SONIC GUN TO SMART DEVICES

YOUR DEVICES LOSE CONTROL UNDER ULTRASOUND/SOUND

Authors

Wang, Zhengbo & Wang, Kang
Alibaba Security
Yang, Bo
CAICT
Li, Shangyuan
Tsinghua University
Pan, Aimin
Alibaba Security

About us

- Who are we:
  A research team of Alibaba security.

- Our research interests:
  Security issues about IoT, AI and their combinations.

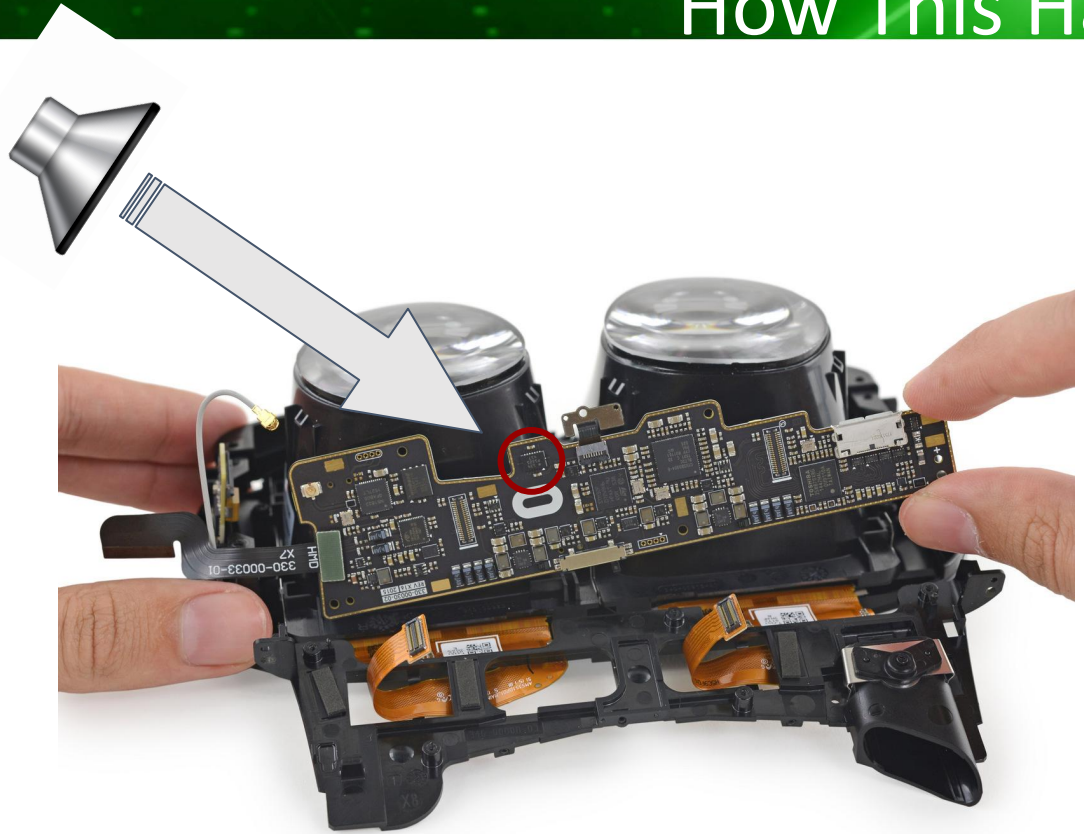
- Previous briefing:
  GPS spoofing (Blackhat Europe 2015)

Outline

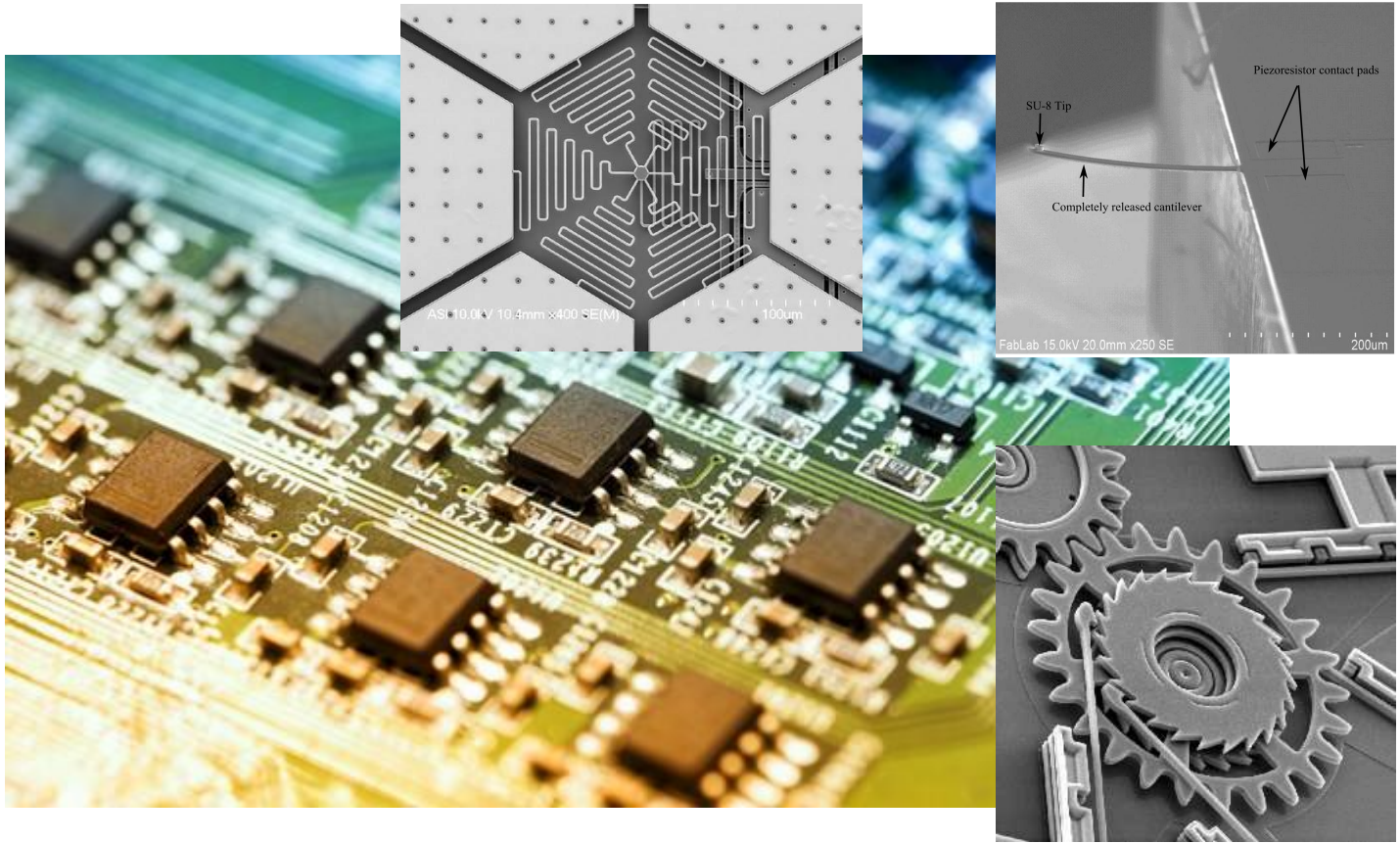
- An attack demo of Oculus headset
- Dig deeper on MEMS
- Other attack attempts on VR devices
- Attack attempts on drones
- Attack attempts on self-balanced vehicles
- 3 Countermeasures
- The END

Attack Demo on Facebook Oculus

How This Happens?



What is MEMS

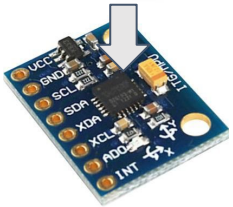

Piezoresistor contact pads
SU-8 Tip
Completely released cantilever
FabLab 15.0kV 20.0mm x250 SE
200um

What is MEMS


12:45
75°F


htc

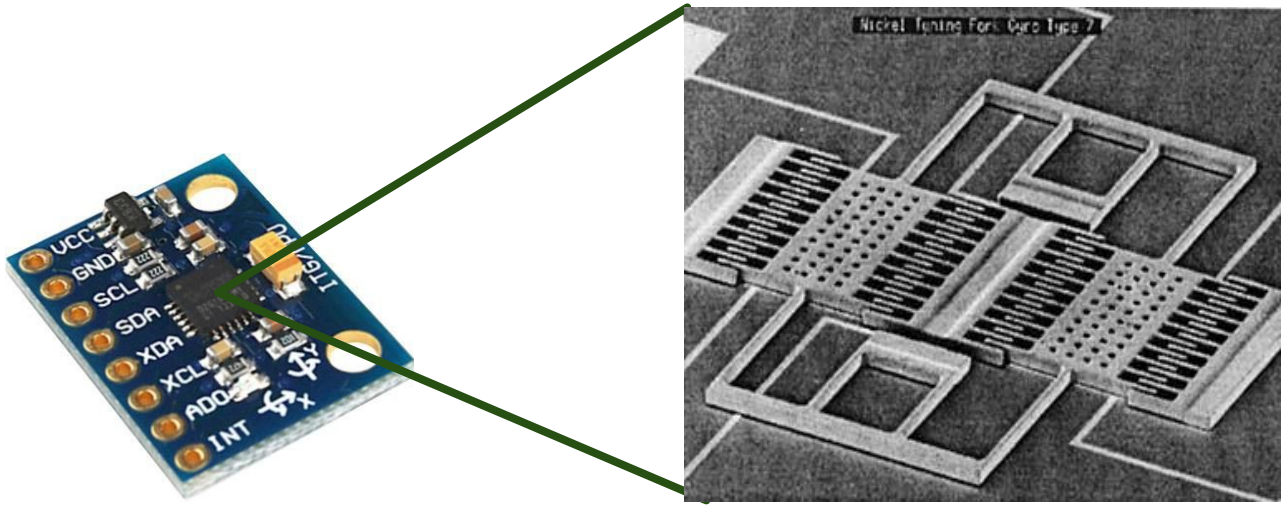

Oculus


VCC
GND
SCL
SDA
XDA
XCL
ADO
INT


htc
SAMSUNG
2:45

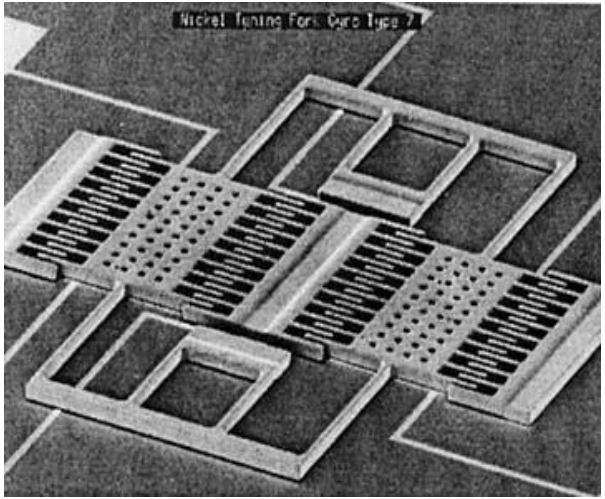
How MEMS Works

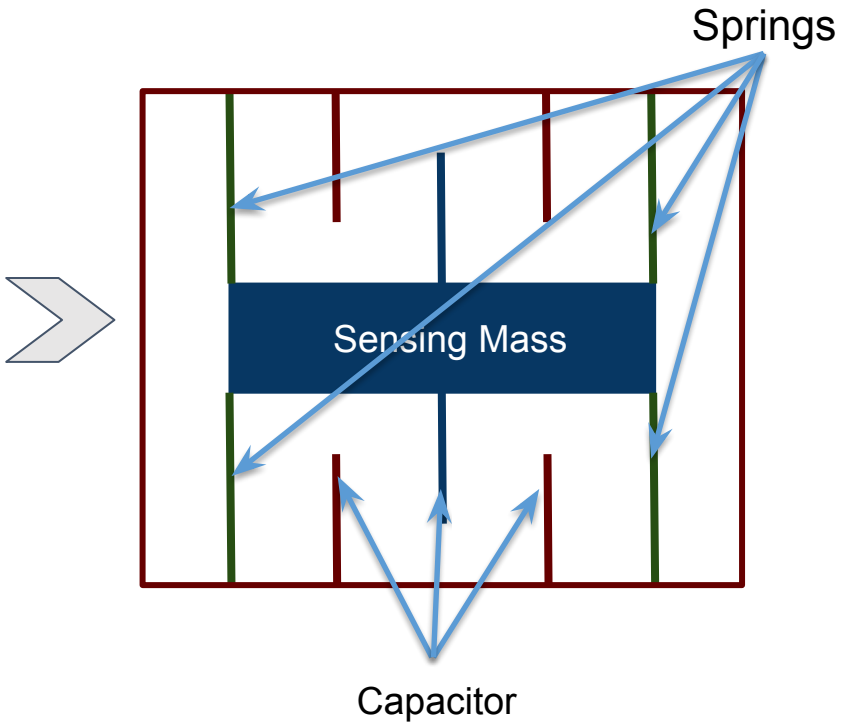
Accelerometer



How MEMS Works

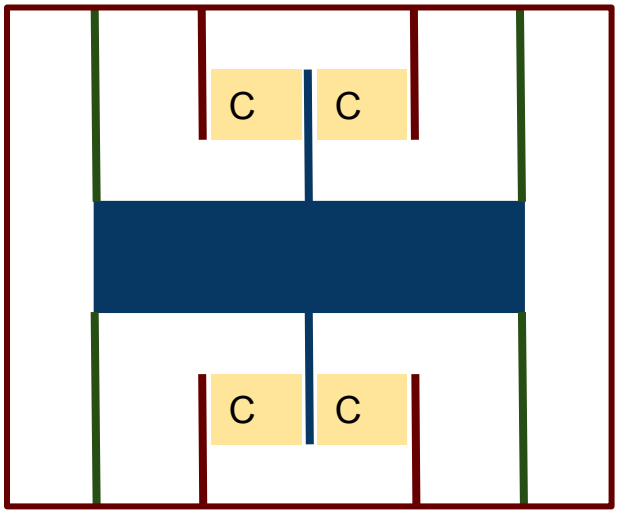
Accelerometer





How MEMS Works

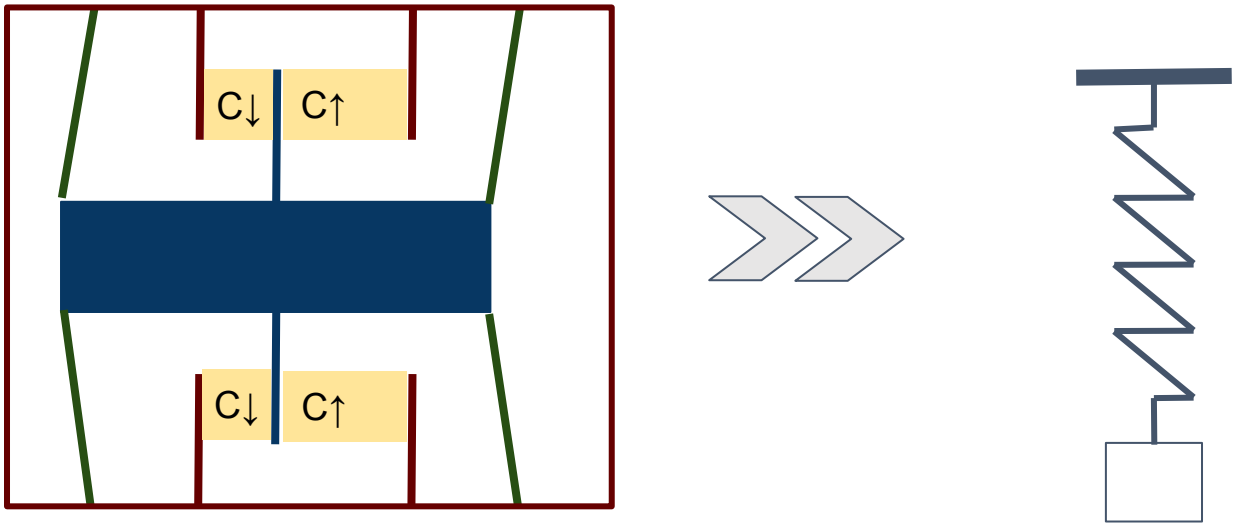
Accelerometer



1 DoF (Degree of Freedom)
Spring-Mass System

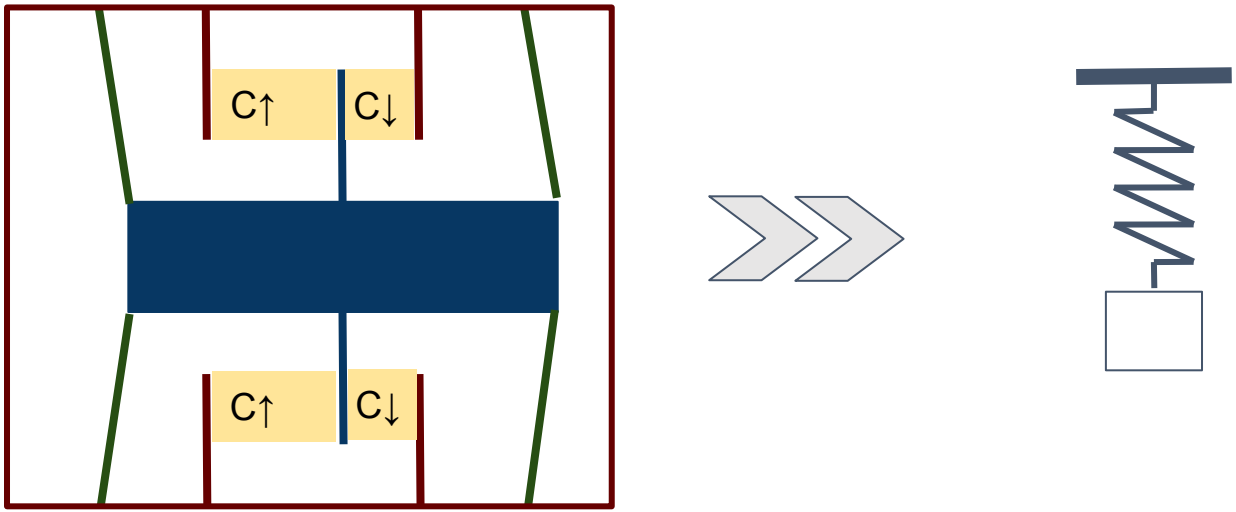
How MEMS Works

Accelerometer



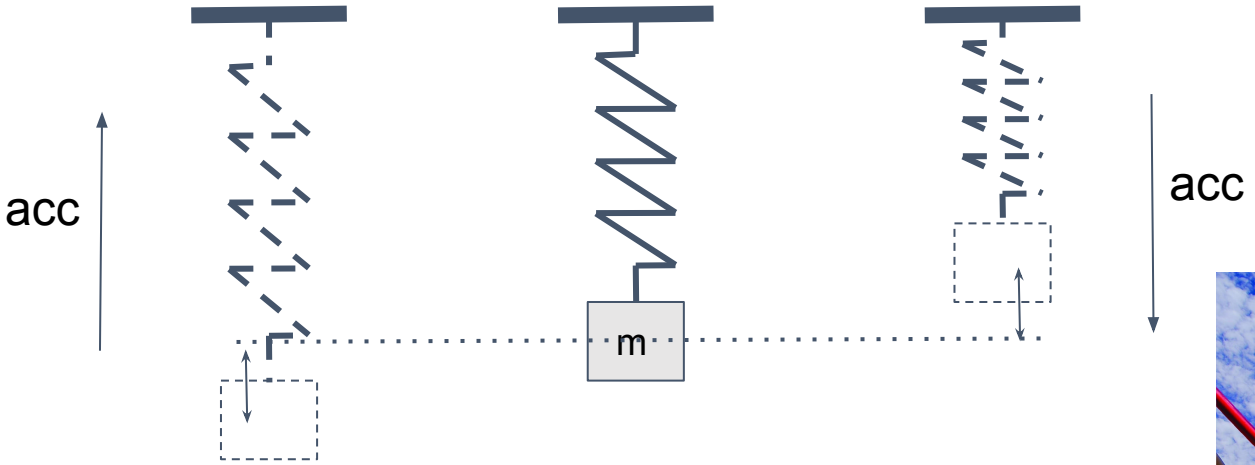
How MEMS Works

Accelerometer



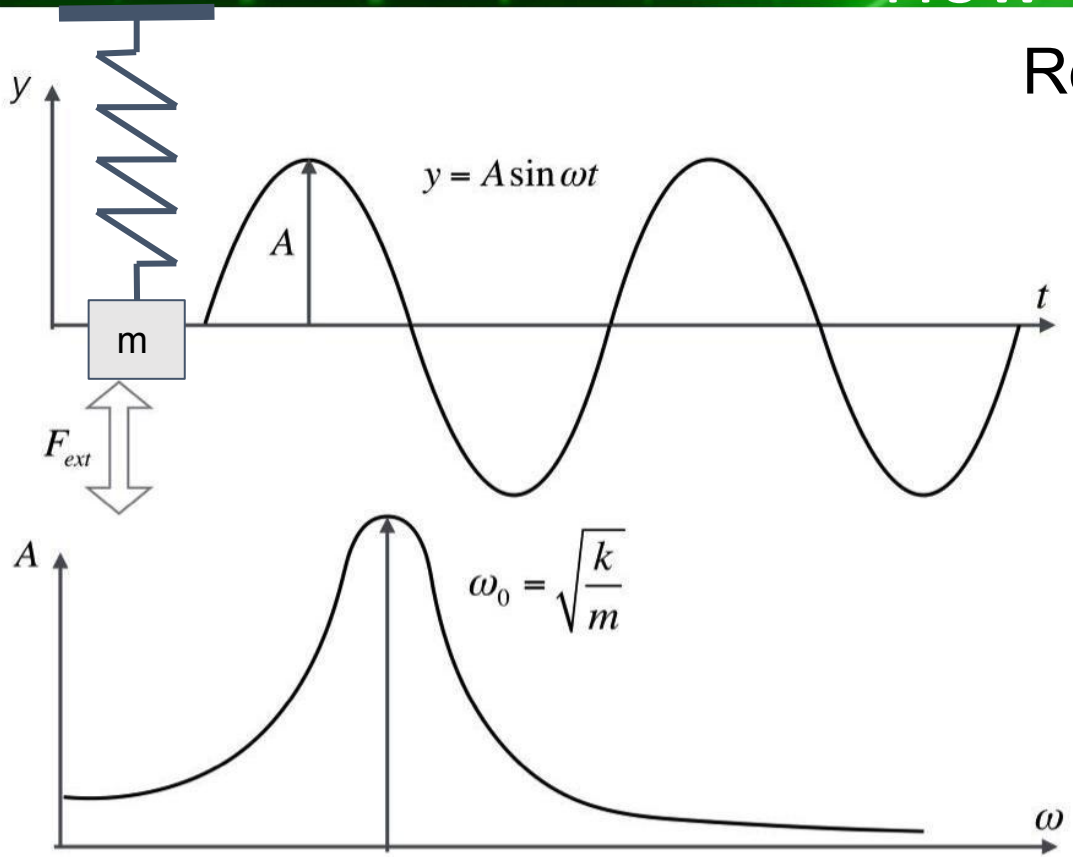
How MEMS Works

Accelerometer



How to Attack

Resonance



Previous Work

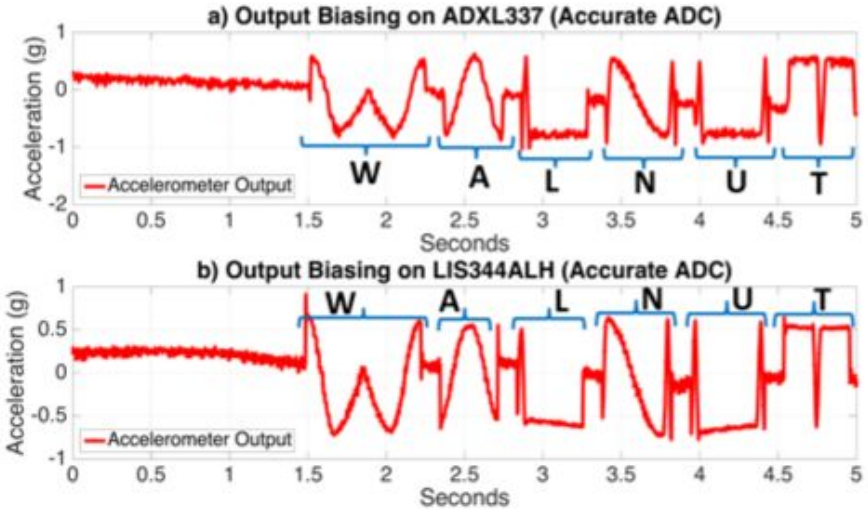
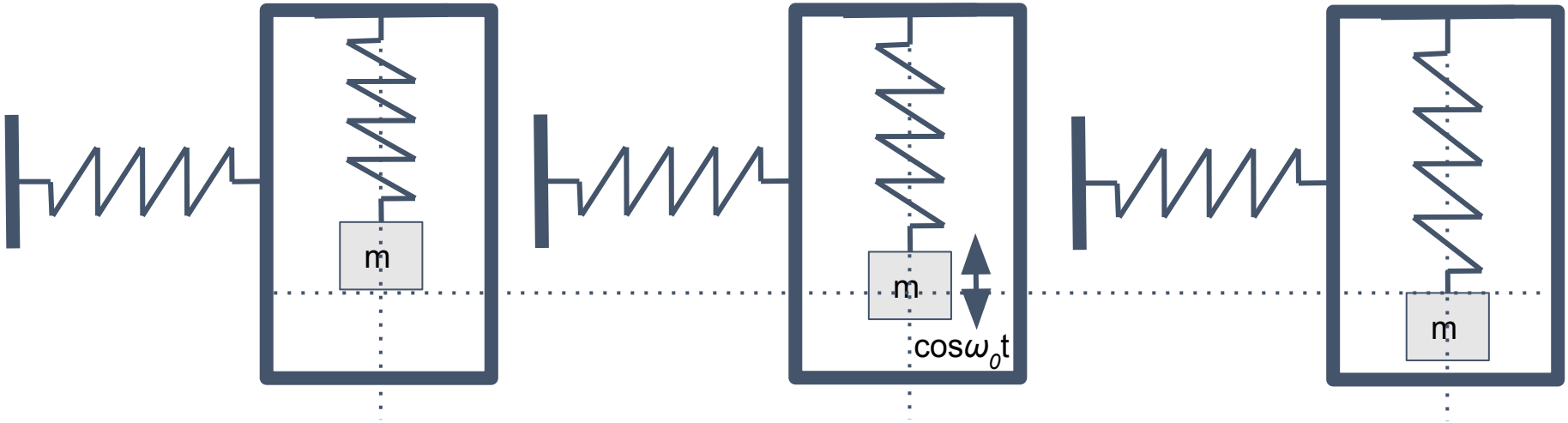


Figure 11. **Spelling WALNUT: Output Biasing Attack on Sensors with Accurate ADCs.** We demonstrate the output biasing attack can control

T. Trippel et al. WALNUT. https://spqr.eecs.umich.edu/walnut/

How MEMS Works

Gyroscope

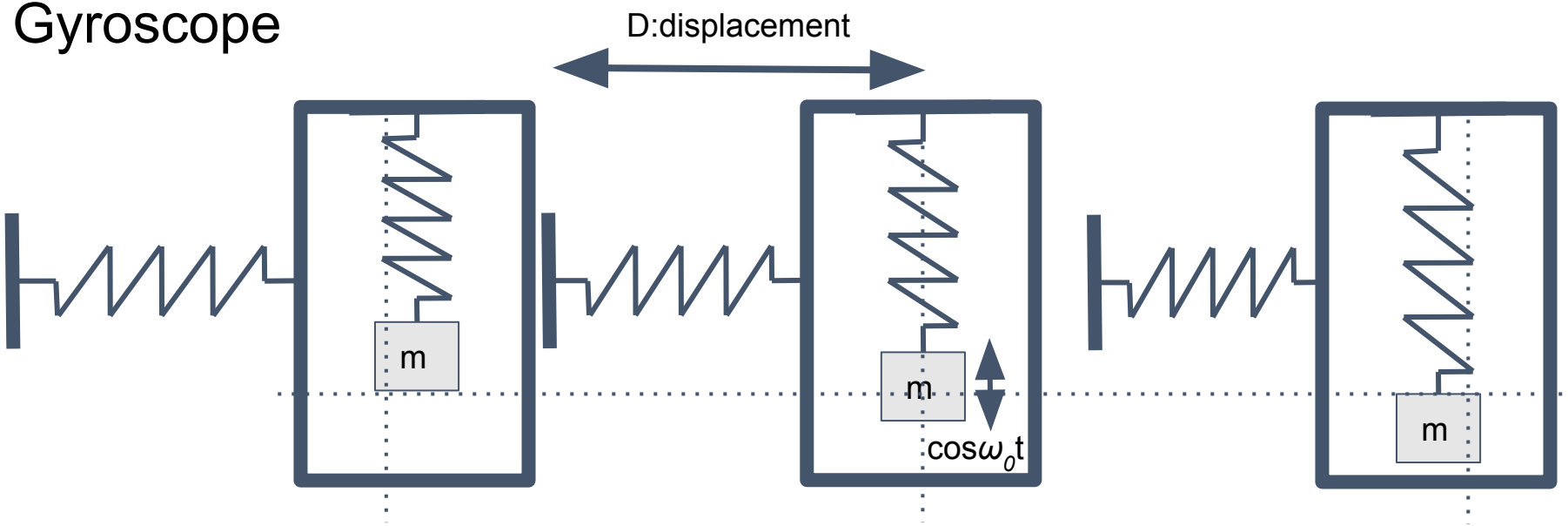


No Rotation

2 DoF (Degree of Freedom)
Spring-Mass System

How MEMS Works

Gyroscope



$D = A \cos \omega_0 t$

$A > 0$: clockwise rotation

$A < 0$: counter clockwise

Coriolis Force

Gyroscope

$$\mathbf{F}_c = 2m\mathbf{v}\times\mathbf{W}$$

$\mathbf{F}_c$ – Coriolis force

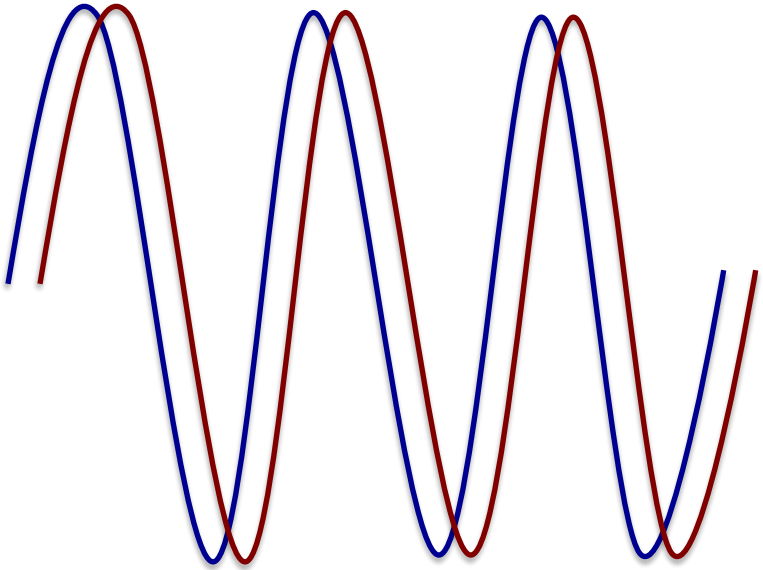
m – vibratory mass

$\mathbf{v}$ – linear velocity

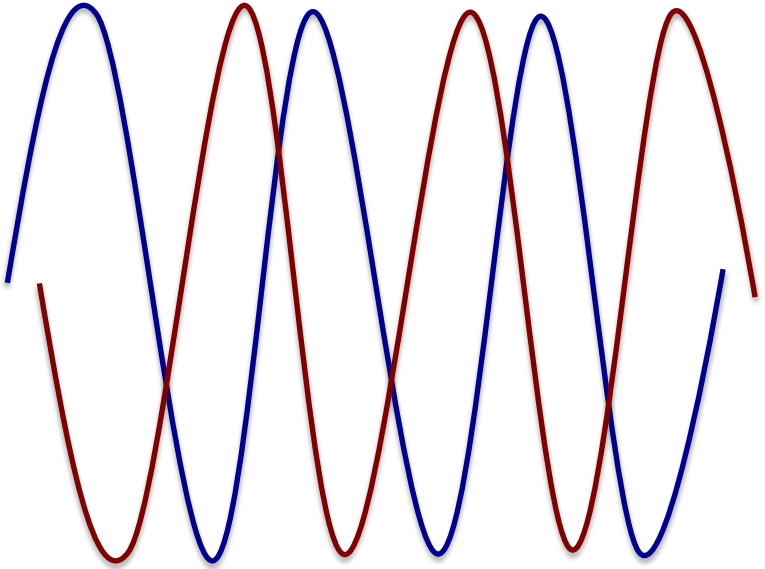
$\mathbf{W}$ - angular rotation

How to Attack

Gyroscope



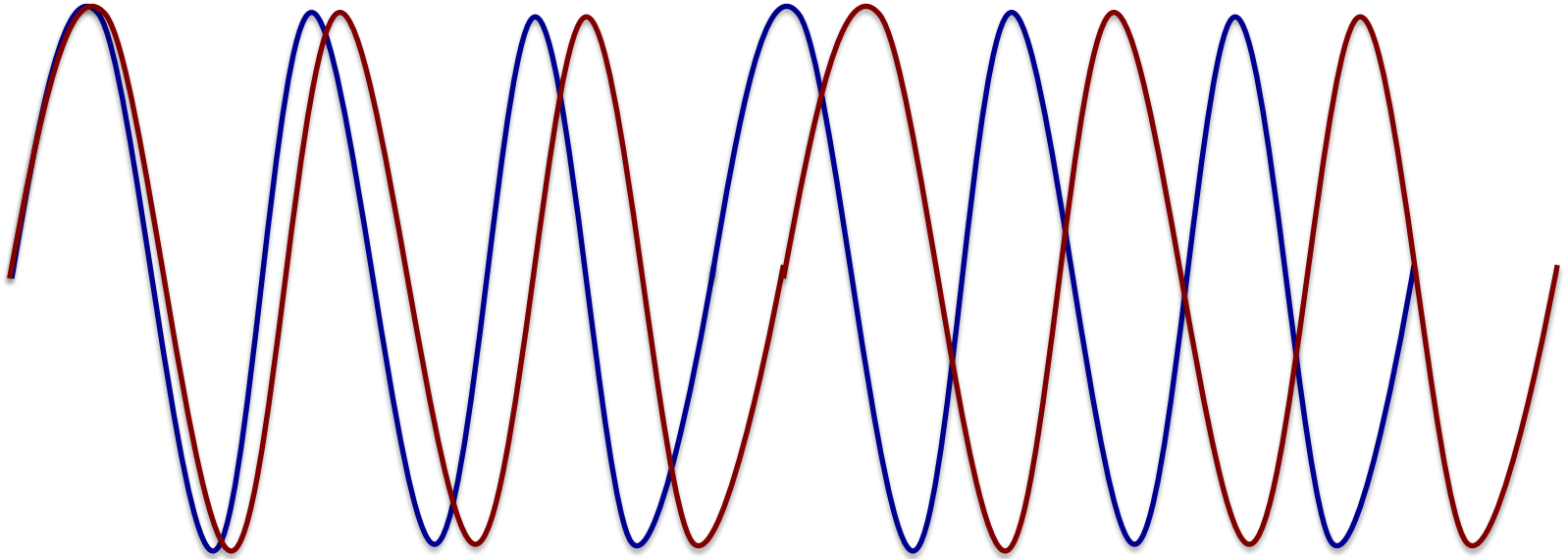
$0 < \Delta\varphi < \pi$
$A > 0$



$pi < \Delta\varphi < 2\pi$
$A < 0$

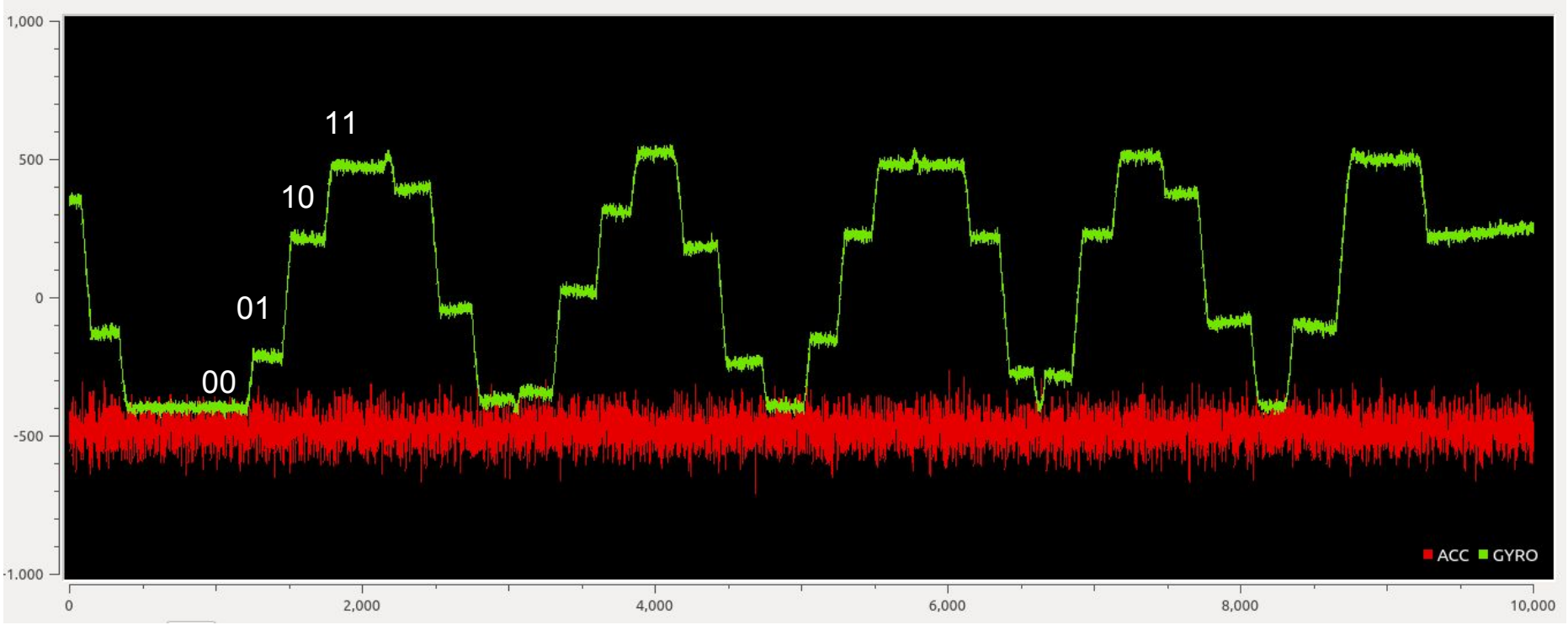
How to Attack

Gyroscope



$\Delta\varphi$: 0 → π

Modulation Demo



Attack Attempts

VR Devices(including Phones)

- Facebook Oculus Rift CV1
- HTC Vive + Controller
- Microsoft HoloLens
- iPhone 7
- Samsung Galaxy S7

Drone

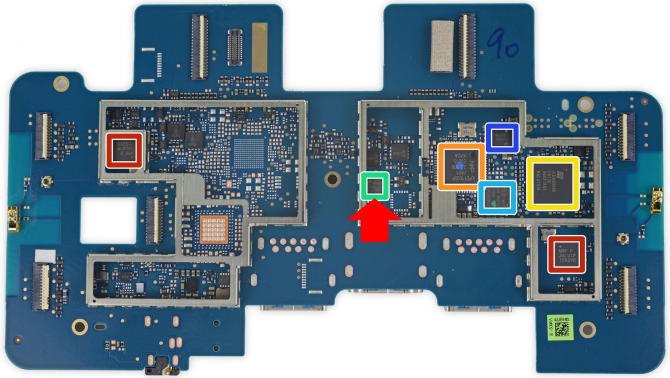
- DJI phantom 3

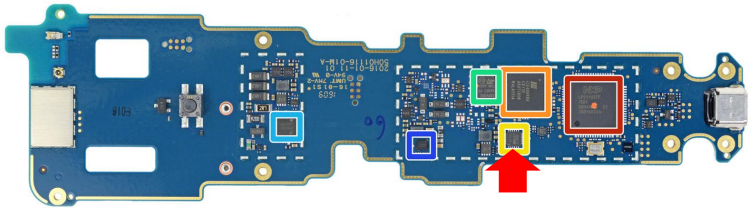
Self Balancing Vehicles(including Toys)

- DIY balancing robot
- Mi Mitu toy robot
- Mi Ninebot Mini

HTC Vive

- HTC Vive Headset





No detailed tear-down Pictures.

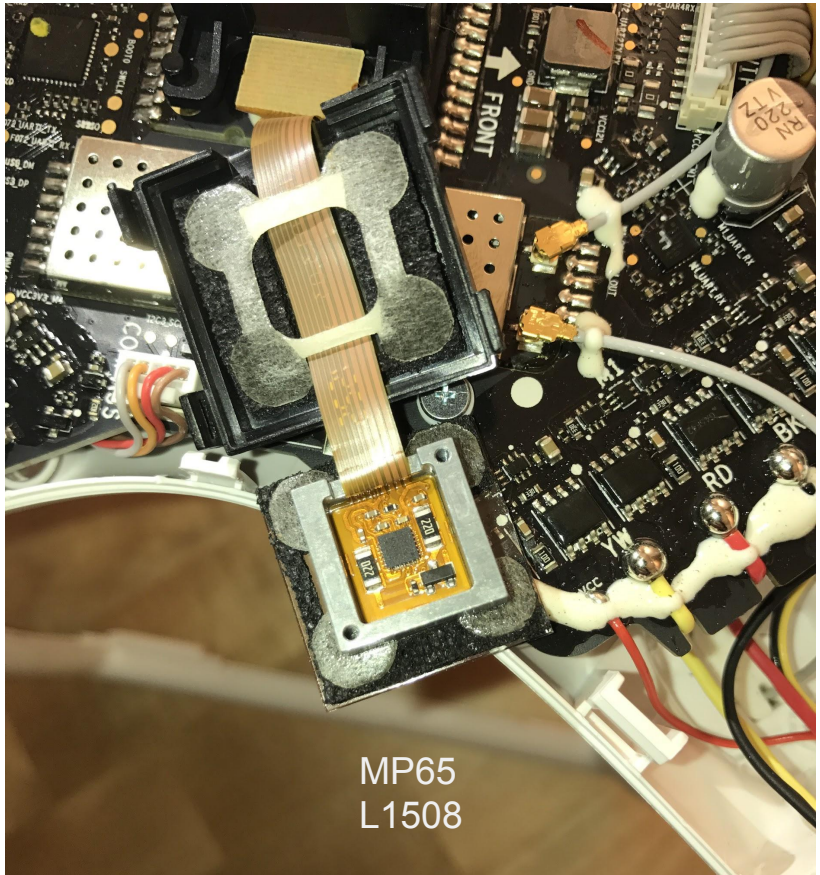
Video Demo: Samsung S7

Unknown chips
Position near rear cam

Video Demo: iPhone 7

Unknown chip

DJI Phantom 3 Standard

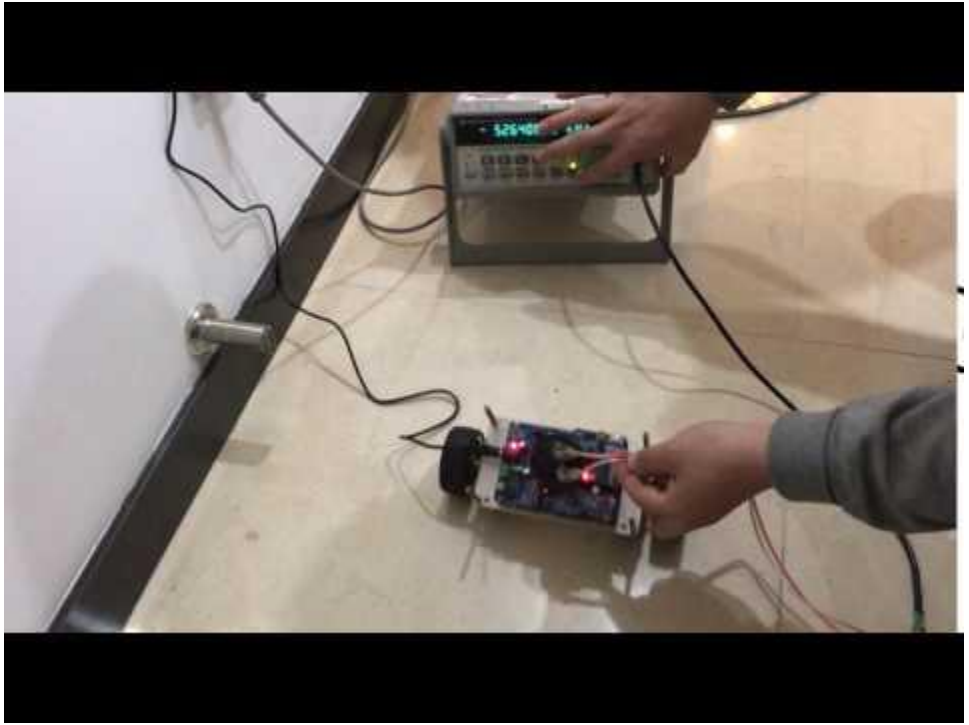


DJI Phantom 3 Standard - Camera

Unknown chips

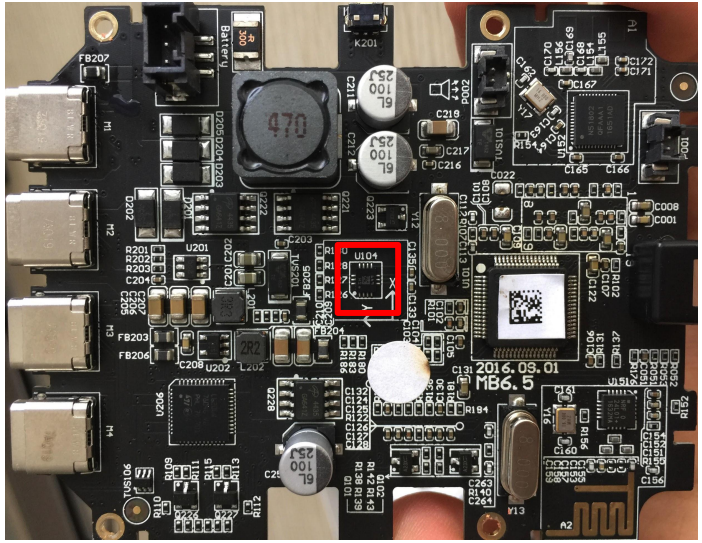
DIY Self-balancing Robot

MPU6050 module



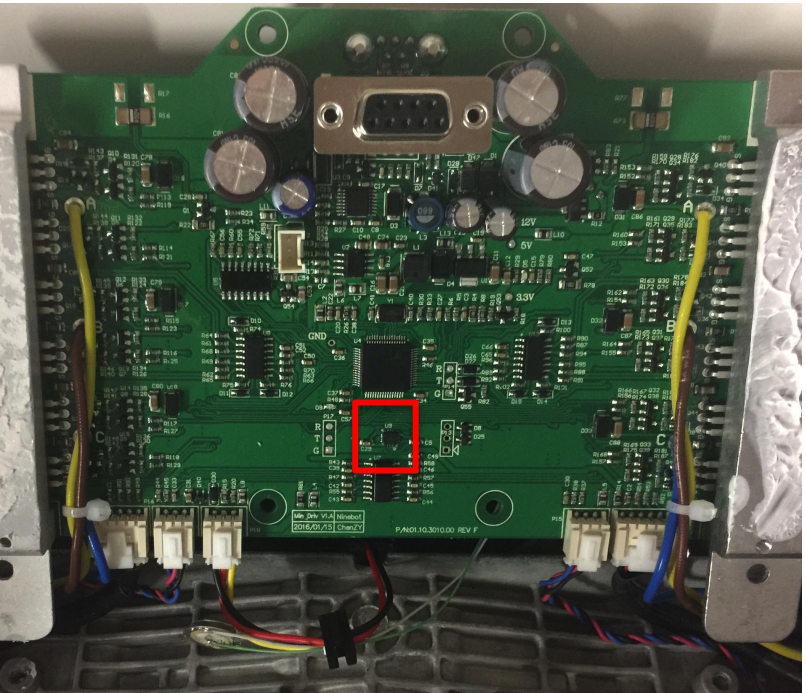
MiTu Self-balancing Robot

- Unknown chip



Commerical Scooter

Unknown chip

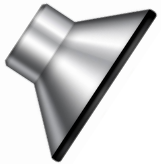


Commerical Scooter

Without PA

With PA

What about real car?



?

BOM

Device	Model	Price
Signal Genenerator	FA20 Max Freq: 20MHz (>> 30kHz) Max Ampl: 20Vpp	$320
Ultrasound Emitter	2425	$0.4
Amplifier	TDA8932	$2
DC Power	LRS-100-24	$10
Signal Generator	UTG9002C Max Freq: 2MHz Max Ampl: 25Vpp	$16

MEMS and Security: An inexhaustive list

	Gyroscope	Accelerometer	Other MEMS*
DoS	Son, et al.	Trippel, et al.	TODO
Manipulation	This work!	Trippel, et al.	TODO
Long Range	TODO	TODO	TODO

* Other MEMS chips include MEMS microphones, barometers, digital micromirror display and so on.

Countermeasures

1. Shell
   - prevent sonic energy from intruding.
   - reflective material with multilayer may be considered.

2. Software
   - actively detect the resonating sound with microphone.
   - warn or perform noise cancelling.

3. Chip
   - new design of MEMS chips that can resist sonic attacks*.

*Serrano D E, et al. PLANS, 2016.

References

1. Man, Kin F. "MEMS reliability for space applications by elimination of potential failure modes through testing and analysis." MEMS Reliability for Critical and Space Applications. Vol. 3880. 1999.
2. Dean, Robert N., et al. "On the degradation of MEMS gyroscope performance in the presence of high power acoustic noise." Industrial Electronics, 2007. ISIE 2007. IEEE International Symposium on. IEEE, 2007.
3. Castro, Simon, et al. "Influence of acoustic noise on the dynamic performance of MEMS gyroscopes." ASME 2007 International Mechanical Engineering Congress and Exposition. American Society of Mechanical Engineers, 2007.
4. Son, Yunmok, et al. "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors." USENIX Security. 2015.
5. Trippel,Timothy, et al. "WALNUT: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks." In Proceedings of the 2nd IEEE European Symposium on Security and Privacy (Euro S&P 2017). To appear.
6. Mikko Saukoski. System and circuit design for a capacitive mems gyroscope, Doctoral Dissertation, 2008.
7. Serrano D E, et al. Environmentally-robust high-performance tri-axial bulk acoustic wave gyroscopes. Position, Location and Navigation Symposium (PLANS), 2016.

Acknowledgement

Sun, Yinan - Tsinghua University

Q&A

Thank you.