FBAR-BASED SENSOR FOR WIRELESS RFID AUTHENTICATION OF INTEGRATED CIRCUITS

Anton A. Shkel, Matin Barekatain, and Eun Sok Kim
Department of Electrical Engineering-Electrophysics
University of Southern California, Los Angeles, California, USA

ABSTRACT

This paper describes an integrated circuit (IC) authentication and tamper detection system, based on a Film Bulk Acoustic Resonator (FBAR) and passive Radio-Frequency Identification (RFID), which allows for wireless detection of tampering or counterfeiting in packaged ICs. We demonstrate the concept through the use of a 2.6 GHz FBAR based on a Zinc Oxide (ZnO) thin film. The FBAR is series connected to a piezoelectric energy harvester, which can generate voltage pulses with a peak amplitude of 56 V when tampering activity is detected. Our measurements validate this concept and demonstrate that we can permanently alter the high frequency resonance characteristics of the FBAR through dielectric breakdown caused by tampering.

INTRODUCTION

Counterfeiting of ICs is a growing global problem, costing an estimated annual loss of $7.5 billion for US-based semiconductor companies alone [1]. Existing methods of assessing whether an IC is a counterfeit involve time-consuming imaging tests, electrical verification, or destructive testing. Additionally, existing authenticity verification methods cannot be applied on a bulk-scale.

IC-level tamper detection sensors have been proposed, for example with integrated photo-detectors [2], to destroy critical program information through detection of tampering activity, but these rely on power from the IC to function. The use of random number generators for generating cryptographic keys, such as those based on tamper-sensitive MEMS arrays [3], is another common counterfeit-prevention technique, however these are only helpful in preventing reverse-engineering and not sensitive to repackaging attempts by the counterfeiter.

In this paper we propose a system containing an embedded tamper sensor to allow for rapid wireless scanning of ICs to detect signs of tampering activity that has produced a permanent change to RFID tag. We demonstrate the wireless tamper detection concept through device fabrication, simulation and measurement.

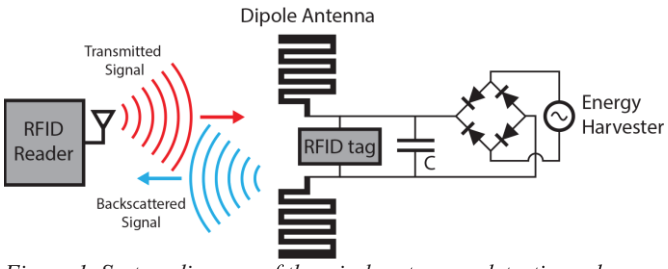


Figure 1. System diagram of the wireless tamper detection scheme. An external RFID reader transmits a sinusoidal signal and measures the backscattered signal strength from the tamper detection chip. The strength of the backscattered signal depends on the relationship of impedances between the RFID dipole antenna and series-connected FBAR. A piezoelectric energy harvester, connected to the FBAR via a rectifier and capacitor, generates a large voltage spike when a sufficient mechanical impulse is applied during the detaching process of the chip. This voltage spike will irreversibly break down the FBAR and permanently alter the characteristic of the backscattered signal.

DEVICE

A common technique employed by counterfeiters to remove an IC from a printed circuit board (PCB) involves raising the IC to an elevated temperature to melt the solder, and then striking the PCB with forceful impacts to remove the IC chip. The proposed system, illustrated in Figure 1, converts these impulses to large voltage pulses using a piezoelectric energy harvester, and irreversibly alters the spectral characteristic of an RFID tag. Such a system can be embedded within an IC package to passively detect tampering activity, and can be designed to be extremely difficult for counterfeiters to reverse the detection mechanism.

The main components of the RFID tag system are the RFID antenna, series-connected FBAR and energy harvester. The resonant frequency of the FBAR (that depends on the thicknesses of the layers) serves as the encoded ID of the tag. The RFID tag is designed to function passively, allowing the integrity of the chip to be assessed without any electrical connection, special configuration, precise alignment, or other measurement complexities that existing tamper detection mechanisms rely on.

Film Bulk Acoustic Resonator (FBAR)

The FBAR is designed such that it is permanently destroyed through dielectric breakdown when exposed to a large voltage. This breakdown will permanently alter the spectral characteristics of the FBAR, which results in an identifiable change in spectral shape of the interrogated signal.

The FBAR is fabricated on a silicon wafer coated with LPCVD Silicon Nitride (SiNx) (Figure 2a). The silicon nitride serves as an etch mask for KOH wet etching, which is used to open a window on the bottom of the wafer and to form a silicon nitride supporting diaphragm. After forming the diaphragm, a bottom electrode is deposited with 0.2 µm thick evaporated aluminum, and patterned. A piezoelectric ZnO layer is then deposited with RF sputtering such

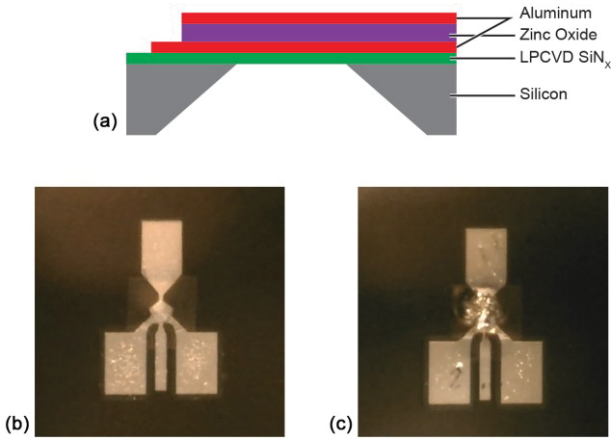


Figure 2. (a) Cross-section diagram of the FBAR device, which is composed of silicon nitride (SiNx), zinc oxide, and aluminum layers on a silicon wafer. (b) Photograph of the FBAR prior to tampering and (c) photograph of the same FBAR after permanent dielectric breakdown induced by tampering.

978-1-940470-03-0/HH2018/$25©2018TRF
DOI 10.31438/trf.hh2018.53

that the thickness is half of the wavelength of the target resonant frequency, for longitudinal waves travelling in bulk ZnO. In this study we target a resonant frequency of 2.6 GHz, which requires a ZnO layer with a thickness of about 0.54 µm. Finally, an aluminum top electrode is deposited and is patterned along with ZnO. The active portion of the resonator, which sits on the supporting diaphragm, has a pentagonal shape in the lateral plane to minimize the lateral resonances and spurious modes. A top view photograph of a completed FBAR is shown in Figure 2b.

The breakdown voltage of the FBAR is determined by the thickness of the FBAR's ZnO layer. For a more sensitive FBAR device that is easier to force into breakdown, it is necessary to increase the interrogation frequency, which limits the interrogation distance and may increase hardware complexity of the interrogator. The top-down photograph of the device after the dielectric breakdown of ZnO is shown in Figure 2c.

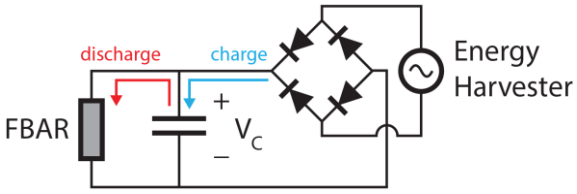


Figure 3. Diagram showing the charging and discharging paths of the energy harvester. An additional capacitor is required to ensure that a sufficient current is developed to permanently breakdown the FBAR and to leverage multiple impacts.

The FBAR is connected with the energy harvester through a full-wave rectifier to ensure a fixed polarity of the potential developed across the FBAR (Figure 3). A capacitor is necessary to accumulate sufficient charge to induce permanent breakdown in the FBAR. This threshold charge was experimentally determined to be a minimum of about 12 µC for a 2.6 GHz FBAR with a minimum threshold voltage applied (5 V). During tampering activity, multiple impacts may be used to remove the IC, so such a capacitor can leverage the multiple voltage peaks generated by the energy harvester to meet the current threshold. The capacitor cannot be too large, however, since the time for charging to the threshold voltage would be too long and also because a large capacitance would complicate impedance matching with the antenna.

We characterized the breakdown of an FBAR with a ZnO thin-film thickness of 0.54 µm with an experimental setup consisting of a Rigol DM3058 for current measurement and a Rigol DP831A for voltage sweeping with a current limit of 2 mA. The breakdown measurements are performed by ramping the applied voltage from zero to 20 V, with sufficient time given at each measurement for the current to stabilize. The results of sweeping the applied voltage and observing the current through a single FBAR are plotted in Figure 4, with error bars indicating the range of leakage currents observed over a period of about 30 seconds.

We can see that dielectric breakdown occurs when about 5 V is applied to the FBAR. Prior to reaching this point, the voltage sweep can be repeated with identical results. Once the breakdown condition of 5 V is reached, the current drawn through the FBAR is consistently elevated above previous low voltage measurements, and the DC resistance drops permanently by about 30 times. But with the current limit from the source, the breakdown does not cause a thermal run away, and the DC resistance increases as the applied voltage is increased until 13 V, at which point we observe a permanent delamination of the electrodes from the FBAR, and the FBAR behaves like an open circuit. This characteristic is repeatably observed in FBARs on a single wafer, but varies with ZnO thickness and quality from batch to batch.

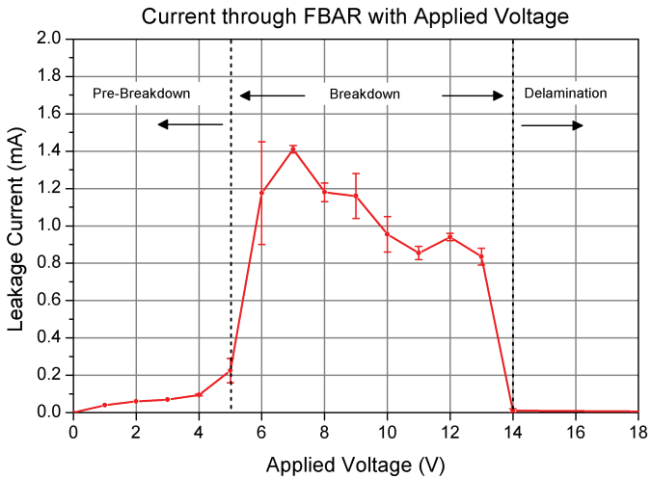


Figure 4. Measured characterization of FBAR breakdown as a function of applied voltage for a Zinc Oxide thickness of 0.54 µm. Breakdown occurs in two phases, with dielectric breakdown occurring at 5 V, and delamination of the metal layer occurring at 13 V. Time-dependent dielectric breakdown occurs in the region between 5 V and 13 V, with delamination occurring given sufficient exposure time.

The breakdown characteristic of the FBAR is time-dependent, consistent with other time-dependent dielectric breakdown mechanisms, such as those in the gate oxide of MOSFETs [4]. This time-dependency can create a breakdown and even delamination at low voltages when exposed over long periods of time, which was observed in 2.6 GHz FBARs when 2 V was applied over a 1 to 2 minute period. In the context of tamper detection, this is not a dependable breakdown mechanism, since pulses supplied by a piezoelectric energy harvester will be short in duration.

The output of piezoelectric energy harvesters is primarily characterized by high voltage and low current. For this reason, we also characterize the breakdown curve as a function of time after applying a voltage step from zero to 20 V (Figure 5). The peak current of 0.141 mA flows through the FBAR, and the current lasts for about 25 ms before the electrodes are delaminated. Integrating this pulse indicates that a total charge of about 1.76 µC is necessary for the FBAR breakdown with a 20 V potential. The total charge necessary for breakdown increases with a reduced voltage peak, and design of a high-voltage output piezoelectric energy harvester is more practical than optimizing current output at low peak voltages.

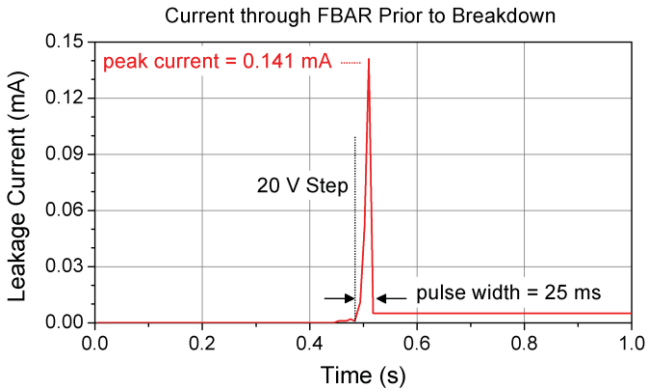


Figure 5. Measured current through FBAR under a step function with a 20 V DC voltage applied. The FBAR draws a current with a peak of 0.141 mA for a duration of 25 ms before permanent breakdown (delamination).

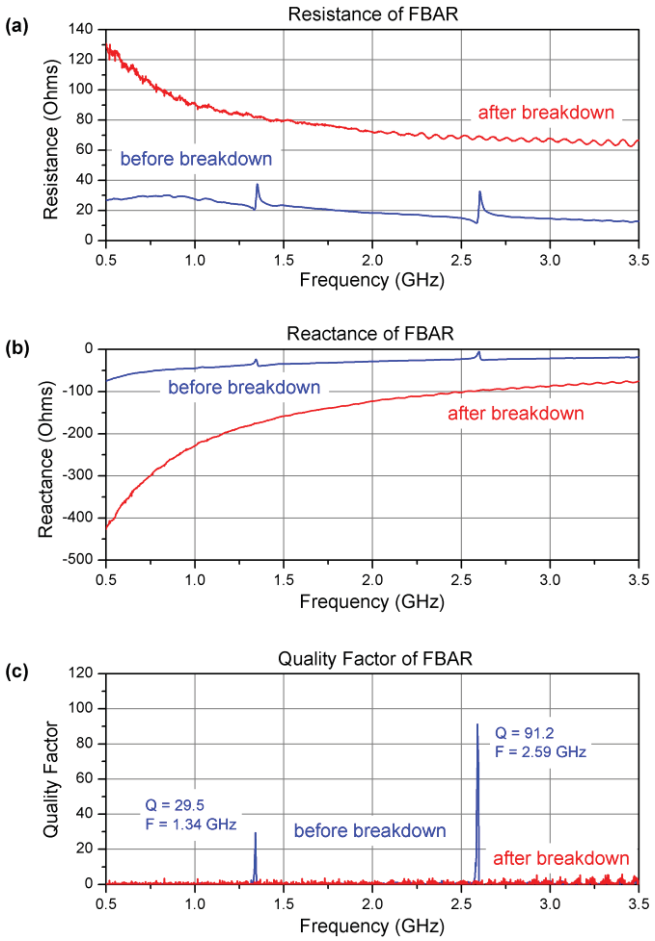


Figure 6. Measured (a) FBAR resistance, (b) FBAR reactance, and (c) estimated quality factor before and after the breakdown of the FBAR, showing a destruction of resonance effects due to tampering.

The high frequency electrical properties of the FBAR are characterized (Figure 6), and the FBAR is measured to have a resonant frequency of 1.34 GHz with a quality factor of 29.5 at the first peak, and a resonant frequency of 2.59 GHz with a quality factor of 91.2 at the secondary peak. After breakdown, the resistance of the FBAR is increased at high frequencies, and the capacitance is reduced.

RFID Antenna

We designed a meandering dipole RFID antenna (Figure 7a) and simulated its electromagnetic characteristics with the SONNET software suite (Figure 7b), to ensure a complementary impedance

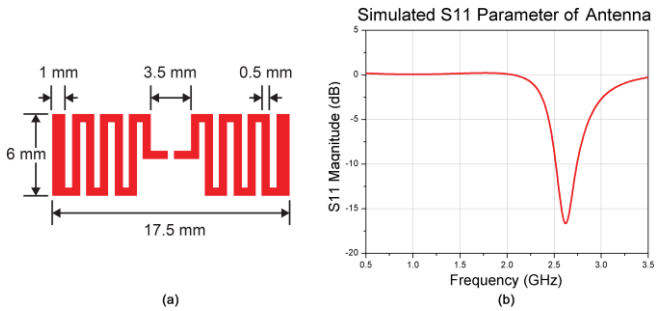
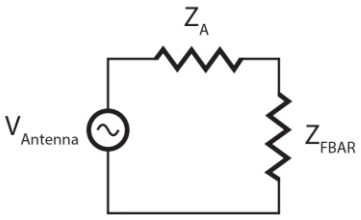


Figure 7. (a) Diagram illustrating the meandering dipole design of the RFID antenna with key dimensions. (b) Simulated S11 parameter of the RFID antenna.



$$P_{re-radiated}=KP_AG$$

$$K=\frac{4R_A^2}{|Z_A+Z_{FBAR}|^2}$$

Figure 8. Circuit diagram showing the method of estimating the backscattered signal power. The re-radiated power is a function of the backscatter coefficient K and the antenna gain G. K is the relative strength of the backscattered power as a function of the antenna impedance and FBAR impedance.

and a matched antenna resonant frequency of 2.6 GHz. To further reduce the dimensions of such a dipole antenna to fit within an IC package, additional meandering can be introduced into the design, for example with spiral loop geometries or fractal geometries [5]. The antenna impedance with this design is primarily capacitive, but can be made more inductive by using T-matching. An alternative antenna design is an inductive loop-based tag, which will provide better impedance matching to the FBAR, but reduce the overall range of the RFID antenna to near-contact.

We estimate the backscattered signal strength using the circuit model shown in Figure 8. From the given expression, we see that the power of the re-radiated signal is dependent on the gain of the antenna, and the backscatter coefficient K. The backscatter coefficient is a function of the antenna impedance and FBAR impedance, with a maximum value achieved when the two are complex conjugates. The estimated impedance of the antenna is obtained from a software simulation, and is applied to the expression along with the measured FBAR parameters to estimate the backscatter coefficient before and after breakdown of the FBAR, shown in Figure 9.

The tag ID in this system is encoded in the spectral signature of the re-radiated signal. Figure 9 shows that the original backscattered signal will have two closely-spaced peaks at 2.59 GHz and 2.70 GHz when the FBAR and antenna are designed to have overlapping frequencies. After the breakdown, the FBAR no longer exhibits high-Q resonance, and the overall capacitance increases. This increases the impedance mismatch between the FBAR and RFID antenna, creating a low-Q peak with a center frequency shifted to 3.04 GHz, and an 11 times weaker maximum backscattered power.

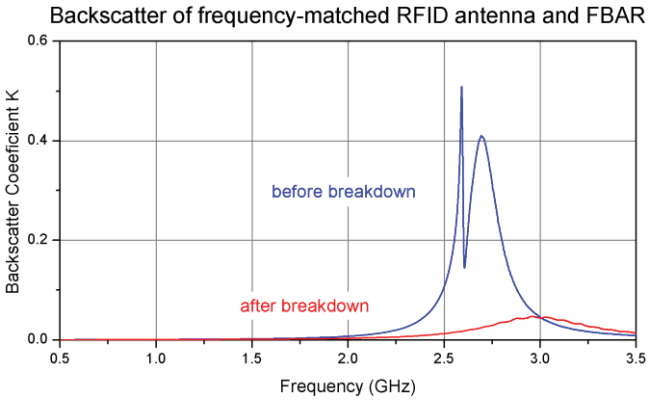


Figure 9. Estimated backscatter coefficient K based on the simulated RFID antenna impedance and measured FBAR impedances before and after the breakdown of the FBAR.

This change in spectral signature can be identified with three receiver measurements of backscattered signal intensity at 2.59 GHz, 2.70 GHz, and the local minimum between them at 2.61 GHz. Common passive RFID interrogators function with tag IDs embedded within time-varying backscattered signals, which are typically implemented with surface acoustic wave (SAW) reflectors or active circuits. However for this application, since the spectral characteristics of the backscattered signal are the coded information that is detected, the RFID interrogator must be implemented to read frequency-encoded tags. Such an encoding scheme has been demonstrated to be effectively interrogated with ultra-wideband pulses [6] and frequency-tunable RFID readers [7].

Energy Harvester

The tamper detection system can be built with an energy harvester based on a piezoelectric PZT bimorph cantilever, fabricated with two bulk PZT layers separated with a spun-on adhesive layer (Figure 10). The energy harvester has dimensions of 11 mm x 1 mm x 0.6 mm, which can be further reduced to fit within a given IC package. With this device, an open circuit voltage of about 2.97 V is measured when 2.6 g acceleration is applied. Since impact pulses of about 50 g are applied during tampering activity, we estimate that the energy harvester will generate about 56 V during the tampering. Since only 5 V is necessary to cause irreversible breakdown of the 2.6 GHz FBAR, there is a sufficient margin for the energy harvester with a similar bimorph geometry to be miniaturized to a such level to be incorporated into IC package. If the generated voltage and current is sufficiently large, the circuit shown in Figure 3 may not be necessary.

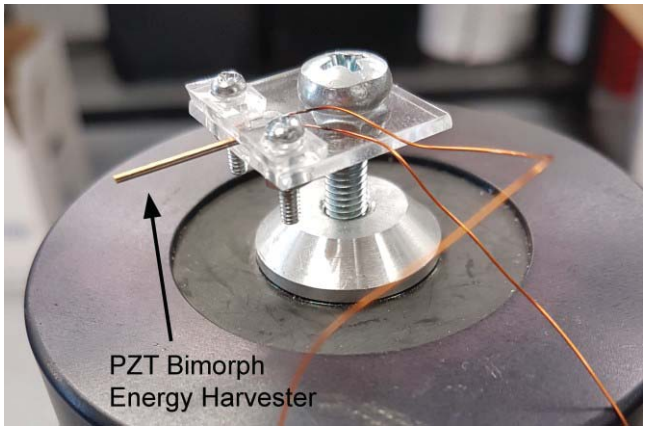


Figure 10. Photograph a bimorph cantilever, clamping system, and shaker. The cantilever has total dimensions of 11 mm x 1 mm x 0.6 mm. Such a cantilever can generate an open circuit voltage of approximately 56 V due to tampering activity.

DISCUSSION

As future work, we aim to integrate this system with a microfabricated energy harvester, such that the entire system can be embedded within a typical IC package. This can be supported by increasing the FBAR resonant frequency to 5 GHz, which would reduce the ZnO thickness of the FBAR and lower the necessary breakdown voltage to about 3 V. This would allow us to relax the constraints on the energy harvester design and further miniaturize the energy harvester. Operating at a higher frequency would also allow miniaturization of the antenna, with the disadvantage of reducing the range for wireless interrogation.

This tamper detection scheme has an advantage over other anti-counterfeiting measures, in that FBAR's exact resonant frequency (which depends on the ZnO thickness) must be known (down to parts-per-thousand level for Q of 1,000) for a counterfeiter to roll-back or duplicate that tamper detection system after the permanent breakdown. Once a tamper detection system is destroyed, the exact resonant frequency cannot be recovered, since ZnO thickness variation over a wafer is typically more than 1%.

A similar tamper detection system could also be implemented with a SAW-based device. Since the resonance frequency of a SAW filter is determined by the spacing of interdigitated electrodes, dielectric breakdown will permanently destroy all surface patterns. Use of SAW filters will also allow integration of reflectors to enable temporally-encoded tag IDs [8].

CONCLUSION

These simulations and measurements are a promising preliminary demonstration of the approach of using dielectric breakdown of FBAR structures for tamper detection in the IC supply chain. Such a detection scheme can be similarly applied for wireless detection of damage during package handling and shipping, and other impact detection applications. The use of this tamper-detection mechanism can also be easily integrated with existing anti-counterfeit measures, such as obfuscation, for more complete protection against many types of attackers.

ACKNOWLEDGEMENT

This work is supported by National Science Foundation under grant CNS-1716953 and Semiconductor Research Consortium under contract 2017-TS-2771.

REFERENCES

[1] F. Koushanfar, et al., "Can EDA Combat the Rise of Electronic Counterfeiting?", Design Automation Conference (DAC) 2012, San Francisco, CA, (2012), pp. 133-138.

[2] D. Shahrjerdi, et al., "Shielding and securing integrated circuits with sensors", Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, 2014.

[3] J. English, et al., "MEMS-assisted cryptography for CPI protection", IEEE Security & Privacy, (2007).

[4] C.H. Ho, S.Y. Kim, and K. Roy. "Ultra-thin dielectric breakdown in devices and circuits: A brief review.", Microelectronics Reliability 55.2, (2015), pp. 308-317.

[5] G. Marrocco, "The art of UHF RFID antenna design: Impedance-matching and size-reduction techniques", IEEE antennas and propagation magazine, 50.1, 2008.

[6] P. Kalansuriya, N.C. Karmakar, and E. Viterbo, "On the detection of frequency-spectra-based chipless RFID using UWB impulsed interrogation", IEEE Transactions on Microwave Theory and Techniques, (2012).

[7] S. Preradovic, and N.C. Karmakar, "Multiresonator based chipless RFID tag and dedicated RFID reader." Microwave Symposium Digest, 2010.

[8] V. P. Plessky, and L. M. Reindl, "Review on SAW RFID tags", IEEE transactions on ultrasonics, ferroelectrics, and frequency control 57.3, 2010.

CONTACT

*A.A. Shkel, tel: +1-949-394-9040; shkel@usc.edu