# UCR: An Unclonable Chipless RFID Tag

**Kun Yang, Domenic Forte, and Mark M. Tehranipoor**

ECE Department, University of Florida
{k.yang}@ufl.edu, {dforte, tehranipoor}@ece.ufl.edu

***Abstract*—While Radio Frequency Identification (RFID) has become popular for commodity and asset tracking and management, the relatively higher price of RFID tags limits its application in the supply chain of low-cost commodities. Recently, cost-effective chipless RFID tags that do not contain a microchip in the transponder have been gaining more attention from industry, academia, and government. Existing chipless RFID tags require removing or shorting of some resonators (i.e., spirals or patch slots) on the substrate to encode data, but this incurs a waste of tag area and increases the manufacturing time/cost of chipless RFID tags. In addition, the identifiers (IDs) generated by existing chipless RFID tags are small, deterministic, and clonable. To mitigate these shortcomings, we propose a new unclonable chipless RFID (UCR) tag that intrinsically generates a unique ID from manufacturing variations. UCR tag consists of a certain number of concentric ring slot resonators, whose resonance frequencies depend on slot parameters and substrate dielectric constant that are sensitive to manufacturing variations. The area of UCR tag is as small as regular quick response (QR) code. Simulation results based on CST Microwave Studio 2015 have verified the effectiveness and reliability of UCR tags. The non-overlapping margin between intra-tag and inter-tag Euclidian distance distributions reaches approximately 50 MHz in the presence of random white Gaussian noise (WGN) with a signal-to-noise ratio (SNR) of 10 dB.**

***Index Terms*—Radio Frequency Identification (RFID), Chipless RFID Tag, Uniqueness, Unclonability**

## I. Introduction

Today's supply chain is highly complex, diverse, and extensive. While globalization has optimized resource allocation and reduced manufacturing cost, it also exposes the supply chain to more risks such as counterfeiting, theft, etc. Not only do these risks compromise the profits and reputations of manufacturers, distributors, and retailers, but they also pose a threat to human and asset safety. In 2014, over twenty thousand Intellectual Property Rights (IPR) infringing seizures were reported with a total value of $1.22 billion [1]. In the same year, FreightWatch International recorded 794 cargo thefts throughout the United States, with the average loss of $232,924 per incident [2]. Track-and-trace techniques form the foundation for an improved supply chain by providing manufacturers, distributors, and retailers with a systematic method to detect and control counterfeiting, theft, etc., but existing approaches are too expensive, inconvenient, unreliable, or insecure.

Traditionally, barcodes have been used to track and trace commodities in the supply chain [3]. Quick response (QR) codes which can include much more information have also been put into use more recently [4]. QR codes can be encrypted to prevent unauthorized access [5], [6]. The authors in [7] proposed to implement secure and noise-free information retrieval from QR codes by combining the optical double random phase encoding (DRPE) encrypting technique with the QR coding to eliminate the noise in the recovered information. However, both barcodes and QR codes are very easy to duplicate because of visibility and controllability of pixel information (even though adversaries cannot recover the actual content from encrypted QR codes). Other shortcomings (e.g., requirement of individual scanning, direct line-of-sight, close proximity to reader, etc.) severely impact their overall utility.

RFID 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 [8]. Compared with barcodes and QR codes, an RFID-based scheme has much more attractive features – support batch scanning, do not require direct line-of-sight for access, and need less human involvement to collect data – making automatic track and trace possible. A series of encryption techniques (e.g., advanced encryption standard (AES), public-key cryptography, elliptic curve cryptography (ECC), etc.) have been proposed for RFID tags to enhance their security and privacy [9]–[11]. The authors in [12], [13] proposed to replace cryptography with ultra wideband (UWB) modulation in secure RFID. Physical unclonable functions (PUFs) have also been proposed to be embedded into RFID tags for anti-counterfeiting and secure applications [14], [15]. An ideal PUF produces a unique and reliable response when issued a challenge. PUFs are more secure than conventional identity storage since they exploit the uncontrollable process variations associated with modern integrated circuit (IC) fabrication [16]. However, relatively higher price of RFID tag limits its application in the supply chain of low-cost commodities.

Recently, cost-effective chipless RFID tags [17]–[19] that do not contain a microchip in the transponder have attracted more and more attention from industry, academia, and government. Compared with conventional IC based RFID tags, chipless RFID tags have the following merits: (i) extremely low price (as low as 0.1 cents) enables their application in the supply chain of low-cost commodities; (ii) elimination of tag memory releases them from the threat of denial-of-service attack performed in the form of overwriting tag memory; (iii) chipless RFID tags have the potential to be directly printed on the products or their packages with conductive ink. Existing chipless RFID tags, however, require either removing or shorting some resonators (i.e., spirals or patch slots) on the substrate to encode data [17], [18]. When one resonator is removed or shorted, the resonance point associated with that resonator will be either removed from the spectrum or shifted outside of the frequency band of interest. One bit is encoded to '1' when the corresponding resonance point exists at a specific frequency, and '0' when the resonance point disappears, or vice versa. Removal of resonators will incur a waste of tag area. Shorting resonators ensures the same layout with all the resonators shorted can be used to produce different chipless RFID tags. When encoding data, the shorting can be removed using laser cutting or conventional etching techniques. Both removing and shorting resonators will increase the manufacturing time/cost of chipless RFID tags. For same designs, the IDs generated by present chipless RFID tags are deterministic and predictable. As a result, they are very easy to clone. Other shortcomings such as small ID size (usually not exceeding 35 bits) and large tag area also limit their utility.

To mitigate the above-mentioned drawbacks of existing solutions and build up the trustworthy visibility into supply chain status, we propose a novel unclonable chipless RFID (UCR) tag. We take advantage of the uncontrollable process variations during tag fabrication to generate a unique and unclonable ID that can be used for tracking and tracing commodities (e.g., food, pharmaceuticals, newspapers, magazines, etc.) in the supply chain. In addition to enhancing supply chain management, UCR tags can also be implanted into passports and driving licenses to help verify the identities of citizens. Furthermore, UCR tag has the potential to expand the scope of the Internet of Things (IoT) by enabling many non-electronic products to be connected to the network. UCR tag consists of a certain number of concentric ring slot resonators, whose resonance frequencies depend on slot parameters and substrate dielectric constant that are sensitive to manufacturing variations. A set of resonance frequencies sensitive to manufacturing variations will be captured and used as the unique ID of each UCR tag. To the best of our knowledge, this is the first time that manufacturing variations have been used to generate the unique ID from chipless RFID tag. The area of our proposed UCR tag is as small as regular QR code. To summarize, we make the following contributions:

- We theoretically analyze the sensitivity of slot resonance frequency towards the variances of slot parameters and take advantage of this sensitivity to develop a new type of unclonable chipless RFID tags that carry unique IDs.
- We propose a novel and efficient look-up method that speeds up the authentication process of UCR tags.
- We evaluate the performance of UCR tags under extremely adverse environmental conditions (i.e., noisy environment, varying angles of plane wave incidence, etc.). Specifically, we analyze the reliability of

UCR tags against random WGN with a SNR of 10 dB and varying angles of plane wave incidence from 0° to 30°.

The remainder of this paper is organized as follows: Section II introduces the related work. Section III discusses the preliminaries needed for developing chipless RFID tags. Section IV describes the proposed UCR tags in detail and how they can provide unique and unclonable IDs. In Section V, we evaluate the performance of UCR tags. Finally, we conclude in Section VI.

## II. Related Work

Chipless RFID tags can be divided into three categories: (i) time-domain reflectometry (TDR) based chipless tags; (ii) spectral signature based chipless tags; and (iii) amplitude/phase backscatter modulation based chipless tags [20]. Due to the page limit, we review only closely related spectral signature based chipless tags.

The authors in  [17], [18] designed a fully passive printable chipless RFID tag by placing multiple spiral resonators close to the microstrip that connects two cross-polarized UWB monopole antennas (one transmitter and one receiver). Spiral resonators with different dimensions will exhibit different resonance frequencies. Data encoding is implemented by either removing the spiral or shorting its turns. Future printing techniques will preserve the layout with all of the spirals shorted and when encoding data the shorting can be removed using laser cutting or conventional etching techniques. The bit width of chipless RFID implemented in this approach will correspond to the number of spiral resonators exploited. As a result, the tag area will be proportional to the bit width of chipless RFID, which is undesirable.

Closest to our work is the slot-loaded dual-polarized chipless RFID tag proposed in [19], where four rectangular metallic patches loaded with multiple slot resonators are used to compose the tag. The logic state of a bit is changed simply by shorting the slot at the corner point, which will take the resonance frequencies of the slots out of the frequency band of interest. To reduce the mutual coupling between the slots, slots with the same polarization for adjacent frequencies are placed alternatively into two patches. To double the number of bits within the same frequency bandwidth, two similar sets are placed in horizontal and vertical polarizations. Since multiple slots can be placed into the same patch, the tag area is significantly smaller than the above-mentioned spiral resonator based tag. One shortcoming of this technique is that the cross-polar response will be too small to recognize if the tag is rotated by an angle larger than a certain limit.

Removing or shorting the resonator (i.e., spiral or patch slot) is necessary for both techniques to change the logic state of the corresponding bit. The manufacturing cost will be unacceptable if different layouts with different resonator shorting states are employed to fabricate the tags. Although the layout can be preserved with all of the resonators shorted and when encoding data the shorting can be removed using either laser cutting or etching techniques, the manufacturing time will be dramatically increased. For a design with specific parameters, the IDs generated in both ways are deterministic and repeatable, which makes these chipless RFID tags very easy to clone.

To overcome the shortcomings of prior work, we develop a new type of unclonable chipless RFID tags by exploiting the uncontrollable process variations during tag fabrication.

## III. Preliminary

In this section, we first review the impact factors of a slot resonator's notch frequency. Next, we compare different slot shapes and choose the most appropriate one as the element of our proposed UCR tag.

### A. Notch Frequency

Figure 1 illustrates the cross-section view of a slot line with labeled geometric parameters. The normalized wavelength of a slot line with air gap $g$, substrate thickness $t$, and relative permittivity of substrate material $\varepsilon_r$ can be approximately computed as [21]

$$\lambda_s/\lambda_0 = F(g,t,\varepsilon_r) - G(\varepsilon_r)\cdot\ln(t/\lambda_0) \tag{1}$$

where

$$F(g,t,\varepsilon_r) = 1.045 - 0.365\ln\varepsilon_r + \frac{0.063g\varepsilon_r^{0.945}}{g+2.3864t} \tag{2}$$

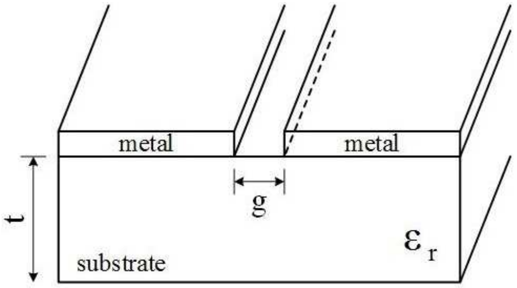


Figure 1: Cross-section view of slot line.

and

$$G(\varepsilon_r) = 0.0599 - \frac{0.083695}{\varepsilon_r} \tag{3}$$

$\lambda_s$ and $\lambda_0$ indicate the slot guided wavelength and the free space wavelength, respectively. Equation 1 holds for $2.22 \leq \varepsilon_r \leq 3.8$, $0.0015 \leq g/\lambda_0 \leq 0.075$ and $0.006 \leq t/\lambda_0 \leq 0.06$. For the frequency band (4 to 10 GHz) of interest, these conditions correspond to an air gap between 0.1125 and 2.25 mm and a substrate thickness between 0.45 and 1.8 mm. The slot length $L$ of a half-wavelength slot-line resonator should conform to the following equation:

$$L = \lambda_s/2 \tag{4}$$

The free space wavelength can be computed as

$$\lambda_0 = c/f_s \tag{5}$$

where $c$ and $f_s$ respectively refer to the speed of light in vacuum and the notch frequency of slot-line resonator. By combining Equations 1, 4 and 5, we can easily derive the following iterative equation solvable for notch frequency of slot-line resonator:

$$f_s = \frac{c}{t}exp\left(\frac{cF-2Lf_s}{cG}\right) \tag{6}$$

Next, we analyze the sensitivity of slot resonance frequency towards the variances of slot parameters (i.e., air gap, substrate thickness, and relative permittivity of substrate material, etc.). Note that we use notch frequency and slot resonance frequency interchangeably in this paper. From Equation 6 we can compute the partial derivatives of notch frequency as

$$\frac{\partial f_s}{\partial g} = \frac{c\Phi\frac{\partial F}{\partial g}}{tG+2L\Phi} \tag{7}$$

$$\frac{\partial f_s}{\partial t} = \frac{cG\Phi\frac{\partial F}{\partial t} - Gf_s}{tG+2L\Phi} \tag{8}$$

$$\frac{\partial f_s}{\partial \varepsilon_r} = \frac{\Phi\left[cG\frac{\partial F}{\partial \varepsilon_r} + (2Lf_s - cF)\frac{\partial G}{\partial \varepsilon_r}\right]}{tG^2+2LG\Phi} \tag{9}$$

where

$$\Phi = exp\left(\frac{cF-2Lf_s}{cG}\right) \tag{10}$$

From Equations 2 and 3 we can compute the partial derivatives of $F$ and $G$ as

$$\frac{\partial F}{\partial g} = \frac{0.1503432t\varepsilon_r^{0.945}}{(g+2.3864t)^2} \tag{11}$$

$$\frac{\partial F}{\partial t} = -\frac{0.1503432g\varepsilon_r^{0.945}}{(g+2.3864t)^2} \tag{12}$$

$$\frac{\partial F}{\partial \varepsilon_r} = -\frac{0.365}{\varepsilon_r} + \frac{0.059535g\varepsilon_r^{-0.055}}{g+2.3864t} \tag{13}$$

$$\frac{\partial G}{\partial \varepsilon_r} = \frac{0.083695}{\varepsilon_r^2} \tag{14}$$

Figure 2 demonstrates the theoretically computed sensitivity of notch frequency to the variances of slot parameters at different frequencies. We limit the analysis to the UWB with a frequency range from 3.1 to 10.6

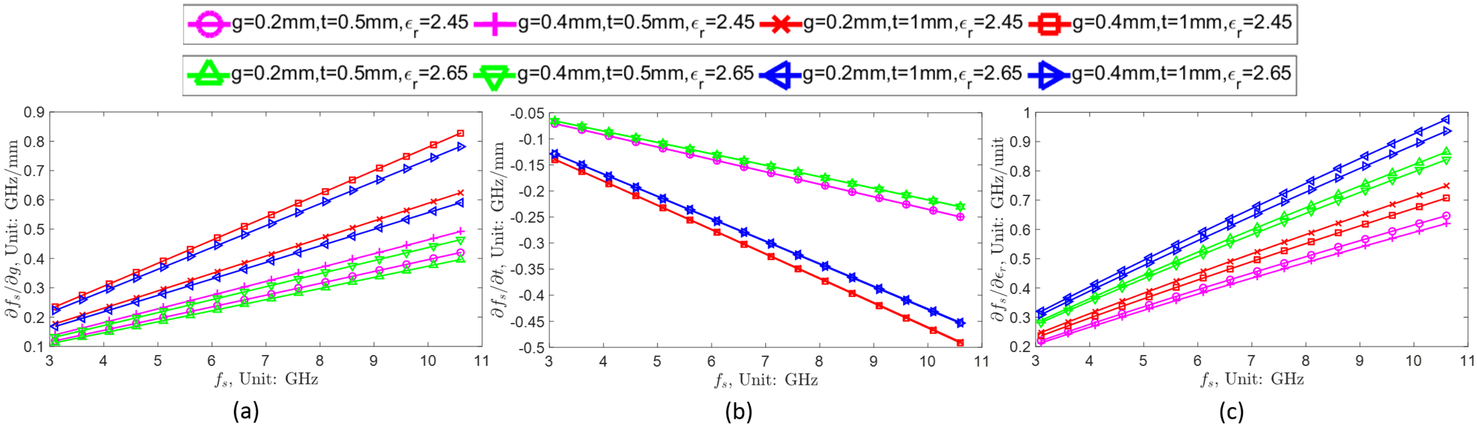


Figure 2: Sensitivity of notch frequency to slot parameters at different frequencies: (a) sensitivity to air gap, (b) sensitivity to substrate thickness, and (c) sensitivity to relative permittivity.

GHz. All the three notch frequency sensitivities (i.e., $\frac{\partial f_s}{\partial g}$, $\frac{\partial f_s}{\partial t}$, and $\frac{\partial f_s}{\partial \varepsilon_r}$) appear linear to the variance of notch frequency in the frequency range of UWB. It is observed that air gap has little impact on the sensitivity of notch frequency to the variance of substrate thickness. The curves of $\frac{\partial f_s}{\partial t}$ with the same substrate thickness and relative permittivity of substrate material but different air gaps are overlapping with each other.

### B. *Slot Shape*

Figure 3 illustrates five common shapes of slot resonators. Note that there are many other slot resonator geometries. Different slot resonator geometries correspond to different equivalent circuits with different resonance characteristics. We limit ourselves to these five shapes for brevity. Circular ring shaped slot resonators will be employed to compose our proposed UCR tag due to the following two reasons:

- Circular ring shaped slot resonator does not require the incident plane wave to be in perfect alignment with the chipless RFID tag. As illustrated in Figure 4(a), if the angle ($\theta$) between the slot direction ($\vec{v}$) and the linear polarization direction ($\vec{e}$) of incident plane wave is larger than a certain limit, the backscattered response from the U-shaped slot resonator will be too weak to be captured. This results from the fact that most components of incident plane wave will serve to stimulate the horizontal slot rather than the vertical slot. As a result, another resonance point will appear at a frequency larger than 9 GHz as shown in Figure 4(a). In contrast, the backscattered response from the circular ring slot resonator will be the same no matter how large an angle the tag is rotated by, as shown in Figure 4(b). Note that we limit ourselves to the comparison between U-shaped and circular ring shaped slot resonators due to the page limit but slot resonators with shapes of (a), (c) and (d) have similar limitations as U-shaped slot resonator.
- The fabrication accuracy of circular ring shaped slot's geometric parameters is harder to control than slots with other shapes, which is conducive to obtaining larger variations during manufacturing. This will result in larger variation in the signatures of chipless RFID tags, making them more suitable as unique identifiers.

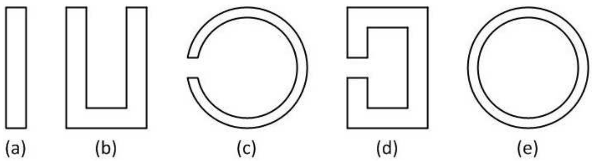


Figure 3: Slot resonator geometries: (a) I-shaped, (b) U-shaped, (c) C-shaped, (d) split square shaped, and (e) circular ring shaped.

## IV. Unclonable Chipless RFID (UCR) Tag

The proposed UCR system is presented in this section. We first describe the architecture and working principle of UCR system, and then introduce a novel and efficient look-up method that could be used at the authentication phase to quickly determine whether the tag under authentication (TUA) belongs to the database.

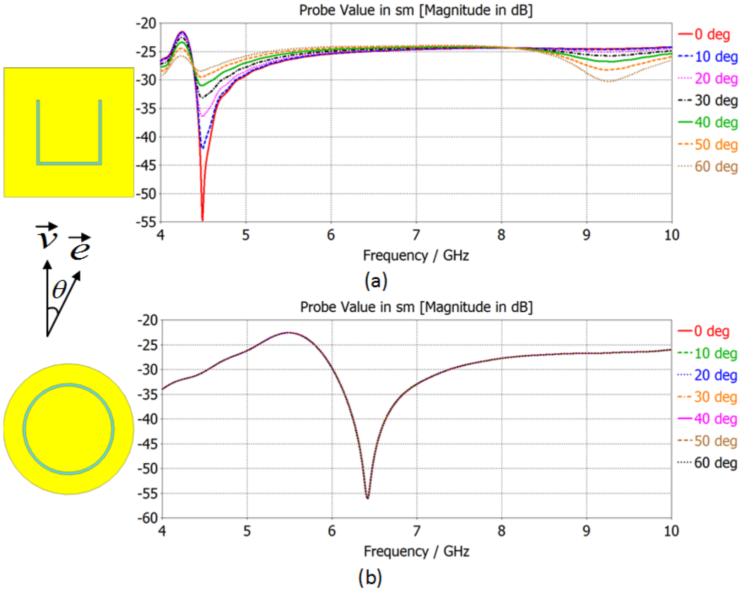


Figure 4: Resonator responses at different angles between slot direction and polarization direction of incident plane wave: (a) U-shaped slot resonator and (b) circular ring shaped slot resonator.

### A. *Architecture and Working Principle*

Figure 5 shows the proposed UCR tag that consists of a certain number of concentric ring slot resonators placed on a certain substrate (e.g., TACONIC TLX-0). When we stimulate the UCR tag with an UWB plane wave, as illustrated in Figure 6, the number of fundamental resonance points in the frequency response spectrum will correspond to the number of slot resonators. A typical UWB RFID reader will be responsible for providing the UWB plane wave and capturing the frequency response spectrum. These resonance points are independent of each other. Due to process variations during tag fabrication, the slot parameters (i.e., trace width, air gap, substrate thickness, and substrate material dielectric constant) of each resonator will shift away from their design values. Note that we use relative permittivity and dielectric constant interchangeably in this paper. Table I illustrates the manufacturing tolerances of five major printed circuit board (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 %. Table II shows the dielectric constant tolerances ($\varepsilon_r$) of six typical high frequency laminates. The dielectric constant tolerances

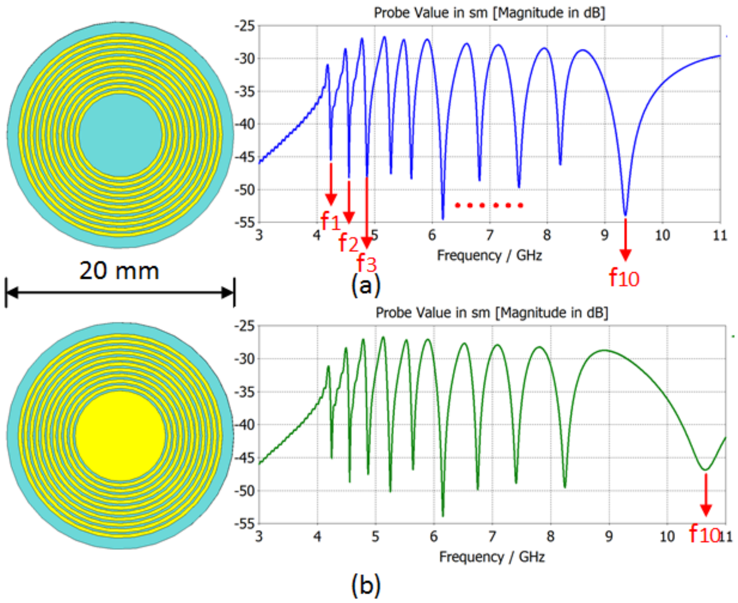


Figure 5: UCR tag that consists of concentric ring slot resonators: (a) central void and (b) central filled.

can range from 1.33 % to 3.49 %. According to the analysis in Section III (see Equations 7, 8, 9 and Figure 2), the resonance frequency of each slot resonator will shift away from its design value due to the variances of slot parameters. Because of the randomness of process variation, the frequency signature of each UCR tag will be unique and different from each other. The vector $(f_1, f_2, ..., f_N)$ will be used as the identifier of each tag, where $f_i$ indicates the resonance frequency of the $i_{th}$ slot resonator. The proposed UCR tag is unclonable since the adversaries cannot easily model the uncontrollable process variations during tag fabrication. For a UCR tag with 10 slot resonators, its diameter will be 20 mm, which is similar to the dimension of QR code. As shown in Figure 5, the central circular pad should be removed from the UCR tag; otherwise the last resonance point will shift far away from the other resonance points, probably outside the UWB frequency range, and its valley point will be flattened, which will reduce the accuracy of measurement.

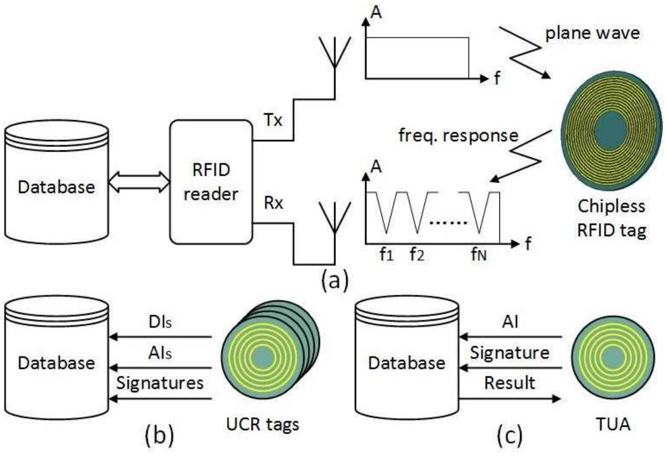


Figure 6: UCR system: (a) working principle, (b) enrollment, and (c) authentication.

Because of noise interference and angle variation of incident plane wave, the signatures captured from the same tag may be slightly different at different times. Euclidean distance between two vectors $\vec{v_i}^j = (f_1^j, f_2^j, ..., f_N^j)$ and $\vec{v_i}^k = (f_1^k, f_2^k, ..., f_N^k)$ will be used to determine whether these two vectors belong to the same tag, where $\vec{v_i}^j$ and $\vec{v_i}^k$ denote the signatures of the $i_{th}$ tag obtained at times $j$ and $k$. The Euclidean distance (ED) between $\vec{v_i}^j$ and $\vec{v_i}^k$ can be computed as follows:

Table I: PCB manufacturing tolerances

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

Table II: PCB laminate $\varepsilon_r$ tolerances

| Supplier | Laminate | $\varepsilon_r$ | $\varepsilon_r$ Tolerance |
|---|---|---|---|
| TACONIC | RF-30 | 3.00 | +/- 0.10 |
| TACONIC | TRF-43 | 4.30 | +/- 0.15 |
| TACONIC | TLX-0 | 2.45 | +/- 0.04 |
| ROGERS | RO3003 | 3.00 | +/- 0.04 |
| ROGERS | RO4350B | 3.48 | +/- 0.05 |
| ROGERS | RT/Duroid 6006 | 6.15 | +/- 0.15 |

$$ED_i^{j,k} = |\vec{v_i}^j - \vec{v_i}^k| = \sqrt{\sum_{r=1}^{N} (f_r^j - f_r^k)^2} \tag{15}$$

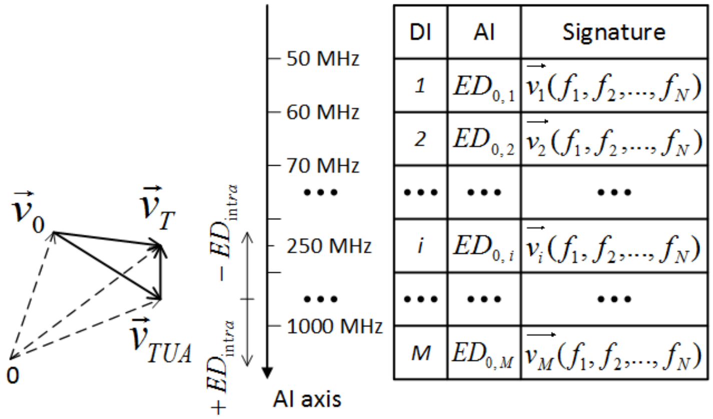
Two signatures are determined to belong to the same tag if their Euclidean distance is not larger than the maximum intra-tag Euclidean distance obtained at the enrollment phase.

### *B. Look-up Method*

Figure 6 shows the framework of UCR system. During the ***enrollment phase***, the signatures of all UCR tags $(\vec{v}_1, \vec{v}_2, ..., \vec{v}_M)$ are measured by the manufacturer. The Euclidean distance $(ED_{0,i})$ between the signature of design value $(\vec{v}_0)$ and the signature of each tag (e.g., $\vec{v}_i$) will be computed and used as the analog index (AI) to look up that tag in the database. All the AIs will be sorted and a corresponding digital index (DI) will be assigned to each tag. All the signatures of UCR tags will be appended to their DIs and AIs and stored in the look-up table as shown in Figure 7. During the ***authentication phase***, we first calculate the Euclidean distance $(ED_{0,TUA})$ between the signature of design value $(\vec{v}_0)$ and the signature of TUA $(\vec{v}_{TUA})$. $ED_{0,TUA}$ will be used to locate TUA on the AI axis as shown in Figure 7. Afterwards, we compare the signature of TUA with its nearest neighbor (i.e., Tag $DI(k)$ satisfying the condition that $|ED_{0,TUA} - ED_{0,DI(k)}|$ is the smallest) on the AI axis. This procedure will automatically terminate if the signature of TUA matches with its $k_{th}$ nearest neighbor; otherwise we move on to its $(k+1)_{th}$ nearest neighbor. This procedure will also terminate if the shift value of TUA on the AI axis has exceeded the maximum intra-tag Euclidean distance $(ED_{intra})$, in which case we determine that TUA does not belong to the database. If the tag record $(\vec{v}_T)$ that matches with TUA exists, there is no chance for us to miss it because of the following triangle inequality:

$$|\,|\vec{v}_T - \vec{v}_0| - |\vec{v}_{TUA} - \vec{v}_0|\,| \leq |\vec{v}_T - \vec{v}_{TUA}| \leq ED_{intra} \tag{16}$$

In other words, the AI distance (i.e., the distance on the AI axis) between TUA and possibly existing target tag, whose signature is $\vec{v}_T$, should not be larger than $ED_{intra}$. The procedure of UCR tag authentication is described in Algorithm 1. Note that there will be only one tag satisfying the condition $|\vec{v}_{TUA} - \vec{v}_{DI(k)}| \leq ED_{intra}$, which is the target tag if it exists, so long as there is no overlapping between inter-tag and intra-tag Euclidean distance distributions. Admittedly, when the number of UCR tags is extremely large, it is possible that inter-tag and intra-tag Euclidean distance distributions will overlap with each other, in which case multiple tag records could match with TUA and the one nearest in Euclidean distance to TUA will be selected. This problem can also be overcome by increasing the feature space (i.e., the number of resonance points in the frequency spectrum) of UCR tags. Compared with exhaustive search, we significantly reduce the look-up time.



| DI | AI | Signature |
|---|---|---|
| 1 | $ED_{0,1}$ | $\vec{v_1}(f_1, f_2, \ldots, f_N)$ |
| 2 | $ED_{0,2}$ | $\vec{v_2}(f_1, f_2, \ldots, f_N)$ |
| ••• | ••• | ••• |
| i | $ED_{0,i}$ | $\vec{v_i}(f_1, f_2, \ldots, f_N)$ |
| ••• | ••• | ••• |
| M | $ED_{0,M}$ | $\vec{v_M}(f_1, f_2, \ldots, f_N)$ |

Figure 7: Look-up table that stores all the signatures of valid tags.

**Algorithm 1** UCR tag authentication

```
 1: procedure AUTHENTICATE($\vec{v}_{TUA}$)
 2:     $\vec{v}_{TUA} \leftarrow$ The signature of TUA
 3:     $\vec{v}_{DI(k)} \leftarrow$ The signature of TUA's $k_{th}$ nearest neighbor on the axis, whose DI is $DI(k)$
 4:     $ED_{0,TUA} \leftarrow$ The Euclidean distance between design value and TUA
 5:     $ED_{0,DI(k)} \leftarrow$ The Euclidean distance between design value and TUA's $k_{th}$ nearest neighbor on the axis
 6:     while $|ED_{0,TUA} - ED_{0,DI(k)}| \leq ED_{intra}$ do
 7:         if $|\vec{v}_{TUA} - \vec{v}_{DI(k)}| \leq ED_{intra}$ then
 8:             printf("TUA matches with Tag %d.", $DI(k)$)
 9:             goto 15
10:         else
11:             $k \leftarrow k+1$
12:         end if
13:     end while
14:     printf("TUA does not belong to the database.")
15: end procedure
```

## V. Evaluation and Simulation Results

In this section, we present the evaluation model and results. We evaluate the performance of UCR tags in terms of uniqueness and reliability. Afterwards, we analyze the resilience of UCR system to the potential attacks.

### A. Evaluation Model

We use CST Microwave Studio 2015 as our simulation platform. Figure 8 illustrates the simulation setup. The proposed chipless RFID tag consists of 10 concentric ring slot resonators placed on the TACONIC TLX-0 substrate. The metallic pattern is made of pure copper. Circularly polarized plane wave is used to stimulate the chipless RFID tag. The radio cross-section (RCS) probe is placed 50 mm away from the tag to detect the backscattered signal. Table III summarizes the simulation parameters. Substrate thickness and dielectric constant, and air gaps conform to normal distributions with design values as the mean values and tolerances as the triples of standard deviations. The frequency band used by UCR tags ranges from 4 GHz to 10 GHz.

Table III: Simulation parameters. $N(\mu, \sigma)$ represents a normal distribution.

| Variable | Parameter | Value |
|---|---|---|
| $sub_d$ | Substrate diameter | 20 mm |
| $t$ | Substrate thickness | N(0.5mm, 0.0423mm) |
| $\varepsilon_r$ | Substrate dielectric constant | N(2.45, 0.0133) |
| $patch_d$ | Patch diameter | 18 mm |
| $h$ | Patch thickness | 0.035 mm |
| $void_d$ | Central void diameter | 7.4 mm |
| $g_i$ | Air gap i (i=1,...,10) | N(0.2mm, 0.0169mm) |

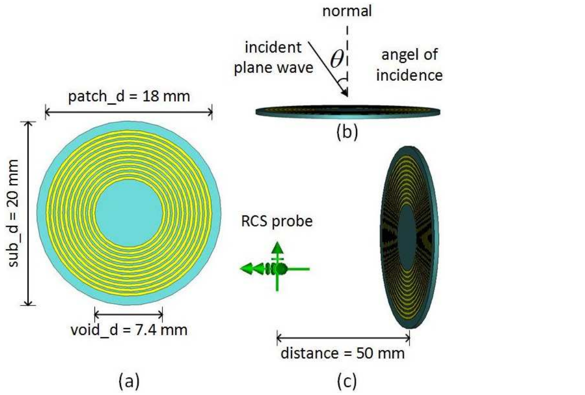


Figure 8: Simulation setup: (a) UCR tag dimensions, (b) angle of incidence, and (c) distance between RCS probe and UCR tag.

### B. Uniqueness

In order to verify the uniqueness of the proposed UCR tags, 100 samples conforming to the constraints depicted in Table III were generated using pseudo random number generators. Table IV shows the statistic standard deviation ($std(f_i)$) of each resonance frequency ($f_i$) for these 100 samples. Standard deviation ($std(f_i)/mean(f_i)$) normalized by the mean value ($mean(f_i)$) of each resonance frequency is also illustrated. It is observed that the standard deviations of resonance frequencies are large enough to differentiate each UCR tag when the tag parameters are conforming to the constraints described in Table III. Figure 9(a) illustrates the Euclidean distance distribution of UCR tags. The minimum value, mean value, and maximum value of Euclidean distances for the 100 samples are 33.2039 MHz, 180.9612 MHz, and 587.0043 MHz respectively. Simulation result demonstrates that the Euclidean distances between signatures of UCR tags are effective at differentiating each other.

### C. Reliability

In this subsection, we evaluate the reliability of UCR tags against environmental noise and varying angles of incident plane wave. 10 UCR tags were measured 10 times at different conditions. Figure 9(b) illustrates the inter-tag and intra-tag Euclidean distance distributions of UCR tags in the presence of random WGN with a SNR of 10 dB. Note that a SNR of 10 dB is a very pessimistic assumption for the RF deployment. 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 50 MHz. Figure 9(c) illustrates the Euclidean distances relative to zero incident angle for 10 tags when angle of incidence varies from $5^\circ$ to $30^\circ$. The larger the angle of incidence is, the larger the Euclidean distance relative to zero incident angle will be. Figure 9(d) shows the inter-tag and intra-tag Euclidean distance distributions of UCR tags when the angle of incident plane wave varies from $0^\circ$ to $20^\circ$. The margin between minimum inter-tag Euclidean distance and maximum intra-tag Euclidean distance reaches approximately 20 MHz. In order to achieve high accuracy of tag authentication, the varying angle of incident plane wave should be not larger than $20^\circ$. Note that when considering environmental noise and varying angles of incident plane wave, the inter-tag Euclidean distance distributions of UCR tags are a little different from the one presented in subsection B, where the inter-tag Euclidean distance distribution is obtained in an ideal condition.

### D. Attack Analysis

In this subsection, we analyze the resilience of UCR system to the potential attacks. UCR system is resistant to the cloning attack since the adversaries cannot easily model the uncontrollable process variations during tag fabrication. UCR system is intrinsically resistant to the denial-of-service attack performed in the form of overwriting tag memory since tag memory has been eliminated from the UCR system. UCR system enables the trustworthy visibility into supply chain status by providing a unique, reliable and unclonable identifier for commodity track-and-trace. Admittedly, the attackers could record the frequency response spectrum

Table IV: Standard deviations of resonance frequencies.

| | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ | $f_7$ | $f_8$ | $f_9$ | $f_{10}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| $std(f_i)$ (MHz) | 23.6045 | 24.1153 | 29.8766 | 35.0085 | 31.5511 | 43.8437 | 40.3017 | 53.3831 | 65.8381 | 72.7412 |
| $std(f_i)/mean(f_i)$ | 0.0056 | 0.0053 | 0.0061 | 0.0066 | 0.0056 | 0.0071 | 0.0059 | 0.0071 | 0.0080 | 0.0078 |

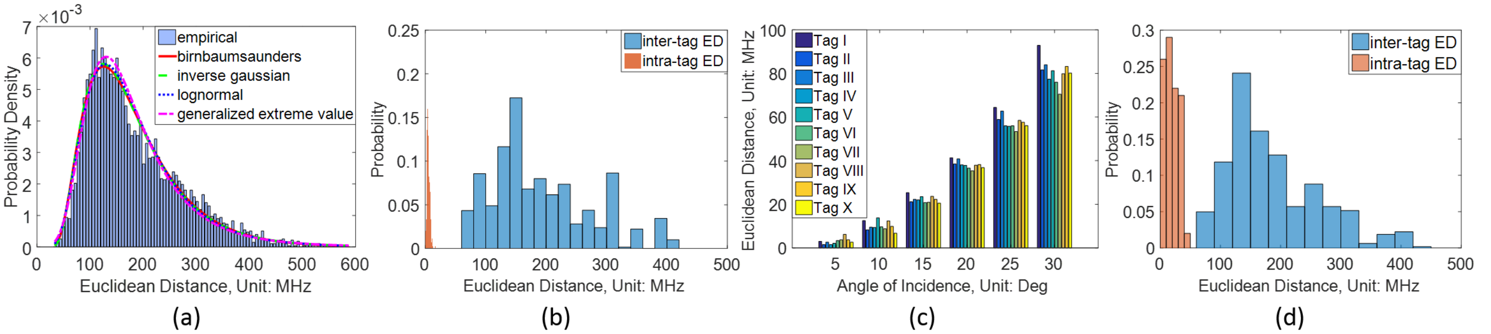


Figure 9: (a) Euclidean distance distribution of UCR tags, (b) Euclidean distance distributions of UCR tags in the presence of WGN with a SNR of 10 dB, (c) Euclidean distances relative to zero incident angle, and (d) Euclidean distance distributions of UCR tags when angle of incidence varies from 0° to 20°.

of one UCR tag and replay the frequency response when a forged tag is being scanned. However, this type of replay attack needs an extra equipment to replay the frequency response, which will be too expensive to be a realistic attack to the supply chain of low-cost commodities. Like many other existing RFID-based solutions, UCR system is susceptible to RF interference. This issue can be addressed by repeating measurements of UCR tags provided that the appearance of RF interference is usually intermittent. UCR system is also susceptible to split attacks (i.e., separating tag from product, swapping tags, etc.), which will be addressed in our future work.

## VI. Conclusion and Future Work

In this paper, we presented a new unclonable chipless RFID (UCR) tag that carries a unique ID. The uniqueness of UCR tags has been verified with a large quantity of tag samples. The reliability of UCR tags has been verified via simulations with random white Gaussian noise and varying angles of plane wave incidence. UCR system not only builds up the trustworthy visibility into supply chain status but also has the potential to expand the scope of the IoT by enabling many non-electronic products (e.g., food, pharmaceuticals, newspapers, magazines, etc.) to be connected to the network. UCR tags can be attached to the packages of products, directly integrated onto the PCBs of electronic products, or even have the potential to be printed on the products or their packages with conductive ink. Compared with existing approaches, UCR system has the following merits: (1) The ID provided by UCR tag is unique and unclonable since it depends on the random and uncontrolable process variations during tag fabrication; (2) UCR tags can be fabricated with the same layout and do not require post-processing (i.e., removing or shorting some of the resonators that compose the chipless RFID tag) to encode data, which significantly reduces the manufacturing time and cost; (3) Compared with exhaustive search, our proposed look-up method dramatically speeds up the authentication process of UCR tags. In future work, we plan to fabricate a large number of UCR tags and test them in a real-world scenario.

## Acknowledgment

This project was supported in part by AFOSR MURI grant under award number FA9550-14-1-0351, and by the National Science Foundation (NSF) under grants CCF-1423282 and CCF-1559772.

## References

[1] U.S. Department of Homeland Security. Intellectual Property Rights Seizures Statistics, Fiscal Year 2014, 2015.

[2] Sean Kilcarr. FreightWatch: Cargo theft risk will rise in 2015, Mar 2015.

[3] Tricia Bishop and Baltimore Sun. UPC bar code has been in use 30 years / Once-controversial technology is now ubiquitous, Jul 2004.

[4] Yue Liu, Ju Yang, and Mongjum Liu. Recognition of QR Code with mobile phones. In *Control and Decision Conference, 2008. CCDC 2008. Chinese*, pages 203–206. IEEE, 2008.

[5] Yu Xiaoyang, Song Yang, Yu Yang, Yu Shuchun, Cheng Hao, and Guan Yanxia. An encryption method for QR code image based on ECA. *International Journal of Security & Its Applications*, 7(5), 2013.

[6] Suraj Kumar Sahu and Sandeep Kumar Gonnade. Encryption in QR Code Using Stegnography. *IJERA International Journal of Engineering Research and Applications*, 3(4), 2013.

[7] John Fredy Barrera, Alejandro Mira, and Roberto Torroba. Optical encryption and qr codes: Secure and noise-free information retrieval. *Optics express*, 21(5):5373–5378, 2013.

[8] Charles Wankel. *21st century management: a reference handbook*. Sage Publications, 2007.

[9] Cédric Hocquet, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and François-Xavier Standaert. Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags. *Journal of Cryptographic Engineering*, 1(1):79–86, 2011.

[10] Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-key cryptography for RFID-tags. In *Pervasive Computing and Communications Workshops, 2007. PerCom Workshops' 07. Fifth Annual IEEE International Conference on*, pages 217–222. IEEE, 2007.

[11] Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, and Ingrid Verbauwhede. Elliptic-curve-based security processor for RFID. *Computers, IEEE Transactions on*, 57(11):1514–1527, 2008.

[12] Dong Sam Ha and Patrick R Schaumont. Replacing cryptography with ultra wideband (UWB) modulation in secure RFID. In *RFID, 2007. IEEE International Conference on*, pages 23–29. IEEE, 2007.

[13] Pengyuan Yu, Patrick Schaumont, and Dong Ha. Securing RFID with ultra-wideband modulation. In *Proceedings of workshop on RFID security (RFIDSec)*, pages 27–39, 2006.

[14] Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. Enhancing RFID security and privacy by physically unclonable functions. In *Towards Hardware-Intrinsic Security*, pages 281–305. Springer, 2010.

[15] Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. Design and implementation of PUF-based" unclonable" RFID ICs for anti-counterfeiting and security applications. In *RFID, 2008 IEEE International Conference on*, pages 58–64. IEEE, 2008.

[16] Blaise Gassend, Dwaine Clarke, Marten Van Dijk, and Srinivas Devadas. Silicon physical random functions. In *Proceedings of the 9th ACM conference on Computer and communications security*, pages 148–160. ACM, 2002.

[17] Stevan Preradovic, Isaac Balbin, Nemai Chandra Karmakar, and Gerhard F Swiegers. Multiresonator-based chipless RFID system for low-cost item tracking. *Microwave Theory and Techniques, IEEE Transactions on*, 57(5):1411–1419, 2009.

[18] 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.

[19] Md Aminul Islam and Nemai Chandra Karmakar. A novel compact printable dual-polarized chipless RFID system. *Microwave Theory and Techniques, IEEE Transactions on*, 60(7):2142–2151, 2012.

[20] Stevan Preradovic and Nemai Chandra Karmakar. Chipless RFID: bar code of the future. *IEEE Microwave Magazine*, 7(11):87–97, 2010.

[21] R Janaswamy and DH Schaubert. Characteristic impedance of a wide slotline on low-permittivity substrates (short paper). *Microwave Theory and Techniques, IEEE Transactions on*, 34(8):900–902, 1986.

[22] Cisco. Radio Frequency Fundamentals, Sep 2014.