6.1820/MAS.453: Mobile and Sensor Computing aka IoT Systems

https://6mobile.github.io/

Lecture 12: Attacks on Acoustic Sensing

Some slides adapted from Nirupam Roy (UMD College Park)

Course Staff

Lecturers

Fadel Adib (fadel@mit.edu)

Tara Boroushaki (tarab@mit.edu)

TAs

Waleed Akbar (wakbar@mit.edu)

Jack Rademacher (jradema@mit.edu)

Announcements

1- Project Proposals due April 1st

2- Lab 3 due today

3- PSet 2 due April 10

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, $


Annual Meeting
Davos 2024
WORLD ECONOMIC FORUM
These students are doing science experiments with their phones

What are we learning today?

IoT Security

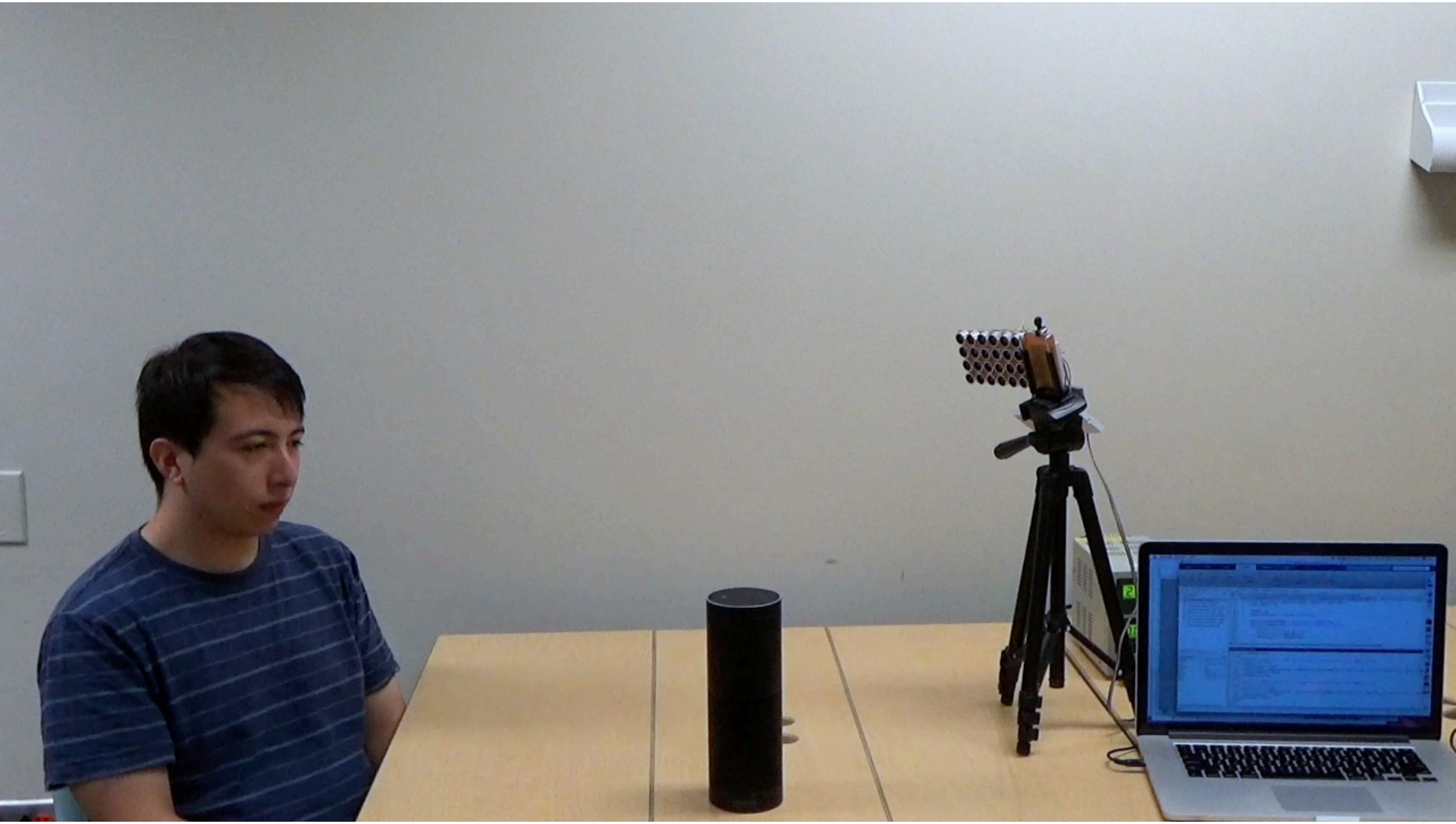
Cyber-Physical Security and Acoustic Attacks

1- Hacking different IoT sensors:

- microphones in smart home devices
- accelerometers in fitbit
- localization in drones
- controller of a pace maker

2- How can you send inaudible voice commands to a microphone?

Mobile Security
Inaudible Voice Commands




YAMAHA
LINE3

Light Commands
Hacking using Laser


UEC
TOKYO

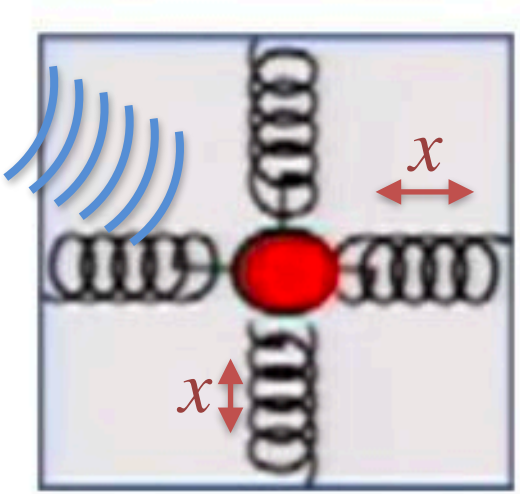

CSE
COMPUTER SCIENCE
AND ENGINEERING
UNIVERSITY OF MICHIGAN

LIGHT COMMANDS

Analog Sensor Security
Acoustic Attacks on MEMS Accelerometers


TITANIUM BULLET TWEETER
PYRAMID

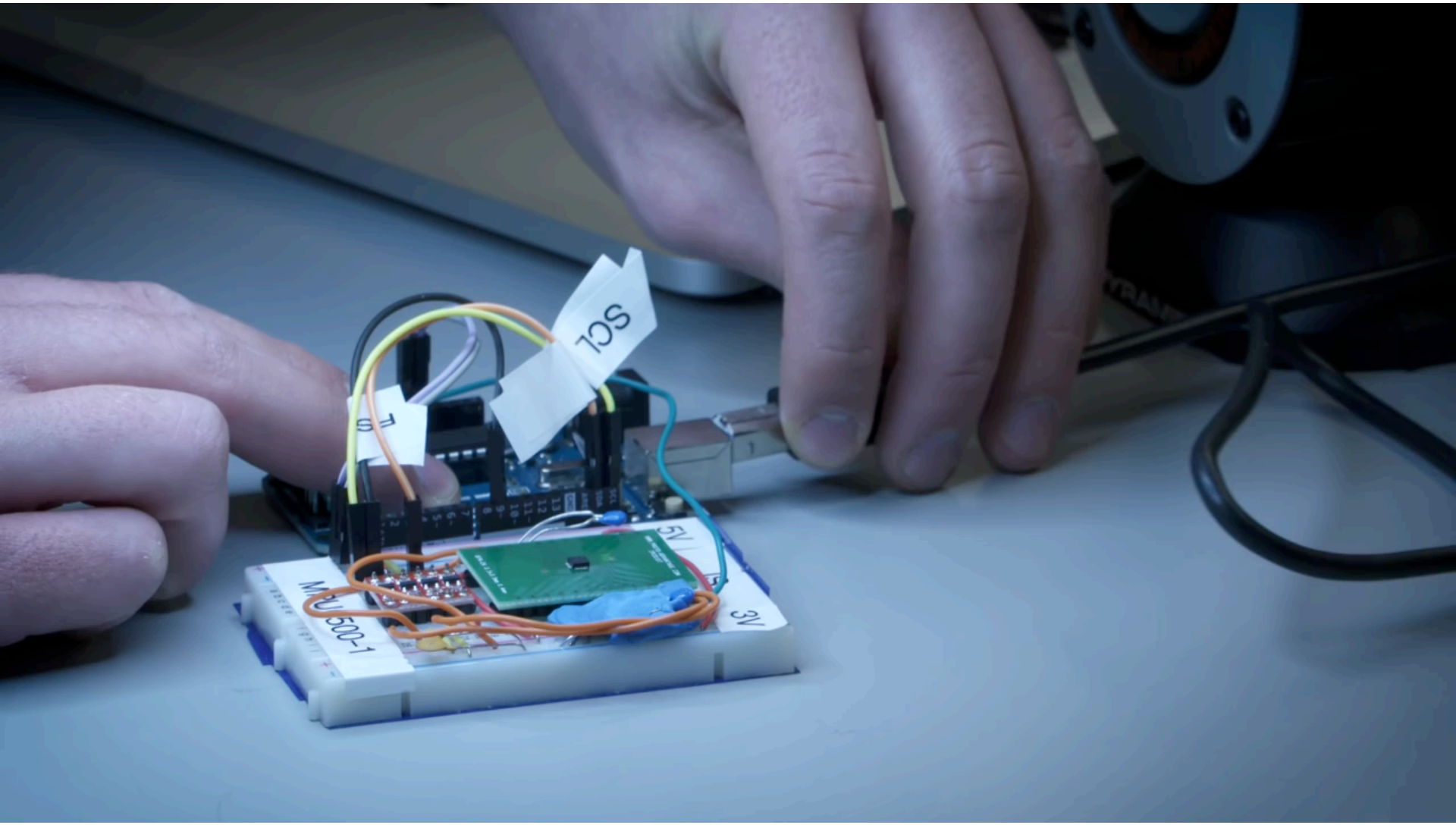
Acoustic
"pressure" waves



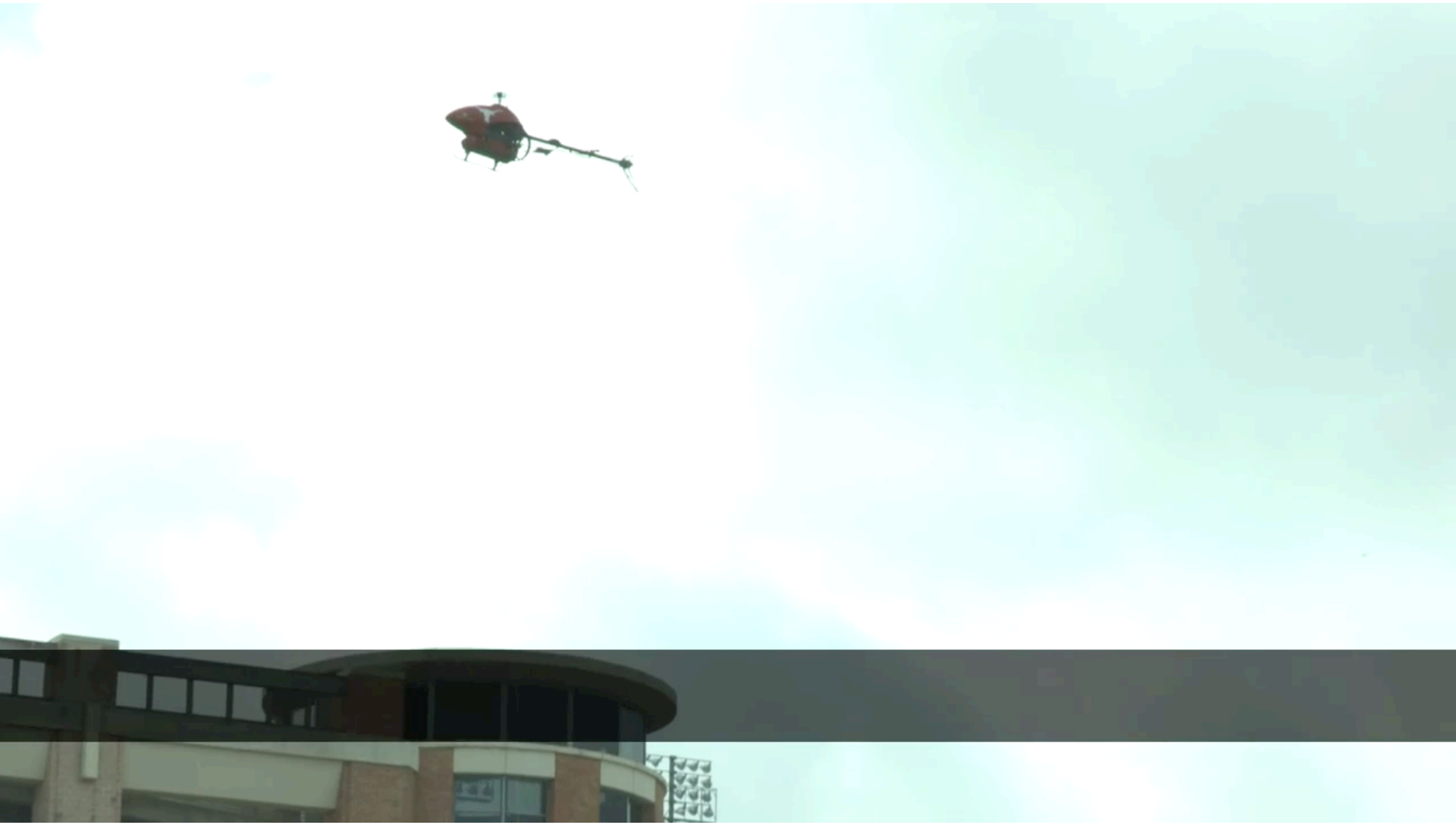
$$F = ma = kx$$

acceleration

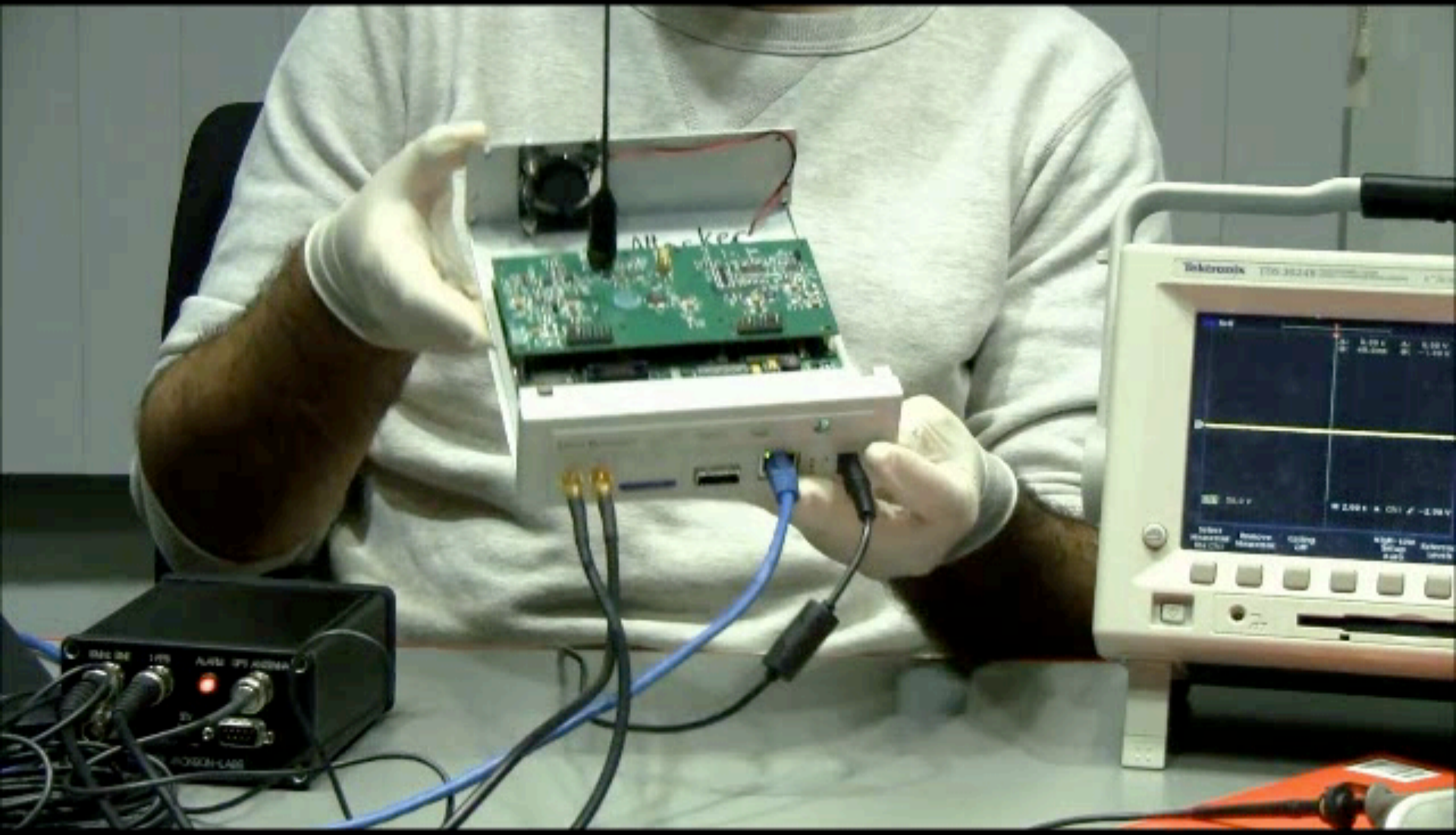
measure
displacement


SCL
5V
3V
MPU 6500-1

Drone Security
Spoofing GPS Signals

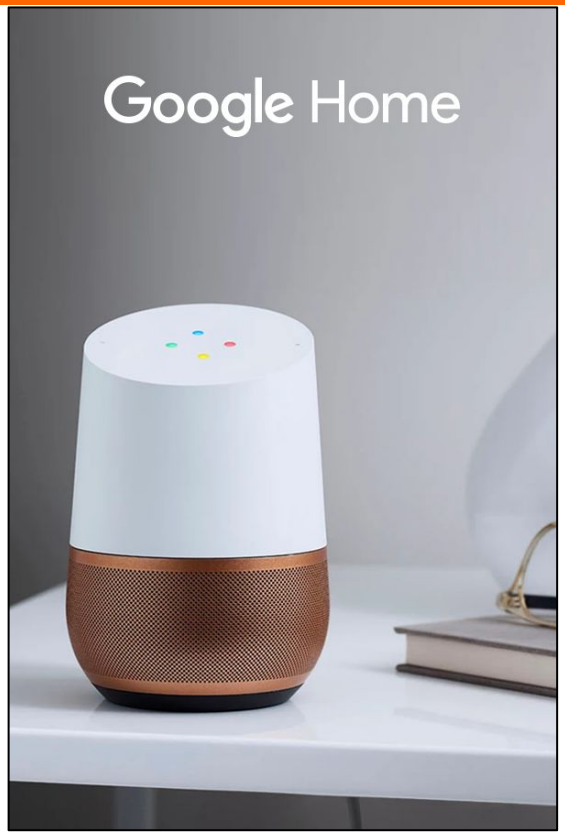


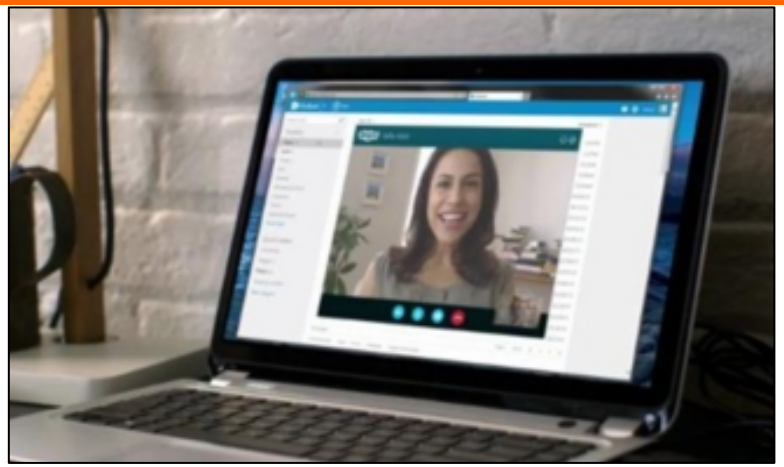
Pacemaker Security
Wireless Control of Pacemaker

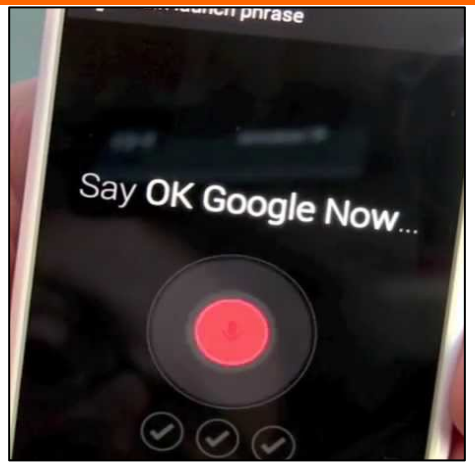

Tektronix

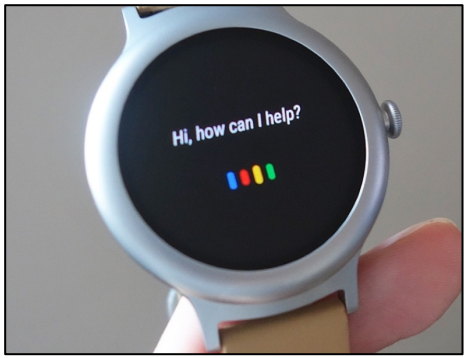
BackDoor: Making Microphones Hear Inaudible Sounds

Microphones are everywhere

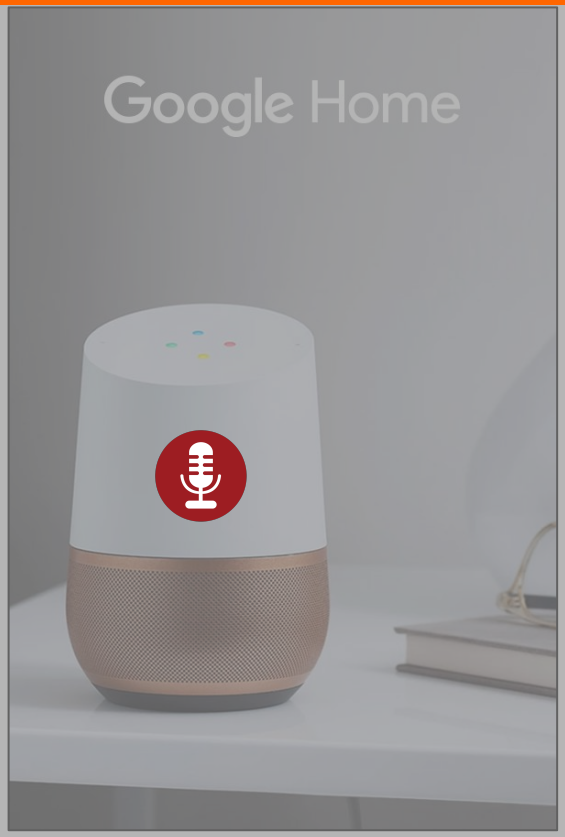


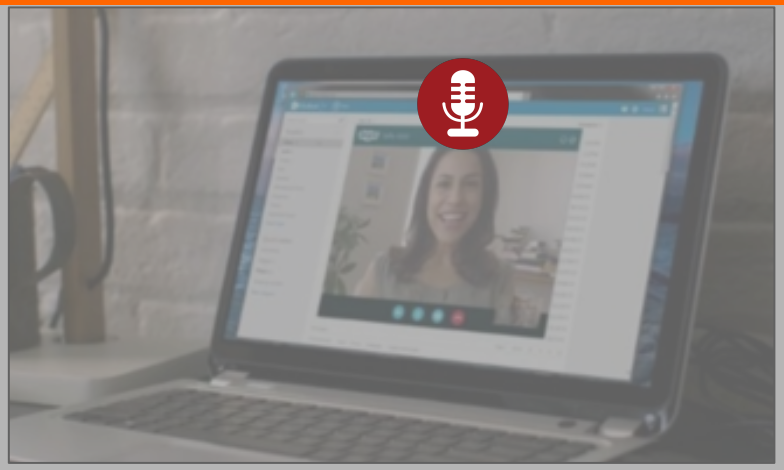


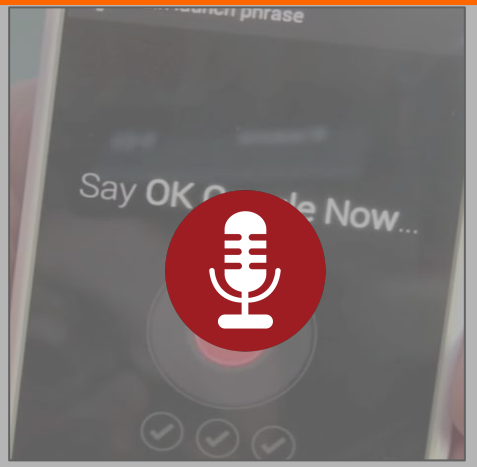


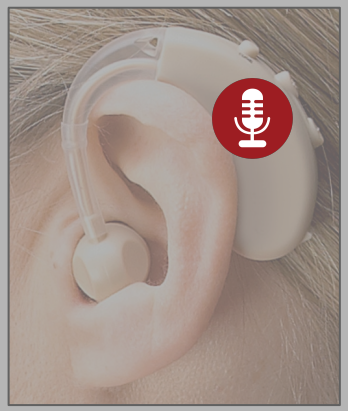


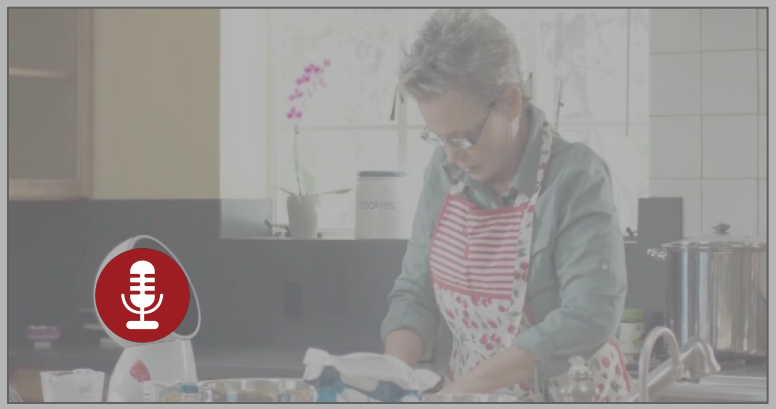
Microphones are everywhere



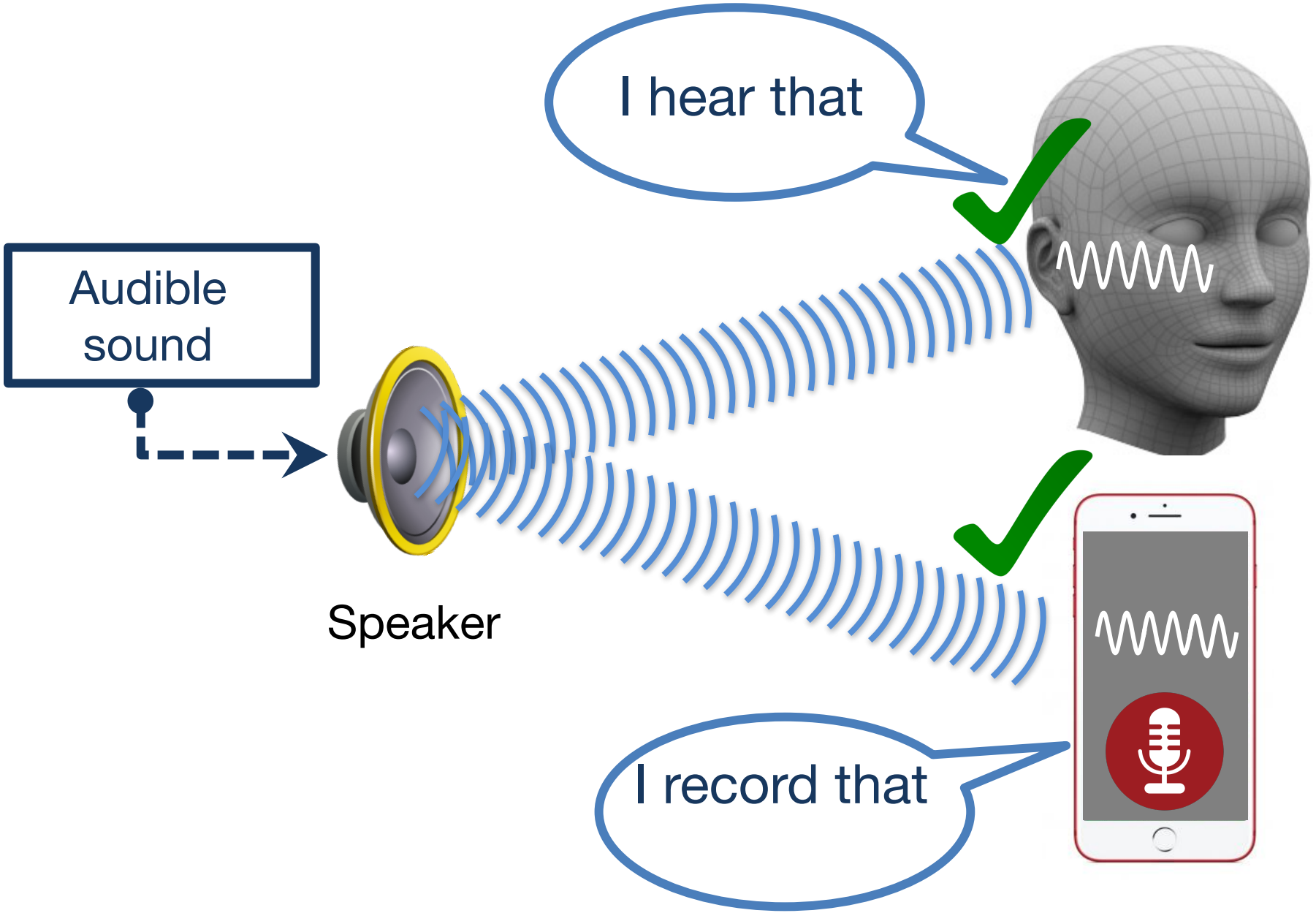




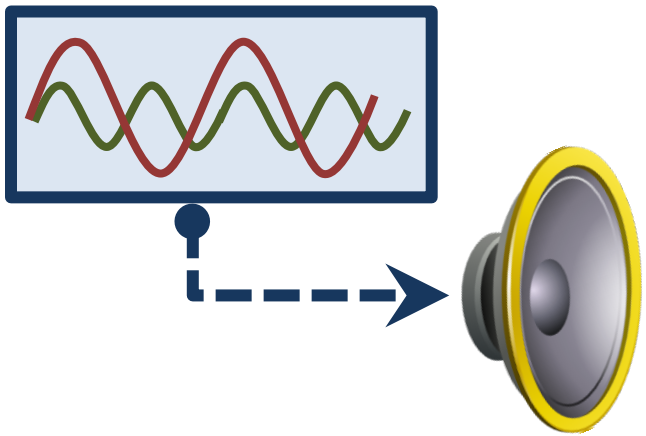




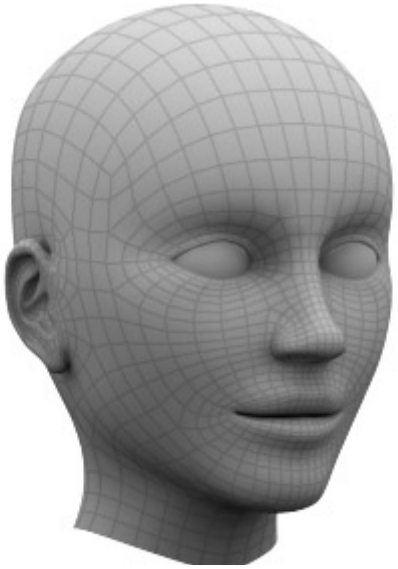
Microphones record audible sounds



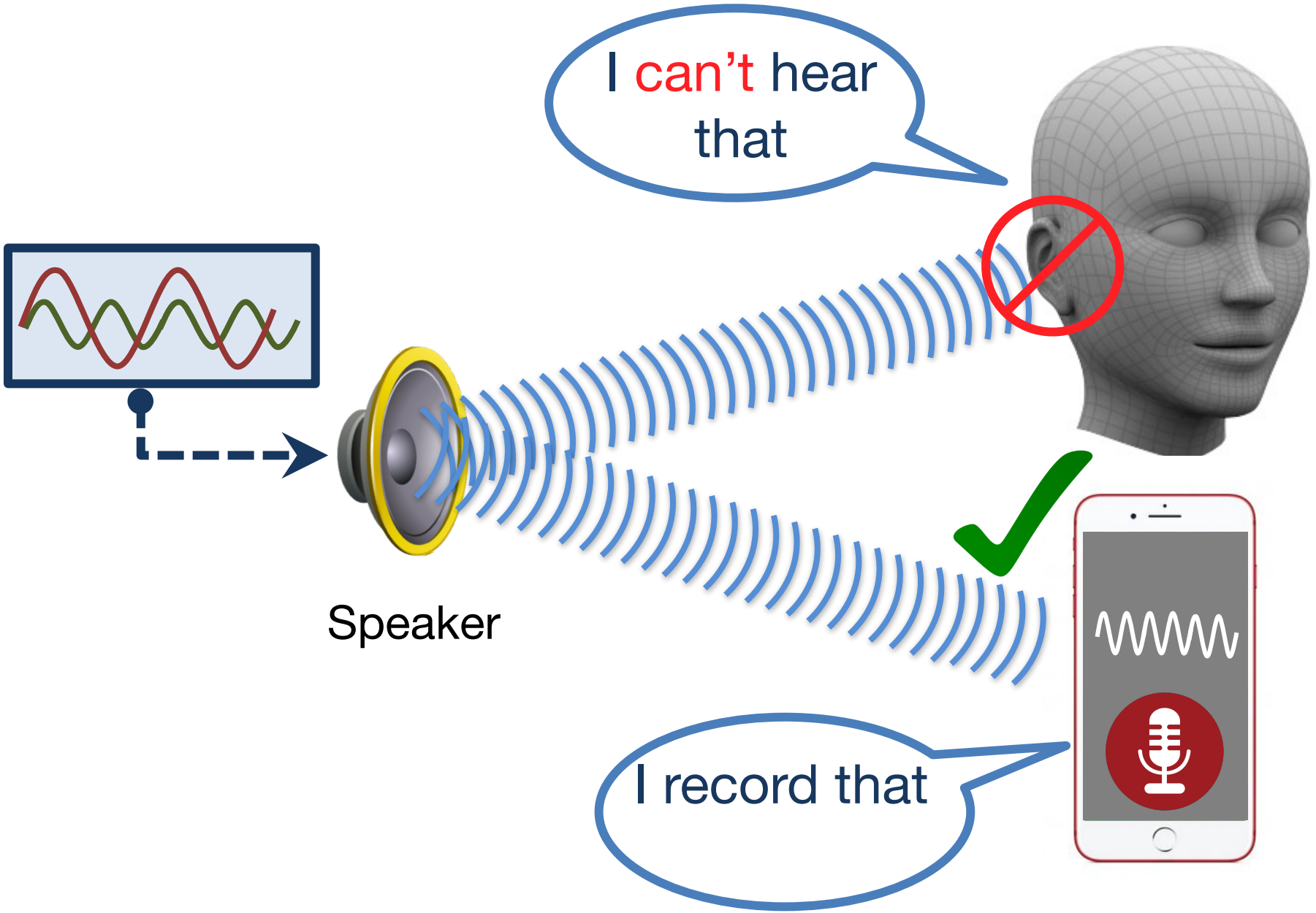
Inaudible, but recordable !



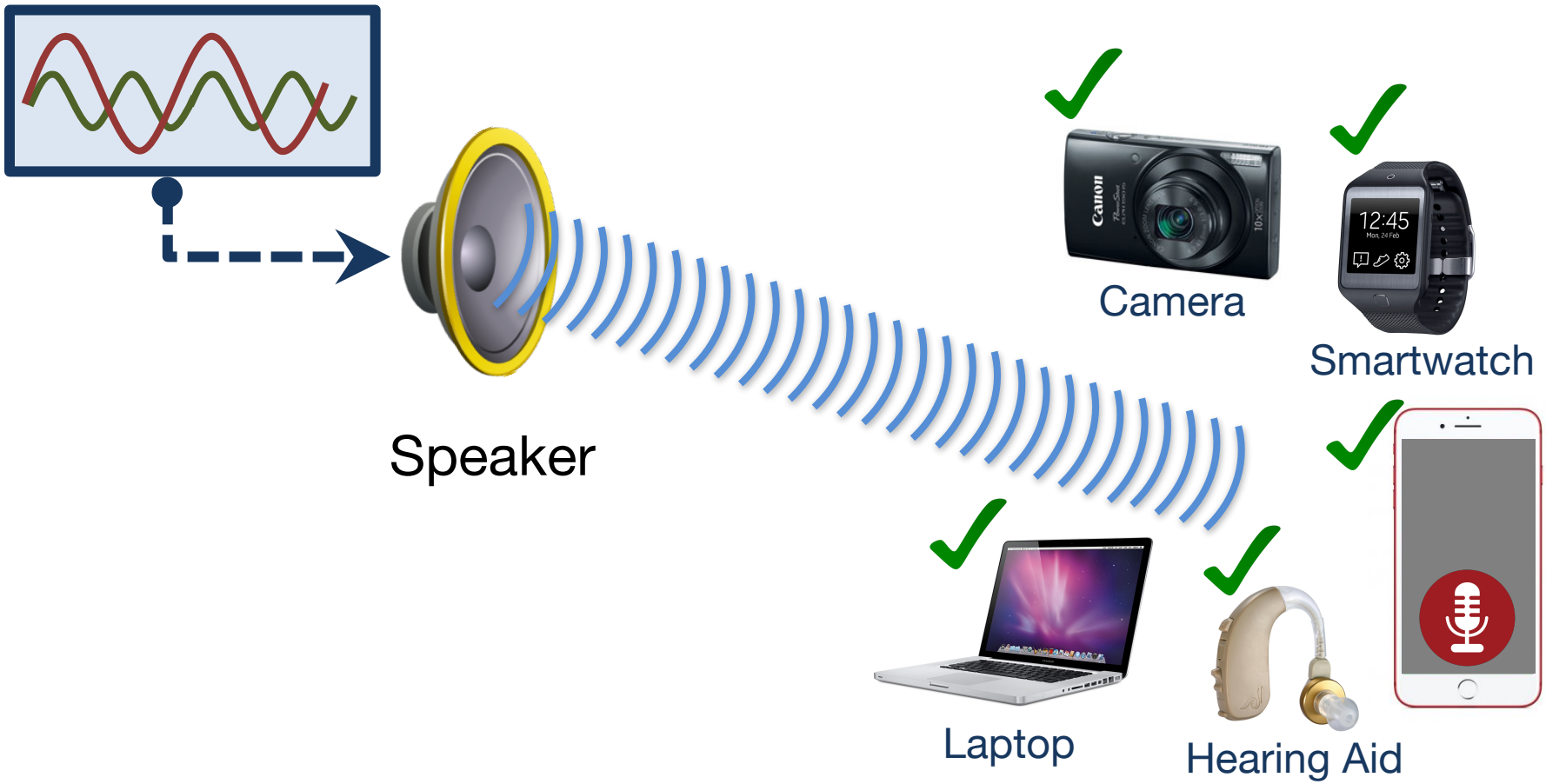
Speaker



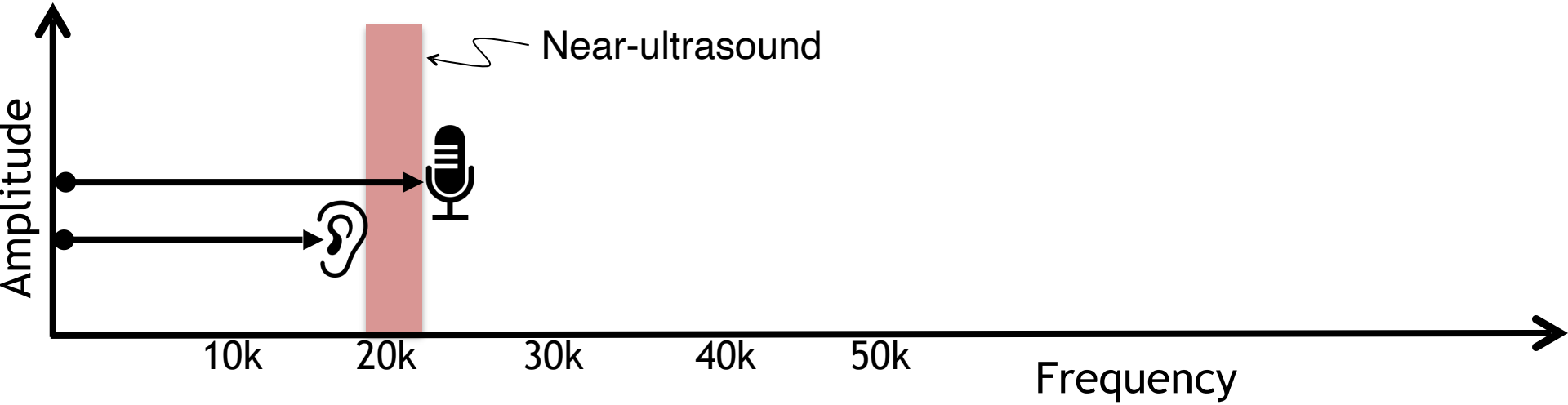
Inaudible, but recordable !



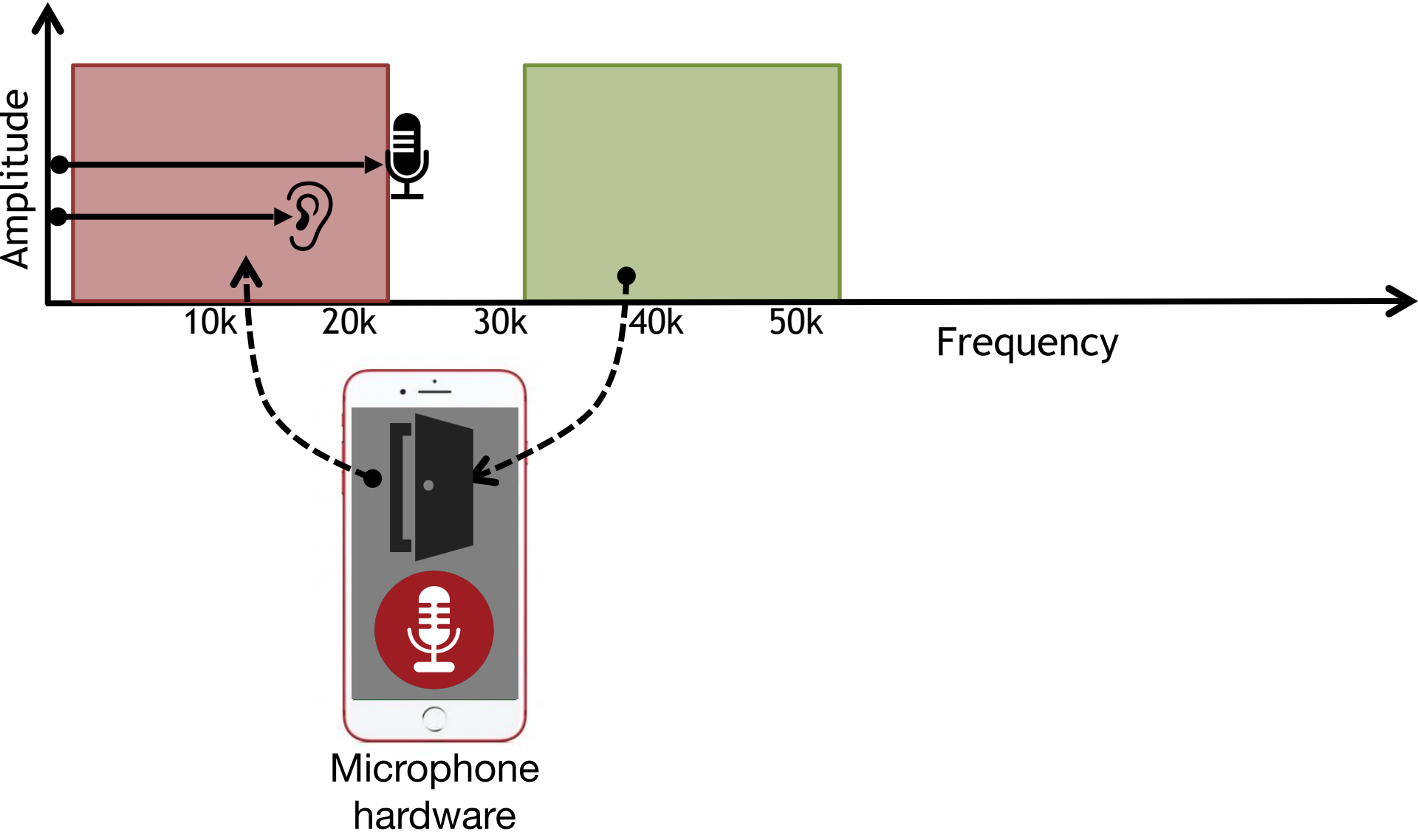
Works with unmodified devices



It's not "near-ultrasound"



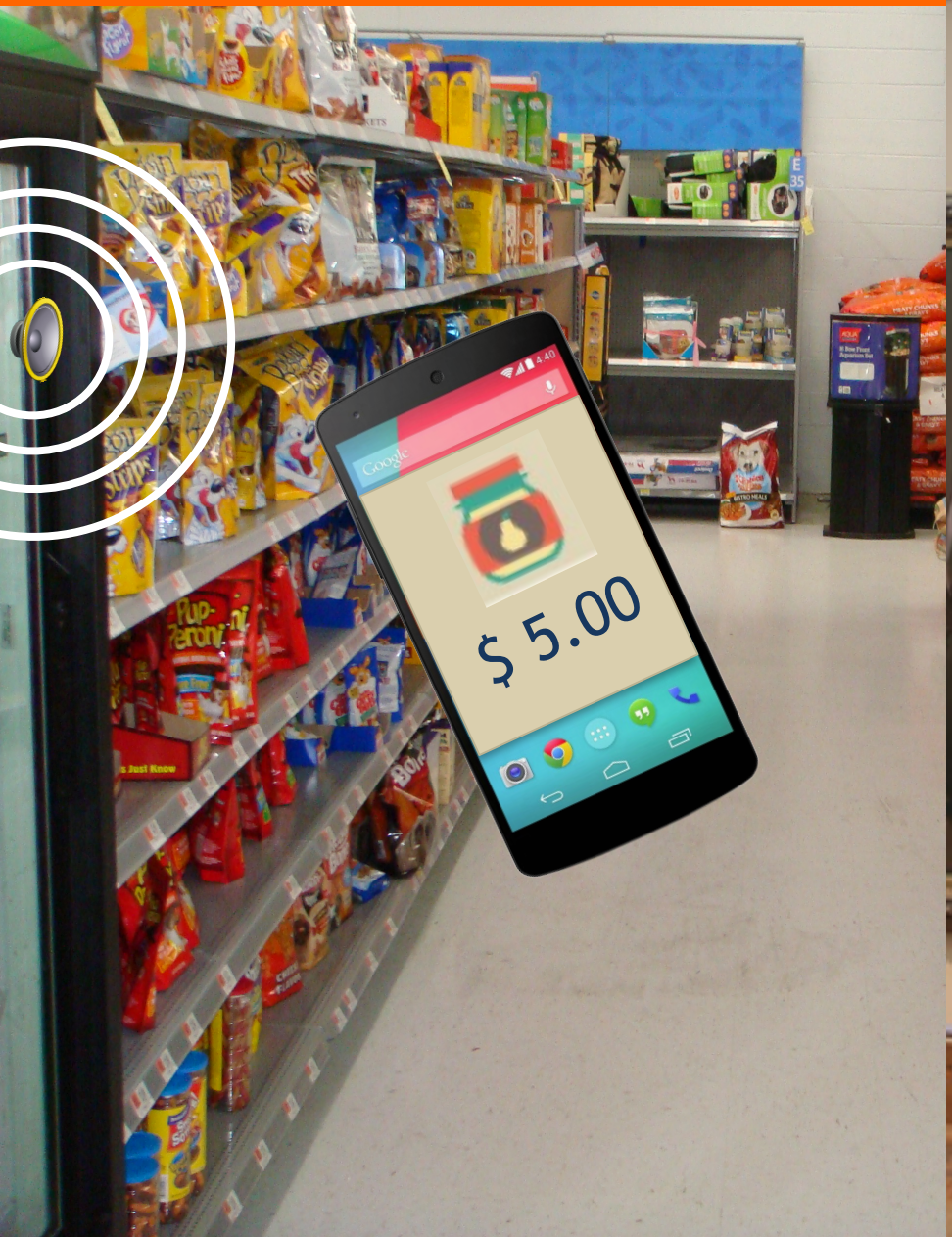
Exploiting fundamental nonlinearity



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

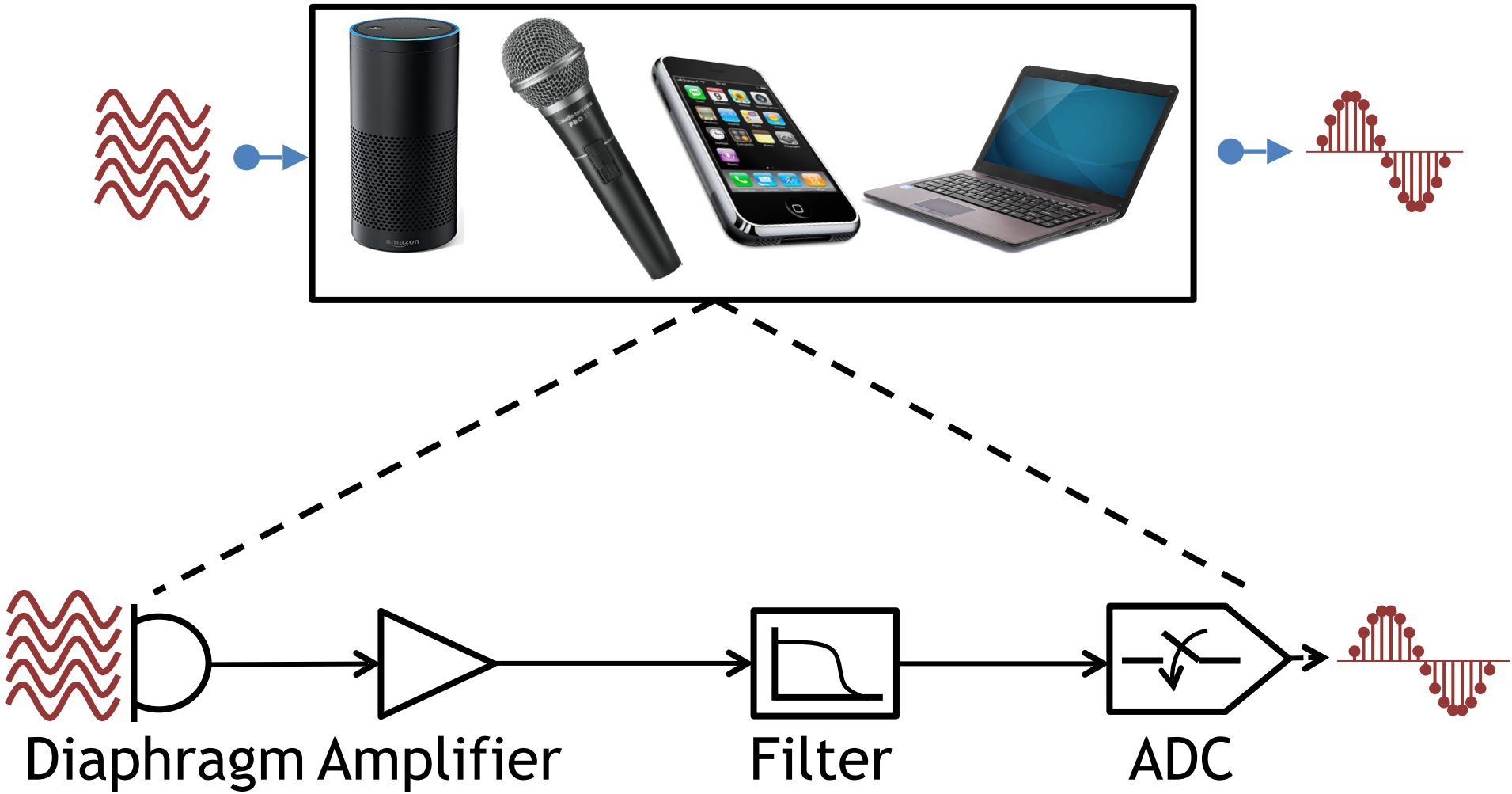
① Microphone Overview

② System Design

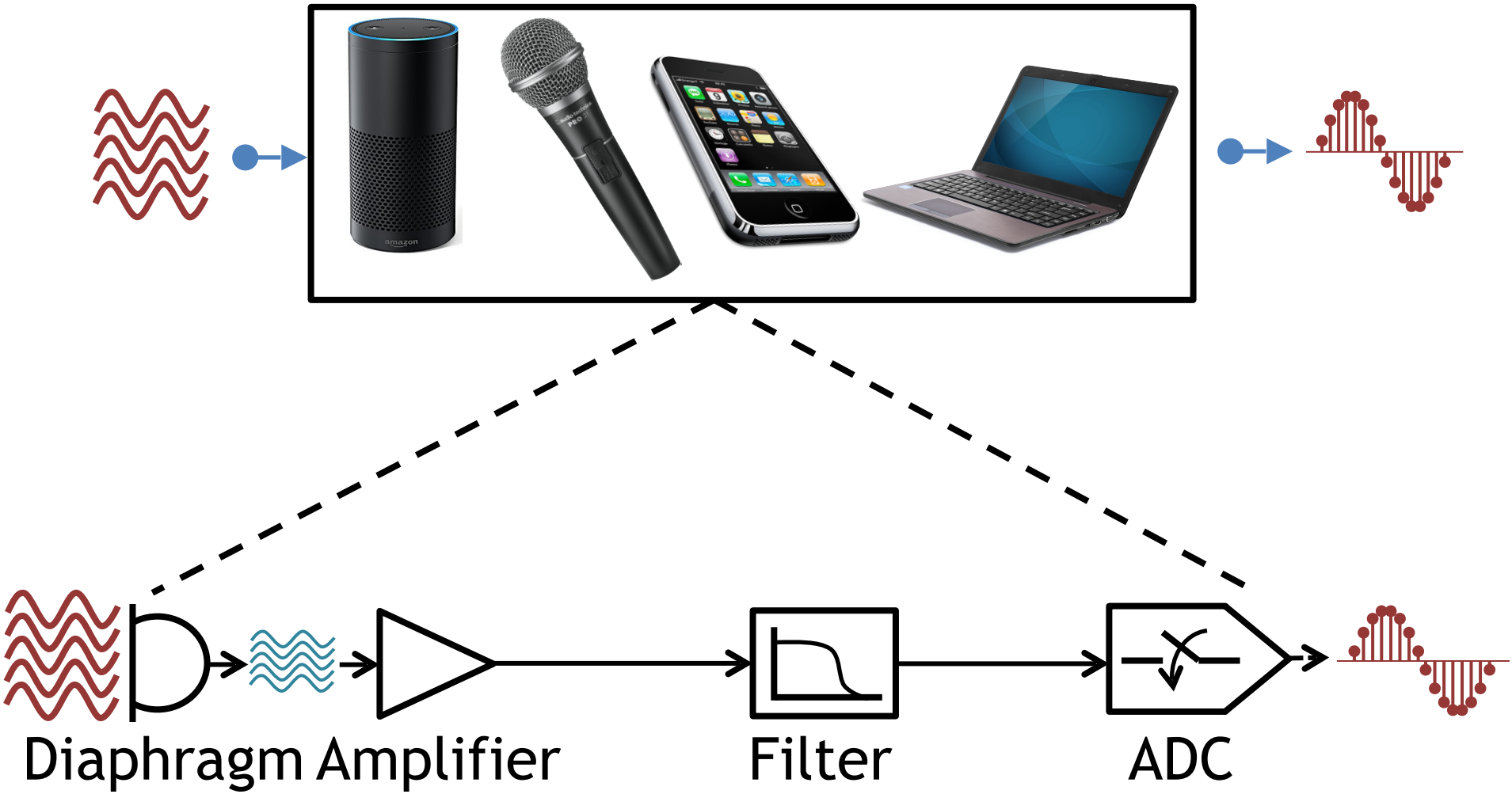
③ Challenges

④ Evaluation

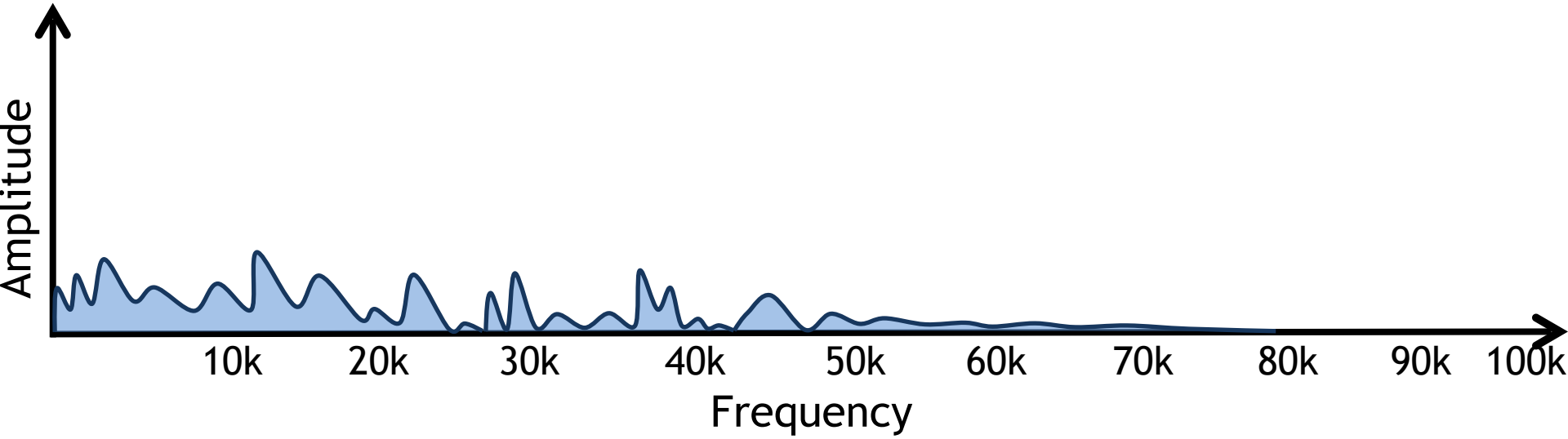
Microphone working principle

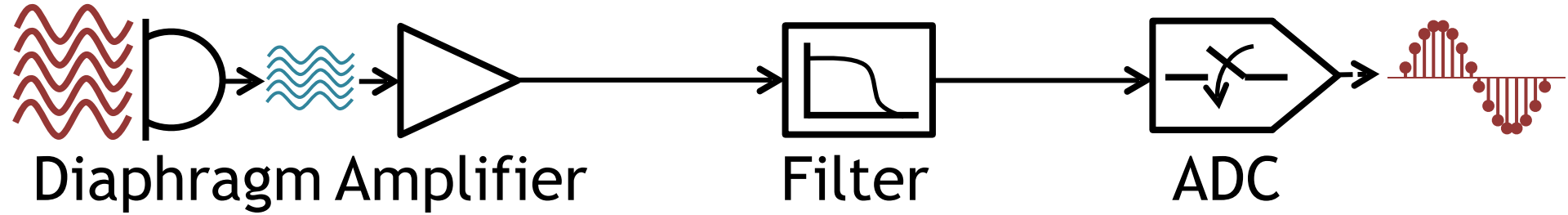


Microphone working principle

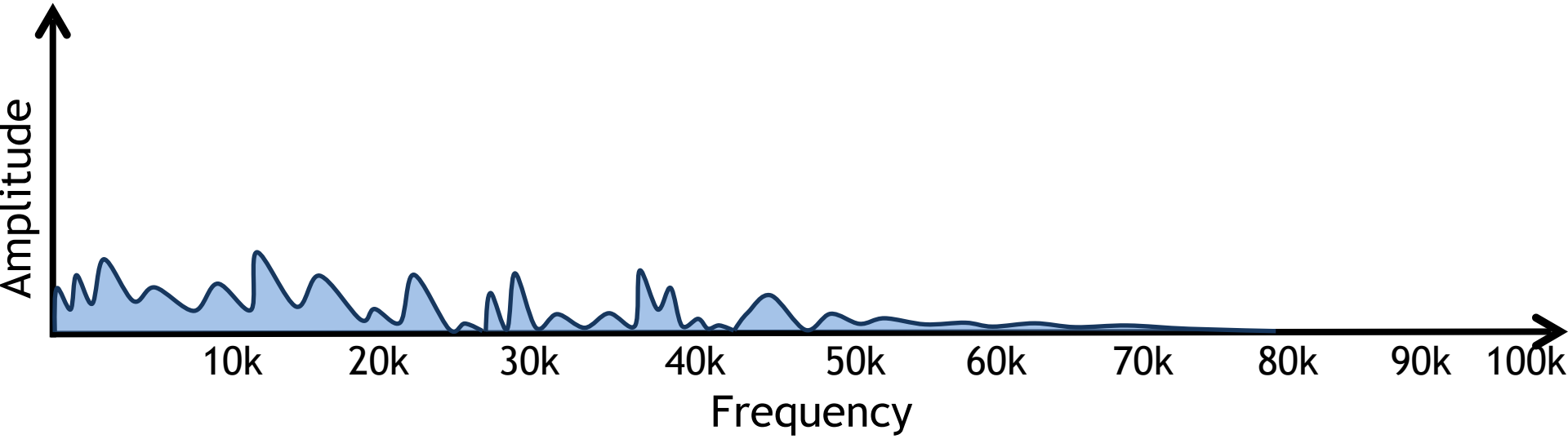


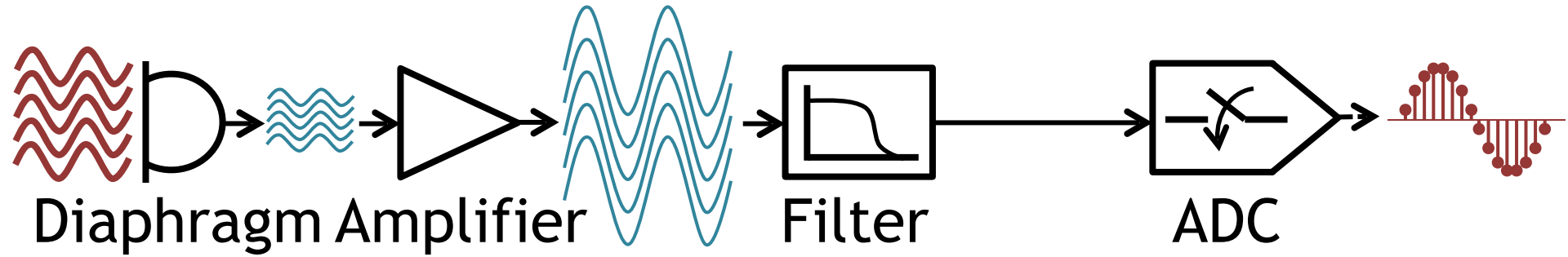
Microphone working principle



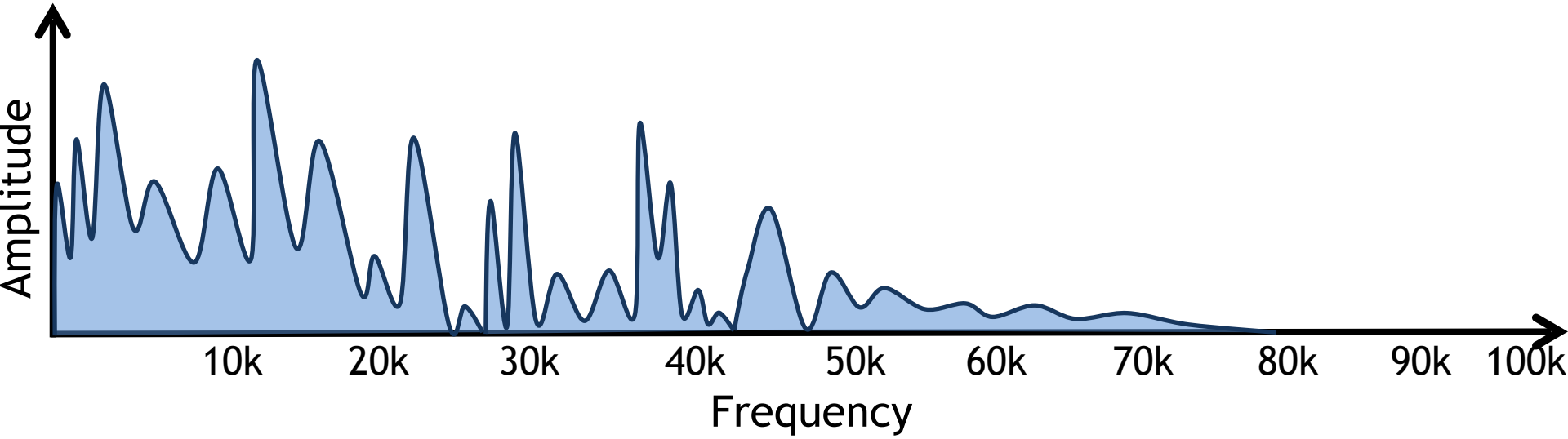


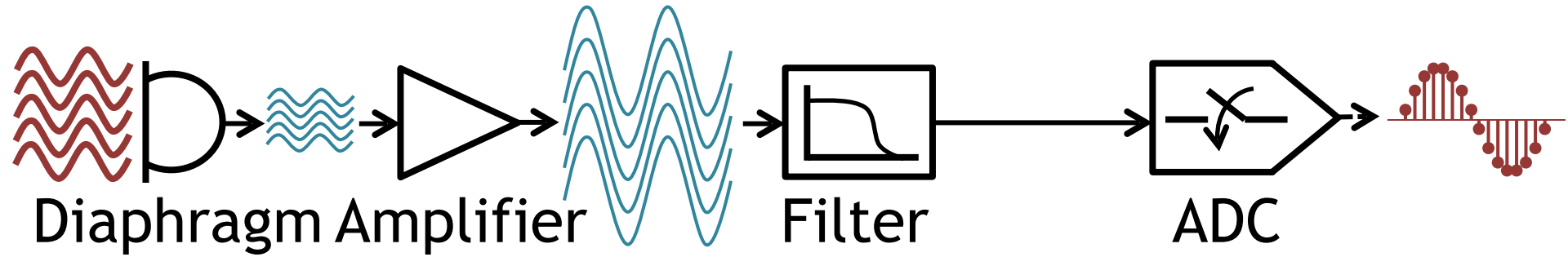
Microphone working principle



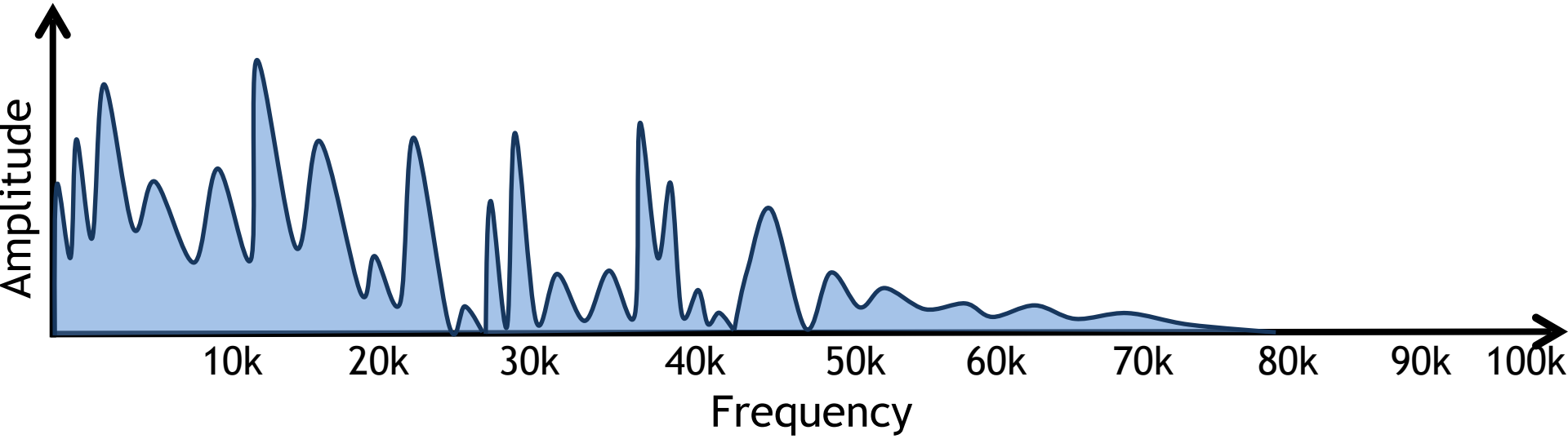


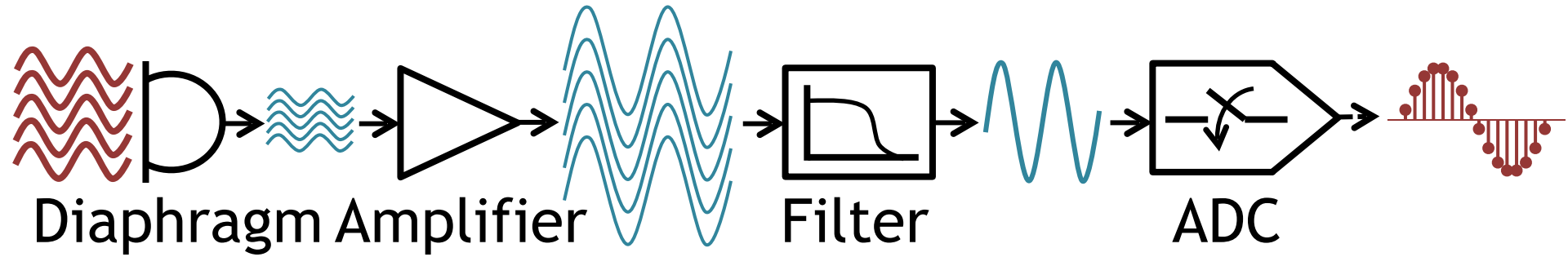
Microphone working principle



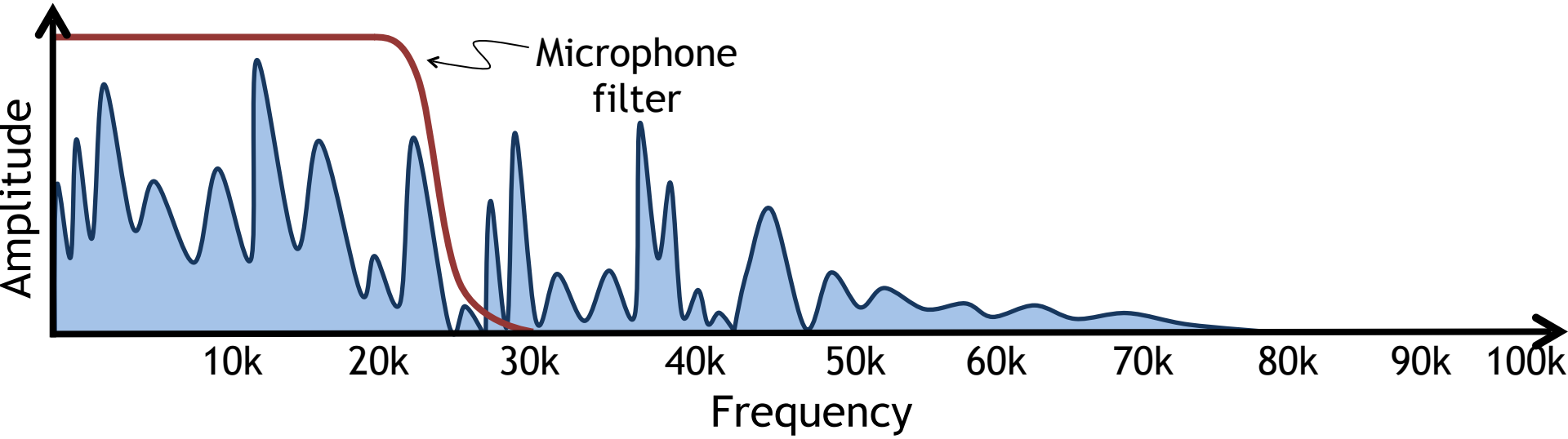


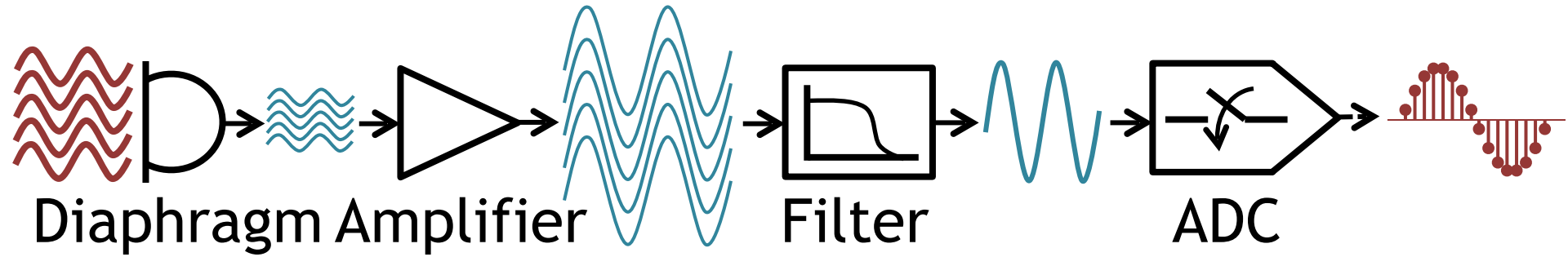
Microphone working principle



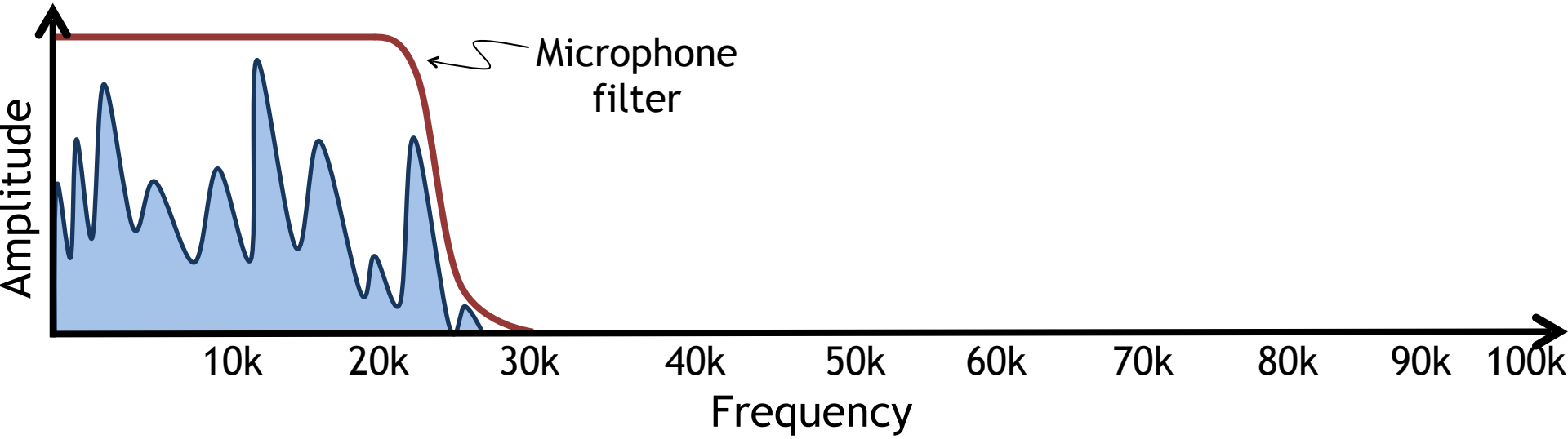


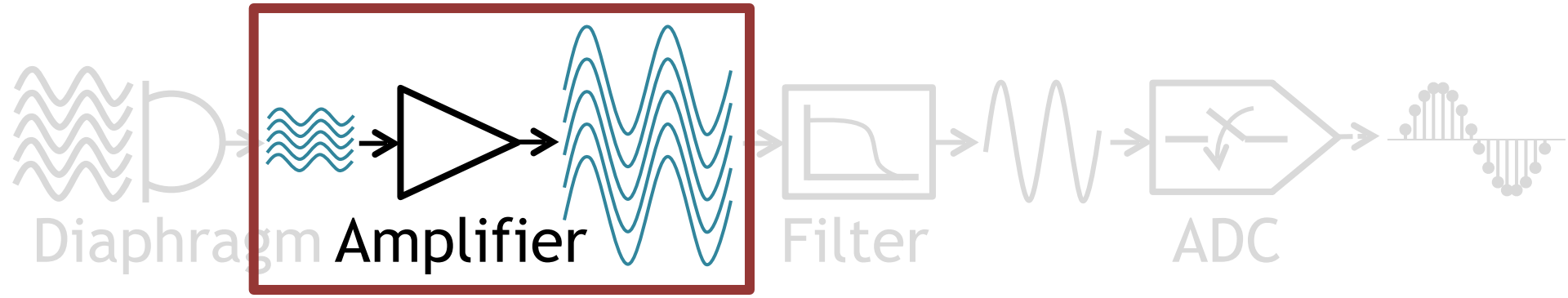
Microphone working principle



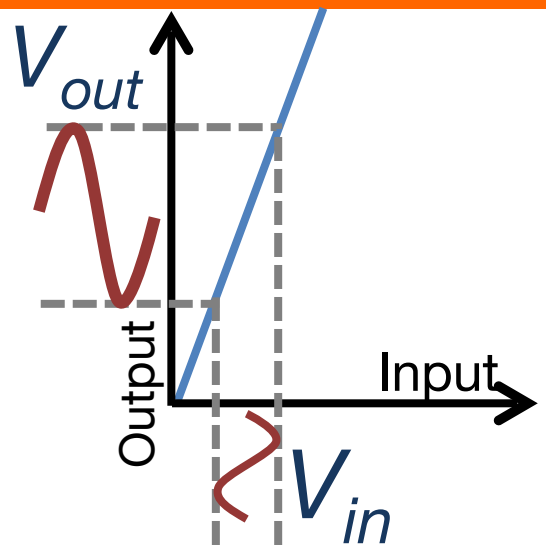


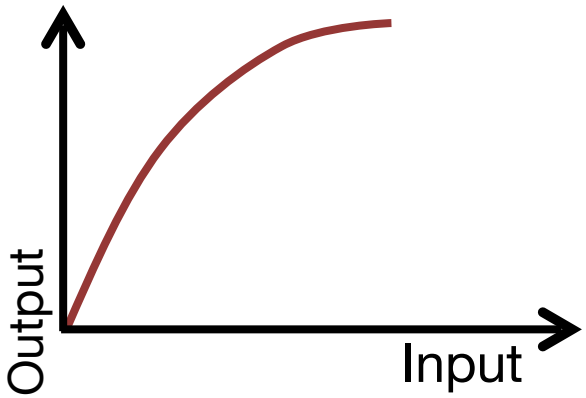
Microphone working principle





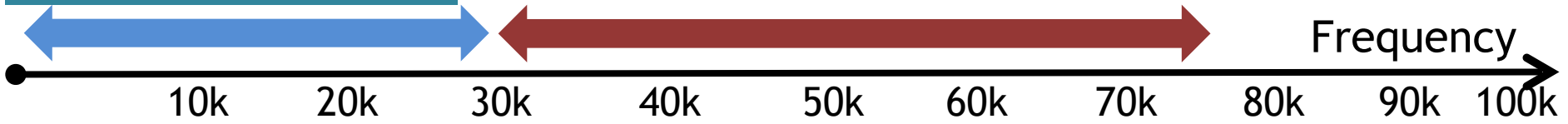
Microphone working principle

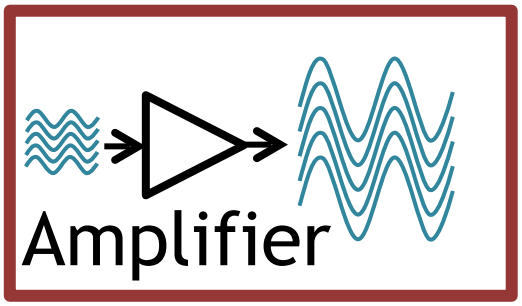




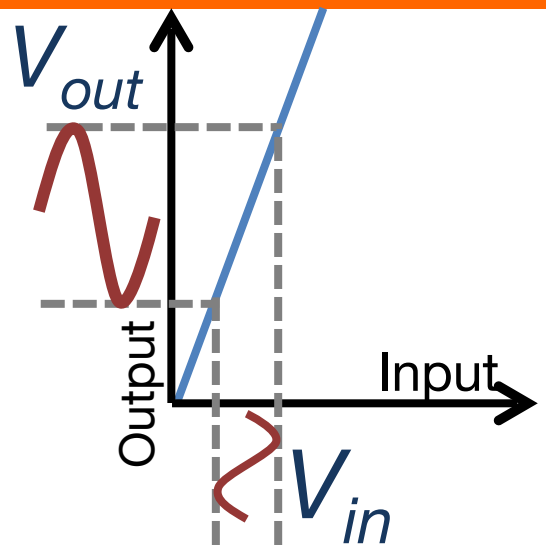
$V_{out} = a_1 V_{in}$

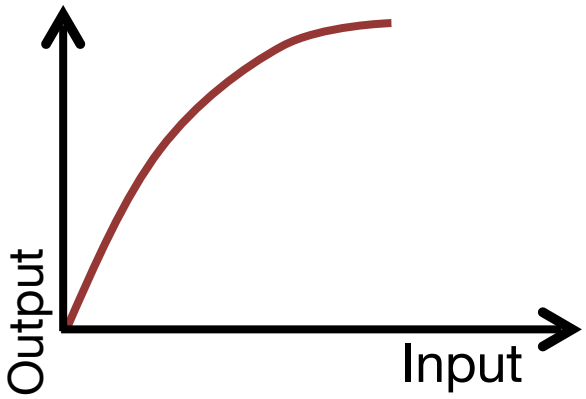
$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$





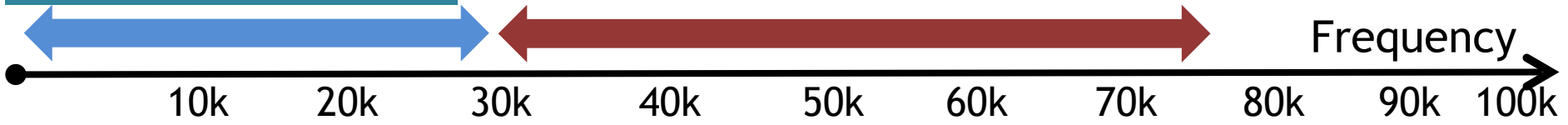
Microphone working principle

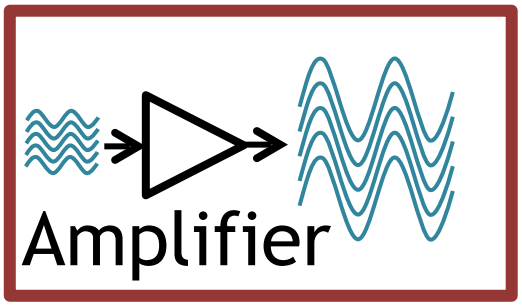




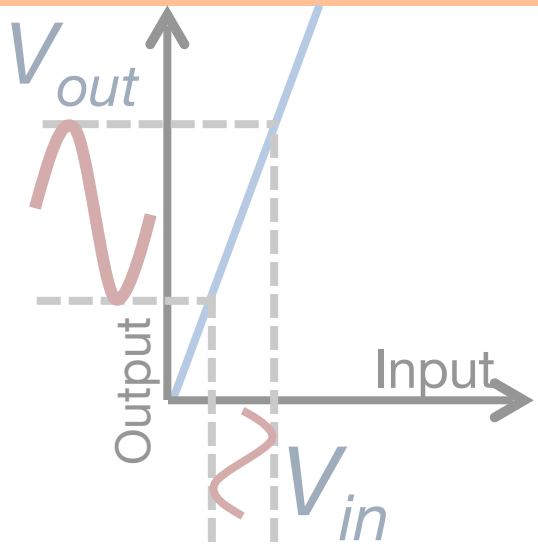
$V_{out} = a_1 V_{in}$

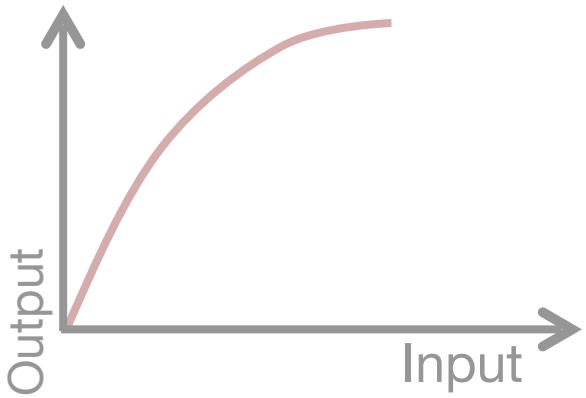
$V_{out} = a_1 V_{in} + a_2 V_{in}^2$





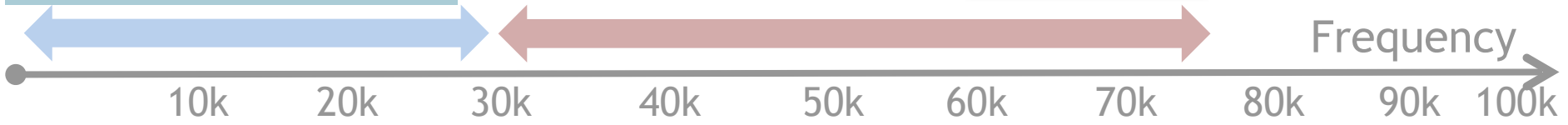
Microphone working principle

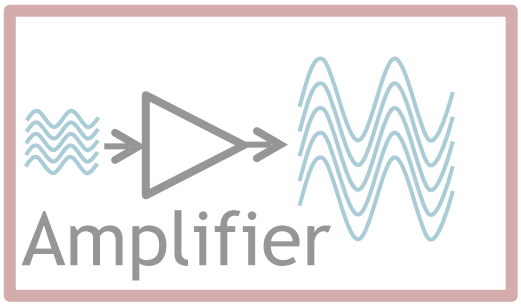




$V_{out} = a_1 V_{in}$

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





Talk outline

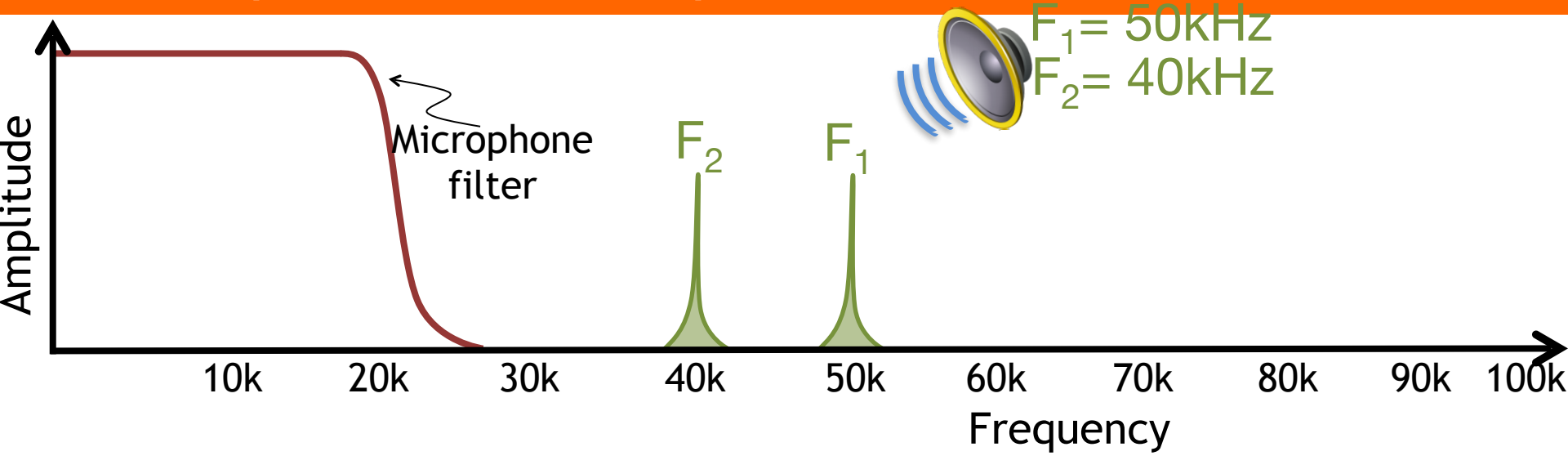
① Microphone Overview

② System Design

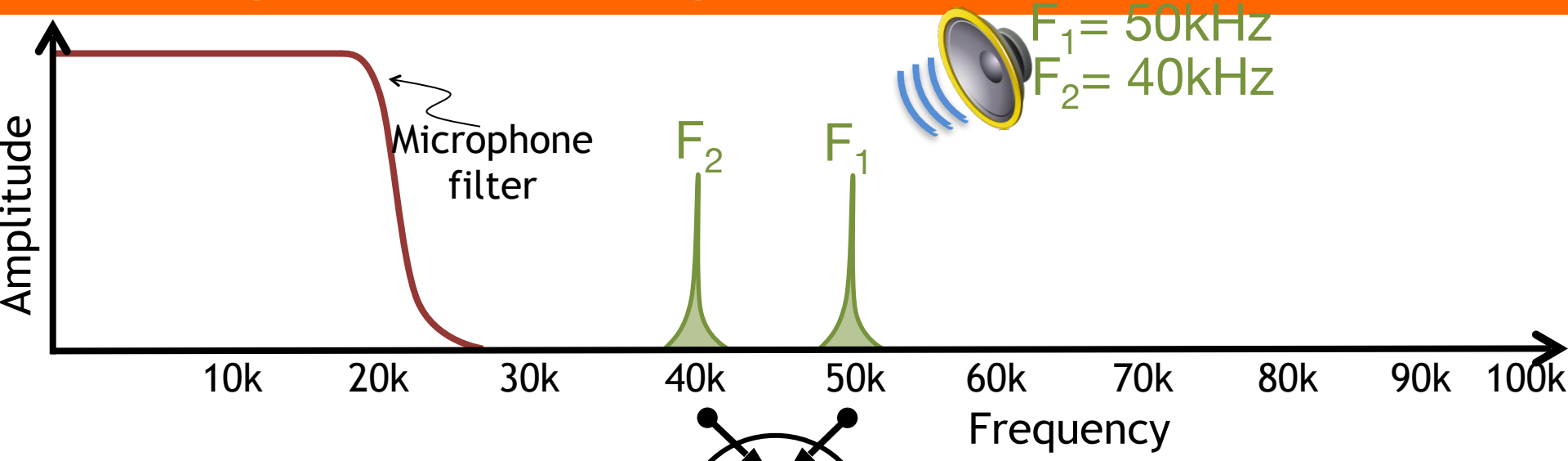
③ Challenges

④ Evaluation

Exploiting amplifier non-linearity



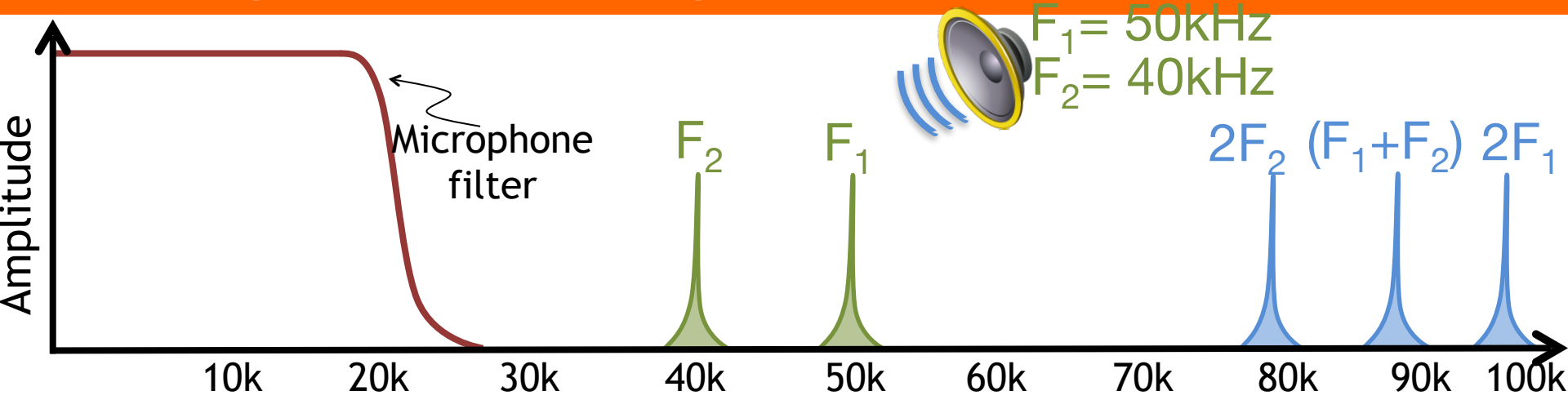
Exploiting amplifier non-linearity



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

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

Exploiting amplifier non-linearity

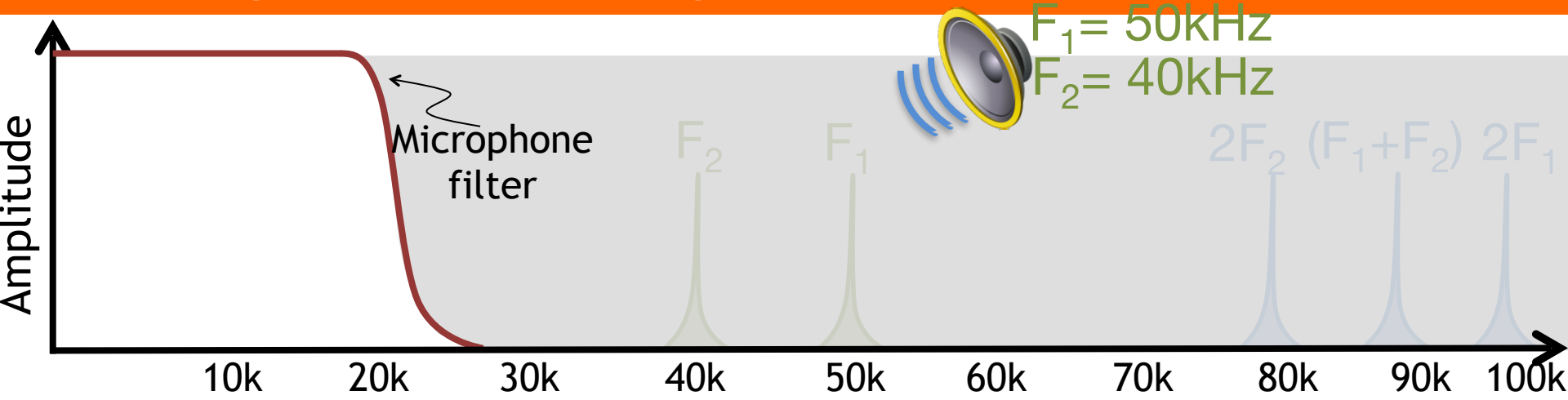


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

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

Exploiting amplifier non-linearity

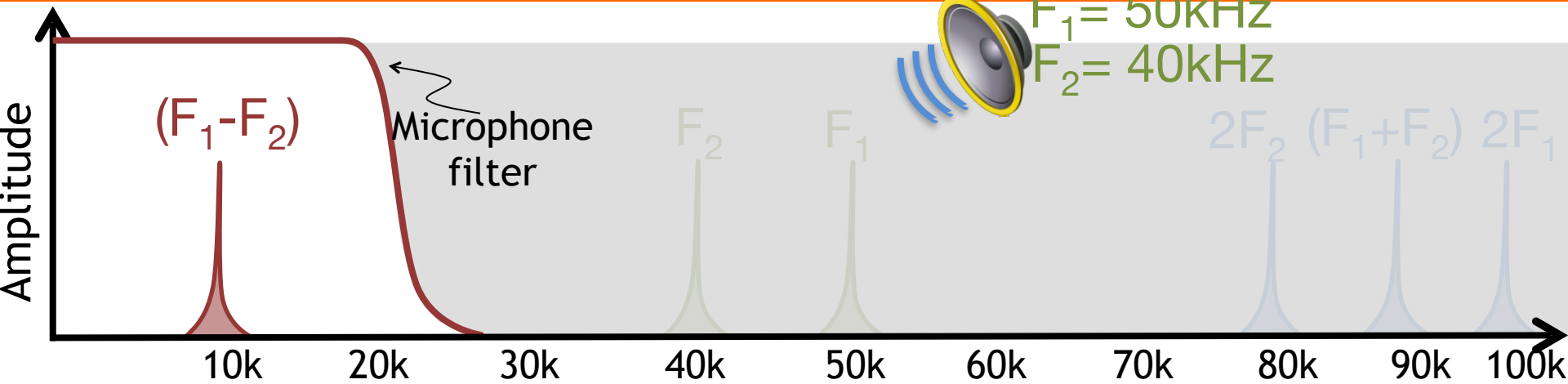


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

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

Exploiting amplifier non-linearity

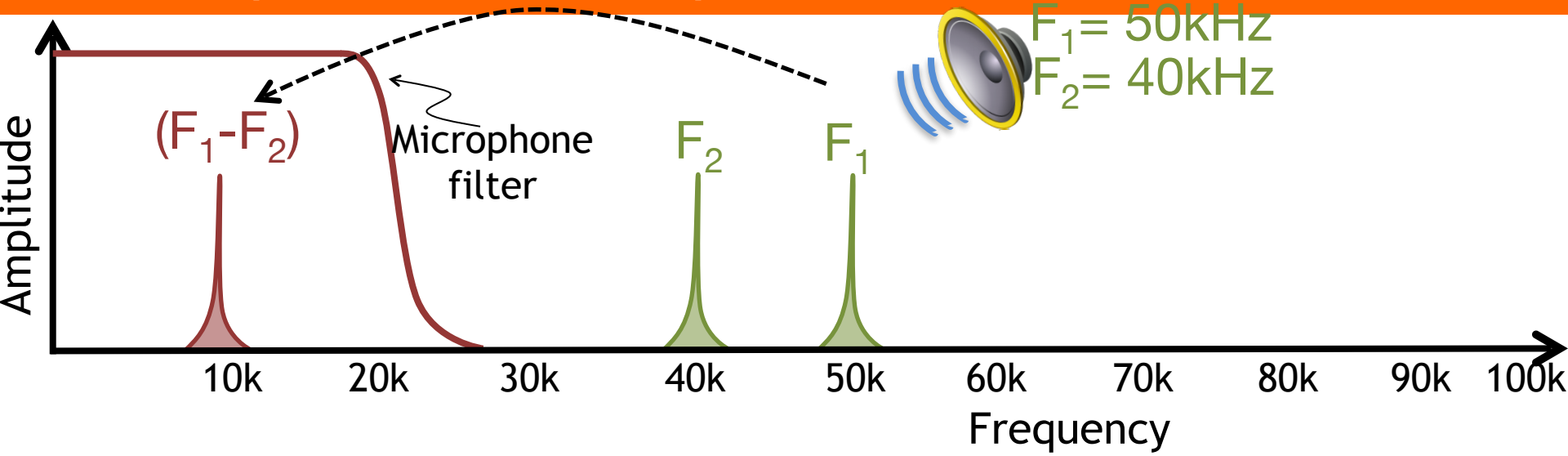


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

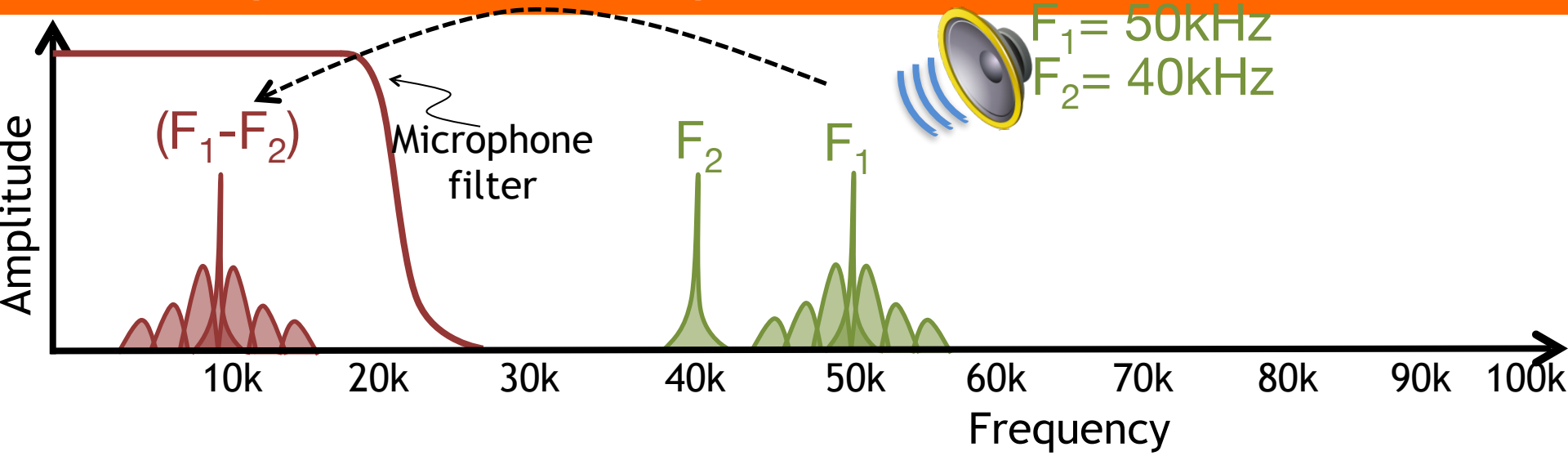
$$(\sin F_1 + \sin F_2)^2 =$$

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

Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Talk outline

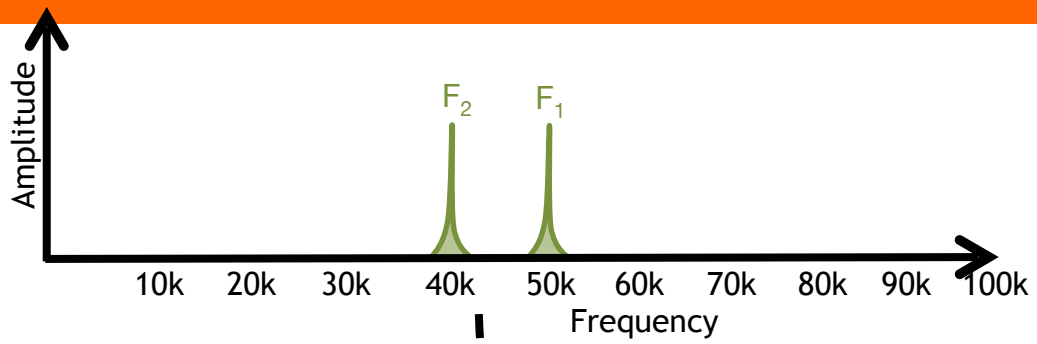
① Microphone Overview

② System Design

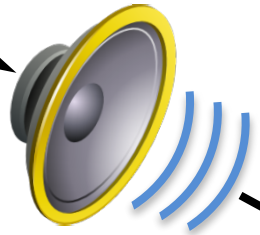
③ Challenges

④ Evaluation

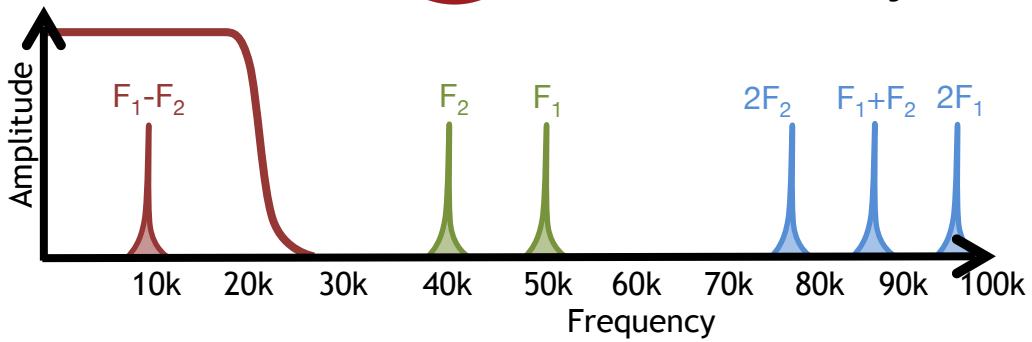
Challenges



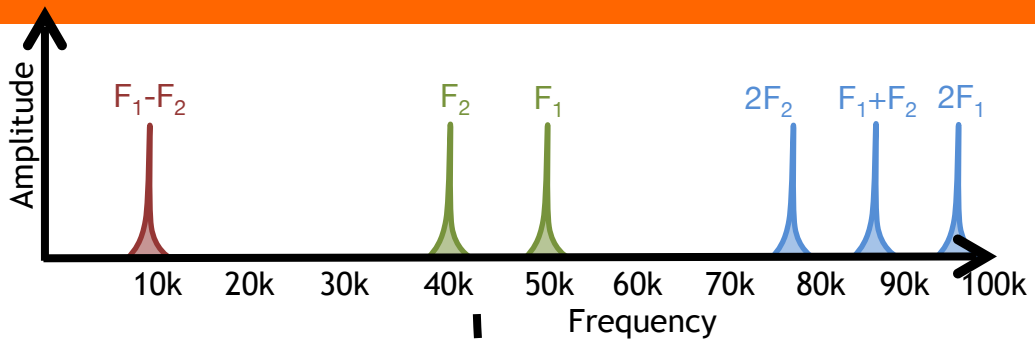
Speaker's nonlinearity



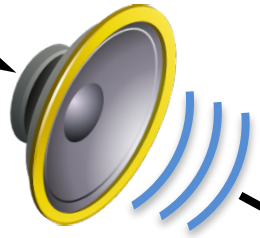
Microphone's nonlinearity



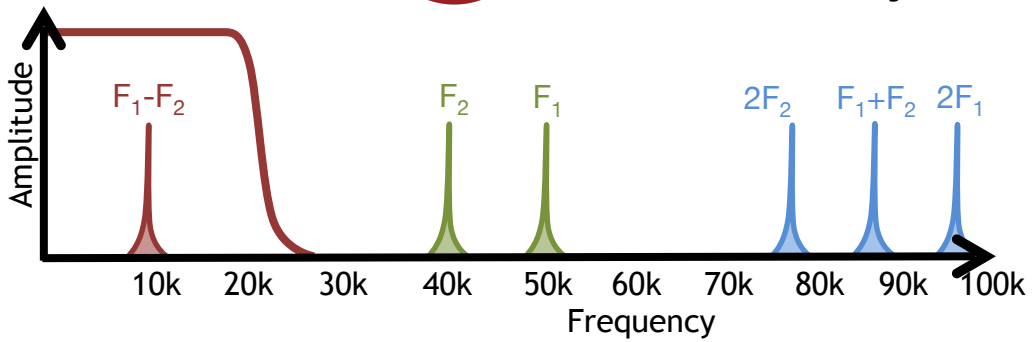
Challenges



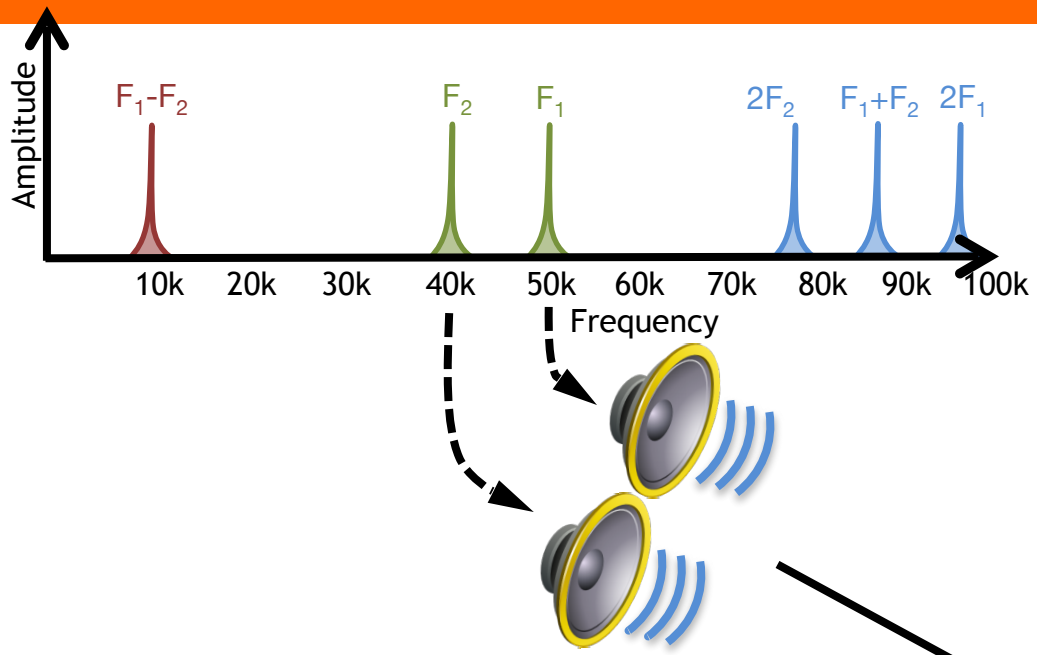
Speaker's nonlinearity



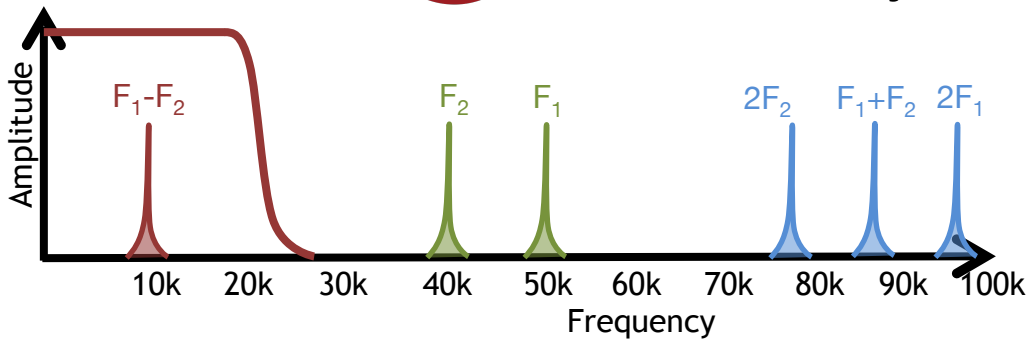
Microphone's nonlinearity



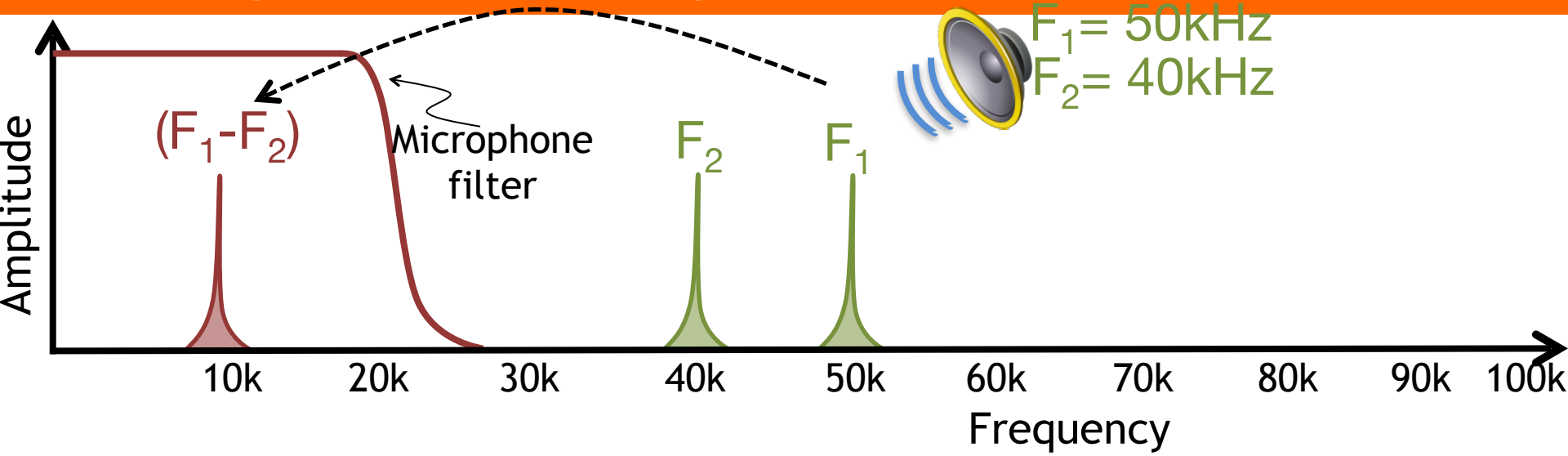
Challenges



Microphone's nonlinearity



Exploiting amplifier non-linearity



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

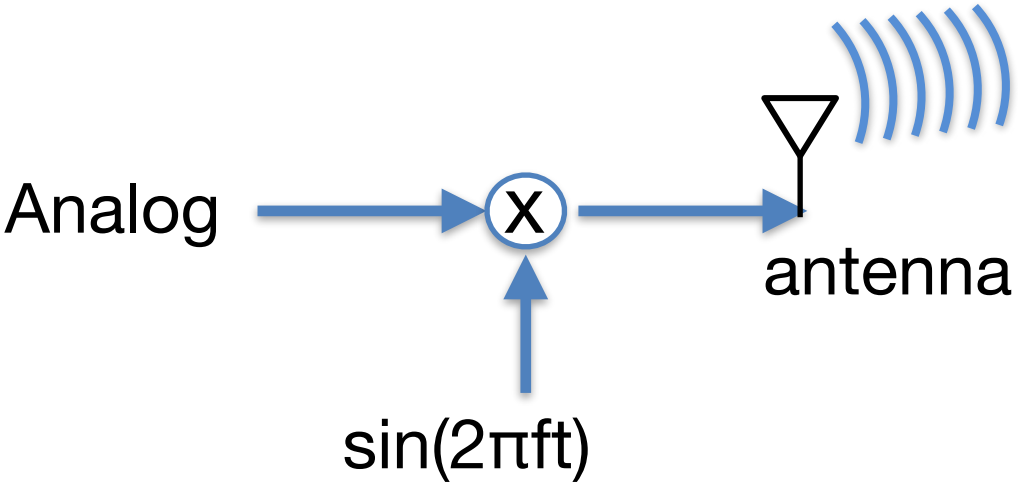
How can we send this command?

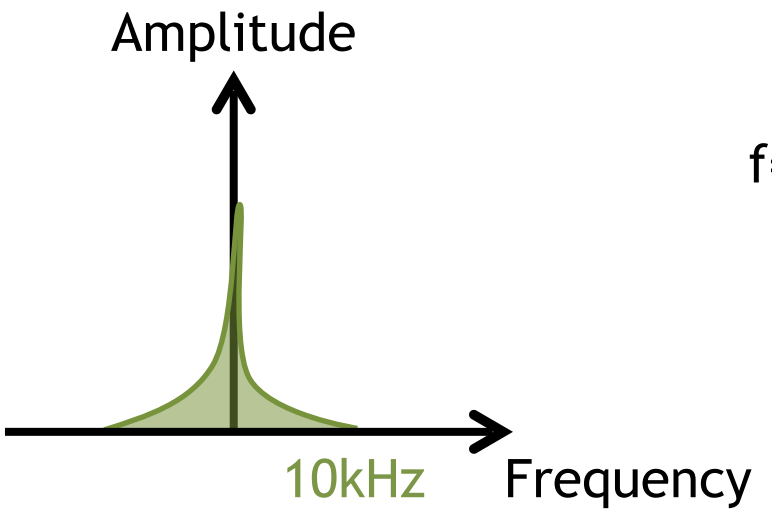
Discuss in pairs for 3 min

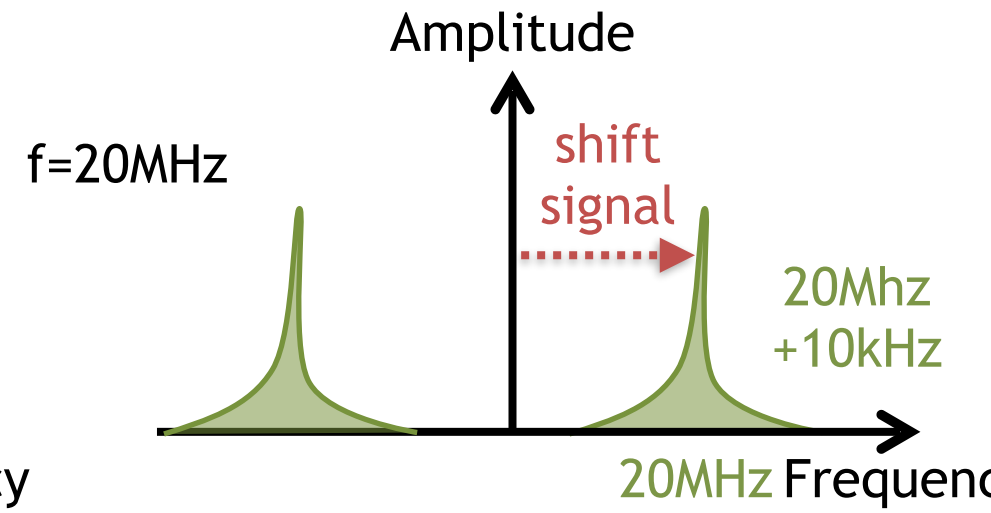
Primer on Modulation

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

Primer on Modulation

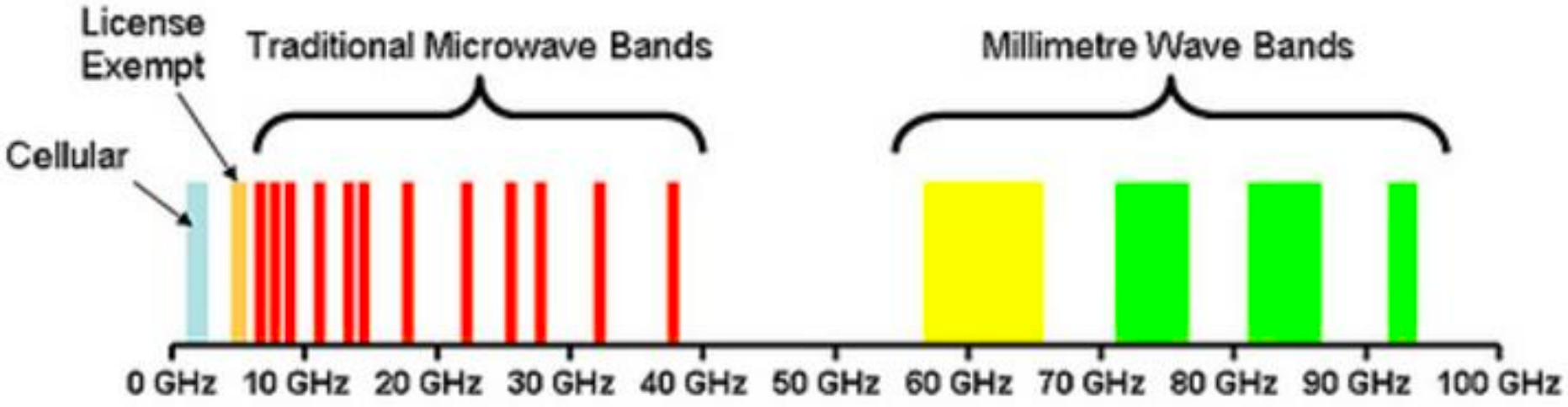






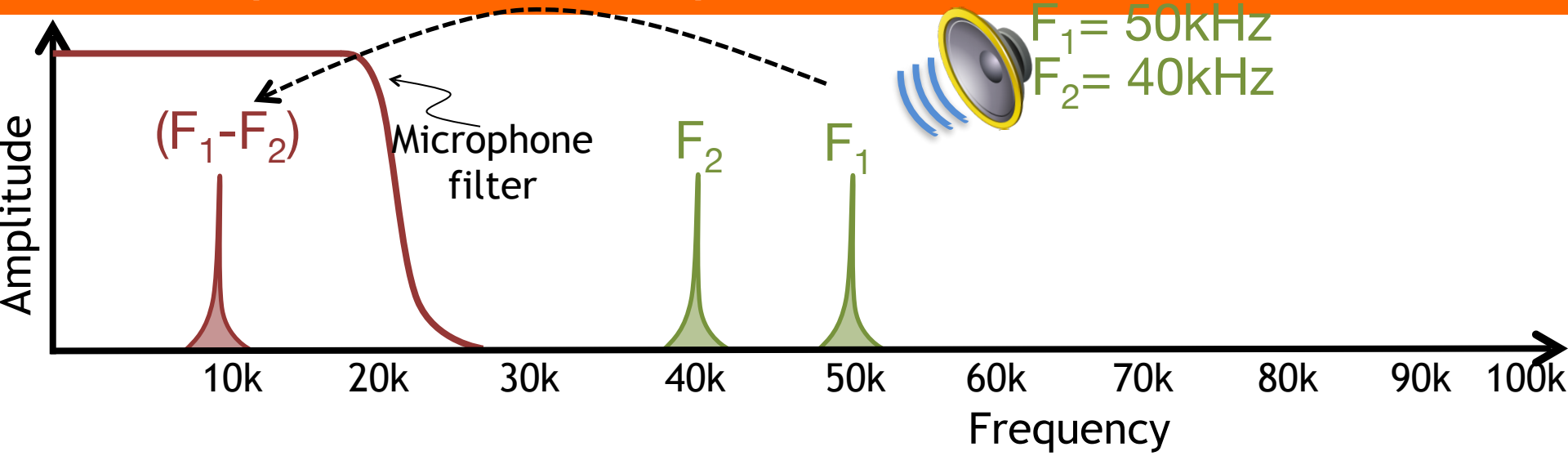
Why is Modulation useful?

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.

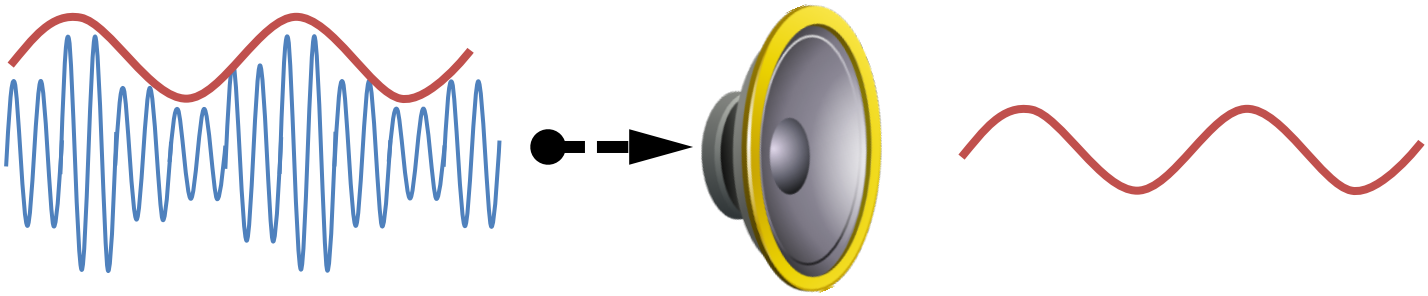
How can we send this command message m(t)?

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

Challenges

Amplitude modulation

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



Ultrasonic speaker

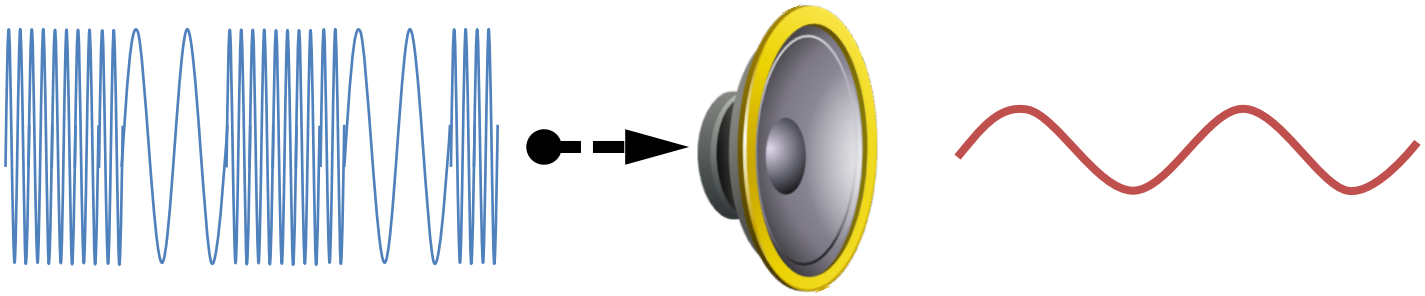
$$\begin{aligned} S^2_{out,AM} &= A_2\{aSin(\omega_m t).Sin(\omega_c t)\}^2 \\ &= -A_2\frac{a^2}{4}\{Cos(\omega_c t - \omega_m t) - Cos(\omega_c t + \omega_m t)\}^2 \\ &= -A_2\frac{a^2}{4}Cos(2\omega_m t) + (terms\ with\ frequencies \\ &\qquad\qquad above\ \omega_c\ and\ DC) \end{aligned}$$

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

Challenges

Frequency modulation

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

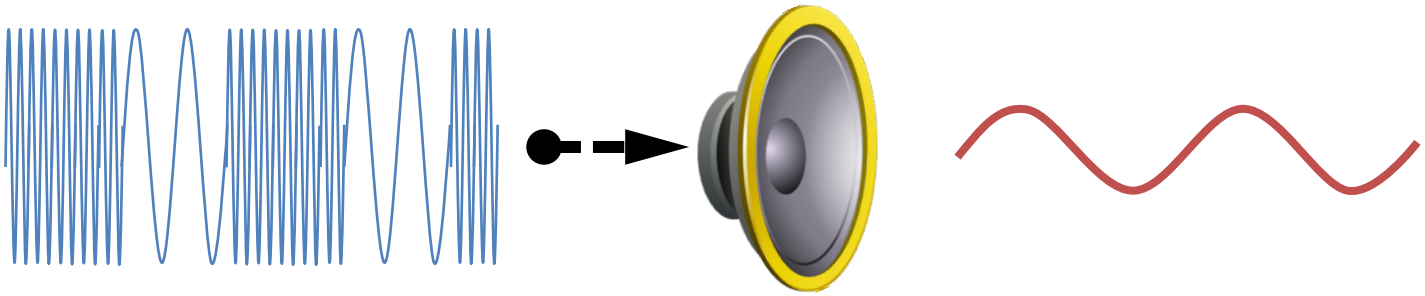


Ultrasonic speaker

Challenges

Frequency modulation

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



Ultrasonic speaker

Talk outline

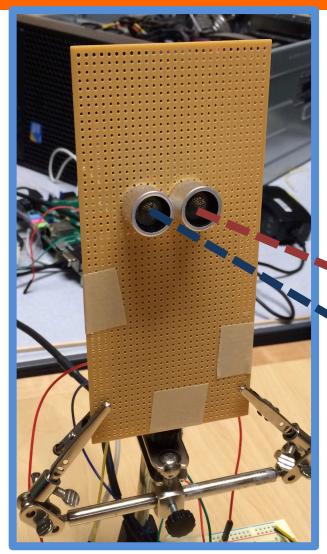
① Microphone Overview

② System Design

③ Challenges

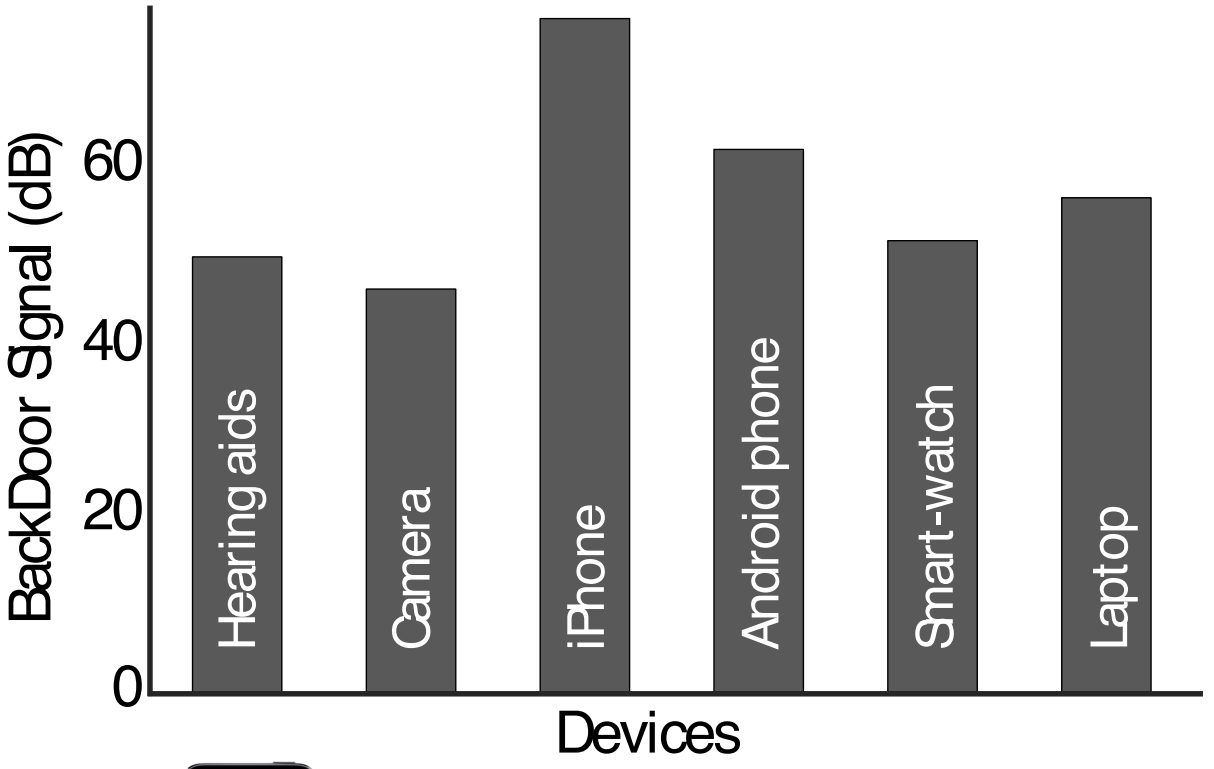
④ Evaluation

Hardware generalizability



40 kHz

50 kHz



Hearing Aid

Camera

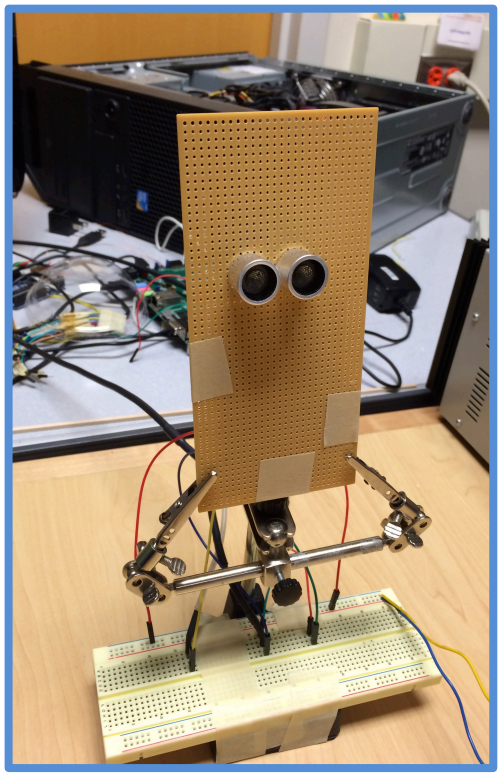
iPhone

Android phone

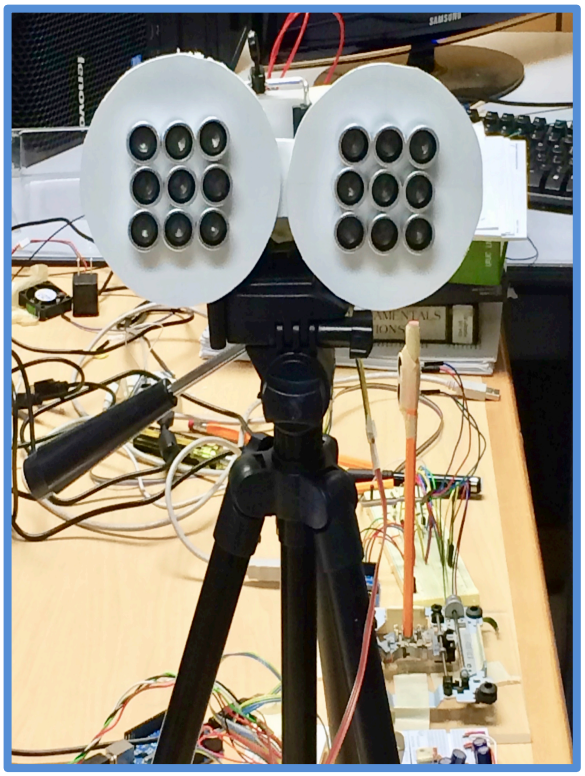
Smartwatch

Laptop

Implementation

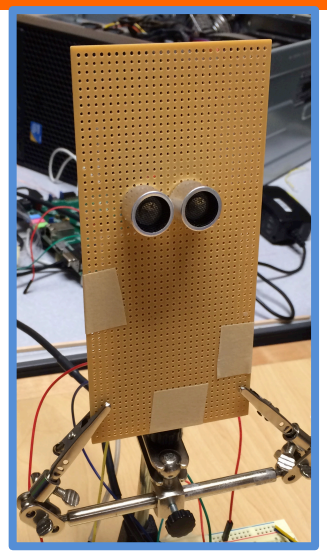


Communication prototype



Jammer prototype

Communication performance

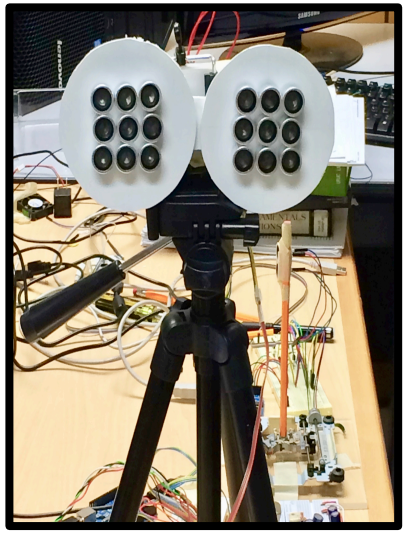


FM data packets

4kbps
up to 1 meter

More power can increase the distance

Jamming performance

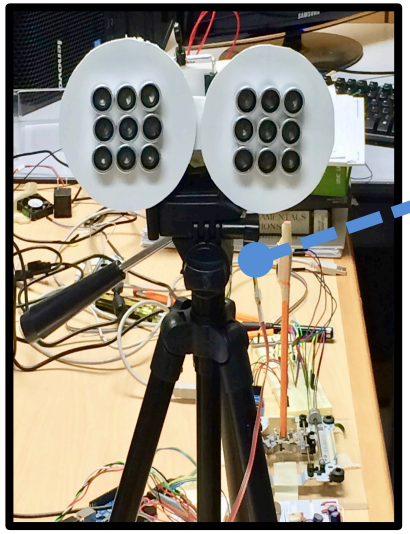


BackDoor jammer

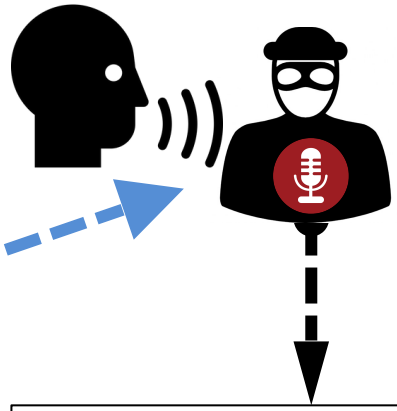
Spy microphone

Jamming performance

2000 spoken words

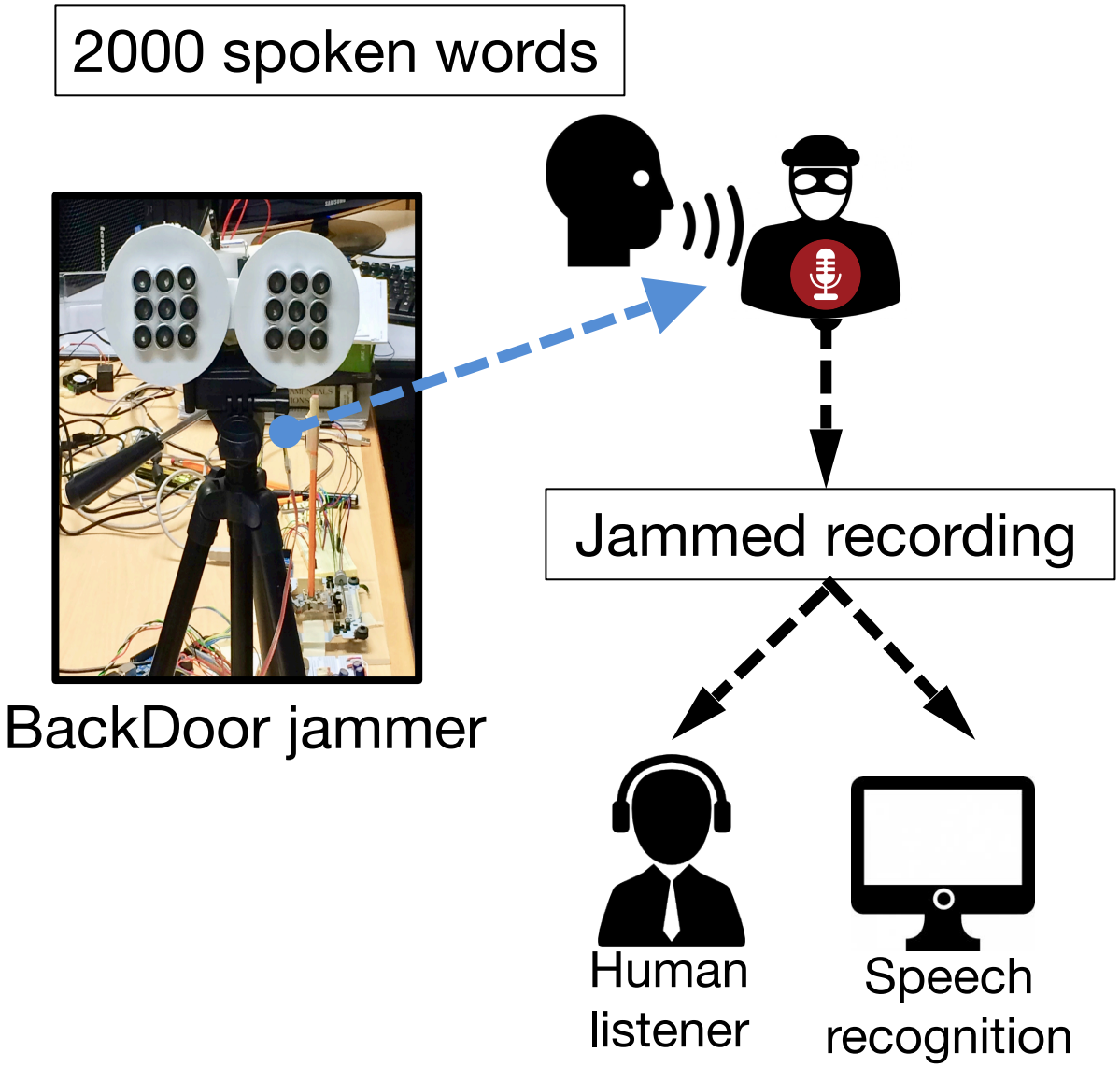


BackDoor jammer

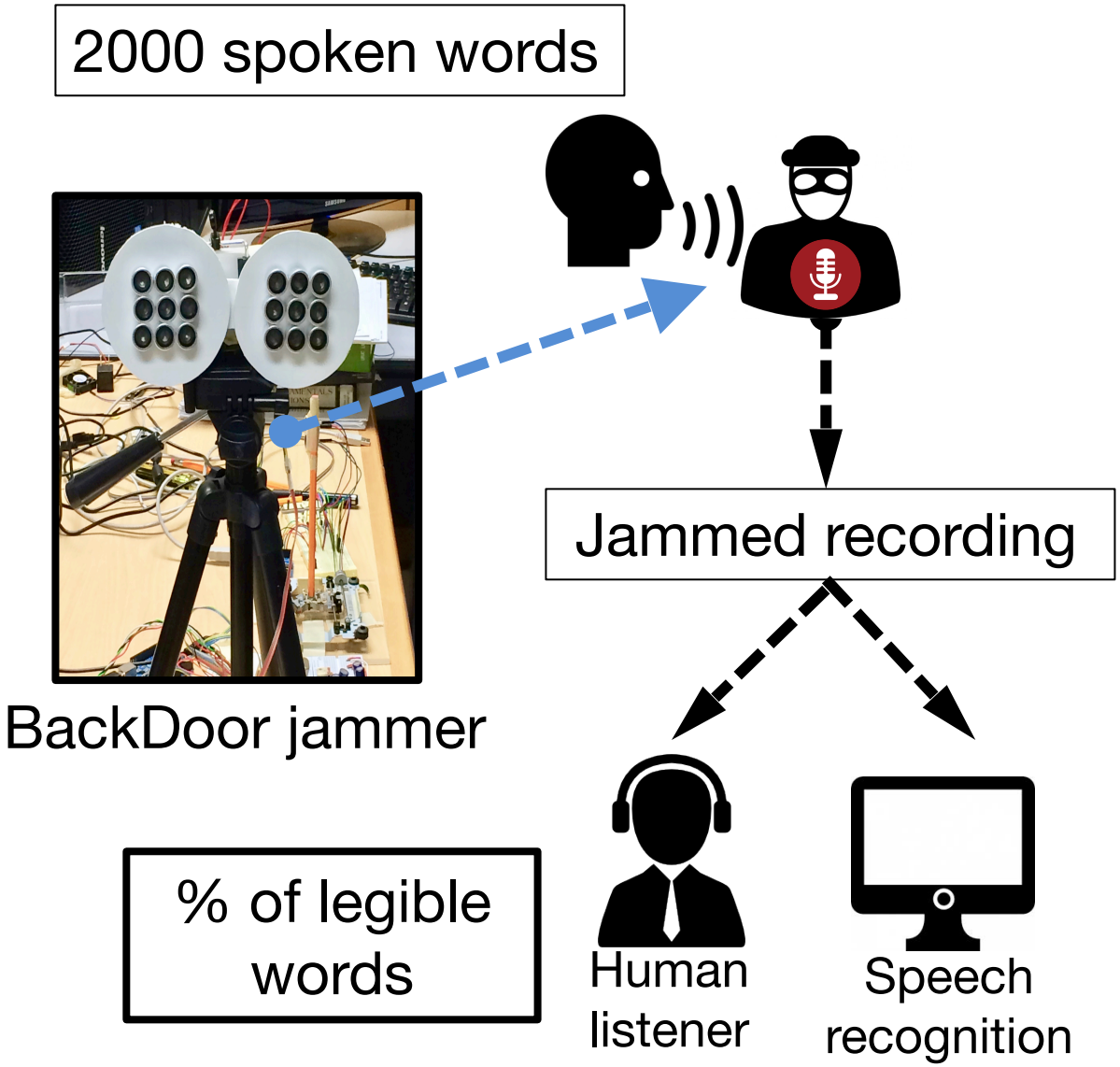


Jammed recording

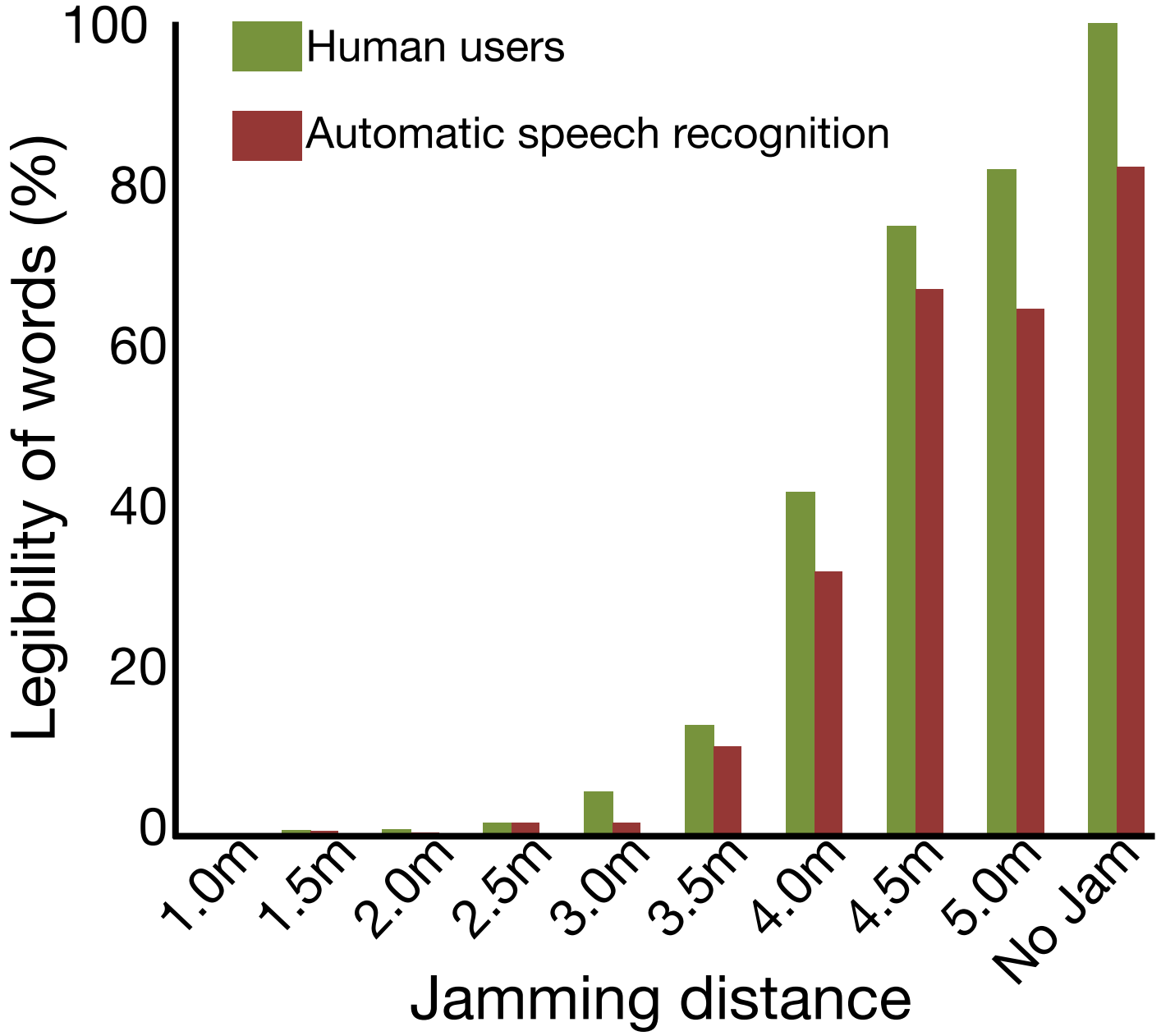
Jamming performance



Jamming performance



Jamming performance



What did we cover today?

IoT Security

Cyber-Physical Security and Acoustic Attacks

1- Hacking different IoT sensors:

- microphones in smart home devices
- accelerometers in fitbit
- localization in drones
- control a pace maker

2- How can you send inaudible voice commands to a microphone?

TODO:

1- Project Proposals due April 1st

2- Lab 3 due today

3- PSet 2 due April 10