A WIRELESS RF AND DC INTERFACE FOR A MEMS-BASED IDENTIFICATION SYSTEM

Joshua D. Cross[1*], John L. Schneiter[1], Grant A. Leiby[2], Steven McCarter[2], Jeremiah Smith[2], and Thomas P. Budka[2]
[1]Cerberex Technologies, Inc. (dba Veratag), Ithaca, NY USA
[2]RF Diagnostics, LLC, Niskayuna, NY USA

Abstract: We describe a wireless system for actuating and detecting the motion of MHz-frequency, low dissipation MEMS resonators. The overall system is essentially a custom-designed RFID-like system, with the tags based upon unique MEMS chips as opposed to conventional RFID chips. The MEMS devices are vacuum encapsulated, rugged, CMOS-compatible, and are approximately 1mm-by-1mm-by-0.5mm. The system is passive in the sense that the DC voltage required to bias the MEMS resonators is scavenged from a UHF signal through the use of an on-tag RF-DC converter. The purpose of the system is to use the unique frequency spectrum of each MEMS-based chip to uniquely identify the chips.

Keywords: MEMS, RFID, identification, power scavenging, vacuum encapsulated

INTRODUCTION

Over the past few years, wireless systems such as RFID and near field communication (NFC) systems have proliferated across a variety of industries and areas of use [1]. Applications for RFID and similar systems include door access, credit card and debit point-of-sale payments, passports, supply chain management, and pharmaceutical anti-counterfeiting. Some of these wireless applications require only an identification number – a wireless barcode to increase efficiency – but others require security to protect personal information and privacy. All systems typically must provide a significant value added for a minimum of cost and with minimal impact to existing infrastructure.

We describe a wireless identification system based upon the resonance frequencies of MEMS resonators. The system – a reader and the associated MEMS-based identification chips – takes advantage of the high frequency and quality factor of MEMS resonators to make attacking the system through frequency reproduction or playback challenging. Additionally, the frequency spectra of MEMS resonators are measurably unique due to fabrication variation, which essentially renders each MEMS chip unique. Thus, the chips act like a biometric token that can be used in a variety of applications.

Herein, we give a general overview of the operation of the system, present the customized reader, and discuss the wireless interface used for rf actuation of the resonators and dc scavenging from a UHF frequency source.

EXPERIMENTAL

We describe the wireless system in terms of its three principle components: the MEMS chips, the reader, and the wireless interface. A schematic of the overall system is shown in Figure 1.

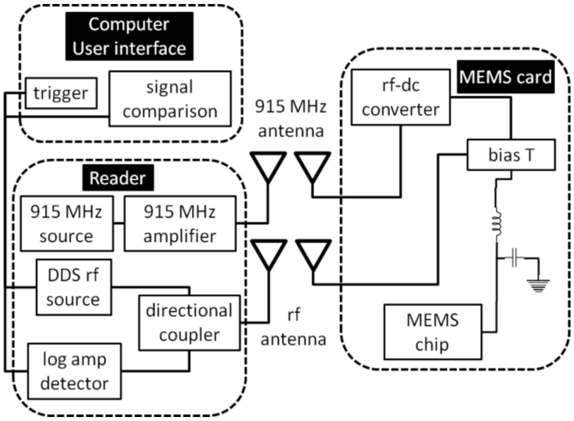

Figure 1: A schematic diagram of the identification system. The main components of the system are the computer user interface, the reader, and the MEMS prototype card.

MEMS chips from both Cornell University Nanoscale Science and Technology Facility (CNF) and Silicon Clocks, Inc. (Fremont, CA) have been successfully fabricated and tested. Chips from the CNF were fabricated by the authors, while those from Silicon Clocks, Inc. were purchased as bare die. CNF chips required vacuum encapsulation, which was performed at Integrated Sensing Systems, Inc. (ISSYS, Ypsilanti, MI). MEMS chips fabricated at the CNF are typically based upon polycrystalline silicon cantilever resonators with frequencies around 4.5

MHz, quality factors around 5,000, and with between 1 and 50 resonators. Chips from Silicon Clocks, Inc. are single resonator devices with frequencies of about 11 MHz and quality factors around 30,000.

MEMS resonators exhibit measurably different frequencies due to fabrication variability. Fundamentally, at least both mass and local stress variability cause frequency variability. We have measured hundreds of devices fabricated from a variety of films, in a variety of geometries, and from a variety of fabrication facilities. All devices exhibit frequency variability (deviation from the nominal design frequency) of at least 0.25% (assuming a normal distribution about a mean and calculated at 99% confidence intervals), and most are closer to 1% or higher. A summary of variability results for 15 sets of resonators is shown in Figure 2.

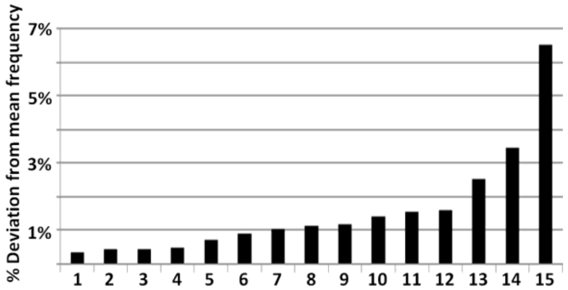

Figure 2: Frequency variability around a nominal design frequency for 15 different sets of MEMS resonators from a variety of foundries and with different design characteristics.

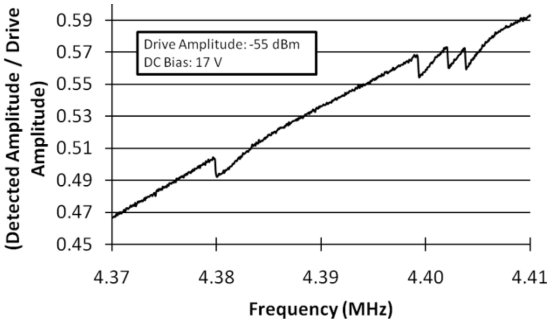

Figure 3: A response curve for a MEMS chip with 4 cantilever devices. The sloping background is due to the impedance matching circuit.

MEMS chips are driven and detected using capacitive coupling between the resonator and a fixed electrode (usually the substrate wafer). It is possible to detect resonator motion without the need for signal amplification or frequency conversion by efficiently impedance matching the MEMS resonators to the overall system impedance (50 Ω) [2]. Impedance matching is achieved with a single inductor-capacitor tank circuit. An example of the frequency spectrum of a CNF MEMS chip with four cantilever resonators is shown in Figure 3.

A PCB is used to hold the MEMS chip, the bias tee, the rf-dc conversion circuit (primarily consisting of an Avago quad ring diode HSMS-280R), and both the rf and UHF antennas. An unpopulated PCB is shown in the photograph of Figure 4. This PCB assembly is referred to as a MEMS card. The MEMS card mimics the form factor of RFID-enabled credit cards and door access cards for demonstration purposes.

The reader is essentially a custom designed reflection mode scalar network analyzer. A computer system is used as a user interface to the reader, a data storage system, and a signal comparison engine. A trigger signal from the computer synchronizes the drive frequency sweep and the logarithmic amplifier detector. The frequency source is an Analog Devices direct digital synthesis chip (AD9852ASVZ) and the detector is an Analog Devices logarithmic amplifier (AD8309). Also in the reader is a UHF VCO source (Minicircuits ZX95-924-S+) that operates at 915 MHz. This is used as a source signal for rf-dc conversion on the MEMS card (Figure 4).

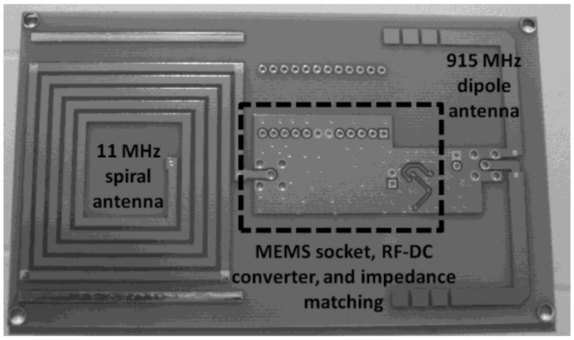

Figure 4: A photograph of the prototype MEMS card.

There are two matched antenna sets required for the wireless interface between the MEMS card and the reader. One antenna set is based upon a spiral antenna geometry that is optimized for operation around the resonance frequency of the MEMS chips (11 MHz for most devices). The 11 MHz spiral antenna is used for the primary (rf) component of the drive and detection. Another antenna set is used for a 915 MHz signal. This signal is used solely as a means of dc-biasing the MEMS chip after it has been converted to dc by an rf-dc conversion circuit on the MEMS card. The 915 MHz antennas are matched dipole antennas, and the transmission efficiency is shown in Figure 5. A Zener diode is used to limit the output dc voltage from the rf-dc conversion circuit to around 15 V.

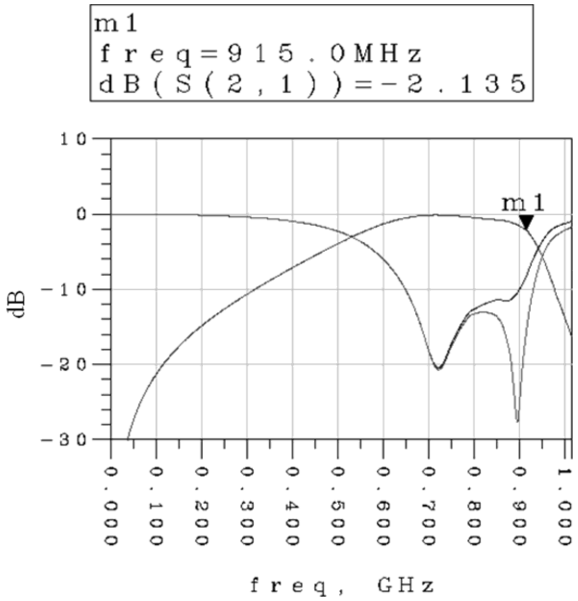

Figure 5: Simulated transmission performance of the 915 MHz dipole antenna used for rf-dc conversion for dc bias of the MEMS chip. "m1" marker is at 915 MHz and shows about 2 dB of loss for a few centimeters of spacing.

DISCUSSION

The system that we have described above operates essentially the same way that a standard RFID system operates [1]. The system is markedly different from a conventional RFID system in that a MEMS chip is used to convey information as opposed to a RAM or ROM-based chip. Also, there is the need to dc-bias the MEMS chips. Note that we have addressed the dc-bias issue through scavenging and conversion of an ambient UHF signal. In this respect, this system is similar to a passive RFID system in that no on-card battery is implemented.

A screenshot from the controlling computer is shown in Figure 6 (with inset of scanning electron micrograph of the actual MEMS devices). In the top portion of Figure 6 the amplitude and frequency data from a MEMS card interrogation are shown. At the bottom of Figure 6 one sees the data condensed into a bar code-like format for comparison against the converted frequency spectra of other MEMS cards. In the simplest implementation of the system, the frequencies and the widths of the MEMS resonator peaks are used to generate the bar code. In a typical identification or authentication application, one would perform the bar code comparison to issue or not to issue a security token (for instance, to grant access to a door).

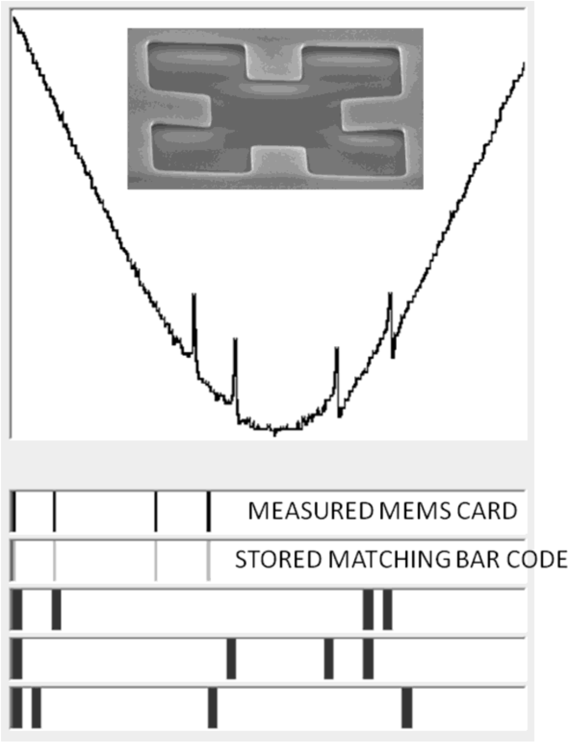

Figure 6: Screenshot from the computer interface with inset of scanning electron micrograph of a typical CNF cantilever device (top). At bottom are shown the barcodes rendered from the spectra for comparison.

The most important aspect of the system with respect to overall signal amplitude of the MEMS resonators is the ability to impedance match between the large effective impedance of the MEMS resonators and the system impedance (50 Ω) [2]. The MEMS resonators manufactured at the CNF, and indeed most flexural MEMS or NEMS resonators, have impedances greater than 100 kΩ [2-5]. The impedance mismatch results in substantially all of the drive signal being reflected from the MEMS devices. Impedance matching can be used to overcome this hurdle, as we have done, but there are limits to achieving an ideal match. The most substantial challenge for us is that the test package, a 24-pin dual in-line package, exhibits a capacitance of approximately 5pF, whereas the effective motional capacitance of the typical resonator is on the order of 10^{-18} Farads, while the gate capacitance is on the order of 500^{-18} Farads. Thus, the 24-pin package represents a huge parasitic capacitance that highly degrades the measurable signal. We are currently revising the MEMS card to eliminate the 24-pin package. We should note that the MEMS chips from Silicon Clocks have much lower motional impedance than do the CNF chips and the impedance matching is significantly better when those chips are employed in the system.

Coupling efficiency between the reader and the MEMS card antennas is also important for optimizing the detected signal amplitude. We generally have not optimized the antenna geometry. As shown in Figure 5, the 915 MHz dipole antenna exhibits approximately 2 dB of loss for an antenna spacing of a few centimeters. Though not ideal, this is acceptable in the current system. We are currently working to reduce this loss and also to achieve a more rotationally symmetric geometry for the 915 MHz dipole antenna by making it a spiral geometry nested within the 11 MHz spiral antenna.

CONCLUSION

We have described a system to be used for identification applications that is based upon a custom, RFID-like reader that wirelessly drives and detects the resonance of MEMS resonators on chips on a prototype PCB card. MEMS resonators, in general, require a dc bias voltage to operate effectively, and we have incorporated a 915 MHz frequency source, from which to convert rf to dc, as a means of passively providing the dc bias. MEMS chips in the prototype system have been fabricated locally, and we have also used commercially available MEMS chips, both of which exhibit frequency variability sufficient to uniquely identify every resonator.

This system is presented as a prototype system for use in identification or authentication applications. As high security, low cost, and simplicity are often required for such systems in real world environments, the system we have described would be very suitable in a number of application areas [1]. The system described herein is highly scalable to include more features of the MEMS resonators. For instance, while the system presented uses essentially only the frequency and bandwidth of each resonator for identification, one could easily include the amplitude, phase, and non-linear behavior of the resonators. Additionally, with modifications to the reader, challenge-and-response types of interactions are possible, making the system potentially highly robust against those that might attempt to attack the system.

ACKNOWLEDGEMENTS

Support and technical assistance for this work is provided by the NSF (grant: IIP-0823009), the Cornell NanoScale Science and Technology Facility (CNF), the Cornell Center for Nanoscale Systems (CNS), the Cornell Center for Materials Research (CCMR), the Cornell Nanobiotechnology Center (NBTC), and Silicon Clocks, Inc.

REFERENCES

[1] Finkenzeller K 2003 *RFID Handbook, 2nd ed.* (Wiley)

[2] Truitt P A, Hertzberg J B, Huang C C, Ekinci K L, Schwab K C 2007 Efficient and Sensitive Capacitive Readout of Nanomechanical Resonator Arrays *Nano Letters* **1** 120-126

[3] Lopez J L, Verd J, Uranga A, Giner J, Murillo G, Torres F, Abadal G, Barniol N 2009 A CMOS-MEMS RF-Tunable Bandpass Filter Based on Two High-Q 22-MHz Polysilicon Clamped-Clamped Beam Resonators *IEEE Electron Device Letters* **30** 718-720

[4] Li M, Tang H X, Roukes M L 2007 Ultra-sensitive NEMS-based cantilevers for sensing, scanned probe and very high-frequency applications *Nature Nanotechnology* **2** 114-120

[5] Zalalutdinov M, Cross J, Baldwin J, Ilic B, Zhou W, Houston B, Parpia J CMOS integrated RF MEMS resonators *Journal of Microelectromechanical Systems* submitted for publication September 2009