A Split Manufacturing Approach for Unclonable Chipless RFIDs for Pharmaceutical Supply Chain Security

Kun Yang, Ulbert Botero, Haoting Shen, Domenic Forte and Mark Tehranipoor
ECE Department, University of Florida
Email: {k.yang, jbot2016, htshen}@ufl.edu; {dforte, tehranipoor}@ece.ufl.edu

***Abstract*—Today's pharmaceutical supply chain suffers from counterfeiting and theft issues, which not only compromise the profits and reputations of manufacturers, distributors, and retailers, but also pose a threat to consumer safety and public health. Track-and-trace techniques form the foundation for an improved supply chain by enabling supply chain owners and/or participants to systematically detect and control counterfeiting, theft, etc., but existing approaches (barcodes, QR codes, and IC-based RFID) are too costly, inconvenient, unreliable, or insecure. While an improvement, existing chipless RFID tags are limited by their complex manufacturing process, large tag area, small identifier (ID) size, and vulnerability to cloning attack. In addition, the pharmaceutical industry lacks a simple and effective way to enable pill-level traceability. To address these problems, we propose a new split manufacturing based pill-level unclonable chipless RFID (pill-level UCR) tag that intrinsically generates a unique ID from multiple entropy sources. Pill-level UCR tag consists of two parts: (i) a certain number of concentric ring slot resonators integrated on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets; and (ii) nontoxic silver particles of random quantity with random diameters filled in random places of each pharmaceutical tablet. The diameter of pill-level UCR tag is as small as 10 mm. Simulation results based on CST Microwave Studio 2015 have verified the effectiveness and reliability of pill-level UCR tags.**

***Index Terms*—Pharmaceutical Supply Chain, Chipless RFID Tag, Split Manufacturing, Pill-Level Traceability, Uniqueness, Unclonability**

I. Introduction

The pharmaceutical supply chain, which spans many geographical areas and involves numerous parties, is the pathway through which prescription and over-the-counter (OTC) drugs are delivered from manufacturing sites to patients. GlobalData predicts that the estimated value of US pharmaceutical market will increase from $395.2 billion in 2014 to $548.4 billion by 2020, which represents a compound annual growth rate (CAGR) of 5.6% [1]. The appearance of new drugs, technological innovations, price fluctuations of raw materials, new supplies and geographies in the chain, as well as evolving tax, regulatory, and market demands are driving change and making the pharmaceutical supply chain more complex. Increased complexity of pharmaceutical supply chain implies increased difficulty to maintain security and quality control. Today's pharmaceutical supply chain suffers from counterfeiting and theft issues, which not only compromise the profits and reputations of manufacturers, distributors, and retailers, but also pose a threat to consumer safety and public health.

A counterfeit drug is a pharmaceutical product that has been deliberately manufactured and sold with the intent to fraudulently represent its source, authenticity or efficacy [2]. Fake or substandard medicines yielded an estimated revenue of $75 billion in 2010 alone, according to the National Association of Boards of Pharmacy [3]. The 2008 case of counterfeit blood thinner heparin is one example of tragedies caused by counterfeit drugs in the United States [4]. In this case, the active ingredient in heparin was replaced with a cheaper counterfeit substitute, causing a series of adverse reactions and nationwide recalls. The counterfeit heparin was eventually suspected to be the cause of as many as 81 deaths. Theft may occur at any stage of pharmaceutical supply chain. Stolen drugs may be later reintroduced to the legitimate supply chain by dishonest supply chain participants. Theft and/or diversion of pharmaceutical products pose severe threats to public health because provenance and authenticity are difficult to be verified for products that leave – and are later reintroduced to – the legitimate supply chain. In 2013, the average loss per pharmaceutical theft incident was $261,819 [5].

Track-and-trace techniques form the foundation for an improved supply chain by providing supply chain owners and/or participants with visibility into supply chain status and enabling them to systematically detect and control counterfeiting, theft, etc., but existing approaches are too costly, inconvenient, unreliable, or insecure. Barcodes have traditionally been used to track and trace commodities in the supply chain. QR codes with greater storage capacity have also been put into use more recently. QR codes can be encrypted to prevent unauthorized information extraction [6]. However, both barcodes and QR codes are very easy to duplicate because of visibility and controllability of pixel information (even though adversaries cannot easily retrieve the actual content from encrypted QR codes). Other shortcomings (e.g., requirement of individual scanning, direct line-of-sight, close proximity to scanner, etc.) severely impact their overall utility.

RFID [7], [8], [9] is growing in popularity as a replacement of barcodes and QR codes. For example, Wal-Mart and the United States Department of Defense have published requirements that their vendors place RFID tags on all shipments to improve supply chain management [10]. Compared with traditional optical labels, an RFID-based track-and-trace system has many engaging features – support batch scanning, do not require direct line-of-sight for access, and need less human involvement for data collection – making automatic track and trace possible. However, the relatively higher price of IC-based RFID tags makes them inappropriate for protecting the supply chain of low-cost commodities.

Compared with IC-based RFID tags, chipless RFID tags [11], [12], [13] without microchips have been gaining more attention recently due to their following merits: (i) extremely low price (as low as 0.1 cents) makes them more appropriate for protecting the supply chain of low-cost commodities; (ii) chipless RFID tags consume near-zero power; (iii) chipless RFID tags can be directly printed on the products or their packages with conductive three-dimensional (3D) printing materials; (iv) elimination of tag memory shelters chipless RFID tags from denial-of-service (DoS) attack carried out in the form of overwriting tag memory; (v) chipless RFID tags are not sensitive to ambient temperature variation unless special substrate materials are used for temperature tracking purpose. Existing chipless RFID tags (more in Section II), however, are limited by complex manufacturing process, large tag area, small ID size (usually not exceeding 35 bits), and vulnerability to cloning attack.

The authors in [14] proposed the first unclonable chipless RFID

(UCR) tag (more in Section II) that intrinsically generates a unique ID from manufacturing variations. However, their proposed UCR tag does not establish an inseparable connection with the object being identified and thus is vulnerable to split attacks (i.e., separating tag from product, swapping tags, etc.).

In addition, the pharmaceutical industry lacks a simple and effective way to enable pill-level traceability. To address these problems, we propose a new split manufacturing based pill-level unclonable chipless RFID (pill-level UCR) tag that intrinsically generates a unique ID from multiple entropy sources. Pill-level UCR tag in essence is a unique object [15] that, upon measurement by an external apparatus, exhibits a small, fixed set of inimitable analog properties that are different from any other entity of the same type. Pill-level UCR tag consists of two parts: (i) a certain number of concentric ring slot resonators integrated on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets; and (ii) nontoxic silver particles of random quantity with random diameters filled in random places of each pharmaceutical tablet. A set of resonance frequencies sensitive to manufacturing variations and randomnesses of silver particles will be captured and used as the unique ID of each pill-level UCR tag. To the best of our knowledge, this is the first unclonable chipless RFID tag that builds up an inseparable connection with the object being identified. The diameter of our proposed pill-level UCR tag is as small as 10 mm. To summarize, we make the following contributions:

- A split manufacturing approach for unclonable chipless RFID tag to establish an inseparable connection between tag and identified object.
- A pill-level track-and-trace technique to protect pharmaceutical supply chain. Each pharmaceutical tablet has its own unique signature. The signatures of all pharmaceutical tablets within the same blister pack would be bound together to add one more layer of security and be resistant against illegal tablet replacement.
- Performance evaluation of pill-level UCR tags under extremely adverse environmental conditions (i.e., noisy environment, varying angles of plane wave incidence, etc.). We also explore and compare a variety of supervised and unsupervised methods for identifying tags based on their UCR responses.

The remainder of this paper is organized as follows: Section II introduces the related work. Section III describes the proposed split manufacturing based pill-level UCR tags in detail and how they can generate unique and unclonable IDs from multiple entropy sources. In Section IV, we evaluate the performance of pill-level tags. We also analyze the resilience of pill-level UCR system to the potential attacks in this section. Finally, we give concluding remarks in Section V.

II. Related Work

Chipless RFID tags can be classified into three main categories: (i) time-domain reflectometry (TDR) based chipless tags [16]; (ii) spectral signature based chipless tags [12], [17]; and (iii) amplitude/phase backscatter modulation based chipless tags [11]. Because of page limit, we review only closely related spectral signature based chipless tags.

The authors in [17], [12] proposed a fully printable, passive and planar chipless RFID tag that consists of a vertically polarized ultra-wideband (UWB) disk-loaded monopole receiving antenna (receiver), a multiresonating circuit, and a horizontally polarized UWB disk-loaded monopole transmitting antenna (transmitter). Cascaded spiral resonators placed closely adjacent to the microstrip that connects the transmitter and receiver are used by the multiresonating circuit to encode data bits. Spiral resonators with different patterns and dimensions will introduce different levels of amplitude attenuations and phase jumps at different frequencies of the spectrum. Data bits are encoded by removing some spirals or shorting their turns. When one spiral resonator is removed or shorted, its corresponding resonance point will either disappear from the spectrum or shift outside the frequency band of interest. One bit is encoded to '1' when the corresponding resonance point appears at a specific frequency, and '0' when the resonance point disappears, or vice versa. This type of chipless tags build up 1:1 correspondence between bit width and number of deployed spiral resonators. Consequently, the tag area will monotonically increase with the increase of bit width, which is undesirable. The manufacturing cost will be unbelievably high if different layouts with different resonator shorting states are used to fabricate the tags. Although the same layout with all the resonators shorted can be used to fabricate the tags and when encoding data the shorting can be removed using laser cutting or traditional etching techniques, the manufacturing time will be significantly increased. For a specific layout, the IDs generated in this way are deterministic and reproducible, making them vulnerable to cloning attack.

The authors in [14] designed the first UCR tag that integrates a certain number of concentric ring slot resonators on a particular laminate. The vector that includes the analog value of each slot resonator's resonance frequency is regarded as the unique ID. However, their proposed UCR tag does not establish an inseparable connection with the object being identified and thus is vulnerable to split attacks. In addition, none of the above-mentioned methods could provide a pill-level traceability for protecting the pharmaceutical supply chain.

To mitigate the shortcomings of existing solutions, we propose a new split manufacturing based pill-level chipless RFID tag for protecting the pharmaceutical supply chain.

III. Pill-Level UCR System

The proposed pill-level UCR system is presented in this section. We first describe the architecture and working principle of pill-level UCR system, and then introduce the machine learning based tag recognition method. Lastly, we present the split manufacturing approach for combating replay attack.

A. Architecture and Working Principle

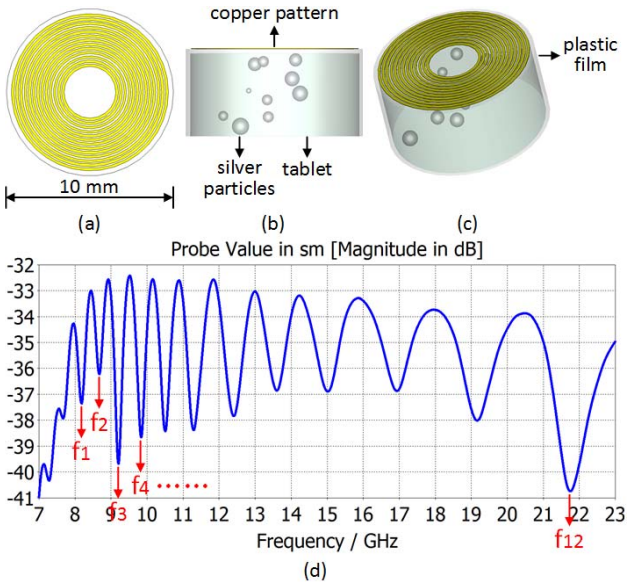

Fig. 1: Pill-level UCR tag that consists of concentric ring slot resonators and nontoxic silver particles: (a) top view, (b) side view, (c) 3D view, and (d) frequency response spectrum.

Figure 1(a), (b), and (c) show the proposed pill-level UCR tag that consists of two parts: (i) a certain number of concentric ring slot resonators integrated on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets; and (ii) nontoxic silver particles of random quantity with

random diameters filled in random places of each pharmaceutical tablet. Note that silver particles are nontoxic and could be broken down by stomach acids [18]. When we stimulate the pill-level UCR tag with a swept-frequency continuous-wave signal (i.e., plane wave), as illustrated in Figure 2(a), the array of resonators will absorb part of the signal energy and introduce attenuations at particular frequencies of the response spectrum. As shown in Figure 1(d), the number of fundamental resonance points in the spectrum will correspond to the number of slot resonators. These resonance points are independent of each other. An RFID reader will be responsible for providing the plane wave and capturing the frequency response spectrum. Since RF signals are capable of traveling through nonmetallic packaging materials such as paper and plastic, pill-level UCR system enables drug authentication without necessarily opening the package, as shown in Figure 2(b).

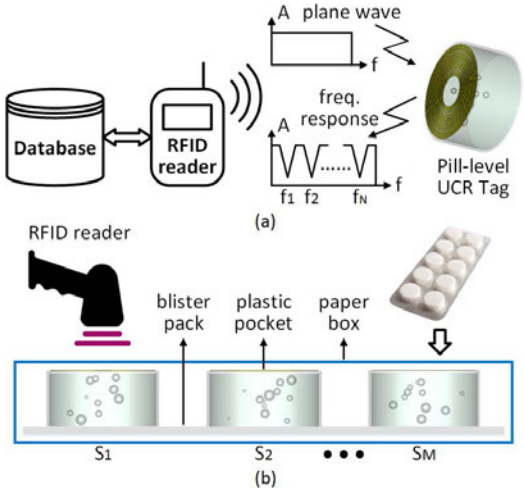

Fig. 2: Pill-level UCR system: (a) working principle and (b) drug authentication without necessarily opening the package.

Due to process variations during tag manufacturing, the slot parameters (i.e., trace width, air gap, substrate thickness, and substrate dielectric constant) of each resonator will deviate from their design values. The set of resonators could be first integrated on an ultra-thin printed circuit board (PCB) (as thin as 100 μm), which could be later adhered to the external surface of plastic cavities or pockets of blister pack with glue. The merit of this approach is that pill-level UCR tags could be directly applied to legacy blister packs. A more cost-effective approach for integrating resonators on plastic cavities or pockets is to directly print blister packs carrying copper patterns using a 3D printer.

TABLE I: PCB manufacturing tolerances

PCB Manufacturer	Trace Width / Air Gap Tolerance	PCB Thickness Tolerance
Advanced Circuits	max($\pm$20%, $\pm$0.002")	max($\pm$10%, $\pm$0.005")
Sunstone	$\pm$ 20%	$\pm$ 10%
Sierra Circuits	$\pm$ 0.001"	$\pm$ 10%
Precision PCBS	$\pm$ 20%	$\pm$ 0.005"
RUSH PCB	$\pm$ 0.005"	$\pm$ 10%

Table I illustrates the manufacturing tolerances of five major PCB manufacturers in the United States. For the trace width and air gap, the maximum deviation between design value and measured value can be as large as 20%. PCB thickness will typically have a tolerance of 10%. The authors in [14] have proved that the resonance frequency of slot resonator is sensitive to variations of slot parameters. The randomnesses of silver particles (i.e., random quantities, random diameters, random positions, random sphericities, etc.) will alter the effective dielectric constant of substrate material and more importantly impact the electromagnetic (EM) field distribution when the tag is being stimulated by the plane wave. Consequently, the resonance frequency of each slot resonator will deviate from its design value due to the variations of slot parameters. Because of the randomnesses of process variations and the randomnesses of silver particles, the frequency signature of each pill-level UCR tag will be unique and different from each other. The proposed pill-level UCR tag is unclonable since the adversaries cannot easily model the uncontrollable process variations during tag fabrication. For a pill-level UCR tag with 12 slot resonators, its diameter could be as small as 10 mm. The signatures $(S_1, S_2, ..., S_M)$ of all tablets within the same blister pack will be bound together to add one more layer of security to be resistant to illegal tablet replacement.

The authors in [14] proposed to use the vector $(f_1, f_2, ..., f_N)$ as the identifier of each UCR tag, where f_i indicates the resonance frequency of the i_{th} slot resonator. Because of noise interference and angle variation of plane wave incidence, the signatures captured from the same tag may be slightly different at different times. Euclidean distance (ED) between two vectors $\vec{v_i}^j = (f_1^j, f_2^j, ..., f_N^j)$ and $\vec{v_i}^k = (f_1^k, f_2^k, ..., f_N^k)$ can be used to determine whether these two vectors correspond to the same tag, where $\vec{v_i}^j$ and $\vec{v_i}^k$ denote the signatures of the i_{th} tag measured at times j and k. The Euclidean distance between $\vec{v_i}^j$ and $\vec{v_i}^k$ can be computed as follows:

$$ED_i^{j,k} = |\vec{v_i}^j - \vec{v_i}^k| = \sqrt{\sum_{r=1}^{N}(f_r^j - f_r^k)^2} \quad (1)$$

Two signatures are determined to correspond to the same tag if their Euclidean distance is not larger than the maximum intra-tag Euclidean distance obtained at the enrollment phase.

B. Machine Learning Based Tag Recognition

Supervised machine learning provides a method of guiding the pill-level UCR system to correctly learn and classify the features that differentiate the tags from one another. One popular supervised learning technique is the linear discriminant analysis (LDA) [19] classifier. By maximizing the variance between different tag measurements and minimizing the variance within same tag measurements, the classifier is able to distinguish between different tags by focusing on the most discriminant features, a la principal component analysis (PCA) [20]. Furthermore, the classification algorithm also serves as a method of dimensionality reduction. The computation of the transformation matrix for LDA is reliant upon being able to compute the inverse within tag scatter matrix, which means the matrix must be non-singular. However, in practice the opposite is often the case with high dimensional data where the size of the data set is smaller than its dimensionality. This is the case for our simulations in Section IV, but may not be so in practical application where a database could contain as many as millions of pill-level tags. For this reason, PCA is still necessary for not only dimensionality reduction but also to ensure the resultant matrices after projection are non-singular. Applying PCA prior to computing LDA is a good practice regardless of the size of the data set, since it helps with avoiding overfitting. Therefore, the procedure for implementing a supervised machine learning based tag authentication system is as follows:

Step 1: Compute the principal components of the tag data set to be enrolled.

Step 2: Project the tag spectra into reduced dimensional space using computed principal components. This also ensures non-singular matrices for subsequent LDA computation.

Step 3: Apply LDA to projected data to compute transformation matrix that can be used for LDA projection and classification.

Step 4: Apply LDA transformation matrix to PCA projected tag spectra and enroll resultant LDA projected tag signatures into database.

Step 5: Use principal components from ***Step 1*** to project the spectrum of tag under authentication (TUA) to reduced dimensional

space. Then apply LDA transformation matrix computed in ***Step 3*** to PCA projected TUA spectrum. If in the projected space TUA has the minimum distance with an enrolled tag compared with all the remaining tag entries, and that distance is smaller than a threshold d_{th} computed from the equal error rate (EER) of the enrolled tag database, we determine that TUA matches with this tag entry; otherwise we determine that TUA does not belong to the database.

However, a potential drawback of this approach is that the computational complexity increases as the size of enrollment increases. For every new enrollment, PCA and LDA would need to be reapplied. For PCA the principal components that capture the most variance at a reduced dimensionality would need to be recalculated. For LDA the projections that maximize the variance between PCA projected different tag measurements and minimize the variance within PCA projected same tag measurements would need to be recalculated. This would be inconvenient and computationally intensive for large data sets.

By supplanting the supervised learning methodology with an unsupervised approach, there would be a tradeoff in a decrease in accuracy for increased computational savings and ease in new tag enrollments. The unsupervised approach would be to simply find a set of features that distinguish tags from one another, such as their resonance points, and merely perform distance calculations or compute the similarity between feature vectors. Examples of measures that could be used include Euclidean distance (mentioned earlier), Lorentzian distance (LD), Manhattan distance (MD), and the normalized correlation coefficient (NCC).

The Lorentzian distance between the feature vector of an enrolled tag $\vec{v}^{Enroll} = (f_1^{Enroll}, f_2^{Enroll}, ..., f_N^{Enroll})$ and the feature vector of TUA $\vec{v}^{TUA} = (f_1^{TUA}, f_2^{TUA}, ..., f_N^{TUA})$ can be computed as follows:

$$LD^{Enroll,TUA} = \sum_{r=1}^{N} ln(1 + |f_r^{Enroll} - f_r^{TUA}|) \quad (2)$$

The Manhattan distance between $\vec{v}^{Enroll}$ and $\vec{v}^{TUA}$ can be computed as follows:

$$MD^{Enroll,TUA} = \sum_{r=1}^{N} |f_r^{Enroll} - f_r^{TUA}| \quad (3)$$

The normalized correlation coefficient between $\vec{v}^{Enroll}$ and $\vec{v}^{TUA}$ can be computed as follows:

$$NCC^{Enroll,TUA} = \frac{(\vec{v}^{Enroll} - \overline{\vec{v}^{Enroll}}) \cdot (\vec{v}^{TUA} - \overline{\vec{v}^{TUA}})}{||\vec{v}^{Enroll} - \overline{\vec{v}^{Enroll}}|| \times ||\vec{v}^{TUA} - \overline{\vec{v}^{TUA}}||} \quad (4)$$

where $\overline{\vec{X}}$, $\vec{X} \cdot \vec{Y}$, and $||\vec{X}||$ respectively indicate the mean value of $\vec{X}$, the dot product between $\vec{X}$ and $\vec{Y}$, and the L^2 norm of $\vec{X}$.

Each measure has properties that are unique and such make it more ideal for certain applications than others. For example, normalized correlation coefficient computes the similarity between two normalized vectors helping to avoid any influence in similarity that could arise from outliers in the feature vectors. Using these distance measures or similarity coefficients as a method of unsupervised classification with a feature vector provides an option for easier enrollment of new tags since all that needs to be enrolled now is the feature vector of the new tag. The procedure for implementing an unsupervised machine learning based tag authentication system is as follows:

Step 1: During the ***enrollment phase***, extract feature vectors (e.g., the set of resonance points) from all pill-level UCR tags and store them in the database.

Step 2: During the ***authentication phase***, extract feature vector from TUA.

Step 3: Look up tag entry that has the minimum distance or maximum similarity with TUA in the database. If the minimum distance is smaller than a threshold d_{th} computed from the EER of the enrolled tag database, we determine that TUA matches with this tag entry; otherwise we determine that TUA does not belong to the database.

C. Split Manufacturing

Figure 3 shows the split manufacturing process for pill-level UCR tags, which includes the following steps:

Step 1: Pharmaceutical manufacturer fills silver particles of random quantity with random diameters in random positions of pharmaceutical tablets. This step could happen at the formulation phase of pharmaceutical manufacturing.

Step 2: The blister pack manufacturer integrates copper pattern (i.e., a certain number of concentric ring slot resonators made of copper traces) on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets. One cost-effective approach for integrating resonators on plastic cavities or pockets is to directly print blister packs carrying copper patterns using a 3D printer.

Step 3: Pharmaceutical packager first fills tablets into the plastic cavities or pockets of blister pack and then packages the blister pack using a paper box that carries the manufacturer's logo. Tamper-evident packaging techniques [21] could be used at this step.

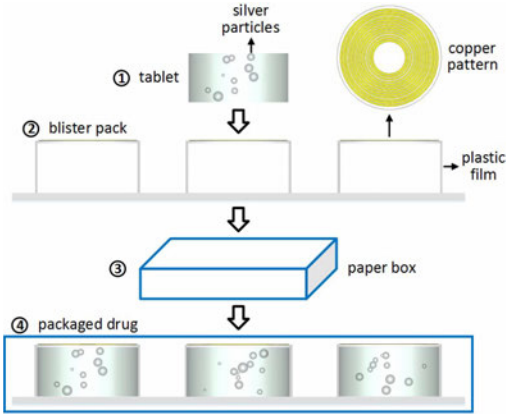

Fig. 3: Split manufacturing process for pill-level UCR.

Note that ***Step 1*** and ***Step 2*** could happen in parallel. Concentric ring slot resonators made by the blister pack manufacturer and silver particles filled by the pharmaceutical manufacturer together comprise our proposed pill-level UCR tag. Entropy sources contributing to the uniqueness of pill-level UCR include process variations during copper pattern manufacturing (i.e., variations of slot geometric parameters and substrate dielectric constant) and randomnesses of silver particles (i.e., random quantities, random diameters, random positions, random sphericities, etc.). In general, RFID tags would be outsourced to a third-party company (blister pack manufacturer in our context). Our proposed split manufacturing approach carries far-reaching significance since it prevents untrusted tag manufacturer from recording the frequency response spectra of all UCR tags and performing replay attack during tag authentication. Admittedly, the adversary could purchase a small number of products carrying authentic tags from the market, recording their frequency response spectra, and performing replay attack during tag authentication. However, the resulting anomaly (a large quantity of tag signatures corresponding to a small number of tags appear at different locations) could easily be detected and isolated at a low cost.

IV. Evaluation

In this section, we present the evaluation model and results. We evaluate the performance of pill-level UCR tags in terms of uniqueness and reliability. We also discuss how to improve the detection accuracy using machine learning algorithms. Lastly, we analyze the resilience of pill-level UCR system to the potential attacks.

A. Evaluation Model

We use CST Microwave Studio 2015 as our simulation platform. Figure 4 illustrates the simulation setup. The proposed pill-level UCR tag consists of two parts: (i) 12 concentric ring slot resonators integrated on the external surface of each plastic cavity or pocket of blister pack that packages pharmaceutical tablets; and (ii) nontoxic silver particles of random quantity with random diameters filled in random places of each pharmaceutical tablet. The metallic pattern is made of pure copper. Circularly polarized plane wave is used to stimulate the pill-level UCR tag. The radio cross-section (RCS) probe is placed 50 mm away from the tag to detect the backscattered signal. Table II summarizes the simulation parameters. Substrate thickness and air gaps conform to normal distributions with design values as the mean values and tolerances as the triples of standard deviations. Quantity and diameters of silver particles conform to discrete uniform distribution and continuous uniform distribution respectively. We randomly distribute the silver particles inside the tablet. The frequency band used by pill-level UCR tags ranges from 7 GHz to 23 GHz.

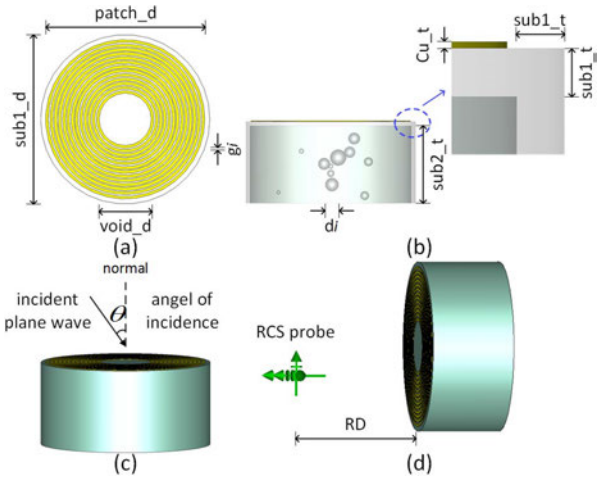

Fig. 4: Simulation setup: (a) top view of pill-level UCR tag and its dimensions, (b) side view of pill-level UCR tag and its dimensions, (c) angle of incidence, and (d) distance between RCS probe and pill-level UCR tag.

TABLE II: Simulation parameters. $N(\mu, \sigma)$ represents a normal distribution. U{a,b} represents a discrete uniform distribution. U(a,b) represents a continuous uniform distribution. Substrate I and II are plastic film and pharmaceutical tablet respectively.

Variable	Parameter	Value
$sub1\_d$	Substrate I diameter	10 mm
$patch\_d$	Patch diameter	9.4 mm
$void\_d$	Central void diameter	3.1 mm
g_i	Air gap i (i=1,...,12)	N(0.1mm, 0.0169mm)
Cu_t	Copper thickness	0.035 mm
$sub1\_t$	Substrate I thickness	0.25 mm
$sub2\_t$	Substrate II thickness	N(5mm, 0.1667mm)
ε_r^1	Substrate I dielectric constant	2.8
ε_r^2	Substrate II dielectric constant	2.42
n_p	Number of particles	U{0, 20}
d_i	Particle i diameter (i=1,...,n_p)	U(0.2mm, 1mm)
RD	Reading distance	50 mm

B. Euclidean Distance Based Tag Recognition

In this subsection, we analyze the effectiveness of Euclidean distance based tag recognition in the presence of environmental noise and with varying angles of plane wave incidence. 20 tag samples conforming to the constraints depicted in Table II were generated using pseudo random number generators. Every sample was measured 5 times at different conditions (i.e., different noise sources, varying angles of plane wave incidence, etc.). Figure 5(a) illustrates the inter-tag and intra-tag Euclidean distance distributions of pill-level UCR tags in the presence of random white Gaussian noise (WGN) with a signal-to-noise ratio (SNR) of 20 dB. 20 dB is usually recommended as the minimum SNR for a good RF deployment of the wireless local area network (WLAN) [22]. The margin between minimum inter-tag Euclidean distance and maximum intra-tag Euclidean distance reaches approximately 103.6 MHz. Figure 5(b) shows the inter-tag and intra-tag Euclidean distance distributions of pill-level UCR tags when the angle of incident plane wave (see Figure 4(c)) varies from 0° to 20°. The margin between minimum inter-tag Euclidean distance and maximum intra-tag Euclidean distance reaches approximately 110.5 MHz. In order to achieve high accuracy of tag recognition, the varying angle of incident plane wave should be not larger than 20°. Simulation result demonstrates that the Euclidean distances between signatures of pill-level UCR tags are effective at differentiating each other.

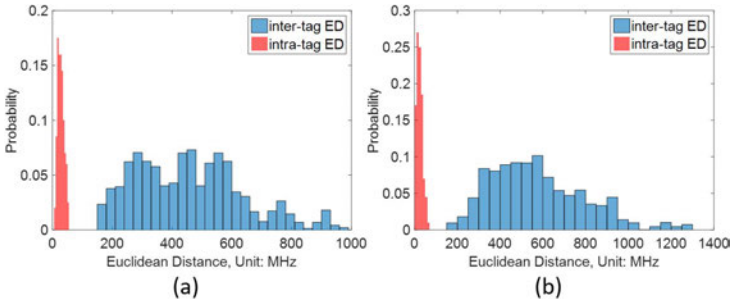

Fig. 5: (a) Euclidean distance distributions of pill-level UCR tags in the presence of WGN with a SNR of 20 dB and (b) Euclidean distance distributions of pill-level UCR tags when angle of plane wave incidence varies from 0° to 20°.

C. Machine Learning Based Tag Recognition

TABLE III: Unsupervised recognition performance comparison

Classification Technique	Recognition Rate
Lorentzian Distance	95.56%
Manhattan Distance	92.65%
Normalized Correlation Coefficient	92.65%
Wavelet Transform Manhattan Distance	98.67%

Next, the effectiveness of using pill-level UCR tags as a means of verification are further strengthened through the use of supervised and unsupervised machine learning techniques. The resonance points in the frequency response spectrum of each pill-level UCR tag are taken as features and used in an unsupervised method for classification/verification. This process simply involves using a valley detection algorithm to detect the resonance points, which appear as local minima in the spectrum bandwidth of 9-21 GHz, and computing the minimum distance or highest similarity with a tag already enrolled in the database. In order to holistically evaluate the usefulness of such an unsupervised classification methodology, the tags are evaluated by selecting a group of tags from a set of measurements to serve as the gallery (enrolled) set and then use the remaining tags to serve as the probe (verification) set. The performance is evaluated in this manner so each measurement group serves as a gallery at least once and as probe the rest of the time. For example, in terms of the data set (15 tags, 15 measurements for each tag) this will result in a total of 3,375 classification attempts for all the tags. Furthermore, three different distance/similarity measures (i.e., Lorentzian distance, Manhattan distance, and normalized correlation coefficient) were used to evaluate the robustness of this technique given that different measures have different advantages. Lastly, Manhattan distance was used again but in conjunction with

the Haar wavelet transform at scale values of 1 to 8. The sum of the diagonals across the resultant distance matrix is used to determine similarity between the tags and the minimum diagonal distance sum represents the correct tag identification. The results for these different unsupervised classification methods are shown in Table III. These results clearly demonstrate that the tags can be effectively identified at a high rate via unsupervised methods. All the scores are above 90% which means that out of the 3,375 classification attempts there were more than 3,037 correct identifications.

By combining the already unique properties of each tag with a powerful supervised classifier in LDA, the system can further improve upon its discriminatory power. This classifier takes the already rich spectrum of each tag and instead of focusing only on a small bit of spectrum information, such as their resonance points, it looks at the most discriminating features of each tag's entire spectrum. However, it is important to note that since each tag spectrum has such a high amount of sampling points, 8000 in the simulations, using the entire spectrum for the classifier would be impractical. Therefore, PCA is applied to the spectra prior to training and classification for dimensionality reduction. Then the resultant signals are used for training the classifier and then testing as well. In order to evaluate the supervised learning approach as holistically as the unsupervised approaches, the LDA classifier went through cross-validation comparing the performance based on different partitions of data used for computing the principal components and different partitions used for training the classifier after PCA. The performance surface in Figure 6 visually shows the results of the cross-validation process for these simulated measurements, where the triple (xT, yM, zS) represents the data set of x tags-y measurements for each tag-z sampling points for each measurement. The figure shows that as long as the classifier is trained on more than 2 sets of measurements, regardless of the amount of data used for computing the principal components, it will outperform almost all of the unsupervised techniques since nearly all of the scores in the upper region are near 100% recognition.

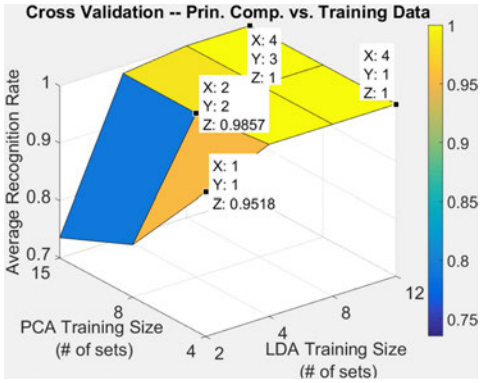

Fig. 6: Overall recognition performance for (15T, 15M, 8000S).

Furthermore, these results emphasize that the unique properties of pill-level UCR tags in conjunction with either supervised or unsupervised learning techniques would make a strong verification system for the pharmaceutical supply chain.

D. Attack Analysis

In this subsection, we analyze the resilience of pill-level UCR system to the potential attacks. Pill-level UCR system is resistant to cloning attack since the adversaries cannot easily model the uncontrollable process variations during tag fabrication. Pill-level UCR system is resistant to split attacks (i.e., separating tag from product, swapping tags, etc.) since it establishes an inseparable connection between tag and identified object. Even if the adversaries could swap the copper patterns on the external surfaces of different plastic cavities or pockets, they cannot simultaneously swap the silver particles embedded in the tablets without changing their initial positions and compromising the tablets. By binding the signatures of different tablets within the same blister pack, pill-level UCR system is resistant to illegal tablet replacement. Pill-level UCR system is intrinsically resistant to DoS attack performed in the form of overwriting tag memory since tag memory has been eliminated from the pill-level UCR tag. As discussed in Subsection III-C, our proposed split manufacturing approach makes it much more difficult for the adversaries to perform replay attack.

V. Conclusion

In this paper, we presented a new split manufacturing based pill-level unclonable chipless RFID (pill-level UCR) tag that intrinsically generates a unique ID from multiple entropy sources. The performance of pill-level UCR tags has been verified via simulations with random white Gaussian noise and varying angles of plane wave incidence. Compared with existing approaches, pill-level UCR system has the following merits: (1) The ID generated from pill-level UCR tag is unique and unclonable since it stems from random and uncontrollable process variations during tag manufacturing. Multiple entropy sources (i.e., manufacturing variations of slot resonators, randomnesses of silver particles, etc.) contribute to the uniqueness of pill-level UCR tag and enlarge the margin between inter-tag and intra-tag signature distributions. (2) Pill-level UCR system builds up an inseparable connection between tag and identified pharmaceutical product, and thus is resistant to split attacks. (3) Pill-level UCR system enables pill-level traceability by making each pharmaceutical tablet have its own unique signature. The signatures of all tablets within the same blister pack are bound together to add one more layer of security to be resistant to illegal tablet replacement.

References

[1] Victoria White. US pharmaceutical market value will approach $550 billion by 2020, says GlobalData, March 2015.
[2] World Heath Organization. Guidelines for the development of measures to combat counterfeit drug, 1999.
[3] Felix Gillette. Inside pfizers fight against counterfeit drugs, January 2013.
[4] Paul Toscano. The dangerous world of counterfeit prescription drugs, October 2011.
[5] Don Hsieh. Pharmaceutical supply chain security best practices, October 2014.
[6] John Fredy Barrera, Alejandro Mira-Agudelo, and Roberto Torroba. Experimental QR code optical encryption: noise-free data recovering. *Optics letters*, 39(10):3074–3077, 2014.
[7] Pim Tuyls and Lejla Batina. RFID-tags for anti-counterfeiting. In *Cryptographers' Track at the RSA Conference*, pages 115–131. Springer, 2006.
[8] Christof Paar. New directions in lightweight cryptographic primitives for RFID applications. In *Presentation at RFID CUSP Workshop*, 2008.
[9] Yong Lee and Ingrid Verbauwhede. Secure and low-cost RFID authentication protocols. In *2nd IEEE International Workshop on Adaptive Wireless Networks (AWiN 2005)*, pages 1–5. IEEE, 2005.
[10] Charles Wankel. *21st century management: a reference handbook*. Sage Publications, 2007.
[11] Stevan Preradovic and Nemai Chandra Karmakar. Chipless RFID: Bar code of the future. *IEEE microwave magazine*, 11(7):87–97, 2010.
[12] Stevan Preradovic, Isaac Balbin, Nemai Chandra Karmakar, and Gerhard F Swiegers. Multiresonator-based chipless RFID system for low-cost item tracking. *IEEE Transactions on Microwave Theory and Techniques*, 57(5):1411–1419, 2009.
[13] Stevan Preradovic and Nemai Chandra Karmakar. Chipless RFID tag. In *Multiresonator-Based Chipless RFID*, pages 77–94. Springer, 2012.
[14] Kun Yang, Domenic Forte, and Mark M Tehranipoor. UCR: An unclonable chipless RFID tag. In *Hardware Oriented Security and Trust (HOST), 2016 IEEE International Symposium on*, pages 7–12. IEEE, 2016.
[15] Ulrich Rührmair, Srinivas Devadas, and Farinaz Koushanfar. Security based on physical unclonability and disorder. In *Introduction to Hardware Security and Trust*, pages 65–102. Springer, 2012.
[16] S Härmä, VP Plessky, CS Hartmann, and W Steichen. SAW RFID tag with reduced size. In *2006 IEEE Ultrasonics Symp*, pages 2389–2392, 2006.
[17] Stevan Preradovic and Nemai C Karmakar. Design of fully printable planar chipless RFID transponder with 35-bit data capacity. In *Microwave Conference, 2009. EuMC 2009. European*, pages 013–016. IEEE, 2009.
[18] Silvers valence is + not ++ and therefore it does not oxidize into a toxic form.
[19] Alan Julian Izenman. Linear discriminant analysis. In *Modern multivariate statistical techniques*, pages 237–280. Springer, 2013.
[20] Jonathon Shlens. A tutorial on principal component analysis. *arXiv preprint arXiv:1404.1100*, 2014.
[21] Mark M Schmissrauter. Tamper evident packaging and method, May 24, 1988. US Patent 4,746,052.
[22] Cisco. Radio frequency fundamentals, September 2014.