RFDNA: A Wireless Authentication System On Flexible Substrates

Gerald DeJean[1], Vasileios Lakafosis[2], Anya Traille[2], Hoseon Lee[2], Edward Gebara[2], Manos Tentzeris[2], and Darko Kirovski[1]
[1]Microsoft Research, One Microsoft Way, Redmond, WA 98052 USA
[2]School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30308 USA
[1]dejean@microsoft.com

Abstract

The design and development of RFDNA, an RF authentication system consisting of wirelessly transmitting and receiving electromagnetic signals in the presence of a constellation of dense metals called certificates of authenticity that act as reflecting obstacles, has been performed [1]. The unique feature of this system is that the authentication is physical (hardware-based). Therefore, an integration process necessitates the manufacturing of certificates of authenticity to be durable and able to withstand normal wear and tear. In this system, one of the drawbacks has been the materials that have been used in the design. The materials for the readers have been designed on bulkier, non-conformable substrates, such as FR4. Additionally, the certificates of authenticity consisted of metal wires that have been densely placed into heated plastic that is hardened to maintain the wires' position. In order to realize a more practical implementation, a new class of certificates of authenticity and readers need to be manufactured on flexible substrates. This paper will focus on the design of a new antenna for an RFDNA reader on flexible substrates.

Introduction

The significance of security to logistics can be directly tied to the importance and value of the product one tries to protect. Although the world of logistics typically focuses on areas of warehouse storage, the transportation of goods, the packaging of materials, and inventory control, it is important to include how better methods of security can be integrated into the overall equation. In studies from 1997-2001, it is noted that between 5-8% of world trade [2], 10% of the pharmaceuticals market [3], and 36% of the software market [4] is counterfeited. In the United States, a 2000 study showed that out of the $250 billion in U. S. currency circulated in the country, around $48 million of it was counterfeit [5]. In addition, a similar study completed in 2000 showed that the piracy rate for Western Europe was 37% [4]. Counterfeiting dates back many years ago with the idea of inscribing small cuts into coins to trick consumers and manufacturers into believing the coin was authentic [6]. Since security procedures have well been implemented as a means of protecting goods, it is obvious that these measures are not enough to circumvent the amount of piracy and counterfeiting that continues to destroy the world economy. Therefore, is there a better means of providing security to goods that does not add complexity or significant time to the process?

Most security methods that have been utilized to this point are implemented in a two-dimensional manner. The idea of barcodes dates back 60 years and was mainly constructed as a fast and simple way to track inventory. In terms of security, barcodes have been extensively used in the airline industry for boarding passes and baggage tags. This level of security presents a potential threat due to its 2D landscape. In a threat scenario, a person X is scheduled to fly to another city and prints his boarding pass from his computer the day before his scheduled flight. An attacker Y remotely accesses X's computer from an unknown location and gains access to a printer image file of X's electronic boarding pass, for example, and effectively assumes X's identity at the airport. The 2D image of the barcode makes this scenario an unlikely but true possibility. In libraries, books are often loaded with a barcode and an accompanying magnetic strip that is demagnetized at checkout. This strip can be easily removed from the book and the book stolen from the library. Watermarking is another way of adding security to the goods and services industry. One can commonly see digital watermarking security on passports, currency, and a person's state, province, or country identification. Since watermarks on licenses are typically verified optically through the human eye, a potential threat to watermarking is the ability to produce a copy of the 2D image (with the appropriate software) and alter it in a way that makes a security agent falsely believe the license is authentic. Holograms can be distorted in a similar manner.

What makes RFDNA an attractive option for a security application is its three-dimensional (3D) physical landscape. Each RFDNA certificate is a random constellation of materials that can be composed of metal wires and/or small dielectric shapes. RFDNA has the same uniqueness as barcodes and watermarks, but the additional dimension of verticality provides more bits of entropy (randomness). Although the hottest technology on the market for inventory control is RFIDs, a major drawback is that RFIDs provide little security. RFIDs (when used for security purposes) utilize a different method of placing the secure information on the chip of the circuit. Unfortunately, any RFID reader that sends out the appropriate RF signal can gain access to the tag, and effectively, read its contents. The near-field communication mechanism of RFDNA certificates circumvents the problem of an unintended interrogator intercepting a signal. To that extent, RFDNA can be used in conjunction with RFID technology to create a "super-tag" that can store information about a product and authenticate or secure its contents.

RFDNA has been demonstrated by researchers at Georgia Tech as well as Microsoft Research using an inexpensive FR4-based PCB circuit board loaded with antennas and other circuitry. This solution has been very successful in proving the concept of RFDNA for scanning planar certificates accurately, but the rigidity of the substrate has limited its use for scanning curved surfaces. For RFDNA to be used on a wider range of products, the scanning of the RF fingerprint has to be capable on curved surfaces. Therefore, there is a

978-1-61284-498-5/11/$26.00 ©2011 IEEE

need for the design of an antenna matrix to be constructed on a flexible substrate that can conform to the surface of a particular product RFDNA is protecting. Some analysis into the design of an RFDNA reader of antennas on flexible substrates is explored.

Defining RFDNA and Understanding Certificates of Authenticity

RFDNA are certificates of authenticity (COAs) in the RF domain. A COA is a digitally signed physical object of fixed dimensions that has a random unique structure which satisfies the following requirements:

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

b.) the cost of manufacturing a COA certificate is several orders of magnitude lower than the cost of exact or near-exact replication of the unique and random physical structure of this certificate, and

c.) 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 certificates 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 $x \in C^N$. This imposes that:

d.) it should be computationally difficult to construct an object of fixed dimensions with a "fingerprint" y such that $\|x-y\| < \delta$, where x is a given "fingerprint" of an unknown COA certificate and δ bounds the proximity of x and 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 certificates 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.

Objects behave as COAs in the electromagnetic field and the kind of properties they offer as counterfeit deterrents are investigated. Radio frequency (RF) COAs are built based upon several near-field phenomena that electromagnetic waves exhibit when interacting with complex, random, and dense objects:

1. Arbitrary dielectric or conductive objects with topologies proportional in size to wave's wavelength behave as significant electromagnetic scatterers [7], i.e., they reradiate large amount of electromagnetic energy into free space.

2. The refraction and reflection of electromagnetic 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 [8, 9, 10].

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 electromagnetic 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 certificate in the high, but still inexpensive range of frequencies (less than 10 GHz). For example, in order to disturb the waves in the near-field of the certificate, a collection of randomly bent, thin conductive wires with lengths randomly set within 3-7cm is constructed. The wires are integrated into a single object using a transparent dielectric sealant illustrated in Fig. 1 [11]. The sealant fixes

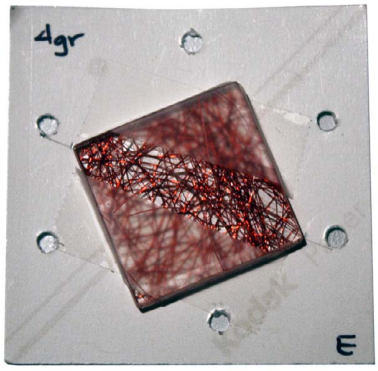


Fig. 1. Illustration of wires affixed in a dielectric sealant [11].

wires' positions within a single object once for all.

The "fingerprint" of such a certificate should represent its 3D structure as well as its dielectric and/or conductive properties. In this research, the authors 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 non-linear building elements such as ferrites and anisotropic materials.

Theoretical Analysis

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

$$\nabla \times H = \frac{1}{c}\frac{\partial D}{\partial t} + \frac{4\pi}{c}J, \quad \nabla \times E = -\frac{1}{c}\frac{\partial B}{\partial t}$$
$$\nabla \cdot D = 4\pi\rho, \quad \nabla \cdot B = 0 \qquad (1)$$

where c is the speed of light in free space, and J and ρ denote the electric current density and charge density, respectively. For most media, the linear relationships are represented as:

$$D = E + 4\pi P = \varepsilon E, \qquad (2)$$
$$B = \mu_0 H + M = \mu H,$$
$$J = \sigma E$$

where ε, μ, and σ are dielectric permittivity, magnetic susceptibility, and material's specific conductivity, respectively, and P and M are the polarization and magnetization vectors, respectively. From (1) and (2), one can derive additional equations that model the propagation of a monochromatic electromagnetic wave:

$$\begin{aligned} \mathrm{F_e}&=\nabla\times\nabla\times\mathrm{E}-\mathrm{k}^2\mathrm{E} \\ \mathrm{F_e}&=-4\pi\left(\frac{\mathrm{ik}}{\mathrm{c}}\mathrm{J}+\mathrm{k}^2\mathrm{P}+\mathrm{ik}\nabla\times\mathrm{M}\right) \end{aligned} \tag{3}$$

$$\begin{aligned} \mathrm{F_m}&=\nabla\times\nabla\times\mathrm{H}-\mathrm{k}^2\mathrm{H} \\ \mathrm{F_m}&=4\pi\left(\frac{1}{\mathrm{c}}\nabla\times\mathrm{J}+\mathrm{k}^2\mathrm{M}-\mathrm{ik}\nabla\times\mathrm{P}\right) \end{aligned} \tag{4}$$

where $k = \omega/c$ is the wavenumber. Equations (3) and (4) fully describe electromagnetic waves in 3D space – however, commonly another form is used for simulation of scattering based upon the Ewald-Oseen extinction theorem [8, 9]. A material medium occupying a volume V limited by a surface S and use $r_>$ and $r_<$ to denote vectors to an arbitrary point outside and inside V, respectively, is considered. The variables are illustrated in Fig. 2.

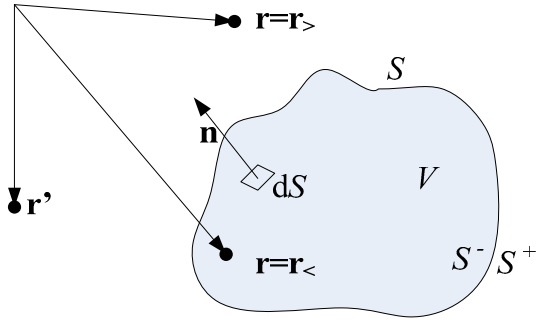


Fig. 2. Illustration of the main variables for (5) – (12).

The dyadic form, G(r,r'), of the scalar Green function, G(r,r'):

$$\mathbb{G}(\mathrm{r},\mathrm{r}')=\left(\mathfrak{I}+\frac{1}{k^2}\nabla\nabla\right)\mathrm{G}(r,r') \tag{5}$$

$$\mathrm{G}(r,r')=\frac{\exp\left(ik\left|r-r'\right|\right)}{\left|r-r'\right|} \tag{6}$$

where G is a unit dyadic, describes a spherical wave at point r sourced from point r'. Now, the generalized extinction theorem [10] states:

$$E(r_<)=\frac{1}{4\pi}\int_V F_e(r')\cdot\mathbb{G}(r_<,r')d^3r'-\frac{1}{4\pi}\sum_e^{(-)}(r_<) \tag{7}$$

$$E^{(i)}(r_<)+\frac{1}{4\pi}S_e(r_<)=0 \tag{8}$$

$$E(r_>)=E^{(i)}(r_>)+\frac{1}{4\pi}S_e(r_>) \tag{9}$$

$$0=\frac{1}{4\pi}\int_V F_e(r')\cdot\mathbb{G}(r_>,r')d^3r'-\frac{1}{4\pi}\sum_e^{(-)}(r_>) \tag{10}$$

where points r and r' are both inside of V (7), inside and outside of V (8), both outside of V (9), and outside and inside of V (10), respectively. $E^{(i)}$ is the incident field upon V and

$$\mathrm{S_e}=\int_{S^-}\left[\begin{aligned}&\left(n\times(\nabla\times E-4\pi\mathrm{ikM})+\frac{4\pi\mathrm{ik}}{c}\mathrm{J}\right)\cdot G(\mathrm{r},\mathrm{r}') \\ &+\left(\mathrm{n}\times\mathrm{E}\right)\cdot\nabla\times G(\mathrm{r},\mathrm{r}')\end{aligned}\right]\mathrm{dS} \tag{11}$$

$$\sum_{\mathrm{e}}^{(-)}(\mathrm{r}_<)=\int_{S^-}\left[\left(\mathrm{n}\times\nabla\times\mathrm{E}\right)\cdot G(\mathrm{r},\mathrm{r}')+\left(\mathrm{n}\times\mathrm{E}\right)\cdot\nabla\times G(\mathrm{r},\mathrm{r}')\right]\mathrm{dS} \tag{12}$$

where S^- signifies integration approaching the surface S from the inside of V and n is an outward unit vector that is normal to dS. An analogous set of equations can be derived for the magnetic field [10]. Equations 11 and 12 and their magnetic analogues are particularly important because 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 various forms which can be adjusted to alternate material conditions (non-magnetic, non-conductor, linear, isotropic, spatially dispersive, etc.).

This analysis is an abbreviated way of explaining RFDNA in terms of Huygens' principle [12] and Babinet's principle [12]. In short, Huygens' principle characterizes wave propagation through an aperture. This principle states that as a wave reaches the interface of an aperture, elements that act like point sources radiate a new group of spherical electromagnetic waves. (This mimics the concept of reflection and reradiation of a source.) Babinet's principle is a complimentary principle that basically states that the complimentary analysis of radiation of a wave through an aperture is the radiation of an obstacle that is the same shape as the aperture. Fig. 3 illustrates diagrams that describe Huygens' principle and Babinet's principle. For RFDNA, the incident waves are represented by the wave of small antennas, and the obstacles are represented by copper wires.

Scanning the Response

To scan the electromagnetic features of an RFDNA certificate, the authors have proposed a scanner designed to expose the subtle variances of near-field responses of these objects to RF waves in [11]. This scanner consists of a single matrix of antennas, where each antenna is capable of

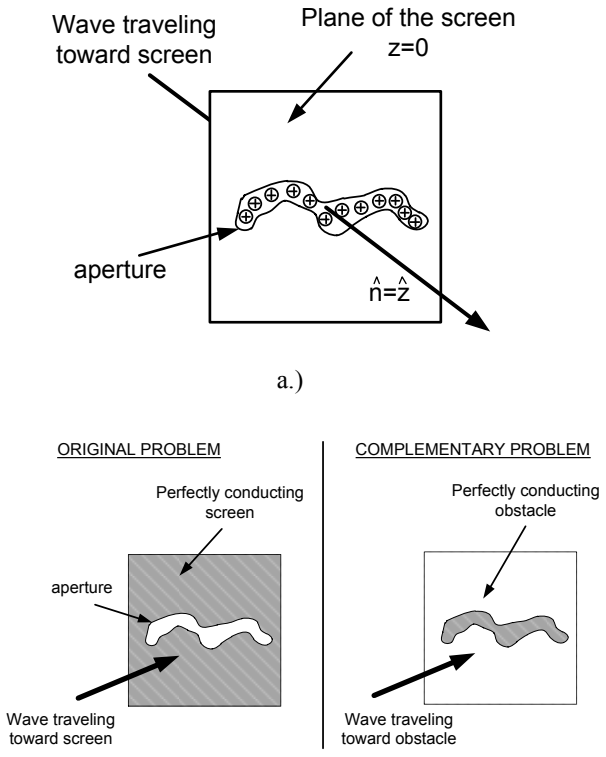


Fig. 3. Diagram of a.) Huygens' principle for solving wave propagation through an aperture and b.) Babinet's principle for solving wave propagation impinging on an obstacle.

operating both as a transmitter and a receiver. While scanning a certificate, it is aligned to a fixed position with respect to the antenna matrix. The RFDNA certificate 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 certificate, its reflection and refraction is dependent upon the 3D positioning of the scatterers embedded in the RFDNA. 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 RFDNA 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 scattering parameters can be obtained for the two-port network. A matrix representation of the relationship between the voltage and the scattering parameters are shown in (13):

$$\begin{bmatrix} V_1^- \\ V_2^- \end{bmatrix} = \begin{bmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{bmatrix} \begin{bmatrix} V_1^+ \\ V_2^+ \end{bmatrix} \tag{13}$$

For example, for a system with M antennas, one can measure M s_{11} and $\binom{M}{2} s_{21}$ parameters. In order to enable this, each antenna is multiplexed to an analog/digital back-end capable of extracting the s_{21} parameter (i.e., insertion loss) for a particular antenna coupling. A complete and more in-depth design of the proposed RFDNA scanner is identified in [11]. In mass production, it is estimated that the price for this reader should be well below US$100. A manufactured prototype is shown in in Fig. 4 [11].

Design of Flexible Antenna Reader Prototype for

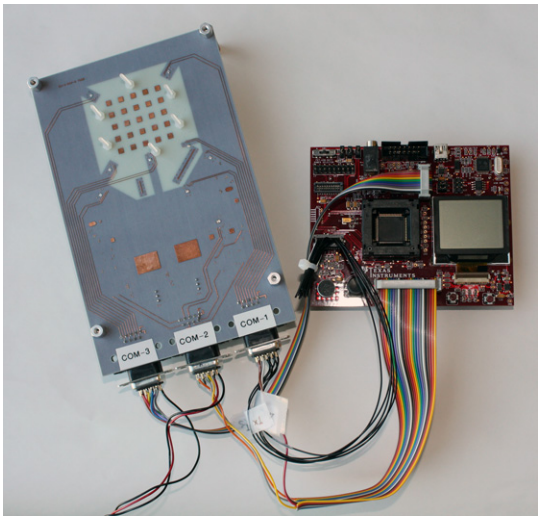


Fig. 4. Illustration of prototype reader for RFDNA [11].

Consideration

To scan the electromagnetic features of an RFDNA certificate that is mounted on a curved surface, the authors have proposed a scanner composed of a matrix of antennas designed at 6.4 GHz. The frequency of operation was selected to maintain a small circuit size. (A lower frequency would have made the design's size too large for a practical application and a higher frequency would have required the trace dimensions and spacings in the design to be too small for cheap board-house fabrication.) The substrate is FastFilm which has a dielectric constant of 2.7 and a loss tangent of 0.0012. The thickness of the material is 0.25 mm (but it can be manufactured to be as small as 0.05 mm). This is more than six times the size of the original prototype of Fig. 4. This substrate thickness reduction allows for the antenna matrix to be flexible for curved surfaces. The metal for the circuit is copper (Cu), and its thickness is about 0.02 mm.

One can naturally assume that the decrease in overall thickness of an antenna whose frequency of operation is close to that of the original design comes at a price and this is true here – the gain is significantly reduced. This is acceptable for this application considering the placement of the certificate with respect to the reader is very close, so the wave propagation in the scanning constitutes a near-field link; therefore, gains above -2 dBi suffice.

An illustration of the new prototype antenna for reader consideration is shown in Fig. 5. The use of patch antennas as radiators has been replaced by a modified planar inverted F antenna (PIFA) element. Replacing the patch antenna backed by a ground plane in which the substrate thickness is critical

for radiation was necessary to achieve strong resonance at a frequency that is well below that expected of a patch antenna with this thickness. The radiating element of the modified PIFA does not have a ground plane directly underneath so the thickness of the substrate is of less importance. The width of the traces is 1 mm, and the total size of the PIFA is 6.3 mm x 5.8 mm. There is a via that is shorted to ground, the feed point location is selected to provide good impedance matching. The square gap (on the right side of the PIFA) is intended to further elongate the current path so that the resonant frequency can be decreased without increasing the total size of the element.

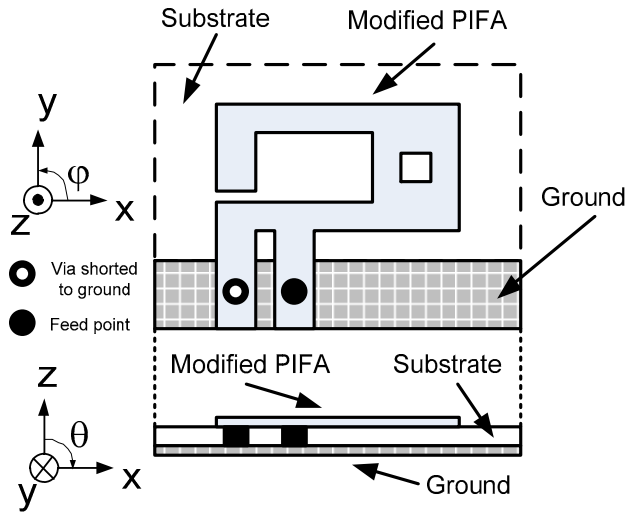
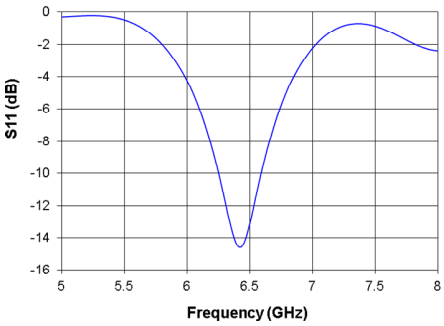


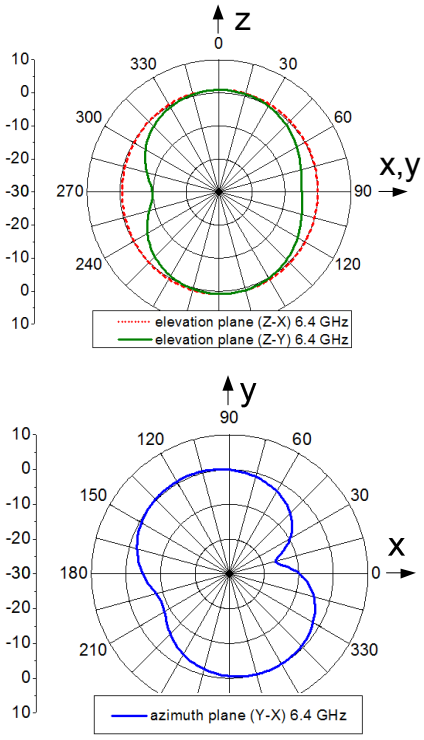
Fig. 5. Illustration of proposed modified PIFA design for an RFDNA reader on a flexible substrate.

The simulated S_{11} performance of the antenna is shown in Fig. 6. In this plot, it is seen that the maximum peak return loss at 6.4 GHz is 14.6 dB; in addition, an 8-dB return loss bandwidth of 7.5% can be obtained. The simulated radiation pattern in one plane is also shown in Fig. 6. As expected, the modified PIFA radiates omnidirectional energy with maximum radiation in the z-direction. The maximum gain is 0.9 dBi. The lowest achievable gain is -0.5 dBi, so the maximum/minimum gain ratio is only 1.4 dB. Despite the fact that the design is on a thin substrate, the simulated radiation efficiency is 0.79. All simulations were performed using CST Microwave Studio, a 3D full-wave solver that solves for electromagnetic fields in the time domain.

In the previous implementation (Fig. 4), 25 total antennas were used to create a 5x5 matrix. Based on the fact that the lateral size of a single modified PIFA is larger than that of the patch used in the 5x5 matrix, a 4x4 matrix is the best possible solution without significantly increasing the lateral size of the reader. After optimizing the modified PIFA, the 4x4 matrix was designed and is shown in Fig. 7. The total size of the antenna matrix is approximately 38 mm x 38 mm. Simulating all the antennas in the matrix when an RFDNA certificate is placed in close proximity to reader will not gain any worthwhile insight into the performance of the matrix. This is due to the vast



a.)



b.)

Fig. 6. Plots of a.) S_{11} in dB and b.) the 2D radiation patterns for the new modified PIFA.

number of mutually dependent factors in the analysis such as coupling between antennas and scattering off of obstacles. In the future, measurements will be conducted to test three figures of merit: the sensitivity of the measurement, the repeatability of measurement, and the entropy of the response. The sensitivity will test how slight a misalignment can be before creating a new response of a given certificate. The repeatability will test how repeatable the response will be when a given certificate is scanned removed and rescanned later. Finally, entropy is a measure of a system's randomness –

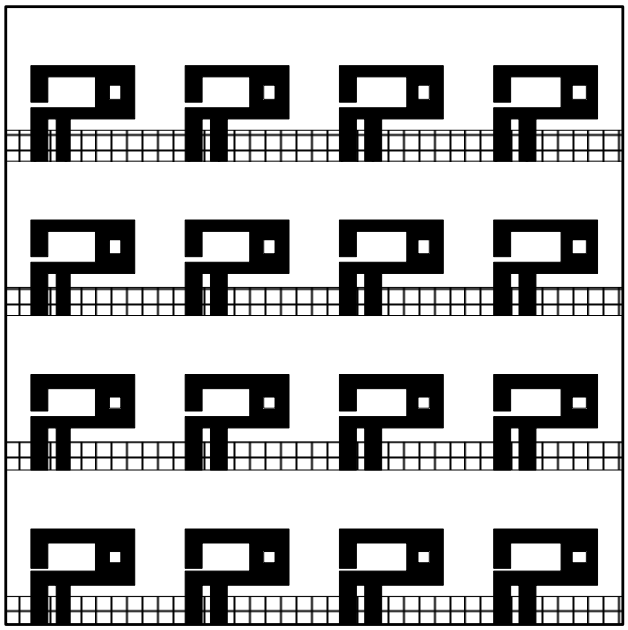


Fig. 7. Illustration of proposed modified PIFA design for an RFDNA reader on a flexible substrate.

a higher value means that the certificate's response is more distinguishable from that of another certificate.

Conclusions

The design of a modified PIFA supported by a flexible substrate that can conform to the surface of a particular product is proposed. This antenna can be integrated for use as a part of an antenna matrix. This implementation will allow the deployment of RFDNA to be utilized for several purposes. One particular application that could potentially utilize RFDNA is tamper-proof seals for medication. This technology can be used to seal medication packages so that opening a package would incur destroying RFDNA's physical structure beyond possible recreation. More information on this design as well as RFDNA as a whole and its possible applications will be presented at the conference.

References

1. G. DeJean and D.Kirovski, "Making RFIDs unique – radio frequency certificates of authenticity," *IEEE AP-S Int. Symp.*, Albuquerque, 2006, pp. 1039–1042.
2. J. Kafchinski. (2009. May 11). *Global Counterfeit Trade* [Online]. Available: http://policy-traccc.gmu.edu/resources/publications/student forum/Chinese%20Counterfieting%20Kafchinski.pdf
3. Xstream Team. (2008. Mar. 22). *Counterfeit Pharmaceutical Statistics* [Online]. Available: http://securepharmachain.blogspot.com/2008/03/counterfeit-pharmaceutical-statistics.html
4. Business Software Alliance. (2002. June). *Seventh Annual BSA Global Software Piracy Study* [Online]. Available: http://www.bsa.org/country/Research%20and%20Statistics/~/media/B7B6D8B30236445AB525A8BDCA869962.ash
5. United States Treasury Department. (2003. March). *The Use and Counterfeiting of United States Currency Abroad* [Online]. Available: http://www.federalreserve.gov/boarddocs/rptcongress/counterfeit2003.pdf
6. K. Barry. (2003. July). *Counterfeits and Counterfeiters: The Ancient World* [Online]. Available: http://www.ancient-times.com/newsletters/ n13/n13.html
7. L. Tsang et al., *Scattering of Electromagnetic Waves*. New York: Wiley, 2001.
8. P. P. Ewald, *Ann der Physik*, vol. 49, pp. 1-56, 1915.
9. 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.
10. E. Wolf, "A generalized extinction theorem and its role in scattering theory," *Coherence and Quantum Optics*, L. Mandel and E. Wolf, Ed. New York: Plenum, 1973.
11. V. Lakafosis, A. Traille, H. Lee, E. Gebara, M. M. Tentzeris, G. R. DeJean, and D. Kirovski, "RF fingerprinting physical objects for anticounterfeiting applications," *IEEE Trans. Microw. Theory Tech.*, vol. 59, no. 2, pp. 504–514, Feb. 2011.
12. G. Smith, *An Introduction to Classical Electromanetic Radiation*, Cambridge, UK: Cambridge University Press, 1997.