particular, although the voltage reference used (3.2V) 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 only few, however, measurements out of 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 analog-to-digital converters [5] 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 [6]. As a result, we conduct 20 consecutive measurements of a CoA at a particular antenna configuration and frequency, store them in the successive approximation register of the MCU and afterward simply average them. Eventually, this deviation easily drops to less than 8%, which still constitutes a source of inaccuracy by itself.

After the above steps are completed, the MCU algorithm performs a check of whether the maximum number of frequency steps up to 5.8 GHz has already been reached, in which case the full frequency spectrum for a single antenna permutation has been swept and the MCU jumps to the next antenna permutation. This is when a check is also done about whether the maximum number of antenna permutations, namely 72, has already been selected; in which case the MCU uploads the captured RFID-CoA fingerprint to the local server before it reverts to its LPM4 sleep mode.

IV. Performance Analysis

This section aims to quantify the uniqueness, or entropy, among different RF fingerprints extracted from different CoA designs by our prototype reader. However, establishing the performance figures behind our RFID-CoA technology is a complicated process. Any dependencies among variables are obfuscated and their independence, although not totally true as an assumption, has been observed in our experiments and is hereafter assumed. Statistical tools that could aid establish independence are for most cases not useful for the simple reason that it is difficult to acquire readings en masse. We have, thus, followed the following approach.

First, we consider a two-class binary classification problem, in which the outcomes are labeled either as positive (P), i.e. measurements of same CoA, or negative (N), i.e. measurements of different CoAs. Out of the four possible outcomes from a binary classifier, we are interested in analyzing the false positive (FP) and false negative (FN) outcomes. Specifically, if the outcome from a prediction is P and the actual value is N then we have a FP, i.e. the CoA is fake and predicted as authentic. Conversely, a FN has occurred when the prediction outcome is N while the actual value is P, i.e. the CoA is authentic and predicted as fake.

[3] Voltage Controlled Oscillator mmIC with buffer amplifier. [Online]. Available: www.hittite.com/content/documents/data_sheet/hmc430lp4.pdf.

[4] 6GHz RMS Power Detector, Linear. [Online]. Available: http://cds.linear.com/docs/Datasheet/5581fa.pdf.

[5] A True System-on-Chip Solution for 2.4-GHz IEEE 802.15.4 and ZigBee Applications, Texas Instruments, April 2009. [Online]. Available: http://focus.ti.com/lit/ds/symlink/cc2530.pdf.

[6] 2.4-GHz Bluetooth® low energy System-on-Chip, Texas Instruments, Oct. 2010. [Online]. Available: http://focus.ti.com/lit/ds/symlink/cc2540.pdf.

From the intra- and inter-CoA differences, we can compute the associated false positive and false negative probabilities.

Let (p_1, p_2, …, p_k) be independent and identically distributed random samples drawn from the distribution of the following array for the same antenna permutation and frequency point: p = (antenna permutation out of 72, frequency point out of 65, 1:k measurements of same CoA). Appropriately, let (n_1, n_2, …, n_k) be independent and identically distributed random samples drawn from the distribution of the following array for the same antenna permutation and frequency point: n = (antenna permutation out of 72, frequency point out of 65, 1:i:k measurements of k different CoA_i). As mentioned previously, this assumption about independence is not totally realistic, but it is difficult to understand the dependency because of the difficulty involved with inverting over Maxwell's equations. In other words, although responses over neighboring transmitter-receiver couplings are dependent due to physical properties of the responses, computing these dependencies is an overly difficult computation task, equivalent to the direct design problem over the Maxwell equations. To make this assumption stronger, however, later in the "score computation" step, we are skipping frequency samples from responses by taking only every 8th frequency sample from the 1st to the 65th.

In order to compute the probability density function (PDF) of a true positive (TP), we read the same RFID-CoA instance multiple times with a single reader in the presence of misalignment noise because of the fact that the plastic poles were not firm enough as they were just glued on the board (see Fig. 5a). This misalignment, on the order of 1mm[7], was substantially higher than what would be expected in a commercial application, as sub-0.1mm mechanical alignment is easy to achieve. For k measurements of the same CoA, we compute the binomial coefficient (k 2), i.e. k*(k-1)/2, differences among samples of the same set (intra- or inter-) for each antenna permutation and frequency point.

All readings for a single antenna coupling are grouped and we estimate the logarithm base 10 of the PDF for each antenna permutation and frequency point of the above random variable by applying the most popular non-parametric way, namely the kernel density estimation (KDE). We use KDE to establish a conservative estimate of the underlying distribution of responses, instead of using histograms that are too rough to be true since they are estimates of PDFs based on data only. The KDE estimates the true distribution from a given histogram given some assumptions that are described in [8]. Specifically, we use the KDE implementation of Botev et al. [8] for estimation of PDFs at the individual antenna pairing level because it is very conservative and limits problems, such as those caused by multimodal densities with widely separated modes. The reason this KDE is conservative is because it fits each point with a thick Gaussian of specific bandwidth and add them up to minimize the distance metric. Each one of the above curves is then extrapolated to calculate the probability of being a TP for each reading of a TN. The sum of the maximum likelihoods then produces final scores for each outcome. In other words, the score is equal to the maximum log-likelihood computed using the aforementioned density estimation technique.

Finally, we model the overall resulting scores as PDFs again using the pure Gaussian based KDE because of the vast amount of data averaged. The result is that we now have the two final PDF "bells" that model the FP (right curve) and FN (left curve) error probabilities. Fig. 6a-c illustrate these two final maximum likelihood results. The x-axis quantifies the average per-coupling score for an instance being measured against its positive (intra-CoA) or negative (inter-CoA) differences. The y-axis captures the maximum likelihood that a specific score corresponds to a hypothesis. These results are based on 10 duplicate measurements of the exact same CoA and on different RF-CoA measurements summarized in different experimental cases (a - d) below. Specifically, for the same CoA measurements, 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 and the whole process is repeated nine times. As for the different CoA measurement scenarios, these include: (a) 17 different CoAs of 2 gr copper wire each, (b) 15 different CoAs of 3 gr copper wire each, (c) 15 different CoAs of 4 gr copper wire each and, finally, (d) all the 47 above different CoAs.

The results of Fig. 6 show that probability of intersection of the FP and FN error probability curves is smaller than 10^{-200} for any of the same gauge copper-based CoA scenarios and almost 10^{-300} considering all available CoAs. In other words, the probability that our system predicts a fake CoA as authentic or predicts an authentic CoA as fake is inconceivably small. In such a situation, where the two curves that describe FP and FN do not meet in the precision range of 64-bit arithmetic, we felt that providing a receiver operating characteristic (ROC) would be too inaccurate.

V. RFID-CoA Application Overview

A. RFID-CoA System Life Cycle: From factory to store

In the previous sections we provided the technical details of the reader and the CoA instance, as well as a performance analysis of our system. In our effort to provide all aspects of our proposed complete anti-counterfeiting solution, we are presenting in this Section the entire life cycle of an RFID-CoA instance ranging from the fabrication process to the point when a client checks out a product.

An example fabrication process that we followed for the first series of our prototype CoAs has been provided in Section II. Regardless, however, of this process, the succeeding stages that a certificate goes through before being attached to a product and making it to the shelf of a store are the same and described below.

The first main procedure, which takes place in the controlled environment of a fabrication facility right after the fabrication has completed, is the *RFID-CoA Issuing*. This procedure consists actually of a number of steps, shown in Fig. 7, that the certificate issuer follows in order to digitally sign the instance's RF fingerprint using traditional and long-trusted cryptography. Specifically, first a reader is used to digitize the unique RF fingerprint of the newly fabricated RFID-CoA instance. This digitized form, which consists of

[7] A first quantification analysis of the response sensitivity to slight misalignment of the COAs with respect to the reader is provided in [7].

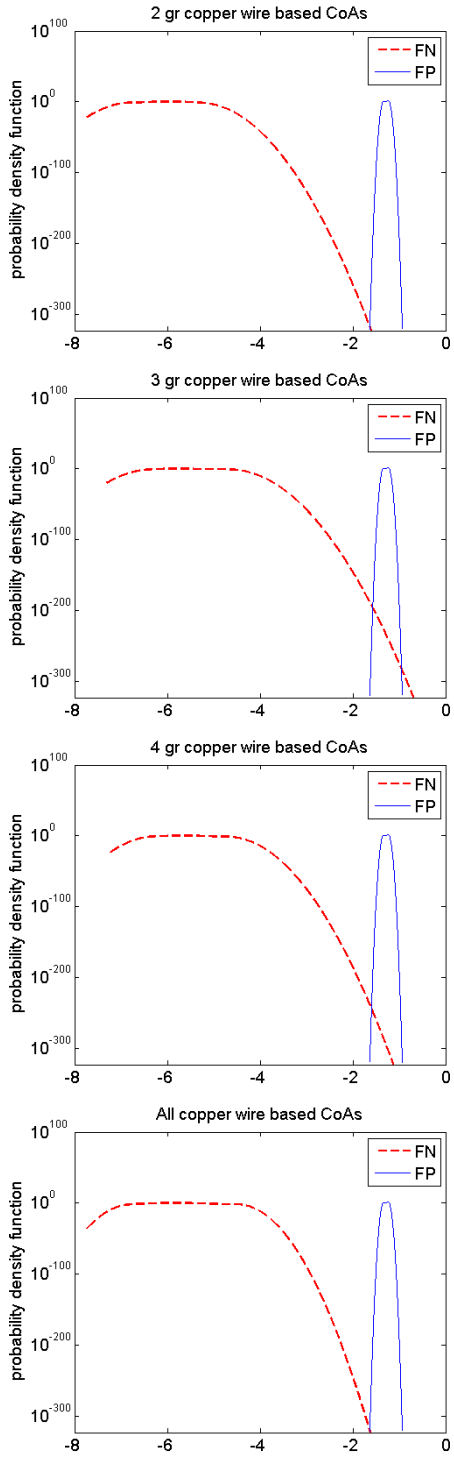

Fig. 6. The probability density function curves that model the false positive (solid) and false negative (dashed) error probabilities for (a) 17 different CoAs of 2 gr copper wire each, (b) 15 different CoAs of 3 gr copper wire each, (c) 15 different CoAs of 4 gr copper wire each and, finally, (d) all the 47 above different CoAs. The x-axis quantifies the average per-coupling maximum log-likelihood computed for a CoA instance against its positive (intra-CoA) or negative (inter-CoA) differences.

eight, 32-bit accuracy readings across the 5 to 5.8 GHz frequency for all 72 antenna permutations (12 x 72 bytes), is compressed, using any of the numerous available compressing algorithms, into a reduced and fixed length bit string (*f*) of 400 bytes. The information associated with the product (*t*), such as product ID, color and expiration date, is afterward appended to the bit string *f*. A copy of the resulting composite bit string *w* is directly stored to the RFID tag chip, as shown in the diagram of Fig. 7. A second copy is hashed using a cryptographically strong algorithm such as SHA256 [9]. This hash is subsequently signed (*s*) by applying a public-key cryptosystem (PKCS), such as RSA [10], and using the issuer's private key. As was the case with the plain initial bit string *w*, the latter's hashed and signed version *s* is also directly encoded onto the RFID chip. It should be noted that, for the choice of the above compressing, signing and encrypting technologies, altogether the amount of information stored in the RFID chip does not exceed 1 KB. This bit size is fully supported by the latest and very widely used EPC gen2 RFID standard that can handle multiple fragmented packets as well as RFID chip manufacturers that provide such 4 Kbytes non-volatile memory, "high capacity" memories in their chips.

The above digitally encoded information $m=s||w$, which essentially contains a plain and a signed version of the CoA's RF fingerprint, is used to validate whether a product is authentic or not; a process that typically takes place during the arrival of the merchandise at a distribution center, a store's warehouse or customs office and/or the check-out process with a cashier. This *RFID-CoA verification* procedure is conceptually shown in Fig. 8. The verifier, who, as described earlier, can be a depot worker or a teller, uses a regular RFID

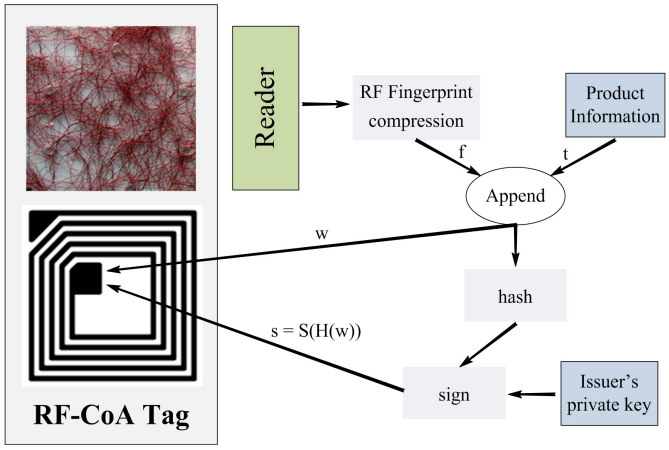

Fig. 7. RFID-CoA Issuing.

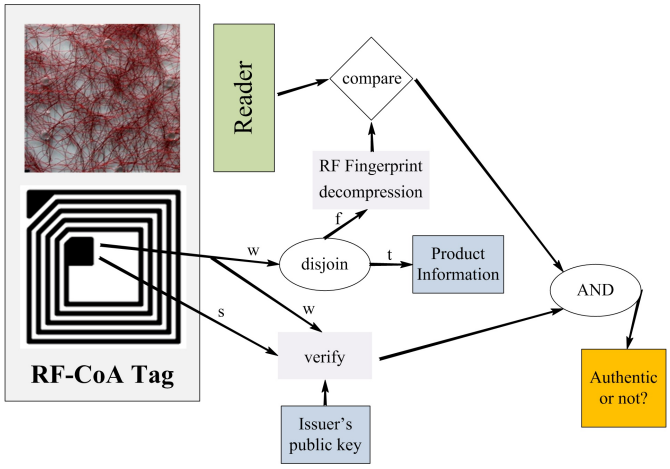

Fig. 8. RFID-CoA Verification.

reader to extract the bit string *m* and verifies the integrity of the plain bit string *w* with respect to its encrypted and signed version (*s*) using the corresponding issuer's public key. If the integrity test is successful, then the verifier can be confident that no one else, except for the possessor of the matching private key, has encrypted the information and, as a result, the compressed RF fingerprint *f* and the associated product data *t* are extracted. The extracted f is finally compared with a new read-out of the tag's CoA that the verifier extracts himself with his own RFID-CoA reader. The comparison / matching is done based on the same distance metric, analyzed in the previous Section, at each antenna coupling (out of 72) and frequency point individually (out of 65).

Only if the level of similarity between these two fingerprints, namely read and extracted, exceeds a pre-defined and statistically validated threshold, the verifier declares the CoA instance to be authentic. As shown in the analysis described in Section IV, this level of similarity corresponds to a worst-case maximum probability for a false alarm of 10^{-200}, which is totally outstanding and not even expected to occur in one's lifetime.

One last note that relates to the ease of use and portability of our RFID-CoA reader within store premises or industrial facilities is that the incorporated MCU chip allows for wireless connectivity and relay of the extracted CoA data on top of the standardized and highly reliable Zigbee Pro and Bluetooth wireless networking standards to a central location and a mobile device, respectively, over AES (Advanced Encryption Standard)-128 bit encrypted wireless links.

B. Potential Attacks

The anti-counterfeiting nature of our system and the consequent benefits from counterfeiting RFID-CoA protected objects render a discussion about potential attacks imperative.

As described above, the RFID-CoA issuing relies on the use of asymmetric key algorithms that involve the use of a public key known to everyone and a secret private key. The keys are related mathematically, but it is virtually impossible to deduce the private key from the public key. So, in our application only the issuer can digitally sign the RFID-CoA with the secret private key. Nevertheless, one potential attack could be to directly compute the issuer's private key. This would allow an adversary to store his one fixed-length bit string *f* and achieve an always-successful signature verification and authenticity validation. The solution to this potential attack is to make the private key computation arbitrarily difficult and time consuming by adjusting the key length of the used public-key crypto-system at the expense of a larger amount of information stored in the RFID chip; as mentioned in the previous subsection, this is totally possible.

A second attack could involve misappropriating signed CoA instances and placing them on counterfeit products. However, this type of attack requires the attacker have knowledge of the exact, unique serial number of the genuine product the CoA was originally intended for. This can only be possible if the issuer's private key is computed, which essentially becomes equivalent to the previous discussed attack, or if the RFID-CoA tag is removed from the original protected product, which is a responsibility of the seller. In the latter case, the particular RFID-CoA tags can just be rendered invalid from the central database.

Also an adversary could potentially attempt to 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, it is required that the counterfeiter not only has physical access to the original CoA but also the ability to accurately scan and reconstruct arbitrary 3D structures and embed them in a soft or hard encapsulating sealant. This results to a very high-cost adversarial manufacturing process. From this last attack's perspective, it is obvious that an RFID-CoA can be used to protect an object, the value of which does not exceed the cost of forging a single CoA instance.

C. Applications

As referred to previously, the cost of an RFID-CoA tag is expected to be double the price of a typical RFID tag in the order of a few USD cents and the prototyping cost of a single reader is lower than 50 USD. Considering, on one hand, that the low cost of the RFID-CoA system can be pushed even further down with the economies of scale and, on the other hand, that a significant part of the trade losses due to counterfeiting can be eliminated, we believe that the implementation potential of the RFID-CoA system in a large array of business applications is great.

VI. Related Work

The use of RFID tags against counterfeiting has been proposed in the past. As mentioned earlier, given that the simple digital encoding of the tags cannot be relied upon, Juels [11] has provided a survey of research efforts to replace the basic RFID tags with "symmetric-key tags" that are capable of computing symmetric-key functions. The same survey cites a number of demonstrated, successful attacks against these tags, as well as research proposals to close these security gaps.

Researchers soon realized that hardware-based CoAs that can complement the RFID tags comprise a more effective solution to the problem. Bauder [12] and Simmons [13] were the first to suggest exploiting the physical properties of disordered systems for authentication purposes based on the Physical Unclonable Function (PUF) of practical cryptography. The PUF provides a mean to produce unclonable tokens for identification based on challenge-response pairs, the idea behind this being that a set of specific challenges applied to the structure are mapped to a set of responses of a complex physical system. Tuyls et al. [14] proposed the fabrication of RFID-tags whose microchips are equipped with a PUF. Although not feasible in the off-line case as in [14], Devadas et al. [15] presented an actual fabrication of a PUF-enabled RFID chip in 0.18μ technology. Our RFID-CoA solution, first of all, does not fall under this PUF category simply because it does not rely on non-reusable, one-time challenge-response pairs with the potential added overhead of recharging the challenge-response database and the entropy of our CoAs do not rely on small, yet indeed

unpredictable, manufacturing process inaccuracies. Moreover, as opposed to the above PUF solutions, our CoA is completely passive, not consuming any power from the tag chip and potentially decreasing its read range, our COAs' fabrication is decoupled from the chip fabrication process and does not require an expensive μ fabrication technology, no RFID reader software modifications are needed and, thus, our solution works with any RFID technology, our authentication procedure is in most cases meant to take place off-line, i.e. without looking up an online database, and our fingerprint entropy is temperature independent.

In addition to the number of limitations and security vulnerabilities of far field communication outlined in Section II, applications in this RF domain have even been proposed to detect the CoA's random structure over the expensive millimeter wave frequency range [16]. Under the same far field category also fall the chipless RFID tags proposed for authentication applications. However, their common main shortcoming is that the entropy they provide is only limited to only a two-digit sequence of bits. Preradovic et al. [17] demonstrate a printable chip-less RFID tag for secure banknote applications in the 5-7 GHz frequency band, the anti-counterfeiting robustness of which relies only on a bit sequence formed by a multi-resonating circuit and CrossID, Inc [18] has tested a chip-less, chemical material based RFID tag with each of the 70 different chemicals being assigned its own position in a 70-digit binary number and entailing the use of 3 to 10 GHz readers.

Regarding the near field domain, on the other hand, Romero et al. [19] describe a method of quantifying the electromagnetic characteristics of the near field coupling nature of the RFID transactions with ISO 14443 tags for counterfeit detection applications. Their finest electromagnetic signature consists of the fundamental and harmonics up to the ninth harmonic of a 13.56 MHz RF carrier that are measured with a real-time oscilloscope with a maximum sampling rate of 20 GHz. Contrary to this platform, our RFID-CoA solution requires no expensive reader to read any harmonics and instead makes use of a less than 50 USD reader, requires no closed-loop, synchronized control system between the RFID reader and an oscilloscope or other reader, and can simply be used with any RFID tag technology of any frequency band.

VII. Conclusion

In this paper, we presented all aspects of our proposed complete anti-counterfeiting system, the RFID-CoA. To the best of our knowledge, our proposed system is the first to add anti-counterfeiting capabilities to traditional RFID tags in a very low-cost and robust manner by simply relying on the near-field observation of very cheap, randomly structured conductive physical objects.

Our system's robustness with virtual not a single false alarm in one's lifetime, its fast and versatile certificate extraction and wireless data relay provision, its resistivity against third-party malicious attacks, its low power operation and portability, and, on top of all, its very low cost are characteristics that make it applicable to nearly any physical object that needs protection against counterfeiters.

Acknowledgments

This work was partially funded by IFC/SRC and the Oversea Distinguished Professor Program. The authors would also like to thank the anonymous reviewers for their insightful comments and Prof. Dale R. Thompson for shepherding this paper.

References

[1] Glaxo-Smith-Kline. 2009, Counterfeiting Report. Available: http://www.gsk.com/responsibility/supply-chain/counterfeiting.htm

[2] B. S. Alliance. 2009, Seventh Annual Global Software Piracy Study. Available: http://portal.bsa.org/globalpiracy2009/studies/globalpiracystudy2009.pdf

[3] M. Robyn, "Market-Driven Fraud: The Impact and Consequences of Counterfeit Products and Intellectual Property Violations," St. Louis, Missouri 2008.

[4] L. Tsang, J. A. Kong, and R. T. Shin, *Theory of microwave remote sensing*. New York: Wiley, 1985.

[5] J. Blair, "Sine-fitting software for IEEE Standards 1057 and 1241," in *Instrumentation and Measurement Technology Conference, 1999. IMTC/99. Proceedings of the 16th IEEE*, 1999, pp. 1504-1506 vol.3.

[6] K. Hejn and A. Pacut, "Sine-wave parameters estimation - the second source of inaccuracy," in *Instrumentation and Measurement Technology Conference, 2003. IMTC '03. Proceedings of the 20th IEEE*, 2003, pp. 1328-1333 vol.2.

[7] G. DeJean and D. Kirovski, "Making RFIDs unique - radio frequency certificates of authenticity," in *Antennas and Propagation Society International Symposium 2006, IEEE*, 2006, pp. 1039-1042.

[8] Z. I. Botev, J. F. Grotowski, and D. P. Kroese, "Kernel density estimation via diffusion," *Annals of Statistics,* vol. 38, pp. 2916-2957, 2010.

[9] National Institute of Standards and Technology (U.S.). (2008). *Secure hash standard (SHS)*. Available: http://purl.access.gpo.gov/GPO/LPS121031

[10] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM,* vol. 21, pp. 120-126, 1978.

[11] A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on,* vol. 24, pp. 381-394, 2006.

[12] D. W. Bauder, "An anti-counterfeiting concept for currency systems," Sandia National Labs, Albuquerque NM, PTK-11990, 1983.

[13] G. Simmons, "A system for verifying user identity and authorization at the point-of sale or access," *Cryptologia,* vol. 8, pp. 1–21, 1984.

[14] P. Tuyls and L. Batina, "RFID-Tags for Anti-counterfeiting," in *Topics in Cryptology – CT-RSA 2006*. vol. 3860, D. Pointcheval, Ed., ed: Springer Berlin / Heidelberg, 2006, pp. 115-131.

[15] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *RFID, 2008 IEEE International Conference on*, 2008, pp. 58-64.

[16] Inkode, Inc. [Online]. Available: http://www.inkode.com

[17] S. Preradovic and N. C. Karmakar, "Design of fully printable chipless RFID tag on flexible substrate for secure banknote applications," in *Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference on*, 2009, pp. 206-210.

[18] CrossID, Inc. [Online]. Available: http://innovya.com/CrossID/

[19] H. P. Romero, K. A. Remley, D. F. Williams, and W. Chih-Ming, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," *Microwave Theory and Techniques, IEEE Transactions on,* vol. 57, pp. 1383-1387, 2009.