IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 17, 2019, accepted July 1, 2019, date of publication July 5, 2019, date of current version July 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2927084

Vulnerability of MEMS Gyroscopes to Targeted Acoustic Attacks

SHADI KHAZAALEH, GEORGIOS KORRES, MOHAMMED EID, MAHMOUD RASRAS, AND MOHAMMED F. DAQAQ

Division of Engineering, New York University, Abu Dhabi 129188, United Arab Emirates

Corresponding author: Mohammed F. Daqaq (mfd6@nyu.edu)

This work was supported by NYUAD.

ABSTRACT The goal of this paper is to assess the vulnerability of MEMS-based gyroscopes to targeted ultrasonic attacks. Towards this objective, a surface micromachined planar MEMS gyroscope is fixed in space and subjected to ultrasonic waves with frequencies near its driving frequency. The ultrasonic input is shown to produce deceptive low-frequency angular velocity readings in the yaw direction. Using physics-based mathematical model of the gyroscope, it is shown that the misalignment between the sensing and driving axes of the gyroscope is the main culprit behind the vulnerability of the gyroscope to ultrasonic attacks. It is also concluded that ultrasonic attacks on MEMS gyroscopes can impose high-security risks. In addition to the attack being barely audible, the resulting deceptive angular velocity signals have a very low frequency content which cannot be attenuated by adding a low-pass filter. Furthermore, the current approach implemented to eliminate unwanted vibrations from the output signal of the MEMS gyroscopes by using an identical proof mass to perform differential measurements is clearly ineffective in shielding the gyroscope from ultrasonic attacks. As such, new measures have to be taken to protect MEMS gyroscopes from targeted acoustic attacks.

INDEX TERMS Acoustic attack, gyroscope, MEMS, security.

I. INTRODUCTION

Due to their small size, very low-power consumption, and easy fabrication in large arrays, micro-electromechanical systems (MEMS) are widely utilized in a variety of domains. This includes, but not limited to, the medical, automotive, aerospace, and the consumer market fields. Spoofing such devices with external attacks could severely damage their integrity. While considerable research has explored the security of MEMS from a system-level perspective; e.g. software, networking, and sensor fusion; the devices themselves remain largely vulnerable to attacks targeting the hardware. This vulnerability can lead to catastrophic failures when a malicious third party attempts to spoof the hardware functionality [1]–[3].

In recent years, it has been reported that some MEMS devices are particularly vulnerable to targeted acoustic attacks. For instance, it has been shown that the output of the MEMS device can be corrupted by a noise signal with frequency matching the natural frequency of the sensor or via acoustic noise [4]. More recently, two studies illustrated that the output of a MEMS device can be biased and controlled using a carefully-designed ultrasonic wave [5], [6]. In particular, it was demonstrated experimentally that, a devised ultrasonic wave which possesses the right intensity and frequency content can maliciously couple to the mechanical part of a MEMS device forcing it to move and produce deceptive signals. This can be used by attackers to trigger an airbag system, force a drone to make an undesired maneuver, or make a chemical sensor provide false radiation readings in a nuclear power plant.

Typically, resonator-type MEMS with high Q-factors are most susceptible to external acoustic attacks. While a high Q-factor makes the device highly sensitive and minimizes power consumption [7], [8], it also makes the system vulnerable to minute vibratory excitations in the vicinity of its resonant frequency. MEMS gyroscopes fall under the category of resonator devices; hence, they can be vulnerable to frequency-matching excitations, namely of the acoustic type. As such, few research studies were carried out in recent years to assess the performance of the gyroscope in acoustically-harsh environments [9], [10]. Results have

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

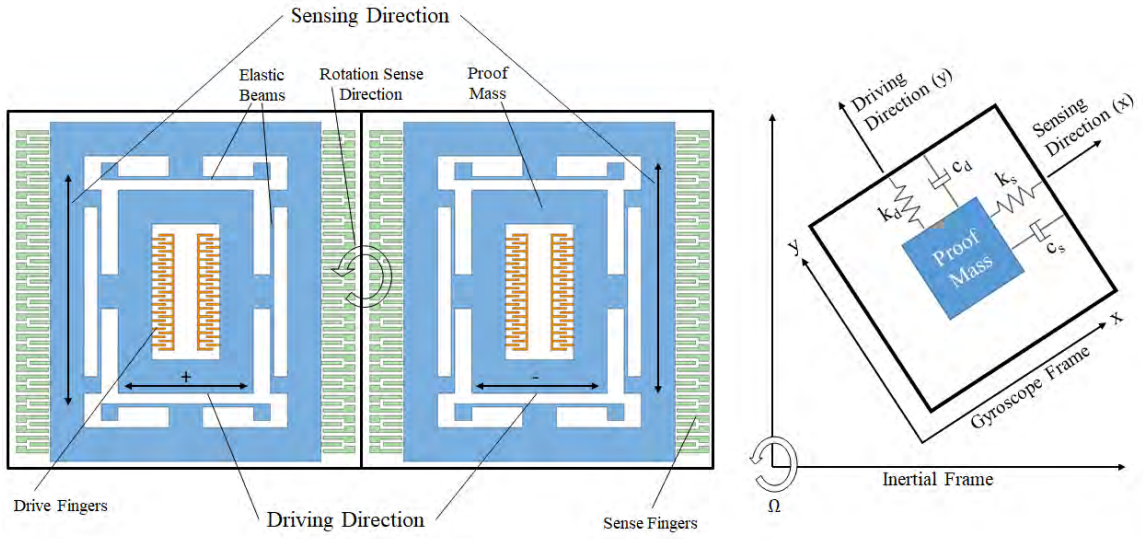

FIGURE 1. A schematic illustration of the mechanical structure of a MEMS gyroscope showing the basic mechanical components [13]–[15].

shown degradation and corruption of the angular velocity measurements in the presence of high power acoustic noise. It was also shown that it is possible to utilize acoustic attacks to manipulate gyroscopic sensors by generating undesirable readings. This imposes serious security risks such as information leak (eavesdropping) or incapacitating flying drones [6], [11], [12].

While all of the research in the open literature focuses on demonstrating the feasibility of acoustic attacks on real-world consumer devices, very little attention has been paid to understanding the main sources of this vulnerability. In particular, as of today, there are no models to capture the behavior of the gyroscope under acoustic attacks. Thus, we still do not understand how the output readings are influenced by the core mechanical and electrical components of the gyroscope.

To fill this knowledge gap, we investigate the vulnerability of a MEMS-based gyroscope to acoustic attacks and propose a theoretical model to understand the sources of vulnerability. We start in section II by providing the basic description of the operation principle of a MEMS gyroscope which is essential towards delineating the influence of the acoustic waves on the device's response. In section III, we perform several experiments on an Analog Devices (ADXRS624) gyroscope, and use the results to show that a stationary gyroscope may generate an angular velocity reading when subjected to acoustic signals at its driving frequency. The magnitude of the resulting deceptive readings is maximized at a specific orientation of the gyroscope with respect to the sound source. In section IV, we analyze the results and show that, although gyroscopes have high resonance frequencies (usually larger than 14 kHz), the generated false output occurs at very low frequencies (0.5 - 190 Hz). We explain that the low-frequency output is a result of the demodulation typically implemented in the readout circuit. This low-frequency output renders the gyroscope more susceptible to acoustic interferences since it cannot be easily attenuated by implementing internal or external low-pass filters. In section V, we develop a physics-based qualitative theoretical model, which shows that the misalignment between the driving and sensing axes of the mechanical sensing structure is the main culprit for the false readings. Finally, in section VI we present the main conclusions and suggest some techniques to mitigate the acoustic attacks.

II. OPERATION PRINCIPLE

A MEMS gyroscope is a simple device used to measure the angular rate of rotation of rigid bodies. As shown in Fig. 1, it consists of a proof mass connected through elastic beams to a fixed support. The proof mass is allowed to move in two orthogonal directions, x and y, also known, respectively, as the sensing and driving directions of the gyroscope. During operation, electrostatic combs apply an alternating electrostatic excitation, $y(t)$, to the proof mass forcing it to move continuously in the y-direction. As a result, when the gyroscope rotates around the z-axis at some angular velocity, Ω, the Coriolis effect produces a force which causes the proof mass to accelerate in the sensing, x-direction, according to

$$a_x = -2\Omega\dot{y}, \tag{1}$$

where $\dot{y}$ is the linear velocity of the mass in the y-direction. It follows that, by knowing $\dot{y}$ and measuring a_x, one can easily measure the angular rate of rotation, Ω.

The aforedescribed process is generally not that simple; the gyroscope is typically placed in environments where the proof mass can also vibrate in the x-direction due to external unwanted vibrations. Thus, the acceleration in the x-direction takes the more general form:

$$a_x = \ddot{x} - 2\Omega\dot{y} - \Omega^2 x, \tag{2}$$

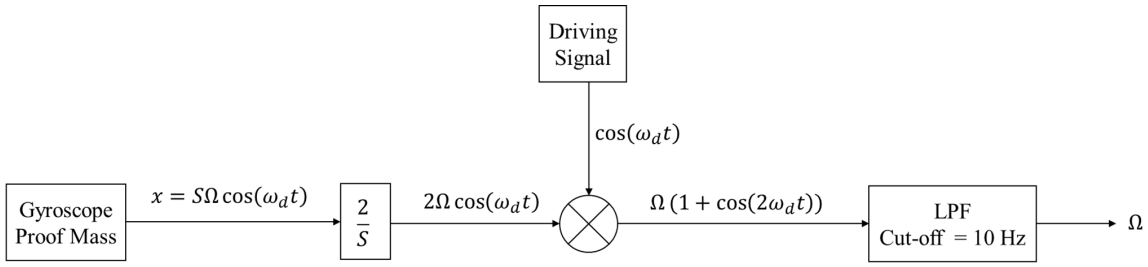

FIGURE 2. A block diagram showing the process in which the output of the gyroscope is demodulated to recover the rate of rotation Ω.

where x and $\ddot{x}$ are, respectively, the displacement and translational acceleration of the poof mass due to unwanted vibrations in the x-direction. As per Equation (2), the acceleration of the mass in the sensing direction now consists of three components. The first, $\ddot{x}$, is due to the translational acceleration of the mass in the x-direction; the second, $-2\Omega\dot{y}$, is due to the Coriolis effect; while the third, $-\Omega^2 x$, is the centrifugal component. Measuring Ω in this more complex scenario requires knowledge of x and $\ddot{x}$, which are quiet difficult to measure. Thus, the translational and centrifugal components of acceleration must be eliminated. Typically, this is achieved by designing the gyroscope to have two identical proof masses instead of one. A differential measurement is then performed by driving both masses in the y-direction at 180° out-of-phase. The out-of-phase driving mode reverses the sign of the driving velocity, $\dot{y}$, between the two masses, while maintaining the sign of the translational and centrifugal components of acceleration. Accordingly, the differential acceleration, a_x, becomes:

$$a_x = -4\Omega\dot{y}, \tag{3}$$

In an actual gyroscope, the driving displacement, y, is harmonic with a fixed frequency ω_d, and an amplitude $|y|$, which is maintained constant by using a feedback loop in an Automatic Gain Control (AGC) circuit [16], [17]. Thus, $\dot{y}$ can be expressed in the form $\dot{y} = |y|\omega_d\cos(\omega_d t)$. The displacement in the x-direction can then be obtained by integrating Equation (3) twice with respect to time to obtain

$$x = S\Omega\cos(\omega_d t), \tag{4}$$

where $S = 4|y|/\omega_d$ is a constant. As shown in Fig. 2, once x is obtained, the angular velocity reading is determined by multiplying the measured displacement signal by $2/S$, then demodulating the outcome by multiplying it with the driving signal, as follows:

$$2\Omega\cos(\omega_d t)\times\cos(\omega_d t) = \Omega(1+\cos(2\omega_d t)). \tag{5}$$

A low-pass filter is then used to attenuate the high-frequency component ($2\omega_d$), while retaining the frequency of the sensed rotation leading to direct reading of the angular velocity, Ω.

III. EXPERIMENTAL TESTING

To illustrate the vulnerabiliy of the gyroscope to acoustic attacks, we test the response of a MEMS gyroscope to acosutic excitations of different magnitudes. To this end, we consider a surface micromachined MEMS gyroscope (ADXRS624) integrated with all the electronics required for the readout circuit on one chip manufactured by Analog Devices [18]. As shown in the schematic depicted in Fig. 1, the gyroscope consists of two identical proof mass sensing structures that are electrostatically-actuated at resonance with 180 degrees out-of-phase signals along the driving y-axis. Due to the Coriolis effect, the rate of rotation (angular velocity) around the axis normal to the chip's top surface, z-direction, can be measured by the movement of the proof masses in the direction perpendicular to the driving axis.

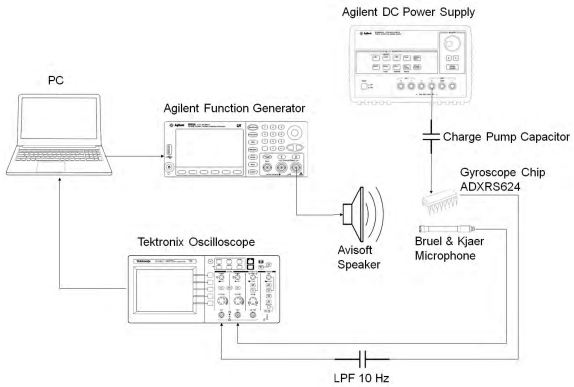

FIGURE 3. Schematic of the experimental setup.

The chip is mounted on an evaluation board (EVAL-ADXRS624) which contains external charge pump capacitors that are mainly utilized to operate the device at 5 V DC. A low-pass filter with a cut-off frequency of 10 Hz is also used to filter any high frequency inputs [19]. As illustrated in Fig. 3, the rest of the experimental setup consists of an Avisoft high-frequency speaker (1−120 kHz), a Tektronix oscilloscope, an Agilent function generator and DC power supply, and a Bruel & Kjaer microphone. As shown in Fig. 4, the speaker is placed facing the side of the gyroscope chip. The function generator is used to drive the speaker to generate the acoustic waves at a specific frequency. The time-domain output of the gyroscope is captured by an oscilloscope and then Fourier transformed to obtain the amplitude and frequency of the output signal as shown in Fig. 5. The figure

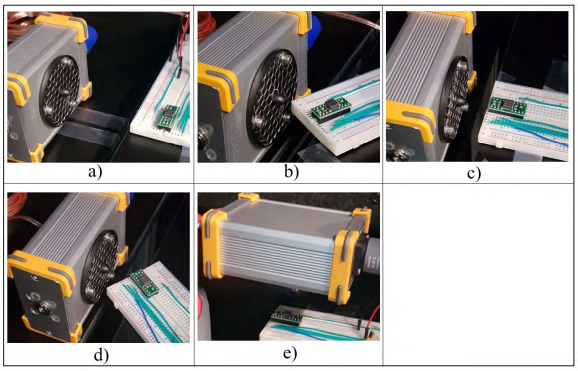

FIGURE 4. Experimental setup showing the speaker facing the gyroscope at different orientations. a) Orientation 1 at 0°, b) Orientation 2 at 45°, c) Orientation 3 at 90°, d) Orientation 4 at 135°, e) Orientation 5 (z-axis).

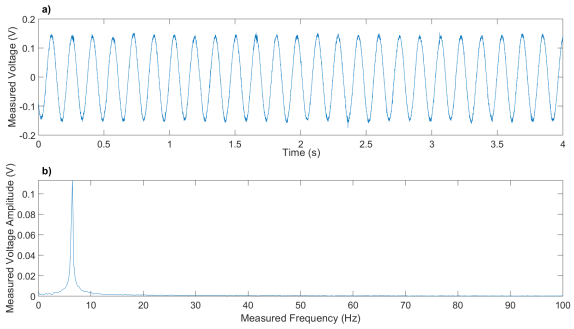

FIGURE 5. Measured a) time-domain output of the gyroscope, and b) its Fourier transform.

presents the measured signal from the gyroscope that was excited with a 15.005 kHz acoustic wave, showing a measured output of 0.12 Vp at 6.5 Hz.

Initially, a frequency sweep is performed to determine the resonance frequency of the gyroscope along the driving axis, which should also correspond to the frequency at which the proof mass is being driven internally. Although Analog Devices reported the resonance frequency of this gyroscope device to be 14 kHz [18], it was found from the measurements that the driving resonance frequency is ~15 kHz.

Next, the vulnerability of the gyroscope to ultrasonic excitations is assessed by investigating the response of the device to ultrasonic inputs with excitation frequencies around the driving frequency, ranging from 14.809 kHz to 15.189 kHz with a 0.5 Hz step. The measurements were repeated at different distances between the speaker and the gyroscope, and with multiple orientations of the gyroscope chip as shown in Fig. 4. The sound pressure level (SPL) was measured at each distance using the microphone. The results[1] are shown in Fig. 6 and Fig. 7, in which the gyroscope's output voltage amplitude is plotted versus the applied frequency (bottom x-axis) and the measured output frequency (top x-axis).

[1]Due to geometrical restrictions, the distance between the speaker and the gyroscope was not kept consistent for each orientation.

While sweeping the frequency of the acoustic wave, some readings were observed at frequencies around 45 kHz. Therefore, measurements were also recorded for excitation frequencies ranging between 44.809 kHz and 45.189 kHz, as shown in Fig. 8.

IV. RESULTS ANALYSIS

The results shown in Fig. 6 indicate that the gyroscope can generate false readings when subjected to acoustic signals with frequencies around the driving resonance of the structure. Based on a sensitivity of 25 mV/°/sec, the maximum measured output voltage is 0.16 Vp, which corresponds to a 6.4 °/sec rate of rotation [18]. This false reading can be further amplified by increasing the intensity of the acoustic signal. Results also demonstrate that the amplitude of the false output is not always directly proportional to the SPL as can be seen specifically in Figs. 6b, 6c, and 6d. This implies that, alongside the intensity of the acoustic waves, there are other factors which could influence the amplitude of the false output. This includes the chip orientation and the radiation pattern of the acoustic wave.

Although the applied acoustic wave was of high frequency (around 15 kHz), which is barely audible, the generated output signals by the gyroscope had very low frequency which equals the difference between the applied frequency and the resonant frequency (~15 kHz). The low frequency nature of the output increases the vulnerability of gyroscopes to acoustic attacks since it cannot be attenuated by employing a low-pass filter even with a very low cut-off frequency (set to 10 Hz in the experiments). Furthermore, the differential measurement mode with two proof masses that is employed to diminish the effect of the translational accelerations in the sensing direction, is clearly not effective in shielding the gyroscope from the acoustic attack. One plausible explanation for the failure of the differential measurement could be in the way that the acoustic wave interacts with the proof masses. In particular, when the package is subjected to external vibrations, both masses are expected to move in an identical fashion, and, hence the differential measurement approach would be effective. On the other hand, the transmission/reflection of the acoustic waves through/of the package and into the gyroscope can generate complex acoustic pressure patterns inside the package which can force the two masses to move with a different amplitude and phase.

Quite interestingly, test results illustrate that the fallacious reading is amplified at a specific orientation of the chip with respect to the acoustic signal line of propagation. While one would expect that the output would be maximized when the driving axis is aligned with the line of propagation of the acoustic wave, results point again to the complex interaction between the acoustic waves and package which can results in complex pressure wave patterns inside the package. This complicates the process of making predictions based on a simple acoustic wave propagation models.

As can be seen in Fig. 8, the gyroscope also produced false output readings, but with a lower amplitude, when the

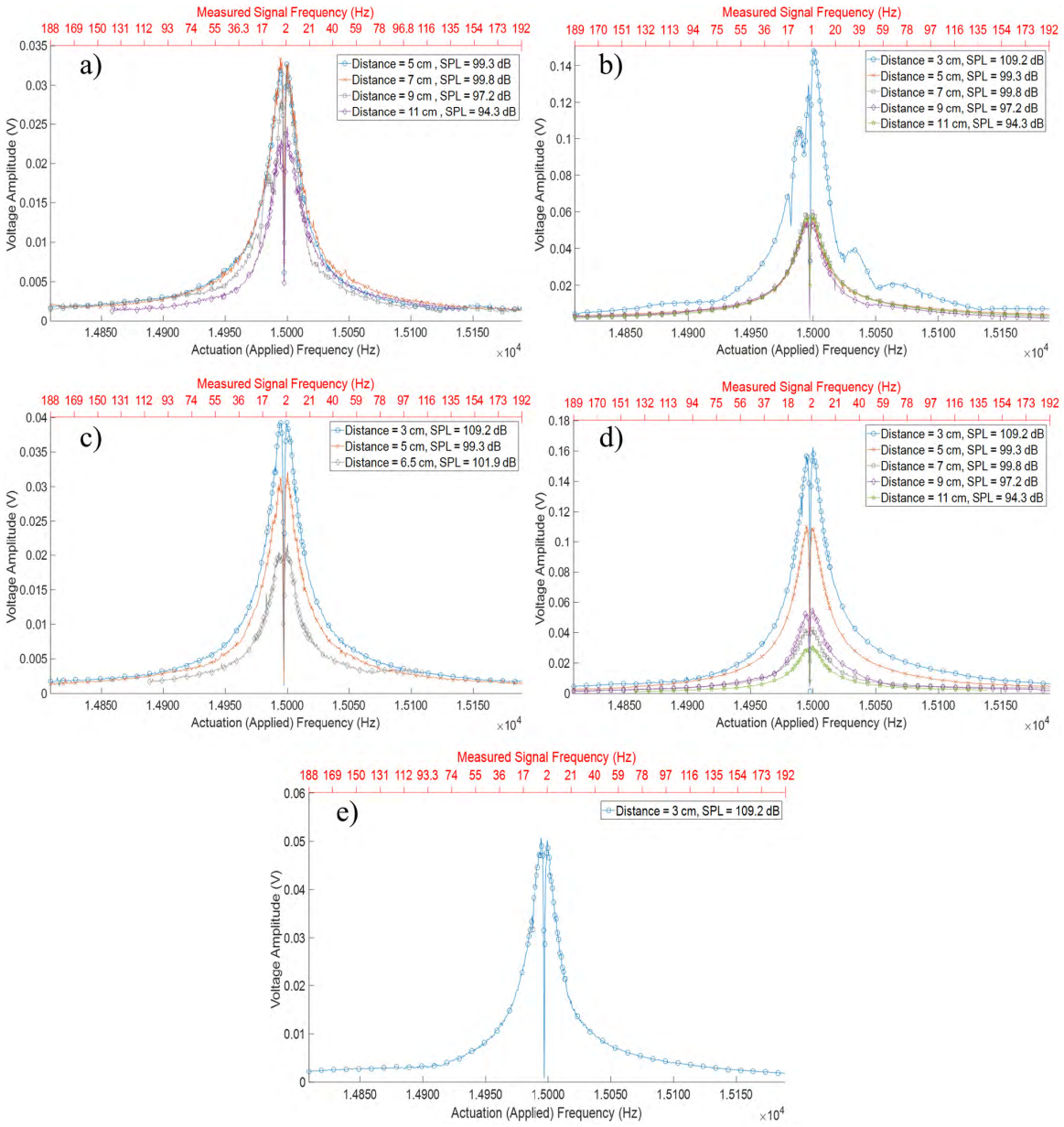

FIGURE 6. Experimental results of the frequency sweep (14.809 kHz - 15.189 kHz). a) Orientation 1 at 0°, b) Orientation 2 at 45°, c) Orientation 3 at 90°, d) Orientation 4 at 135°, e) Orientation 5 (*z*-axis).

frequency of the acoustic signal was around 45 kHz, which is equal to three times the fundamental frequency. As will be explained further in section V, this is due to the driving signal being in the form of a square wave rather than purely harmonic.

V. THEORETICAL MODEL OF THE ACOUSTIC ATTACK

We believe that the vulnerability of the gyroscope to acoustic attacks is due to the quadrature error, which is a performance indicator parameter for gyroscopes and is defined as the error in the output due to the misalignment between the driving and sensing axes which causes the driving motion to couple to the sensing motion [15]. In particular, when the driving axis is driven at resonance, the proof mass moves at the excitation frequency but is 90° out-of-phase due to it being at resonance. If the sensing direction is not exactly orthogonal to the driving direction, some of the energy gets coupled to the sensing direction causing it to move which produces a false reading. This error is usually accounted for by employing a demodulator in the readout circuit. The demodulator is used to separate the driving signal's frequency from the actual sensing frequency of rotation by multiplying the driving signal with the output of the gyroscope and passing it through a low-pass filter. However, the demodulator works only when the sensing signal has exactly the same frequency as the driving signal. This also explains the dip in the frequency response (Fig. 6)

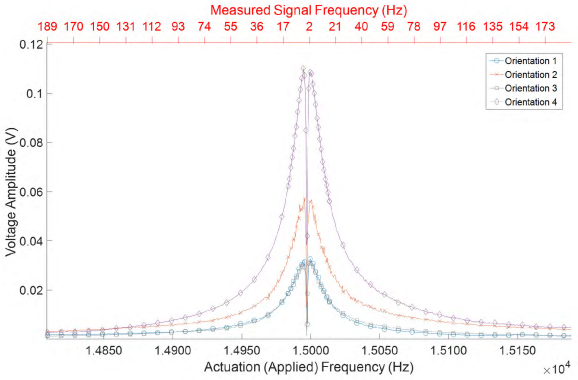

FIGURE 7. Comparing gyroscope's output for the different chip orientations at 5 cm distance (99.3 dB SPL) each.

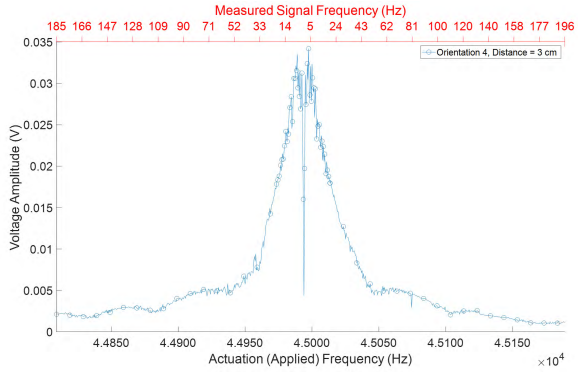

FIGURE 8. Experimental results of the frequency sweep 44.809 kHz - 45.189 kHz at orientation 4 and 3 cm distance (109.2 dB SPL).

when the gyroscope is excited by an acoustic signal with frequency exactly equals to the driving frequency, which was found to be 14.997 kHz. However, due to the demodulation, any slight deviation from this frequency causes the gyroscope to generate measurable output with frequency equals to the difference between the driving frequency and the frequency of the acoustic signal.

For perfectly orthogonal driving and sensing directions, the equations of motion of the gyroscope can be written as:

$$m_s(\ddot{x} - 2\Omega\dot{y} - \Omega^2 x) + c_s(\dot{x} - \Omega y) + k_s x = f_{acx}, \tag{6a}$$
$$m_d(\ddot{y} + 2\Omega\dot{x} - \Omega^2 y) + c_d(\dot{y} - \Omega x) + k_d y = f_d + f_{acy}, \tag{6b}$$

where m, c, and k are the mass, damping coefficient, and spring constant, respectively. The subscripts, s, and, d, indicate sensing and driving directions, respectively. The term $\ddot{y}$ is the translational acceleration in the y-direction. The forces are the electrostatic driving force f_d, and the components of the ultrasonic excitation f_{acx} and f_{acy} acting in the x and y directions, respectively. These forces can be expressed as sinusoidal signals in the time domain as follows:

$$f_d = D\cos(\omega_d t), \tag{7a}$$
$$f_{acx} = A_x\cos(\omega_{ac} t - \phi_0), \tag{7b}$$
$$f_{acy} = A_y\cos(\omega_{ac} t - \phi_0), \tag{7c}$$

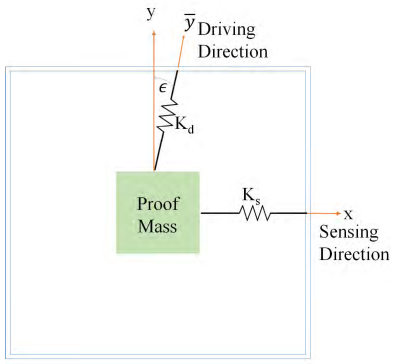

FIGURE 9. Schematic of the misalignment between the sensing and driving direction due to fabrication imperfections.

where D and ω_d are, respectively, the amplitude and frequency of the driving force; A_x and A_y are the amplitudes of the ultrasonic excitation in the x and y directions; ω_{ac} is its frequency, and ϕ_0 is the phase of the acoustic signal with respect to the phase of the driving force taken here as a reference. Since the device was held stationary during testing, the angular velocity term Ω can be canceled out and Equations (6a) and (6b) simplify to:

$$m_s\ddot{x} + c_s\dot{x} + k_s x = f_{acx}, \tag{8a}$$
$$m_d\ddot{y} + c_d\dot{y} + k_d y = f_d + f_{acy}. \tag{8b}$$

In the previous equations, the sensing and driving directions are considered to be perfectly orthogonal. To incorporate the misalignment between those directions into the model, the driving axis is reoriented at an angle ϵ with respect to the y-axis, as shown in Fig. 9. Accordingly, the equations can be rewritten as

$$m_s\ddot{x} + c_s\dot{x} + k_s x + c_d\dot{\delta}\sin\epsilon + k_d\delta\sin\epsilon = f_{acx} + f_d\sin\epsilon, \tag{9a}$$
$$m_d\ddot{y} + c_d\dot{\delta}\cos\epsilon + k_d\delta\cos\epsilon = f_d\cos\epsilon + f_{acy}. \tag{9b}$$

Here, δ is the displacement along the tilted axis $\bar{y}$. In order to nondimensionalize the equations and represent them in terms of resonance frequencies (ω_s and ω_d) and damping ratios (ζ_s and ζ_d), the following dimensionless terms were introduced:

$$X = \frac{x}{l_g}, \quad Y = \frac{y}{l_g}, \quad \tau = t\omega_d, \quad \bar{k} = \frac{k_d}{k_s}, \quad \omega_1 = \frac{\omega_{ac}}{\omega_d},$$
$$\omega_2 = \frac{\omega_s}{\omega_d}, \quad \omega_3 = \frac{\omega_{ac}}{\omega_s}, \quad D_s = \frac{D}{m_s\omega_d^2 l_g}, \quad D_d = \frac{D}{m_d\omega_d^2 l_g},$$
$$\bar{A_x} = \frac{A_x}{m_s\omega_d^2 l_g}, \quad \bar{A_y} = \frac{A_y}{m_d\omega_d^2 l_g},$$

where l_g is a unit length scale, chosen here to be the gap length between the sensing fingers. Assuming that the angle ϵ is very small such that $\delta = y$, the nondimensionalized equations become:

$$X'' + 2\zeta_s\omega_2 X' + \omega_2^2 X + 2\zeta_d\bar{k}\omega_2^2 Y'\sin\epsilon + \frac{\bar{k}}{\omega_2^2}Y\sin\epsilon$$
$$= \bar{A_x}\cos(\omega_1\tau - \phi_0) + D_s\cos(\tau)\sin\epsilon \tag{10a}$$

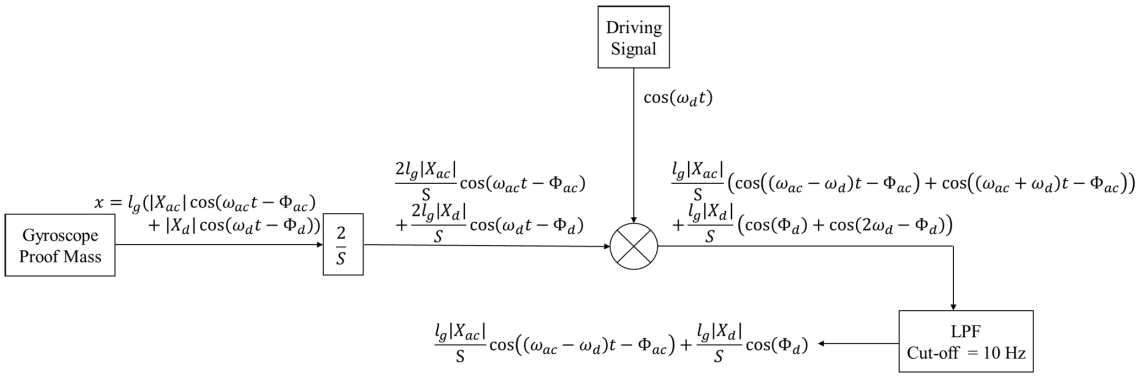

FIGURE 10. A block diagram showing the false output by the acoustic attack when the sensing displacement signal passes through the readout circuit's stages of amplitude adjustment, demodulation, and low-pass filtering.

$$Y'' + 2\zeta_d Y' \cos\epsilon + Y\cos\epsilon = D_d \cos\epsilon\cos\tau + \bar{A}_y \cos(\omega_1\tau - \phi_0), \quad (10b)$$

where the prime represents a derivative with respect to the nondimensional time, τ. Equation (10b) indicates that the nondimensional displacement, X, in the sensing direction consists of two components: X_{ac} and X_d, where X_{ac} is the displacement emanating from the ultrasonic excitation, and X_d is the displacement emanating from the electrostatic excitation in the driving direction. The latter is transferred to the sensing direction due to the misalignment, which elastically couples both directions. By solving Equations (10a) and (10b), the steady-state displacement in the sensing direction can be expressed as follows:

$$\begin{aligned} X &= X_{ac} + X_d = |X_{acx}|\cos(\omega_1\tau - \phi_0 - \phi_{ac}) \\ &\quad - |X_{acy}|\cos(\omega_1\tau - \phi_0 - \phi_y) \\ &\quad + |X_{d1}|\cos(\tau - \theta_d) - |X_{d2}|\cos(\tau - \phi_d), \end{aligned} \quad (11)$$

where the amplitudes and phases of the response are given in Appendix. Note that with some algebraic manipulations the previous equation can be rewritten as

$$X = |X_{ac}|\cos(\omega_1\tau - \Phi_{ac}) + |X_d|\cos(\tau - \Phi_d), \quad (12)$$

where

$$\begin{aligned} |X_{ac}| &= \sqrt{|X_{acx}|^2 + |X_{acy}|^2 + 2|X_{acx}||X_{acy}|\cos(\phi_{ac} - \phi_y)}, \\ |X_d| &= \sqrt{|X_{d1}|^2 + |X_{d2}|^2 + 2|X_{d1}||X_{d2}|\cos(\phi_d - \theta_d)}, \end{aligned} \quad (13)$$

and

$$\begin{aligned} \Phi_{ac} &= \tan^{-1}\left(\frac{|X_{acx}|\sin(\phi_0 + \phi_{ac}) + |X_{acy}|\sin(\phi_0 + \phi_y)}{|X_{acx}|\cos(\phi_0 + \phi_{ac}) + |X_{acy}|\cos(\phi_0 + \phi_y)}\right) \\ \Phi_d &= \tan^{-1}\left(\frac{|X_{d1}|\sin(\theta_d) + |X_{d2}|\sin(\phi_d)}{|X_{d1}|\cos(\theta_d) + |X_{d2}|\cos(\phi_d)}\right). \end{aligned} \quad (14)$$

Upon re-dimensionalizing the output displacement, we obtain

$$x = l_g\left(|X_{ac}|\cos(\omega_{ac}t - \Phi_{ac}) + |X_d|\cos(\omega_d t - \Phi_d)\right). \quad (15)$$

By inspecting Equation (15), it becomes evident that, even when the gyroscope does not undergo any angular rotation in the yaw direction, the sensing combs will measure a displacement due to both of the acoustic excitation and the misalignment. The output displacement, x generated by the acoustic attack is a combination of oscillations at the driving frequency, ω_d, and the frequency of the acoustic wave, ω_{ac}.

As described previously in Section II and shown in Fig. 10, the readout circuit takes the displacement X multiplies it by $2/S$ and demodulates it by multiplying it by the driving signal, then filters it by passing it through a low pass filter. This yields the following false angular velocity reading.

$$\Omega_{false} = \frac{l_g}{S}\left(|X_{ac}|\cos\left((\omega_{ac} - \omega_d)t - \Phi_{ac}\right) + |X_d|\cos(\Phi_d)\right) \quad (16)$$

Equation (16) shows that the false output is a sinusoidal signal with amplitude $\frac{l_g|X_{ac}|}{S}$ and frequency equals to $\omega_{ac} - \omega_d$, which matches the results obtained in the experimental measurements. When the frequency of the acoustic wave matches exactly the driving frequency (resonance condition), $\omega_{ac} - \omega_d$ becomes equal to 0, and in turn, Ω_{false} is minimized based on the phase Φ_{ac}. This explains the dip in the measured frequency response at frequencies equal to the driving frequency. There is also a constant term $\frac{l_g|X_d|}{S}\cos(\Phi_d)$ which causes a shift in the output. This term is generated solely by the driving signal and is not affected by the acoustic excitation, and it is normally compensated for by the electronics in the readout circuit.

The theoretical model of the acoustic attack was implemented and the results were compared with the experimental measurements. The parameters used in the model were based on a case study in [15] of an Analog Devices gyroscope (ADXRS150) which is similar in design to the ADXRS624. The parameters are listed in TABLE 1. Using the driving displacement $|y|$, the amplitude of the driving force was determined by the relation $D = \frac{k_d|y|}{Q_d} = 3.45 \times 10^{-6}\,N$. The misalignment angle ϵ was set to 1°, which is a reasonable value for batch microfabrication without trimming [15]. Since the gyroscope was oriented such that the driving axis is aligned with the acoustic source; based on the experimental results, the acoustic forces A_x and A_y were set as $4 \times 10^{-9}\,N$ and $16 \times 10^{-9}\,N$, respectively. Finally, the phase of the acoustic signal, ϕ_0, was arbitrarily chosen to be $\pi/3$ based on the

TABLE 1. Parameters used in the theoretical model [15].

Parameter	Value
m_d	$2.5 \times 10^{-9}\ kg$
m_s	$4.1 \times 10^{-9}\ kg$
k_d	$22.2\ N/m$
k_s	$85.6\ N/m$
ω_d	$94248\ rad/s\ (15\ kHz)$
ω_s	$144513\ rad/s\ (23\ kHz)$
Q_d	$45\ (\zeta_d = \frac{1}{90})$
Q_s	$18\ (\zeta_s = \frac{1}{36})$
$\|y\|$	$7\ \mu m$

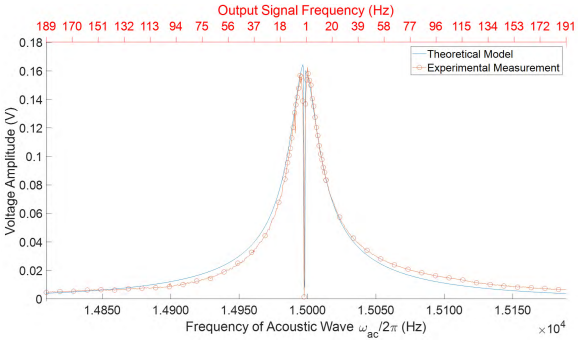

FIGURE 11. Results of the theoretical model compared with the experimental measurements.

fact that the acoustic wave could reach the gyroscope at any phase delay with respect to the driving signal. The results of the theoretical model and the experimental measurements are shown in Fig. 11, indicating good agreement.

In the aforementioned theoretical model, the reference signal used for the demodulation was assumed to be a pure sinusoidal signal having a single frequency. Nevertheless, the actual signal consists of a square wave which can be expressed, using Fourier expansion, as a sum of sines as follows:

$$Demod_{ref} = \frac{4}{\pi}\left(\sin\omega_d t + \frac{1}{3}\sin 3\omega_d t + \frac{1}{5}\sin 5\omega_d t + \ldots\right) \tag{17}$$

When the difference between ω_{ac} and $3\omega_d$ is less than 10 Hz, and the output from the gyroscope's displacement is multiplied with the reference signal by the demodulator, a low frequency signal is generated due to the second component in equation (17). In this case, the false reading after filtering becomes

$$\Omega_{false} = \frac{4l_g}{\pi S}\left(\frac{1}{3}|X_{ac}|\sin\left((\omega_{ac}-3\omega_d)t-\Phi_{ac}\right)+|X_d|\sin(\Phi_d)\right) \tag{18}$$

This explains the results obtained in Fig. 8, in which ω_{ac} was swept around 45 kHz. The reduced amplitude compared to the sweep around 15 kHz is due to the presence of a $\frac{1}{3}$ factor and the fact that the 45 kHz frequency is away from resonance.

VI. CONCLUSION

Resonantor MEMS gyroscopes are susceptible to external interferences occurring at the vicinity of their resonant frequency. This can be exploited by attackers to force the device to produce malicious readings disrupting its functionality and imposing security risks. The vulnerability of MEMS based gyroscopes to external attacks in the form of acoustic excitation was studied in this paper. We tested an analog gyroscope device by exposing it to acoustic signals with frequencies close to its driving resonance (15 kHz), and it was found to produce false readings of angular velocity oscillating at low frequencies (0.5 - 190 Hz). Although the device operates with two identical proof masses to diminish the effect of linear acceleration by differential measurement, this approach seemed ineffective in shielding the device from acoustic attacks. The low-frequency output was a result of the demodulation employed in the readout circuit which is necessary for normal operation of the device. The output of the demodulator was a signal with frequency equals to the difference between the driving and the acoustic signals' frequency. This imposes higher security risks since the false readings could not be attenuated by adding a 10 Hz low-pass filter despite the fact that the device was excited with high-frequency acoustic noise that is almost inaudible. Moreover, it was found that the amplitude of the false output is greatly affected by the orientation of the gyroscope chip with respect to the sound source. Finally, we assumed that the misalignment between the driving and sensing axes was the main cause of the false output generated by the gyroscope when subjected to acoustic noise around its driving resonance. Accordingly, a theoretical model of the acoustic attack was constructed, taking into account the main mechanical and electrical components influencing the output, and was found to be in good correlation with the measurement.

Acoustic attacks impose real threat on the integrity of MEMS-based gyroscopes; thus, measures need to be taken to improve the resistance of these devices to such attacks. For instance, in the driving circuit, the y-displacement is being controlled by a feedback loop where separate sensing fingers are used to measure the displacement in the y-direction. These fingers can be utilized to detect any large y-displacement at resonance and halt the operation of the gyroscope. This approach prevents the attacker from further spoofing the output and compromising the system; however, it does not prevent the attacker from disabling the gyroscope sensor.

Shielding the gyroscope from acoustic noise is another mitigation method to the acoustic attacks. Covering the sensor with acoustic dampening materials, such as foam, can attenuate the acoustic signal preventing it from penetrating the package. Nevertheless, foam adds bulk to the packaging of the gyroscope, which adversely influences the compactness of the MEMS device and raises the temperature of the board, making it less suitable to be used in embedded systems.

Since the root cause of the acoustic interference is the misalignment between the sensing and driving axes, an optimum solution would be to improve the fabrication process to

eliminate this misalignment. Some spring structures were investigated by Analog Devices to minimize the misalignment by using pivoting linkage between the springs [15]; however, further exploration needs to be carried out for improvement.

APPENDIX

Amplitudes and Phases Appearing in Equation (11)

$$
\begin{aligned}
|X_{acx}| &= \frac{\bar{A_x}}{\omega_2^2\sqrt{(1-\omega_3^2)^2+(2\zeta_s\omega_3)^2}},\\
|X_{acy}| &= \bar{k}\sin\epsilon\frac{\bar{A_y}}{\sqrt{\left((1-\omega_3^2)^2+(2\zeta_s\omega_3)^2\right)}}\\
&\quad\times\frac{\sqrt{1+(2\zeta_d\omega_1)^2}}{\sqrt{\left((\cos\epsilon-\omega_1^2)^2+(2\zeta_d\omega_1\cos\epsilon)^2\right)}}\\
|X_{d1}| &= \sin\epsilon\frac{D_s}{\sqrt{(1-\omega_2^2)^2+(2\zeta_s\omega_2)^2}}\\
|X_{d2}| &= \sin\epsilon\frac{D_s}{\sqrt{\left((1-\omega_2^2)^2+(2\zeta_s\omega_2)^2\right)}}\\
&\quad\times\frac{\sqrt{1+(2\zeta_d)^2}}{\sqrt{\left((\cos\epsilon-1)^2+(2\zeta_d\cos\epsilon)^2\right)}}\\
\phi_d &= \tan^{-1}\left(\frac{2\zeta_d\cos\epsilon}{\cos\epsilon-1}\right)+\tan^{-1}\left(\frac{2\zeta_s\omega_2}{\omega_2^2-1}\right)\\
&\quad-\tan^{-1}(2\zeta_d)\\
\phi_y &= \tan^{-1}\left(\frac{2\zeta_d\omega_1\cos\epsilon}{\cos\epsilon-\omega_1^2}\right)+\tan^{-1}\left(\frac{2\zeta_s\omega_3}{1-\omega_3^2}\right)\\
&\quad-\tan^{-1}(2\zeta_d\omega_1),\\
\theta_d &= \tan^{-1}\left(\frac{2\zeta_s\omega_2}{\omega_2^2-1}\right),\qquad \phi_{ac}=\tan^{-1}\left(\frac{2\zeta_s\omega_3}{1-\omega_3^2}\right)
\end{aligned}
\tag{19a}
$$

REFERENCES

[1] D. F. Kune, J. Backes, S. S. Clark, D. Kramer, M. Reynolds, K. Fu, Y. Kim, and W. Xu, "Ghost talk: Mitigating EMI signal injection attacks against analog sensors," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 145–159.

[2] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.* Berlin, Germany: Springer, 2013, pp. 55–72.

[3] Y. Shoukry, P. Martin, Y. Yona, S. Diggavi, and M. Srivastava, "Pycra: Physical challenge-response authentication for active sensors under spoofing attacks," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur.*, 2015, pp. 1004–1015.

[4] P. Soobramaney, "Mitigation of the effects of high levels of high-frequency noise on mems gyroscopes," Ph.D. dissertation, Dept. Mech. Eng., Auburn Univ., Auburn, AL, USA, 2013.

[5] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging doubt on the integrity of MEMS accelerometers with acoustic injection attacks," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS&P)*, Apr. 2017, pp. 3–18.

[6] Y. Tu, Z. Lin, I. Lee, and X. Hei, "Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors," in *Proc. 27th USENIX Secur. Symp.*, 2018, pp. 1545–1562.

[7] K. Tanaka, Y. Mochida, M. Sugimoto, K. Moriya, T. Hasegawa, K. Atsuchi, and K. Ohwada, "A micromachined vibrating gyroscope," *Sens. Acutators A, Phys.*, vol. 50, nos. 1–2, pp. 111–115, 1995.

[8] B. Kim, M. A. Hopcroft, R. N. Candler, C. M. Jha, M. Agarwal, R. Melamud, S. A. Chandorkar, G. Yama, and T. W. Kenny, "Temperature dependence of quality factor in MEMS resonators," *J. Microelectromech. Syst.*, vol. 17, no. 3, pp. 755–766, 2008.

[9] R. N. Dean, G. T. Flowers, A. S. Hodel, G. Roth, S. Castro, R. Zhou, A. Moreira, A. Ahmed, R. Rifki, B. E. Grantham, D. Bittle, and J. Brunsch, "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jun. 2007, pp. 1435–1440.

[10] R. N. Dean, S. T. Castro, G. T. Flowers, G. Roth, A. Ahmed, A. S. Hodel, B. E. Grantham. D. A. Bittle, and J. P. Brunsch, "A characterization of the performance of a MEMS gyroscope in acoustically harsh environments," *IEEE Trans. Ind. Electron.*, vol. 58, no. 7, pp. 2591–2596, Jul. 2011.

[11] Y. Michalevsky, D. Boneh, and G. Nakibly, "Gyrophone: Recognizing speech from gyroscope signals," in *Proc. 23rd USENIX Secur. Symp.*, 2014, pp. 1053–1067.

[12] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking drones with intentional sound noise on gyroscopic sensors," in *Proc. 24th USENIX Secur. Symp.*, 2015, pp. 881–896.

[13] J. A. Geen, S. J. Sherman, J. F. Chang, and S. R. Lewis, "Single-chip surface micromachined integrated gyroscope with 50°h allan deviation," *IEEE J. Solid-State Circuits*, vol. 37, no. 12, pp. 1860–1866, Dec. 2002.

[14] C. Patel and P. McCluskey, "Modeling and simulation of the MEMS vibratory gyroscope," in *Proc. 13th Intersoc. Conf. Therm. Thermomech. Phenomena Electron. Syst.*, May/Jun. 2012, pp. 928–933.

[15] V. Kaajakari, *Practical MEMS: Design of Microsystems, Accelerometers, Gyroscopes, RF MEMS, Optical MEMS, and Microfluidic Systems*. Las Vegas, NV, USA: Small Gear, 2009.

[16] D. J. Kim and R. T. M'Closkey, "A systematic method for tuning the dynamics of electrostatically actuated vibratory gyros," *IEEE Trans. Control Syst. Technol.*, vol. 14, no. 1, pp. 69–81, Jan. 2006.

[17] R. Yi, B. Han, and W. Sheng, "Design on the driving mode of MEMS vibratory gyroscope," in *Proc. Int. Conf. Intell. Robot. Appl.* Berlin, Germany: Springer, 2008, pp. 232–239.

[18] *Adxrs624 Datasheet and Product Info | Analog Devices*. Accessed: Mar. 27, 2019. [Online]. Available: https://www.analog.com/en/products/adxrs624.html

[19] *Evaluation Board User Guide UG-152*. Accessed: Mar. 27, 2019. [Online]. Available: https://www.analog.com/media/en/technical-documentation/user-guides/ug-152.pdf

SHADI KHAZAALEH received the B.Sc. degree in mechanical engineering from the Jordan University of Science and Technology, Irbid, Jordan, in 2011, and the M.Sc. degree in microsystems engineering from the Masdar Institute of Science and Technology, Abu Dhabi, United Arab Emirates, in 2016. He was a Research Engineer with the EECS Department, Masdar Institute. He has been working on the design, predictive modeling, fabrication, and the characterization of piezoelectric MEMS devices for applications in gesture recognition, medical imaging, fingerprint identification, and microfluidics. He is currently a Research Engineer with New York University, Abu Dhabi, focusing on MEMS hardware security.

GEORGIOS KORRES studied applied mathematics with the School of Science and Engineering, University of Crete. He received the master's degree in numerical simulations in engineering from ANSYS, Polytechnic School of Madrid (UPM). He was involved for several years with the development of educational software and hardware regarding educational robotics. He is currently a Senior Research Engineer with the Applied Interactive Multimedia Laboratory, New York University, Abu Dhabi. Previously, he has also dealt with industrial automation (mainly in the field of recycling industry). His research interests include development of new types of sensors and actuators, and the use of these in human–computer interaction.

MOHAMMED EID received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Canada, in 2010. He was a Teaching and Research Associate with the University of Ottawa, from 2008 to 2012. He is currently an Assistant Professor of electrical engineering with New York University, Abu Dhabi (NYUAD). He has coauthored the book *Haptics Technologies: Bringing Touch to Multimedia*, (Springers, 2011), the Technical Chair of the Haptic-Audio-Visual Environment and Gaming (HAVE) Symposium in several years (2013, 2014, 2015, and 2017). He has more than 90 conferences and journal publications, and 5 patents. His current interests include acoustic-based mid-air tactile stimulation, affective haptics, haptic modeling, and neurohaptics. He is the recipient of several best paper awards in several international conferences such as ICBAE 2016, DS-RT 2008 and the prestigious ACM Multimedia 2009 Grand Challenge Most Entertaining Award for HugMe: Synchronous Haptic Teleconferencing System.

MAHMOUD RASRAS received the Ph.D. degree in physics from the Catholic University of Leuven, Belgium. He has more than 11 years of industrial research experience as a Member of Technical Staff at Bell Labs, Alcatel-Lucent, NJ, USA. He was a Faculty Member and the former Director of the SRC/GF Center-for-Excellence for Integrated Photonics, Masdar Institute (part of Khalifa University). He is currently an Associate Professor of electrical and computer engineering with New York University, Abu Dhabi (NYUAD). He authored and coauthored more than 120 journals and conference papers, and holds 33 U.S. patents. He is an Associate Editor of *Optics Express* and a Guest Editor - MDPI.

MOHAMMED F. DAQAQ received the B.Sc. degree in mechanical engineering from the Jordan University of Science and Technology, in 2001, and the M.Sc. and Ph.D. degrees in engineering mechanics from Virginia Tech, in 2003, and 2006, respectively. In 2006, he joined the Department of Mechanical Engineering, Clemson University, as an Assistant Professor and went through the ranks to become a tenured Associate Professor, in 2012. In 2016, he became the D. W. Reynolds Endowed Scholar of mechanical engineering with Clemson University. In 2017, he joined the ranks of New York University, Abu Dhabi. He is currently a Global Network Professor of mechanical engineering with New York University, NY, USA and New York University, Abu Dhabi. His research interests include the application of various nonlinear phenomena to improve the performance of micro-power generation systems, microelectromechanical systems, and vibration assisted manufacturing processes. His research is funded through several grants from the National Science Foundation, including the 2010 CAREER Award. His research has also been recognized at the national level through several awards including the 2016 C. D. Mote Jr. Early Career Award from the ASME Design Division, the 2014 Gary Anderson Early Achievement Award from the ASME Aerospace Division, the 2014 Eastman Chemical Award for research excellence, and the 2012 Clemson University Board of Trustees Award for Faculty Excellence. He currently serves as an Associate Editor for the *Journal of Vibration and Acoustics* and as a Subject Editor for the *Journal Nonlinear Dynamics*.