Identifying RF Identification Cards from Measurements of Resonance and Carrier Harmonics

Henry P. Romero, Kate A. Remley, *Senior Member, IEEE,* Dylan F. Williams, *Fellow, IEEE*, Chih-Ming Wang, Timothy X. Brown

***Abstract*—We show that careful measurements of the unloaded resonance frequency and quality factor of radio frequency identification proximity cards allow identification of different card models and, for the set of cards we studied, identification with minimal error of individual cards of the same model. Furthermore, we show that card identification performance is improved by considering an electromagnetic signature that combines measurements of the energy at carrier harmonics during a reader-card transaction together with measurements of unloaded resonance frequency and quality factor.**

***Index Terms*—Authentication, Electromagnetic Signature, Resonance Frequency**

I. Introduction

We demonstrate a method for identifying individual radio frequency identification (RFID) cards based on measurements of electrical resonance and measurements of the energy at carrier harmonics during a reader/card transaction. We show that, for the test sample studied, measurements of electrical resonance allow us to identify individual cards that belong to the same or different card models with low error. The accuracy of correctly identifying cards from their corresponding measurements is improved if measurements of both electrical resonance and the energy at carrier harmonics are used.

Our goal is to show that underlying differences that distinguish RFID cards, such as different circuit layouts, different circuit element dimensions, and variations within manufacturing tolerances of circuit components, can be measured through electromagnetic measurements and quantified to create an electromagnetic signature. This ability to identify electromagnetic signatures could benefit security and assurance [1] and could be paired with digital device identifiers to detect counterfeit cards [2].

Identification of electronic devices based on electromagnetic measurements is not new, but previous efforts have focused generally within the context of other technologies such as radar, cellular phones, wireless local area networks (WLAN), Bluetooth, and Ethernet. The military has tracked enemy radio transmitters while cellular carriers have combated cloning fraud with proprietary implementations of this idea [3]. For WLAN and Bluetooth technologies, Hall *et al.* [4] characterized the period immediately following power on with Fourier and wavelet transforms. Remley *et al.* [5] also studied WLAN devices and used a cross-correlation metric on part of the emitted RF waveform to identify cards. In an approach similar to cross-correlation, Gerdes *et al.* [6] used matched filters to identify Ethernet devices. For high-frequency RFID devices, Danev *et al.* [7] observed the response of an RFID card to the initial reader inquiry and characterized individual cards from the start of their response and by a high-dimensional principal component analysis of the frequency content of their response. Similarly, in Romero *et al.* [8], the measured energies at the third and fifth harmonics of the carrier frequency during the reader inquiry of an RFID transaction were shown to be an effective electromagnetic signature for reliably distinguishing between different card makes and models.

We studied RFID proximity cards operating under the ISO standard 14443 [9] at 13.56 MHz. Specifically, we studied only the Type A standard within ISO 14443. Our method here adapts and extends the results in [8] by considering electromagnetic signatures based on measurements of the unloaded resonance frequency and quality factor (Q), and by identifying individual cards both within and between card models rather than simply between card models. To measure the resonance frequency and Q, we use a network analyzer, which is a relatively economical and small measurement device for frequencies below 50 MHz. For example, Agilent and Anritsu offer handheld spectrum analyzers [10]. Cost and size considerations would ease implementation of a security system based on identification of RFID cards through the electromagnetic signature explored here. With this electromagnetic signature, we demonstrate reasonable identification of individual RFID cards.

In addition, we consider an electromagnetic signature that combines both measurements of electrical resonance and measurements of carrier harmonics as in [8]. We consider not only measurements of the carrier harmonics at the nominal value of 13.56 MHz, but also measurements of the energy at the carrier harmonics when the frequency of the radio frequency carrier differs from 13.56 MHz. With this larger electromagnetic signature, we demonstrate increased accuracy in identification of individual RFID cards relative to the resonance-only electromagnetic signature.

II. Resonance in an RFID card

A. Theory

The RFID cards we consider are designed to operate in the unlicensed industrial, scientific, and medical (ISM) frequency

Work partially supported by U.S. government, not subject to U.S. copyright

H. P. Romero and T. X. Brown are with the University of Colorado, Boulder, CO 80309 USA, (e-mail: romeroh@colorado.edu).

K. A. Remley, D. F. Williams, and C.-M. Wang are with the National Institute of Standards and Technology, Boulder, CO 80305 USA (phone: 303-497-3652 e-mail: {remley,dylan}@ boulder.nist.gov).

band near a carrier frequency of 13.56 MHz. In fact, they are tuned to a slightly higher frequency so that operation within the ISM band is still assured in the presence of multiple cards. We consider two central quantities related to the tuning of these cards: the resonance frequency and the quality factor.

The angular resonance frequency ω_0 can be defined as the angular frequency at which the reactance of the resonator vanishes, as this indicates that the energies in the electric and magnetic fields are balanced. We define the quality factor[11] as

$$Q = \frac{\omega_0 \, W}{P}, \tag{1}$$

where W and P are the stored energy and the average dissipated power in a resonator at ω_0, respectively. To estimate the quality factor and resonance frequency of an RFID card, we represent our measurement system (Figure 1a) consisting of a test fixture, cables, and an RFID card with a one-port lumped element circuit model (Figure 1b). We are then able to write the unloaded angular resonance frequency ω_0 and quality factor Q_0 in terms of the resistance R_0, capacitance C_0, and inductance L_0 of the parallel RLC equivalent circuit of the RFID card as

$$Q_0 = \frac{R_0}{\omega_0 L_0} \qquad\qquad \omega_0 = \frac{1}{\sqrt{C_0 L_0}}. \tag{2}$$

Unfortunately, we cannot isolate the RFID resonator and must observe it through a coupling circuit consisting of a broadband antenna coil. The ensemble of circuit elements of the measurement setup resonates differently from how the RFID circuit would resonate alone, and thus the loaded Q and angular resonance frequency (Q_L and ω_L) differ from the unloaded Q and angular resonance frequency of the RFID card alone (Q_0 and ω_0). For the measurement setup as a whole, the maximum energy stored is lower, and the average power dissipated is higher than it would be for the RFID card alone. The loaded Q and resonance frequency are dependent on the coupling circuit, cable, and specific vector network analyzer used in the measurement.

To obtain only the resonance parameters associated with the RFID card, we must treat our measurements as if they were produced by the circuit in Figure 1(b). To do this, we apply a linear phase shift and use a procedure developed in [12] to estimate the unloaded quality factor and resonance frequency from a set of measured reflection coefficients near the frequency of resonance.

B. Measurements

To excite resonance in a RFID proximity card, we coupled energy into the card via a coupling antenna and observed the reflection coefficient at various frequencies of a one-port network that connects to this coupling antenna (Figure 1). We measured on a frequency grid spanning from 10 MHz to 30 MHz that was wide enough to capture the resonance behavior for all the cards studied. We carefully controlled the placement of our coupling circuit with respect to the RFID card to ensure repeatability of our measurements. Furthermore, we found it necessary to calibrate the reference plane as close as possible to the coupling circuit and to take precautions that our connections between the VNA and coupling circuit were precise and stable.

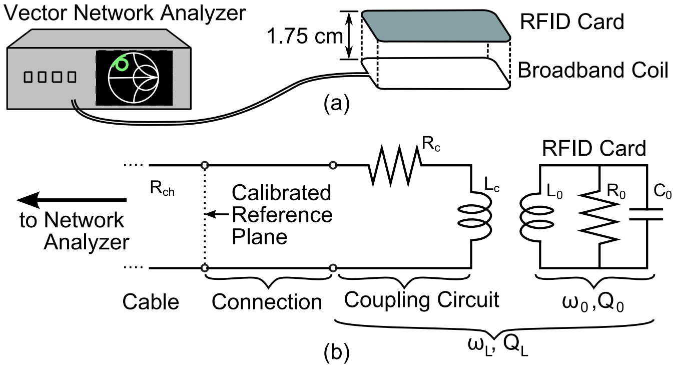

Fig. 1. Measurement system for measuring resonance in RFID cards. (a) Coupling with RFID card (b) Equivalent Circuit

Our coupling antenna was a coil antenna of approximately the same dimensions as the RIFD card itself. We used a test fixture (Figure 1(a)) to ensure that the orientation and distance were consistent between measurements, as we found that the orientation and distance between the coupling coil and RFID card were important and affected the measurements significantly. Our test fixture ensured that the coupling coil and RFID card were in parallel planes of a fixed distance apart. Furthermore, we took care to control the relative placement of the RFID card and coupling coil in each of these planes to within a millimeter, as we found it important that the relative positions of the card and coupling coil in their respective planes were consistent.

Choosing the distance between the coil and the card represented a trade-off between competing goals. Placing the RFID card and coil far apart lowers the level of coupling between the RFID card and the coil, and leads to resonance frequency measurements more representative of the RFID card. However, lower coupling also leads to small signals and low signal to noise ratios. Conversely, placing the RFID card and coil close together improves the signal to noise ratio, but creates large coupling factors. With large coupling factors it becomes a challenge to correctly extract the unloaded resonance characteristics from the measured loaded resonance characteristics. As a balance between the competing objectives of reducing noise and reducing coupling, we chose a distance of approximately 1.75 cm. At this distance, the coupling and noise were low enough to enable a consistent calculation of the unloaded resonance frequency and quality factor.

We note that this measurement procedure had difficulty in reliably exciting resonance of RFID cards that were contact as well as contact-less; that is, the cards could communicate via a direct metal-to-metal contact in addition to the magnetic coupling.

C. Post-Processing

To extract the unloaded resonance frequency and quality factor from the measured reflection coefficients, we take steps to compensate for the distortions introduced into the data

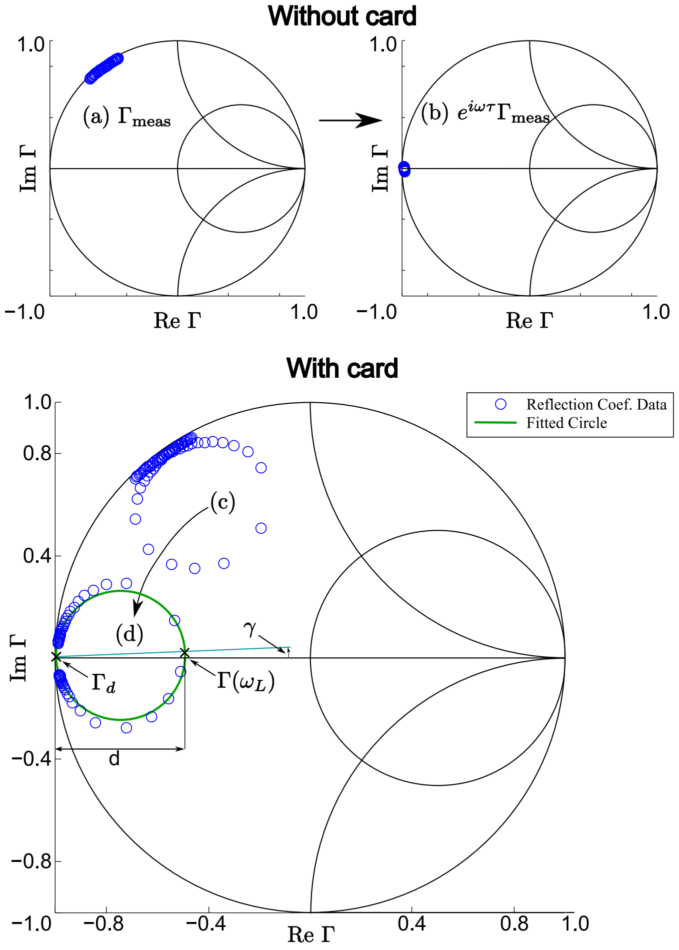

Fig. 2. Determining unloaded resonance frequency and Q by first applying a linear phase shift and then fitting a circle. (a) Measured reflection coefficient data without the card present (Γ_{meas}). (b) A linear phase shift, $e^{i\omega\tau}$, is chosen so that the frequency dependence in the measured data without the card present is negligible. (c) Measured reflection coefficient data with the card present form a loop in the complex plane. (d) Data with card present after applying the linear phase shift determined in (b). Here, the data can be modeled well by a narrowband circle approximation to estimate the unloaded frequency and Q factor.

by the intervening circuit elements between the calibrated reference plane and the RFID card. We model the intervening circuit elements as consisting of a short transmission line segment followed by a lossy coupling inductor (Figure 1(b)).

1) Compensating For The Connections: To compensate for the connection between the cable and the coupling antenna, which consists of simply an adapter and two short parallel traces, we model the connection as a transmission line. To shift our reference plane to the end of this transmission line, we multiply the data by a linear phase shift, $e^{i\omega\tau}$, where τ is the elapsed time necessary for a radio signal to propagate from the calibrated reference plane to the coupling antenna. We choose the value of τ so that the measured reflection coefficient without the card present demonstrates negligible frequency dependence over the frequency range of interest. We obtain a first-order approximation of this value by manually choosing different values of τ and qualitatively assessing which option offers the best reduction in frequency dependence. We show the process of determining τ in Figure 2 (a)-(b).

2) Narrowband Approximation Near Resonance: After applying the linear phase shift, we use the method of Kajfez [12] to calculate the unloaded resonance frequency and Q factor. For a one-port resonant network, such as the circuit in Figure 1(b), a good narrowband approximation of the reflection coefficient Γ, as observed from the calibrated reference plane, is

$$\Gamma(\omega) = \Gamma_d + \frac{d e^{-i\gamma}}{1 + iQ_L 2\frac{\omega-\omega_L}{\omega_0}}, \qquad |\omega-\omega_L| \ll \omega_0, \tag{3}$$

where d is the diameter of the resonance loop, γ is the rotation angle of the resonance loop (measured with respect to the the line connecting Γ_d and the origin), and ω is the angular frequency (that is, $2\pi f$, where f is frequency), and Γ_d is the de-tuned reflection coefficient (the reflection coefficient that is obtained if the RFID card were not present), which is related to the circuit parameters in Figure 1(b) by

$$\Gamma_d = \frac{R_c + jL_c - R_{ch}}{R_c + jL_c + R_{ch}}. \tag{4}$$

In (4), R_{ch} is the characteristic impedance of the transmission line, and R_c, X_c are respectively the loss and reactance of the coupling circuit; Γ_d is representative of the losses in the coupling circuit. If the losses in the coupling circuit are minimal (if R_c is small), then Γ_d lies close to the unit circle and the measured reflection coefficient data lie close to the boundary of the Smith chart. On the other hand, if the coupling losses are greater, then Γ_d lies farther from the unit circle and the measured reflection coefficient data do not lie on the boundary of the Smith chart.

An illustration of the parameters $\Gamma_d, d,$ and γ with respect to a measured reflection coefficient resonance loop is given in Figure 2(d). The rational term in (3) describes a circle in the complex plane, and Γ_d simply shifts that circle. Noting that (3) describes a circle in the complex plane leads to a method for estimating the parameters in (3): fitting a circle to reflection coefficient data near resonance.

3) Circle Fit: To fit a circle to (3), we define $t = 2\frac{\omega-\omega_L}{\omega_0}$, and write

$$\Gamma(t) = \frac{a_1 t + a_2}{a_3 t + 1}, \tag{5}$$

where $\{a_1, a_2, a_3\}$ are complex numbers that can be related to $\Gamma_d, Q_L,$ and d as

$$\Gamma_d = \frac{a_1}{a_3} \qquad Q_L = \operatorname{Im}(a_3) \qquad d = \left|\frac{a_1 - a_2 a_3}{Q_L}\right|. \tag{6}$$

As (5) represents a linear relationship between the a_k, they can be estimated from a linear least-squares fit from the scattering parameter data $\Gamma(\omega)$, provided that we know ω_0 and ω_L. Unfortunately, we cannot know the unloaded angular resonance frequency ω_0 directly from the data initially. The loaded angular resonance frequency ω_L is easily estimated by locating the frequency corresponding to the minimum magnitude of the reflection coefficient during resonance, as this is the resonance frequency of the entire measurement system. To estimate ω_0, we take $\omega_0 \approx \omega_L$ and use an iterative process with a least-squares fit at each iteration. Once the iterations have converged, we choose the refined ω_0 as the

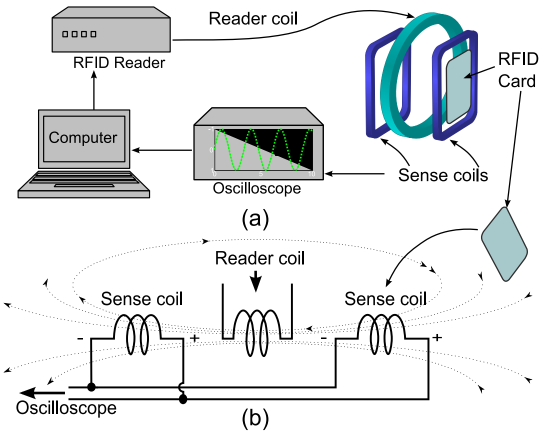

Fig. 3. (a) Measurement system for measuring the energy at carrier harmonics in RFID cards (b) Illustration of near-field nature of an ISO 14443 transaction. We use two symmetrically placed sense coils on both sides of the reader coil to detect changes in the electromagnetic field at the same distance that the RFID card is located. We subtract the measured signal from one sense coil from the other so that we may cancel to first order the reader field in the absence of an RFID card.

unloaded angular resonance frequency. The details of the iterative refinements on ω_0 are given in the Appendix.

The relationship between the unloaded Q and loaded Q can be defined in terms of a coupling factor κ, which is in turn defined as the ratio of the power dissipated in the external coupling circuit to the power dissipated in the resonator. This relationship is

$$Q_0 = (1+\kappa)Q_L. \tag{7}$$

The coupling factor can be deduced from the diameter of the measured Q circle with

$$\kappa = \frac{1}{(d_2/d)-1}, \tag{8}$$

where d_2 is a factor dependent on the losses present in the system [12]. The details of the calculation of d_2 are given in the Appendix.

III. Energy at Carrier Harmonics

To obtain the energy at the carrier harmonics of the RFID card, we performed the same measurements as in [8]. The measurement system (Figure 3) involved a test fixture to measure the electromagnetic field passing through the RFID card during an ISO 14443 Type A transaction. We sampled the measured electromagnetic signal at 1.25 GHz and recorded 150 μs of the signal to capture the entire reader inquiry. Then, we calculated the energy present in the third carrier harmonic in this portion of the signal. The restriction to the reader inquiry and the third harmonic are choices that were found to be adept for forming a rudimentary electromagnetic signature in [8]. We constructed a signature consisting of the energy at the third carrier harmonic when the carrier frequency is operating at 13.56 MHz and when the carrier is operating at 12.56 MHz. We found this combination to provide better discrimination than the electromagnetic signature consisting of the third and fifth carrier harmonic at 13.56 MHz.

IV. Identifying Cards

A. Electromagnetic Signatures

Our electromagnetic signatures consist of low dimensional vectors of a few representative measured quantities. From our resonance measurements and measurements of energy at carrier harmonics, we found that the following two electromagnetic signatures can identify individual cards well:

$$\mathbf{S}^{(1)} = \begin{pmatrix} f_0 \\ Q_0 \end{pmatrix} \qquad \mathbf{S}^{(2)} = \begin{pmatrix} f_0 \\ Q_0 \\ E_{13.56\text{MHz}}(3f_c) \\ E_{12.56\text{MHz}}(3f_c) \end{pmatrix}, \tag{9}$$

where f_0 and Q_0 are the measured unloaded resonance frequency and unloaded quality factor, and $E_{13.56\text{MHz}}(3f_c)$ and $E_{12.56\text{MHz}}(3f_c)$ are the measured energies in dBm of the 3rd harmonic of the carrier frequency when the carrier frequency is operating at 13.56 MHz and 12.56 MHz, respectively.

In Figure 4 repeat measurements of the first signature $\mathbf{S}^{(1)}$ can be observed directly for several different cards. We see that this signature separates different card models very well and is sufficient to distinguish with relatively low error among different cards within the same model. Figure 4 illustrates a measurement set of 20 cards with 18 repeat measurements per card. The 20 cards consist of four different card manufacturers each represented by five different individual cards from a specific batch. Between each repeat measurement, the card was removed from the measurement fixture, then re-inserted.

B. Card Classification

To associate a given electromagnetic signature with the corresponding card that produced that electromagnetic signature, we use a statistical model to select the most probable card to have produced the given signature. We model each measurement of the signature, $\mathbf{S}_c^{(n)}$, of card c as a sample drawn from a multivariate Gaussian probability distribution, $\mathbf{S}_c^{(n)} \sim \mathcal{N}(\mu_c, \mathbf{\Sigma}_c)$. We consider both the case that the distribution of each card's measurements will vary in a different manner around their respective means and the case that the distribution of each card's measurements will vary in the same manner around their respective means. The first case requires that for each card c, a separate covariance matrix $\mathbf{\Sigma}_c$ is estimated, while the second case requires that a pooled covariance $\mathbf{\Sigma}$ is estimated.

The separate covariance matrix estimates have smaller degrees of freedom and are hence less stable than the pooled covariance estimate. The use of the pooled covariance estimate, however, requires the restrictive assumption that each card's measurements must vary in the same manner around their respective means. As a balance between stable estimates and generality of our statistical model, we choose to regularize the separate covariance estimates for each card with the pooled estimate by defining a parameter α such that $0 \le \alpha \le 1$ and by defining a new covariance estimate as

$$\mathbf{\Sigma}_{\alpha,c} = (1-\alpha)\mathbf{\Sigma} + \alpha\mathbf{\Sigma}_c. \tag{10}$$

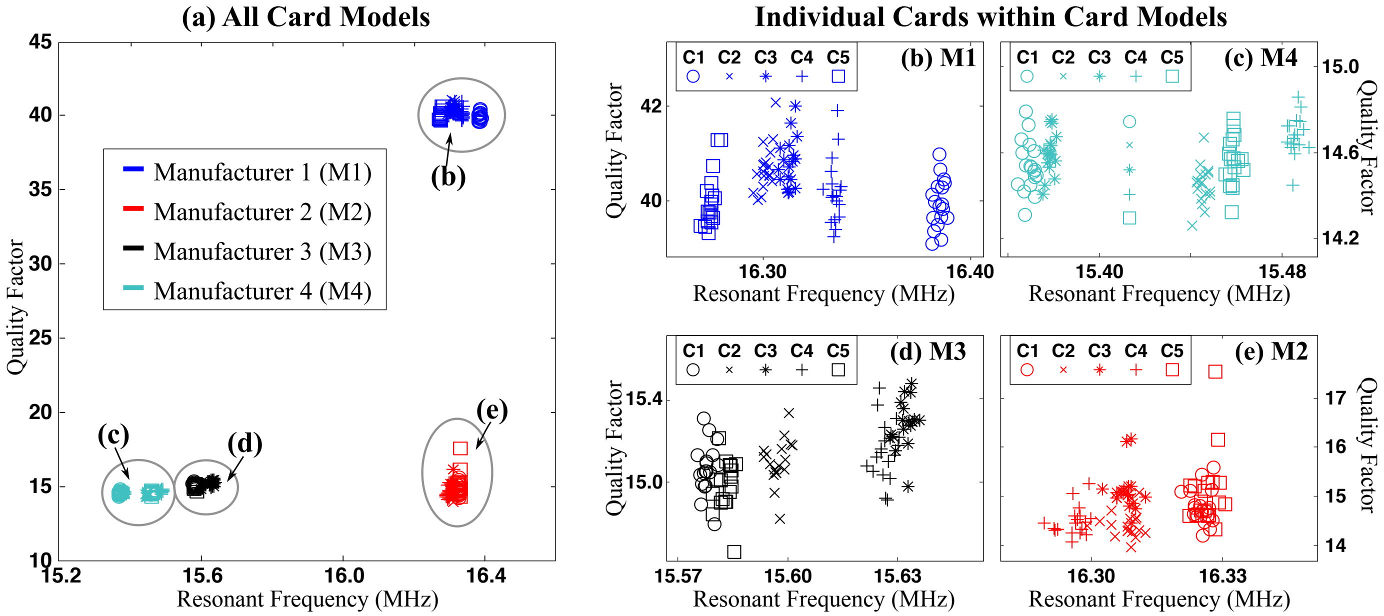

Fig. 4. Unloaded angular resonance frequency (ω_0) and unloaded quality factor (Q_0) measurements from four different card models. For each card model, five different cards were measured and for each card, 18 repeat measurements were taken. (a) All measurements collectively illustrated. Measurements from within card models formed clusters and are encircled; each of the four clusters were distinct and non-overlapping, allowing for perfect identification of the card model from these measurements. (b)(c)(d),(e) Within card models, where Cx refers to the x^{th} card of each manufacturer. Measurements from individual cards also formed distinct clusters from which we can identify individual cards.

With the parameter α, we introduce the ability to fine-tune an algorithm so that it may perform better on a given classification task. This method is known as regularized discriminant analysis [13].

Estimating the probability that a specific card produced a given signature involves two steps. First, the parameters of the Gaussian distribution must be estimated, and second, the probability of the measurement belonging to each of the cards must be computed. To estimate the parameters, we collect several measurements of the electromagnetic signature $\mathbf{S_{c,k}}^{(n)}$. In this notation, $k = 1, \ldots, N_c$ indexes the N_c repeat measurements for each card c. From these training samples, standard normal theory concludes that maximum-likelihood estimates of the Gaussian distribution parameters are

$$\hat{\mu}_c = \frac{1}{N_c}\sum_{k=1}^{N_c} \mathbf{S}_{c,k}^{(n)} \tag{11}$$

$$\hat{\mathbf{\Sigma}}_c = \frac{1}{N_c-1}\sum_{k=1}^{N_c}\left(\mathbf{S}_{c,k}^{(n)}-\hat{\mu}_c\right)\left(\mathbf{S}_{c,k}^{(n)}-\hat{\mu}_c\right)^{\mathrm{T}} \tag{12}$$

$$\hat{\mathbf{\Sigma}} = \frac{1}{N-C}\sum_{c}\sum_{k=1}^{N_c}\left(\mathbf{S}_{c,k}^{(n)}-\hat{\mu}_c\right)\left(\mathbf{S}_{c,k}^{(n)}-\hat{\mu}_c\right)^{\mathrm{T}}, \tag{13}$$

where $N = \sum_c N_c$ is the total number of measurements and C equals the number of cards.

With the estimated Gaussian parameters, we can evaluate the probability of a measured electromagnetic signature $\mathbf{S}^{(n)}$ belonging to card c under our statistical model. We then say that the most probable card $\hat{c}$ to have produced that measurement is the card that corresponds to the highest of those computed probabilities. Choosing the card with the highest probability of generating the measurement observed, that is $P(\mathbf{S}^{(n)})$, is equivalent to choosing the card that minimizes the value of δ_c, where δ_c is defined as

$$\begin{aligned}\delta_c &= -2\log(P(\mathbf{S}^{(n)}))\\ &= (\mathbf{S}^{(n)}-\hat{\mu}_c)^{\mathrm{T}}\hat{\mathbf{\Sigma}}_{\alpha,c}^{-1}(\mathbf{S}^{(n)}-\hat{\mu}_c)+\log|\hat{\mathbf{\Sigma}}_{\alpha,c}|.\end{aligned} \tag{14}$$

Hence, an electromagnetic signature is identified with a card $\hat{c}$ according to the rule $\hat{c} = \operatorname{argmin}_c \delta_c$.

C. Estimation of Future Error

To estimate the future error of a given classifier, we randomly split measured data into a training set consisting of 75 % of the data and a testing set consisting of the remaining 25 % of the data. With the training set, the parameters of the statistical model in regularized discriminant analysis are estimated. With the testing set, comparing the actual card that produced a given electromagnetic signature and the prediction from regularized discriminant analysis of the most likely card to have produced that measurement affords a statistical estimate of future error. Repeating this estimate several times, we can obtain an estimate of the expected future error on identifying cards from their electromagnetic signature [13].

To choose the optimal α for regularized discriminant analysis, we use a future error estimate on card identification for several values of α. We then choose the α corresponding to the minimal predicted future error.

D. Results with Measurements

To demonstrate the results of card identification, we estimate the future error as described above by repeating the random split into training and testing data 500 times. We report in Tables I and II the fraction of times that the electromagnetic

Predicted Card from Resonance Measurements Only

Actual Card		M1					M2					M3					M4				
		C1	C2	C3	C4	C5	C1	C2	C3	C4	C5	C1	C2	C3	C4	C5	C1	C2	C3	C4	C5
M1	C1	1																			
	C2		0.998	0.002																	
	C3		0.002	0.998																	
	C4				1																
	C5					1															
M2	C1						0.722				0.278										
	C2							0.74	0.152	0.108											
	C3							0.165	0.835												
	C4								0.001	0.999											
	C5						0.548				0.452										
M3	C1											0.883				0.117					
	C2												1								
	C3													0.813	0.187						
	C4													0.205	0.795						
	C5											0.163				0.837					
M4	C1																1				
	C2																	1			
	C3																		1		
	C4																			1	
	C5																				1

TABLE I

CONFUSION MATRIX FOR IDENTIFICATION OF CARDS FROM MEASUREMENTS OF RESONANCE FREQUENCY AND Q-FACTOR.

signature corresponding to card x is predicted as belonging to card y when card x was measured.

1) Resonance Data Only: In Table I, we see the results of applying regularized discriminant analysis to measurements of the electromagnetic signature consisting only of the unloaded resonance frequency and unloaded Q, that is $\mathbf{S}^{(1)}$. We found that $\alpha = 0$ produced the best results. For each card, 18 repeat measurements of the electromagnetic signature $\mathbf{S}^{(1)}$ were taken. Some manufacturers offer clear distinction between individual cards, while others are difficult to tell apart in the space of all possible electromagnetic signatures $\mathbf{S}^{(1)}$. With this signature and algorithm, our average estimated overall accuracy for identifying individual cards was 90 %.

2) Resonance Data combined with Harmonic Data: If we consider the electromagnetic signature $\mathbf{S}^{(2)}$, which consists of the measured unloaded resonance parameters combined with the measurements of the energy at the carrier harmonics during an ISO 14443 transaction, we can identify individual cards within different card models with greater accuracy. In Table II, we report the accuracy of identifying cards from measurements of $\mathbf{S}^{(2)}$. For each card, 12 repeat measurements of the electromagnetic signature $\mathbf{S}^{(2)}$ were taken. We see that the confusion among cards for the second model (M2) studied, reduced substantially, and any increase in confusion among individual cards in other models was minimal. Here, regularized discriminant analysis with $\alpha = 0.4$ achieved an estimated overall accuracy of 96 % for identifying individual cards.

E. Threat Model

To provide a context for the use of an electromagnetic signature in strengthing RFID security, we consider an RFID counterfeiting attempt as belonging to one of four categories of attacks.

1) The counterfeit RFID card does not correctly spoof a digital transaction. For this attack, we assume that any standard reader would reject the counterfeit card for transmitting an incorrect unique identification number or failing to sidestep cryptographic security measures.
2) The attacker correctly spoofs a digital transaction, but either manufactures his own card or purchases a re-programmable card from another manufacturer. In this study, we've illustrated that electromagnetic signatures corresponding to different makes and models differ significantly and cluster tightly, and as such, we can defend well against this attack.
3) The attacker correctly spoofs a digital transaction and uses a counterfeit card of the same make and model as the card to be counterfeited; and only a small number of cards is in the pool of allowed cards. Under this model, we've shown that we can still defend well against this attack.
4) The attacker correctly spoofs a digital transaction, uses a counterfeit card of the same make and model as the card to be counterfeited, and the pool of allowed cards is large. Under this model, we will run into problems. Our analysis has shown that cards of the same make and model cluster tightly together; by considering more and more cards of the same make and model , the ability to distinguish cards from each other will steadily diminish.

To address the last and most general threat model, we could prevent the identification error from decreasing to zero by framing the card identification task as a hypothesis test. Any hypothesis test would use the same statistical models estimated previously in Section IV-B. Given a specific error tolerance, the test would reduce to finding an appropriate threshold on the Manahalobis distance measure:

$$\mathrm{dist}(\mathbf{S}^{(n)}, \hat{\mu}_c) = (\mathbf{S}^{(n)} - \hat{\mu}_c)^{\mathrm{T}} \hat{\mathbf{\Sigma}}_{\alpha,c}^{-1} (\mathbf{S}^{(n)} - \hat{\mu}_c), \qquad (15)$$

such that a new measurement will be identified as belonging to a counterfeit card if the threshold is exceeded. This threshold can be chosen so that two possible errors are controlled: that

Predicted Card from Resonance and Harmonic Measurements

Actual Card		M1					M2					M3					M4				
		C1	C2	C3	C4	C5	C1	C2	C3	C4	C5	C1	C2	C3	C4	C5	C1	C2	C3	C4	C5
M1	C1	1																			
	C2		.966	.034																	
	C3		.013	.987																	
	C4				1																
	C5					1															
M2	C1						1														
	C2							.836	.01	.154											
	C3								1												
	C4							.003		.997											
	C5										1										
M3	C1											.898				.102					
	C2												1								
	C3													.91	.09						
	C4													.163	.837						
	C5											.106				.894					
M4	C1																.989		.011		
	C2																	1			
	C3																.001		.999		
	C4																			1	
	C5																				1

TABLE II
CONFUSION MATRIX FOR IDENTIFICATION OF CARDS FROM MEASUREMENTS OF RESONANCE FREQUENCY, Q-FACTOR, AND THIRD HARMONIC ENERGY.

of misclassifying the correct card as a counterfeit card (that is, a false negative) or that of classifying a counterfeit card as the correct card (that is, a false positive), where lowering one error comes at the expense of raising the other. We can choose an optimal threshold such that an appropriate risk-loss function, such as a weighted sum of the square of the two errors, is minimized.

V. CONCLUSION

We have shown that RFID proximity cards of different makes and models can be identified through precise measurement of the small-signal linear frequency response of cards combined with measurements of the energy at carrier harmonics. Furthermore, we have demonstrated the possibility of extending this result to differentiation between RFID cards of the same make and model. Identifying individual RFID proximity cards from our sample set with an accuracy as high as 96 % indicates that the underlying differences between RFID proximity cards can be quantified through electromagnetic measurements.

Good performance involving only the resonance measurements implies that perhaps an economical anti-counterfeiting device consisting of a network analyzer can be implemented. As resonance measurements are independent of the underlying standard, the results could potentially be applicable to other standards at 13.56 MHz (such as ISO 14443 Type B).

Our results here require precise positioning of the RFID cards to within a millimeter in a fixed plane. With more precise and varied electromagnetic measurements, perhaps we can decrease the identification error rate or achieve the same error rate with fewer restrictions on the position of the RFID card.

APPENDIX

To calculate the unloaded angular resonance frequency, we iteratively refine ω_0 to approximate the true unloaded angular frequency. For our description below, we denote the quantities associated with the n^{th} iteration with a superscript (n) and take our initial guess for the unloaded angular resonance frequency to be the loaded resonance frequency, $\omega_0^{(0)} = \omega_L$. Each iteration proceeds by defining $t^{(n)} = 2(\omega - \omega_0^{(n)})/\omega_0^{(n)}$ and fitting a circle with least squares to the measured data $\Gamma(t^{(n)})$ to get the circle fit parameters $a_k^{(n)}$. We then calculate the quantities in (6) with $a_k^{(n)}$ in place of a_k, as well as the following quantities, where the superscript $*$ refers to complex conjugation, and for clarity we use a_k rather than $a_k^{(n)}$:

$$\Gamma_c = \frac{a_1 - a_2 a_3^*}{a_3^* - a_3} \tag{16}$$

$$\Gamma_{L2} = 2\Gamma_c - \Gamma_d \tag{17}$$

$$\Delta z = \frac{a_2 - \Gamma_{L2}}{\Gamma_{L2} a_3 - a_1}. \tag{18}$$

The iterative update to $\omega_0^{(n)}$ is as used in [12] with

$$\omega_0^{(n+1)} = \omega_0^{(n)} \left(1 + \frac{\Delta z^{(n)}}{2}\right). \tag{19}$$

Calculating the unloaded Q factor from the loaded estimate at each iteration involves simply correcting by a multiplicative factor $(1 + \kappa)$, where κ is the coupling factor that can be calculated from (8). The factor d_2 in (8) can be calculated, as in [12], with

$$\psi = \arctan(\Gamma_d - \Gamma_c) - \arctan(\Gamma_d) \tag{20}$$

$$d_2 = \frac{1 - |\Gamma_d|^2}{1 - |\Gamma_d| \cos(\psi)}. \tag{21}$$

After two iterations, the estimates $\omega_0^{(n)}$, $\kappa^{(n)}$, and $Q_L^{(n)}$ change little. As the second iteration estimates varied less than 0.01% from the previous iteration estimates, we chose the unloaded angular resonance frequency and quality factor to be those values from the second iteration:

$$Q_0 = (1 + \kappa^{(2)}) Q_L^{(2)}, \qquad \omega_0 = \omega_0^{(2)}.$$

Acknowledgment

The authors thank Bill Riddle for help with Q calculations, David Novotny for technical advice, and Nathan Orloff for insightful suggestions. Bill, David, and Nathan are with the NIST Electromagnetics Division in Boulder, CO.

References

[1] T. Daniels, M. Mina, and S. F. Russell, "Short Paper: A Signal Fingerprinting Paradigm for General Physical Layer and Sensor Network Security and Assurance," *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, pp. 219-221, Sept. 2005

[2] D. A. Knox and T. Kunz, "Secure Authentication in Wireless Sensor Networks Using RF Fingerprints," *Embedded and Ubiquitous Computing, 2008. EUC '08. IEEE/IFIP International Conference on* , vol.1, pp.230-237, Dec. 2008

[3] M. J. Riezenman, "Cellular security: better, but foes still lurk". *IEEE Spectrum*, pp. 39-42. June 2000.

[4] J. Hall, M. Barbeau, and E. Kranakis, "Detection of rogue devices in Bluetooth networks using radio frequency fingerprinting" in *Proc. 3rd IASTED Int. Commun. Comput. Networks Conf.*, ., Lima, Peru, Oct. 2006, pp. 108-113.

[5] K. A. Remley, C. A. Grosvenor, R. T. Johnk, D. R. Novotny, P. D. Hale, M. D. Mckinley, A. Karygiannis, and E. Antonakakis, "Electromagnetic signatures of WLAN cards and network security" in *Proceedings 2005 IEEE Symposium on Signal Proc. and Inf. Tech.*, pp. 484-488.

[6] R. M. Gerdes, T. E. Daniels, M. Mina, and S. F. Russell. "Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach." *Proceedings of the Network and Distributed System Security Symposium, NDSS 2006, San Diego, California, USA*

[7] B. Danev, T. S. Heydt-Benjamin, S. Capkun, "Physical-layer Identification of RFID Devices" in *Proceedings of the USENIX Security Symposium*, 2009.

[8] H. P. Romero, K. A. Remley, D. F. Williams, and C. .M. Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards". *Microwave Theory and Techniques , IEEE Transactions on*, vol. 57, pp. 1383-1387. May 2009.

[9] ISO/IEC FCD 14443, Identification cards—Contactless integrated circuit(s) cards—Proximity cards.

[10] We use product names only to describe our experiments. NIST does not endorse commercial products. Other products may work as well or better.

[11] S. Ramo, J. R. Whinnery, and T. V. Duzer, *Fields and Waves in Communications Electronics*. Hoboken, NJ: John Wiley & Sons, 1994.

[12] D. Kajfez, *Q Factor* Oxford, MS: Vector Fields, 1994.

[13] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning*. New York, NY: Springer, 2009.