



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

<https://6mobile.github.io/>

Lecture 11: Attacks on Acoustic Sensing

Fadel Adib

6mobile@mit.edu

Some slides adapted from Nirupam Roy (UMD College Park)

Announcements

- 1- Project Proposal instructions out. Due March 3
- 2- PSet 2 out. Due April 9
- 3- Lab 3 due today.

Project Timeline

March 31

Project
Proposal

April 15

Final
Components

May 5

Abstracts
Due

April 7-9

Project
Meetings

April 21 - May 7

Project
Meetings

May 12

Presentations
+ Demos

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, \$

What are we learning today?

IoT Security

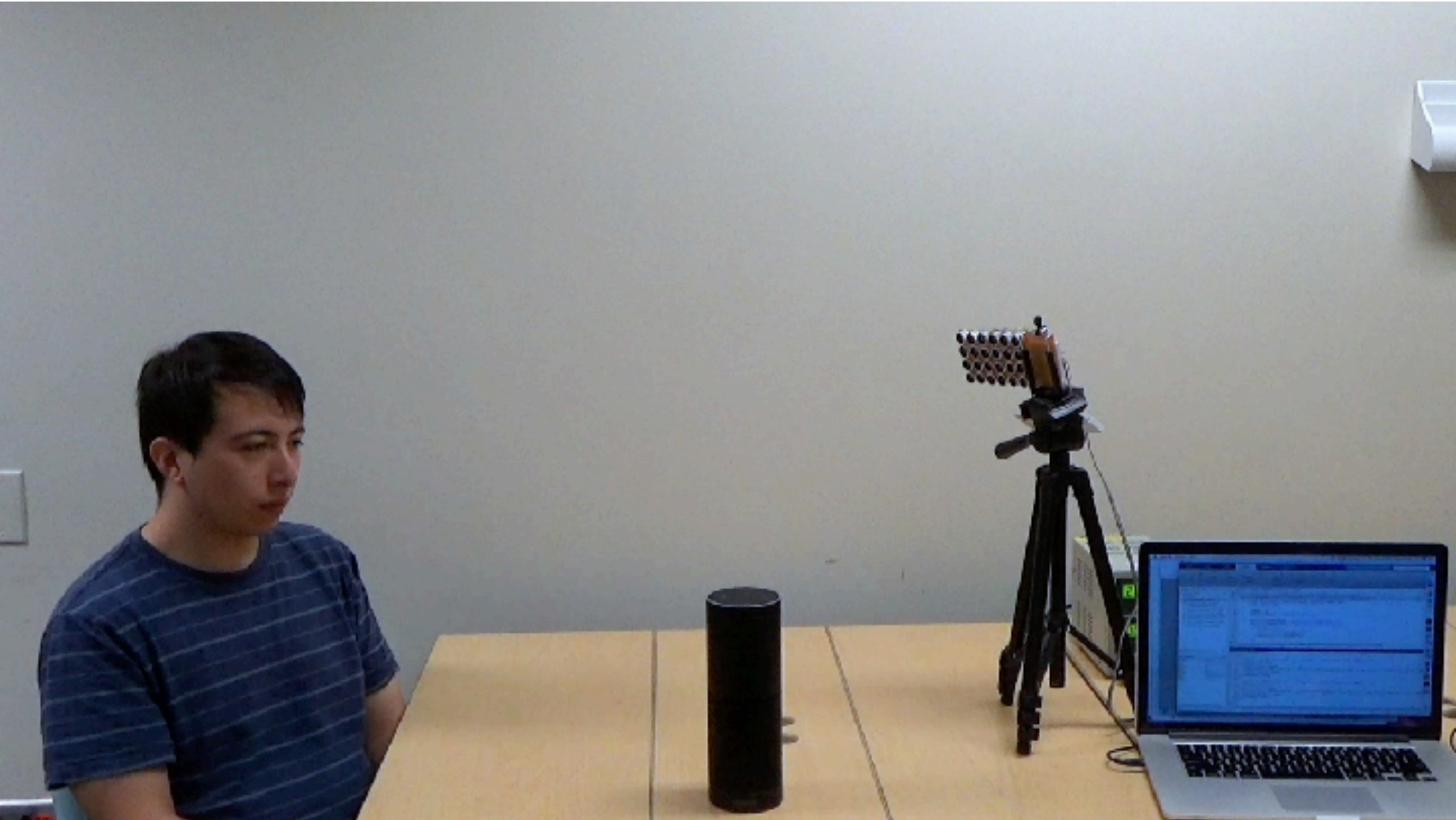
Cyber-Physical Security and Acoustic Attacks

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





Light Commands
Hacking using Laser



CSE COMPUTER SCIENCE
AND ENGINEERING
UNIVERSITY OF MICHIGAN

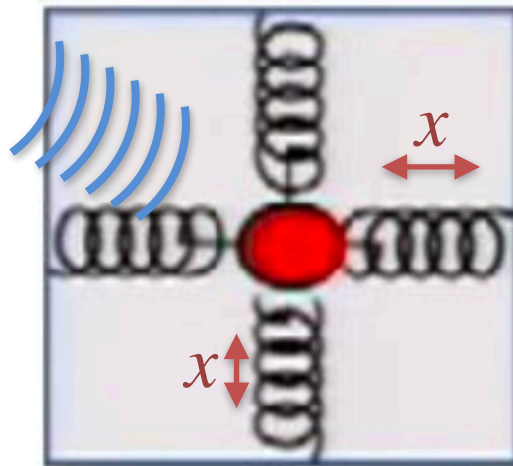


LIGHT COMMANDS

Analog Sensor Security
Acoustic Attacks on MEMS
Accelerometers



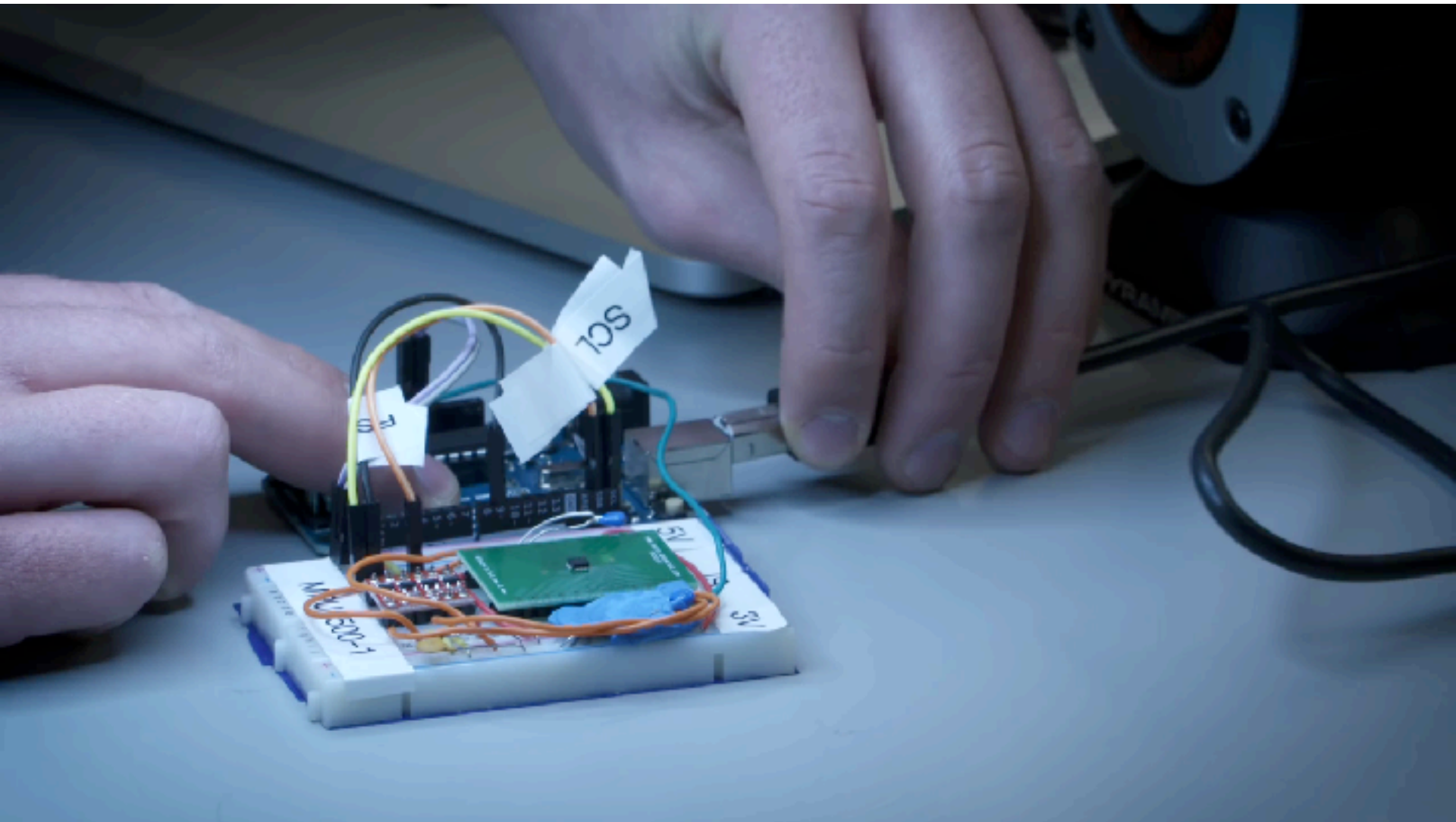
Acoustic
“pressure” waves



$$F = ma = kx$$

acceleration

measure
displacement

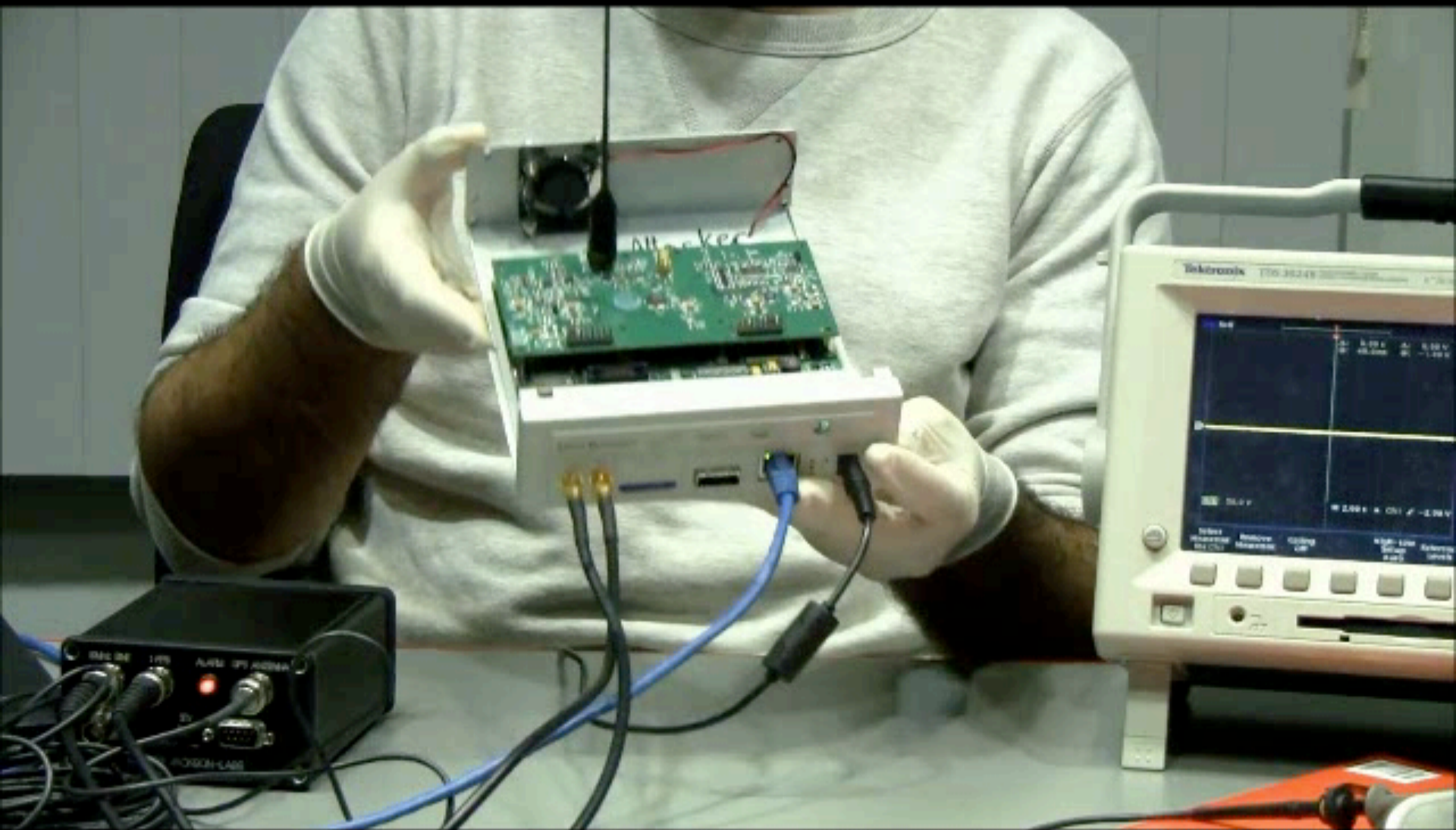


Drone Security
Spoofing GPS Signals



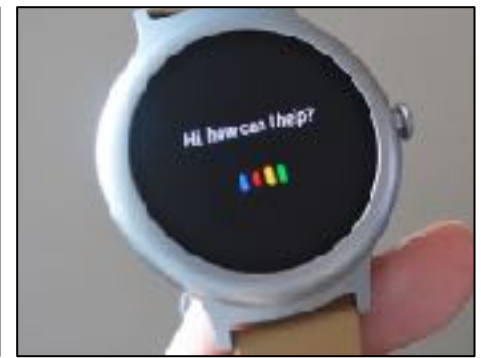
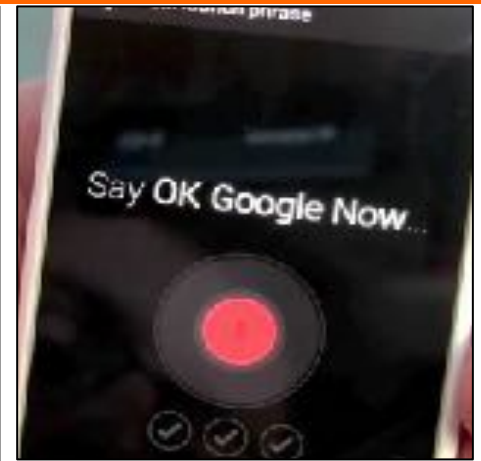
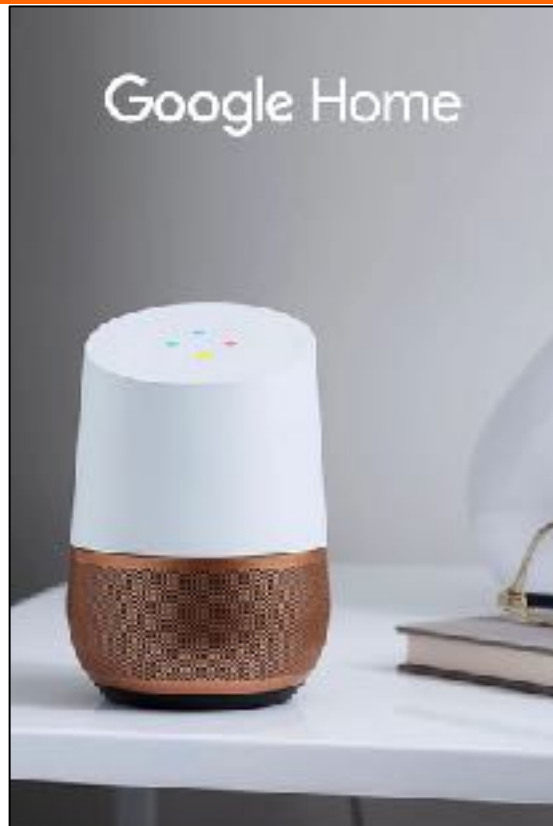
Pacemaker Security

Wireless Control of Pacemaker

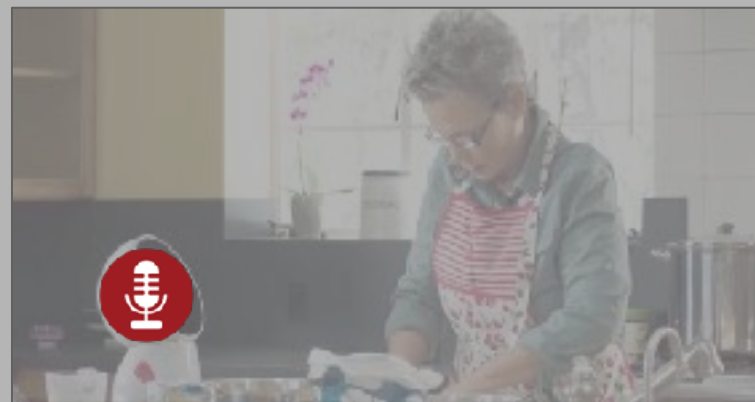
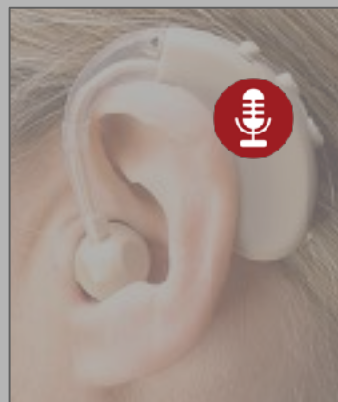
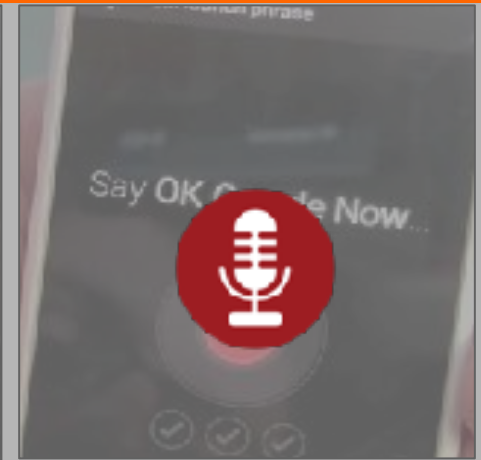
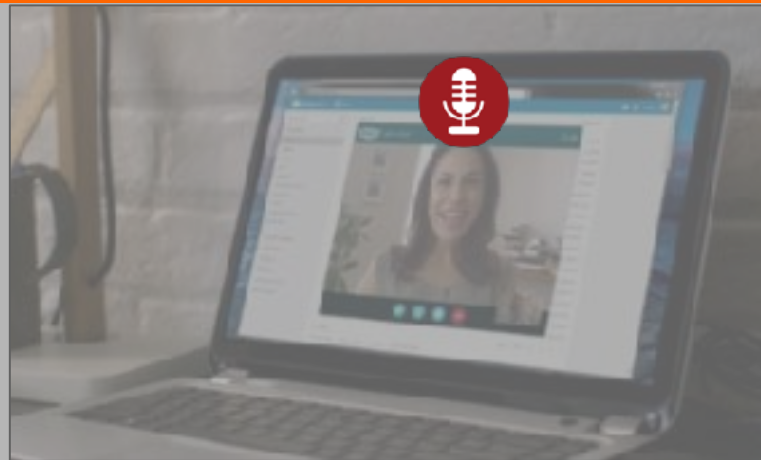


BackDoor: Making Microphones Hear Inaudible Sounds

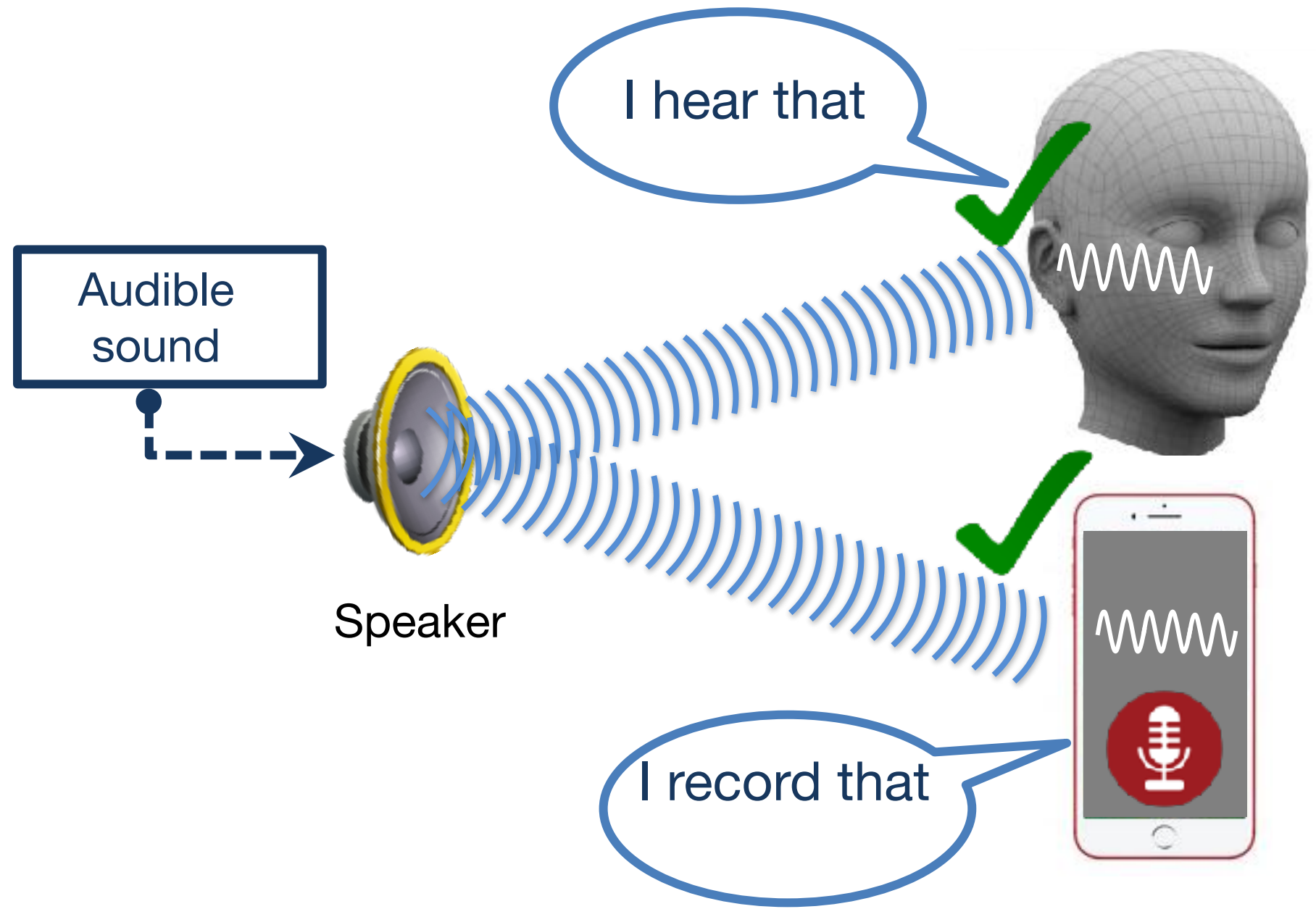
Microphones are everywhere



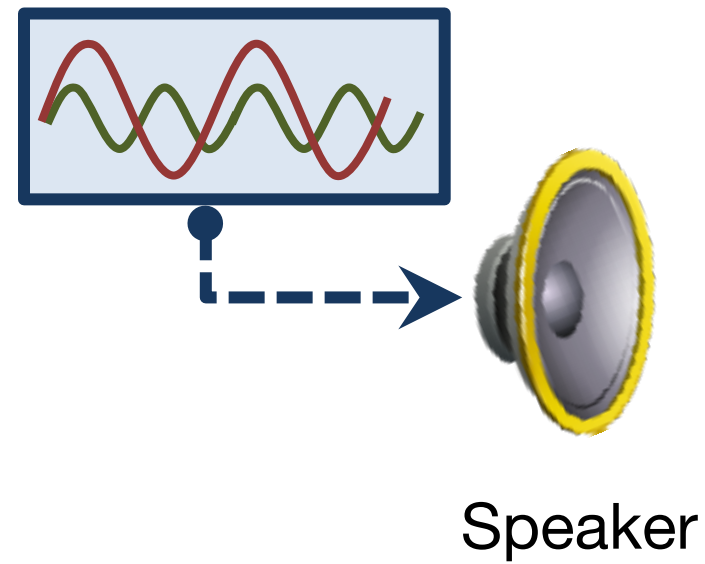
Microphones are everywhere



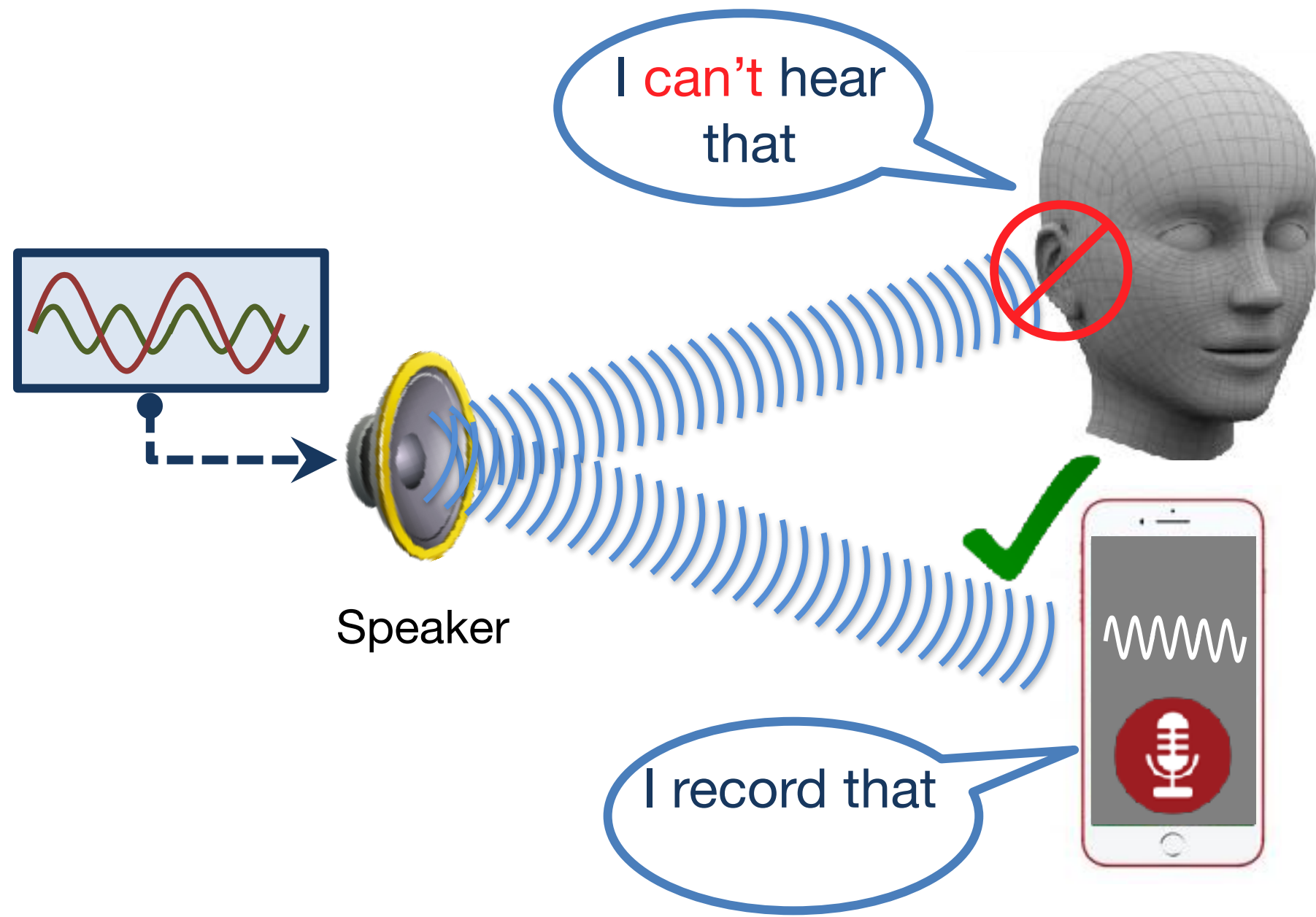
Microphones record audible sounds



Inaudible, but recordable !



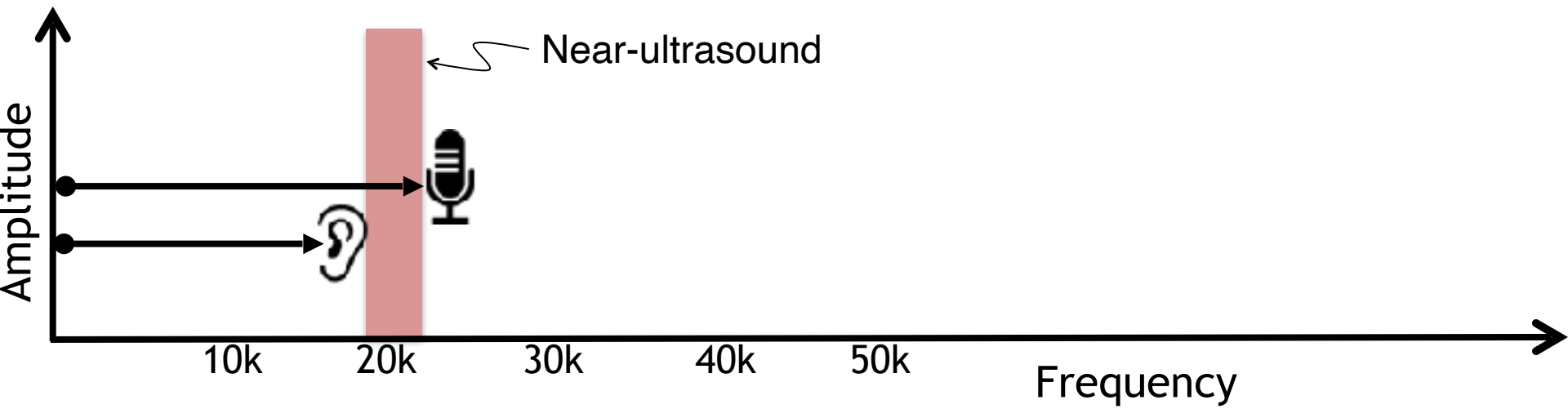
Inaudible, but recordable !



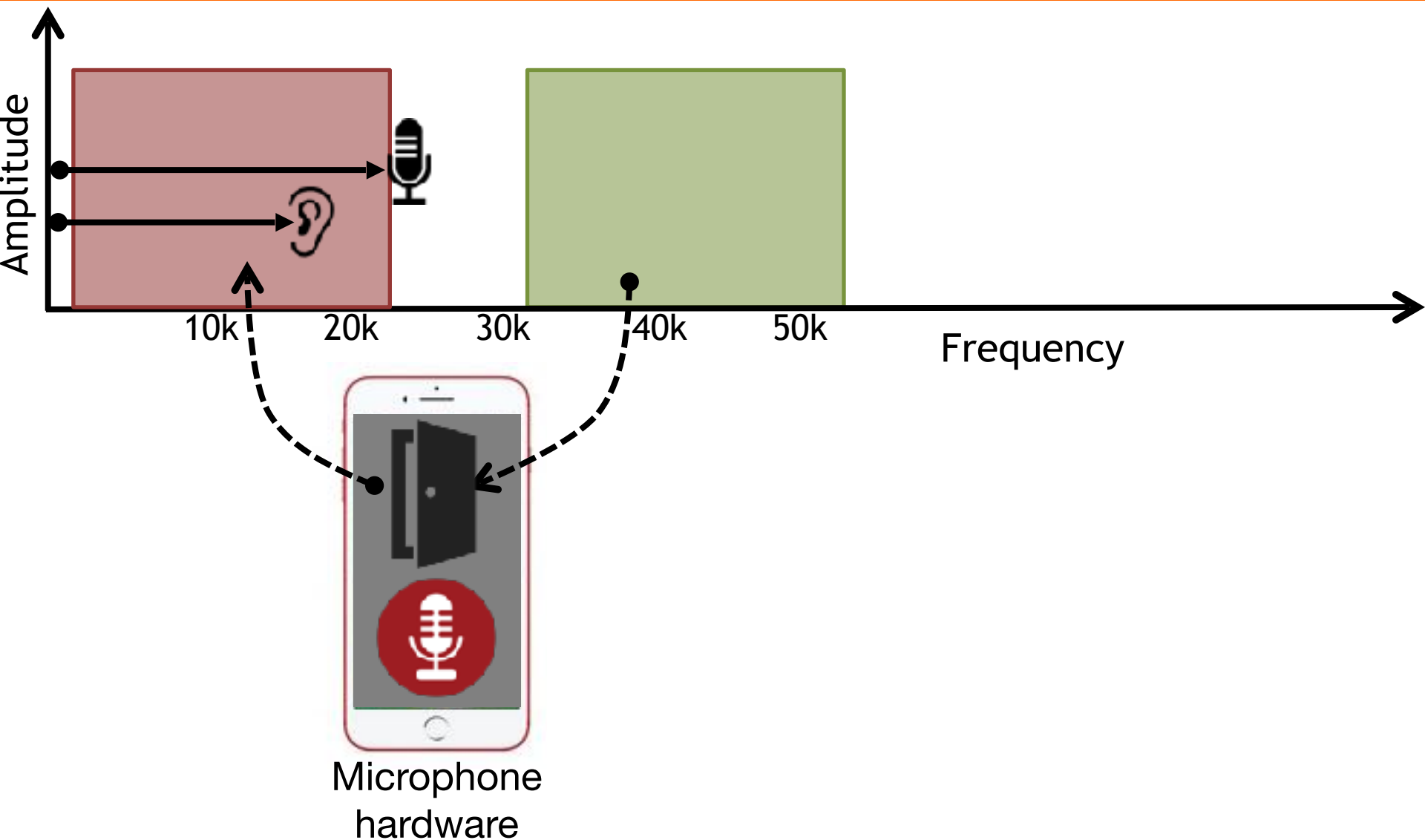
Works with unmodified devices



It's not "near-ultrasound"



Exploiting fundamental nonlinearity

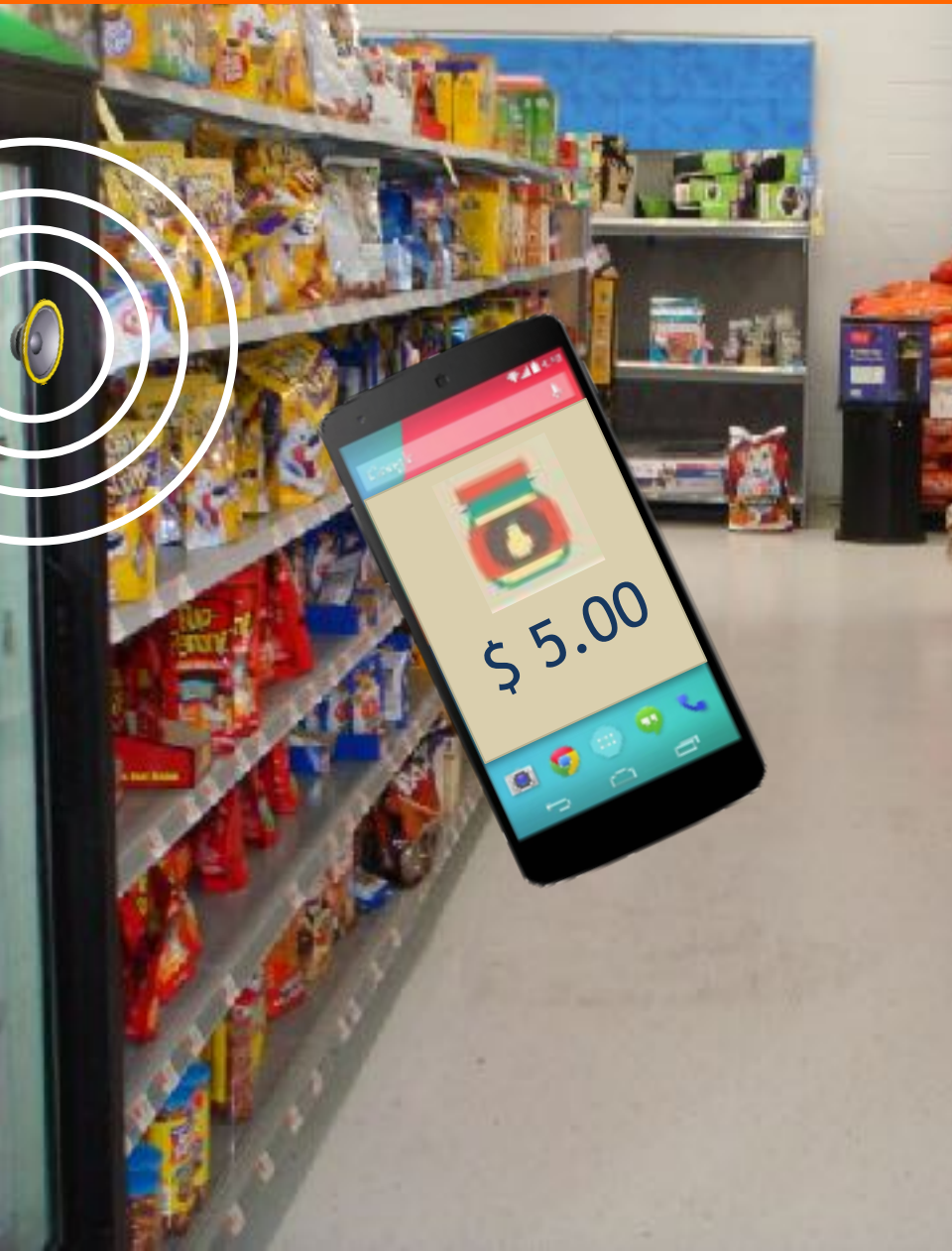


What can we do with it?

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

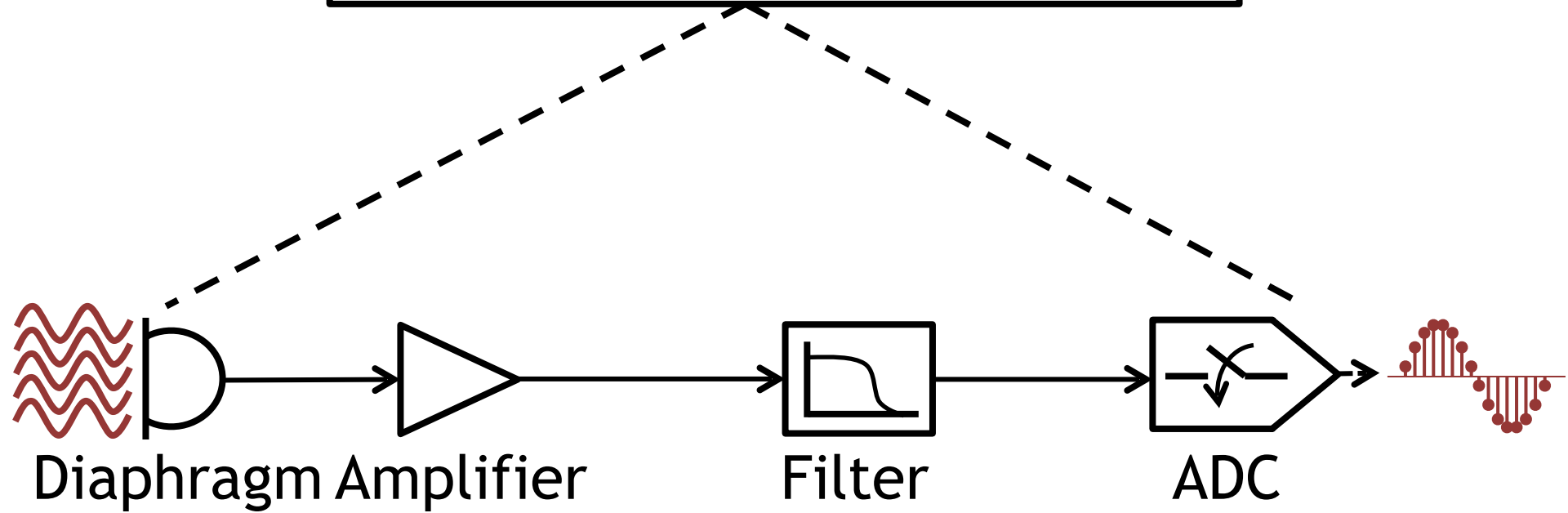
① Microphone Overview

② System Design

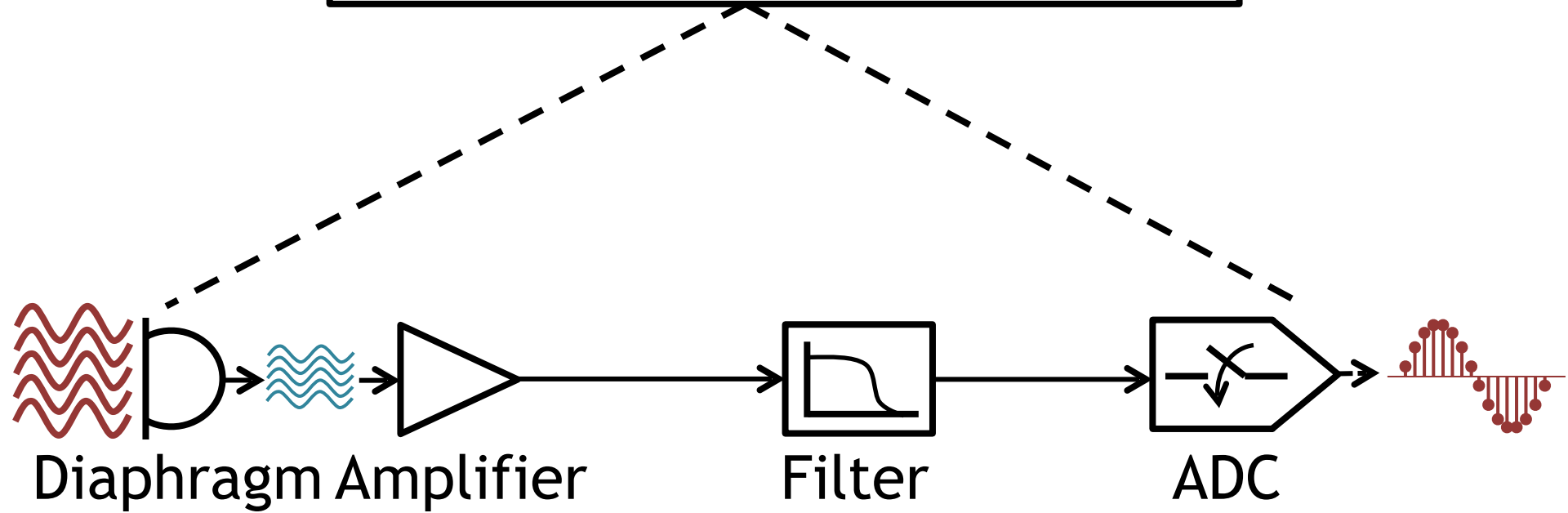
③ Challenges

④ Evaluation

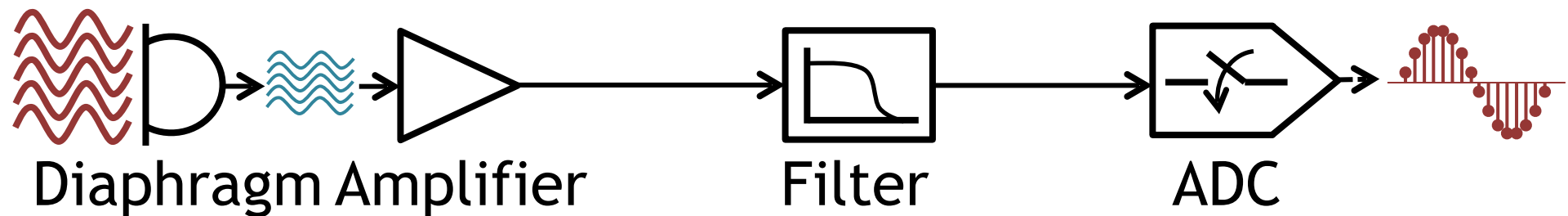
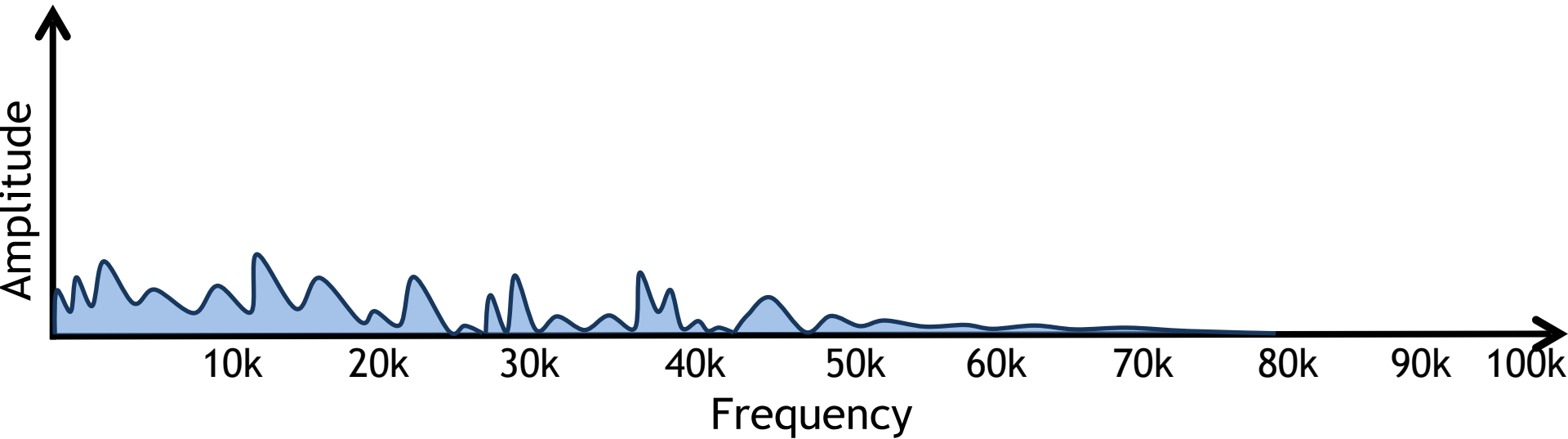
Microphone working principle



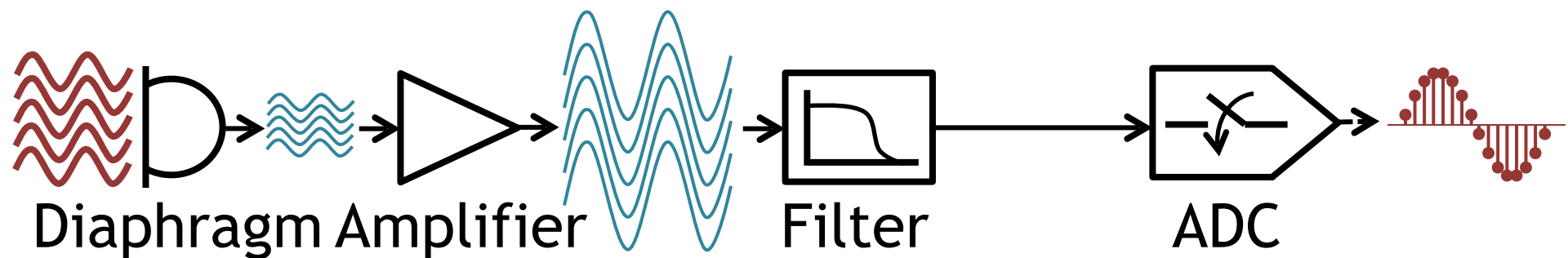
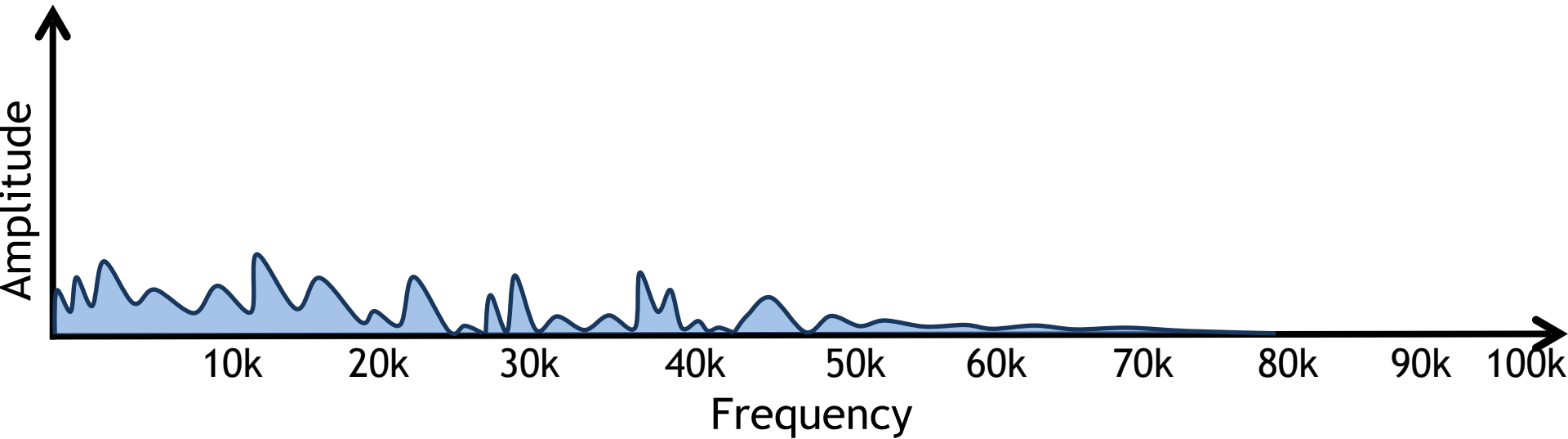
Microphone working principle



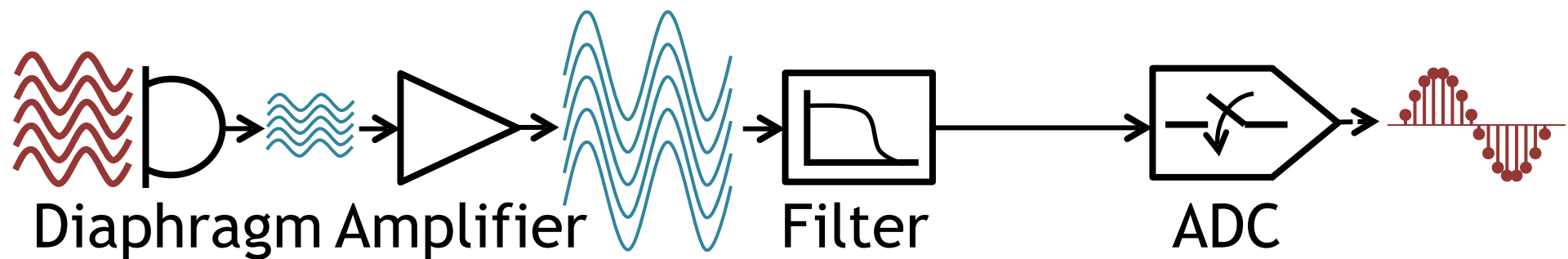
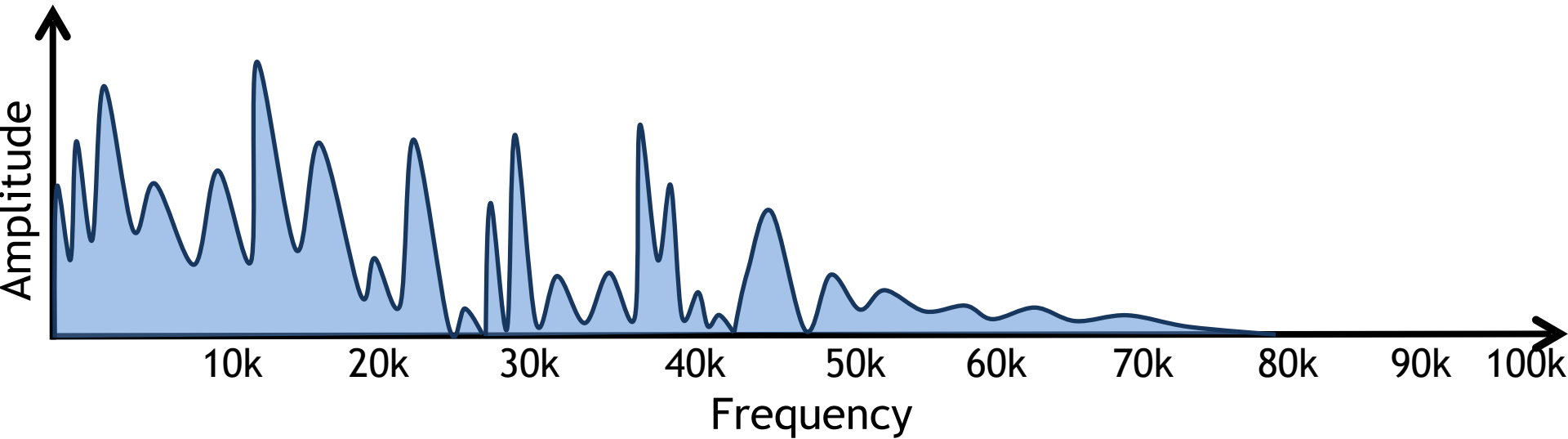
Microphone working principle



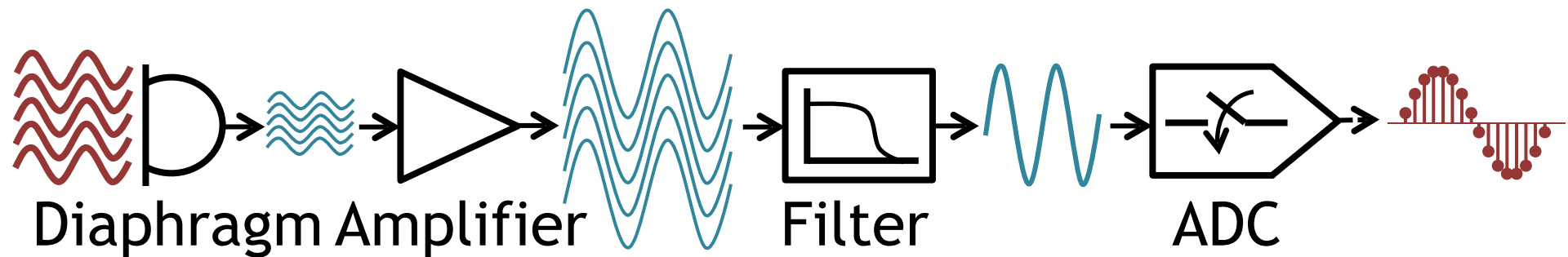
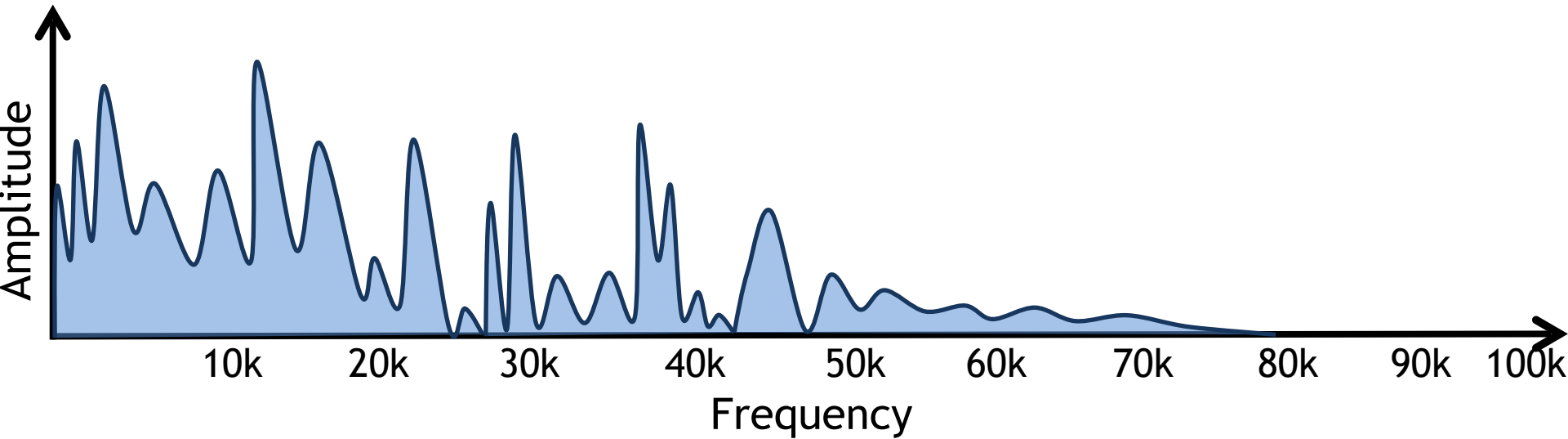
Microphone working principle



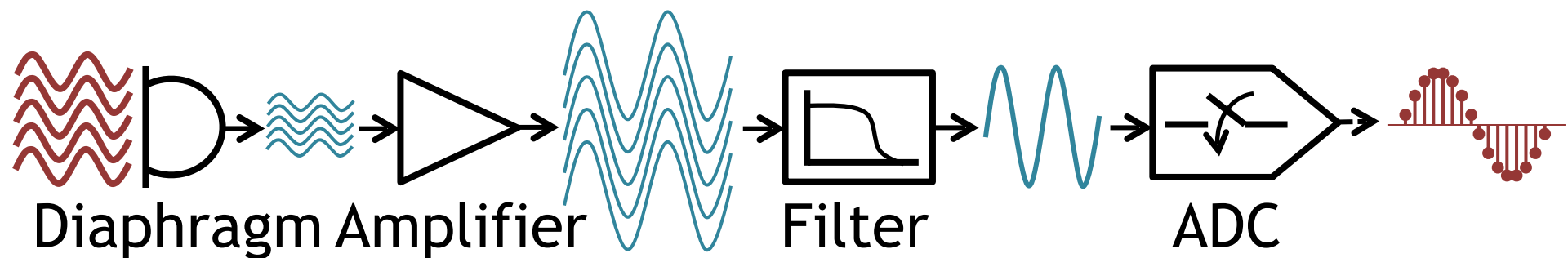
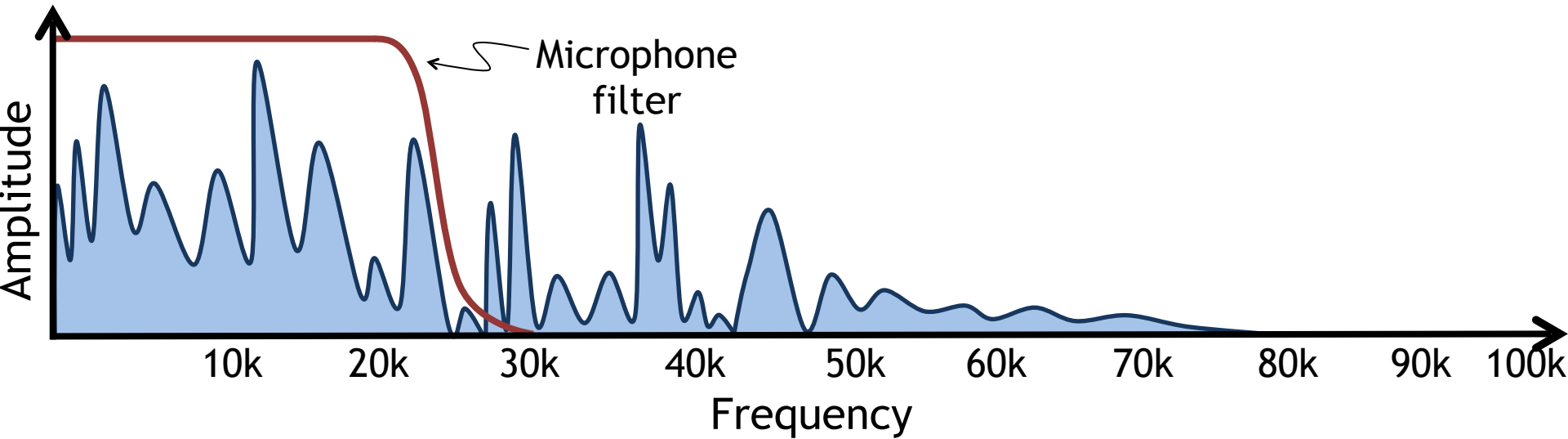
Microphone working principle



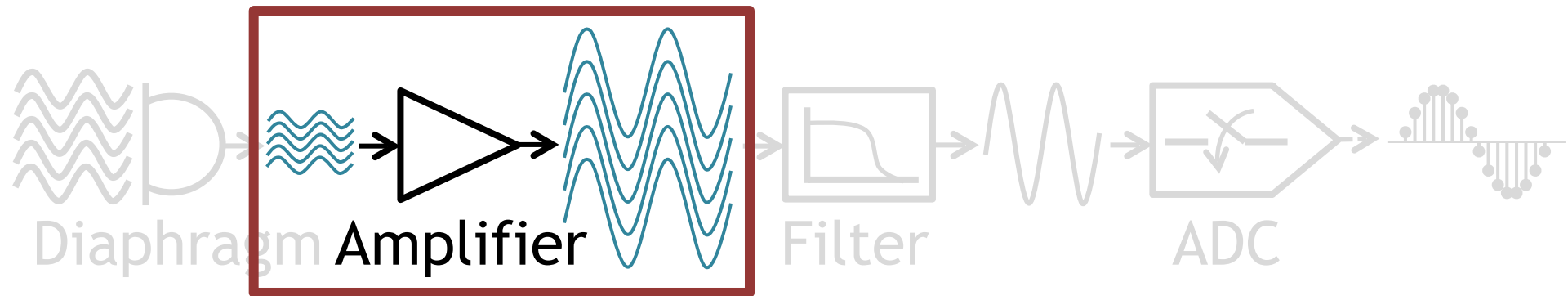
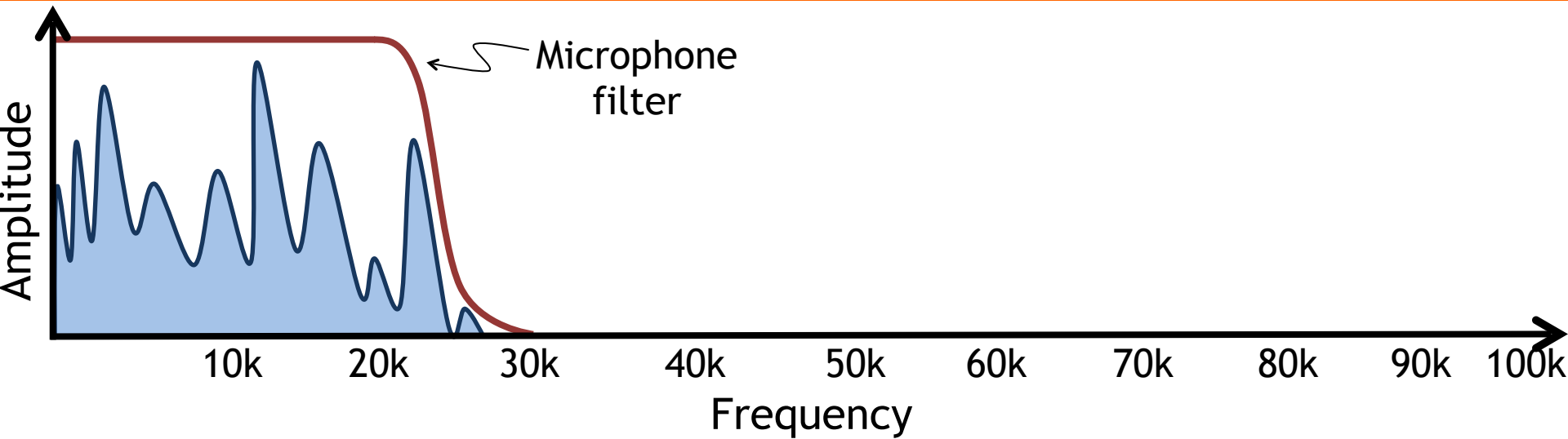
Microphone working principle



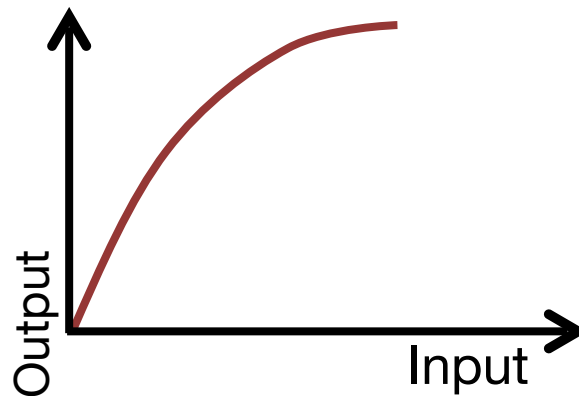
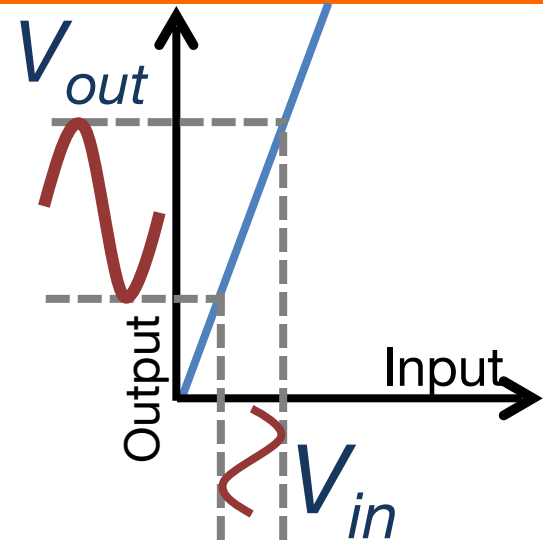
Microphone working principle



Microphone working principle



Microphone working principle



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

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

10k

20k

30k

40k

50k

60k

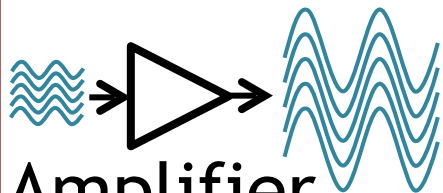
70k

80k

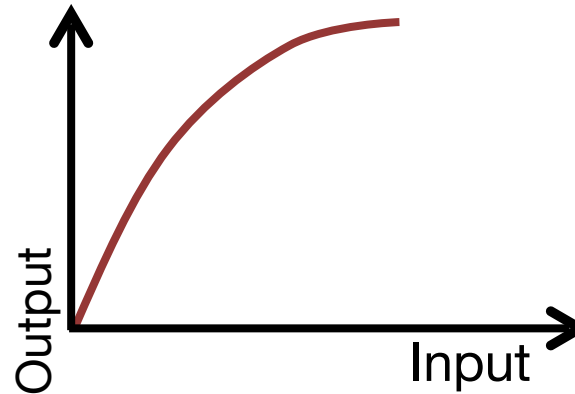
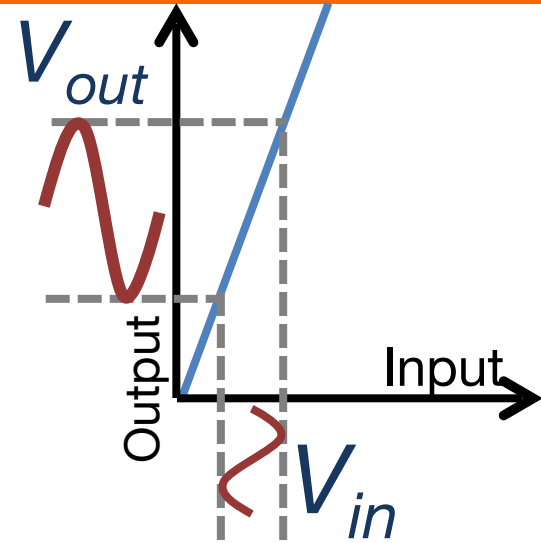
90k

100k

Frequency

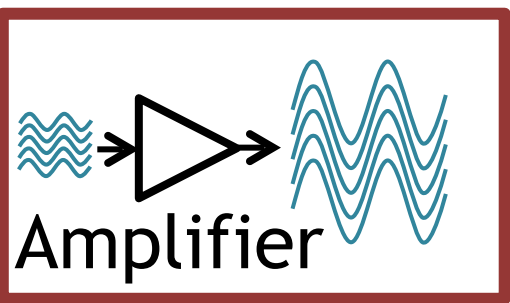
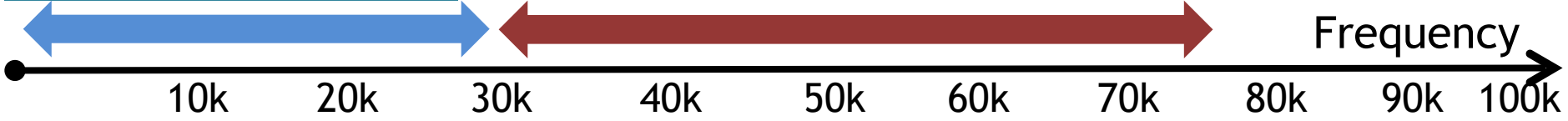


Microphone working principle

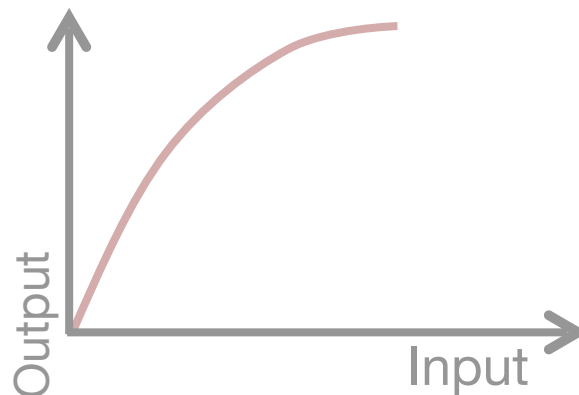
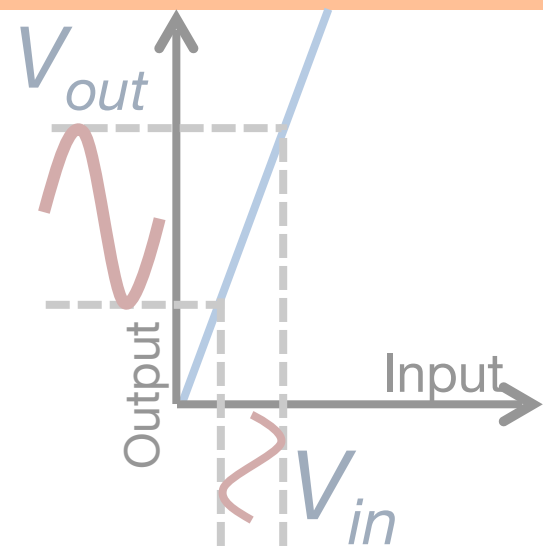


$$V_{out} = a_1 V_{in}$$

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



Microphone working principle



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

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

Frequency

10k

20k

30k

40k

50k

60k

70k

80k

90k

100k



Talk outline

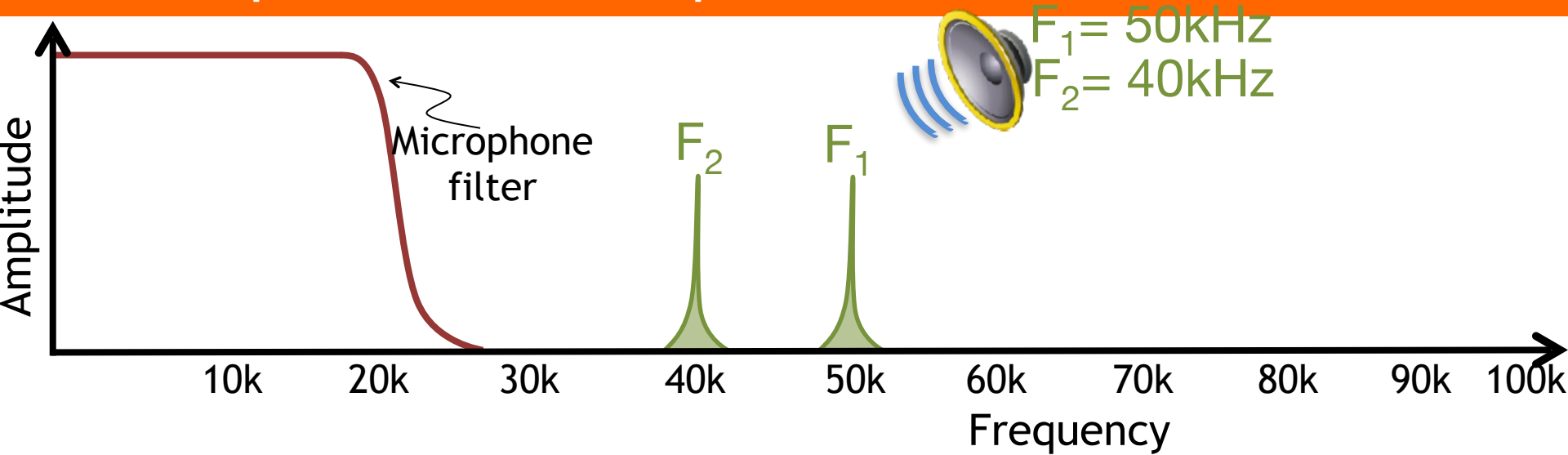
① Microphone Overview

② System Design

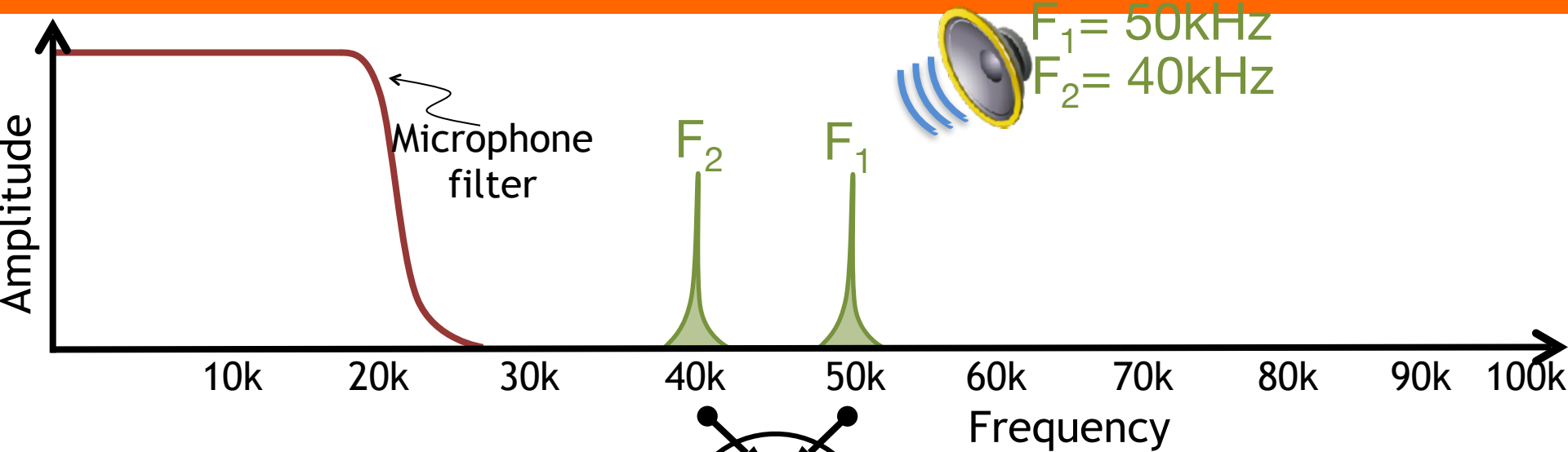
③ Challenges

④ Evaluation

Exploiting amplifier non-linearity



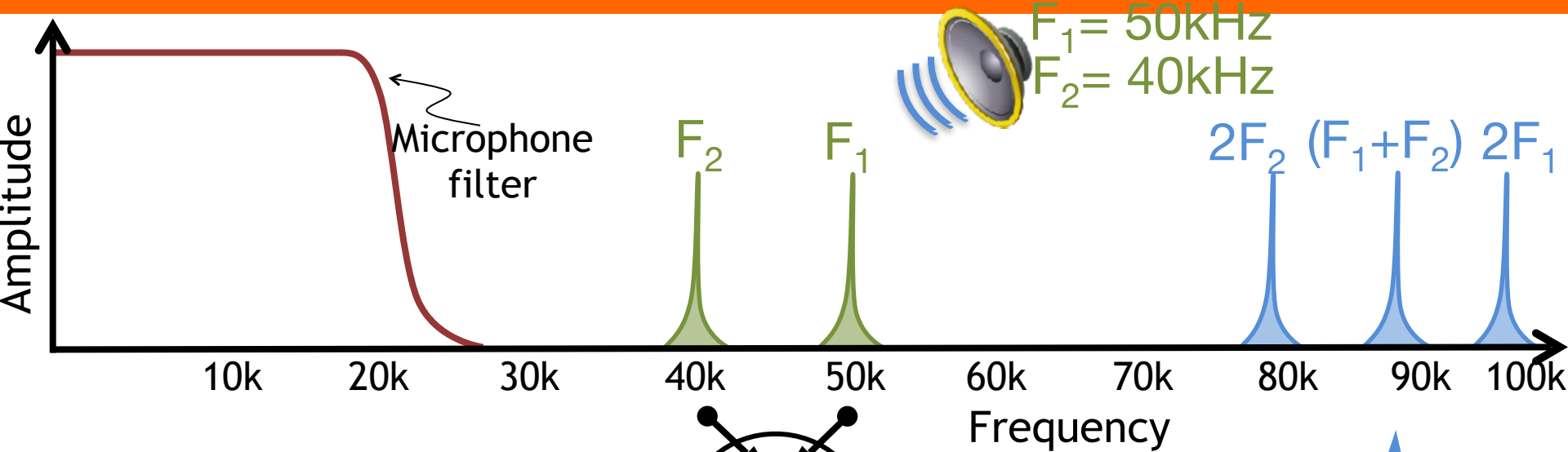
Exploiting amplifier non-linearity



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

$$\begin{aligned} (\sin F_1 + \sin F_2)^2 = & \cos 2F_1 \\ & + \cos 2F_2 \\ & + \cos (F_1 + F_2) \\ & + \cos (F_1 - F_2) \end{aligned}$$

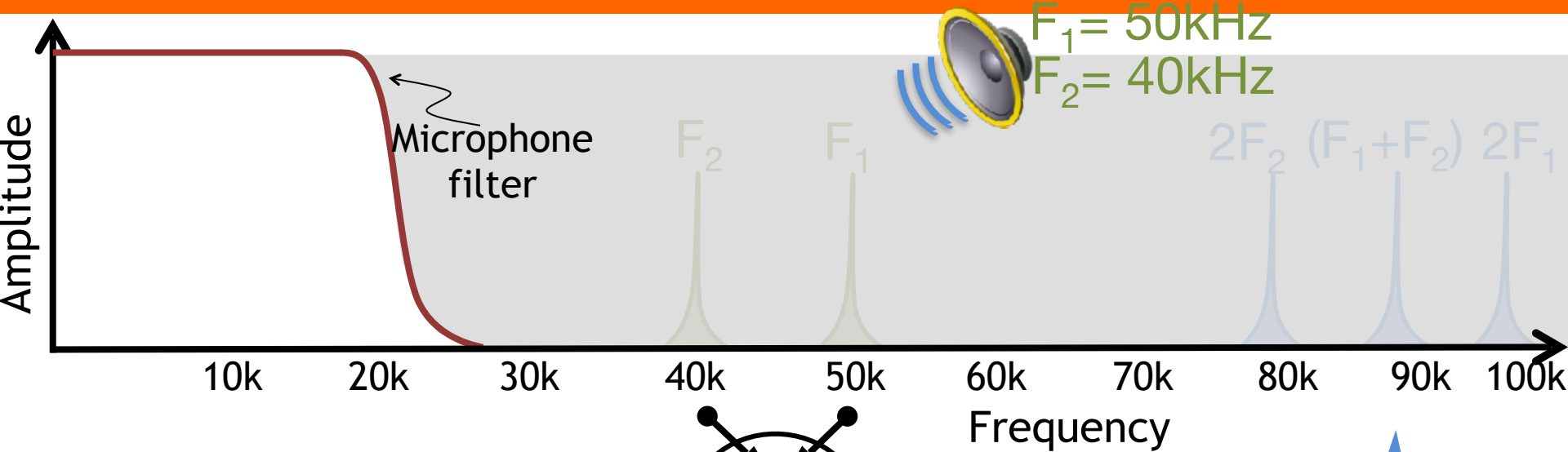
Exploiting amplifier non-linearity



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

$$\begin{aligned} (\sin F_1 + \sin F_2)^2 = & \cos 2F_1 \\ & + \cos 2F_2 \\ & + \cos (F_1 + F_2) \\ & + \cos (F_1 - F_2) \end{aligned}$$

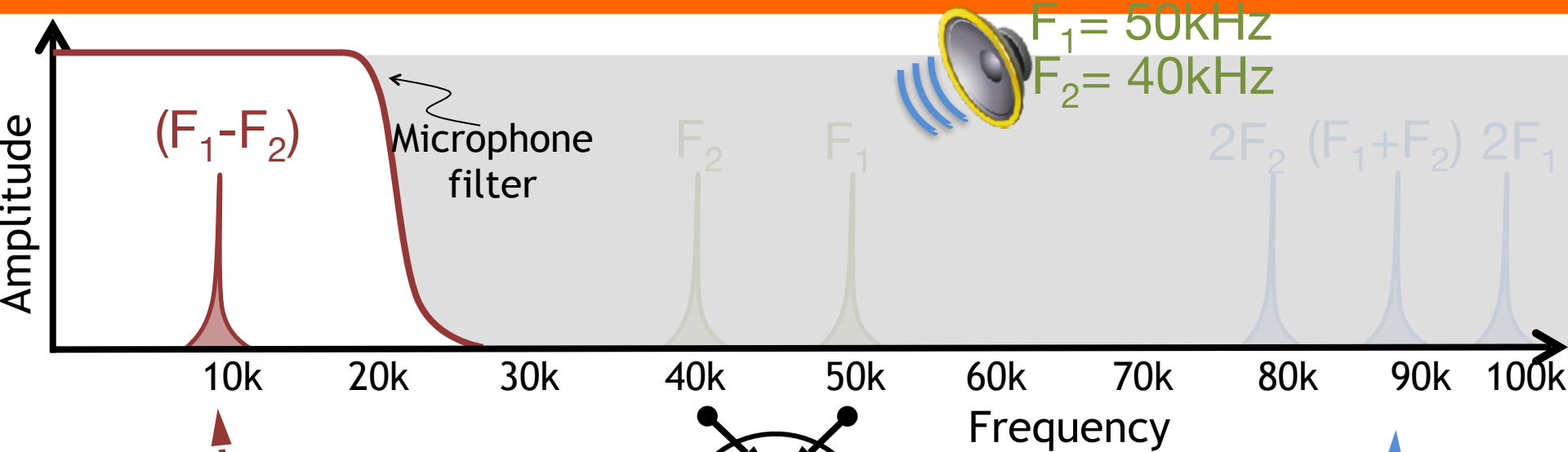
Exploiting amplifier non-linearity



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

$$\begin{aligned} (\sin F_1 + \sin F_2)^2 = & \cos 2F_1 \\ & + \cos 2F_2 \\ & + \cos (F_1 + F_2) \\ & + \cos (F_1 - F_2) \end{aligned}$$

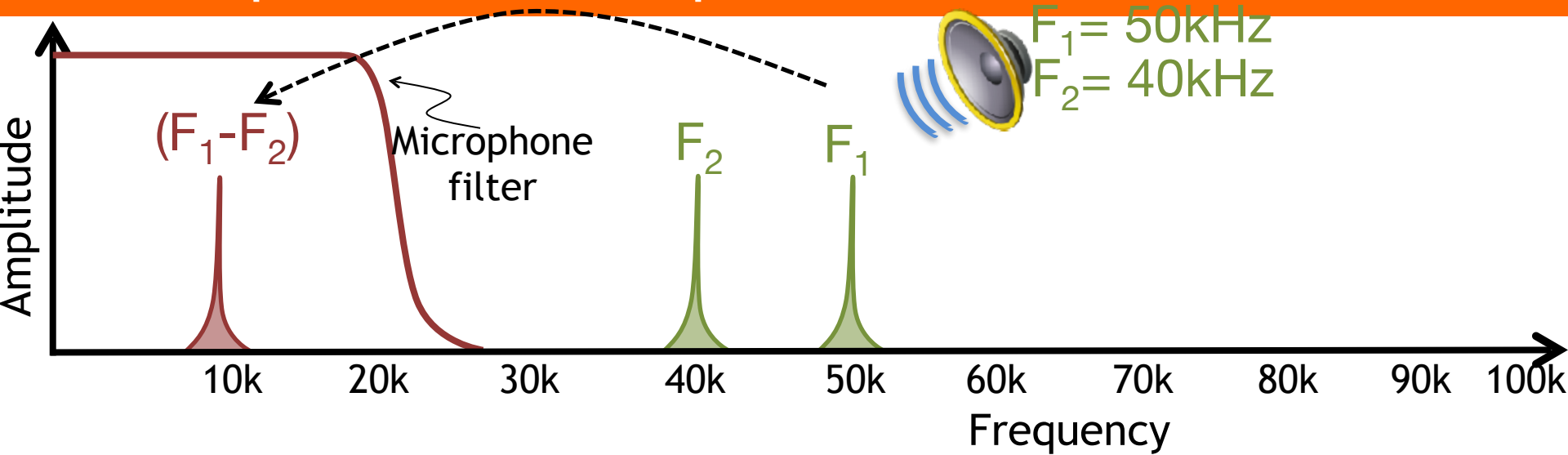
Exploiting amplifier non-linearity



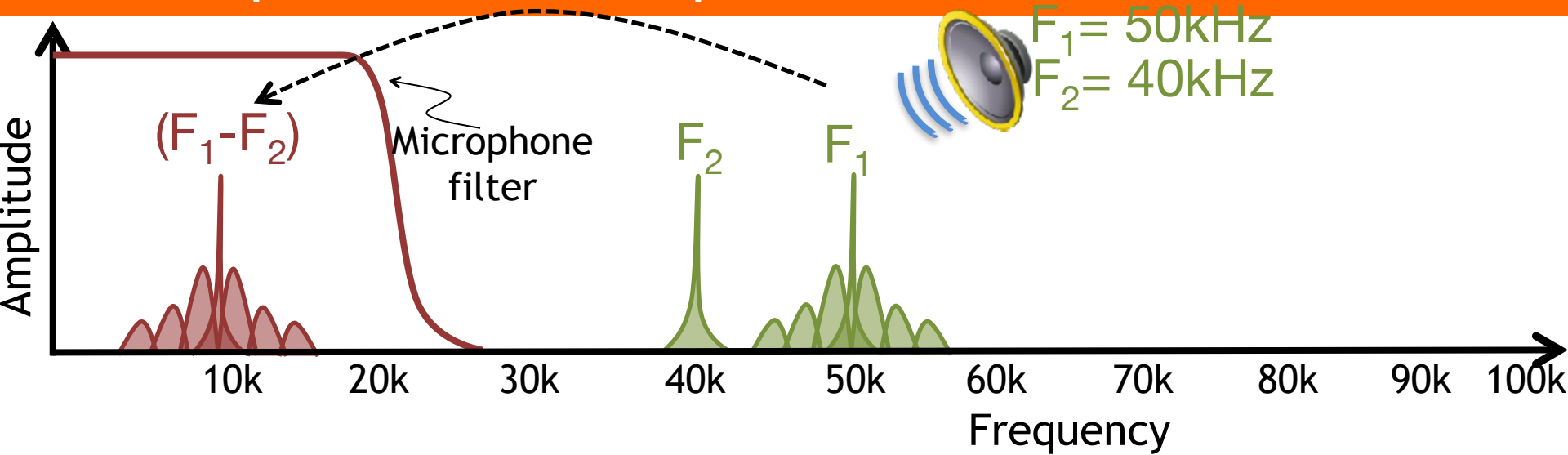
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$\begin{aligned} (\sin F_1 + \sin F_2)^2 = & \cos 2F_1 \\ & + \cos 2F_2 \\ & + \cos (F_1 + F_2) \\ & + \cos (F_1 - F_2) \end{aligned}$$

Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Talk outline

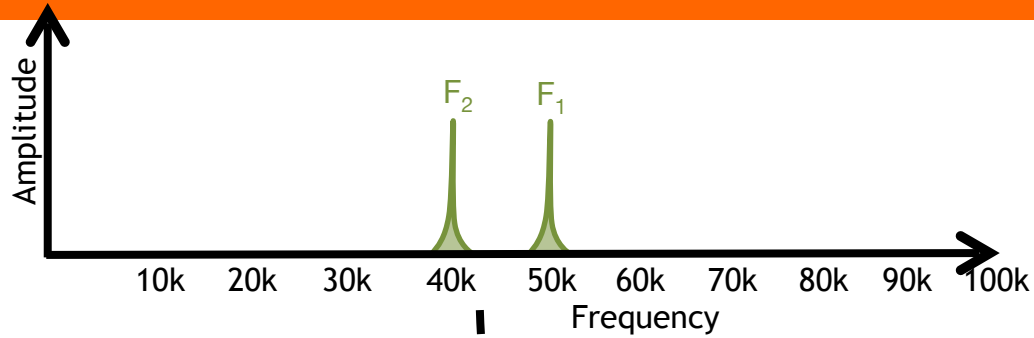
① Microphone Overview

② System Design

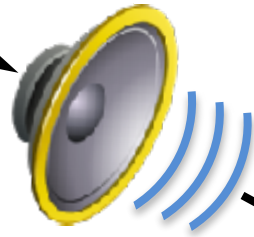
③ Challenges

④ Evaluation

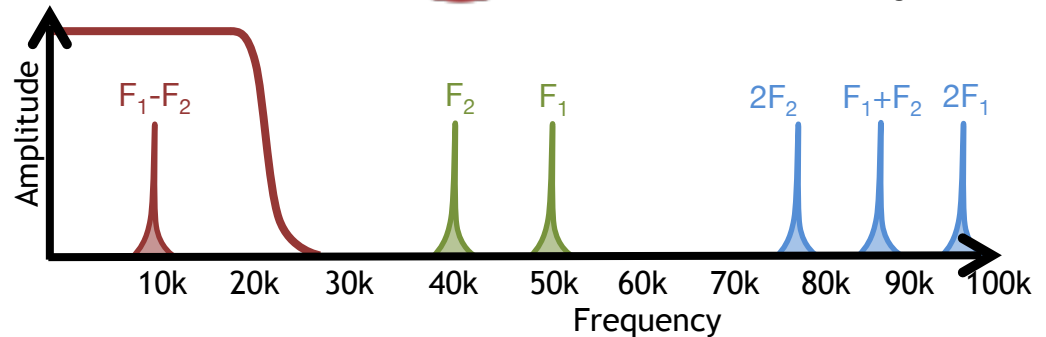
Challenges



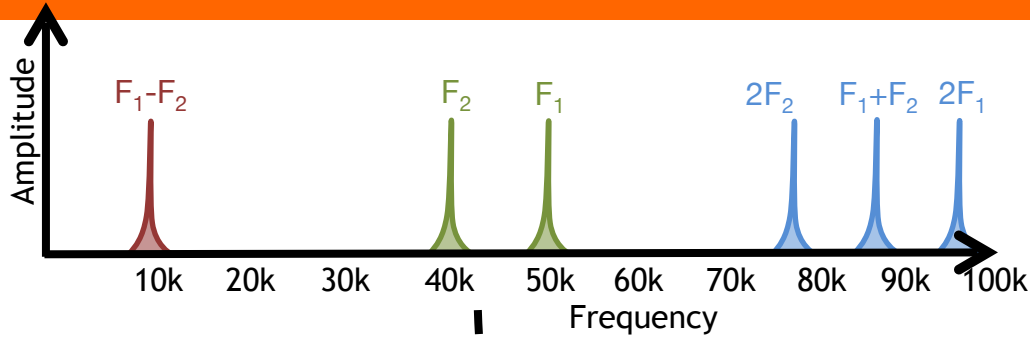
Speaker's nonlinearity



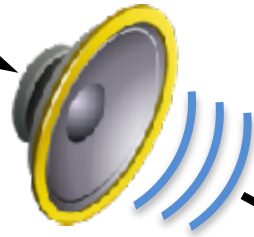
Microphone's nonlinearity



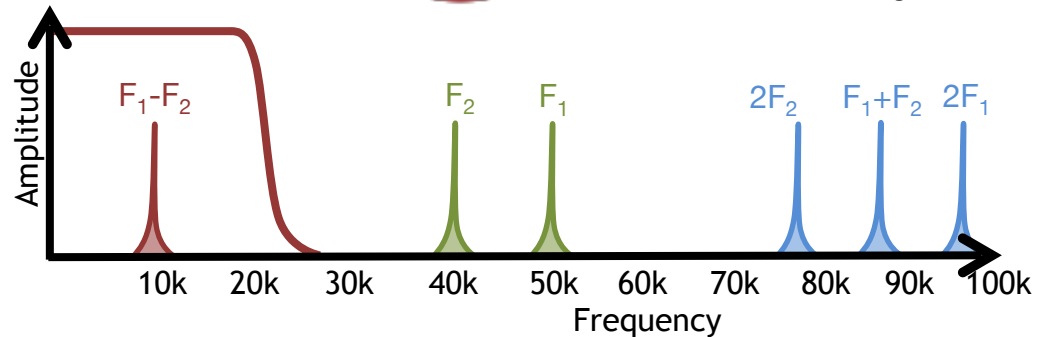
Challenges



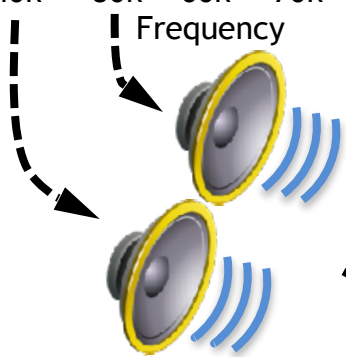
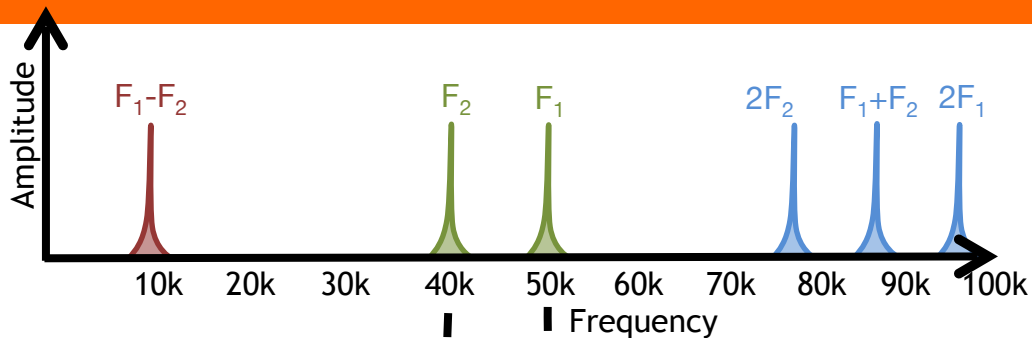
Speaker's
nonlinearity



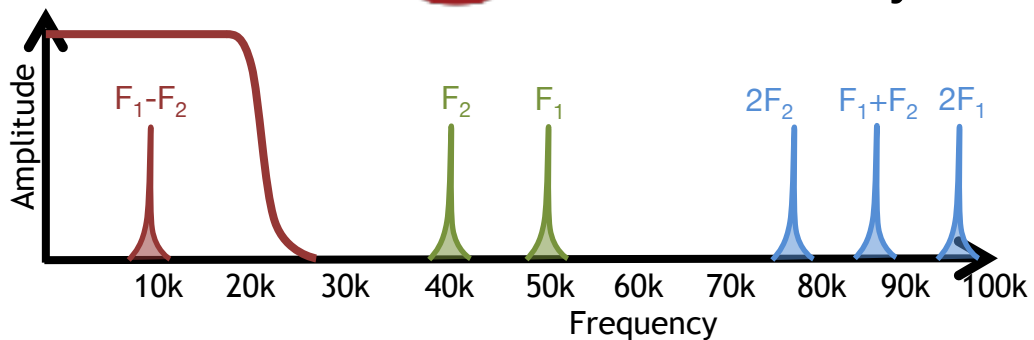
Microphone's
nonlinearity



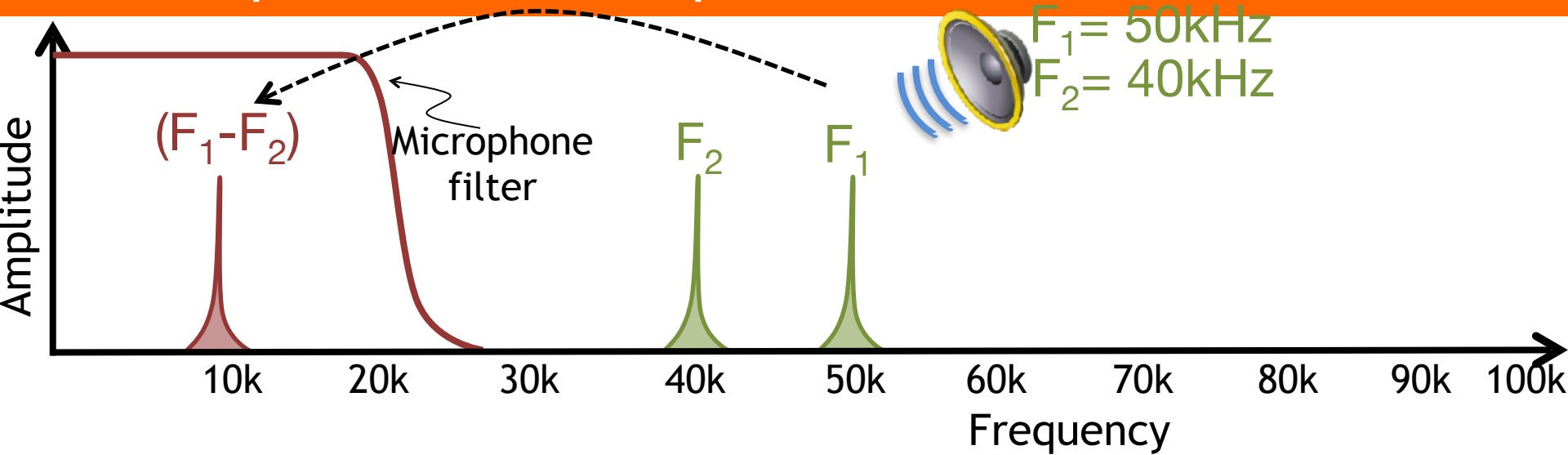
Challenges



Microphone's
nonlinearity



Exploiting amplifier non-linearity



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

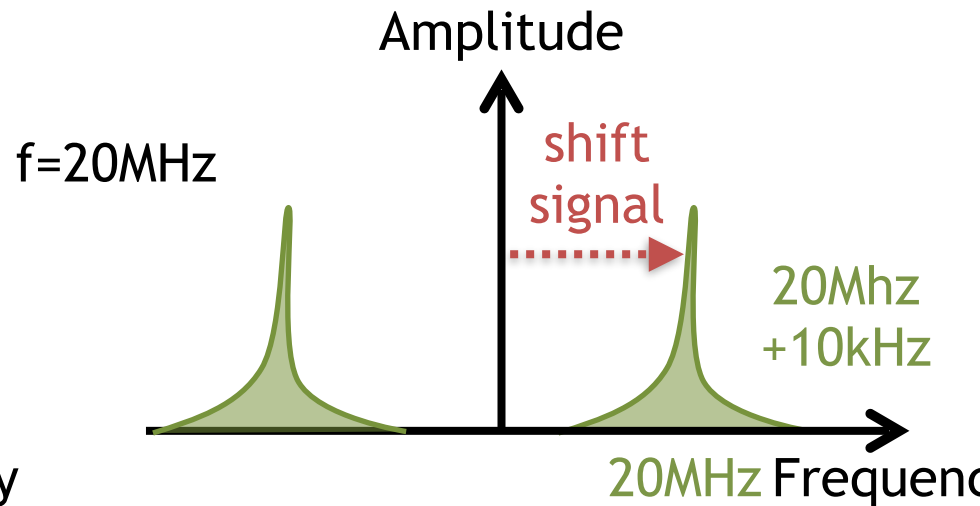
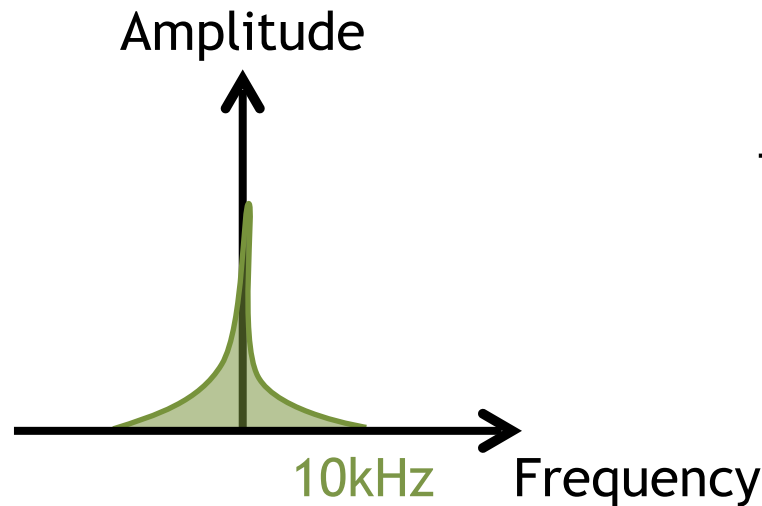
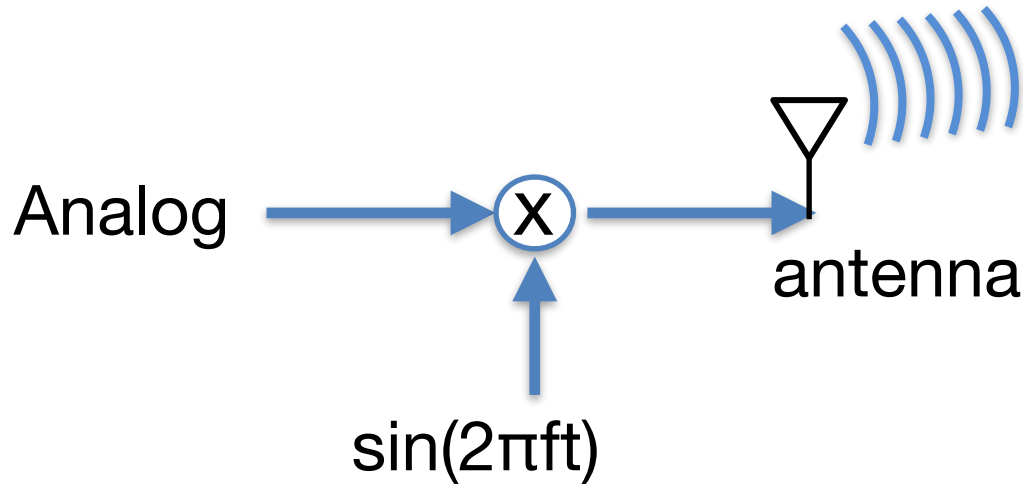
How can we send this command?

Discuss in pairs for 3 min

Primer on Modulation

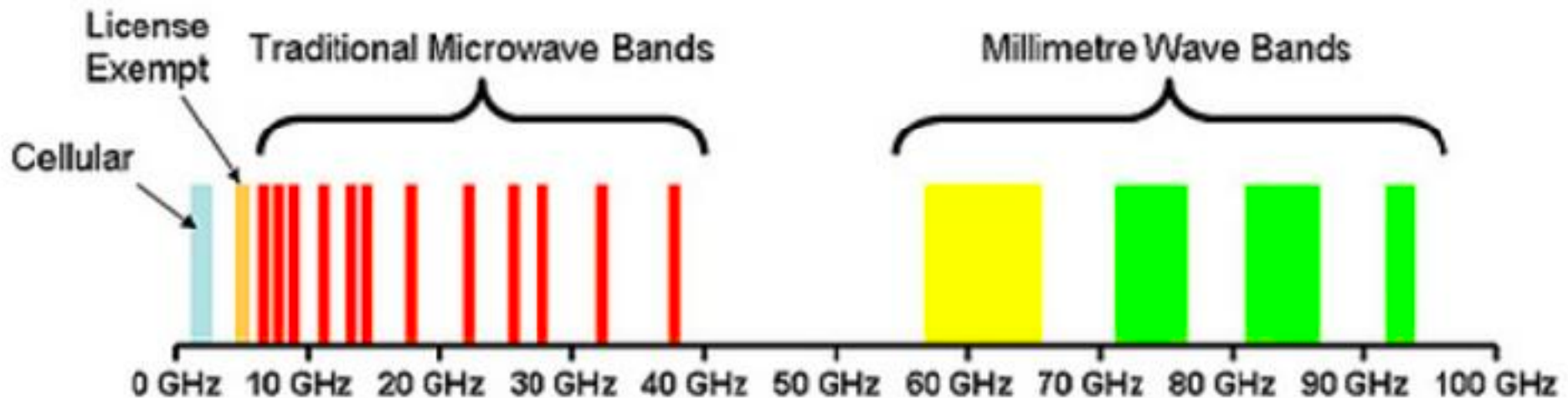
E.g., We send WiFi at 2.4GHz or 5GHz
What does this mean and Why?

Primer on Modulation



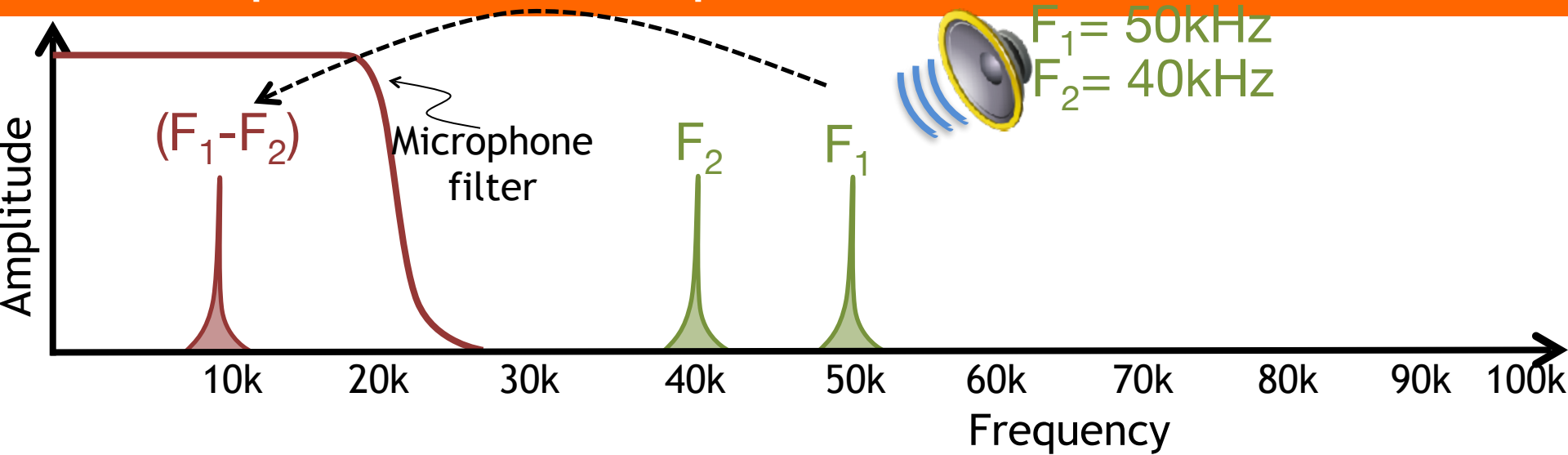
Why is Modulation useful?

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.

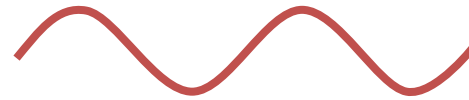
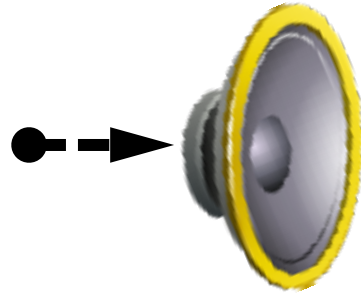
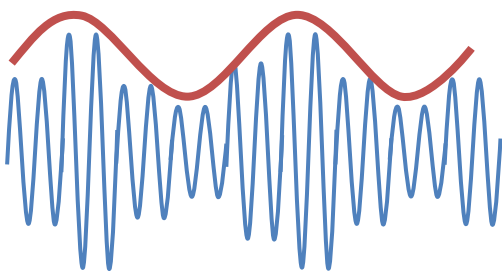
How can we send this command message $m(t)$?

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

Challenges

~~Amplitude modulation~~

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



Ultrasonic speaker

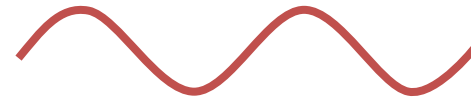
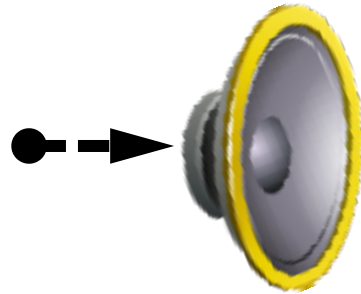
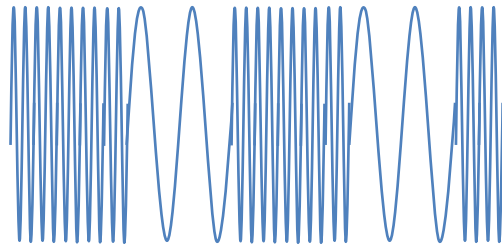
$$\begin{aligned} S_{out,AM}^2 &= A_2 \{ a \sin(\omega_m t) \cdot \sin(\omega_c t) \}^2 \\ &= -A_2 \frac{a^2}{4} \{ \cos(\omega_c t - \omega_m t) - \cos(\omega_c t + \omega_m t) \}^2 \\ &= -A_2 \frac{a^2}{4} \cos(2\omega_m t) + (\text{terms with frequencies} \\ &\quad \text{above } \omega_c \text{ and DC}) \end{aligned}$$

Problem: speaker has non-linearities
=> Audible sound

Challenges

Frequency
modulation

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

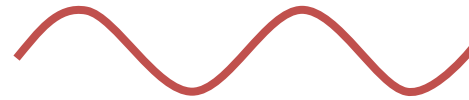
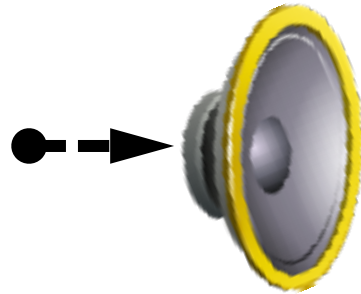
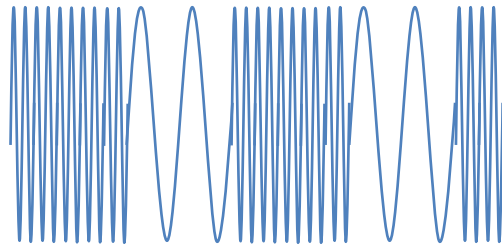


Ultrasonic
speaker

Challenges

Frequency
modulation

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

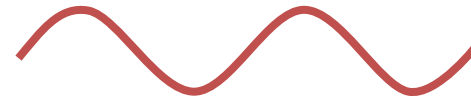
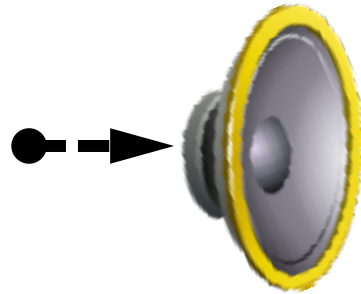
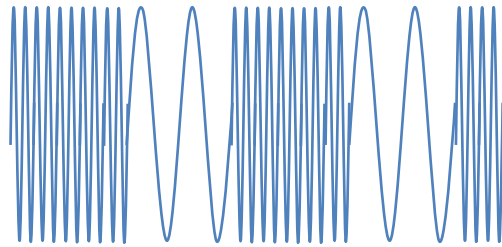


Ultrasonic
speaker

Challenges

Frequency modulation

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



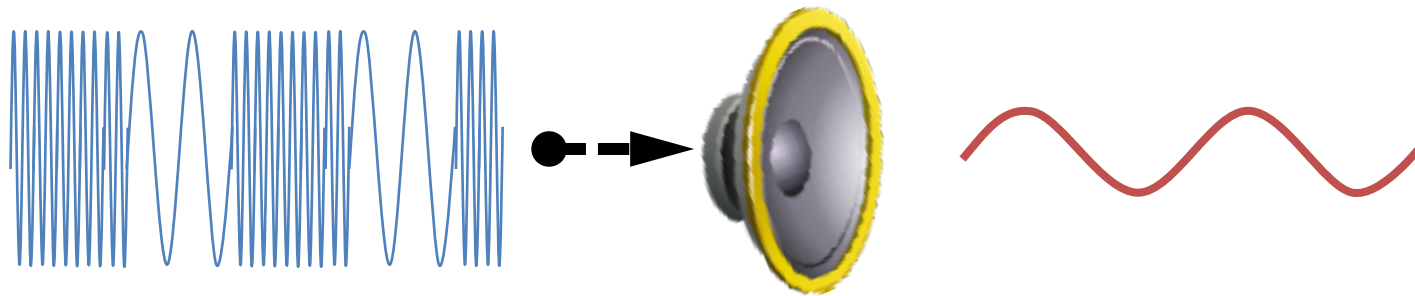
Ultrasonic speaker

$$S_{FM}^2 \sim 1 + \cos(2\omega_c t + \text{other terms})$$

Problem: microphone
can't measure
inaudible sound

Solution?

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



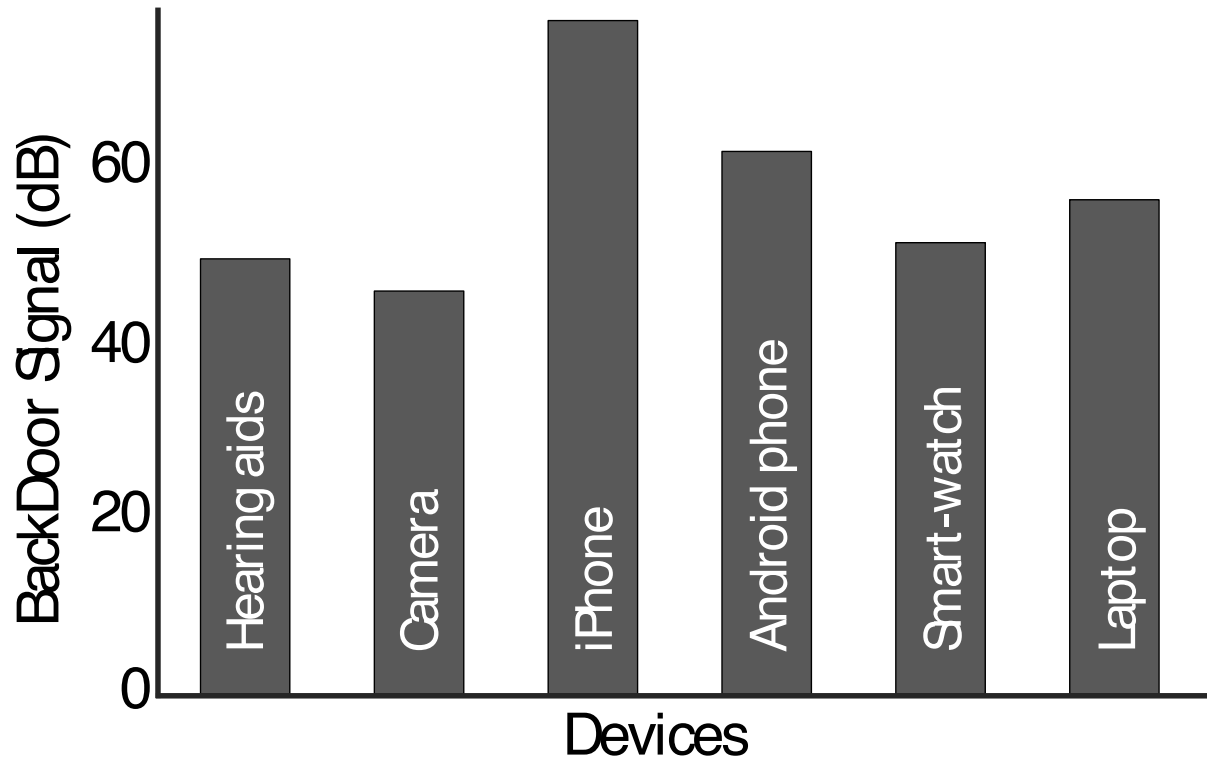
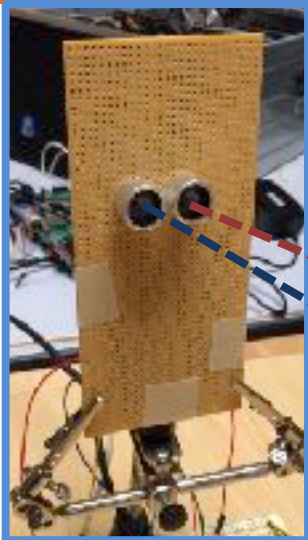
Ultrasonic
speaker

Add another speaker
How do we structure its
signal?

Talk outline

- ① Microphone Overview
- ② System Design
- ③ Challenges
- ④ Evaluation

Hardware generalizability



Hearing Aid



Camera



iPhone



Android phone

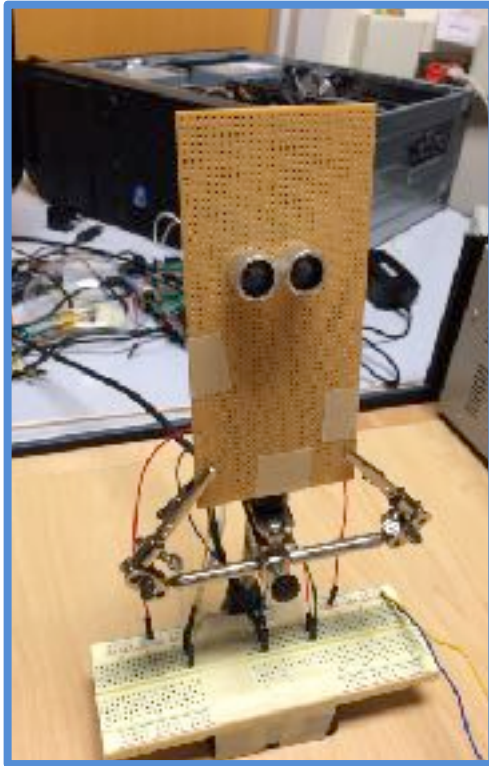


Smartwatch

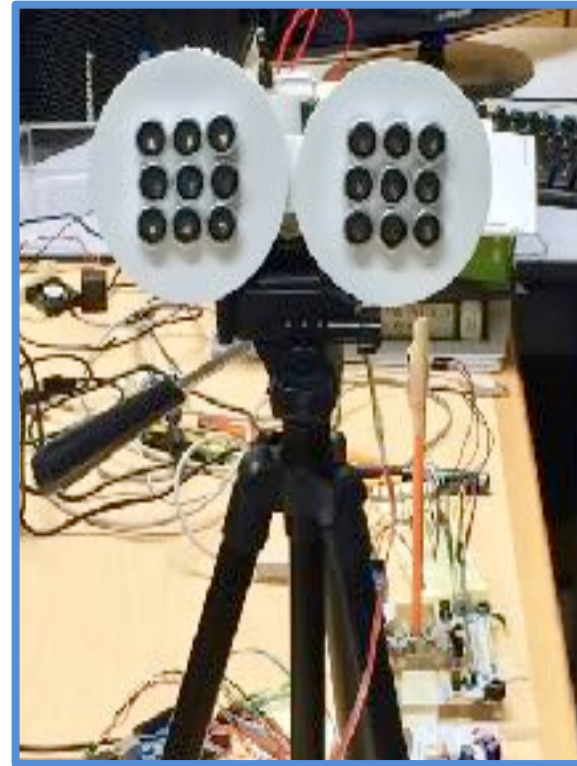


Laptop

Implementation

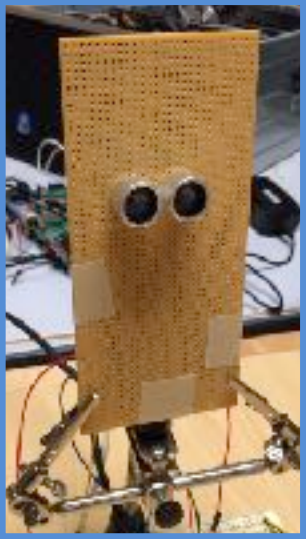


Communication
prototype



Jammer
prototype

Communication performance



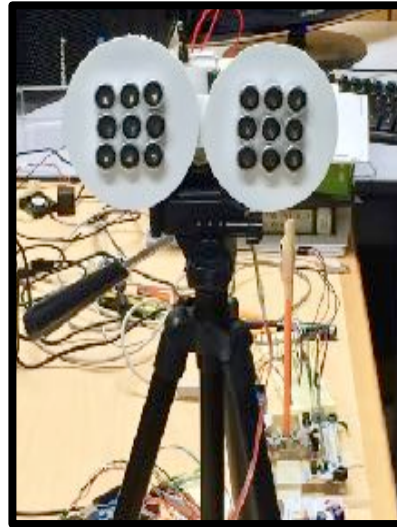
FM data packets

4kbps
up to 1 meter



More power can increase the distance

Jamming performance



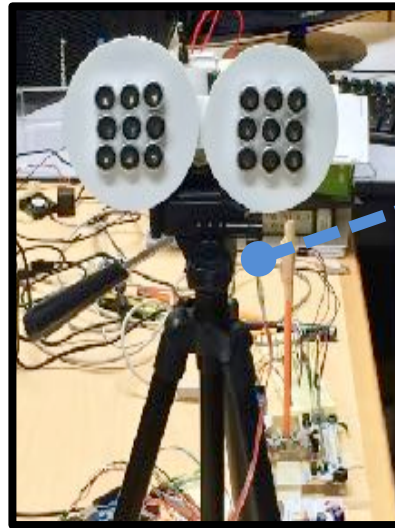
BackDoor jammer



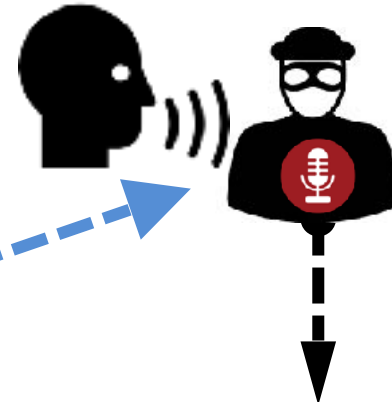
Spy
microphone

Jamming performance

2000 spoken words



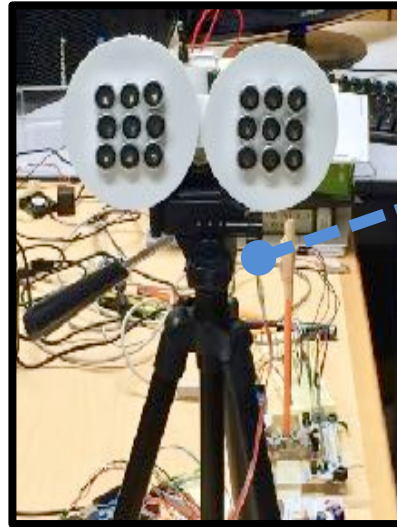
BackDoor jammer



Jammed recording

Jamming performance

2000 spoken words



BackDoor jammer



Jammed recording



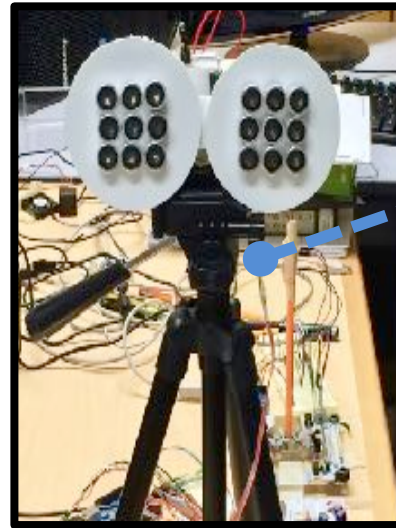
Human listener



Speech recognition

Jamming performance

2000 spoken words



BackDoor jammer



Jammed recording



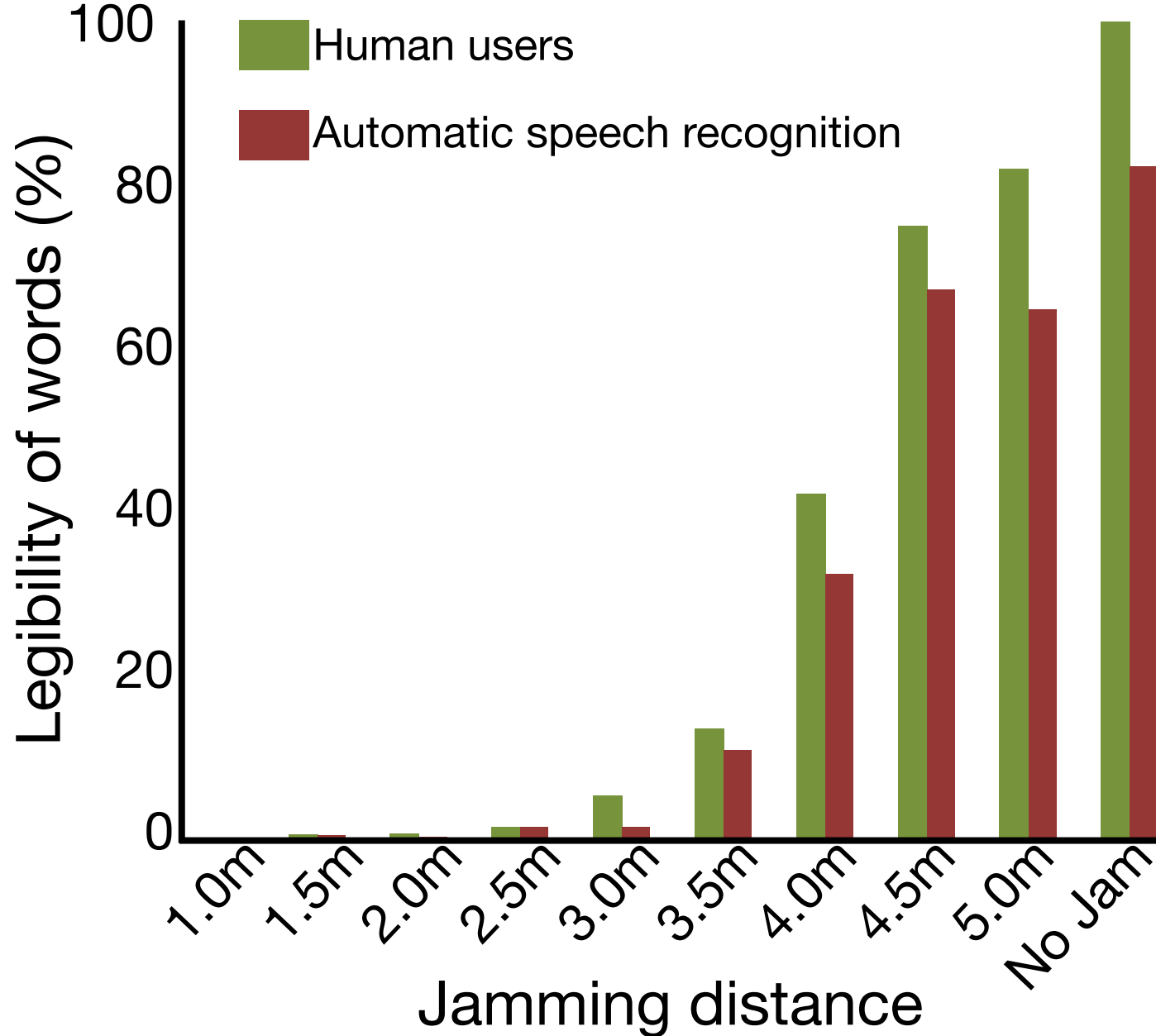
Human listener



Speech recognition

% of legible words

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?