Certifying Authenticity using RF Waves

Gerald DeJean† and Darko Kirovski‡
† School of ECE, Georgia Institute of Technology, Atlanta, GA 30332, USA
‡ Microsoft Research, Redmond, WA 98052, USA

Abstract— **A certificate of authenticity (COA) is an inexpensive physical object that has a random unique structure with high cost of near-exact reproduction. An additional requirement is that the uniqueness of COA's random structure can be verified using an inexpensive device. We propose a design for objects that behave as COAs in the electromagnetic field. The objective is to complement RFIDs so that they are physically, not only digitally, unique and hard to replicate. By enabling this feature, we hope to create a super-tag whose information about the product can be read within a relative far-field, and also whose authenticity can be verified within its near-field with low probability of a false alarm. A peculiar feature of our system, not exhibited in previous proposals, is the difficulty of creating a COA instance that produces a given response. In this paper, we outline a proposal for the design of RFCOA instances, we present a prototype reader, and analyze the achieved system entropy.**

I. Introduction

A COA is a digitally signed physical object that has a random unique structure which satisfies three requirements:

- the cost of creating and signing original COAs is small, relative to a desired level of security,
- the cost of manufacturing a COA instance is several orders of magnitude lower than the cost of exact or near-exact replication of the unique and random physical structure of this instance, and
- the cost of verifying the authenticity of a signed COA is small, again relative to a desired level of security.

An additional requirement, mainly impacted by a desired level of usability, is that a COA must be robust to ordinary wear and tear. COA instances can be created in numerous ways. We investigate which objects behave as COAs in the electromagnetic (EM) field and the kind of properties they offer as counterfeit deterrents. RFCOAs are built based upon several **near-field** phenomena that RF waves exhibit when interacting with complex, random, and dense objects:

- Arbitrary dielectric or conductive objects with topologies proportional in size to wave's wavelength behave as significant electromagnetic scatterers [1], i.e., they reradiate large amount of electromagnetic energy into free space.
- Refraction and reflection of RF waves at the boundary of two media can produce hard-to-predict near-field effects; the phenomenon is modeled based upon the generalized Ewald-Oseen extinction theorem [2].

In general, an object created as a random constellation of small (diameter $>$ 1mm) randomly-shaped conductive and/or dielectric objects should have distinct behavior in its near-field when exposed to EM waves coming from a specific point and with frequencies across the RF spectrum.

The key to system efficacy is to produce a reader capable of reliably extracting an RF "fingerprint" from a COA instance in the high, but still inexpensive range of frequencies (e.g., 5-6GHz). In order to disturb the near-field of the COA instance, we build it as a collection of randomly bent, thin conductive wires with lengths randomly set within 3-7cm. The wires are integrated into a single object using a transparent dielectric sealant illustrated in Figure 1. The sealant fixes wires' positions within a single object once for all.

The "fingerprint" of such a COA instance should represent the 3D structure of the object. To address this issue, we propose a reader built as a matrix of antennas with an analog/digital back-end. Each antenna can behave as a transmitter or receiver of RF waves in a specific frequency band supported by the back-end processing. For different constellations of dielectric or conductive objects between a particular transmitter-receiver coupling, the scattering parameters for this coupling are expected to be distinct. Hence, in order to compute the RF "fingerprint," the reader collects the scattering parameters for each transmitter-receiver coupling in the group of antennas.

Reader's measurements represent the EM effects that occur in the near-field of the transmitter, the COA instance, and the receiver; distances between any two objects are proportional to the wavelengths of interest. We observe EM effects in the near-field for several reasons:

- It is hard to maliciously jam near-field communication.
- The reader can operate with low-power, low-efficiency antenna designs.
- The variance of the EM field is relatively high in the near-field, causing better distinguishing characteristics. Far field responses typically represent certain average characteristics of random discrete scatterers ([3], Chapter §6), thus, such responses lose the ability to represent the scatterer's random structure.
- Computing the actual RF responses numerically is a hard task. In general, while all RF phenomena are analytically explained using the Maxwell equations, even fundamental problems such as computing responses from simple antennas with regular geometries, are notoriously intensive computational tasks with arguable accuracy [1], [4].

We built a prototype RFCOA scanner as a matrix of 5x10 antennas that measure the unique RF "fingerprint" of an RFCOA instance as a collection of transmission responses in the 5-6GHz frequency range for each transmitter-receiver coupling on the reader. RFCOA instances were placed at about 0.5mm from the antenna matrix, i.e., in the near-field of the scanner.

While the analog/digital back-end in our testbed was resolved using an off-the-shelf network analyzer, we speculate that a custom reader could cost less than US$100 if manufactured en masse.

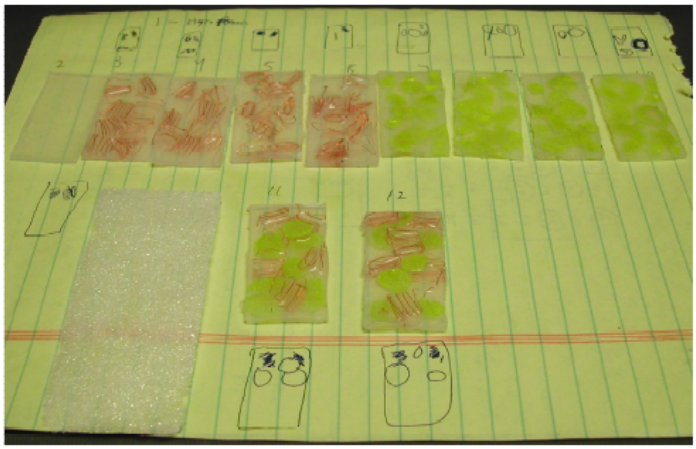

Fig. 1. Examples of RFCOA instances built from 22gauge copper wire as a conductive resonator, Play-doh objects of different shape and Dragon Skin^{TM}silicone rubber as sealant. They were equally sized at 25x50x3mm using an acrylic mold. At retail prices of each of the components, the price per instance was around five cents. Aluminum wire and mass production should bring the pricing to the sub-cent range per instance.

A. Issuing, Verification, and Attacks

When creating an RFCOA instance, the issuer digitally signs instance's RF response using traditional cryptography as follows. First, the unique RF "fingerprint" is digitized and compressed into a fixed-length bit string f. Next, f is concatenated to the information t associated with the tag (e.g., product ID, expiration date, assigned value) to form a combined bit string $w = f||t$. Message w is then hashed using a cryptographically-strong algorithm $H()$ such as SHA256 [5]; next, the hash is signed using the private key of the issuer to create a message $m = w||S(H(w))$. Function $S()$ is the signing primitive of an adopted public-key cryptosystem (PKCS) such as RSA [6]. Message m is encoded directly onto the COA instance using existing technologies such as 2-D barcodes or RFIDs. In order to reduce the length of m, one possibility is to use a PKCS based upon elliptic curves [7]. Message m is used to validate in-field that the produced instance is authentic. Each RFCOA instance is associated with an object whose authenticity the issuer wants to vouch.

Once issued, an RFCOA instance can be verified **off-line** and in-field by anyone using a trusted reader, i.e., a reader that contains the corresponding public key of the issuer. Verifying a COA instance involves the following steps. First, the verifier reads $m = w||S(H(w))$ from the attached physical storage and verifies the integrity of w with respect to $S(H(w))$ using issuer's public key and a verification primitive $V()$ that corresponds to $S()$. In case the integrity test $V(w, S(H(w)))$ is successful, the original RF "fingerprint" f and associated data g are extracted from w. The verifier proceeds to scan the actual RF "fingerprint" of the attached RFCOA, i.e., obtain a new reading of the instance's RF properties, and compare them with f. If the level of similarity between f and f' exceeds a pre-defined and statistically validated threshold, the verifier declares the COA instance to be authentic and displays t. In all other cases, the reader concludes that the instance is not authentic, i.e., it is either counterfeit or erroneously scanned.

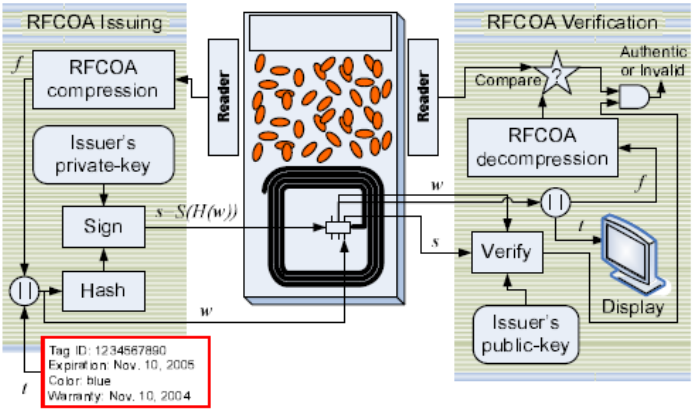

Fig. 2. Issuing and verifying an RFCOA.

To counterfeit protected objects, the adversary needs to:

(*i*) compute the private key of the issuer – a task which can be made arbitrarily difficult by adjusting the key length of the used public-key crypto-system [5], or

(*ii*) devise a manufacturing process that can exactly replicate an already signed COA instance – a task which is not infeasible but requires certain expense by the malicious party – the forging cost dictates the value that a single COA instance can protect [8], or

(*iii*) misappropriate signed COA instances – a responsibility of the organization that issues COA instances.

From that perspective, COA can be used to protect objects whose value roughly does not exceed the cost of forging a single COA instance including the accumulated development of a successful adversarial manufacturing process (*ii*).

B. Related Work

COAs in the RF domain have been proposed by several companies [9], [10], [11], [12], [13], all of them aiming to detect COA's random structure in the far-field. Such detection is prone to spoofing; also such COAs can be relatively easily near-exactly replicated. Because the detection is taking place in the far-field, some of these systems operate in the "expensive" 60GHz frequency range. The motivation for the research focus presented in this paper is complex. First, our RFCOA designs require a true 3D manufacturing (3DM) ability by the counterfeiter, i.e., the ability to create arbitrary 3D structures and embed them in a soft or hard encapsulating sealant. In certain scenarios, the structures could be made from homogeneous liquids. In all cases, the cost of near-exact replication of such COAs is greatly raised. Second, since the readout of their random structure does not require a reader-object contact, RFCOAs may be built with superior wear and tear properties. Next, as shown later in this manuscript, for a credit-card sized RFCOA and a reader that operates in the 5-6GHz frequency subband, the entropy of the readout response

from RFCOAs easily tops several thousand bits making the likelihood of accidental collusion negligent.

Our proposal has an important qualitative feature not exhibited by other types of COAs. For a given RF "fingerprint" f, it is difficult to numerically design the 3D topology of an instance that would produce f accurately. Practically, let's assume the application where credit cards are protected using RFCOAs. By accessing full credit card information from a merchant database (e.g., holder's name, card's number and expiration date, PIN code, *and* COA response), it would be still difficult for the adversary to create a physical copy of the original credit card produced by the issuing bank even if the counterfeiter owned a 3DM. To complete the operation, the adversary would have to gain physical access to the original credit card and accurately scan its 3D structure.

II. RFCOA Scanner

In order to scan the EM features of an RFCOA, we propose a scanner designed to expose the subtle variances of near-field responses of these objects to RF waves. We introduce an RFCOA scanner that consists of an antenna matrix, where each of the antennas is capable of operating both as a transmitter and a receiver. The antennas are multiplexed to an analog/digital back-end capable of extracting the $s_{2,1}$ parameter (i.e., insertion loss) for a particular antenna coupling. During the read-out, the antenna matrix is placed against the RFCOA instance. The instance should have an absorbent and/or reflective background so that the environment behind the tag does not affect its RF response. By placing the instance in the close proximity of the antenna matrix as illustrated in Figure 3, one can collect numerous measurements including all s-parameters. For example, for a system with M antennas, one can measure M $s_{1,1}$ and $\binom{M}{2}$ $s_{2,1}$ parameters. The positioning of the instance with respect to the reader should be approximately the same for each reading. Depending upon the accuracy of the analog and digital circuitry as well as the noise due to external factors, one can aim to maximize the entropy of this response.

A. Individual Antenna Patch Design

We designed a prototype scanner in two steps. First, we designed an individual microstrip antenna patch with an operating frequency close to the 5GHz range with an emphasis on miniaturization. As we wanted to pack as many as possible antennas in a credit-card sized space, we opted for two minimization techniques: folding [14] and meandering [15]. Although the two techniques have already been applied to individual designs, to the best of our knowledge this is the first study, both in simulation and implementation, that combines the two methods into a single design. It is illustrated in Figure 3; its technical characteristics and design strategy are detailed in [17]. The major criteria in the return loss plot is the resonance of the antenna at a frequency around 5GHz. In simulation of this system, the return loss is -16dB at a resonant frequency of 4.933GHz. The physical size of a single patch antenna that operates around the same frequency for a similar size substrate (RF60) is approximately five times larger than the design considered in this paper.

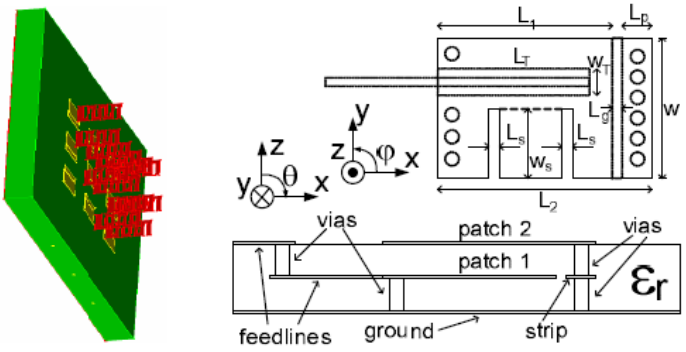

Fig. 3. (left) Simulation setup for an RFCOA reader built as a matrix of patch antennas and a low entropy constellation of resonant pieces placed in close proximity of the reader. (right) Detailed design of the individual microstrip antenna and connecting vias using folding and meandering.

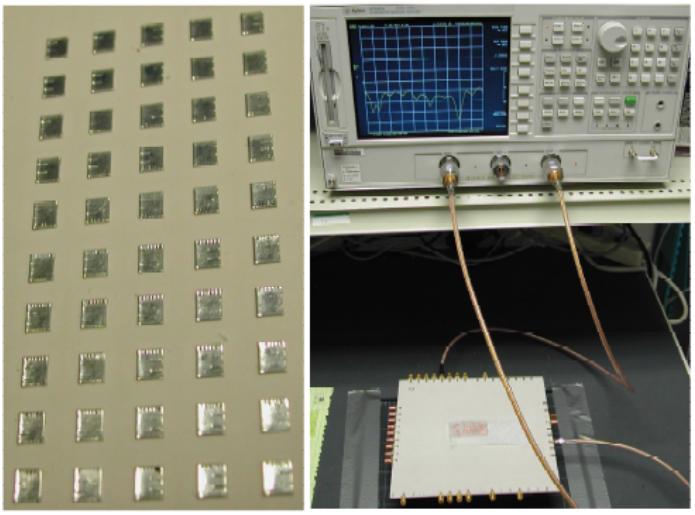

Fig. 4. Prototype antenna matrix (left) and an experiment (right). The RFCOA is isolated from the matrix panel using a 20 mil layer of styrofoam.

Based upon the simulated design, we constructed an extended panel prototype that consists of 50 antennas (five rows, ten columns). It was designed and fabricated on RF60 substrate with a total thickness of 62 mils. The fabrication of the design was performed by Prototron Circuits, Inc. Fifty edge mount RF coaxial connectors were soldered to the ends of all feedlines of the antennas. Transmission measurements of the antennas were performed using an Agilent 8753E vector network analyzer. Calibrations were performed to the end of the coaxial cables. The $s_{2,1}$ parameter was taken for many antenna couplings. The tester would manually attach and detach the ends of the cables to the connectors to switch to the different parameters. Figure 4 illustrates the prototype and Figure 1 presents the developed RFCOA test-instances.

III. Empirical Evaluation

In the first set of experiments, we aimed at quantifying the response sensitivity to slight misalignment of the COA

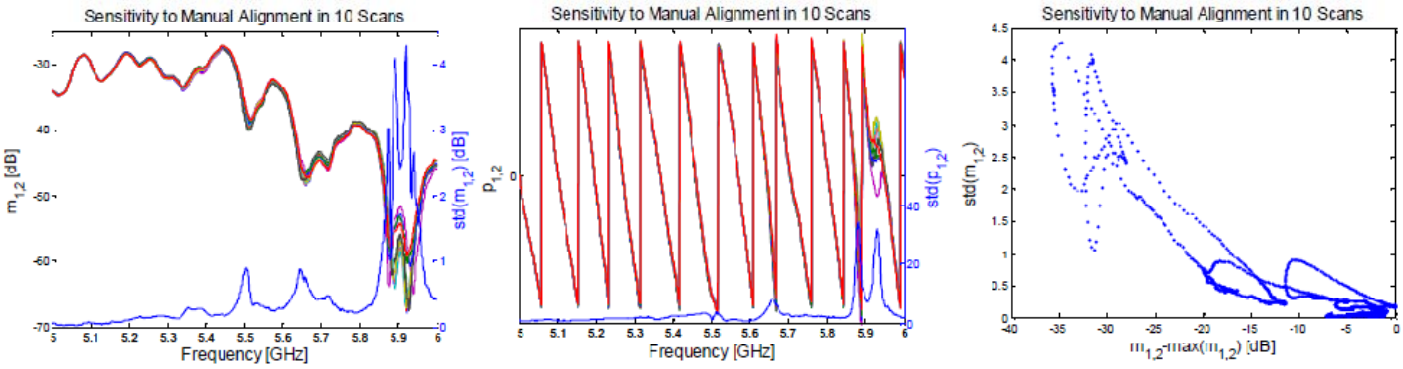

Fig. 5. The values and standard variation of the resulting readings for the magnitude $m_{2,1}$ and phase $p_{2,1}$ of the complex response $s_{2,1}$ recorded for ten manual "best-effort" alignments of a single ★-instance. We activated antennas **1** (transmitter) and **5** (receiver).

instance with respect to the reader antenna matrix. In the second set, our goal was to estimate the response entropy as perceived by the verifier. Figure 6 illustrates the set of antenna couplings active during each experiment. As we did not build a multiplexer for antenna ports, we had to limit our data collection process to only a subset of all possible active couplings as each reading was manually calibrated. For each antenna coupling we present only data collected for the following cases: (•) an RFCOA instance that consisted of Dragon Skin™only, and (★) eight RFCOA instances with copper wire embedded in Dragon Skin™. Each RFCOA instance was separated from the antenna matrix using a 0.5mm thick slice of styrofoam. Tests with COA instances built using a mix of two dielectrics required three times greater COA thickness to produce the same variance of the RF "fingerprint." Thus, we focus our presentation on the selected benchmark.

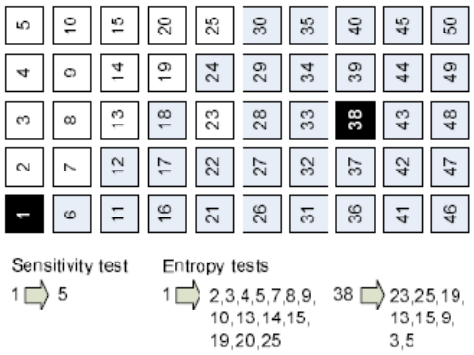

Fig. 6. Selected antenna couplings for the two sets of experiments. Sensitivity to misalignment was tested with antennas **1** and **5** as a transmitter-receiver pair. Entropy tests were conducted with antennas **1** and **38** as transmitters and a range of other antennas as receivers.

A. The Alignment Test

In the first experiment, we activated antennas **1** (transmitter) and **5** (receiver) and placed one of the ★-instances over the antenna matrix. We recorded its response and took additional nine readings, each time by removing the instance completely from the matrix board and then manually realigning it to approximately the same position as in the initial reading. Positioning precision was in the order of 1mm. The actual values and standard variation of the resulting readings for the magnitude $m_{2,1}$ and phase $p_{2,1}$ of the complex response $s_{2,1}$, are illustrated in Figure 5. At lower frequencies and higher transmission efficacy, the alignment variances $\sigma_m(f)^2 = \mathrm{Var}[m(f)_{2,1}], \sigma_p(f)^2 = \mathrm{Var}[p(f)_{2,1}]$ were substantially lower. Noticeable peaks in σ_m and σ_p were recorded towards the lower end of signal gaps at $f = \{5.5, 5.65, [5.85, 5.95]\}$GHz. Within the range $f \in [5.85, 5.95]$GHz, σ_m reached as high as 4.5dB and the recorded response values were about 30dB lower than response's peak P. We conclude that weak response values should be proportionally ignored. The fact that σ_m was below 1.5dB (mostly lower than 0.5dB) for response values as low as $P - 20$dB, is optimistic. Slight misalignment affected less the phase information. Finally, in real-life scenarios where alignment is achieved mechanically with better than 0.1mm precision, we expect to have significantly lower alignment variance, $\sigma_m < 0.2$dB and $\sigma_p < 3$. Only other significant source of noise in the detector are manufacturing inaccuracies which may contribute additional 0.3dB of noise [16].

B. The Entropy Tests

Next, we conducted a set of experiments to evaluate the entropy of the conceived ★-instance as identified by the developed scanner. We activated antennas **1** and **38** as transmitters and series of 14 and 8 coupled receiver antennas respectively, illustrated in Figure 6. Thus, we had a total of 22 couplings which is a small subset compared to the total of 1225 possible couplings in the system. For each coupling, we recorded the response of a single •-instance and eight ★-instances within the $f \in [5, 6]$GHz frequency range at 1601 equidistant frequencies. In order to report the resulting entropy, we performed the following steps. For each ★-instance $i \in \{1 \ldots 8\}$, we computed the differential response: $\hat{m}\{i\}(x, y) = m_{2,1}\{i\}(x, y) - m_{2,1}\{\bullet\}(x, y)$, where x and y denote the transmitter and receiver antenna respectively and $\{\}$ encases the type of object scanned. The results for all measured $\hat{m}\{i\}(x, y)$ are illustrated in Figure 7. Next, we computed the Euclidean distance $d\{i, j\}(x, y) = ||\hat{m}\{i\}(x, y) - \hat{m}\{j\}(x, y)||$ for each $i, j \in \{1 \ldots 8\}, i \neq j$. Then, we estimated the distribution of $d\{i, j\}(x, y)$ for each

(x, y) using a χ^2-model and a maximum likelihood estimator. The estimated probability distribution curves: $\int_a^b \gamma_{x,y}(t)dt = \Pr[E[d\{i,j\}(x,y)] \in [a,b]]$ were computed for each individual antenna coupling (x, y). If we assume that the noise margin for the readers when assessing the RF features of a COA instance, is 0.5dB, then for $d_T = 32$, we have a false negative error rate of $\varepsilon_{FN} \ll 10^{-6}$. Thus, we set the detection threshold at d_T and establish ε_{FN}; then, we estimate the entropy of a single COA instance as perceived by the developed COA scanner as: $H = -\log_2 \prod_{\forall(x,y)\in\mathcal{A}} \gamma_{x,y}(d_T)$, where $\mathcal{A}$ is the set of all antenna couplings. In our case, $|\mathcal{A}| = 1225$. In our computation, for antenna couplings (a, b) that were not measured, we assumed $\gamma_{x,y}$ such that the Euclidean distance between x and y was closest to the distance between a and b for the set $\mathcal{A}'$ of all measured responses (i.e., $(a, b) \in \mathcal{A} - \mathcal{A}'$ and $(x, y) \in \mathcal{A}$). Using this assumption, we estimated $H = 53832$ bits. It is important to stress that this entropy quantifies the likelihood of a false positive as: $\log_2(\varepsilon_{FP}) = H$. It does not specify the difficulty of computing and manufacturing a false positive.

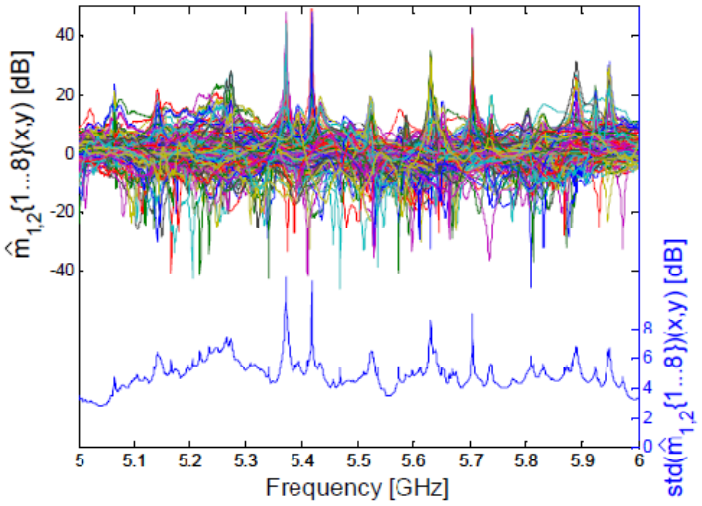

Fig. 7. For each ★-instance i, we illustrate all measured differential responses $\hat{m}\{i\}(x, y)$ where x and y denote the transmitter and receiver antenna respectively. The figure also depicts the corresponding standard deviation of all measured instances and all antenna couplings per frequency subband.

Definition 1: **An RF "fingerprint"** of an RFCOA instance consists of a set of complex $s_{2,1}$-parameters observed over a specific frequency band and collected for (a subset of) all possible antenna couplings on the reader. Each analog $s_{2,1}$-parameter is sampled at arbitrary frequencies and individually quantized using an arbitrary quantizer.

Returning to Subsection I-A, signal f may consist of the raw or compressed RF "fingerprint" as defined in Def.1. The compression may be lossy or lossless with respect to the digitized fingerprint extracted from a single instance.

IV. Attack Scenarios

By assuming that the RF "fingerprint" is a real vector $f \in \mathbb{R}^N$, we formulate the key problems as follows.

Problem 1: **Blind Analysis.** Given an RF "fingerprint" f of an authentic RFCOA instance extracted using a known RFCOA scanner, find a three-dimensional object X capable of producing an RF response f' such that $||f' - f|| < d_T$, where the detection threshold d_T is a proportionally small scalar.

Problem 2: **Known X Manufacturing.** An additional requirement is to develop a manufacturing process that can produce X in large quantities at a relatively low price P.

As detailed in [8], in order for the counterfeiter to make profit, P must be smaller than the profit that the counterfeit product can fetch on the market.

Two layers of difficulty are imposed upon the counterfeiter: computational (Pr.1) and manufacturing (Pr.2). Due to brevity, we conjecture that both of these problems are hard and pose them as a security challenge to the community. RFCOAs can be used in scenarios where either one or both challenges are used to protect a physical object.

V. Summary

We have proposed the first system for manufacturing and verification of COAs which exhibit their random behavior in the RF near-field. A peculiar feature of our system, not exhibited in previous proposals, is the conjectured difficulty of creating a COA instance that produces a specific response. We demonstrated a working prototype of the system that has helped us estimate system performance from the perspective of response repetitiveness and entropy.

References

[1] L. Tsang, et al. Scattering of Electromagnetic Waves. Wiley Interscience, 2000 & 2001.

[2] E. Wolf. A generalized extinction theorem and its role in scattering theory. Coherence and Quantum Optics, L. Mandel and E. Wolf (eds.), Plenum, New York, 1973.

[3] L. Tsang, et al. Theory of Microwave Remote Sensing. Wiley-Interscience, New York, 1985.

[4] Microwave Engineering Europe. CAD benchmark. October 2000 – February 2001. Available on-line at: `http://i.cmpnet.com/edtn/europe/mwee/pdf/CAD.pdf`

[5] A.J. Menezes, et al. Handbook of Applied Cryptography. CRC Press, 1996.

[6] R.L. Rivest, et al. A method for obtaining digital signatures and public-key cryptosystems. *Comm. of the ACM*, vol.21, no.2, pp.120–126, 1978.

[7] N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, Vol.48, (no.177), pp.203–209, 1987.

[8] D. Kirovski. Toward An Automated Verification of Certificates of Authenticity. *ACM Electronic Commerce*, pp.160–9, 2004.

[9] J. Collins. RFID Fibers for Secure Applications. RFID Journal, 2004. Available on-line at: `http://www.rfidjournal.com/article/articleview/845/1/14`.

[10] CrossID, Inc. Firewall Protection for Paper Documents. Available on-line at: `http://www.rfidjournal.com/article/articleview/790/1/44`.

[11] Inkode, Inc. Available on-line at: `http://www.inkode.com`.

[12] Creo, Inc. Available on-line at: `http://www.creo.com`.

[13] RF SAW, Inc. Available on-line at: `http://www.rfsaw.com/tech.html`

[14] R.L. Li, et al. Development and analysis of a folded shorted-patch antenna with reduced size. IEEE Transactions on Antennas and Propagation, Vol.52, no.2, pp.555–562, 2004.

[15] S. Dey, et al. Circularly polarized meander patch antenna array. IEEE Intl. Symp. on Antennas and Propagation, Vol.2, pp.1100–1103, 1996.

[16] Prof. M. Tentzeris. Personal communication, 2006.

[17] G. DeJean and D. Kirovski. Making RFIDs Unique – Radio Frequency Certificates of Authenticity. IEEE AP-S, to appear 2006.