Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards

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

***Abstract*—We investigate a technique for counterfeit detection of high-frequency radio frequency identification (RFID) cards based on the electromagnetic characteristics of the cards rather than the digital information that they transmit. We describe a method of quantifying the electromagnetic signature of an RFID card and identify a small set of features that is sufficient to correctly classify a test set of cards. Furthermore, we show that our measurements indicate that the features most useful for distinguishing cards are contained within the reader inquiry rather than the card response, a reflection of the near-field coupling nature of the RFID transactions in ISO 14443.**

***Index Terms*—Authentication, electromagnetic signatures, radio frequency identification (RFID).**

I. Introduction

We demonstrate that key electromagnetic waveform features extracted from a measured radio frequency (RF) signal allow us to distinguish between radio frequency identification (RFID) cards produced by different manufacturers. This method is based on comparing electromagnetic field measurements from a single reader/card handshake for several cards of the same model and of differing models and manufacturers.

We detail the measurement setup, explain the key electromagnetic waveform features found, and use a simple classification scheme of these features to demonstrate that a card manufacturer can be predicted with minimal error over several randomized trials. This result leads us to believe that with more features and with a more advanced classification scheme, it may be possible to identify cards in more rugged environments and within manufacturers.

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 Ethernet, radar, cellular phones, wireless local area networks (WLAN), and Bluetooth. Kohno *et al.* [1] identify individual ethernet cards remotely over a network through clock skew estimates derived from TCP/IP timestamps. The military has tracked enemy radio transmitters while cellular carriers have combated cloning fraud with proprietary implementations of this idea [2]. For WLAN and Bluetooth technologies, Hall *et al.* [3] characterize the time immediately following power on using Fourier and wavelet transforms. Here, classification of devices is based on subsequent use of Hotelling's T^2 statistics. Again for WLAN devices, Remley *et al.* [4] use a cross-correlation metric on a larger part of the transaction to identify cards. Its application to RFID systems was outlined in the context of general RFID security in Juels [5]. Periaswamy *et al.* [6] studied the identification of 900-MHz RFID systems, where the identification is based on measurements of the minimum power needed for a transaction at various frequencies.

Our work adapts and extends these ideas to a different technology by considering novel metrics. Specifically, we consider 13.56 MHz "proximity" RFID cards operating under ISO 14443, where transactions occur in the near field of the operating RF carrier. We choose a different section of the electromagnetic signal from which to extract an electromagnetic signature than the sections previously considered in the study of the electromagnetic signatures of other far-field wireless technologies. We demonstrate that the near-field nature of the transactions allows for flexibility in the choice, and that a reliable electromagnetic signature is derived from the reader inquiry.

We introduce an analysis with greater bandwidth than previously considered that allows us to capture potential nonlinear behavior. We show that this finer resolution of detail allows distinct identification of RFID cards. To implement this broadband analysis, we use a real-time oscilloscope with a maximum sampling rate of 20 GHz to measure the fundamental and harmonics up to the ninth harmonic of a 13.56-MHz RF carrier. We show that the higher harmonics of the signal form a good basis for a reliable electromagnetic signature.

II. Measurement

A. Overview

Our work has focused on electromagnetic measurements of ISO 14443 Type A cards. Under the ISO 14443 standard, RFID transactions between a transmitting antenna, or reader, and receiving antenna, or card, occur over fractional lengths of the 13.56-MHz carrier wavelength. With these distances, inductive coupling, rather than radiation or backscattering, is the primary electromagnetic transmission mechanism. This differentiates our work from previous work in that WLAN, Bluetooth, and even 900-MHz RFID systems all operate in the far field, or over several wavelengths of the operating RF carriers.

We operate within the ISO 14443 standard as a starting point; the initial reader inquiry (REQA) always contains the same string of bits and the initial tag response is a generic 16-bit

Manuscript received June 26, 2008; revised January 22, 2009. First published April 14, 2009; current version published May 06, 2009. This work was supported in part by the U.S. Government.

H. P. Romero is with the Applied Math Department, University of Colorado at Boulder, 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 (e-mail: remley@boulder.nist.gov; dylan@boulder.nist.gov; jwang@boulder.nist.gov).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TMTT.2009.2017318

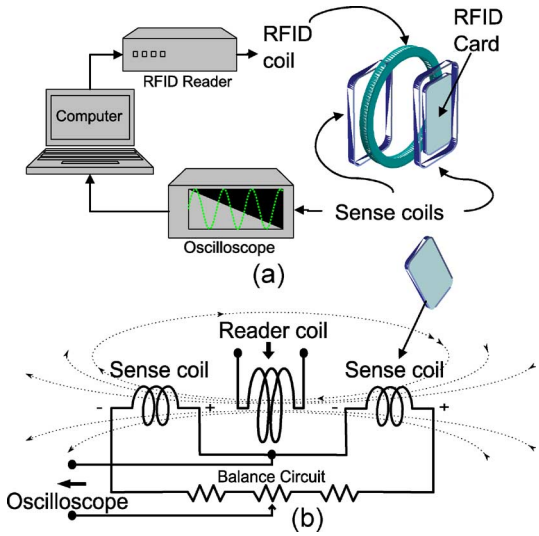


Fig. 1. (a) Measurement setup. (b) Illustration of near-field nature of an ISO 14443 transaction. We measure the electromagnetic signal on both sides of the reader coil and connect these measured signals so that, to first order, we cancel the reader field.

response (ATQA). To measure the electromagnetic signals, we sample the current induced in a pair of sense coils by the changing magnetic field in close vicinity of an RFID card. These broadband sampled signals are later analyzed and key features are extracted to create an electromagnetic signature.

The underlying digital transmission operates at a rate of 1 bit per 128 RF carrier cycles and consists of square pulses with various modulation depths. The reader communicates through full on-off keying with 100% modulation, while the card load modulation has only a small influence on the amplitude of the reader field. In the card response, half of the duration of a single bit contains four higher frequency square pulses sent at subcarrier rate of one pulse per 16 carrier cycles. As a result, the card response contains a broad array of significant spectral content.

A full reader-card transaction follows a state-machine flow starting with a query (REQA) to identify any Type A cards within its field. The following 16-bit card response (ATQA) is generic and identifies the card as a Type A proximity card. It contains a small code that allows the reader to determine if multiple cards are in the field. Subsequent stages of communication proceed to narrow communication to a single card, wherein the card's unique identifying (UID) number and any application-specific information is exchanged. We focus only on the initial REQA–ATQA handshake because it is simple, easily reproducible, and the bit sequence in the reader inquiry, as well as the first part of the card's response, was uniform across all cards we tested.

B. RF Identification Card Test Fixture

The measurement setup is depicted in Fig. 1. The electromagnetic transaction and measurements are carried out using a test fixture described below, while a computer and commercial reader provide the digital commands necessary to step through a reader–card transaction. It is a closed-loop system where the computer initiates a transaction through the reader and then records electromagnetic field measurements of that transaction.

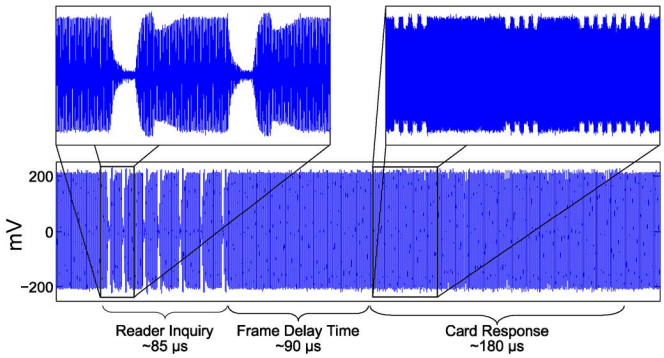


Fig. 2. Sample measurement consisting of the first reader–card handshake in an ISO 14443 transaction where the reader wishes to identify all Type A cards within range and the card responds that it is a Type A card.

The RFID card test fixture consists of a reader coil, two sense coils, and a slot that holds the card in a fixed position parallel to the reader coil at a distance of 4 cm. The fixture we use is a commercially available fixture designed for ISO 10373-6 testing, a standard that provides test protocols for ISO 14443 compliance.

The two sense coils, placed symmetrically on opposite sides of the reader coil, sample the magnetic field in close proximity to the card. One coil senses the electromagnetic field dynamics primarily without the presence of card, and the other primarily with the presence of a card. The two signals are out-of-phase because of inverted wiring in the 10373-6 test fixture so connecting these signals, as in Fig. 1(b) cancels, to a first order, the reader field without the presence of a card. This balance is fine tuned by a small resister network so that nominally, when no card is in the field, the current generated in one coil cancels the current generated in the other. The imbalance created by the presence of a card in the field yields a measurement of a reader–card transaction sensitive to the effects due to the card.

C. Oscilloscope/Data Recording

We sample the signal with a real-time oscilloscope at a rate approximately 90 times the carrier frequency. This provides ten data points per cycle of the ninth carrier harmonic, a resolution sufficient to allow detailed study of the first nine carrier harmonics. At 1.25 GHz, this sampling rate is well within the 20-GHz maximum sampling rate of our oscilloscope. Capturing the correct frame of a reader–card transaction is coordinated by a trigger signal from the reader.

III. Time Alignment

A. Algorithm Based on Phase Information

A typical oscilloscope measurement of a single reader–card transaction is depicted in Fig. 2. The trigger signal from the reader ensures that all the measurements are roughly aligned to within a few RF carrier cycles of each other. However, the trigger and sampling processes are not perfect and comparison of time-dependent features necessitates that all measurements are time aligned.

We time align on a section of the signal that contains an integer number of bit-rate cycles and contains the reader inquiry

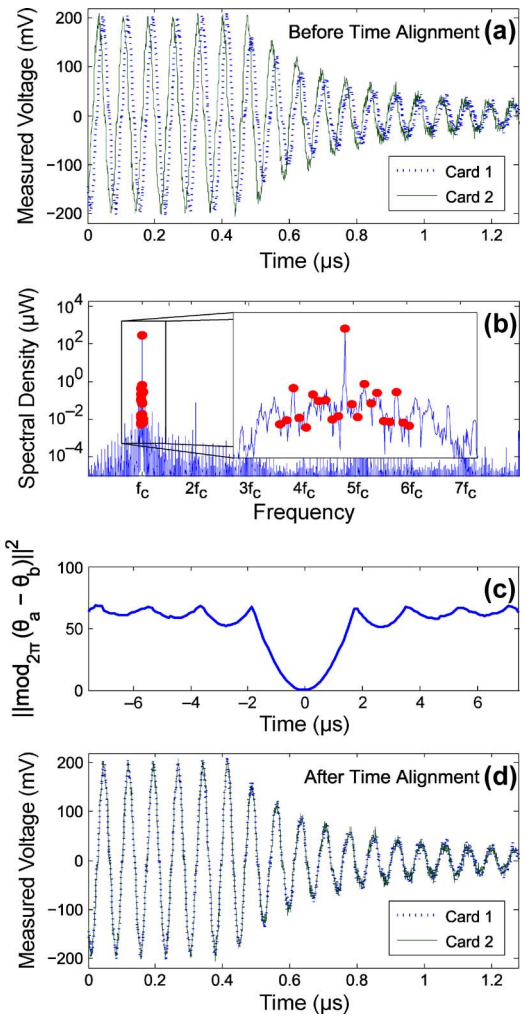


Fig. 3. Time-alignment procedure. (a) Two unaligned RFID responses of two different cards from the same manufacturer. (b) Key frequencies with significant energy around a RF carrier whose phase information is fed into the algorithm. (c) Squared norm of modulo 2π phase difference between cards after applying linear phase shifts. (d) RFID responses aligned with an error-minimizing time shift.

and most of the card response. To time align signals, we use the method of [7] that minimizes the error between the target and measured relative phase components in a signal, as illustrated in Fig. 3. The algorithm hinges on the fact that a delay in time translates to a linear phase shift in the frequency domain and that frequencies containing significant energy are largely responsible for the shape of the time-domain signal. Denote $\mathbf{f} = [f_1, \ldots, f_N]$ and $\theta_x = [\theta_{1,x}, \ldots, \theta_{N,x}]$ as the set of key frequencies and their corresponding phases, respectively, for a measurement x. Let t_a and t_b denote the times at which two measurements (a and b) start with respect to the start of the triggered reader inquiry. The goal of the algorithm is to determine the discrepancy between these two times. An initial rough estimate considers the phase differences between the first two measured phase components and their target values

$$(t_a - t_b)_{\text{est}} = \frac{[\theta_{2,b}(t_b) - \theta_{2,a}] - [\theta_{1,b}(t_b) - \theta_{1,a}]}{2\pi(f_1 - f_2)}. \quad (1)$$

This estimate is refined by minimizing with respect to t_b the following error (where $\text{mod}_{2\pi}$ is the modulo with respect to 2π):

$$E(t_b) = \sum_{i=1}^{N} \left(\text{mod}_{2\pi}\left[\theta_{i,a} - \theta_{i,b}(t_b)\right]\right)^2. \quad (2)$$

For this algorithm we use the phase information at the carrier and its sidebands since these frequencies carry the most energy. Two primary advantages of this method are robustness and a time offset estimate that can be a fractional number of samples. The robustness derives from the use of the time-alignment method described above on a select set of frequencies so that noise presented at other frequencies is bypassed. The ability to find time offsets that are a fraction of the sampling period implies that the accuracy of the algorithm is not limited by the sampling rate.

IV. Features in Transient Response

With the time-alignment in hand, observation of the transient features of a signal can be studied. A typical reader–card transaction cycles through three possible states: the reader is transmitting, the card is responding, or neither the reader, nor the card is actively modulating the reader-generated carrier field. Between the reader inquiry and card response is a transitional stage that allows for synchronization and card charging. This is a fixed period of time defined by the governing ISO 14443 standard as the "frame delay time." A sample sequence of these three stages is shown in Fig. 2.

By modulating the ambient field, the reader and card change the signal from steady state. These transient changes differ depending on the particular card in the reader field. Key features in these transients allow identification of cards. One of these features is a phase delay introduced into the reader or card modulated signal between the start and end of a modulation pulse. Another is the variation in the shape of the envelope as it decays and rises during modulation.

A comparison of the envelope of the average reader inquiries and card responses for each of the four manufacturers studied is depicted in Fig. 4. We see that there are differences between cards during the reader inquiry despite an identical reader coil and command among all the measurements. These differences are a reflection of the coupled nature of the system. The inductive loop antennas and corresponding electronics of the card and reader affect the signal regardless of whether or not they are actively modulating the signal.

Fig. 4(a) and (b) illustrates different distinguishing features in the reader inquiry [see Fig. 4(a)] versus the card response [see Fig. 4(b)]. Features linked to transient effects such as ringing, phase shifts, and different rising and falling edge shapes are more pronounced in the reader inquiry because the modulation depth is greater. During the card response, the principle variations between cards are staggered rising/falling edges and even different modulation depths. When the rising and falling edges are offset, they are offset by the same amount, suggesting that the entire card response is delayed by a few carrier cycles and that the frame delay time varies among cards. In the ISO 14443 standard, the allowable frame delay tolerance is 400 ns.

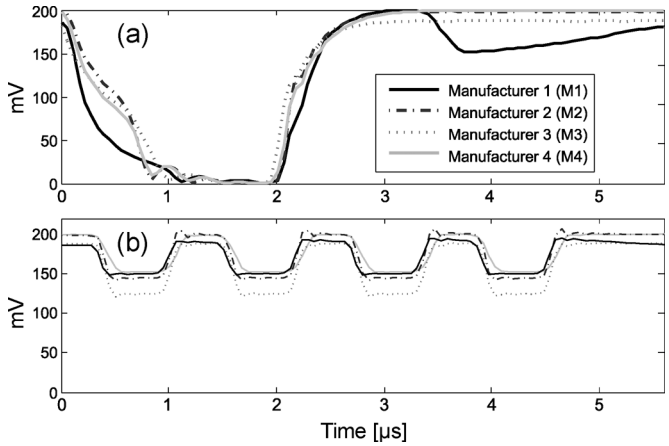


Fig. 4. Signal envelopes averaged over 50 measurements per manufacturer of the: (a) reader inquiry and the (b) card response.

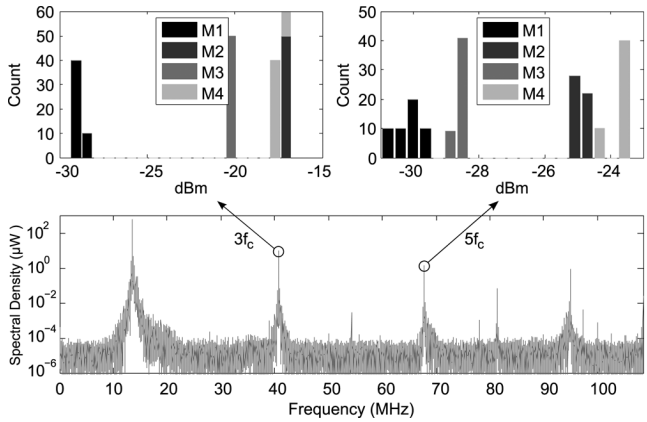


Fig. 5. Repeatability of spectral content measurements. The x-axis represents the magnitude of the frequency response at a particular frequency and the y-axis represents the measurement count for those magnitudes. Counts are represented as stacked bars: for example, in the top left figure, the counts at approximately -17 dBm should be read as 50 counts for manufacturer 2 (M2) and ten counts for manufacturer 4 (M4).

V. Features in Frequency Response

A. Magnitude and Phase of Key Frequencies

There are several signal features in the frequency domain that reproducibly and repeatably distinguish the four card manufacturers we studied. A typical Type A transaction has a great deal of spectral content, a result of the pulse modulation used to transmit data. Furthermore, this modulation is significantly different between the reader inquiry and card response: the reader inquiry contains single pulses per bit spaced at irregular intervals and the card response contains several sub carrier pulses during half of a transmitted bit.

We focus on frequencies having significant energy such as the carrier frequency, its harmonics, and associated sidebands. These frequencies are less susceptible to noise and offer repeatable and reproducible measurements. Our study of higher order harmonics is motivated by the possibility of examining unique nonlinear behavior, which is typically difficult to replicate or counterfeit.

Our time-alignment procedure provides a means to study the phase, as well as the magnitude of the frequency response. Of the higher energy frequencies that we studied, the odd carrier harmonics above the fundamental and associated sidebands contained the most energy and ability to distinguish manufacturers. Specifically, the third and fifth harmonics distinguished manufacturers in a very repeatable and reproducible manner. Fig. 5 demonstrates repeatability and card identification at the fifth harmonic for measurements taken within the same day. Binned counts of magnitude and phase measurements were well localized and offered distinct separation between manufacturers.

This localization and separation is reproducible over a time frame of half a year. In Fig. 6, three sets of 200 measurements taken over six months at two-month intervals illustrate that the distribution of binned counts of magnitude and phase measurements at the fifth harmonic changes little. However, the measurements of different manufacturers are not always clearly separated.

If we consider multiple features together, then the within manufacturer localization and between manufacturer sepeartion improves. In Fig. 7, we consider the energy at the third and fifth harmonic and observe that manufacturer measurements cluster around four distinct sample means. A simple classification

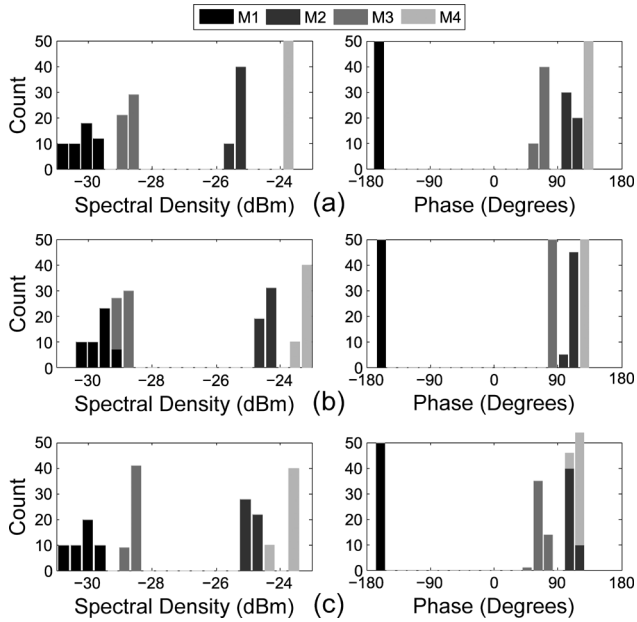


Fig. 6. Three experimental distributions of spectral data at the fifth carrier harmonic taken at two-month intervals demonstrate reproducibility. The left plots are the measured spectral density and right plots are the measured phase. (a) Dataset recorded in January. (b) Dataset recorded in March. (c) Dataset recorded in May of the same year.

scheme performs well: first, compute the sample means for each manufacturer; then, subsequently classify according to proximity to the calculated means. Each future measurement is classified to the manufacturer cluster whose distance between the measurement and the cluster mean is the smallest.

The effective classification boundaries of are illustrated in Fig. 7. We estimated the prediction error rate of this classification scheme by computing the manufacturers' cluster means on a randomly selected 80% subset of the entire dataset and predicting the manufacturer of the remaining 20% of the dataset. Repeating this process 500 times with different random subsets yielded no classification errors for this particular data set.

Our example is with a small feature set and on a small set of 20 cards. With a larger sample set of cards, the small margin

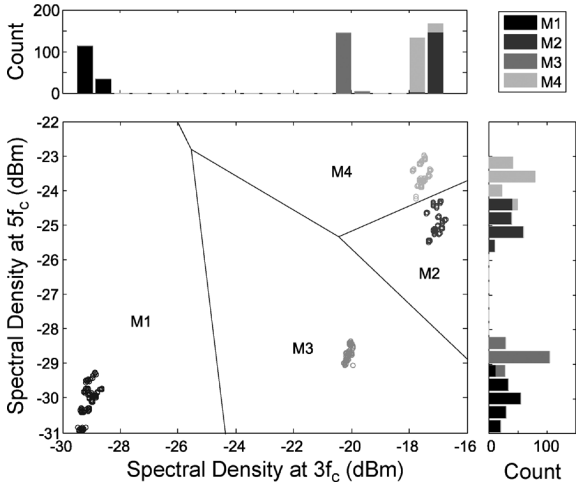


Fig. 7. Scatter plot of third and fifth harmonic magnitude measurements that demonstrates reproducibility over time and illustrates a method of identifying card manufacturers. Three groups of 200 measurements taken at two-month intervals are represented. The lines represent decision boundaries for classification based on proximity to the cluster mean of each manufacturer. The graphs on the top and side count the distribution of card measurements in each dimension.

between manufacturers two and four may lead to incorrect classification. The improvement of classification between one feature to two features suggests that with a higher dimensional feature set and more sophisiticated classifier, reliable classification could be achieve with a larger set of manufacturers and in more rugged measurement environments.

VI. Conclusion

We found that the presence of the card affects the signal at all times. As a result, analysis of both the card response and the reader inquiry provides a fertile ground for card identification. We also found that higher harmonics of the carrier frequency present better discrimination ability than the fundamental carrier frequency. Finally, we presented reasonable evidence that RFID card manufacturers can be distinguished automatically with our broadband measurement apparatus.

We have shown that there exists a minimal set of features that distinguishes cards. With an extended feature set and better classifiers, we hope to extend these results to the identification of cards within a certain model and identification in more rugged environments.

Acknowledgment

The authors thank T. Karygiannis, Information Technology Laboratory, National Institute of Standards and Technology (NIST), Gaithersburg, MD, as well as D. Novotny and D. Kuester, both with the Electromagnetics Divison, NIST, Boulder, CO, for technical advice.

References

[1] T. Kohno, A. Broido, and K. C. Claffy, "Remote physical device fingerprinting," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 2, pp. 93–108, Apr.–Jun. 2005.

[2] M. J. Riezenman, "Cellular security: Better, but foes still lurk," *IEEE Spectr.*, vol. 37, no. 6, pp. 39–42, Jun. 2000.

[3] J. Hall, M. Barbeau, and E. Kranakis, "Detecting 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.

[4] 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 *Proc. IEEE Signal Inf. Technol. Symp.*, 2005, pp. 484–488.

[5] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 2, pp. 381–394, Feb. 2006.

[6] S. C. G. Periaswamy, D. R. Thompson, and J. Di, "Fingerprinting RFID tags," *IEEE Trans. Dependable Secure Comput.*, submitted for publication.

[7] K. A. Remley, D. F. Williams, D. M. M.-P. Schreurs, G. Loglio, and A. Cidronali, "Phase detrending for multisine signals," in *61st ARFTG Conf. Dig.*, Spring, 2003, pp. 73–83.

Henry P. Romero received the B.S. degree in electrical engineering and applied mathematics from the University of Colorado at Boulder, in 2007, and is currently working toward the M.S. degree in applied mathematics at the University of Colorado at Boulder.

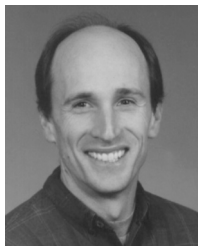
In 2007, he became a Research Assistant with the National Institute of Standards and Technology (NIST), Boulder, CO, where he has been studying methods of characterizing RFID cards from measurements of the electromagnetic fields.

Mr. Romero s a member of Eta Kappa Nu (HKN) and the Society of Industrial Applied Mathematicians (SIAM).

Kate A. Remley (S'92–M'99–SM'06) was born in Ann Arbor, MI. She received the Ph.D. degree in electrical and computer engineering from Oregon State University, Corvallis, in 1999.

From 1983 to 1992, she was a Broadcast Engineer in Eugene, OR. From 1989 to 1991, she was Chief Engineer of an AM/FM broadcast station. In 1999, she joined the Radio-Frequency Technology Division (now the Electromagnetics Division), National Institute of Standards and Technology (NIST), Boulder, CO, as an Electronics Engineer. Her research activities include metrology for wireless systems, characterizing the link between nonlinear circuits and system performance, and developing methods for improved radio communications for the public safety community.

Dr. Remley is editor-in-chief of the *IEEE Microwave Magazine*. She was the recipient of the Department of Commerce Bronze and Silver Medals and the Automatic RF Techniques Group (ARFTG) Best Paper Award.



Dylan F. Williams (M'80–SM'90–F'02) received the Ph.D. degree in electrical engineering from the University of California at Berkeley, in 1986.

In 1989, he joined the Electromagnetic Fields Division, National Institute of Standards and Technology (NIST), Boulder, CO, where he develops metrology for the characterization of monolithic microwave integrated circuits and electronic interconnects. He has authored or coauthored over 80 technical papers.

Dr. Williams is editor-in-chief of the IEEE Transactions on Microwave Theory and Techniques. He was the recipient of the Department of Commerce Bronze and Silver Medals, the Electrical Engineering Laboratory's Outstanding Paper Award, two ARFTG Best Paper Awards, the ARFTG Automated Measurements Technology Award, and the IEEE Morris E. Leeds Award.

Chih-Ming Wang received the Ph.D. degree in statistics from Colorado State University, Fort Collins, in 1978.

In 1988, he joined the Statistical Engineering Division, National Institute of Standards and Technology (NIST), Boulder, CO. He has authored or coauthored over 80 journal papers. His research interests include statistical metrology and the application of statistical methods to physical sciences.

Dr. Wang is a Fellow of the American Statistical Association (ASA). He was the recipient of the Department of Commerce Bronze Medals and several awards from the ASA.