RF-DNA: Radio-Frequency Certificates of Authenticity

Gerald DeJean and Darko Kirovski
Microsoft Research, Redmond, WA 98052, USA

Abstract

A certificate of authenticity (COA) is an inexpensive physical object that has a random and unique multidimensional structure S which is hard to near-exactly replicate. An inexpensive device should be able to scan object's physical "fingerprint," i.e., obtain a set of features in the form of a multidimensional signal $\mathbf{x}$ that pseudo-uniquely represents S. For a given "fingerprint" $\mathbf{x}$ and without access to S, it should be computationally difficult to construct an object of fixed dimensions with a "fingerprint" $\mathbf{y}$ which is at a bounded proximity from $\mathbf{x}$ according to a standardized distance metric. We introduce 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 introduce a tag whose information about the product can be read within a relative far-field, and also whose authenticity can be reliably verified within its near-field. In order to counterfeit a tag, the adversary faces two difficulties – a computational and a manufacturing one. The computational difficulty stems from the hardness of solving linear inverse problems in the electromagnetic field. In order to create an actual tag, the adversary must also manufacture a multidimensional object with a specific three-dimensional topology, dielectric properties, and conductivity.

1 Introduction

Between 7-8% of world trade,[1] 10% of the pharmaceuticals market,[2] and 36% of the software market[3] is counterfeit. We cluster all piracy efforts into two groups:

- PIRACY – where the buyer is confident that the purchased object is not genuine due to an uncharacteristically low price – however, she willingly executes the trade. Such transactions do not gain substantial revenues to the pirate, hence, it is arguable whether losses due to such events could be accounted as lost revenue for the legal copyright owner. The benefit of "free" marketing, brand popularization, and/or platform adoption could outweigh the realistic revenue loss due to piracy.
- COUNTERFEITS – where the seller fools the buyer into believing that the merchandise is authentic and collects the full "legal-market" price on the product. In this case, the pirate collects substantial revenue with profit margins typically higher than that of the original manufacturer due to lack of development and marketing costs.

To the best of our knowledge there does not exist a study which breaks down piracy estimates into the above categories, however for certain markets such as pharmaceuticals nearly all illegal

[1] According to Interpol, World Customs Organization and International Chamber of Commerce estimates that roughly 7-8% of world trade every year is in counterfeit goods.

[2] Glaxo-Smith-Kline in a study with the US Food and Drug Administration estimated that counterfeit drugs account for 10% of the global pharmaceuticals market.

[3] The Business Software Alliance estimates that 36% of software sales worldwide are counterfeit.

trade can be claimed to be counterfeits. With hundreds of billions of dollars lost to counterfeits each year, we are the first to develop RF-DNA – unique RFIDs with an aim to address this problem. Note that traditional RFIDs with encoded digital information could be easily replicated and thus, are not capable of resolving the problem or tag authenticity.

1.1 Certificate of Authenticity

A certificate of authenticity (COA) is a digitally signed physical object of fixed dimensions that has a random unique structure which satisfies the following requirements:

R1 the cost of creating and signing original COAs is small, relative to a desired level of security,

R2 the cost of manufacturing a COA instance is several orders of magnitude lower than the cost of near-exact replication of the unique and random physical structure of this instance, and

R3 the cost of verifying the authenticity of a signed COA is small, again relative to a desired level of security.

The key to the analysis of COA instances is the extraction of its "fingerprint," i.e., a set of features that reliably represents its multi-dimensional structure. This process is typically based on a specific physical phenomenon and produces a cardinality-N vector of complex numbers $\mathbf{x} \in \mathbb{C}^N$. This imposes that:

R4 it should be computationally difficult to construct an object of fixed dimensions with a "fingerprint" $\mathbf{y}$ such that $||\mathbf{x} - \mathbf{y}|| < \delta$, where $\mathbf{x}$ is a given "fingerprint" of an unknown COA instance and δ bounds the proximity of $\mathbf{x}$ and $\mathbf{y}$ with respect to a standardized distance metric $|| \cdot ||$.

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. For example, when covering a surface with an epoxy substrate, its particles form a low-rise but random 3D landscape which uniquely reflects light directed from a certain angle – COAs based upon this idea were first proposed by Bauder and Simmons from the Sandia National Labs and used for weapons control during The Cold War [1].

1.2 Radio Frequency COAs

We investigate which objects behave as COAs in the electromagnetic (EM) field and the kind of properties they offer as counterfeit deterrents. Radio frequency (RF) COAs are built based upon several **near-field** phenomena that EM 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 EM scatterers [2], i.e., they reradiate large amount of EM energy into free space.

- The refraction and reflection of EM waves at the boundary of two media can produce hard-to-predict near-field effects; the phenomenon can be modeled using the Maxwell equations or the generalized Ewald-Oseen extinction theorem [3, 4, 5].

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 (up to 300GHz). 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). For example, 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 type of sealant used could affect greatly the invariance to moisture, stretching, wear-and-tear, and other hazards. In this paper we do not address these effects – we speculate that materials with desired characteristics could be produced in an inexpensive fashion [6].

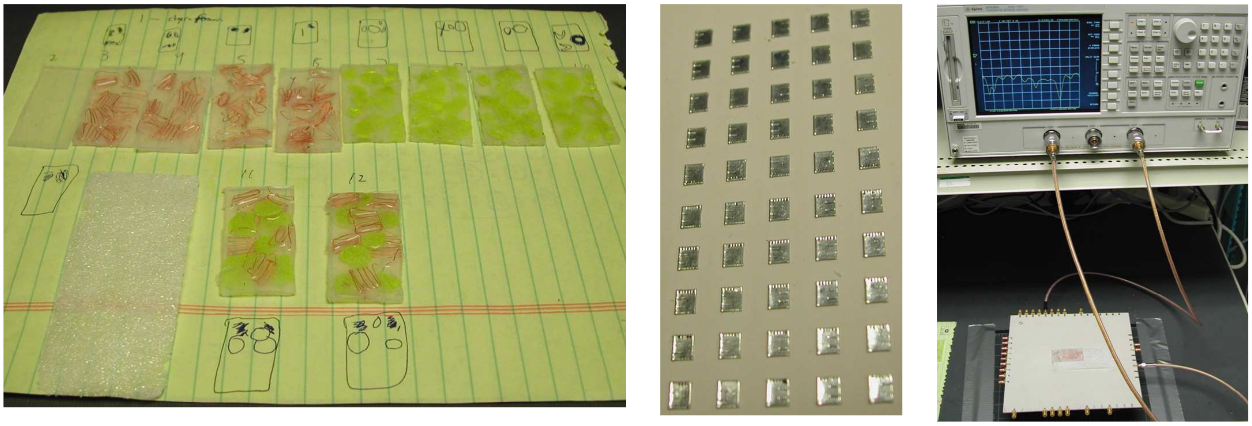

Figure 1: (left) Examples of RF-DNA instances built from copper wire, play-doh and Dragon Skin$^{\mathrm{TM}}$. The instances were created using standard 22gauge copper wire as a conductive resonator, Play-Doh objects of different shape and Dragon Skin$^{\mathrm{TM}}$silicone rubber as sealant. They were all equally sized at 25x50x3mm using an acrylic mold. At retail prices of each of the components, the price per instance was US$0.05. Aluminum wire and mass production should bring the pricing to the sub-cent range per instance. (center, right) Prototype of an RF-DNA scanner: a custom built antenna matrix and a network analyzer.

The “fingerprint” of such a COA instance should represent its 3D structure as well as its dielectric and/or conductive properties. In this paper we consider isotropic materials which result in a linear system, i.e., the effects from two individual objects can be superpositioned to compute the resulting effect of their combined structure. The system can be further complicated by considering dielectrics with non-linear EM properties as well as other non-linear building elements such as ferrites and anisotropic materials.

We introduce an RF-DNA reader built as a group (e.g., 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. The key to the security of RF-DNA is the fact that the response for a single transmitter-receiver, x-y, coupling $C(x,y)$ is strongly **dependent** upon other responses for transmitter-receiver couplings in the neighborhood of C. That way, requirement **R4** is imposed in RF-DNA as a difficult global optimization problem.

We stress that reader's measurements represent 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 difficult to maliciously jam near-field communication.
- The reader can operate with extreme 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 ([7], Chapter §6), thus, such responses lose the ability to represent the scatterer's random structure.
- Computing the actual EM responses numerically is a difficult task. We consider two different computing tasks: the forward and the inverse design process. In the case of a forward design task, the geometry of the reader and the RF-DNA instance is known – the objective is to compute the resulting RF response, i.e., "fingerprint." In the inverse design problem, for a given "fingerprint" $\mathbf{x}$ and a known geometry of the reader, the goal is to construct a COA instance whose fingerprint is in the close proximity of $\mathbf{x}$. In general, while all EM 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 [2, 8].

We built a prototype RF-DNA scanner as a matrix of 5x10 antennas that measure the unique response "fingerprint" of an RF-DNA instance as a collection of transmission (e.g., $s_{2,1}$-parameter) responses in the 5-6GHz frequency range for each transmitter-receiver coupling on the reader. RF-DNA 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 expensive off-the-shelf network analyzer, we speculate that a custom reader could cost less than US$100 if manufactured en masse. Figure 1 illustrates the proposed RF-DNA scanner prototype.

1.3 Logistics

When creating an RF-DNA instance, the issuer digitally signs instance's EM response using traditional public-key cryptography. First, the "fingerprint" is scanned, 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 $w = f||t$. One way to sign the resulting message w is to use the Bellare-Rogaway recipe, PSS-R [9], for signing messages using RSA [10] with message recovery. The resulting signature s as well as w are encoded directly onto the COA instance using existing technologies such as an RFID. Each COA instance is associated with an object whose authenticity the issuer wants to vouch. Once issued, an RF-DNA instance can be verified off-line by anyone using a reader that contains the corresponding public key of the issuer. In case the integrity test is successful, the original response "fingerprint" f and associated data g are extracted from w. The verifier proceeds to scan in-field the actual RF "fingerprint" f' of the attached instance, i.e., obtain a new reading of the instance's EM properties, and compare them with f. If the level of similarity between f and f' exceeds a pre-defined and statistically validated threshold δ, the verifier declares the instance to be authentic and displays t. In all other cases, the reader concludes that the instance is not authentic. In order 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 [10, 11, 12], 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 [13], or

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

COA instances are generic "objects of value." They have a fully horizontal perspective of possible applications. The value that one COA instance represents, approximately equals the cost to forge this instance [13]. Inexpensive verification makes COAs particularly attractive for several traditional applications as well as for a myriad of new ones. Currency, checks, money orders, credit cards, license and product tags, warranties, receipts, endorsements, ownership documents, proofs of purchase/return, proof of repair, coupons, tickets, identity documents, visas, seals, tamper-evident hardware can all be produced using COAs. Note that the RF-DNA must be firmly attached to the associated object as an adversary may remove, substitute, or attach valid RF-DNAs at will. Most of these problems can be rectified by devaluing RF-DNAs at point of sales or by recording transactions on the RF-DNA itself. For example, a license tag may consist of two independently identifiable RF-DNA instances, where one is destroyed at purchase time to signal a sold product. The same procedure can be used to signal and/or value product's "N^{th} owner."

One of the key features of RF-DNAs is that their "fingerprints" do not reveal their physical structure in a straightforward fashion. Practically, assume the application where credit cards are protected using RF-DNAs. Then, 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's "fingerprint"), it would be still difficult for the adversary to create a physical copy of the original credit card produced by the issuing bank. To complete the operation, the adversary would have to gain physical access to the original credit card and accurately scan its 3D structure (e.g., using X-rays or other 3D imaging systems). Finally, the adversary still faces the task of actually building the 3D object, a task that, we speculate, requires significant costs.

1.4 Related Work

In the 1970s Bauder and Simmons were the first to propose COAs created as sprayed epoxy on a two dimensional substrate for weapons verification purposes during The Cold War [1]. Several years later they proposed to use a collection of fibers randomly positioned in an object using a transparent gluing material which permanently fixes fibers' positioning [14]. Readout of the random structure of a fiber-based COA could be performed in numerous ways using the following fact: if one end of a fiber is illuminated, the other end will also glow. Bauder proposed fiber-based COAs for banknote protection - fibers in that proposal were fixed using a semi-transparent material such as paper [14]. To the best of our knowledge, only few efforts have followed the pioneering work by Bauder and Simmons. Church and Littman have worked on extraction of random optical-fiber patterns in the context of currency anti-counterfeiting [15, 16]. Pappu has created a class of physical one-way functions via speckle scattering [17, 18]. He has focused on Gabor wavelets to produce short digests of the natural randomness collected from an optical phenomenon. His Ph.D. thesis has a solid survey of the related but scarce work [17]. Recently, Kirovski evaluated a system for automatic verification of fiber-based COAs [13]. Finally, COAs in the EM domain have been proposed by several companies [19, 20, 21, 22, 23], all of them aiming to detect COA's random structure in the far-field. Such detection is prone to spoofing; in addition, such COAs can be relatively easily near-exactly replicated. Because the detection is taking place in the far-field, many of these systems operate in the "expensive" 60GHz frequency range.

The motivation for the research focus presented in this manuscript is complex. First, our RF-DNA designs force the counterfeiter to manufacture a given complex 3D structure and embed it in a soft or hard encapsulating sealant. The structures could be made from homogeneous liquids in certain scenarios. In both cases, the cost of near-exact replication of such COA instances is greatly raised. Second, since the readout of their random structure does not require a reader-object contact, RF-DNAs may be built with superior wear-and-tear properties. Next, as shown later in this manuscript, for a credit-card sized RF-DNA instance and a reader that operates in the 5-6GHz frequency subband, the entropy of the readout response from RF-DNAs easily tops several thousand bits making the likelihood of accidental collusion negligent. Finally, RF-DNAs are the first type of COA that satisfies the requirement **R4** from Section 1.

2 The RF-DNA Scanner

In order to scan the EM features of an RF-DNA instance, we proposed a scanner designed to expose the subtle variances of near-field responses of these objects to RF waves in [24]. We introduced a scanner that consisted of a single antenna matrix, where each antenna was capable of operating both as a transmitter and a receiver. While scanning a COA instance, it is aligned to a fixed position with respect to the antenna matrix. The RF-DNA instance should have an absorbent and/or reflective background so that the environment behind the tag does not affect its RF response. When an RF wave initiated by one of the antennas hits the COA instance, its reflection and refraction is dependant upon the 3D positioning of the scatterers embedded in the RF-DNA. This creates a distinct RF response, in particular in the near-field, that can be received by any of the remaining antennas on the panel. Each receiver obtains a view of the RF-DNA from its own perspective. The total voltage V_n of a device or port equals the sum of the voltage input into a device V_n^+ and the voltage received from a device V_n^-: $V_n = V_n^+ + V_n^-$. For two antennas under test, four specific s-parameters can be obtained for the two-port network. A matrix representation of the relationship between the voltage and the s-parameters is shown in Eqn.1:

$$\begin{bmatrix} V_1^- \\ V_2^- \end{bmatrix} = \begin{bmatrix} s_{1,1} & s_{1,2} \\ s_{2,1} & s_{2,2} \end{bmatrix} \begin{bmatrix} V_1^+ \\ V_2^+ \end{bmatrix}. \qquad (1)$$

For example, for a system with M antennas, one can measure M $s_{1,1}$ and $\binom{M}{2}$ $s_{2,1}$ parameters. In order to enable this, each antenna is multiplexed to an analog/digital back-end capable of extracting the $s_{2,1}$ parameter (i.e., insertion loss) for a particular antenna coupling. The actual design of the proposed RF-DNA scanner is identified in [24]. In mass production, we estimate that the price for this reader should be well below US$100 [25]. Figure 1 illustrates the manufactured prototype and the simulation setup.

3 Empirical Evaluation of "Fingerprint's" Uniqueness

Experimentally, we quantified system's sensitivity to slight misalignment and estimated the response entropy as perceived by the verifier. Fig.2 illustrates the set of antenna couplings active during each experiment. We considered (★) eight RF-DNAs with copper wire embedded in Dragon

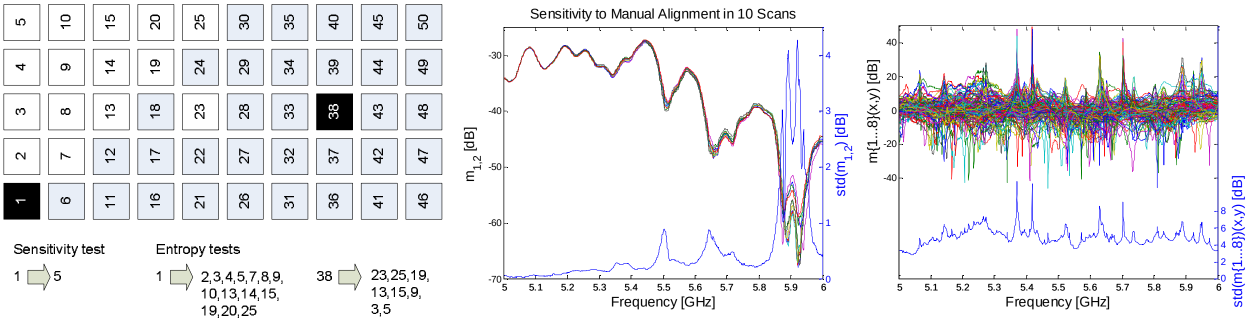

Figure 2: (left) Experimental setup: misalignment sensitivity was tested by coupling antennas **1** and **5**; entropy tests were conducted with **1** and **38** as transmitters and a range of other antennas as receivers. (center) Plot of the magnitude of $s_{2,1}$ recorded for ten manual alignments of a single ★-instance. (right) For each ★-instance i, we illustrate all measured differential responses $m_{2,1}\{i\}$. The figures also depict the corresponding standard deviations.

Skin$^{\text{TM}}$. First, we activated antennas **1** (T) and **5** (R) and placed one of the ★-instances over the scanner. We recorded its response and took additional 9 scans, each time by removing the instance completely from the scanner and then manually realigning it to approximately the same position as in the initial scan. Positioning precision was $\sim$ 1mm. The actual values and variance of the resulting readings for the magnitude $m_{2,1}$ of the response $s_{2,1}$, are given in Fig.2. The standard deviation of $m_{2,1}$, σ_m, was lower than 0.5dB for response values as low as 20dB below the peak. In real-life scenarios, alignment can be achieved with precision better than 0.1mm; thus, we expect to have significantly lower alignment noise of $\sigma_m < 0.2$dB. Other major source of noise in the detector is manufacturing inaccuracy which may contribute additional 0.3dB [26].

In the second set of experiments, we activated antennas **1** and **38** as transmitters and series of 14 and 8 coupled receiver antennas respectively, illustrated in Fig.2. Thus, we had a total of 22 couplings, a small subset compared to the total of 1225 possible couplings. For each coupling (x, y), we recorded the response of all ★-instances within the $f \in [5, 6]$GHz range at 1601 equidistant frequencies. We computed the Euclidean distance $d\{i, j\}(x, y) = ||m_{2,1}\{i\}(x, y) - m_{2,1}\{j\}(x, y)||$ for each $i, j \in \{1 \dots 8\}, i \neq j$. 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. We denote the estimated probability distribution curves as: $\int_a^b \gamma_{x,y}(t)dt = \Pr\left[E[d\{i, j\}(x, y)] \in [a, b]\right]$. If we assume that reader's noise margin is 0.5dB, then for $\delta_T = 32$, we have a false negative error rate of $\varepsilon_{FN} \ll 10^{-6}$. Based on such δ_T, we estimate the entropy of a single COA as perceived by our COA scanner as $H = -\log_2 \prod_{\forall(x,y)\in\mathcal{A}} \gamma_{x,y}(\delta_T)$, where $\mathcal{A}$ is the set of all antenna couplings. 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. Using this assumption, we estimated $H > 50000$ bits only from the magnitude data. For brevity, we do not analyze phase data in this manuscript.

Estimate H is computed under the assumption that responses for distinct transmitter-receiver couplings are independent. This assumption is not true – as a matter of fact the core claim of security is related to the fact that distinct responses from antennas that are close are dependent. That is to force the adversary into a global optimization problem. On the other hand, it is difficult to create an analytic tool or a manufacturing procedure that can identify and explore the inter-response dependencies. Therefore H is, in a sense, relatively accurate estimate of how difficult is to design using a computer-aided design tool a given RF-DNA instance to the standards presented earlier in this section. As a central discussion, in the remainder of this paper we evaluate the difficulty of computing EM properties of objects as used in the RF-DNA system.

Definition 1 ***An RF "fingerprint"*** $\mathbf{x} \in \mathbb{C}^{F\binom{M}{2}}$ *of an RF-DNA consists of a set of complex* $s_{2,1}$*-parameters observed over a specific frequency band and collected for (a subset of or) all possible* $\binom{M}{2}$ *antenna couplings using a reader with* M *antennas. Each analog* $s_{2,1}$*-parameter is sampled at* F *arbitrary frequencies and individually quantized using an arbitrary quantizer.*

4 Attack Scenarios

In this section, we evaluate the difficulty of counterfeiting RF-DNA instances. By assuming that the RF "fingerprint" is a complex vector $f \in \mathbb{C}^N$, we formulate the key problems as follows.

Problem 1 ***Blind Analysis.*** *Given an RF "fingerprint"* $\mathbf{x}$ *of an authentic RF-DNA instance extracted using a known RF-DNA scanner, find a three-dimensional object* S *capable of producing an RF response* $\mathbf{x}'$ *such that* $||\mathbf{x}' - \mathbf{x}|| < \delta_T$*, where the detection threshold* δ_T *is a small scalar.*

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

There are two layers of difficulty imposed upon the counterfeiter: a computational one (Pr.1) and a manufacturing one (Pr.2). RF-DNAs can be used in scenarios where either one or both challenges are used to protect a physical object. We approach the two problems separately. Under the assumption that manufacturing in 3D is a prohibitively expensive process, in this paper we focus on formalizing Pr.1 and establishing its difficulty. We start this discussion by reminding the reader that the likelihood of a false positive ε_{FP} is negligible (as seen from a simple prototype and the analysis in Section 3) and that an elaborate search process is required to produce S.

4.1 Forward Design

In this subsection, we review the process of simulating the effect of an RF-DNA in the presence of EM waves. This procedure is important as it represents a direct step in the inverse design process. We refer the reader to review the basic concepts in EM theory in Appendix A. To the best of the knowledge of the authors, providing analytical or numerical solutions to Maxwell's equations is not a simple task in particular when field values are computed in the near-field of the scatterers. Within the scope of the application (most research in the field targets radar, medical imaging, communication, and geophysics applications), the existing techniques focus on either analytically simplifying the Maxwell equations via approximations for a particular constrained application and then solving the approximations numerically or numerically solving the generic Maxwell equations for isotropic materials [27]. Analytical approximation techniques are typically used in constrained scenarios with relatively poor results for general cases. For example one of the focuses is on approximating rough surfaces with a Gaussian distribution and computing the first and second order statistics of the exerted EM far-field [28, 29, 2, 7, 30]. For an arbitrary field setup, one likely must revert to a numerical EM field solver. In the remainder of this subsection, we review the speed and accuracy of the most efficient numerical approaches.

Here, the objective is to compute the Maxwell equations for isotropic dielectric materials:

$$\nabla \times \mathbf{H} = \frac{1}{c}\frac{\partial \mathbf{D}}{\partial t} + \frac{4\pi}{c}\mathbf{j}, \quad \nabla \times \mathbf{E} + \frac{1}{c}\frac{\partial \mathbf{B}}{\partial t} = 0, \quad \mathbf{B} = \mu\mathbf{H}, \quad \mathbf{D} = \varepsilon\mathbf{E} \tag{2}$$

in free space/time, where $\mathbf{E}$ and $\mathbf{H}$ represent the electric and magnetic field density, respectively, c is speed of light in vacuum, $\mathbf{j}$ denotes electric current density, and ε and μ are dielectric permittivity and magnetic permeability, respectively. In material media, the response to the excitation produced by these fields is described by the electric displacement $\mathbf{D}$ and the magnetic flux density $\mathbf{B}$.

Traditional approach to fast and accurate simulation of Eqns.2 is to: first, convert Eqns.2 into the frequency domain, discretize the free space into $K = K_x \times K_y \times K_z$ small volumetric units, and rewrite Eqns.2 in the form of partial differential equations to create a system of linear equations $\mathbb{A}\mathbf{q} = \mathbf{b}$, where $\mathbf{q}$ is a vector of $3K$ elements that represent the values of the EM fields in each unit per dimension, vector $\mathbf{b}$ represents the source of EM activity, and matrix $\mathbb{A}$ represents the field equations for each cell. This matrix is large and sparse. The solution to the system of linear equations fulfills the objective of the simulation. EM solvers usually are chosen for a specific performance feature-set: speed, accuracy, stability, and memory.

Speed. There are numerous methodologies used for finding solutions to partial differential equations such as: Finite-Difference Time-Domain (FDTD) [27, 31], Finite Element Method (FEM) [32, 33], Method of Moments (MOM) [34], and the Finite Integration Technique (FIT) [35]. Commercial simulators typically offer several solvers as they usually offer distinct advantages for certain problem specifications [36]. In general, the computational complexity for most techniques is linked to their accuracy; accurate methodologies are typically superlinear: $\mathcal{O}(K \log K)$ for improved MOM, FIT, and FEM [37] and $\mathcal{O}(K^{1.33})$ for FDTD [38], where K equals the number of unknown variables, i.e., discrete elements (typically, simple volumetric unit cubes or other polyhedrons) used to model the simulated EM environment. Due to the overall simplicity of programming FDTD approaches, they are preferred in certain cases over the other asymptotically more efficient techniques. Although most of the pareto-point solvers offer advantages, their performance as generic field solvers is often within one order of magnitude for equivalent level of accuracy [8]. Modern methods is a result of several decades of research in electromagnetism and numerical analysis.

Accuracy. Besides speed, another important feature of EM solvers is their accuracy versus measurements on systems manufactured according to simulated specifications. Here it is important to notice that there exists vast amount of literature as all published designs are typically supported with characteristics obtained via simulation and manufacturing/measurement. An example of the substantial discrepancy in accuracy and performance of modern field solvers can be observed in a recent comparison study of six state-of-the-art solvers [8]. For a relatively simple semi-2D structure, a vivaldi antenna with an operating frequency at $f_0 = 4.5$GHz, modeled with approximately $K \approx 10^5$ discrete elements, individual simulation results for the $s_{2,1}$-parameter in the 3-7GHz band, differed up to 12dB with additional substantial differences with respect to actual measurements of the physical implementation of the structure. Interestingly, the results among different solvers for the same antenna specification differed on the average for 3dB in the neighborhood of f_0. The fastest program in the suite returned its results after approximately one hour on a 800MHz Pentium processor. We expect to see noise of about 0.5dB in the RF-DNA scanner when reading the same RF-DNA instance using different instances of the same scanner design.

Let's consider one of the fastest practical methodologies that solve $\mathbf{E}$ and $\mathbf{H}$ fields via systems of partial differential equations, the FDTD [27]. The equations are solved in a leap-frog manner; the electric field is solved at a given instant in time, then the magnetic field is solved at the next instant, and the process is iterated. In FDTD, unknowns represent small volumetric cells. As we are interested in sub-wavelength effects, in order to achieve a desired level of accuracy of 1dB, we mesh the space using cubic cells $(\Delta x)^3$ with sides of at most $\Delta x \leq \lambda/2000$ [27, 39], where wavelength $\lambda > 0.05$m for the considered range of 5-6GHz. Hence, the model of an RF-DNA object sized at 50mm×25mm×2mm and placed on our reader, should result in a mesh of $K > 10^8$ unknowns. In order to achieve numerical stability of simulation, most variants must choose the time step Δt during the numerical analysis according to the Courant-Friedrich-Levy condition $\Delta t \leq \Delta x \sqrt{3}/c$, where c is the fastest speed of light across all considered media and $\Delta x\sqrt{3}$ is the longest straight path in the considered cell unit. In order to achieve relative accuracy, the basic step of the numeric analysis is repeated C times where typically $10^6 > C > 10^4$ for the frequency range of interest (5-6GHz). Note that there exist certain variants of FDTD that are unconditionally stable (3D ADI-FDTD, [40]), however require more processing to achieve the same level of accuracy [39].

In summary, the memory requirements of current computing systems as well as their processing power have impacted that some of the largest EM simulations today are on the order of $K = 10^7$ unknowns providing results that typically are several dB off from the same parameters obtained via high-precision manufacturing and measurements. It is difficult to formally analyze simulation errors for most solvers in the generic case, thus, we do not evaluate the computational complexity (in the traditional sense) for the task to simulate a scanning of an RF-DNA instance for a desired level of accuracy ($\ll$0.5dB) – from most modern studies, we speculate that accurate forward simulation (better than 0.5dB per sample of the "fingerprint") of proposed RF-DNAs is not feasible.

The key to the efficacy of our system is to build RF-DNA objects such that they are relatively small but exhibit distinct and strong variance of transmission parameters when placed between two antennas (one in transmitting mode and one in receiving mode). In this paper, we explore resonators; however other phenomena could significantly and profoundly affect transmission such as randomly shaped and positioned metamaterials[4] [41, 42] or discrete dielectric and ferromagnetic scatterers [7]. Ultimately, by combining scatterers with different properties, it is more difficult to find accurate approximations that can accelerate a field solver.

4.2 Inverse Design

Even if the adversary could accurately solve the forward design process, she would still have to search within the solution space H (see Section 3) in order to solve Pr.1. One naïve strategy is that the adversary must launch a localized search process for an RF-DNA instance which visually corresponds to authentic instances (three-dimensional object of fixed dimensions such as a credit card) and which satisfies the constraints posed in Pr.1.

This inverse problem is actually well known in several research fields, in particular medical imaging (electroencephalography – EEG) and geophysics research. In general, the problem is considered to be ill-posed (term introduced by Hadamard in 1902 – a problem whose solution does not exist or it is not unique or it is not stable under perturbations on data). In general, the objective in this problem is to detect scatterers given a particular dataset obtained via EM probing. In EEG research, substantial efforts have been targeted towards identifying the number of probes that are required to identify the unique solution (electrical activity in the brain) that produces the observed EM signals [43]. From that perspective, it is important in our system that the number of antenna couplings is sufficient to represent the 3D structure of an RF-DNA instance. Techniques that succeed in relatively inaccurate solutions to inverse problems combine the forward and inverse design step and iterate it numerous times. A survey of such schemes is presented in [44, 45] – in summary, best known systems achieve to solve some ill-defined inverse problems with prior knowledge of solution structure for $K \approx 10^3$ in substantial amount of time. As formal analysis of such methodologies is not provided, we conjecture that solving Pr.1 is a task which is well beyond reach of modern inverse design tools. A topic of further research is to understand the ill-posedness of Pr.1.

[4] Materials that exhibit negative index of refraction.

4.3 Superpositioning

The adversary can use the fact that the system is linear [26] and try to obtain a desired "fingerprint" $\mathbf{x}$ by combining atomic objects with known, simulated "fingerprints." A simple RF-DNA instance X that consists of two separate non-overlapping atomic objects X_1 and X_2, satisfies the following property: $f(X) = f(X_1) + f(X_2)$, where function f returns the "fingerprint" of its argument. Note that two different atomic objects can have the same geometric shape; however, their responses will be different with high likelihood if these shapes are positioned at distinct locations relative to the RF-DNA scanner. The goal of the adversary is to design a large set of m atomic objects $\mathbb{X} = \{X_1, \ldots, X_m\}$ and simulate $f(X_1), \ldots, f(X_m)$. Then, the adversary would launch a search over $\mathbb{X}$ in order to find a subset $\mathbb{Y} \subset \mathbb{X}$ of non-overlapping shapes such that:

$$\left|\left| \sum_{X_i \in \mathbb{Y}} f(X_i) - f \right|\right| < \delta_T \tag{3}$$

and that the composition of all objects in $\mathbb{Y}$ is contained in the volume of a single RF-DNA instance.

Although seemingly attractive, this approach has several associated difficulties. First, while performing the summation in Eqn.3, the error accumulates. Thus, a necessary condition for the attack is that the average simulation-manufacturing error is smaller than 0.5dB$/|\mathbb{Y}|$. Next, assuming that such an error can be achieved, it is questionable whether a solution to Eqn.3 can be found based upon $\mathbb{X}$ only. While at least one solution to this problem certainly exists (e.g., the authentic RF-DNA), searching over non-overlapping shapes in $\mathbb{X}$ may not yield necessarily a viable solution.

Superpositioning is likely to be effective only using a non-overlapping set of parametric canonical atomic objects. We define a parametric canonical atomic object as an atomic object such that it arbitrarily affects (based upon a set of parameters) only a narrow frequency band of the response for a single antenna coupling and has negligible effect on all other bands of this coupling as well as any other antenna coupling. An additional requirement is that all considered canonical atomic objects are non-overlapping. The design of such objects is not straightforward, however, if successful, it would significantly simplify this attack.

4.4 Dimensionality Reduction

One trivial simplification of Pr.1 is to search for X that has reduced dimensionality. As manufacturing of 2D or layered 2D objects is typically inexpensive, by solving the reduced problem, one can achieve the overall goal using constrained resources. Here we stress that the sealant used in creating COA instances should be transparent. Thus, the person verifying an RF-DNA instance can always visually inspect its structure. Existence of a metallic 3D structure and absence of a 2D object with dimensions similar to instance's dimensions, signals a potentially authentic instance. In order to fool such a simple verifier, the adversary must construct the 2D object using transparent material with the same optical refraction properties as the sealant and conductor-like RF properties. Also the adversary must find a way to mimic the visuals of metallic 3D structures without introducing significant additional RF effects. To the best of our knowledge, we believe that such a task is difficult with modern materials but do not exclude its importance both computationally and from the perspective of manufacturing. Needless to mention, improved hardware verifiers could be deployed to detect a 2D COA instance in case such attacks become viable.

In summary, all mentioned attacks rely on the accuracy of field solvers – a feature that is difficult to achieve with modern numerical analysis methods in timely manner. While the problem is easily defined (Pr.1), as opposed to traditional cryptographic procedures [46], its computational complexity is difficult to address in formalities standard to computer science (e.g., $\mathcal{O}()$) because of the result accuracy required from the EM solver. For most modern EM solvers these complexities are known to be exceptionally high however they have never been formalized to a level that could state a current formal computational bound $\mathcal{O}()$ on Pr.1. Thus, here we conjecture the inherent difficulty to solve Pr.1, and pose an open problem to all related research communities.

5 Summary

In this paper, we have proposed the first system for manufacturing and verification of certificates of authenticity which exhibit their random behavior in the EM 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. Finally, we pointed out to several important attack scenarios that are difficult to undertake with modern simulation and manufacturing capabilities.

References

[1] D.W. Bauder. Personal Communication.

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

[3] P.P. Ewald. Ann. der Physik, Vol.49, 1-56, 1915.

[4] C.W. Oseen. Uber die Wechrelwirkung zwischen zwei elektrischen Dipolen und uber die Drehung der Polarisationsebene in Kristallen und Flussigkeiten. Ann. der Physik, Vol.48; pp.1-56, 1915.

[5] 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.

[6] P.S. Neelakanta. Handbook of Electromagnetic Materials. CRC Press, Boca Raton, FL, USA, 1995.

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

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

[9] M. Bellare and P. Rogaway. The exact security of digital signatures how to sign with RSA and Rabin. EUROCRYPT, pp.399–414, 1996.

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

[11] ANSI X9.62-1998. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 1998.

[12] IEEE 1363-2000: Standard Specifications For Public Key Cryptography, 2000.

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

[14] D.W. Bauder. An Anti-Counterfeiting Concept for Currency Systems. Research report PTK-11990. Sandia National Labs. Albuquerque, NM, 1983.

[15] S. Church and D. Littman. Machine reading of Visual Counterfeit Deterrent Features and Summary of US Research, 1980-90. *Four Nation Group on Advanced Counterfeit Deterrence*, Canada, 1991.

[16] Commission on Engineering and Technical Systems (CETS). Counterfeit Deterrent Features for the Next-Generation Currency Design. The National Academic Press, 1993.

[17] R. Pappu. Physical One-Way Functions. Ph.D. Thesis, MIT, 2001.

[18] R. Pappu, et al. Physical One-Way Functions. Science, Vol.297, no.5589, pp.2026–30, 2002.

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

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

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

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

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

[24] G. DeJean and D. Kirovski. Radio Frequency Certificates of Authenticity. IEEE Antenna and Propagation Symposium, 2006.

[25] MetaGeek, Inc. WiSpy. Available on-line at: `http://www.metageek.net`.

[26] M. Tentzeris. Personal communication, 2006.

[27] K. Yee. Numerical solution of inital boundary value problems involving maxwell's equations in isotropic media. IEEE Transactions on Antennas and Propagation, Vol.14, no.3, pp.302–307, 1966.

[28] M. Born and E. Wolf. Principles of Optics: Electromagnetic Theory of Propagation, Interference and Diffraction of Light. Pergamon Press, Oxford, 1975.

[29] M. Nieto-Vesperinas. Scattering and Diffraction in Physical Optics. John Wiley & Sons, Inc., New York, 1991.

[30] S.K. Cho. Electromagnetic scattering. Springer-Verlag, New York, 1990.

[31] A. Taflove and S.C. Hagness. Computational Electrodynamics: The Finite-Difference Time-Domain Method. Artech House Publishers, 2005.

[32] P. Monk. Finite Element Methods for Maxwell's Equations. Clarendon Press, 2003.

[33] Ansoft Corp. HFSS: 3D EM Solver. Available on-line at: `http://www.ansoft.com/products/hf/hfss/new.cfm`.

[34] R.F. Harrington. Field Computation by Moment Methods. Wiley-IEEE Press, 1990.

[35] M. Clemens and T. Weiland. Discrete electromagnetism with the finite integration technique. Electromagnetics Research, pp.65-87, 2001.

[36] CST Corp. Microwave Studio. Available on-line at: `http://www.cst.de/Content/Products/MWS/Solvers.aspx`.

[37] P. Xu and L. Tsang. Scattering by rough surface using a hybrid technique combining the multilevel UV method with the sparse matrix canonical grid method. Radio Science, Vol.40, 2005.

[38] W.C. Chew. Waves and Fields in Inhomogenous Media. Wiley-IEEE Press, 1999.

[39] S.G. Garcia, et al. On the Accuracy of the ADI-FDTD Method. IEEE Antennas and Wireless Propagation Letters, Vol.1, No.1, pp.31–4, 2002.

[40] T. Namiki. 3-D ADIFDTD MethodUnconditionally Stable Time-Domain Algorithm for Solving Full Vector Maxwells Equations. IEEE Transactions on Microwave Theory and Techniques, Vol.48, no.10, pp.1743–47, 2000.

[41] G. Veselago, Sov. Phys. Usp. 10, 509, 1968.

[42] R.A. Shelby, et al., Science 292, 77 (2001).

[43] C.M. Michel, et al. EEG source imaging. Clinical Neurophysiology, Vol.115, (no.10), pp.2195–222, 2004.

[44] E. Haber, et al. Inversion of 3D electromagnetic data in frequency and time domain using an inexact all-at-once approach. Geophysics, Vol.69, (no.5), pp.1216–1228, 2004.

[45] D.B. Avdeev. Three-dimensional electromagnetic modelling and inversion: from theory to application. Surveys in Geophysics, Vol.26, pp.767–799, 2005.

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

Appendix A

In general, electromagnetic fields are characterized by their electric and magnetic field intensity: **E** and **H**, respectively. In material media, the response to the excitation produced by these fields is described by the electric displacement **D** and the magnetic flux density **B**. The interaction between these variables is described using the Maxwell's equations:

$$\begin{aligned} \nabla \times \mathbf{H} &= \frac{1}{c}\frac{\partial \mathbf{D}}{\partial t} + \frac{4\pi}{c}\mathbf{j} \\ \nabla \times \mathbf{E} + \frac{1}{c}\frac{\partial \mathbf{B}}{\partial t} &= 0 \\ \nabla \cdot \mathbf{D} &= 4\pi\rho \\ \nabla \cdot \mathbf{B} &= 0, \end{aligned} \tag{4}$$

where c is speed of light in vacuum, and $\mathbf{j}$ and ρ denote electric current density and charge density, respectively. For most media, we have linear relationships:

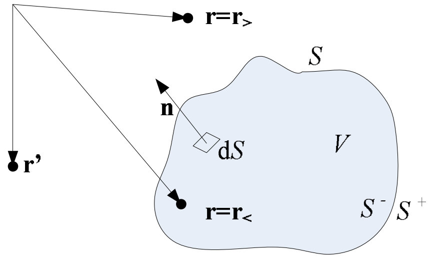

Figure 3: Illustration of the main variables in Eqn.10-13.

$$\mathbf{D} = \mathbf{E} + 4\pi\mathbf{P} = \varepsilon\mathbf{E}, \mathbf{B} = \mathbf{H} + 4\pi\mathbf{M} = \mu\mathbf{H}, \mathbf{j} = \sigma\mathbf{E}, \tag{5}$$

where ε, μ, and σ are dielectric permittivity, magnetic permeability, and material's specific conductivity, respectively, and **P** and **M** are the polarization and magnetization vectors respectively. From the curls in Eqns.4 and 5, one can derive the equations that model propagation of a monochromatic (time-dependency factor $\exp(i\omega t)$) electromagnetic wave:

$$\begin{aligned} \mathbf{F}_e &= \nabla \times \nabla \times \mathbf{E} - k^2\mathbf{E} \\ &= -4\pi\left[\frac{ik}{c}\mathbf{j} + k^2\mathbf{P} + ik\nabla \times \mathbf{M}\right] && (6) \\ \mathbf{F}_m &= \nabla \times \nabla \times \mathbf{H} - k^2\mathbf{H} \\ &= 4\pi\left[\frac{1}{c}\nabla \times \mathbf{j} - ik\nabla \times \mathbf{P} + k^2\mathbf{M}\right], && (7) \end{aligned}$$

where $k = \frac{\omega}{c}$ is the wavenumber. Eqns.6 and 7 fully describe electromagnetic waves in 3D space – however, commonly another form is used for simulation of scattering based upon the Ewald-Oseen extinction theorem[5] [3, 4]. We consider a material medium occupying a volume V limited

[5] This theorem was derived later from the Maxwell equations in [5].

by a surface S and use $\mathbf{r}_>$ and $\mathbf{r}_<$ to denote vectors to an arbitrary point outside and inside V respectively. The variables are illustrated in Figure 3. The dyadic form $\mathbb{G}(\mathbf{r}, \mathbf{r}')$ of the scalar Green function $G(\mathbf{r}, \mathbf{r}')$:

$$\mathbb{G}(\mathbf{r}, \mathbf{r}') = (\mathcal{G} + \frac{1}{k^2}\nabla\nabla)G(\mathbf{r}, \mathbf{r}'), \tag{8}$$

$$G(\mathbf{r}, \mathbf{r}') = \frac{\exp(ik|\mathbf{r} - \mathbf{r}'|)}{|\mathbf{r} - \mathbf{r}'|} \tag{9}$$

where $\mathcal{G}$ is a unit dyadic, describes a spherical wave at point $\mathbf{r}$ sourced from point $\mathbf{r}'$. Now, the generalized extinction theorem [5] states:

$$\mathbf{E}(\mathbf{r}_<) = \frac{1}{4\pi}\int\limits_V \mathbf{F}_e(\mathbf{r}') \cdot \mathbb{G}(\mathbf{r}_<, \mathbf{r}')d^3r' - \frac{1}{4\pi}\overset{(-)}{\sum_e}(\mathbf{r}_<) \tag{10}$$

$$\mathbf{E}^{(i)}(\mathbf{r}_<) + \frac{1}{4\pi}\mathbf{S}_e(\mathbf{r}_<) = 0 \tag{11}$$

$$\mathbf{E}(\mathbf{r}_>) = \mathbf{E}^{(i)}(\mathbf{r}_>) + \frac{1}{4\pi}\mathbf{S}_e(\mathbf{r}_>) \tag{12}$$

$$0 = \frac{1}{4\pi}\int\limits_V \mathbf{F}_e(\mathbf{r}') \cdot \mathcal{G}(\mathbf{r}_>, \mathbf{r}')d^3r' - \frac{1}{4\pi}\overset{(-)}{\sum_e}(\mathbf{r}_>), \tag{13}$$

where points $\mathbf{r}$ and $\mathbf{r}'$ are both inside V (Eqn.10), inside and outside of V (Eqn.11), both outside of V (Eqn.12), and outside and inside V (Eqn.13) respectively. $\mathbf{E}^{(i)}$ is the incident field upon V and:

$$\begin{aligned} \mathbf{S}_e = \int\limits_{S^-} \Big[\Big(\mathbf{n} \times (\nabla \times \mathbf{E} - 4\pi ik\mathbf{M}) + \frac{4\pi ik}{c}\mathbf{j}\Big) \cdot \mathbb{G}(\mathbf{r}, \mathbf{r}') \\ +(\mathbf{n} \times \mathbf{E}) \cdot \nabla \times \mathbb{G}(\mathbf{r}, \mathbf{r}')\Big]\, dS \end{aligned} \tag{14}$$

$$\begin{aligned} \overset{(-)}{\sum_e} = \int\limits_{S^-} \big[(\mathbf{n} \times \nabla \times \mathbf{E}) \cdot \mathbb{G}(\mathbf{r}, \mathbf{r}') + \\ (\mathbf{n} \times \mathbf{E}) \cdot \nabla \times \mathbb{G}(\mathbf{r}, \mathbf{r}')\big]\, dS, \end{aligned} \tag{15}$$

where S^- signifies integration approaching the surface S from the inside of V and $\mathbf{n}$ is a unit vector outward normal to dS. An analogous set of equations can be derived for the magnetic field [5]. Here, of particular importance, are Eqns.11 and 12 and their magnetic analogues as they govern the behavior of the electromagnetic field inside and outside of V when the source is outside of V. They can be restated in different famous forms which can be adjusted to alternate material conditions (non-magnetic, non-conductor, linear, isotropic, spatially dispersive, etc.) (see [29] for survey).