# 6.808: Mobile and Sensor Computing aka IoT Systems

http://6808.github.io

## Lecture 13: IoT Security
## Cyber-Physical Security and Acoustic Attacks

Some slides adapted from Nirupam Roy (UMD College Park)

### Course Staff


**Lecturers:** Fadel Adib (fadel@mit.edu)

Hari Balakrishnan (hari@csail.mit.edu)

Maya Nielan (mnielan@mit.edu)

Sayed Saad Afzal (afzals@mit.edu)


### Announcements

1- Project Proposals due March 16

2- Lab 4 out; due March 30

3- PSet 2 due April 4

4- Grades will be out this week

# Project Timeline


Feedback to refine your ideas

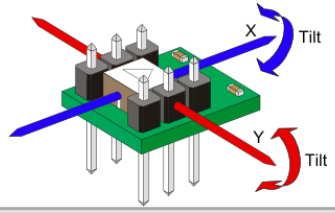
1. Feedback is to help you excel on the final project
2. Project is biggest chunk of class (40%) - by comparison, labs combined are 25%
3. Started learning the challenge in an IoT system: motivation, idea, time, $

# Class Timeline

## 4 Quadrants of IoT

### Sensing Tasks & Modalities

- Localization
- Inertial
- Camera-based




### Computation

Sensor Proc. & Fusion (localization, inertial, split proc., fusion)

### Power/Energy

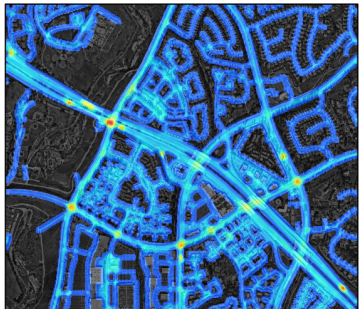
Energy management & harvesting

### Connectivity

- Connectivity tech
- Mesh architectures
- Battery-free IoT

## Emerging Application Domains & Cross-Cutting Topics

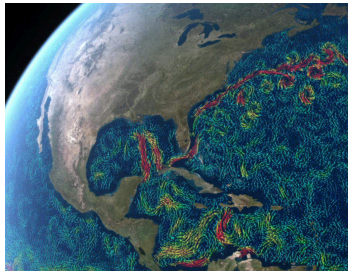
1. Transportation



2. Health


3. Agriculture

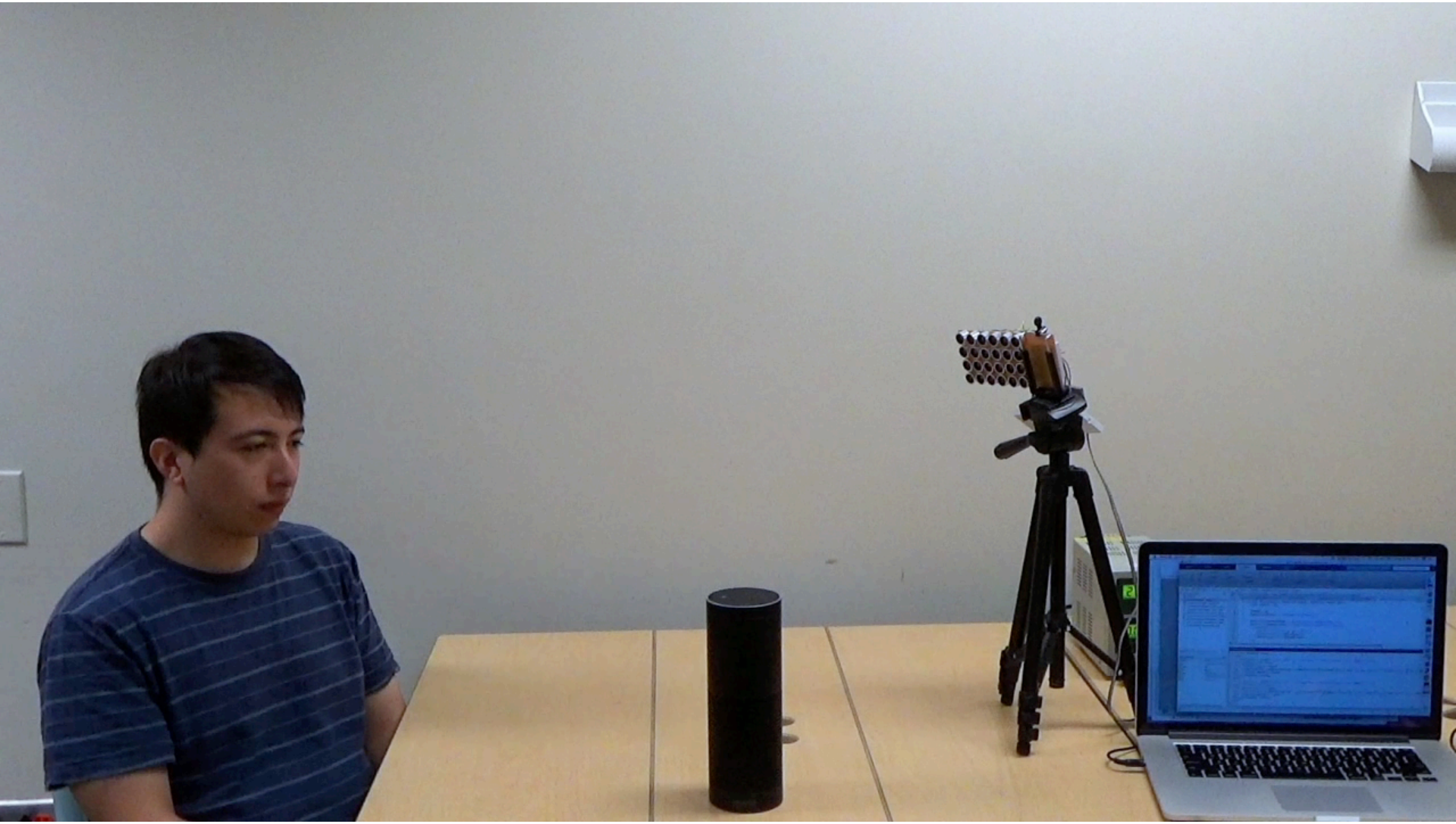
4. Oceans/ Climate



5. Security/ Privacy

This lecture

# Mobile Security
# Inaudible Voice Commands




YAMAHA
LINE3

# Light Commands
Hacking using Laser


UEC
TOKYO

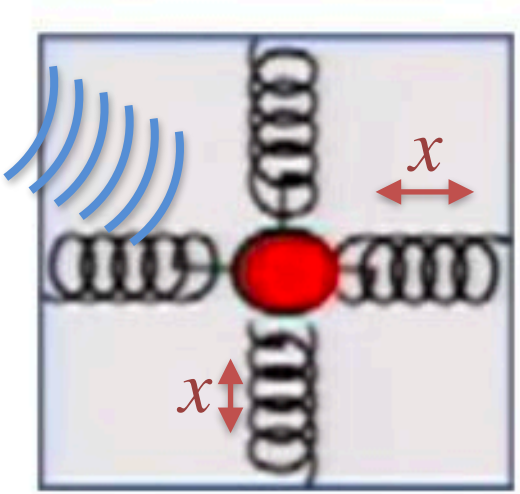

CSE
COMPUTER SCIENCE
AND ENGINEERING
UNIVERSITY OF MICHIGAN

# LIGHT COMMANDS

# Analog Sensor Security
# Acoustic Attacks on MEMS Accelerometers


TITANIUM BULLET TWEETER
PYRAMID

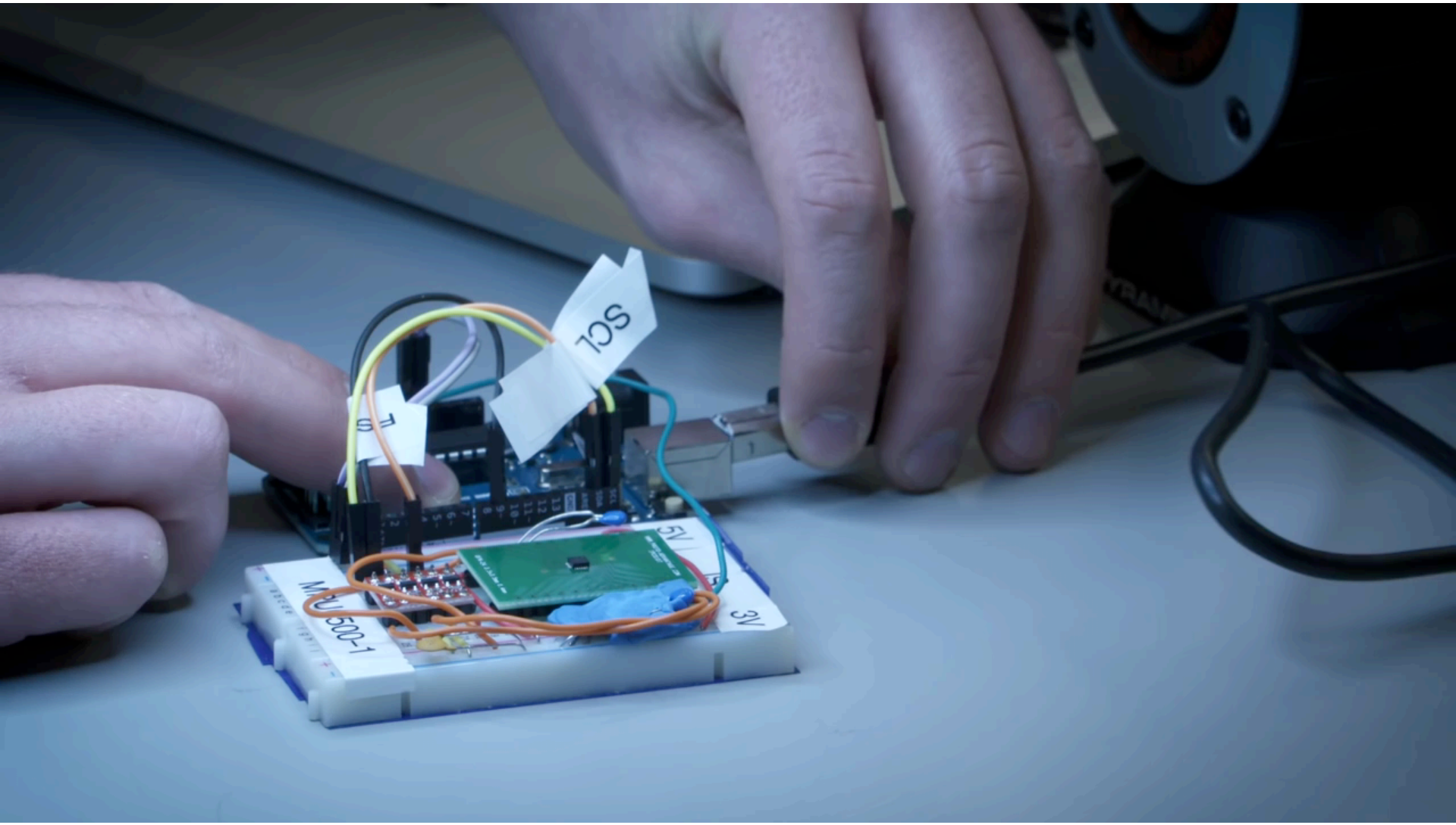
Acoustic
"pressure" waves



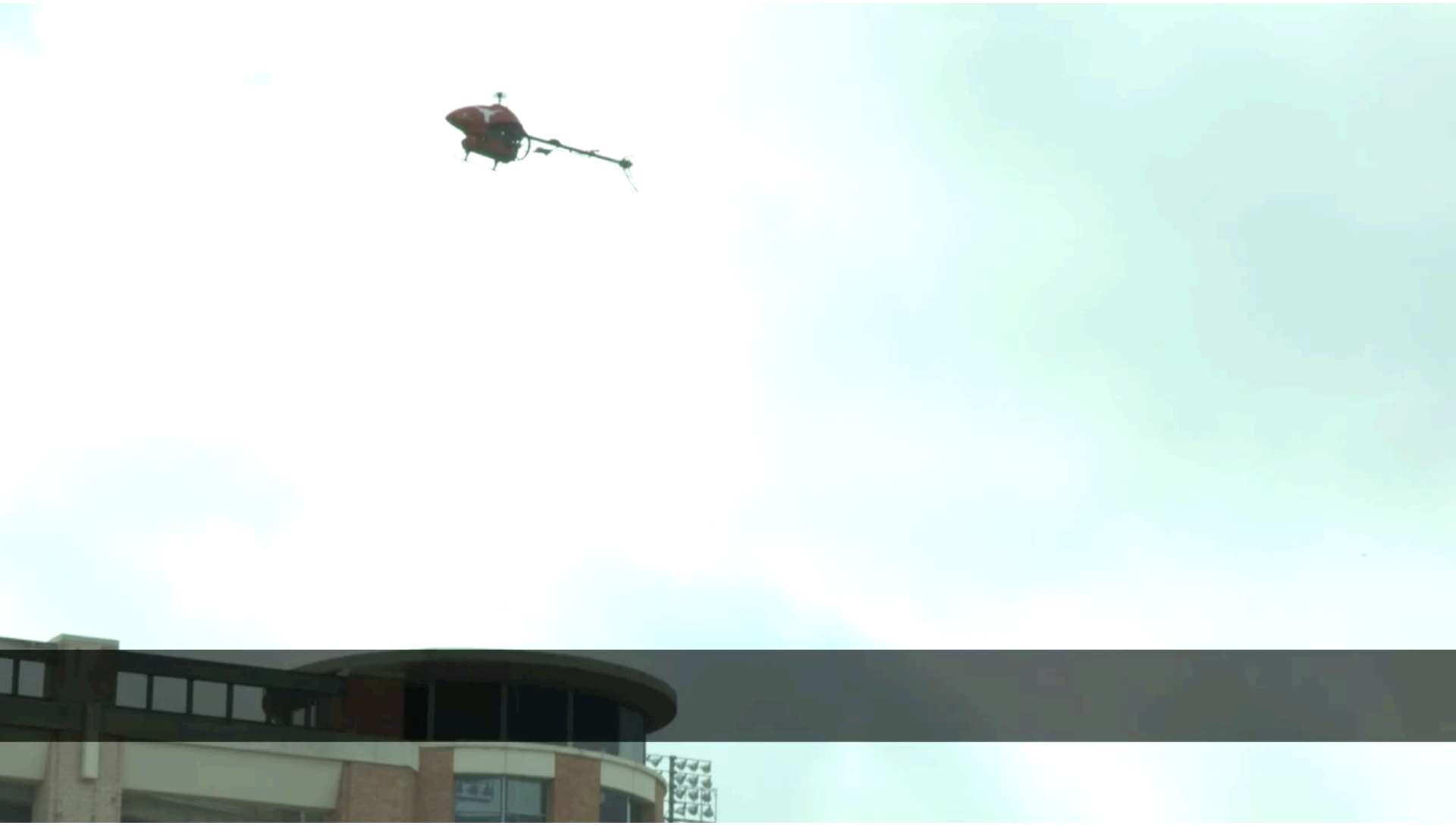

$$F = ma = kx$$

acceleration

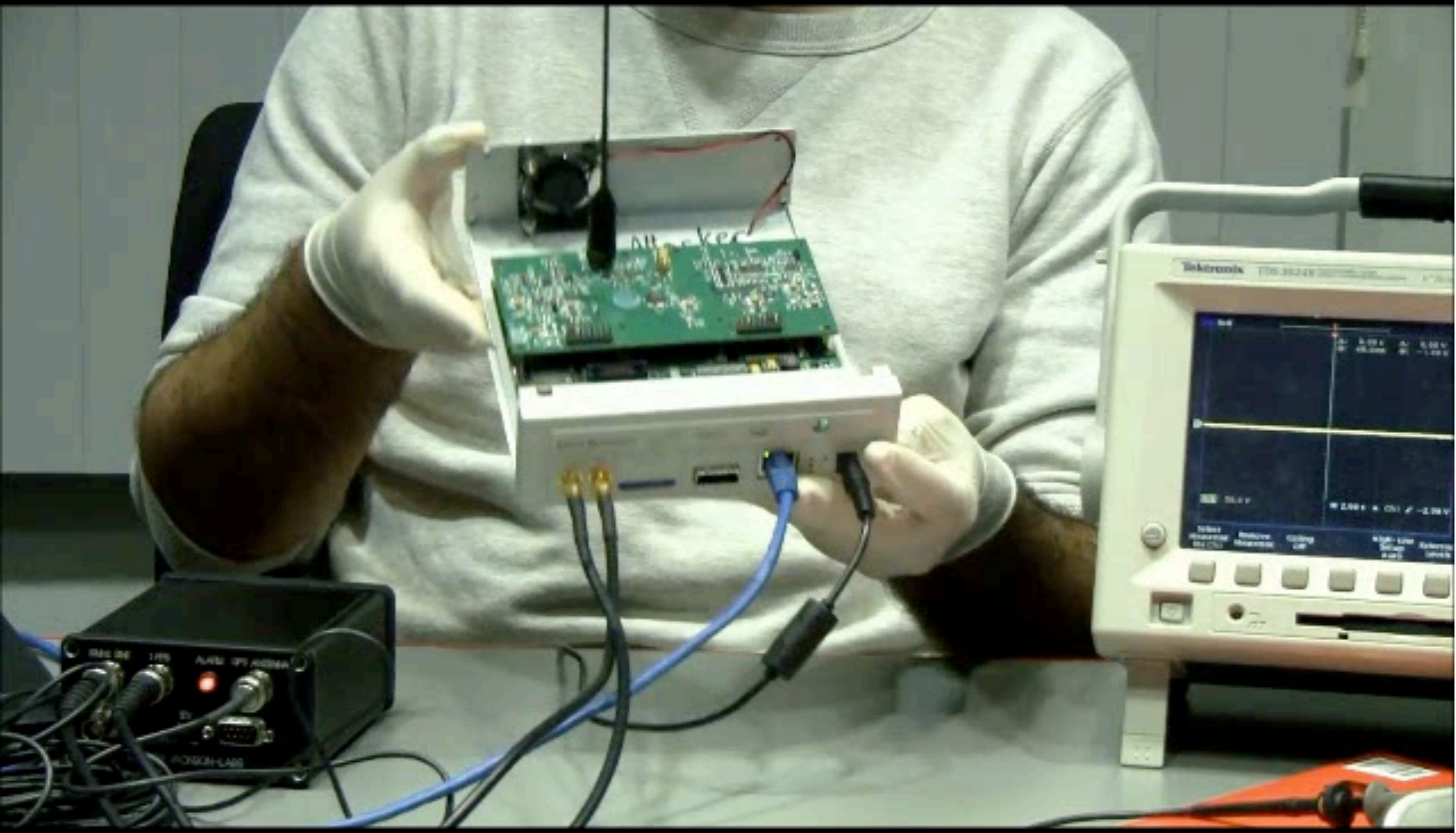
measure
displacement


SCL
5V
3V
MPU 6500-1

# Drone Security
## Spoofing GPS Signals

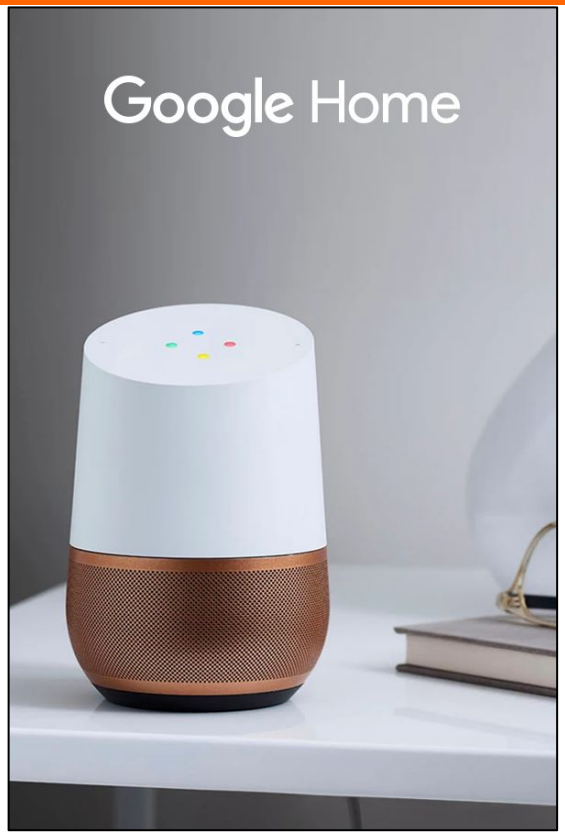


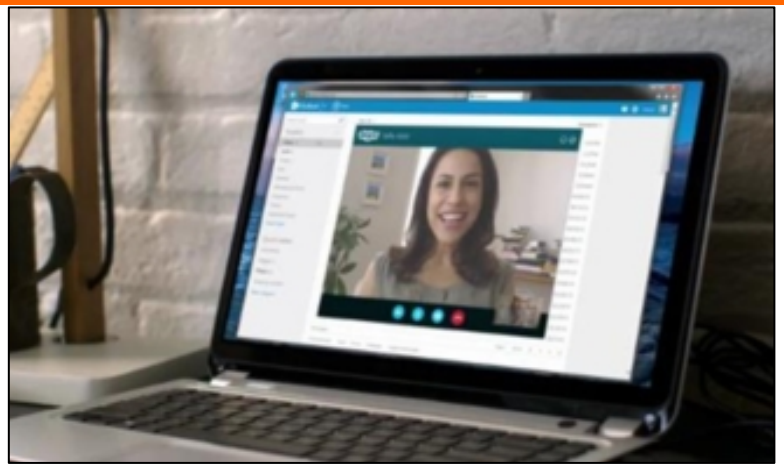
# Pacemaker Security
# Wireless Control of Pacemaker

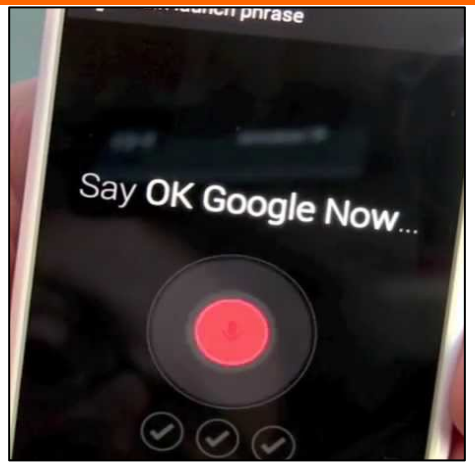

Tektronix

# BackDoor: Making Microphones Hear Inaudible Sounds

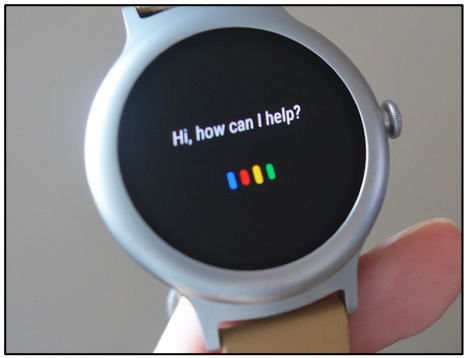
# Microphones are everywhere



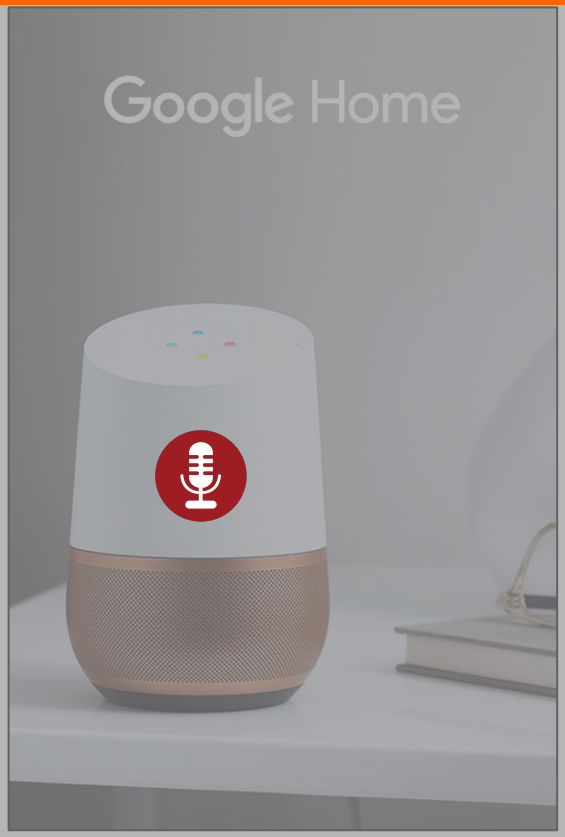


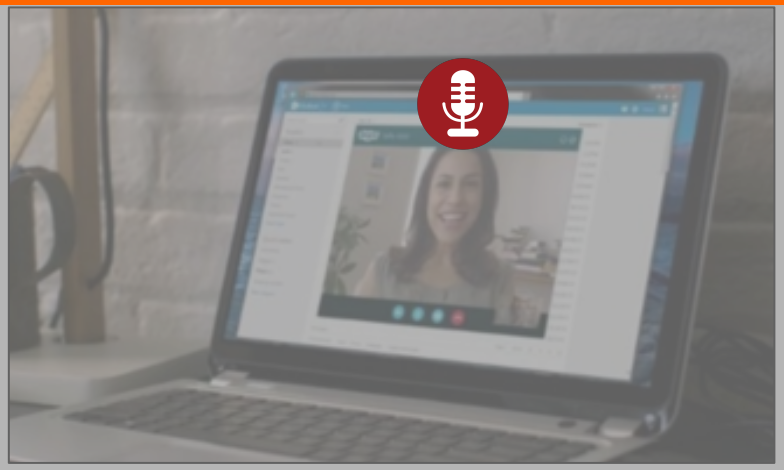


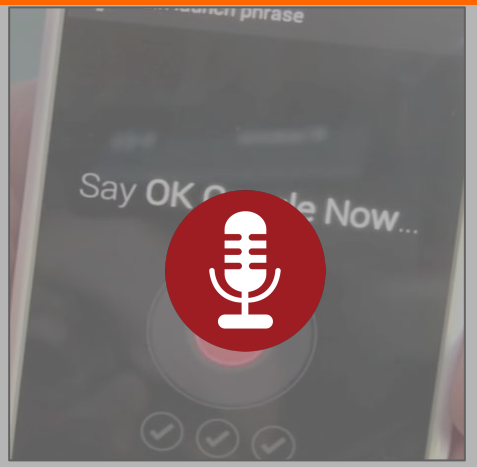




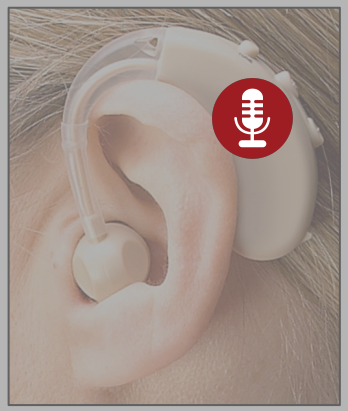
# Microphones are everywhere

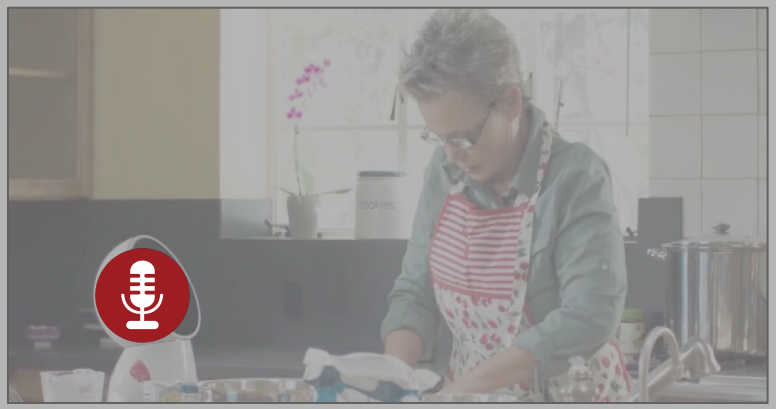


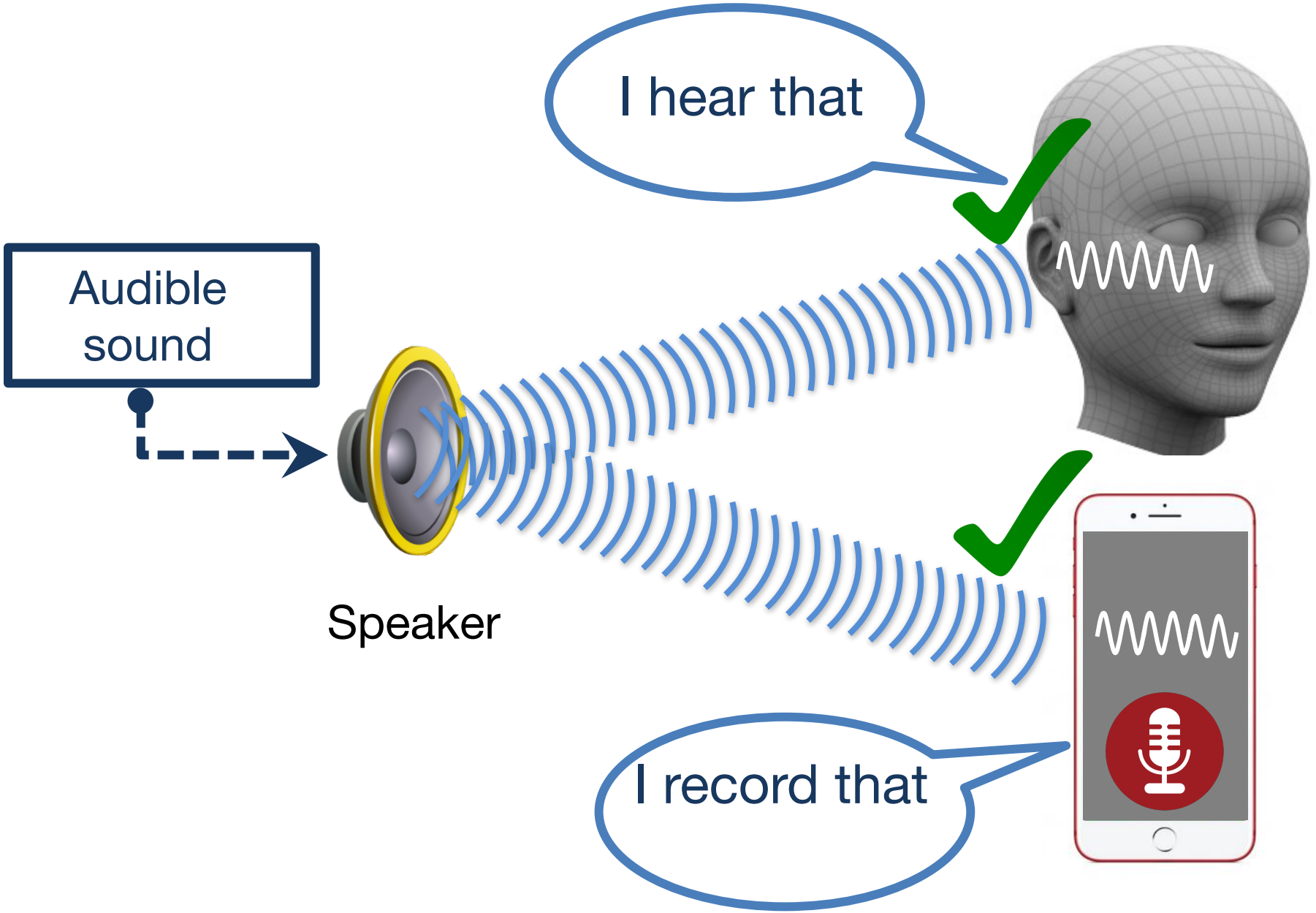




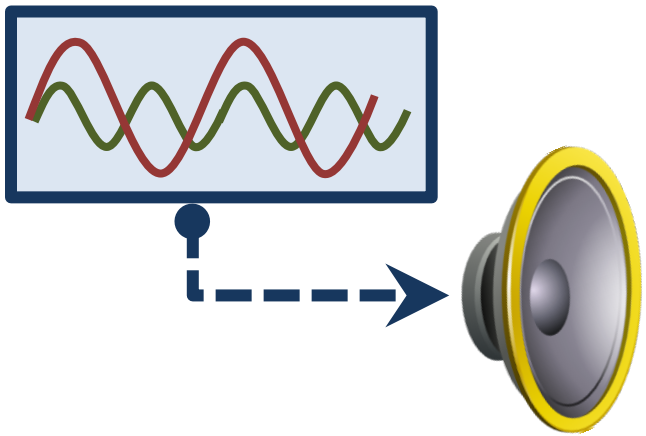


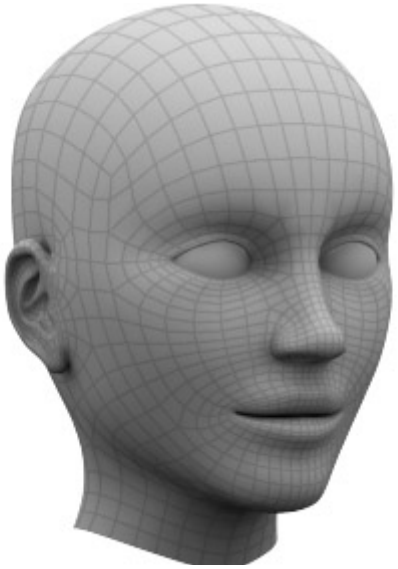
# Microphones record audible sounds



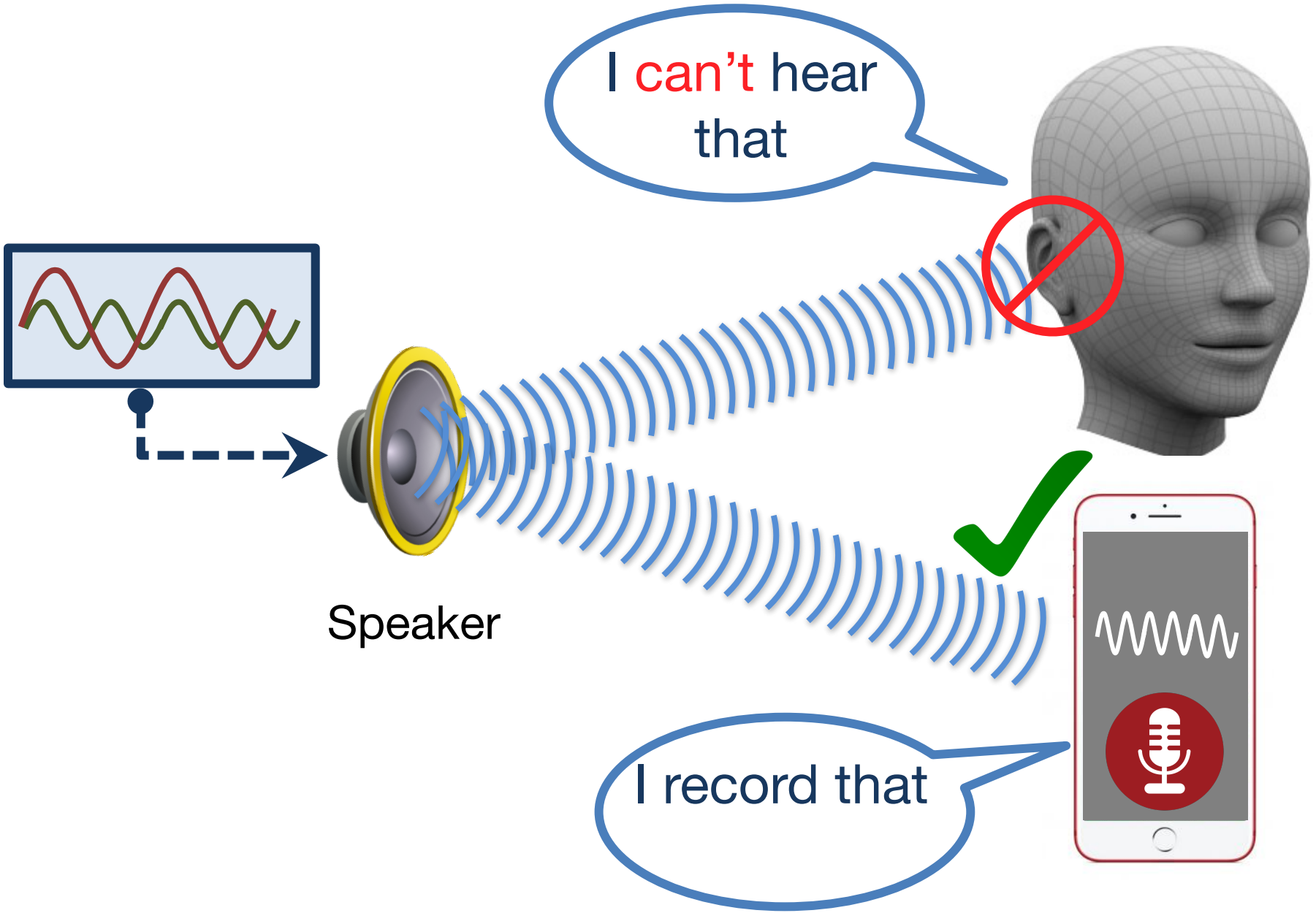
# Inaudible, but recordable !



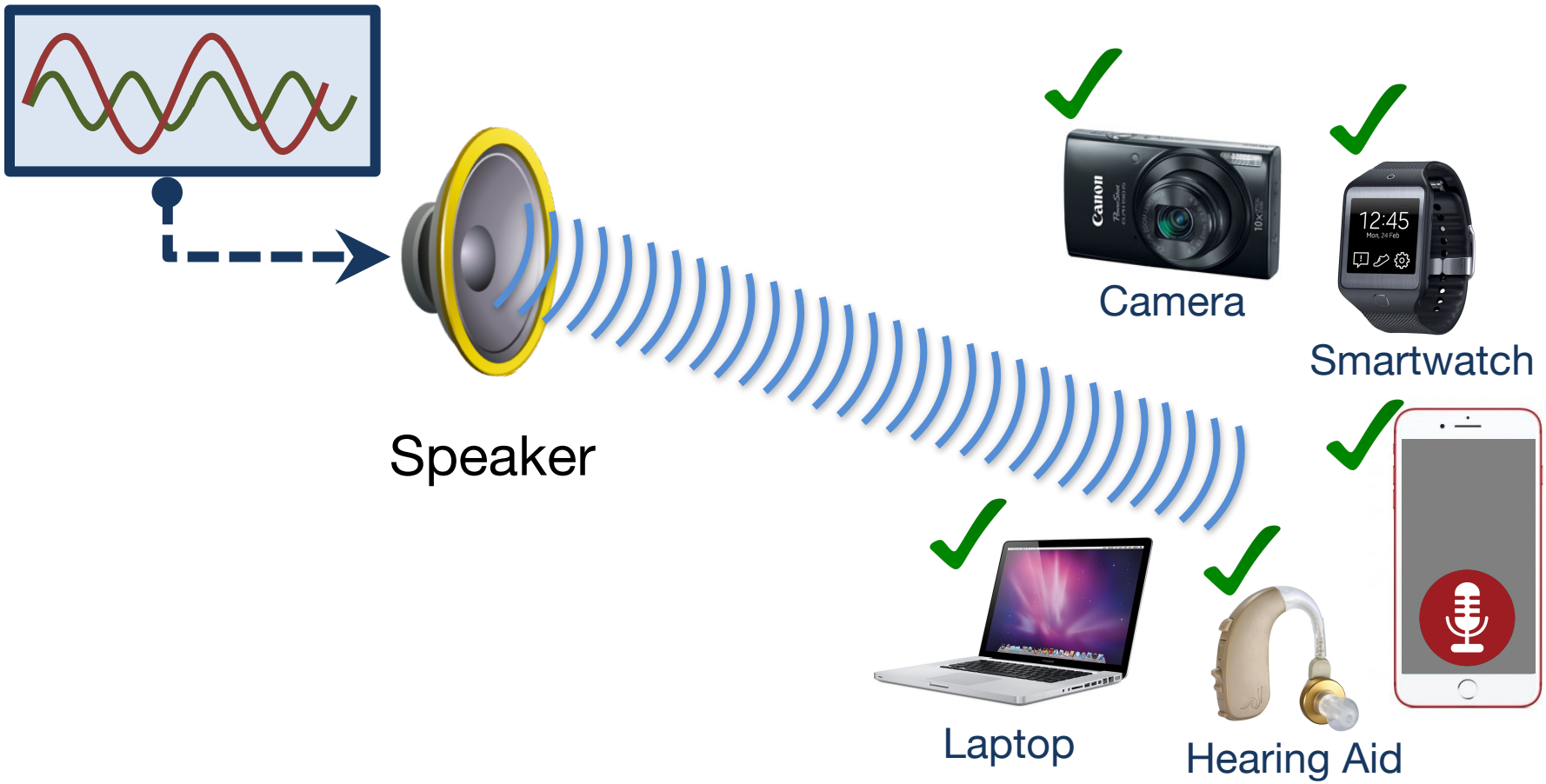
Speaker



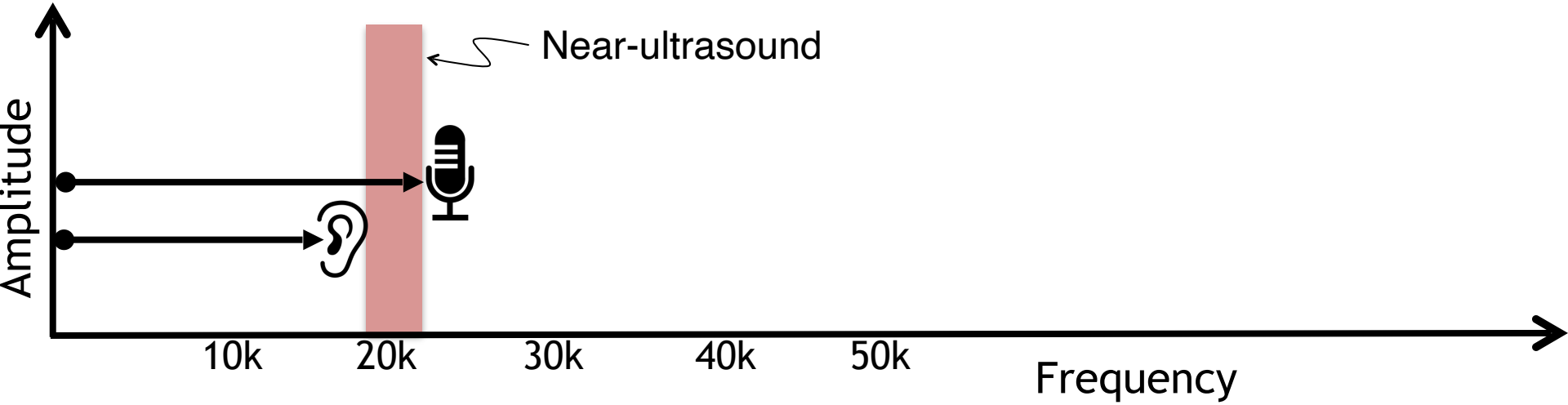
# Inaudible, but recordable !



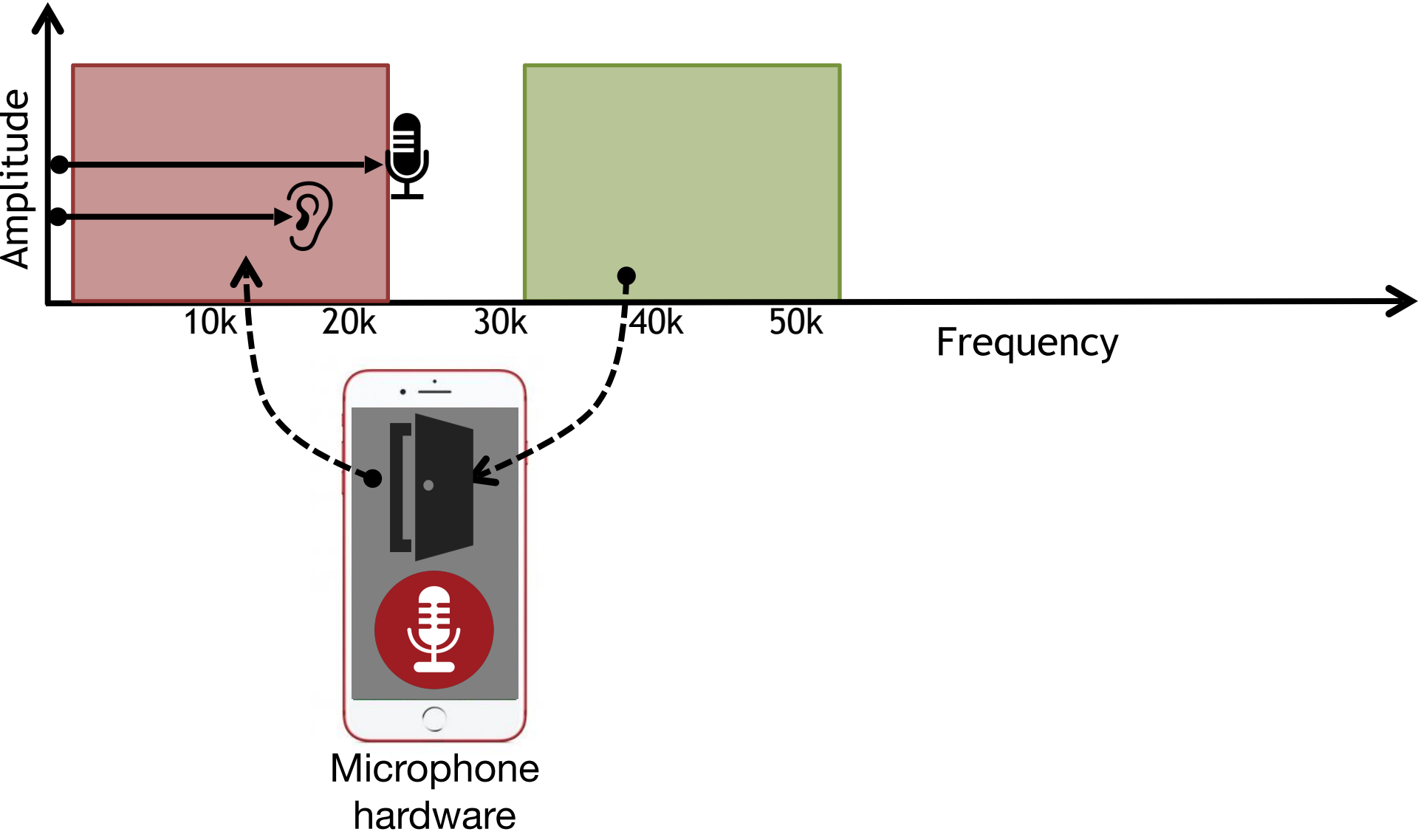
# Works with unmodified devices



# It's not "near-ultrasound"



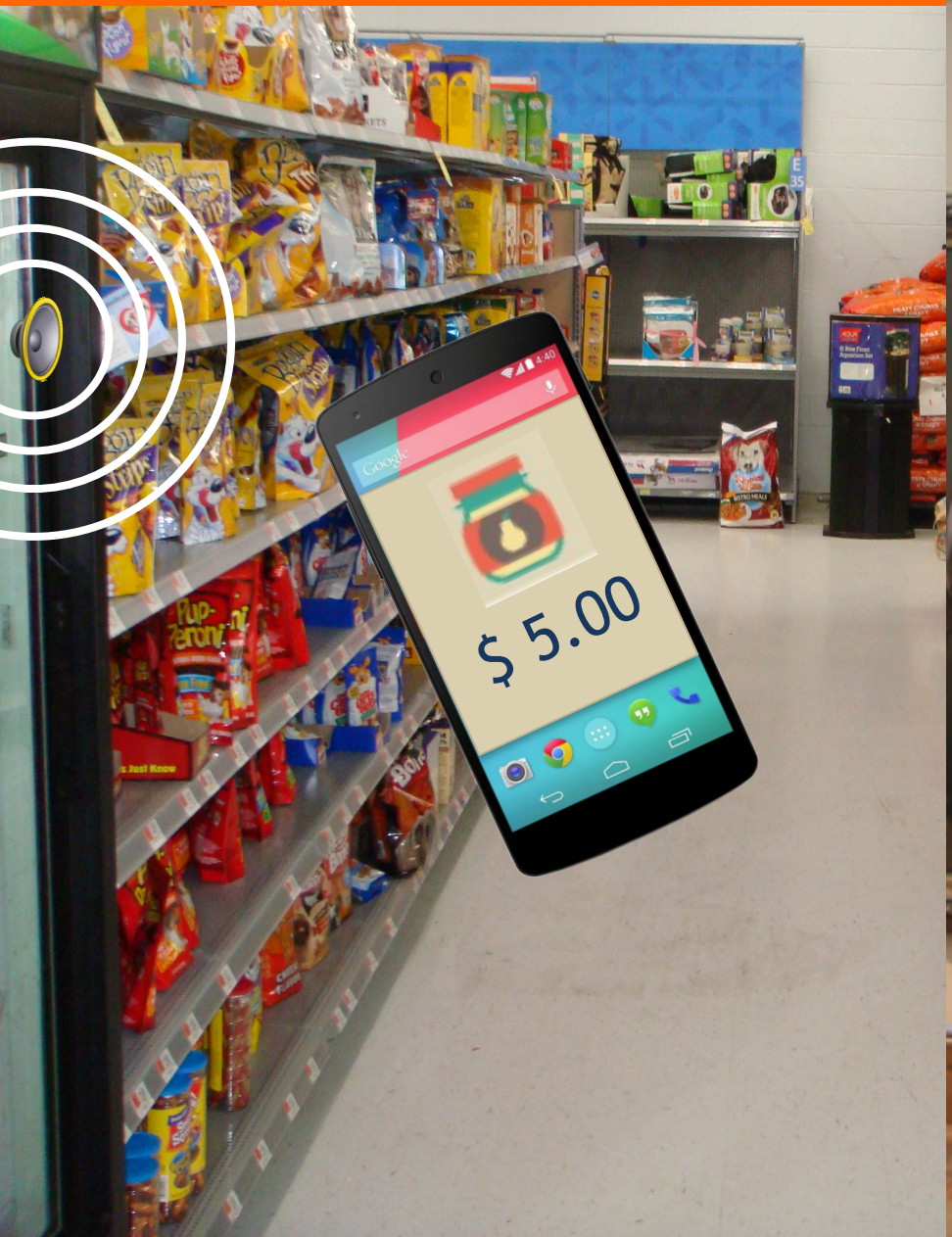
# Exploiting fundamental nonlinearity



# What can we do with it?

# Application: Acoustic jammer

# Application: Acoustic communication




# Threat: Acoustic DOS attack

# Threat: Acoustic DOS attack

Jamming
hearing aids

# Threat: Acoustic DOS attack

Jamming
hearing aids

Blocking
911 calls

# Talk outline

① Microphone Overview

② System Design

③ Challenges

④ Evaluation

# Talk outline

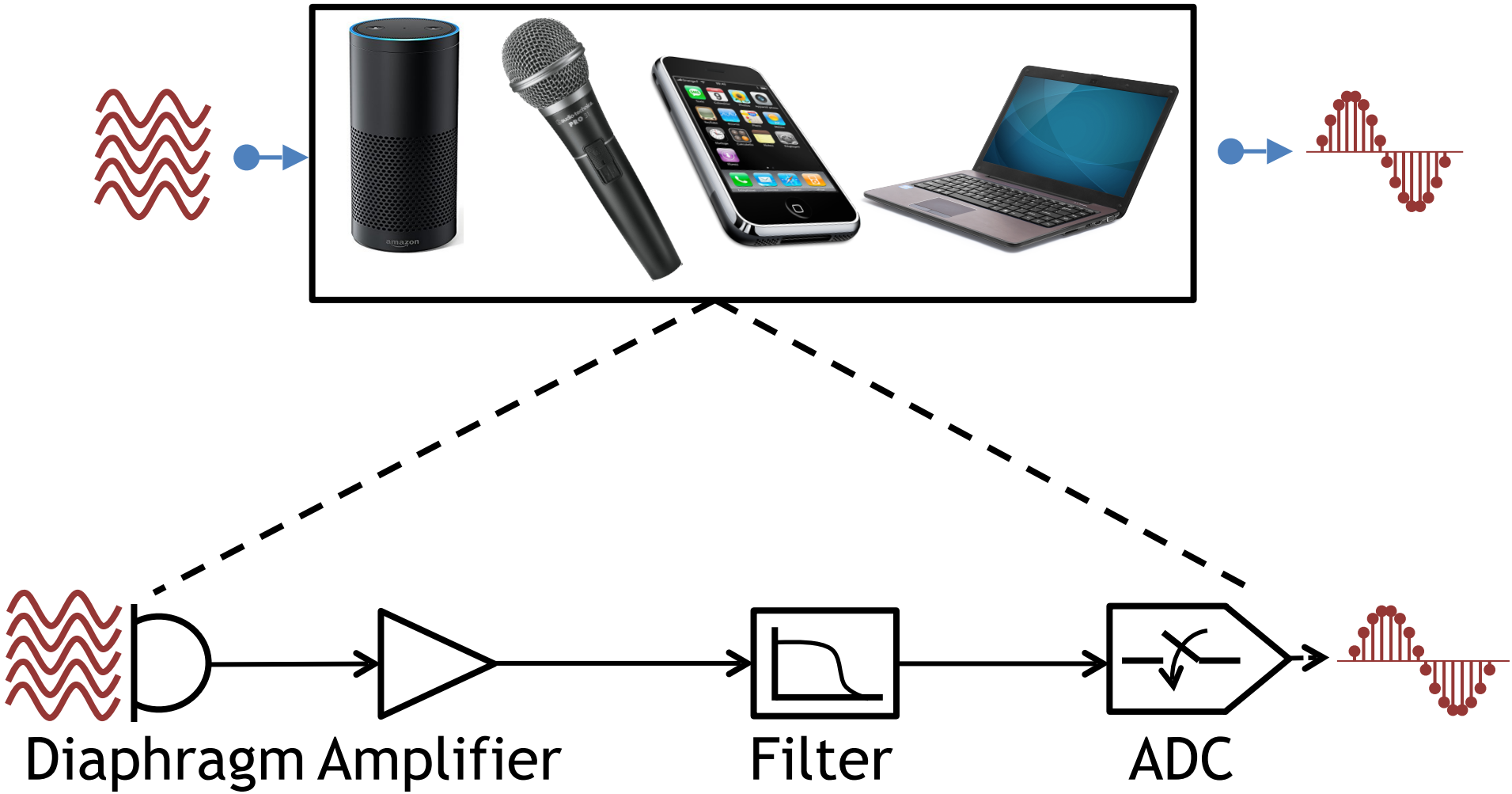
① Microphone Overview

② System Design

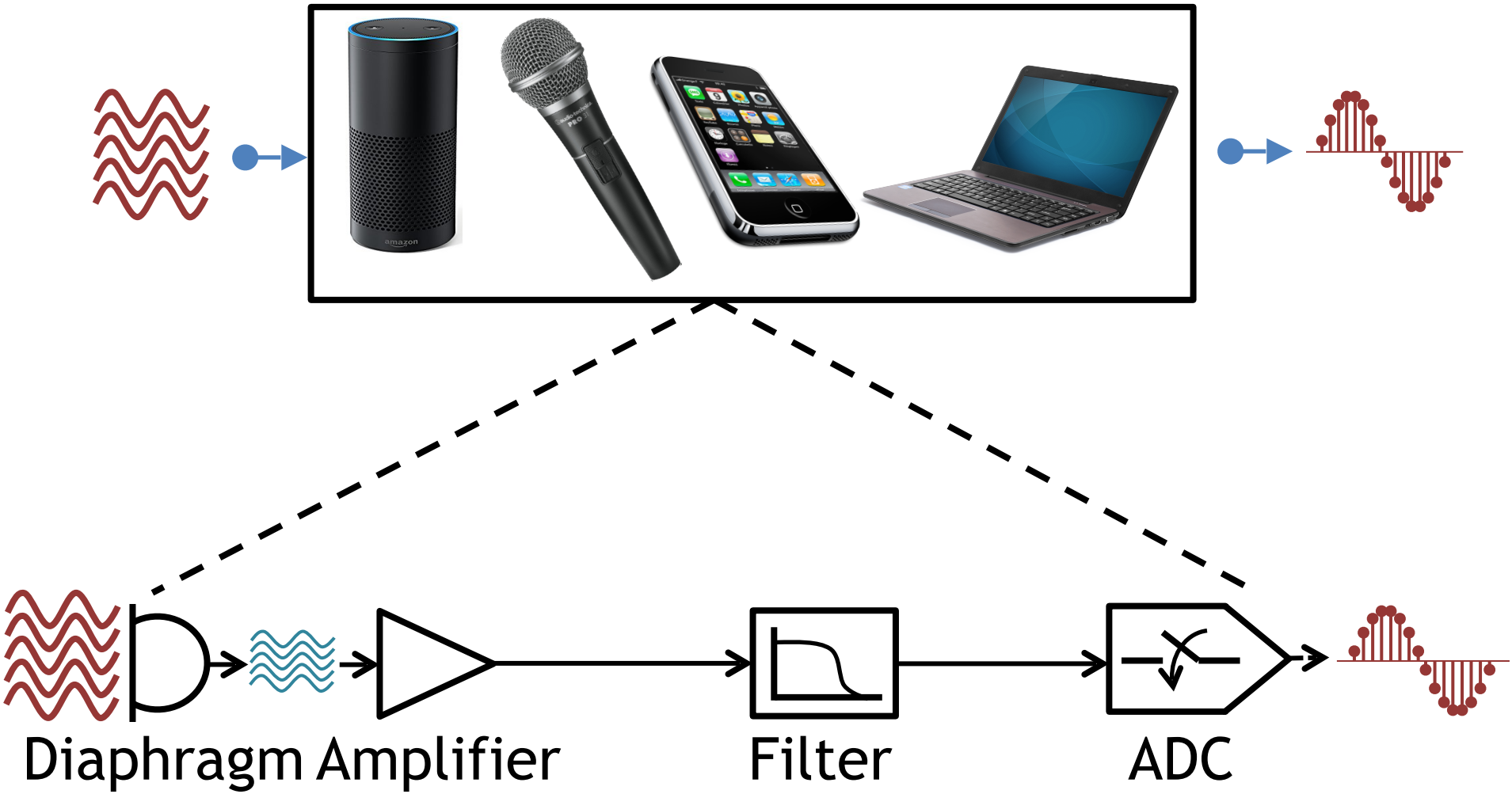
③ Challenges

④ Evaluation

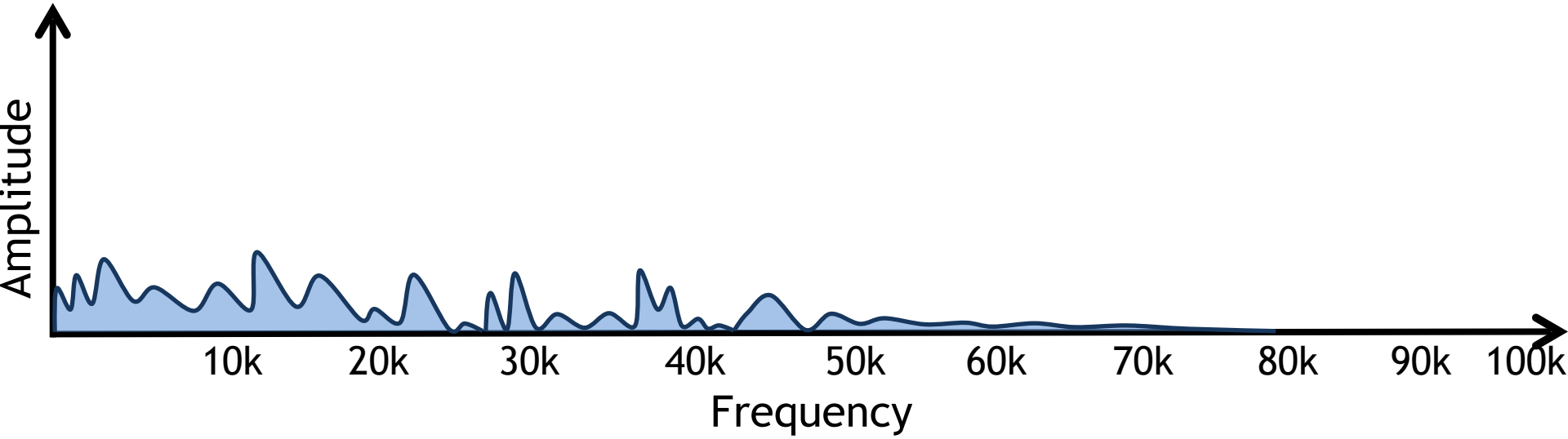
# Microphone working principle

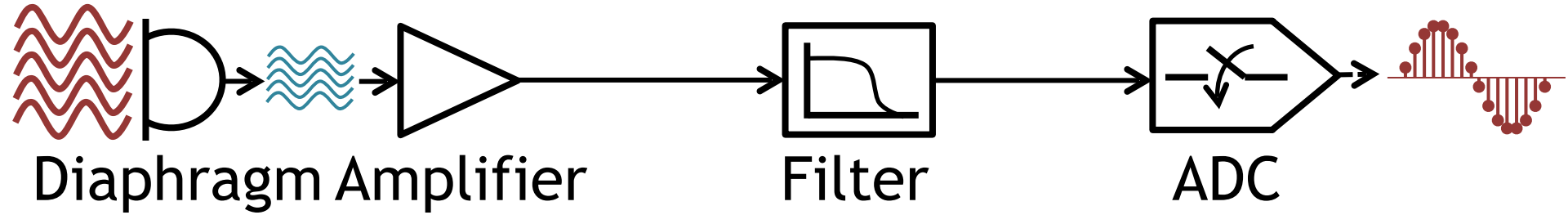


# Microphone working principle

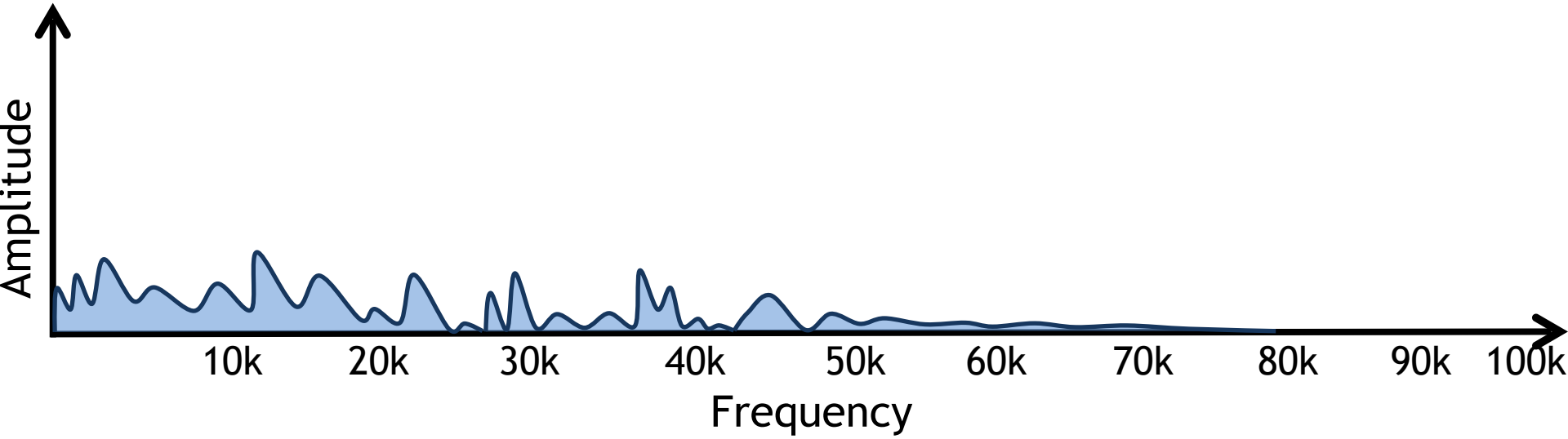


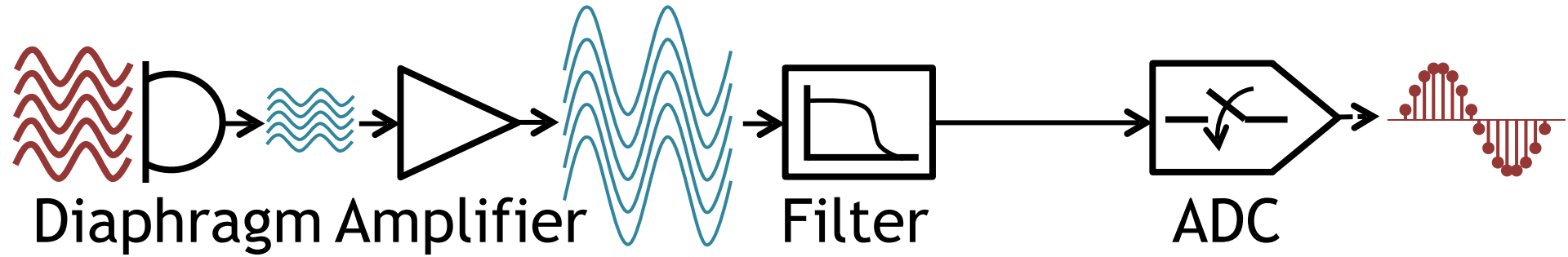
# Microphone working principle



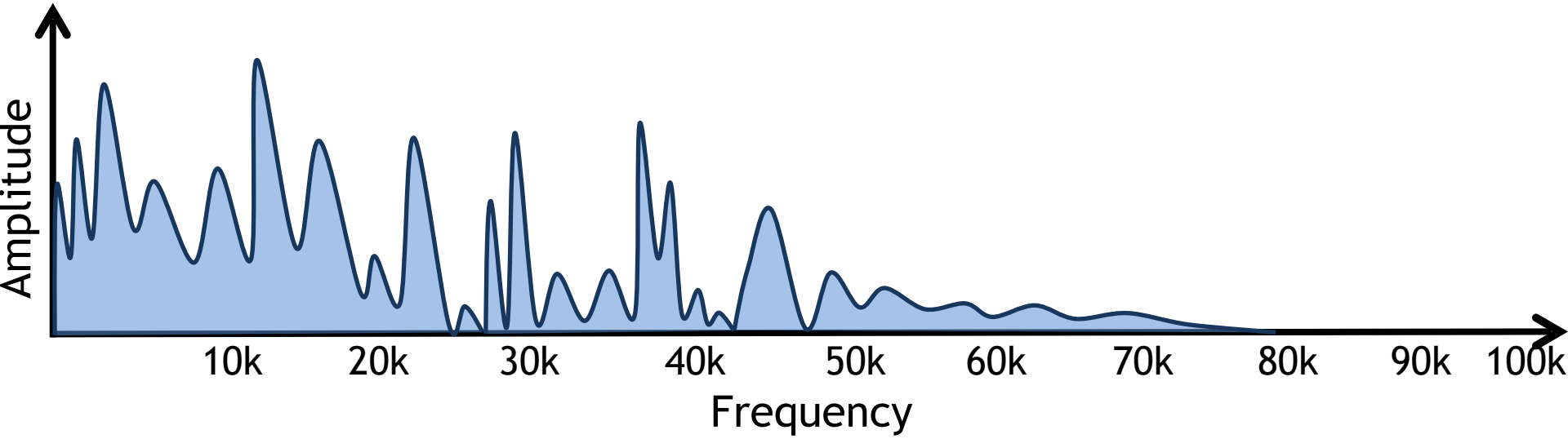



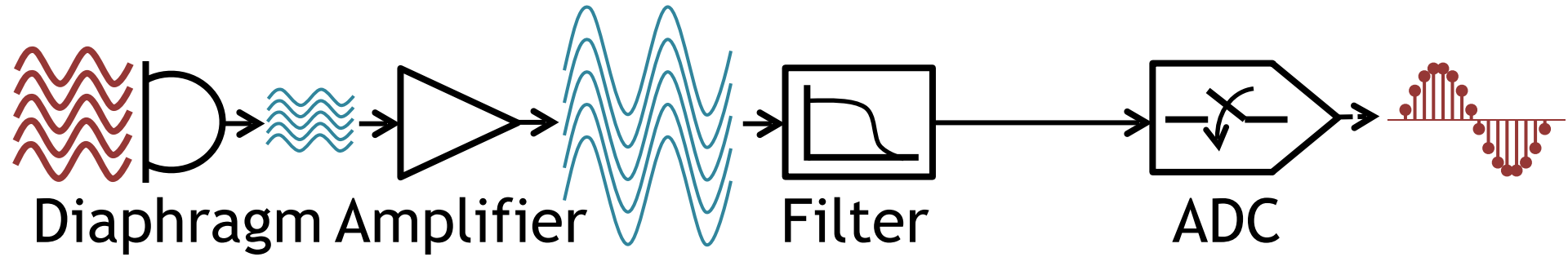
# Microphone working principle



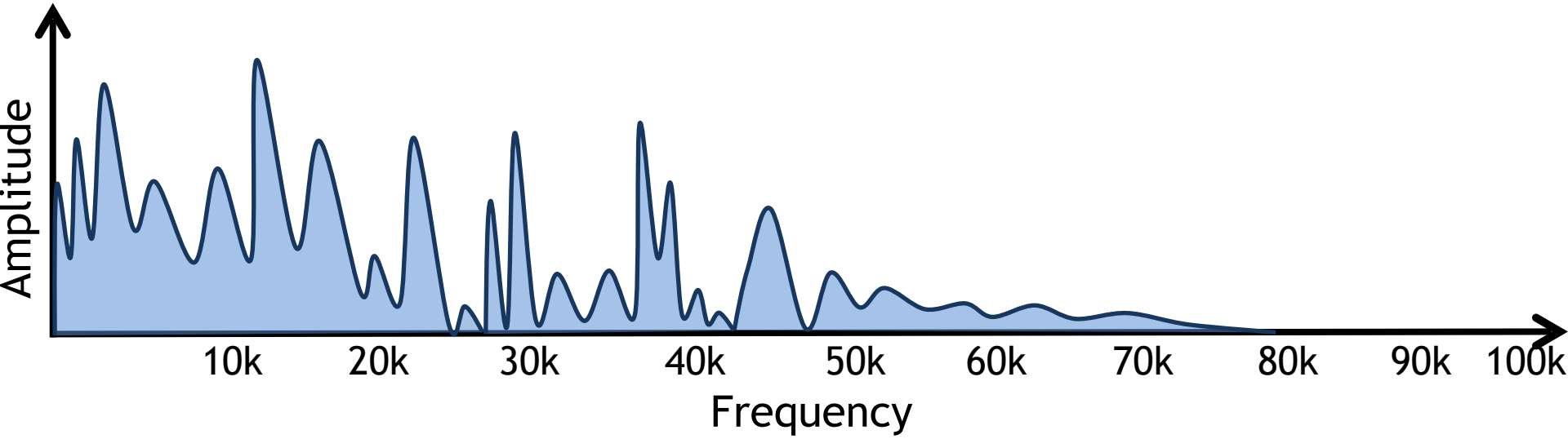



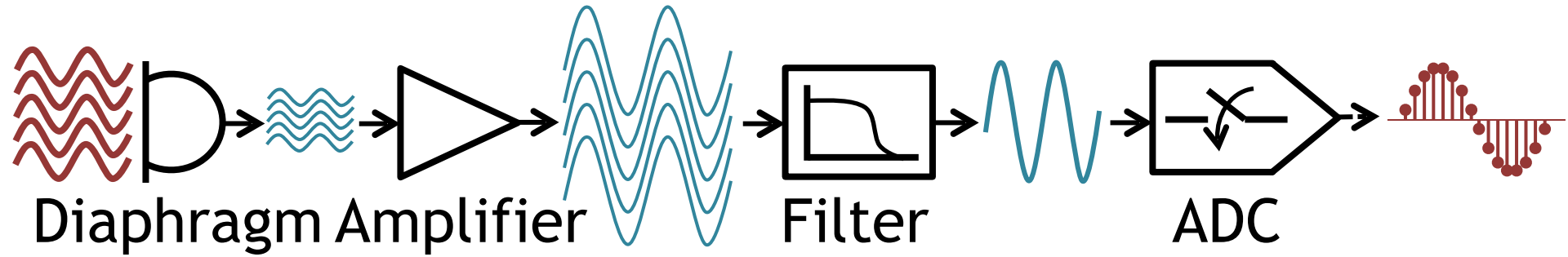
# Microphone working principle



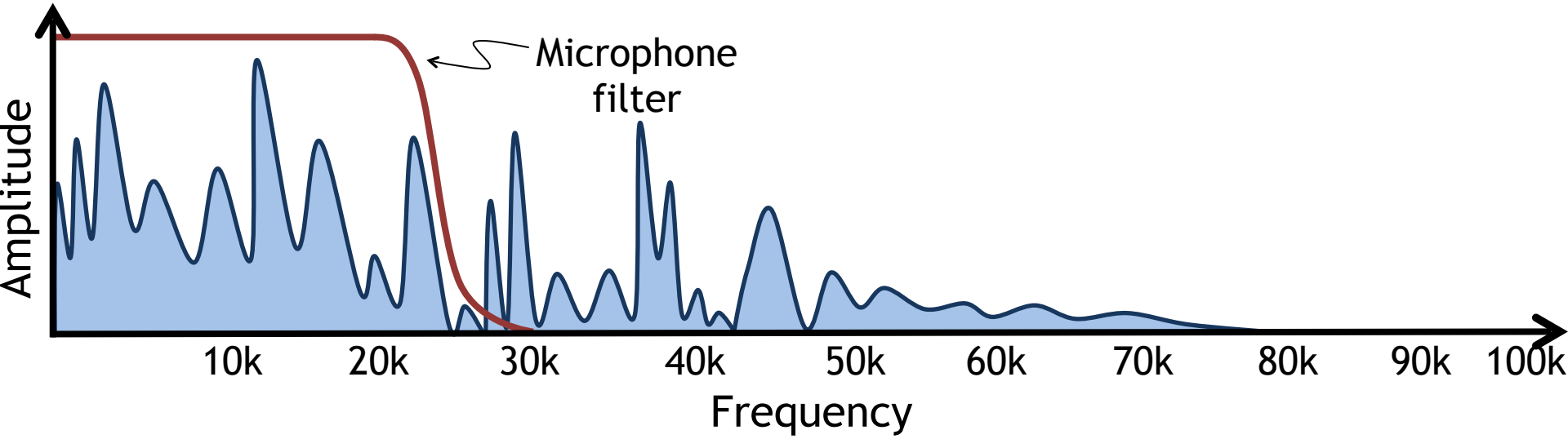



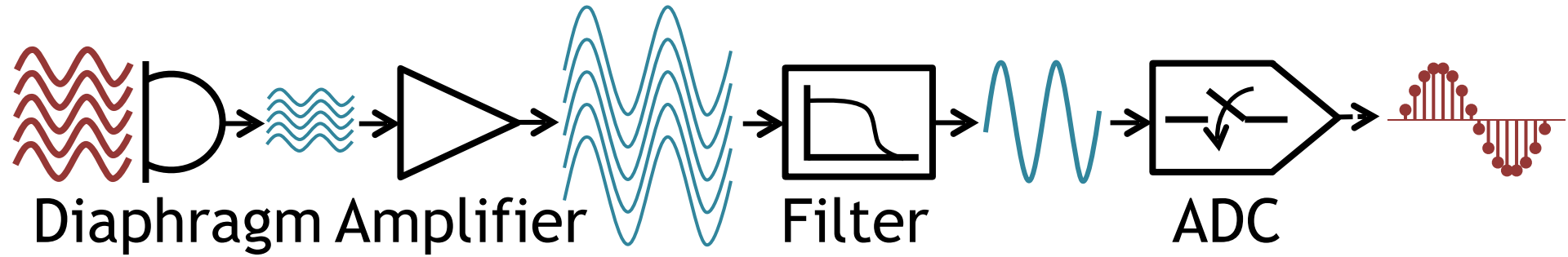
# Microphone working principle



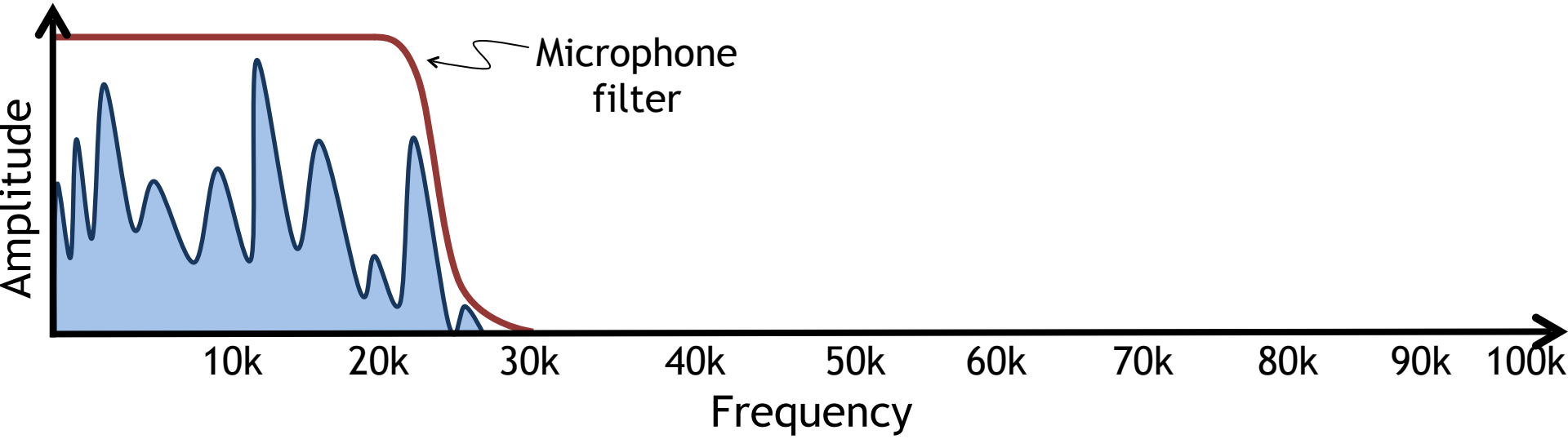



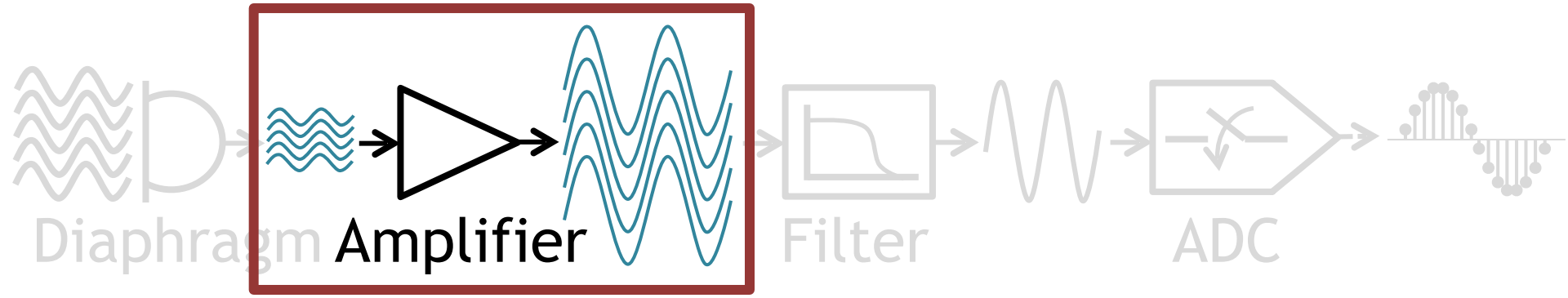
# Microphone working principle



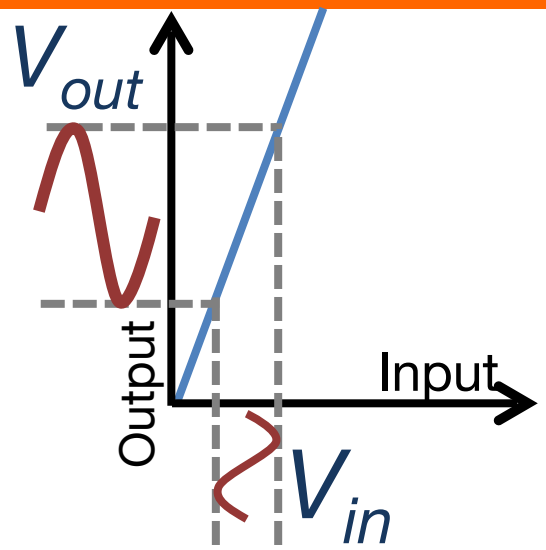



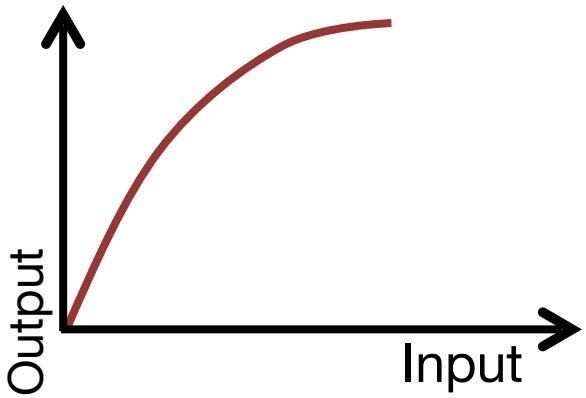
# Microphone working principle



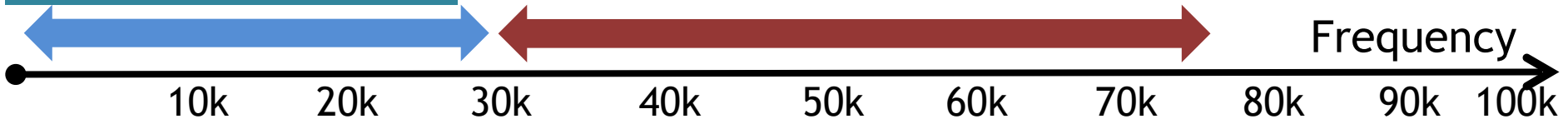
# Microphone working principle

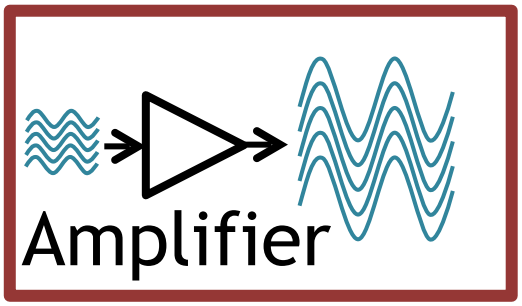


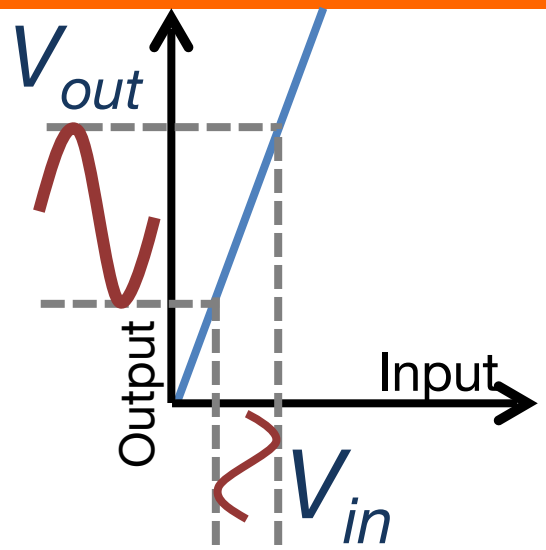

$V_{out} = a_1 V_{in}$

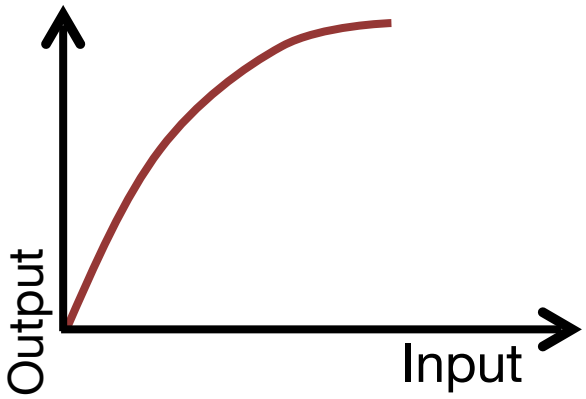
$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$



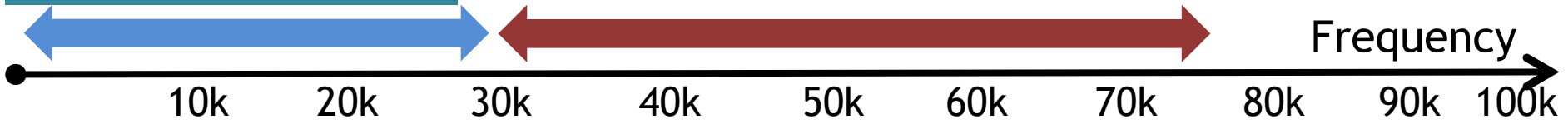
# Microphone working principle

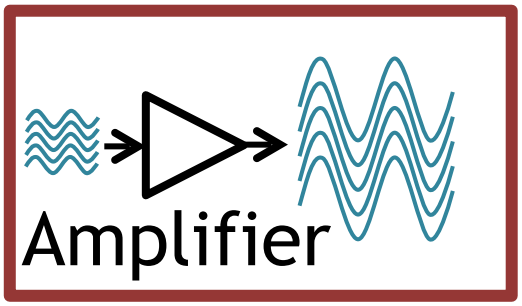


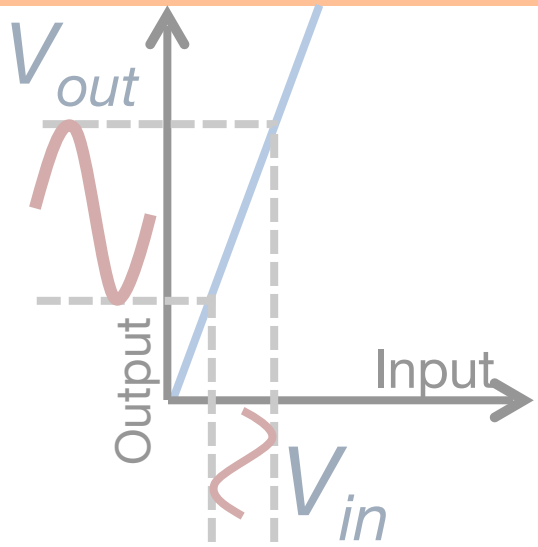

$V_{out} = a_1 V_{in}$

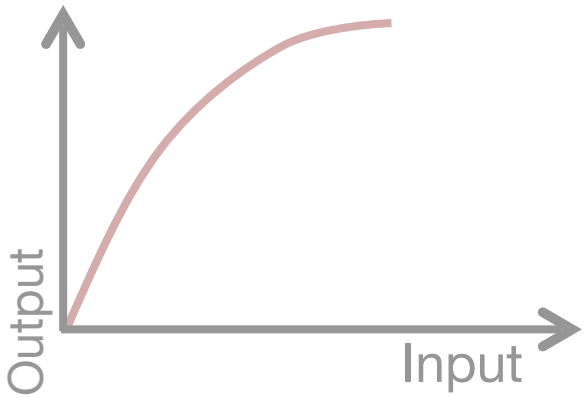
$V_{out} = a_1 V_{in} + a_2 V_{in}^2$



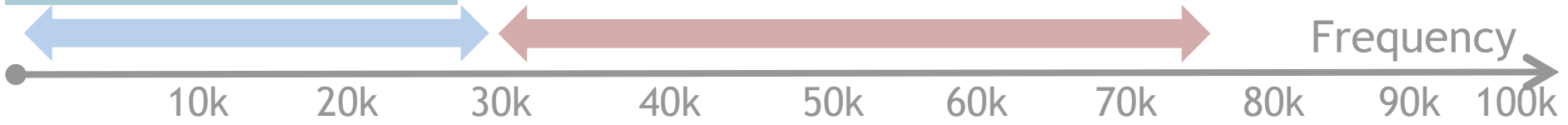
# Microphone working principle

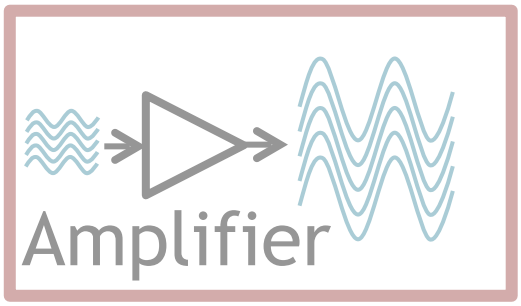



$V_{out} = a_1 V_{in}$

$V_{out} = a_1 V_{in} + a_2 V_{in}^2$



# Talk outline

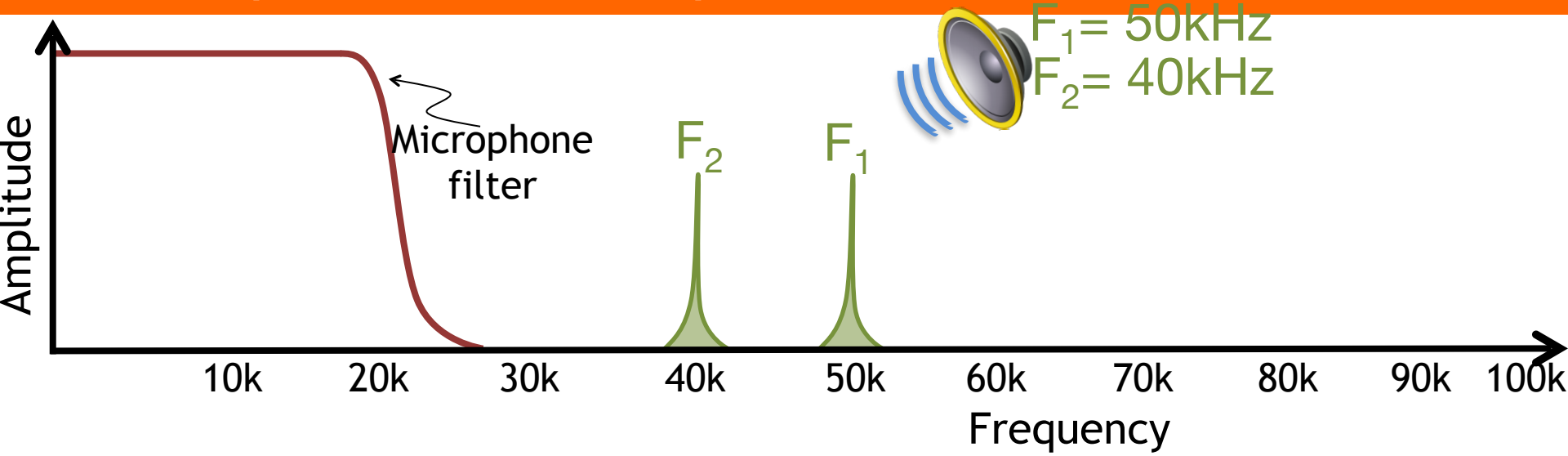
① Microphone Overview

② System Design

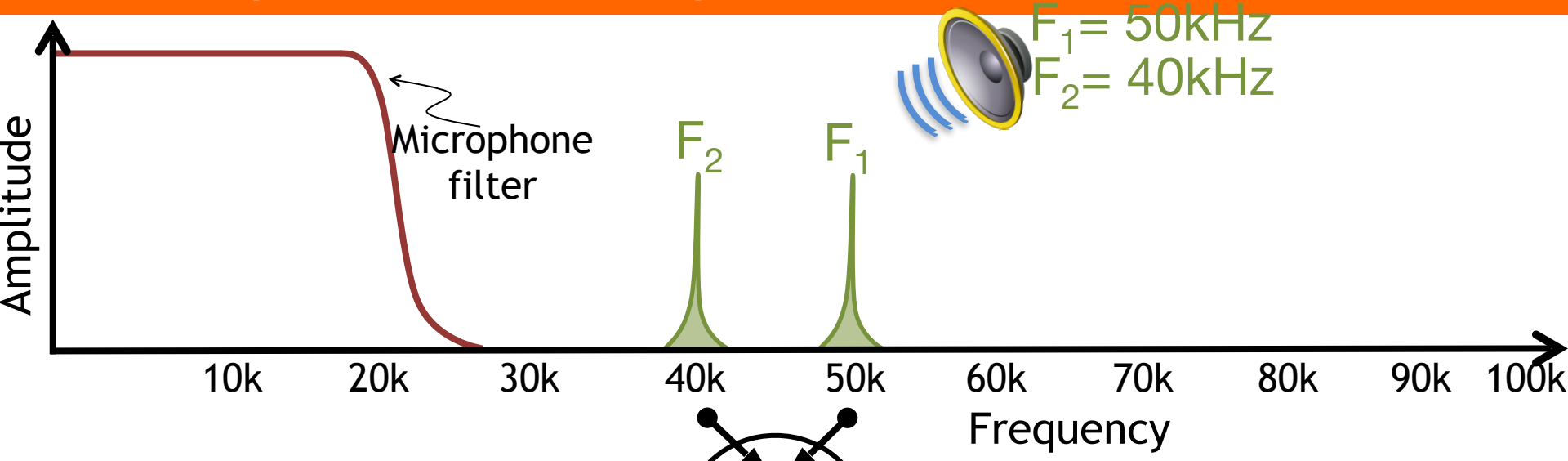
③ Challenges

④ Evaluation

# Exploiting amplifier non-linearity



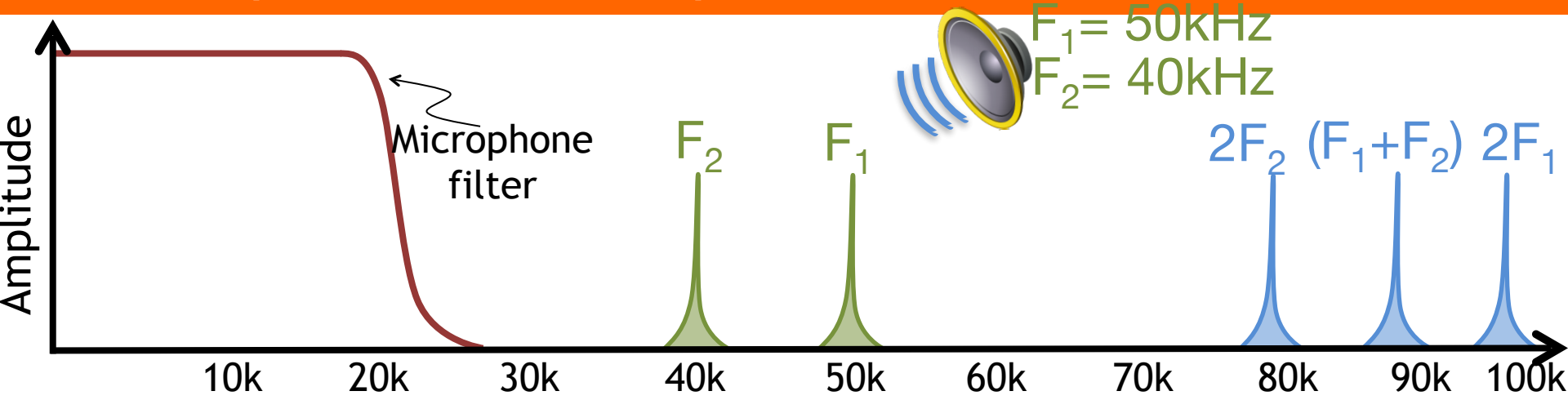
# Exploiting amplifier non-linearity




$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 = \cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

# Exploiting amplifier non-linearity

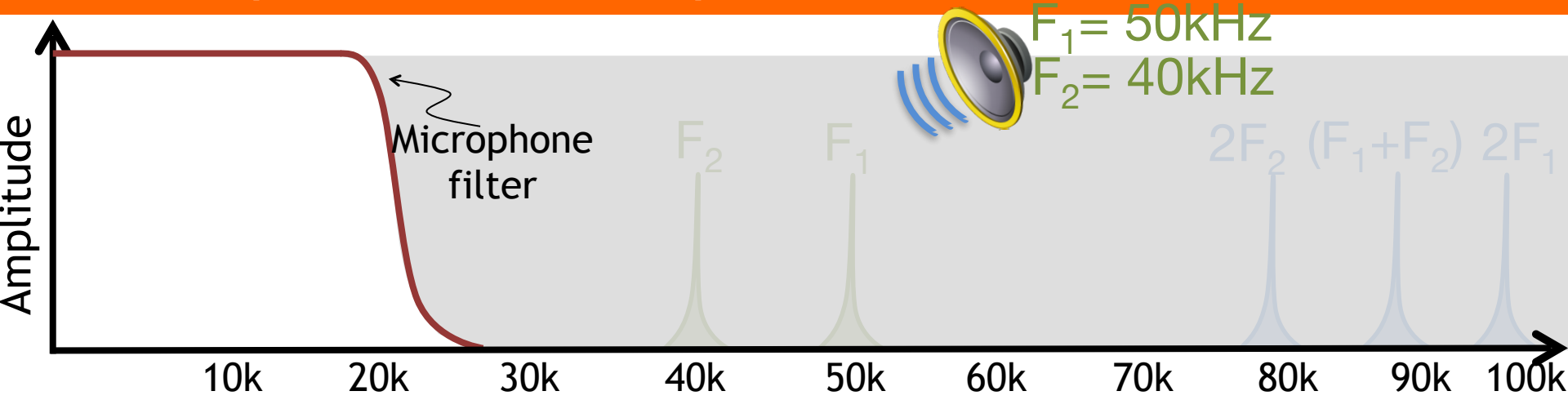



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$( \sin F_1 + \sin F_2 )^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

# Exploiting amplifier non-linearity

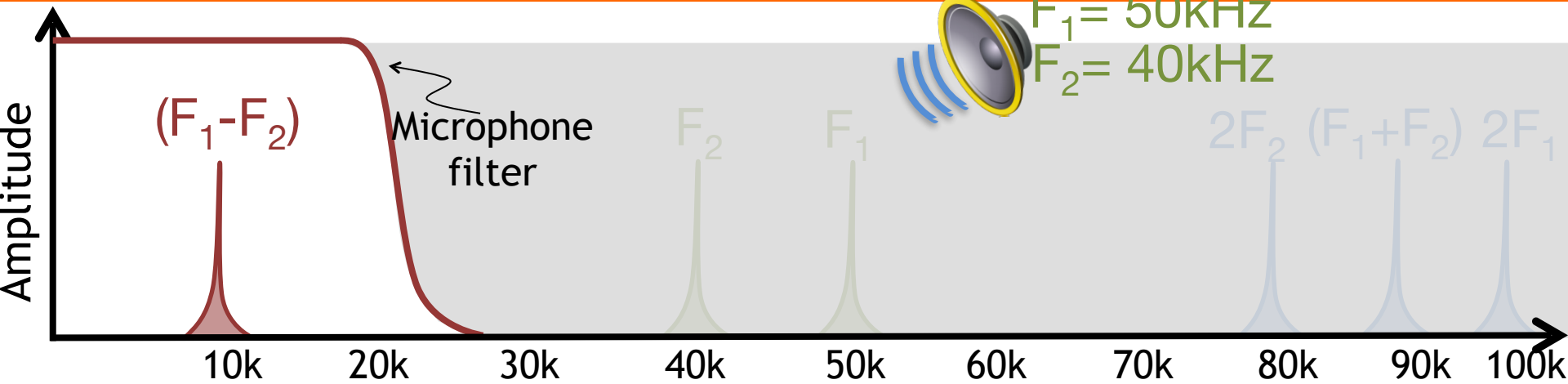



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

# Exploiting amplifier non-linearity

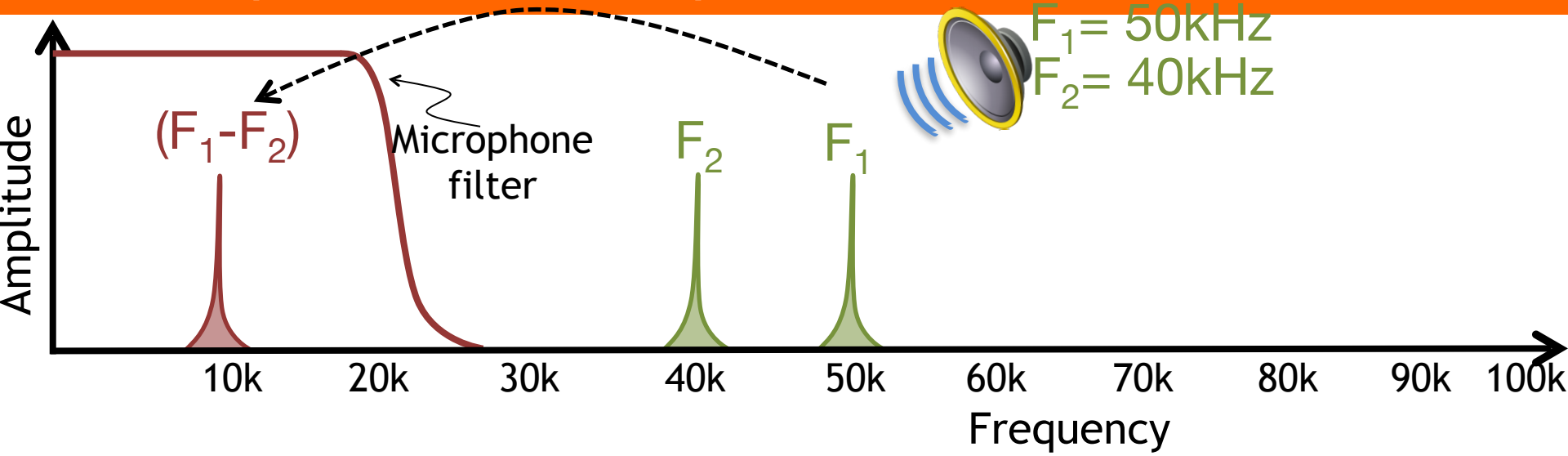



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

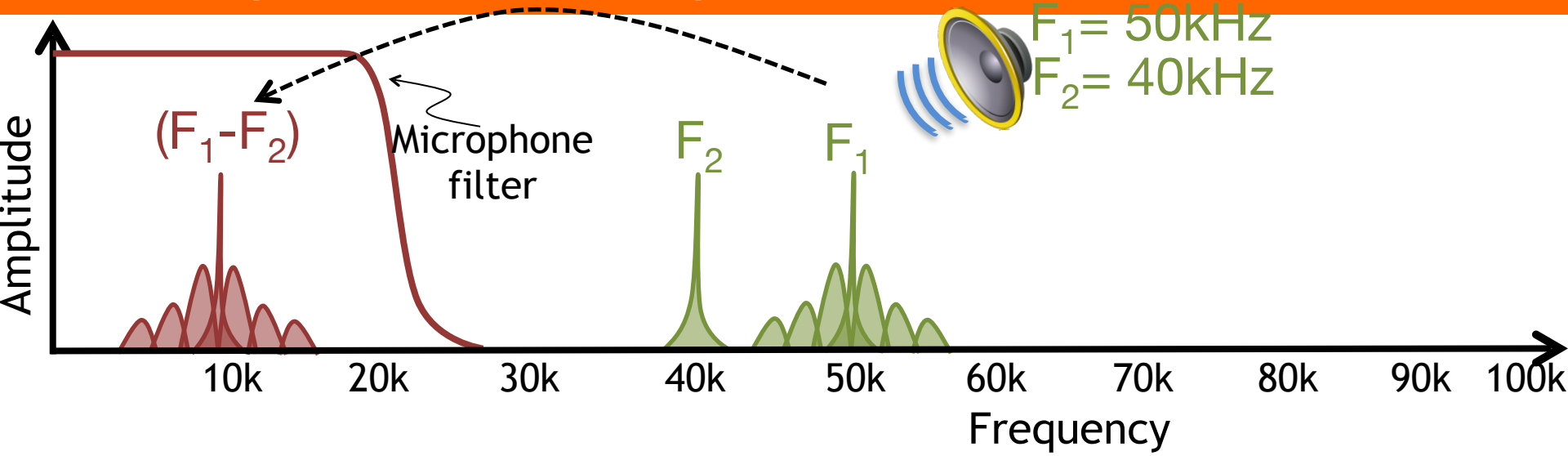
$$(\sin F_1 + \sin F_2)^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

# Exploiting amplifier non-linearity



# Exploiting amplifier non-linearity



# Talk outline

① Microphone Overview

② System Design

③ Challenges

④ Evaluation

- Stretching Break!

# Talk outline

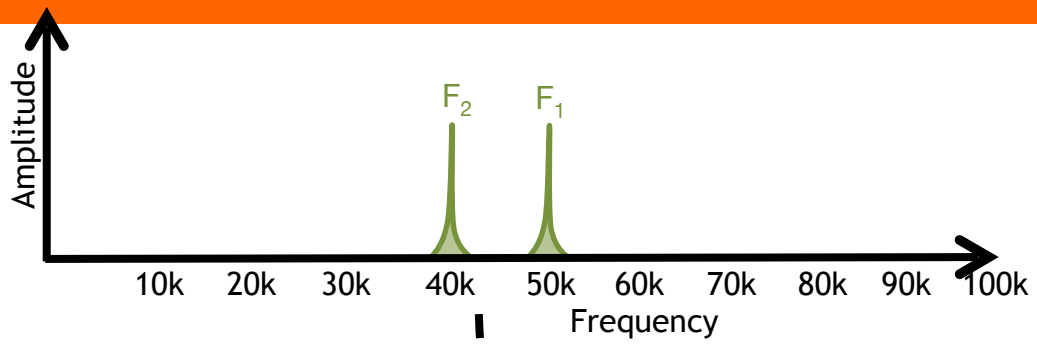
① Microphone Overview

② System Design

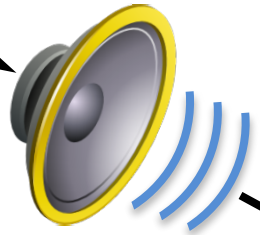
③ Challenges

④ Evaluation

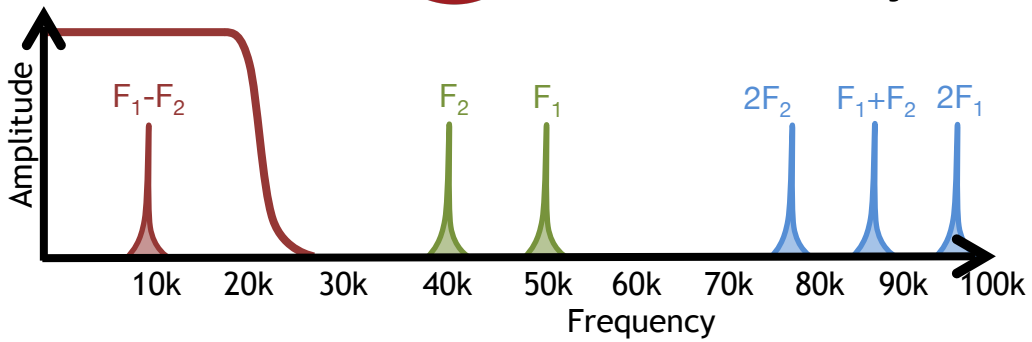
# Challenges



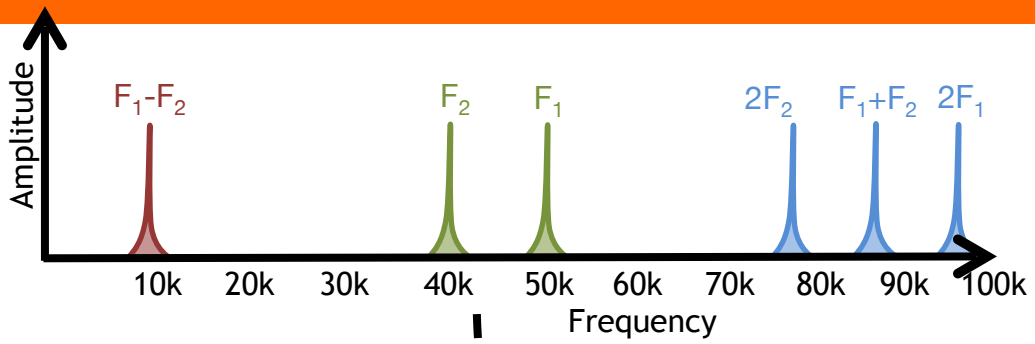

Speaker's nonlinearity



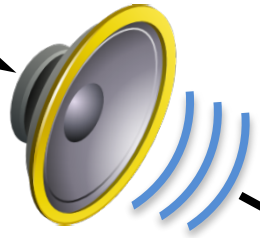
Microphone's nonlinearity



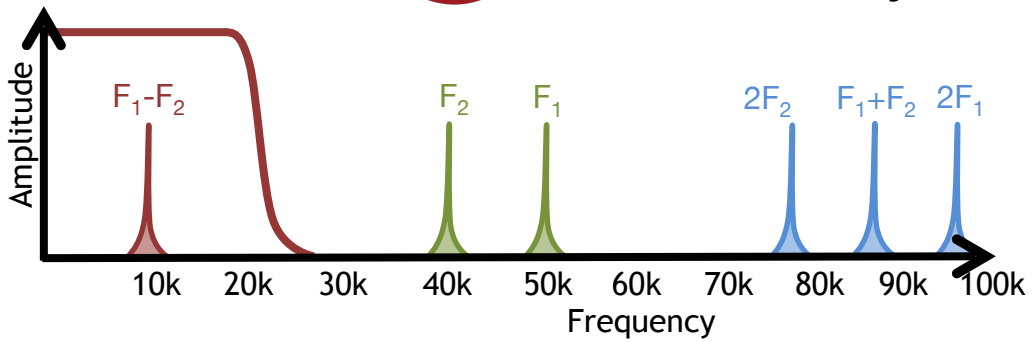
# Challenges



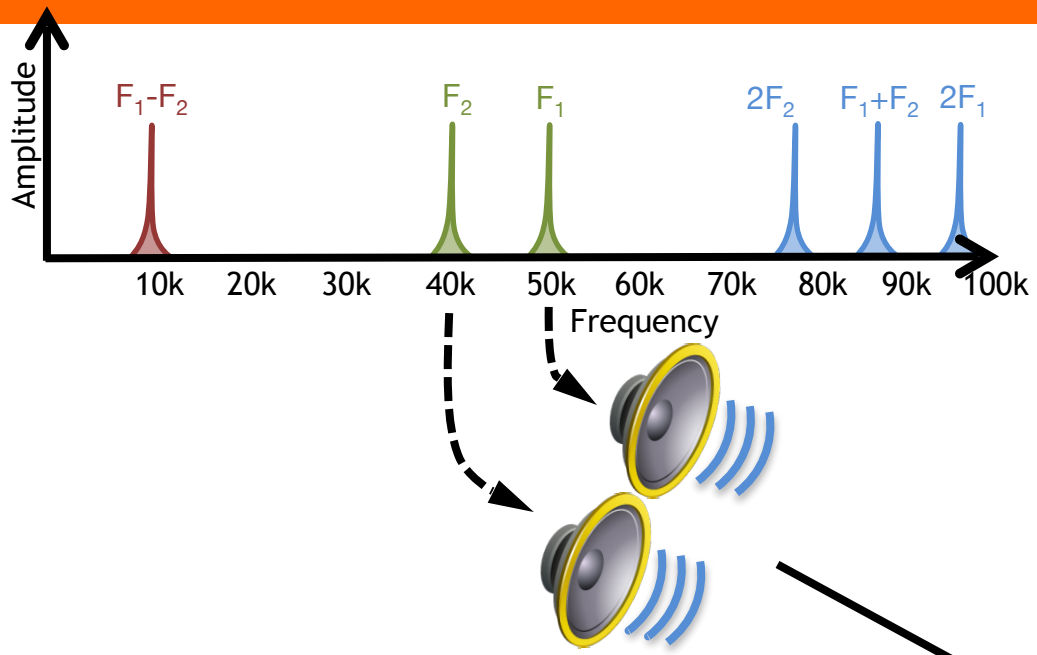

Speaker's nonlinearity



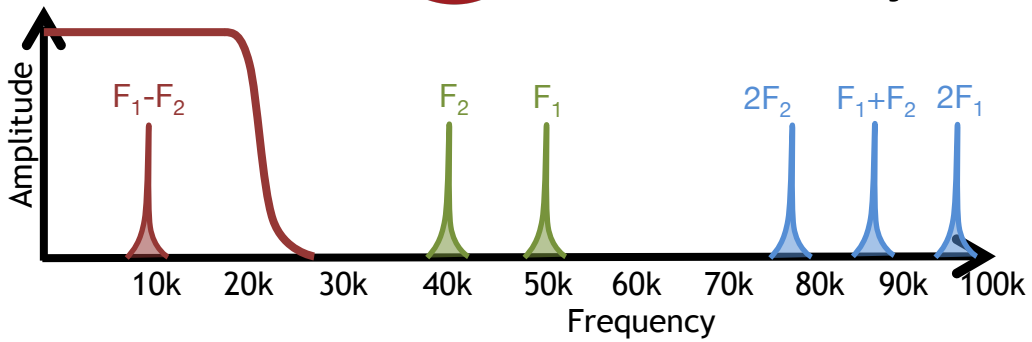
Microphone's nonlinearity



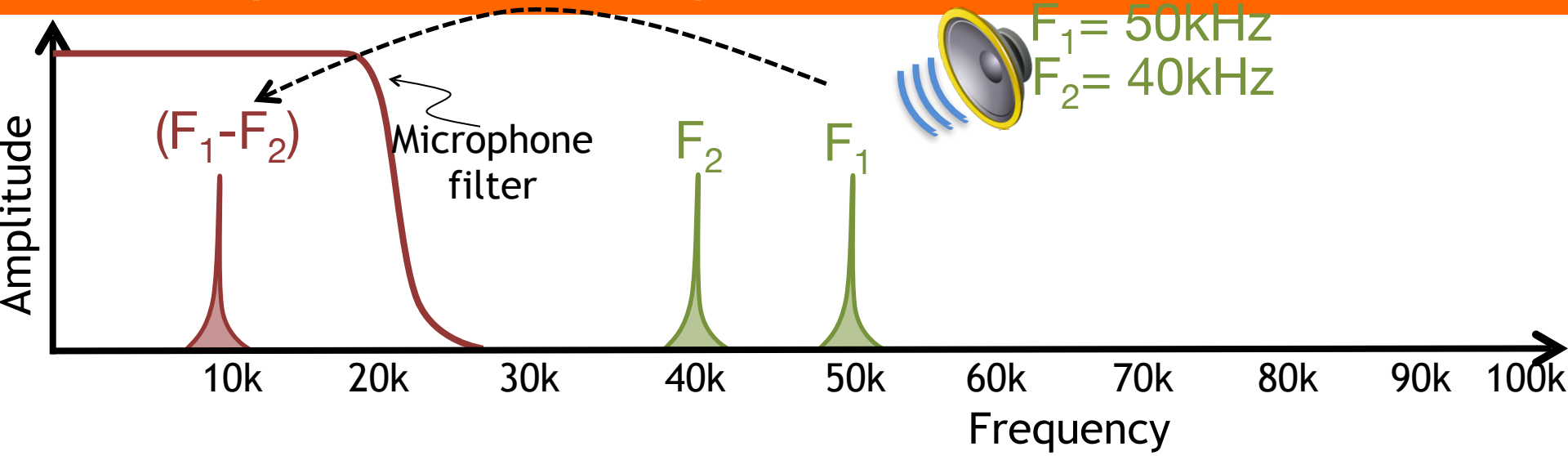
# Challenges




Microphone's nonlinearity



# Exploiting amplifier non-linearity



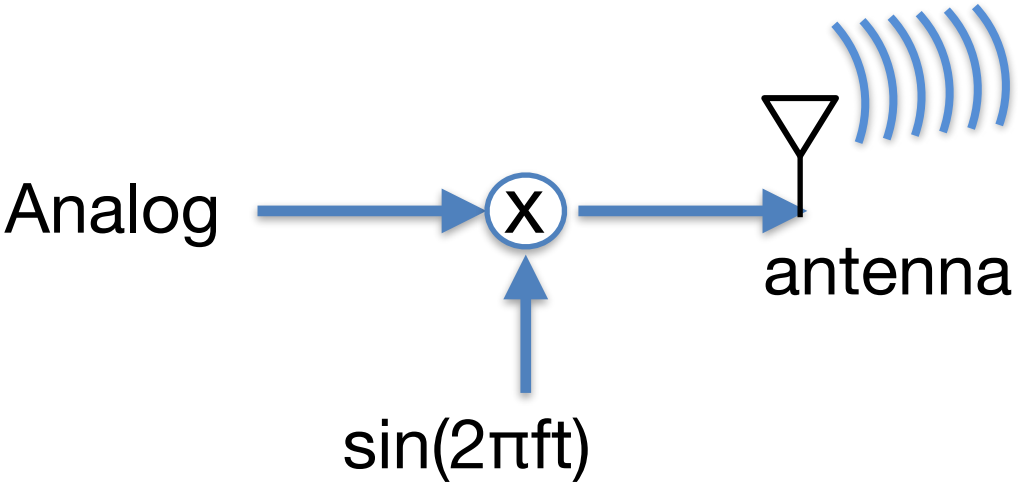

Not sending a single “tone” (sine wave), but sending a command.

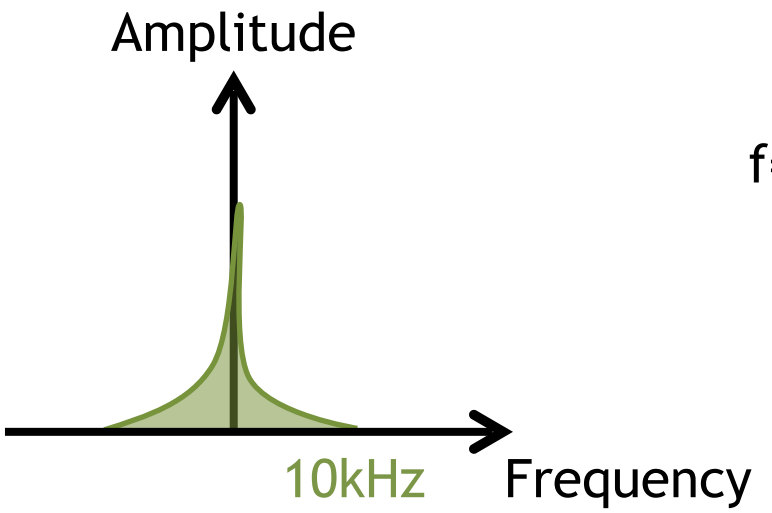
How can we send this command?

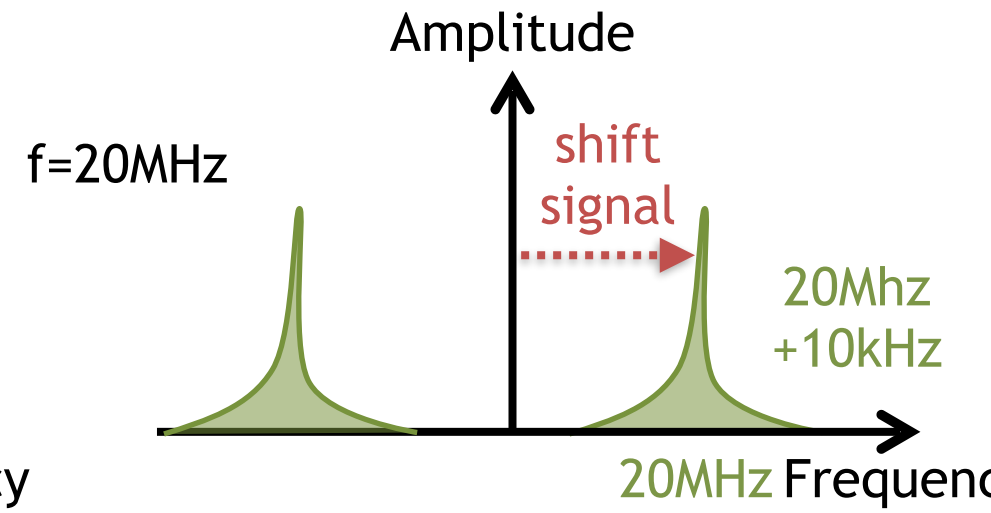
# Primer on Modulation

E.g., We send WiFi at 2.4GHz or 5GHz
What does this mean and Why?

# Primer on Modulation

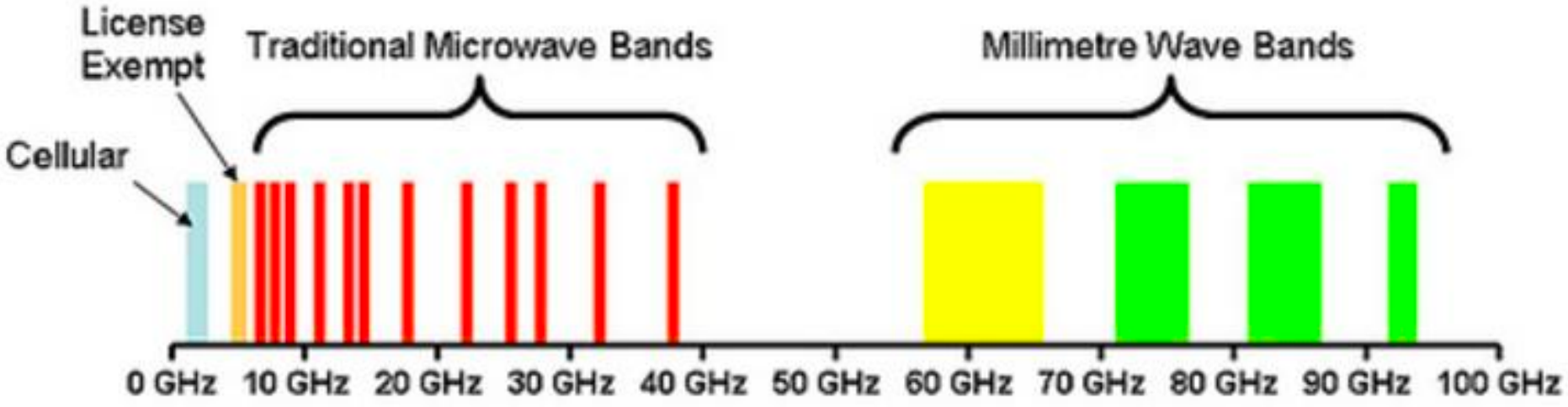


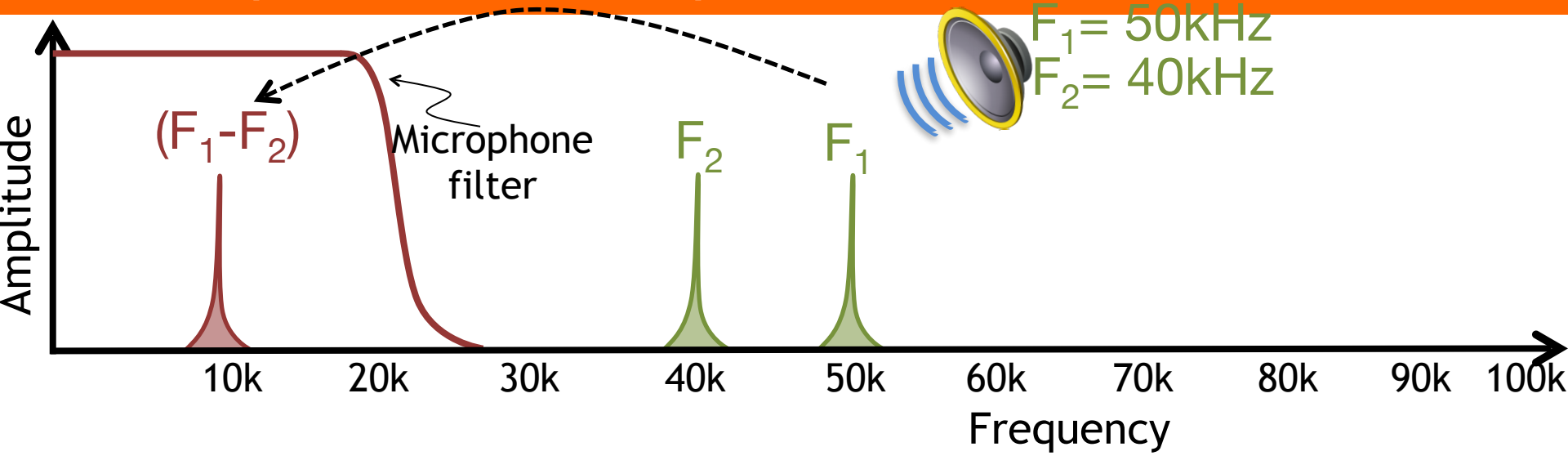
# Why is Modulation useful?

1. Interference, Technology Co-existence
2. Spectrum Access (Legal)
3. Antenna size (wavelength/4)




WiFi? LTE? 5G?

# Exploiting amplifier non-linearity




Not sending a single “tone” (sine wave), but sending a command/message.

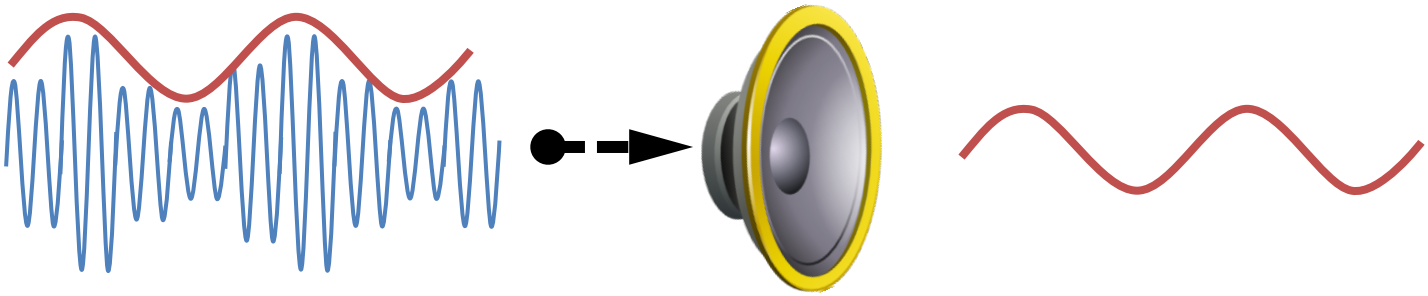
How can we send this command message m(t)?

$m(t) \times \sin(2\pi ft)$

# Challenges

Amplitude modulation

$$S_{AM} = a \cdot \underbrace{\sin(\omega_m t)}_{\text{message}} \cdot \underbrace{\sin(\omega_c t)}_{\text{carrier}}$$



Ultrasonic speaker

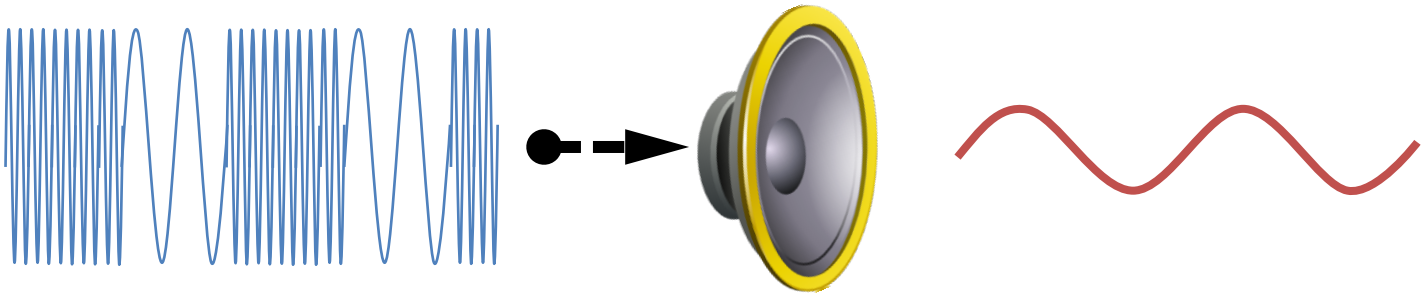
$$\begin{aligned} S^2_{out,AM} &= A_2\{aSin(\omega_m t).Sin(\omega_c t)\}^2 \\ &= -A_2\frac{a^2}{4}\{Cos(\omega_c t - \omega_m t) - Cos(\omega_c t + \omega_m t)\}^2 \\ &= -A_2\frac{a^2}{4}Cos(2\omega_m t) + (terms\ with\ frequencies \\ &\qquad\qquad above\ \omega_c\ and\ DC) \end{aligned}$$

<u>Problem:</u> speaker has non-linearities => Audible sound

# Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$

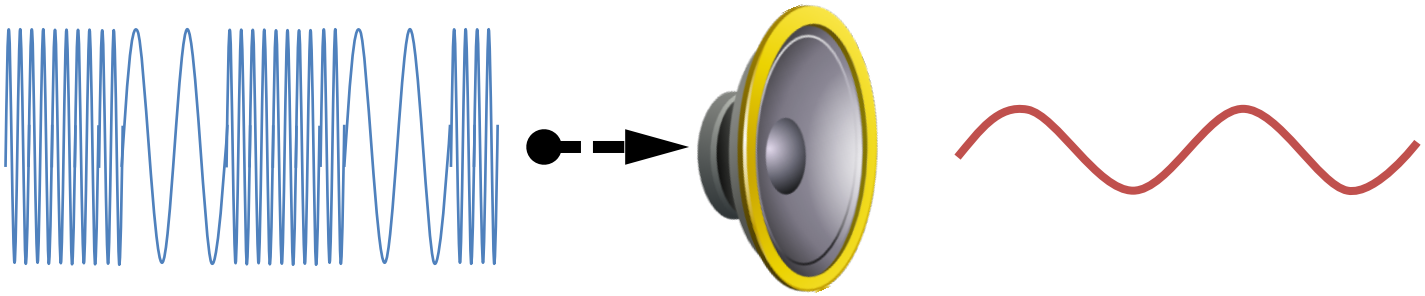


Ultrasonic speaker

# Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



Ultrasonic speaker

# Talk outline

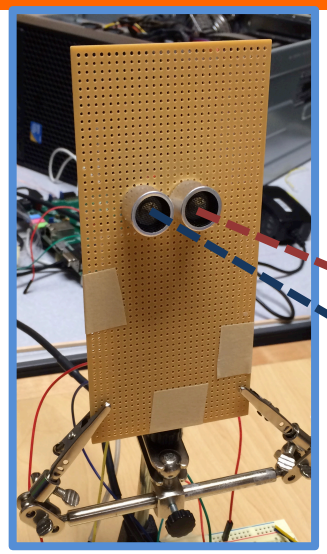
① Microphone Overview

② System Design

③ Challenges

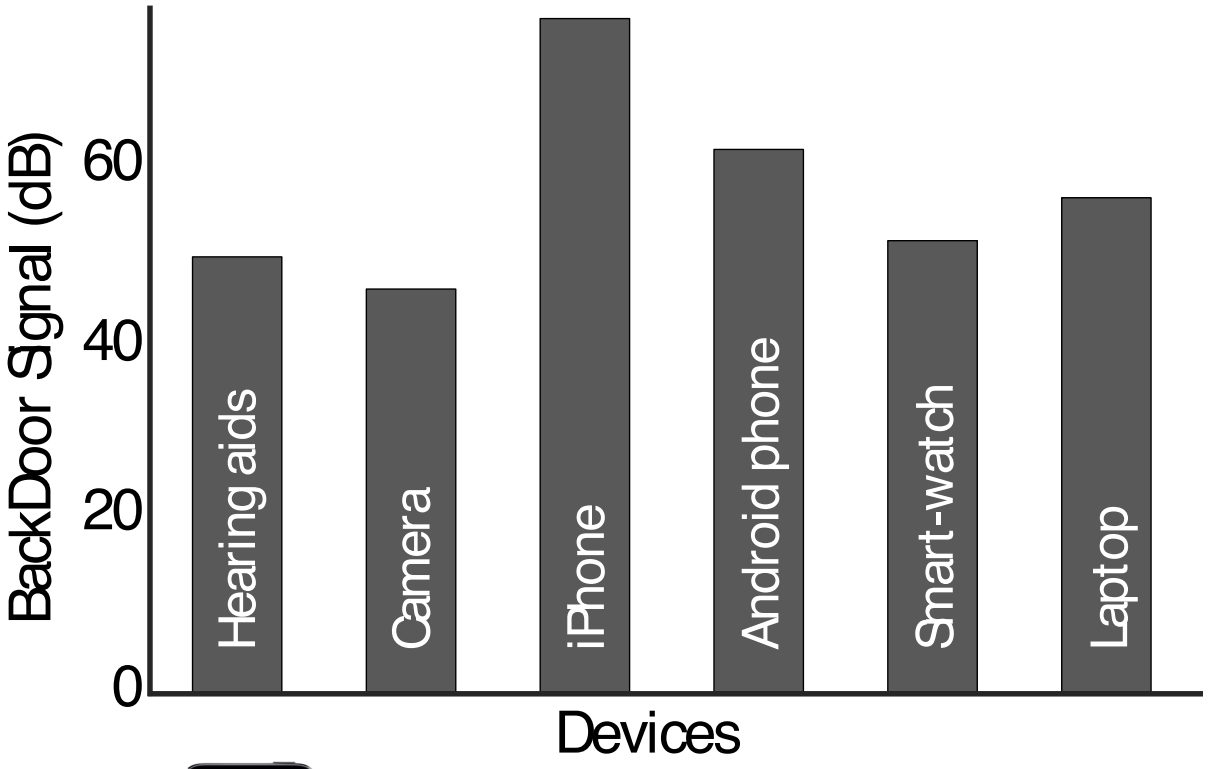
④ Evaluation

# Hardware generalizability



40 kHz

50 kHz




Hearing Aid

Camera

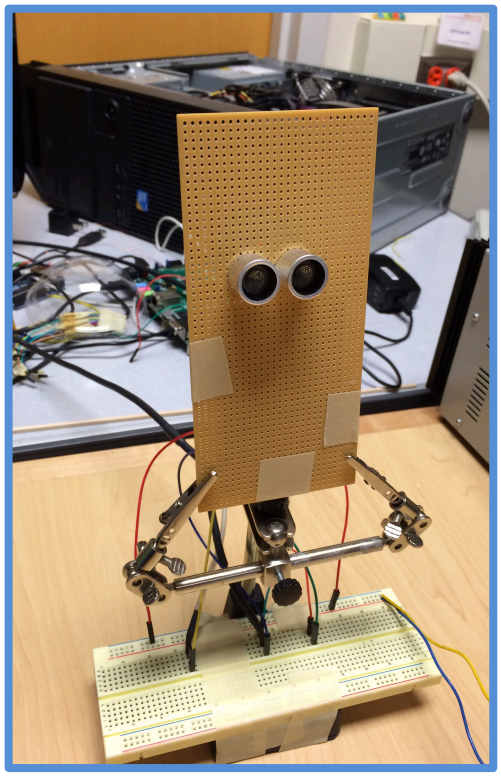
iPhone

Android phone

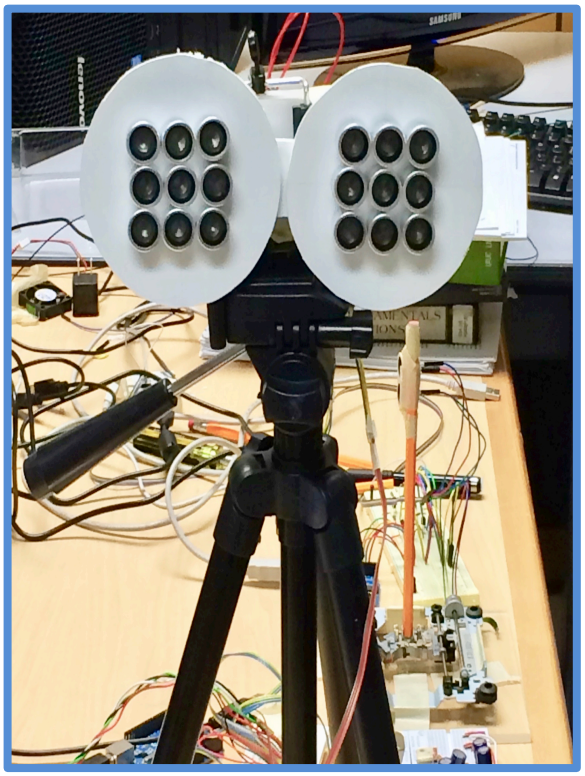
Smartwatch

Laptop

# Implementation

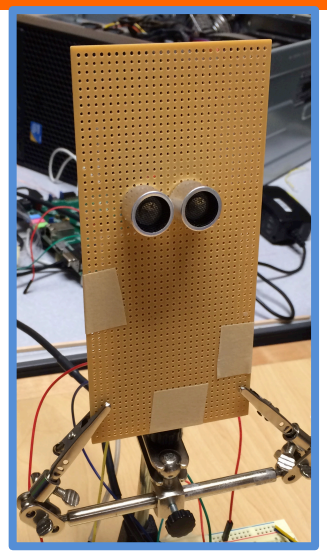


Communication prototype



Jammer prototype

# Communication performance

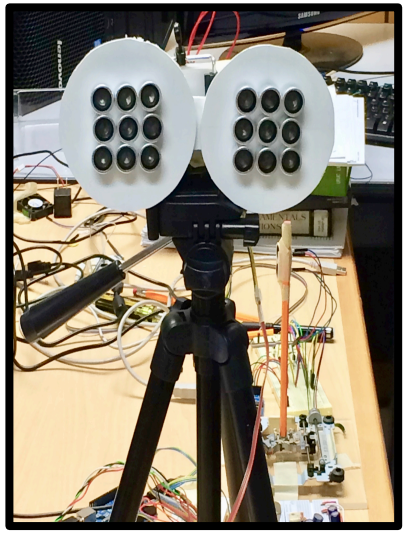


FM data packets


4kbps
up to 1 meter

More power can increase the distance

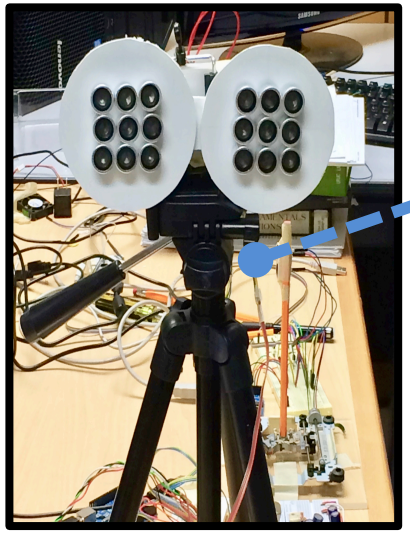
# Jamming performance



BackDoor jammer

Spy microphone

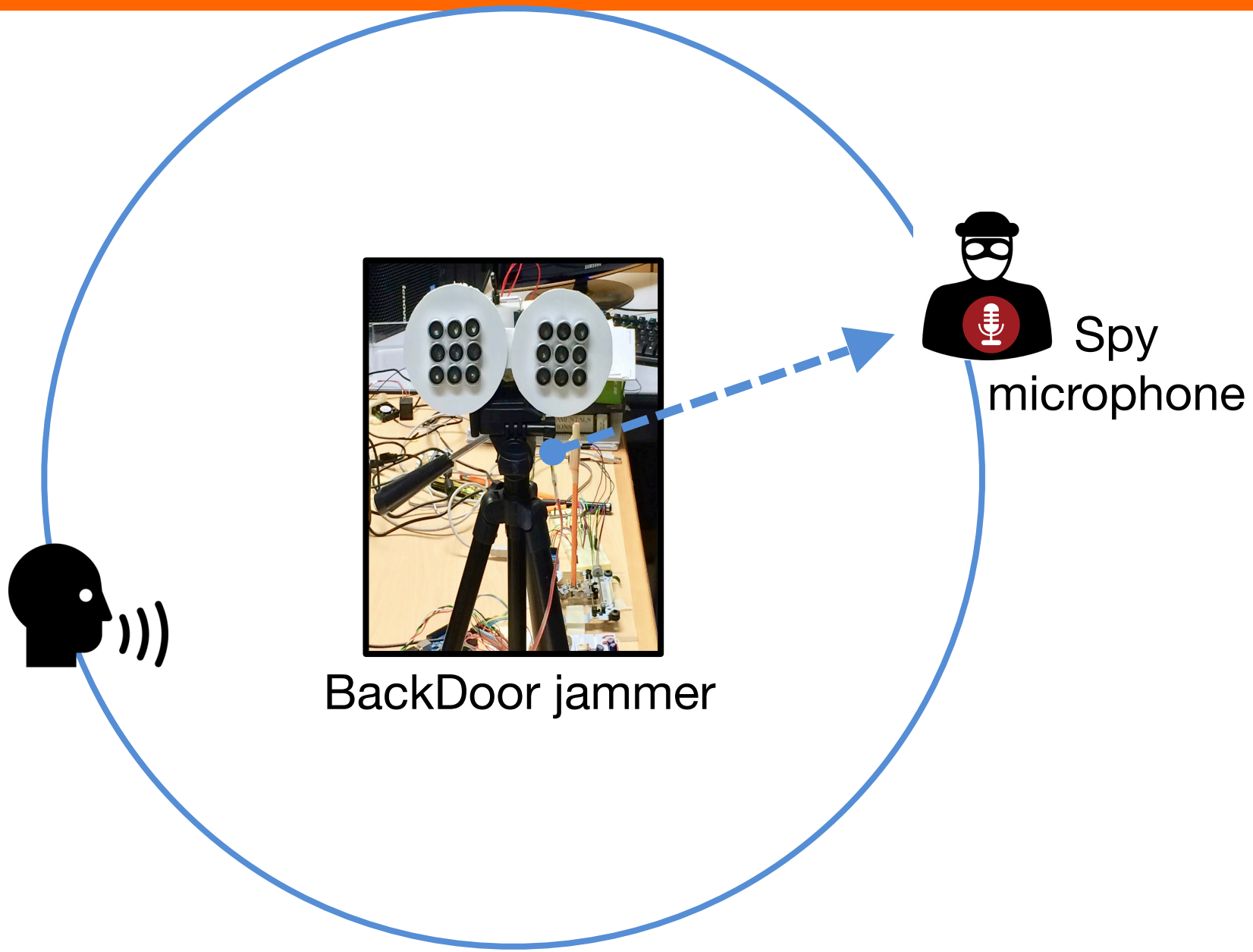
# Jamming performance



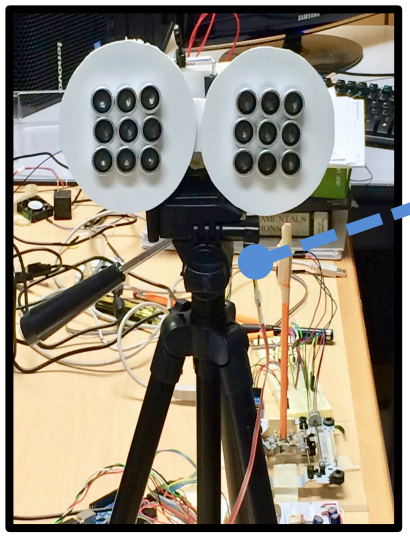
BackDoor jammer

Spy microphone

# Jamming performance



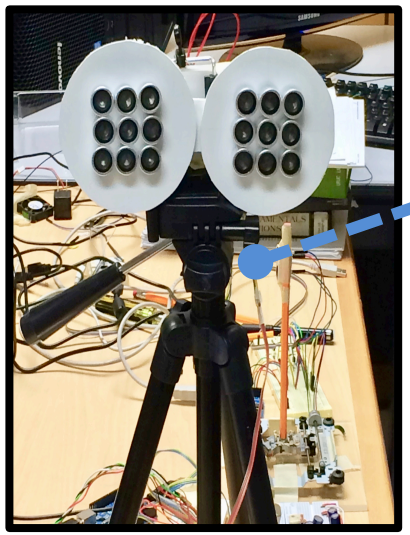
# Jamming performance



BackDoor jammer

Spy microphone

# Jamming performance

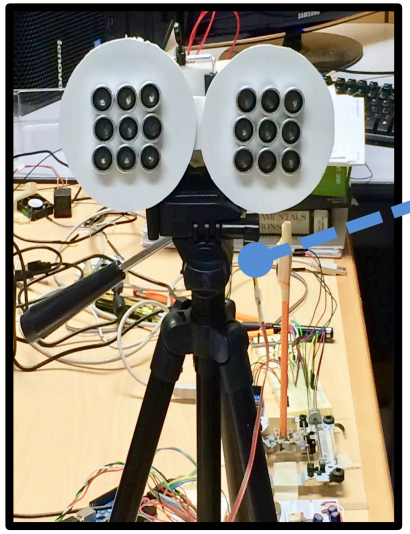


BackDoor jammer

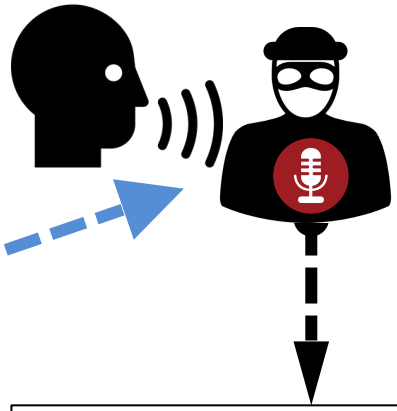
Spy microphone

# Jamming performance

2000 spoken words

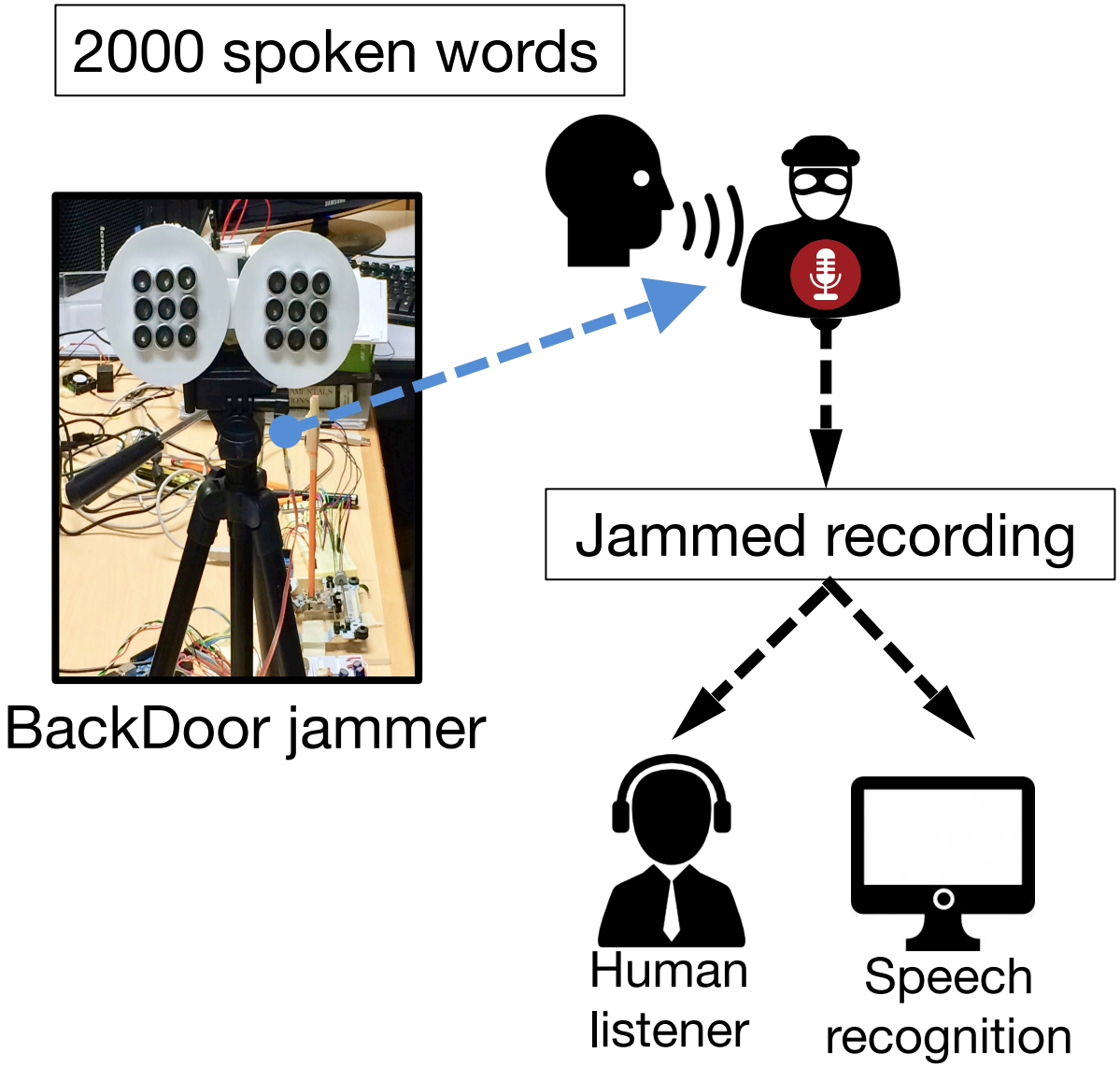


BackDoor jammer

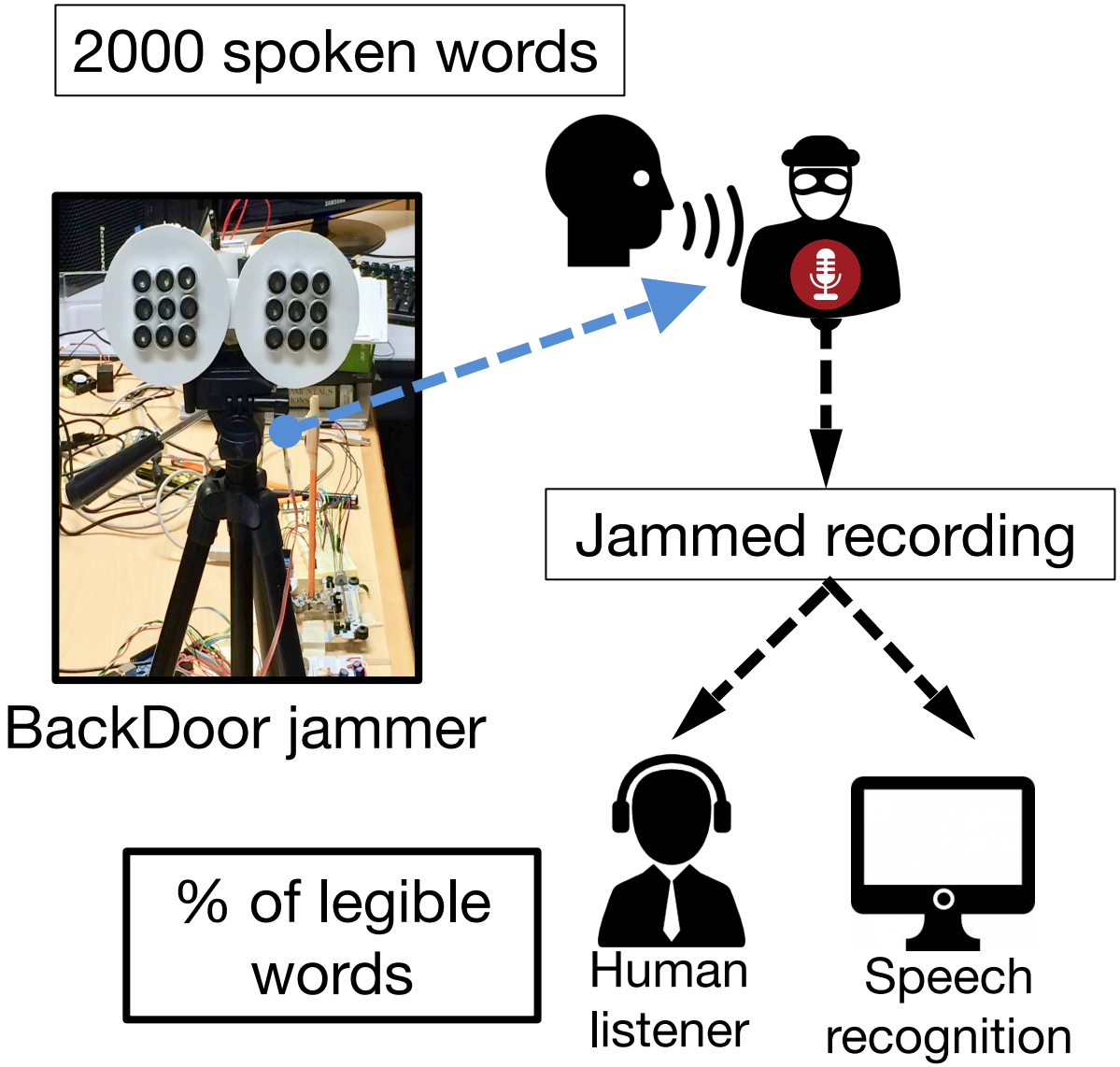


Jammed recording

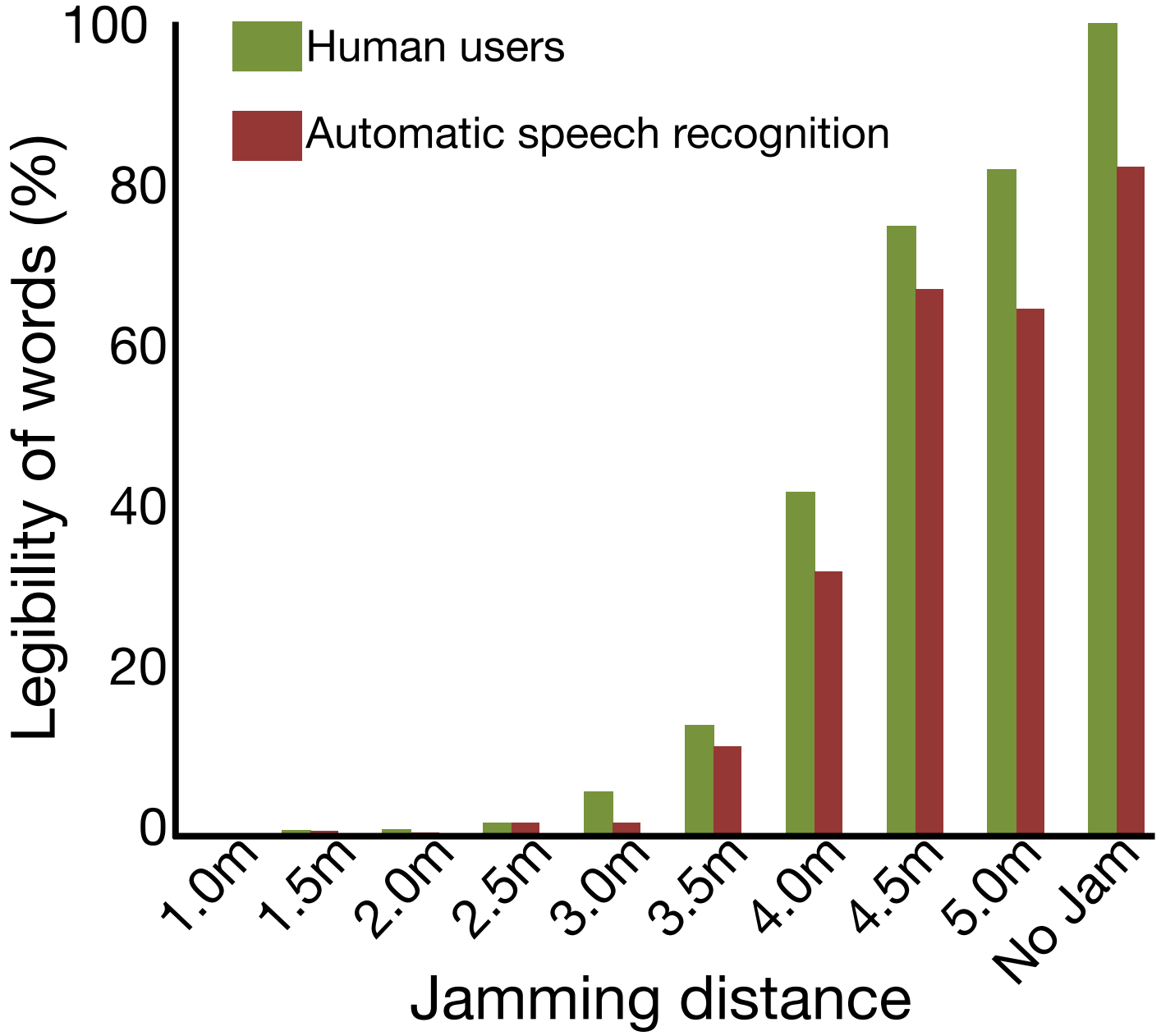
# Jamming performance



# Jamming performance



# Jamming performance



How would you design a system to secure against this attack?

# Finally, a Likely Explanation for the "Sonic Weapon" Used at the U.S. Embassy in Cuba

## Researchers say bad engineering, not a deliberate attack, may be to blame

By **Jean Kumagai**

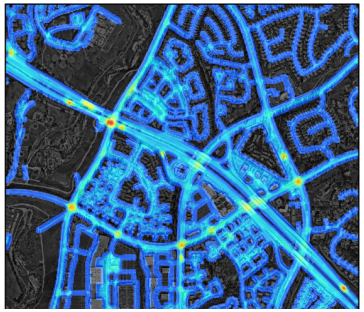
# Summary

- IoT Security: both digital and analog
- "Sensor" security & attacks:
  - Mobile acoustic attacks (inaudible voice commands)
  - Light commands (laser)
  - Analog Sensor attacks (on MEMS accelerometers)
  - Drone Security (Spoofing GPS)
  - Medical Security (Hacking Pacemakers)
- Modulation schemes
  - Mechanism & benefits
  - Inter-modulation
- Fundamentals have implications beyond IoT (e.g., Cuban "acoustic attack")

# Remainder of the Class

Emerging Application Domains & Cross-Cutting Topics

1. Transportation

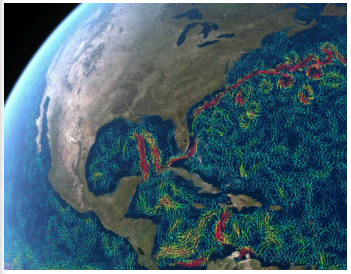


2. Health


3. Agriculture

Next lecture

4. Oceans/ Climate



5. Security/ Privacy

**TODO:**

1- Project Proposals due March 16

2- Lab 4 out; due March 30

3- PSet 2 due April 4

4- Grades will be out this week